Daniel Kliewe

Entwurfssystematik für den präventiven Schutz Intelligenter Technischer Systeme vor Produktpiraterie

Design framework for the preventive protection of Intelligent Technical Systems from product piracy

Bibliografische Information Der Deutschen Bibliothek
Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.ddb.de abrufbar.

Band 365 der Verlagsschriftenreihe des Heinz Nixdorf Instituts

ISSN (Print): 2195-5239
ISSN (Online): 2365-4422
ISBN: 978-3-942647-84-7

Satz und Gestaltung: Daniel Kliewe

Hersteller: readbox unipress in der readbox publishing GmbH
Münster

Printed in Germany

Geleitwort

Systems Engineering für den Entwurf Intelligenter Technischer Systeme ist die verbindende Leitidee des Heinz Nixdorf Instituts und des damit verbundenen Fraunhofer-Instituts Entwurfstechnik Mechatronik IEM.

Mechatronische Systeme beruhen auf dem engen Zusammenwirken unterschiedlicher Fachdisziplinen wie Maschinenbau, Elektro-, Regelungs- und Softwaretechnik. Auf Grundlage der Weiterentwicklung der Informations- und Kommunikationstechnik entstehen Intelligente Technische Systeme. Diese innovativen Systeme wecken große Begehrlichkeiten bei Imitatoren. Gleichzeitig entstehen neue Herausforderungen beim Schutz der Systeme. Auf der anderen Seite bietet die Informations- und Kommunikationstechnik große Potentiale zur Verbesserung des Systemschutzes. Ein wesentlicher Aspekt für die Umsetzung eines effektiven Systemschutzes ist die frühzeitige Berücksichtigung von Schutzmaßnahmen.

Vor diesem Hintergrund hat Herr Kliewe eine Entwurfssystematik für den präventiven Schutz Intelligenter Technischer Systeme vor Produktpiraterie entwickelt. In dieser werden die Anforderungen der Systeme an ihren Schutz aufgenommen. Darauf aufbauend werden wirksame Schutzmaßnahmen für Intelligente Technische Systeme herausgearbeitet. Weiterhin wird die Darstellung der Maßnahmen grundlegend überarbeitet, um so den Anforderungen des fachdisziplinübergreifenden Systementwurfs gerecht zu werden. Speziell für den imitationsgeschützten Entwurf liefert Herr Kliewe ein Vorgehensmodel und integriert so die Aspekte des Systemschutzes in die frühen Phasen der Systementwicklung.

Mit seiner Dissertation bewegt sich Herr Kliewe auf einem hochaktuellen und sehr herausfordernden Gebiet. Er integriert Forschungsgebiete, die bislang eher isoliert betrachtet wurden: Produktpiraterie und Schutz Intelligenter Technischer Systeme, Systems Engineering und musterbasierte Entwicklung Intelligenter Technischer Systeme. Anhand eines anspruchsvollen Validierungsbeispiels belegt Herr Kliewe zudem die Praxisrelevanz der Entwurfssystematik. Die Arbeit ist ein weiterer wichtiger Baustein für unsere Paderborner Schule des Entwurfs intelligenter technischer Systeme.

Paderborn, im Januar 2017

Prof. Dr.-Ing. J. Gausemeier Prof. Dr.-Ing. R. Dumitrescu

Entwurfssystematik für den präventiven Schutz Intelligenter Technischer Systeme vor Produktpiraterie

zur Erlangung des akademischen Grades eines
DOKTORS DER INGENIEURWISSENSCHAFTEN (Dr.-Ing.)
der Fakultät Maschinenbau
der Universität Paderborn

genehmigte
DISSERTATION

von
Dipl.-Ing. Daniel Kliewe
aus *Beckum*

Tag des Kolloquiums:	22. Dezember 2016
Referent:	Prof. Dr.-Ing. Jürgen Gausemeier
Korreferent:	Prof. Dr.-Ing. Frank-Lothar Krause

Vorwort

Die vorliegende Dissertation entstand während meiner Tätigkeit als wissenschaftlicher Mitarbeiter am Fraunhofer-Institut Entwurfstechnik Mechatronik IEM. Sie ist das Ergebnis meiner Arbeit im Rahmen von Forschungs- und Industrieprojekten.

Mein herzlicher Dank gilt Herrn Professor Dr.-Ing. Jürgen Gausemeier für die stets fordernde fachliche als auch persönliche Aus- und Weiterbildung in meiner Zeit als wissenschaftlicher Mitarbeiter. Ich danke ihm besonders für seinen persönlichen Einsatz bei der Betreuung meiner wissenschaftlichen Ausbildung.

Herrn Professor Dr.-Ing. Frank-Lothar Krause danke ich für die Übernahme des Korefe-rats.

Besonders danken möchte ich Herrn Professor Dr.-Ing. Roman Dumitrescu. Er stellte mich 2012 bei der damaligen Fraunhofer Projektgruppe ein und schenke mir großes Vertrauen, sowohl in meine Arbeit als auch in meine Person. Mit großer Dankbarkeit betrachte ich die zurückliegenden Jahre und die gemeinsamem Erlebnisse.

Ferner danke ich allen Arbeitskollegen für den Gemeinschaftsgeist und das angenehme Arbeitsklima. Für das konstruktive Feedback im Rahmen meiner Dissertation danke ich besonders: Katharina Altemeier, Dr.-Ing. Arno Kühn, Martin Rabe und Dr.-Ing. Harald Anacker. Darüber hinaus danke ich allen Studierenden, die mich bei meiner Arbeit durch ihre Abschlussarbeiten oder ihre studentische Hilfstätigkeit unterstützt haben.

Wesentliche Ergebnisse dieser Dissertation wurden innerhalb des Forschungsprojektes „Prävention gegen Produktpiraterie (3P)“ erarbeitet, das im Rahmen des Spitzenclusters Intelligente Technische Systeme OstWestfalenLippe (it's OWL) gefördert wurde. Dem ganzen 3P-Team danke ich für die angenehme und zielgerichtete Zusammenarbeit.

Meinem Freundeskreis danke ich für das Diskutieren der Dissertation und auch für die notwendige Unterstützung. Hervorheben möchte ich Erika Herbort, Johannes Stemmer und Sebastian Wigger.

Abschließend gilt mein herzlichster Dank meiner gesamten Familie, besonders bedanken möchte ich mich bei meinen Eltern, Gabi und Willi Kliewe, die mir das Abitur, das Studium sowie die Promotion ermöglichten. Sie unterstützten mich, wo immer sie konnten. Ein großer Dank geht auch an meinen Bruder Marcel Kliewe und seine Freundin Anna-Christin Langer, die mir durch unvergessliche Erlebnisse neue Motivation gaben.

Die größte Kraft und den größten Rückhalt erhielt ich durch meine Freundin Carolin Meermeier. Danke für dein Verständnis, dein Feedback und deine Liebe!

Paderborn, im Januar 2017 Daniel Kliewe

Liste der veröffentlichten Teilergebnisse

[PEK13] PETER, S.; ECKELT, D.; KLIEWE, D.: Gegen Produktpiraterie erfolgreich vorgehen. In: Maschinenbau und Metallbearbeitung Deutschland, Ausgabe August 2013, August 2013, S.44

[EAK14] ECKELT, D.; ALTEMEIER, K.; KLIEWE, D.: Präventiver Produktschutz – Ein ganzheitlicher Ansatz für die Bedrohungsanalyse. In: Industrie Management, GITO Verlag, Januar 2014, S.55-58

[KKD+15a] KLIEWE, D.; KÜHN, A.; DUMITRESCU, R.; GAUSEMEIER, J.: Challenges in Anti-Counterfeiting of Cyber-Physical Systems. In: WORLD ACADEMY OF SCIENCE, ENGINEERING AND TECHNOLOGY (Hrsg.): International Science Index 101 – International Journal of Social, Behavioral, Educational, Economic, Business and Industrial Engineering Vol: 9, No: 5, Tokyo, Mai 2015, S.3566-3573

[KKD+15b] KLIEWE, D.; KAISER, L.; DUMITRESCU, R.; GAUSEMEIER, J.: Approach for identifying components worthy of protection of Cyber-Physical Systems (CPS) based on a system model. In: Jurnal Teknologi (Sciences & Engineering) Vol: 76, No: 4, Bali, August 2015, S.7-11

[KAD+16] KLIEWE, D.; ANACKER, H.; DUMITRESCU, R.; WEGEL, A.: Model-based representation of protective measures as Solution Patterns. In: Procedia Technology Vol: 26, Paderborn, Mai 2016, S.341-348

Zusammenfassung

Die Unternehmen des deutschen Maschinen- und Anlagenbaus sowie verwandter Branchen entwickeln Intelligente Technische Systeme. Diese werden weltweit erfolgreich vermarktet, sie sind jedoch durch Produktpiraterie bedroht. Den Produktpiraten bieten sich zahlreiche Angriffsmöglichkeiten, um das Know-how der Systeme zu stehlen und so illegale Imitate anzufertigen. Diese Bedrohungen müssen bereits im fachdisziplinübergreifenden Systementwurf berücksichtigt werden.

Zur Sicherstellung des wirksamen Systemschutzes wird die *Entwurfssystematik für den präventiven Schutz Intelligenter Technischer Systeme vor Produktpiraterie* vorgestellt, die diesen bislang zu wenig beachteten Entwurfsaspekt im Zuge der Entwicklung Intelligenter Technischer Systeme abdeckt. Die Systematik besteht aus vier Bestandteilen. Die Grundlage bilden die Schutzanforderungen Intelligenter Technischer Systeme. Auf deren Basis werden wirksame Schutzmaßnahmen identifiziert. Um den Anforderungen des Systementwurfs zu begegnen wird die Darstellung der Maßnahmen grundlegend überarbeitet. Darüber hinaus wird ein Vorgehensmodell entwickelt. Durch die Systematik wird die Integration des präventiven Schutzes in den Systementwurf gewährleistet.

Die Validierung der Entwurfssystematik erfolgt anhand eines praxisnahen Beispiels. Hier wird die Neuentwicklung einer präventiv vor Produktpiraterie geschützten Landmaschine exemplarisch aufgezeigt.

Summary

German companies in the machine building and plant engineering industry as well as related industries develop Intelligent Technical Systems. These are sold worldwide, but they are threatened by imitation. There is a variety of possible attacks offered to the imitators to steal the system know-how and thereby manufacture illegal imitations. These threats need to be considered in the interdisciplinary system design.

To ensure the effective system protection the *design framework for the preventive protection of Intelligent Technical Systems from product piracy* has been introduced, which covers this so far undervalued design aspect in the course of the development of Intelligent Technical Systems. This framework consists of four elements. The basis is built on protection requirements of Intelligent Technical Systems. On their basis protective measures are identified. To encounter the requirements of the system design, the description of protective measures is revised. Also a procedure model is developed. The framework guarantees the integration of the preventive protection in the system design.

The validation of the design framework is executed according to a practical example. By this example, the new development of an agricultural machine that is preventively protected against imitation is shown.

Inhaltsverzeichnis

Seite

Anhang

Seite

1 Einleitung

Die vorliegende Arbeit ist im Rahmen der anwendungsorientierten Forschung am Fraunhofer-Institut Entwurfstechnik Mechatronik IEM in Paderborn entstanden. Im Fokus der Arbeit steht das Thema Schutz für Intelligente Technische Systeme (ITS) vor Produktpiraterie. Die wissenschaftliche Untersuchung des Themas war Gegenstand der Nachhaltigkeitsmaßnahme „Prävention gegen Produktpiraterie – Innovationen schützen“ (3P) im Rahmen des Spitzenclusters Intelligente Technische Systeme OstWestfalenLippe – kurz it's OWL. It's OWL ist ein vom Bundesministerium für Bildung und Forschung (BMBF) gefördertes Technologie-Netzwerk mit 174 Partnern aus Wirtschaft und Wissenschaft. In diesem werden Forschungsprojekte im Kontext ITS bearbeitet. Ziel der Nachhaltigkeitsmaßnahme 3P ist die Sensibilisierung der Unternehmen des Spitzenclusters hinsichtlich der Bedrohungen durch Produktpiraterie sowie die Befähigung, diesen wirksam zu begegnen. Aufgabe des Fraunhofer IEM ist hierbei die Sicherstellung des Schutzes Intelligenter Technischer Systeme. Dieser Herausforderung nimmt sich die vorliegende Arbeit an und beschreibt eine *Entwurfssystematik für den präventiven Schutz Intelligenter Technischer Systeme vor Produktpiraterie*.

1.1 Problematik

Die Produkte des Maschinen- und Anlagenbaus sowie verwandter Branchen befinden sich in der Weiterentwicklung von mechatronischen hin zu **Intelligenten Technischen Systemen**. Diese Systeme zeichnen sich durch die Vernetzung und daraus resultierenden Kommunikationsfähigkeiten, zunehmende Funktionsintegration sowie inhärente Teilintelligenz aus. Sie sind mit Hilfe vier zentraler Eigenschaften charakterisiert: adaptiv, robust, vorausschauend und benutzungsfreundlich. Aufgrund der neuartigen Eigenschaften besitzen die Systeme eine Reihe von Funktionen, die erstmalig in technischen Erzeugnissen umgesetzt werden. Bedingt durch die **Adaptivität** interagieren sie mit ihrem Umfeld und passen sich diesem autonom an. So können sie sich während der Laufzeit in einem vom Entwickler[1] vorausgedachten Rahmen weiterentwickeln. Unsicherheiten oder fehlende Informationen können durch die **Robustheit** bis zu einem gewissen Grad ausgeglichen werden. Ebenso bewältigen sie unerwartete und vom Entwickler nicht berücksichtigte Situationen in einem dynamischen Umfeld Die **Vorausschau** ermöglicht den Systemen auf Basis von Erfahrungswissen die künftigen Wirkungen von Einflüssen zu antizipieren. So werden Gefahren frühzeitig erkannt und passende Strategien zur Bewältigung ausgewählt. Die Systeme passen sich durch die **Benutzungsfreundlichkeit** dem Benutzerverhalten an und stehen in einer bewussten Interaktion mit diesem [Dum10], [GTD13].

[1] Die Inhalte der vorliegenden Arbeit beziehen sich gleichermaßen auf Frauen und Männer. Aus Gründen der besseren Lesbarkeit wird ausschließlich die männliche Form verwendet.

Die Erfolgschancen deutscher Unternehmen werden durch die negativen Auswirkungen von **Produktpiraterie** massiv bedroht. Produktpiraterie wird als Oberbegriff für das illegale Imitieren eines Systems und den Diebstahl von Know-how verwendet. Im Kontext Produktpiraterie wird zwischen Originalherstellern und Imitatoren unterschieden [Koe12a]. Zwingende Voraussetzung für eine führende Position Deutschlands im Bereich ITS ist, dass sich die Investitionen der deutschen Originalhersteller in die Erforschung und Entwicklung dieser innovativen Systeme rentieren. Die Rendite ist gefährdet, wenn die Innovationen schnell imitiert werden können. Die Imitatoren profitieren von den neuen Möglichkeiten der Intelligenten Technischen Systeme. Auf Basis der Systemvernetzung entsteht eine Vielzahl neuer Schnittstellen wie Verbindungen in die Cloud (also zu einem externen Rechenzentrum), Kommunikationsschnittstellen zu anderen Systemen oder Fernwartungszugänge. Die hieraus resultierenden neuen Angriffspunkte erleichtern es den Imitatoren das Know-how der Originalhersteller zu stehlen [BSI14b]. Aus diesem Grund ist die zentrale Herausforderung der *präventive Schutz Intelligenter Technischer Systeme vor Produktpiraterie*.

Zum Schutz des Know-hows, zur Angriffsabwehr und zur Erschwerung des Imitationsprozesses bieten sich eine Reihe von Maßnahmen an. Die Schutzmaßnahmen für ITS sind eigenständige komplexe Systeme. Diese müssen zudem auf interne Daten der Systeme zugreifen. Daher sind für den wirksamen Schutz Intelligenter Technischer Systeme die Maßnahmen als Teil des Systems zu integrieren. Dementsprechend ist der Zeitpunkt bei der Berücksichtigung der Schutzmaßnahmen von entscheidender Bedeutung. Nur durch eine frühzeitige Betrachtung im **fachdisziplinübergreifenden Systementwurf** wird die effektive und effiziente Umsetzung des präventiven Schutzes sichergestellt. Zentrale Herausforderung in der Systementwicklung ist ein frühzeitiges und disziplinübergreifendes Verständnis sowohl der Schutzmaßnahmen als auch der Systeme an sich. Ein potentieller Ansatz, um diesen Herausforderungen in geeigneter Weise zu begegnen, ist das Systems Engineering (SE).

Beim SE steht das ganzheitliche Systemdenken im Fokus. Durch dieses entsteht bei allen beteiligten Disziplinen ein einheitliches und ganzheitliches Systemverständnis [INC12]. Das Model-Based Systems Engineering (MBSE) unterstützt die an der Entwicklung beteiligten Mitarbeiter bereits während des Systementwurfs mit Hilfe eines Systemmodells. So wird das disziplinübergreifende Verständnis sichergestellt.

Voraussetzung für die Sicherstellung des *präventiven Schutzes Intelligenter Technischer Systeme vor Produktpiraterie* ist, dass wirksame Schutzmaßnahmen zur Verwendung im Systementwurf bereitstehen. Hierzu bedarf es der Analyse der Schutzanforderungen dieser Systeme, der Identifikation wirkungsvoller Schutzmaßnahmen, der grundlegenden Überarbeitung der Darstellung der Schutzmaßnahmen sowie der Verankerung der Aspekte des Systemschutzes im musterbasierten Entwurf Intelligenter Technischer Systeme. Es besteht demnach Handlungsbedarf für eine *Entwurfssystematik für den präventiven Schutz Intelligenter Technischer Systeme vor Produktpiraterie*.

1.2 Zielsetzung

Ziel der Dissertation ist eine *Entwurfssystematik für den präventiven Schutz Intelligenter Technischer Systeme vor Produktpiraterie*. Diese soll die Integration des Aspekts des Schutzes vor Produktpiraterie in den Systementwurf sicherstellen. Insbesondere für interdisziplinäre Entwicklungsteams soll die Berücksichtigung des Systemschutzes in den frühen Phasen der Entwicklung vereinfacht werden. So wird gewährleistet, dass sowohl der Know-how-Diebstahl verhindert als auch der Imitationsprozess erschwert wird. Mit Hilfe der entwickelten Systematik werden die Entwurfsaspekte wie Nachhaltigkeit, Benutzungsfreundlichkeit, Sicherheit, Resilienz oder Kosten um den Aspekt Schutz vor Produktpiraterie erweitert.

Die Systematik besteht aus insgesamt vier Bestandteilen. Die Grundlage der Systematik bilden die **Schutzanforderungen Intelligenter Technischer Systeme**. Diese müssen erfüllt sein, um den präventiven Systemschutz sicherzustellen. Zur bestmöglichen Erfüllung der Schutzanforderungen werden **wirksame Schutzmaßnahmen** identifiziert. Dies wird z. B. auf Grundlage der Untersuchung neuartiger Technologien forciert. Die **Darstellung der Schutzmaßnahmen** ist ein weiterer Bestandteil der vorliegenden Arbeit. Ein effektiver Schutz für ITS ist nur dann möglich, wenn der Aspekt des Schutzes bereits im Entwurf der Systeme Berücksichtigung findet. Hierfür müssen die bereitgestellten Schutzmaßnahmen so adaptiert werden, dass sie in den modellbasierten Systementwurf integriert werden können. Darüber hinaus muss es möglich sein, bereits erarbeitete Lösungen zum Schutz der Systeme wiederzuverwenden. Hier bieten Lösungsmuster das Potential, erfolgreich eingesetztes Wissen zu dokumentieren und erneut einzusetzen. Zur frühzeitigen Berücksichtigung des Systemschutzes wird abschließend ein Vorgehen zur **Integration des präventiven Schutzes in den musterbasierten Systementwurf** erarbeitet. Die einzelnen Bestandteile ergeben zusammen die *Entwurfssystematik für den präventiven Schutz Intelligenter Technischer Systeme vor Produktpiraterie*.

Durch die Erforschung und Vermarktung Intelligenter Technischer Systeme erarbeiteten sich die Originalhersteller Wettbewerbsvorteile. Die vorliegende Dissertation trägt wesentlich dazu bei, diese Vorteile möglichst lange zu erhalten. So kann die Rendite der Investitionen in Forschung und Entwicklung sichergestellt und der Innovationsstandort Deutschland gestärkt werden.

Die Anwendbarkeit der Systematik soll anhand eines Anwendungsbeispiels validiert werden. Dazu wird exemplarisch die Entwicklung eines Mähdreschers betrachtet.

1.3 Vorgehensweise

In **Kapitel 2** wird zunächst die Problemanalyse aufgezeigt. Hier wird das Forschungsfeld der Arbeit definiert. Darüber hinaus werden relevante Begriffe erläutert. Weiterhin werden die Grundlagen zu den Themen ITS, Produktpiraterie und fachdisziplinübergrei-

fender Entwurf dargelegt. Aufgrund der Weiterentwicklung von mechatronischen hin zu vernetzen Systemen mit inhärenter Teilintelligenz ergeben sich sowohl für den Schutz der Systeme als auch für deren Entwicklung neue Herausforderungen. Diese werden untersucht und aufgezeigt. In der Problemabgrenzung sind die wesentlichen Handlungsfelder der vorliegenden Arbeit zusammengefasst. Die Problemanalyse schließt mit der Ableitung von Anforderungen an die angestrebte *Entwurfssystematik*.

Die Anforderungen werden in **Kapitel 3** mit dem Stand der Technik verglichen. Zuerst werden bestehende Schutzmaßnahmen betrachtet. Hier sind einige Sammlungen von Maßnahmen zum Schutz gegen Produktpiraterie aufgeführt. Ebenfalls werden bestehende Ansätze zum Entwurf präventiv imitationsgeschützter Systeme untersucht. Um die Entwicklung innovativer Systeme zu ermöglichen, sind sowohl Modellierungstechniken, als auch interdisziplinäre Entwurfsmuster[2] notwendig. Die Modellierungstechniken dienen der ganzheitlichen und disziplinunabhängigen Darstellung der Systeme. Muster ermöglichen die Wiederverwendung von bereits vorhandenem Lösungswissen. Die Analyse des Stands der Technik wird fortgesetzt durch die Untersuchung von Ansätzen zum musterbasierten Entwurf Intelligenter Technischer Systeme. Den Abschluss des Kapitels bildet eine Gegenüberstellung der untersuchten Ansätze mit den in Kapitel 2 ermittelten Anforderungen. Es wird ersichtlich, dass dringender Handlungsbedarf in Form der Ausarbeitung der angestrebten *Entwurfssystematik* besteht.

Kapitel 4 beinhaltet eine detaillierte Beschreibung der *Entwurfssystematik*. Es stellt den Kern der vorliegenden Arbeit dar. Zunächst wird ein Überblick über die Bestandteile der Systematik und ihr Zusammenwirken gegeben. Anschließend werden die Schutzanforderungen Intelligenter Technischer Systeme identifiziert. Für die Verbesserung des Schutzes der intelligenten Systeme werden wirksame Schutzmaßnahmen bestimmt. Um den Einsatz der Schutzmaßnahmen in den frühen Phasen der Entwicklung zu ermöglichen, wird die bisherige Darstellung der Schutzmaßnahmen grundlegend überarbeitet. Die Resultate fließen in das Vorgehen zur Integration des präventiven Schutzes in den musterbasierten Entwurf Intelligenter Technischer Systeme ein und komplettieren die *Entwurfssystematik*.

In **Kapitel 5** wird die entwickelte Systematik anhand eines praxisbezogenen Anwendungsbeispiels validiert. Das Beispiel ist so gewählt, dass die Erfüllung der aufgestellten Anforderungen sowie der Nutzen der *Entwurfssystematik* überprüft werden können.

Kapitel 6 fasst die Ergebnisse der Arbeit zusammen und zeigt den Ausblick auf zukünftige Forschungsfelder auf. Der **Anhang** enthält ergänzende Informationen zur vorliegenden Arbeit.

---

[2] Ein Muster beschreibt ein Problem sowie den Kern der Lösung für dieses Problem [AIS+77].

2 Problemanalyse

Ziel der Problemanalyse ist die Identifikation von Anforderungen an die *Entwurfssystematik für den präventiven Schutz Intelligenter Technischer Systeme vor Produktpiraterie*. In Kapitel 2.1 werden die hierfür wesentlichen Begriffe definiert und die Ausrichtung der Arbeit beschrieben. Das Kapitel 2.2 beschreibt ITS und deren Eigenschaften. Anschließend wird das Themenfeld Produktpiraterie sowie die Herausforderungen für den Schutz Intelligenter Technischer Systeme in Kapitel 2.3 analysiert. In Kapitel 2.4 liegt der Schwerpunkt auf dem fachdisziplinübergreifenden Systementwurf. Hier werden moderne Entwurfsmethodiken für ITS beschrieben und deren Herausforderungen skizziert. Kapitel 2.5 umfasst eine Problemabgrenzung und stellt die Handlungsfelder dar. Das Resultat der Problemanalyse sind die beschriebenen Anforderungen an die zu entwickelnde Systematik in Kapitel 2.6.

2.1 Begriffserläuterungen und Ausrichtung der Arbeit

Ziel der vorliegenden Arbeit ist eine *Entwurfssystematik*, die den *präventiven Schutz Intelligenter Technischer Systeme vor Produktpiraterie* sicherstellt. Hieraus lassen sich drei Begriffe ableiten, die zu erläutern sind: Entwurfssystematik, ITS und Produktpiraterie.

Der Begriff **Entwurfssystematik** setzt sich aus zwei Bestandteilen zusammen. Im Rahmen der Produktentstehung umfasst der *Entwurf* die Festlegung eines fachdisziplinübergreifenden Lösungskonzepts [VDI2206]. Dies wird auch als Systementwurf oder als Konzipierung bezeichnet. Der Entwurf enthält alle wesentlichen physikalischen und logischen Wirkungsweisen des zukünftigen Produkts bzw. Systems[3]. Der Begriff *Systematik* wird insbesondere in der Biologie verwendet. Dort beschreibt er die systematische Benennung und Bestimmung von Lebewesen und Pflanzen [LL06]. Im Duden wird eine Systematik definiert als die:

> *„planmäßige, einheitliche Darstellung, Gestaltung nach bestimmten Ordnungsprinzipien“ [Bib15-ol].*

Im technischen Zusammenhang wird eine Konstruktionssystematik nach HANSEN definiert als:

> *„[…] das planmäßige, wissenschaftliche Kombinieren der Einzelerkenntnisse der Technik zum Aufbau eines technischen Gebildes“ [Han55, S.36].*

---

[3] *„Ein System ist eine in einem betrachteten Zusammenhang gegebene Anordnung von Elementen, die miteinander in Wechselwirkung stehen. Diese Anordnung wird aufgrund bestimmter Vorgaben von ihrer Umgebung abgegrenzt“ [DIN19226].*

Abgeleitet aus der Herleitung von DUMITRESCU (vgl. [Dum10, S.6]) beschreibt die *Entwurfssystematik für den präventiven Schutz Intelligenter Technischer Systeme vor Produktpiraterie* ein Rahmenwerk, das ein Vorgehensmodell sowie Hilfsmittel zur erfolgreichen Umsetzung des Entwurfs präventiv geschützter Systeme bereitstellt. Das Vorgehensmodell strukturiert den Entwurf Intelligenter Technischer Systeme nach aufgabenspezifischen Gesichtspunkten. Hilfsmittel können z. B. Methoden, Spezifikations-/Modellierungstechniken oder Lösungsmuster[4] sein.

ITS sind innovative, hochgradig komplexe Systeme. Sie sind mit ihrer Umwelt vernetzt und zeichnen sich insbesondere durch inhärente Teilintelligenz aus [its12]. Somit sind die Systeme in der Lage sich ihrer Umgebung und den Wünschen der Anwender anzupassen, Nutzen zu stiften sowie Ressourcen zu sparen. Darüber hinaus sind sie intuitiv zu bedienen und verlässlich [GAC+13]. Der deutsche Maschinen- und Anlagenbau sowie verwandte Branchen beeinflussen die Entwicklung der Systeme maßgeblich. Die Branchen werden sich langfristig durch die Weiterentwicklung von mechatronischen zu vernetzen Systemen mit inhärenter Teilintelligenz verändern (vgl. [its12], [VDM14b]).

In der vorliegenden Arbeit werden Begriffe im Kontext **Produktpiraterie** verwendet, die nicht intuitiv voneinander abgegrenzt werden können wie Wissen und Know-how oder Imitation und Plagiat. Zur Sicherstellung des einheitlichen Verständnisses, werden im Folgenden die für die Ausarbeitung wichtigsten Begriffe erläutert.

Unter dem Oberbegriff Geistiges Eigentum wird allgemein alles **Wissen**[5] eines Menschen verstanden [Spr15-ol]. In der Wirtschaft wird oft der englische Begriff Intellectual Property (IP) verwendet. Nach der WORLD INTELLECTUAL PROPERTY ORGANIZATION (WIPO) gliedert sich IP in Schutzrechte und Urheberrechte [WIP08]. Durch Urheberrechte wird die schöpferische Leistung einer natürlichen Person automatisch geschützt. Das Urheberrecht entsteht mit der Schöpfung eines Werkes und bedarf keiner Anmeldung [Lor12]. Im Gegensatz dazu müssen Schutzrechte angemeldet werden. Schutzrechte sind z. B. Patente und Gebrauchsmuster. Diese geben dem Schutzrechtsinhaber für einen begrenzten Zeitraum das Recht zur ausschließlichen Nutzung seiner Erfindung [Nee07]. MITTELSTAEDT erweitert die Definition von IP um die Aspekte Betriebsgeheimnisse, Know-how, Lizenzen etc. Er stellt heraus, dass IP einem Unternehmen Wettbewerbsvorsprünge gegenüber der Konkurrenz ermöglicht. Dennoch wird der Schutz des Unternehmenswissens (IP) in vielen Firmen vernachlässigt. Es fehlen der Wille sich mit dem Thema zu befassen sowie ein systematischer Schutzansatz [Mit09].

---

[4] vgl. Kapitel 2.4.5

[5] *„Wissen bezeichnet die Gesamtheit der Kenntnisse und Fähigkeiten, die Individuen zur Lösung von Problemen einsetzen. Dies umfasst sowohl theoretische Erkenntnisse als auch praktische Alltagsregeln und Handlungsanweisungen. Wissen stützt sich auf Daten und Informationen, ist im Gegensatz zu diesen jedoch immer an Personen gebunden. Wissen entsteht als individueller Prozess in einem spezifischen Kontext und manifestiert sich in Handlungen“ [PRR06, S.40].*

Unternehmenswissen kann in unterschiedlichsten Arten vorliegen, z. B. Wissen der Mitarbeiter, Wissen, welches in Patenten enthalten ist, oder Wissen in Prozessen. Das unterschiedliche Wissen muss mit individuellen Maßnahmen geschützt werden. Ausgewählte Maßnahmen, wie der Schutz durch Betriebsgeheimnisse, Patente, Lizenzen oder auch vereinzelte technische Maßnahmen, sind in den meisten Unternehmen (wenn auch oft lückenhaft) bereits vorhanden (vgl. [VDM14a], [VDM16]).

Ein großer Teil des Unternehmenswissens steckt in den Produkten des Unternehmens wie Aufbau oder Funktionsweise des Produktes, eingesetzte Materialien oder Soft- und Firmware. **Produktgebundenes Wissen** wird von LINDEMANN ET AL. abstrahiert als artefaktgebundenes Wissen wie folgt definiert:

> *„Artefaktgebundenes Wissen ist in Produkten oder Komponenten hinterlegt. Durch die Geschäftsmodelle der Investitionsgüterindustrie muss alles artefaktgebundene Wissen beim Verkauf von Maschinen und Ersatzteilen an eine unkontrollierbare Öffentlichkeit übergeben werden“ [LMP+12a, Glossar].*

Dieses produktgebundene oder auch systeminhärente Wissen wird von vorhandenen (technischen) Schutzmaßnahmen nicht vollständig geschützt und ist somit ungeschützt in den Produkten vorhanden. Das illegale Extrahieren des Wissens aus den Produkten ist die Hauptursache für Imitationen [VDM14a, S.14], [VDM16, S.18]. Der Schutz des systeminhärenten Wissens steht daher im Fokus der zu entwickelnden Systematik.

Der Begriff **Know-how** steht in enger Verbindung mit dem Begriff Wissen und wird als eine spezielle Form von Wissen verstanden [OEC96]. Know-how stellt nach SCHNAPAUFF das Handlungswissen dar. Mit dem Begriff Handlung ist in diesem Zusammen die Art des Wissens gemeint „*wie man etwas tut*“ [Sch09, S.81]. Da es in dieser Arbeit um technische Systeme geht, wird hier die technisch orientierte Know-how-Definition von SAUTER und BUNTE verwendet:

> *„Know-how ist die Summe des technischen Wissens, über das ein Unternehmen zur Herstellung eines bestimmten Produkts oder für ein Verfahren verfügen kann“ [SB89].*

Angelehnt an die Definition des Know-hows wird der Begriff **Lösungswissen** abgegrenzt. Lösungswissen beschreibt die Gesamtheit des technischen und methodischen Wissens, über das ein Unternehmen zur Herstellung eines Produktes verfügt [Ana15].

Ein Originalhersteller kann sich durch Know-how und damit verbundene innovative Produkte Alleinstellungsmerkmale gegenüber seinen Wettbewerbern erarbeiten. Mit Hilfe von Know-how-Diebstahl kann ein Imitator die Innovation zeitnah nachbauen. So geht das Alleinstellungsmerkmal des Originalherstellers bereits kurze Zeit nach Markteinführung des Originals verloren [Kle13, S.23ff.].

Vergehen wie Know-how-Diebstahl, Fälschungen und Plagiate werden als **Produktpiraterie** bezeichnet und gelten als „*das Verbrechen des 21. Jahrhunderts*“ [KA11, S.3]. VOIGT ET AL. definieren Produktpiraterie aufbauend auf der Arbeit von MEISTER als:

> *„[…] das gezielte illegale Kopieren der Leistung (engerer Pirateriebegriff) als auch das ‚Schmarotzen am Image der Marke‘ sowie die Übernahme von Ideen des Innovators (weiter Pirateriebegriff)“ [VBS08, S.89] aufbauend auf [Mei90, S.34].*

In der vorliegenden Arbeit wird der **engere Pirateriebegriff** betrachtet. Der technische Schutz des produktinhärenten Know-hows sowie der Kopierschutz (bzw. Plagiatsschutz) für technische Systeme stehen im Fokus der Arbeit. Hierzu werden produktbezogene Schutzmaßnahmen forciert. Diese gliedern sich in kennzeichnende und informationstechnische Schutzmaßnahmen (vgl. Bild 2-8). Aufgrund der Fokussierung auf den technischen Schutz des systeminhärenten Wissens werden der rechtliche Schutz sowie die Geheimhaltung des Unternehmenswissens nicht explizit berücksichtigt.

Im Themenfeld Produktpiraterie existieren unterschiedliche Begriffe zur Abgrenzung und Beschreibung von Nachahmungen. Im Fall von **Imitationen** werden Produkteigenschaften teilweise oder vollständig nachgeahmt. Ein Imitat ist legal, wenn der Originalhersteller keine Schutzrechte besitzt. Dies kann nur unter moralischen Gesichtspunkten betrachtet werden. **Fälschungen** oder **Markenpiraterie** sind regelmäßige Verletzungen von nichttechnischen gewerblichen Schutzrechten wie Marken oder Geschmacksmustern. **Plagiate** verletzen im Gegensatz dazu technische gewerbliche Schutzrechte wie Patente oder Gebrauchsmuster. Der Schutz vor Plagiaten steht im Fokus der vorliegenden Arbeit. **Vertragsverstöße** betreffen Verträge zwischen Partnern, z. B. können Lizenzverträge durch Überproduktion gebrochen werden (vgl. Bild 2-1) [Koe12b].

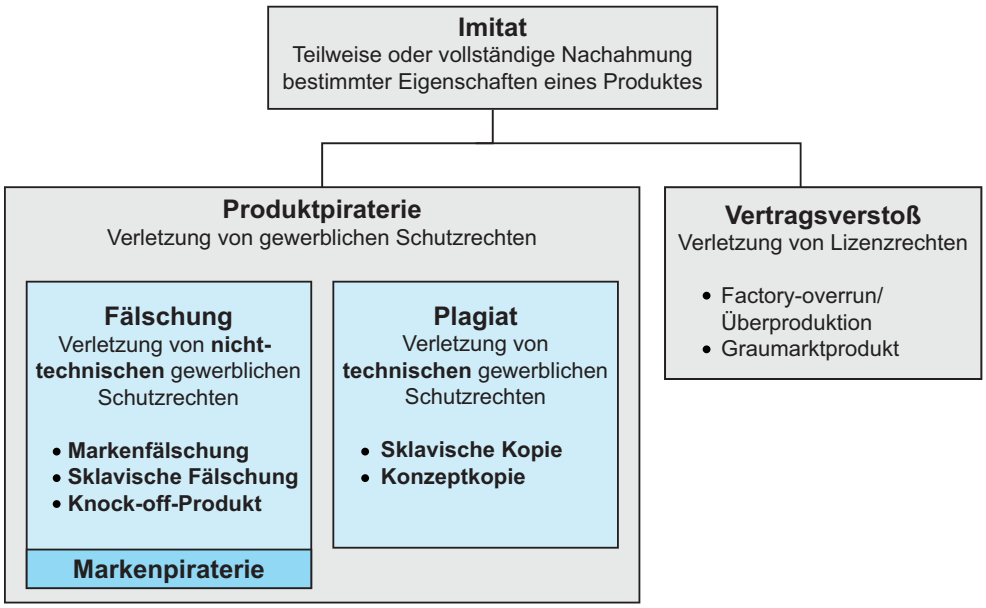


Bild 2-1: Kategorien von Imitaten nach KÖSTER [Koe12a]

Originalhersteller, Kunden und Plagiatoren zählen zu den Stakeholdern im Bereich Produktpiraterie. Sicherer Verlierer durch Know-how-Verlust und Imitate sind die Originalhersteller. Sie werden nicht nur um die Rendite ihrer Innovationen gebracht, sondern müssen sich ggf. auch mit den Mängeln von Imitaten auseinandersetzen und Schadensersatz leisten. Die Kunden zählen ebenfalls zu den Verlierern, da sie getäuscht und benachteiligt werden. Getäuscht sind sie, wenn sie ein Imitat erwerben, das sie für ein Originalprodukt halten. Einen Nachteil erfahren sie, wenn das Preis-Leistungs-Verhältnis nicht ihren Erwartungen entspricht, da z. B. wichtige Funktionen fehlen. Ernsthafte Gefahr besteht, wenn sicherheitsrelevante Eigenschaften nicht vorhanden oder nicht ausreichend sind. In diesem Fall kann eine Gefährdung von Personen und Gesundheit vorliegen. Die Plagiatoren zählen zu den Gewinnern. Sie erwirtschaften mit Leichtigkeit große Gewinne, können ihr Know-how aufstocken und so ggf. zu neuen, legalen Wettbewerbern werden [Koe12a].

Typischerweise versucht ein Originalhersteller mit Hilfe von Innovation seinen Vorsprung gegenüber den Wettbewerbern zu sichern. Nach KLEINE beginnt ein regulärer Imitator ab dem Zeitpunkt der Markteinführung mit dem Imitationsprozess. Ein Plagiator zeichnet sich dadurch aus, dass er sich bereits vor der Markteinführung das Know-how durch Diebstahl aneignet. Dies geschieht oft noch während sich die Innovation in der Entwicklung befindet. Auf Grundlage des illegal erworbenen Know-hows kann der Plagiator bereits frühzeitig mit dem Imitationsprozess starten. Die Komplexität in der Entwicklung wird stark verringert, da die Lösungen des Originalsystems nachgebaut oder übernommen werden können. Auf Basis des Know-how-Diebstahls wird der Imitationsprozess zusätzlich verkürzt. So kann das Plagiat kurz nach Markteinführung des Originalsystems angeboten werden [Kle13, S.88ff.]. Diese Verkürzung des Innovationsvorsprungs ist in Bild 2-2 dargestellt.

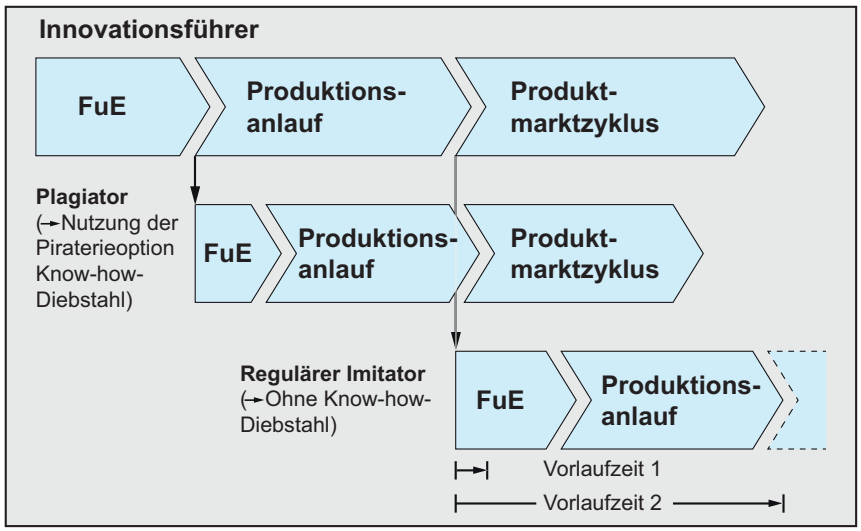


Bild 2-2: Verkürzung des Innovationsvorsprungs durch Produktpiraterie nach KLEINE [Kle13, S.92]

Festzuhalten bleibt, dass ganz gleich welche Art von rechtlich oder moralisch unerlaubtem Nachbau auftritt, der Schaden immer beim Originalhersteller sowie häufig auch beim Kunden liegt und Verlust von Image und Umsatz, Ärger, Frust sowie unter Umständen Gefahr für Leib und Leben bedeutet.

Dieser Schaden wird sich zukünftig weiter erhöhen, da ITS große Begehrlichkeiten wecken und zahlreiche Angriffsmöglichkeiten bieten. Aufgrund der Vernetzung der Systeme entsteht eine neue Angriffsform, sog. **Cyberattacken oder -angriffe** [BSI14a], [BRW15]. Durch Cyberattacken können Hacker von außen auf das System zugreifen und Schaden anrichten. Der Zugriff geschieht über Verbindungen zum Internet oder Kommunikationsverbindungen zwischen den Systemen. Der Fokus der vorliegenden Arbeit liegt auf dem technischen, präventiven Schutz der Systeme vor Know-how-Diebstahl und unerlaubtem Nachbau. Aus diesem Grund werden Cyberattacken ausschließlich als Angriff auf das systeminhärente Know-how verstanden. Die Möglichkeiten der Manipulation (durch das Einschleusen von Schadcode) werden nicht betrachtet.

Die Arbeit ist auf die Entwicklung einer *Entwurfssystematik für den präventiven Schutz Intelligenter Technischer Systeme vor Produktpiraterie* ausgerichtet. So sollen das Know-how in den Systemen präventiv gesichert und die Systeme per se vor unerlaubtem Nachbau geschützt werden. Durch Cloud Computing werden zunehmend systeminhärente Daten ausgelagert. So wird die Trennung von internen und externen Systemdaten immer schwieriger. Für einen effektiven Schutz müssen auch extern gelagerte Systemdaten gesichert werden. Nicht berücksichtigt wird der Schutz von Unternehmenswissen, welches bspw. in Dokumenten oder Dateien gespeichert ist. Ebenso wird das Ausspionieren der Mitarbeiter (Social Engineering) nicht berücksichtigt.

Aufgrund des Technologiesprungs sowie neuer Angriffsformen, z. B. Cyberattacken, entstehen besondere Herausforderungen an den Schutz vernetzter Systeme. Aus den Herausforderungen lassen sich konkrete Anforderungen ableiten. Diese werden als **Schutzanforderungen Intelligenter Technischer Systeme** bezeichnet.

Die erarbeitete Systematik soll in der Praxis die Systementwickler in die Lage versetzen, präventiv geschützte ITS zu entwickeln. Die Aspekte des Schutzes werden hierfür fachdisziplinübergreifend beschrieben und in etablierte Standards des Systementwurfs (vgl. Kap. 2.4) integriert. Anhand der überarbeiteten Darstellung der Maßnahmen (vgl. Kap. 4.4) wird zudem die Wiederverwendung von Lösungswissen ermöglicht.

2.2 Intelligente Technische Systeme

Moderne mechatronische Systeme beruhen auf dem synergetischen Zusammenwirken unterschiedlicher Fachdisziplinen wie Maschinenbau, Elektro-, Regelungs- und Softwaretechnik [KFG07, S.35]. Sie sind Erzeugnisse des Maschinen- und Anlagenbaus sowie verwandter Branchen, z. B. der Automobil- oder Luftfahrtindustrie [VDI2206]. Bedingt durch die zunehmende Digitalisierung entwickeln sich mechatronische Systeme zu ver-

netzten und intelligenten Systemen. Die sog. Intelligenten Technischen Systeme vollziehen einen Innovationssprung und werden sich künftig deutlich vom aktuellen Stand der Technik unterscheiden. Der Einsatz innovativer Technologien und das Zusammenspiel zahlreicher (zum Teil auch fachfremder) Disziplinen ermöglichen diesen Innovationssprung. Insbesondere im Maschinen- und Anlagenbau werden die Innovationen größtenteils durch die fachfremden Disziplinen angeregt. Informationstechnologie und nichttechnische Disziplinen wie Verhaltens-, Sprachwissenschaften oder Neurobiologie bringen neue Aspekte in die Entwicklung ein. Mit Hilfe von Sensoren, Aktoren und kognitiven Funktionen werden die Systeme lernfähig und können sich ihrer Umwelt sowie den Wünschen des Benutzers anpassen [its12], [GTD13]. In den folgenden Abschnitten werden die Grundlagen mechatronischer Systeme erläutert sowie die Eigenschaften Intelligenter Technischer Systeme beschrieben.

2.2.1 Grundstruktur mechatronischer Systeme

Die bei mechatronischen Systemen zugrunde liegende Struktur besteht in der Regel aus einem Grundsystem, Sensoren, Aktoren und einer Informationsverarbeitung [KFG07, S.38]. Auf das System wirken verschiedene Einflüsse, z. B. der Mensch über die Mensch-Maschine-Schnittstelle oder die Umgebung. Diese Grundstruktur ist in Bild 2-3 dargestellt und wird im Folgenden erläutert [VDI2206].

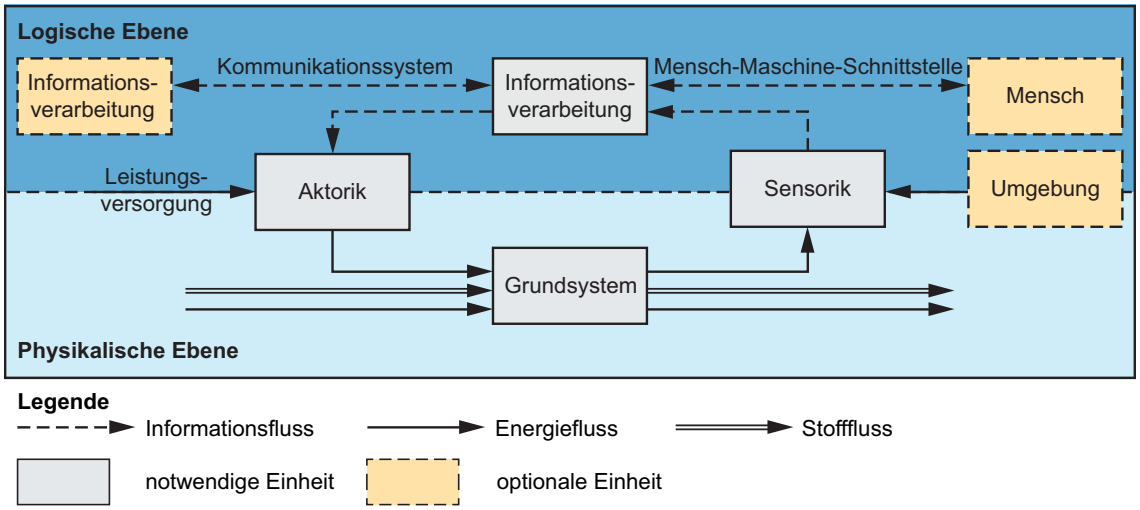


Bild 2-3: Grundstruktur eines mechatronischen Systems nach [VDI2206, S.14]

Grundsystem: Das Grundsystem ist das Kernelement der physikalischen Ebene. Es stellt eine mechanische, elektromechanische, hydraulische oder pneumatische Struktur oder eine Kombination aus diesen dar.

Sensorik: Die Sensoren erfassen die Zustandsgrößen des mechatronischen Systems. Zusätzlich identifizieren sie die Einflüsse der Umgebung.

Informationsverarbeitung: Die von der Sensorik aufgenommenen Eingangsgrößen werden zur Informationsverarbeitung übermittelt. Diese bestimmt die Einwirkungen auf

das Grundsystem. Hierdurch können dessen Zustandsgrößen in gewünschter Weise beeinflusst werden. Die Informationsverarbeitung muss nicht nur interne Informationen des Systems berücksichtigen, sondern auch externe. Diese werden über externe Schnittstellen ermittelt und können z. B. Informationen anderer Systeme oder des Benutzers sein.

Aktorik: Hier erfolgt die Umsetzung der Einwirkungen direkt am Grundsystem. Dies geschieht auf Basis der Beeinflussung der Zustandsgrößen.

Die Elemente des Systems sind durch Flüsse verbunden. Diese unterteilen sich in Stoff-, Energie- und Informationsflüsse (vgl. Kap. 3.3.1, Tabelle 3-2) [PBF+07, S.43].

Zusammenfassend weisen mechatronische Systeme eine sehr hohe **Komplexität** auf. Diese resultiert aus der steigenden Anzahl von verkoppelten Elementen. Die Elemente müssen im Rahmen der Ausarbeitung zwischen verschiedenen Fachdisziplinen konkretisiert werden (Heterogenität). Hinzu kommen die Wechselwirkungen zwischen den Elementen, die sich auf die Komplexität eines Systems auswirken. Weiter werden immer mehr Funktionen aus unterschiedlichen Disziplinen in ein System integriert, wodurch die Komplexität ansteigt [BHL07-ol, S.8], [VDI2206, S.4]. Die Folge ist, dass der Umgang mit und die Beherrschung der Komplexität eine zentrale Herausforderung in der Entwicklung mechatronischer Systeme darstellt. Um einen Überblick über die Variantenvielfalt der Systeme zu erlangen wird im Folgenden deren Klassifizierung beschrieben.

2.2.2 Klassen mechatronischer Systeme

GAUSEMEIER ET AL. teilen mechatronische Systeme in drei Klassen ein. Diese sind in Bild 2-4 dargestellt.

Bild 2-4: Klassen mechatronischer Systeme [GAC+13]

Klasse 1: Die *räumliche Integration von Mechanik und Elektronik* hat als Ziele die Miniaturisierung, Funktionsintegration, höhere Zuverlässigkeit sowie geringere Herstellkosten. Die Systeme sind in der Aufbau- und Verbindungstechnik zu finden [GAC+13].

Klasse 2: Solche Systeme werden als *Mehrkörpersysteme mit kontrolliertem Bewegungsverhalten* bezeichnet. Der Fokus liegt auf der Verbesserung der Verhaltensweise. Sie können selbstständig auf Veränderungen in der Umgebung reagieren [GAC+13].

Klasse 3: *Intelligente, vernetzte Systeme* stellen die Weiterentwicklung mechatronischer Systeme dar. Sie entstehen durch die Evolution von Informations- und Kommunikationstechniken und deren Integration in technische Systeme [Dum10].

Im Rahmen der vorliegenden Arbeit ist es erforderlich, die Systeme der Klasse 3 detailliert zu untersuchen. Die Untersuchung ist im folgenden Abschnitt beschrieben.

2.2.3 Eigenschaften Intelligenter Technischer Systeme

Systeme der Klasse 3 entstehen anhand des Innovationssprungs von mechatronischen hin zu vernetzten Systemen mit inhärenter Teilintelligenz. Diese Systeme werden als **ITS** bezeichnet. Nach DUMITRESCU wird die Entwicklung dieser Systeme durch vier allgemeine Technologie-Trends ermöglicht [Dum10, S.1]:

Miniaturisierung der Elektronik: Die Miniaturisierung ermöglicht die Entwicklung geeigneter Hardware für ITS. Dies geschieht in Verbindung mit der Parallelisierung der Informationsverarbeitung durch Multikernprozessoren, der Steigerung der Speicherkapazität und der Reduzierung des Energiebedarfs [HS09], [aca11].

Softwaretechnologie als Innovationstreiber: Moderne maschinenbauliche Erzeugnisse werden zunehmend mit Software durchdrungen. Hierdurch werden innovative Funktionen ermöglicht [DAB+10], [SW07].

Vernetzung von Informationssystemen: Die Vernetzung geschieht mit dem Ziel, Systeme des physischen Alltags in der virtuellen Welt zu integrieren. So sind aktuelle Forschungsfelder entstanden, die sich mit der elektronischen, größtenteils drahtlosen Vernetzung von informationsverarbeitenden Systemen befassen. Damit wird die weltweite Nutzung von Daten und Diensten ermöglicht. Auf Grundlage der Vernetzung entstehen komplexe Abhängigkeiten zwischen Systemen, Informationsnetzen und Menschen über die gesamte Wertschöpfung hinweg [Bro10], [Gro15], [Her15].

Fortgeschrittene Mechatronik: Die Leistungsfähigkeit mechatronischer Systeme geht über die mechanischer Systeme deutlich hinaus und basiert auf dem engen Zusammenwirken verschiedener Fachdisziplinen (vgl. Kap. 2.2). Aufgrund der Digitalisierung und der damit verbundenen zunehmenden Durchdringung mit Informations- und Kommunikationstechnik werden intelligente Systeme realisierbar. Diese verfügen über Eigenschaften wie Selbstoptimierung, Selbstkoordination oder Selbstheilung [Trä09, S.4], [GB12].

Eine weitere Voraussetzung für den Innovationssprung ist das Zusammenwirken verschiedener Disziplinen wie die Symbiose von Informatik und Ingenieurswissenschaften und der daraus resultierenden Verwendung von Techniken der künstlichen Intelligenz[6]. Durch die Integration von Sensoren und Aktoren können die Systeme ihre Umwelt wahrnehmen. Unter Einbeziehung nichttechnischer Disziplinen wie Verhaltens-, Sprachwissenschaften oder Neurobiologie können zudem eigenständige Anpassungen der intelligenten Systeme realisiert werden [GDJ+14], [its12].

ITS zeichnen sich durch vier charakteristische Eigenschaften aus. Sie sind adaptiv, robust, vorausschauend und benutzungsfreundlich (vgl. Kap. 1.1) [Dum10].

Um die beschriebenen Eigenschaften zu realisieren, wird die Grundstruktur des mechatronischen Systems zu einem kognitiven[7] System weiterentwickelt. Die vorhandenen Wirkungsabläufe werden erweitert und nicht ersetzt [Str98], [GAC+13], [GTD13].

Mit Hilfe der Integration kognitiver Funktionen[8] sollen ITS in die Lage versetzt werden, intelligent und flexibel auf veränderte Betriebsbedingungen zu reagieren. Es ist notwendig, die starre Kopplung zwischen Sensorik und Aktorik durch kognitive Informationsverarbeitung zu erweitern. Das aus der Kognitionswissenschaft stammende Dreischichtenmodell für die Verhaltenssteuerung [Str98] veranschaulicht die **Informationsverarbeitung**. Das Modell ist in dem Technologiekonzept Intelligenter Technischer Systeme integriert. Dieses ist in Bild 2-5 dargestellt.

In der untersten Ebene des Schichtenmodells findet sich die **nicht kognitive Regulierung** wieder. Ein Lernprozess ist aufgrund der starren Kopplung zwischen der Sensorik und der Aktorik grundsätzlich nicht möglich. In der mittleren Ebene, der **assoziativen Regulierung**, erfolgt der Lernprozess anhand der Konditionierung. Dies wird als assoziatives Lernen bezeichnet.

Die oberste Ebene des Dreischichtenmodells beinhaltet die **kognitive Regulierung**. Hierdurch sind kognitive Systeme in der Lage, Probleme zu antizipieren, sich an neue Aufgaben anzupassen und aus den gemachten Erfahrungen zu lernen. Alle höheren und bewussten Stufen der Informationsverarbeitung werden unter kognitivem Lernen[9] zusammengefasst [GAC+13].

---

[6] Mit Hilfe von Techniken der künstlichen Intelligenz werden kognitive Fähigkeiten in technische Systeme integriert [RN05].

[7] Nach LENZEN wird Kognition als diejenige Fähigkeit definiert, die es Menschen ermöglicht, sich intelligent und flexibel zu verhalten [Len02]. Nach STRUBE greift die Kognition zwischen der Reizaufnahme und dem darauf folgenden Verhalten ein [Str96].

[8] Nach STRUBE sind kognitive Funktionen u. a.: Wahrnehmen, Erkennen, Enkodieren, Speichern, Erinnern, Denken, Problemlösen, Lernen, Gebrauch der Sprache sowie motorische Steuerung [Str96].

[9] Lernen bezeichnet den Erwerb neuen Wissens oder die Umstrukturierung von bereits vorhandenem Wissen [GRS03].

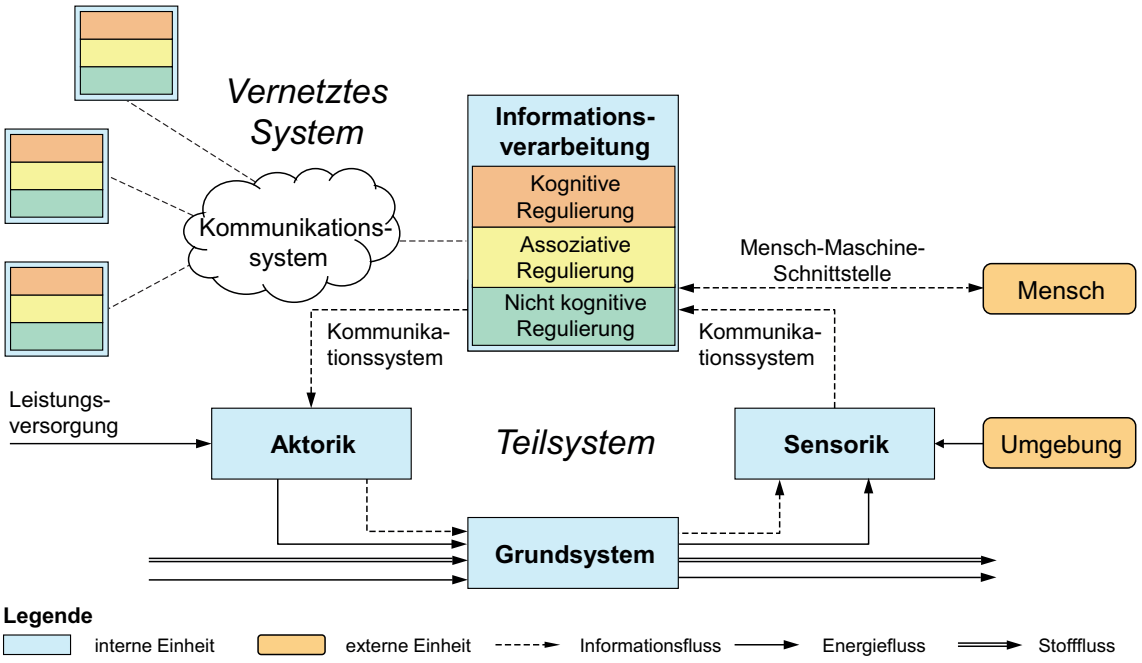


Bild 2-5: Technologiekonzept Intelligenter Technischer Systeme [GTD13]

Der Informationsverarbeitung wird eine zentrale Rolle zuteil. Mit Hilfe des Kommunikationssystems wird die Interaktion mit den internen Sensoren und Aktoren ermöglicht. Darüber hinaus ist die Informationsverarbeitung für die Kommunikation mit anderen vernetzen (Teil-)Systemen zuständig. Aufgrund der intensiven Interaktion der Einheiten Intelligenter Technischer Systeme, werden Fähigkeiten unterschiedlicher Fachdisziplinen zur Realisierung benötigt. Die Disziplinen zur Umsetzung solch einer komplexen Informationsverarbeitung sind die Regelungs- und Softwaretechnik sowie die höhere Mathematik. Zusätzlich wird auf die Techniken der künstlichen Intelligenz zurückgegriffen [GTD13], [Ana15].

Angesichts der innovativen Informationsverarbeitung, der Verbreitung des Internets, der Entwicklung von Cloud Computing sowie der Leistungsfähigkeit eingebetteter Systeme[10] spielt die geographische Lage der Systeme keine Rolle mehr. ITS kommunizieren und kooperieren über geographische Grenzen hinweg. Erst das Zusammenspiel der Einzelsysteme erschließt die Funktionalität des vernetzen Gesamtsystems. Dieses wird nicht mehr ausschließlich durch eine globale Steuerung beherrschbar sein, sondern durch hochdynamische Strategien kontrolliert. Hierbei ist die Informationsverarbeitung nicht statisch. Diese passt sich im Sinne der geforderten Gesamtfunktionalität, welche ebenfalls dynamisch und veränderlich ist, an [GAC+13], [GTD13].

[10] *"Eingebettete Systeme stellen eine Kombination aus Hard- und Softwarekomponenten dar, die in einem technischen Kontext eingebunden sind und die Aufgabe haben, ein System zu steuern, zu regeln oder zu überwachen. Ein eingebettetes (embedded) System verrichtet vordefinierte Aufgaben, oftmals mit Echtzeitberechnungsanforderungen" [BBB+10, S.4].*

ITS zeichnen sich weiterhin durch ihre **Kommunikationseigenschaften** aus (vgl. Bild 2-5). Durch diese Eigenschaften sind sie in der Lage, sich mit anderen Systemen zu vernetzen. Besonders die Entwicklung des Kommunikationssystems sowie die Integration in technische Systeme spielt bei dem Innovationssprung eine bedeutende Rolle [GTD13]. So entstehen völlig neue Möglichkeiten wie Produkt-Service-Systeme (PSS). Diese betrachten das System und die zugehörige Dienstleistung über den gesamten Lebenszyklus gleichermaßen und ermöglichen so ein kombiniertes Produkt-Service-Geschäft [EBD+15]. Die Kombination aus System und Dienstleistung bietet die Möglichkeit für Schutzmaßnahmen. LINDEMANN ET AL. definieren das Anbieten von PSS (vgl. Tabelle 4-3) und GAUSEMEIER ET AL. beschreiben hybride Leistungsbündel als strategische Schutzmaßnahmen (vgl. Kap. 2.3.2) [LMP+12a], [GGL12]. In der vorliegenden Arbeit werden die Dienstleistungen als Bestandteil des Intelligenten Technischen Systems betrachtet, da sie ohne das technische System keinen Mehrwert bieten.

Zusammenfassend stellen ITS das Ergebnis der Evolution mechatronischer Systeme in den Bereichen der Softwaretechnik, des Internets und der eingebetteten Systeme dar. Eingebettete Systeme, die über Kommunikationseinrichtungen in enger Verbindung mit digitalen Netzen stehen sowie physikalische Vorgänge mittels Sensorik und Aktorik überwachen und steuern, werden von BROY als Cyber-Physical Systems (CPS) definiert [Bro10]. CPS und ITS sind durch identische Eigenschaften charakterisiert. Daher beschreiben beide Ausdrücke dieselben Systeme und werden gleichgesetzt (vgl. Bild 2-5).

Mechatronische Systeme durchlaufen eine Entwicklung zu innovativen Systemen, welche sich insbesondere durch verbesserte Kommunikationseigenschaften sowie inhärente Teilintelligenz auszeichnen. Hieraus ergeben sich **Vorteile** Intelligenter Technischer Systeme [OWL15-ol]:

- Entlastung des Benutzers durch neue Funktionalitäten der Systeme
- Verbesserung der Entwicklung, Einrichtung und Wartung
- Steigerung der Zuverlässigkeit, Sicherheit und Verfügbarkeit
- Effizienzsteigerung des Energie- und Materialeinsatzes
- Umsetzung individualisierter und wandelbarer Produktionsprozesse

Herausforderungen in der Entwicklung Intelligenter Technischer Systeme ergeben sich insbesondere durch die steigende Komplexität der Systeme, die weiter zunehmende Interdisziplinarität sowie die Intensivierung des benötigten Wissens. Der Fokus der zu entwickelnden Systematik liegt auf dem präventiven Schutz der Systeme vor Produktpiraterie. Aus diesem Grund wird im folgenden Abschnitt das Themenfeld Produktpiraterie untersucht und detailliert erläutert.

2.3 Produktpiraterie

Ohne Innovationen gibt es kein Wachstum. Folglich sind Innovationen ein zentraler Erfolgsfaktor für deutsche Unternehmen (vgl. [VDM14b]). Eine Studie von PricewaterhouseCoopers (PwC) belegt, dass die Bedeutung von Innovationen in Zukunft weiter steigen wird. Mehr als 80 Prozent der befragten Unternehmen[11] halten Innovationen schon heute für wichtig oder unverzichtbar, um im globalen Wettbewerb zu bestehen. Die Relevanz des Themas steigt für 88 Prozent der Befragten in den nächsten fünf Jahren weiter an [GSS15].

Erfolgreiche Unternehmen vertreiben innovative Produkte, fahren hohe Gewinne ein und sind bei Aktionären und Kunden gut angesehen. An diesem Erfolg der Unternehmen versuchen Imitatoren, z. B. Produktpiraten, zu partizipieren. Die **Motivation** für das Imitieren von erfolgreichen Produkten liegt auf der Hand. Das Hauptmotiv des Imitators ist die geringere Kostenposition. Daraus ergibt sich ein Preisvorteil (vgl. Bild 2-6) und eine vielversprechende Aussicht auf hohe Gewinne. Entweder bietet der Imitator das Produkt zu einem niedrigeren Preis als das Originalprodukt an und spekuliert auf hohe Verkaufszahlen. Hier besteht das Risiko, dass die Kunden die Fälschung erkennen. Oder er verlangt einen dem Originalprodukt angeglichenen Preis und hat so eine hohe Gewinnmarge. Der Nachteil ist die vermutlich geringere Anzahl an verkauften Produkten [Nee07, S.48ff.]. Ein Vergleich der Bestandteile der Produktkosten des Originalherstellers (Innovators) und des Imitators ist in Bild 2-6 dargestellt.

Durch den Vergleich wird deutlich, dass die Bestandteile der Produktkosten unverändert bleiben, jedoch fallen für den Imitator in vielen Positionen deutlich geringere Kosten an. Die Produktkosten setzen sich in beiden Fällen aus den Entwicklungskosten, den Materialkosten, den Produktionskosten, den Kosten für Marketing bzw. Vertrieb sowie den Logistikkosten zusammen. Zu späteren Zeitpunkten im Produktlebenszyklus (PLZ) können noch Gewährleistungs- und Garantiekosten sowie Produkthaftungskosten entstehen. Das Äquivalent zu den Entwicklungskosten des Originalherstellers sind die Adaptionskosten des Imitators. Unter Adaptionskosten fallen die Kosten für das Reverse Engineering[12] und der Aufwand zur Beschaffung der Information, die zur Fertigung benötigt werden. Je größer die Differenz zwischen den Entwicklungs- und Adaptionskosten ist, desto höher ist die Gewinnmarge für den Imitator. Speziell bei den Marketingkosten hat der Imitator Vorteile, da er von der Marketingarbeit des Originalherstellers profitiert. Ähnlich verhält es sich bei den Gewährleistungs- und Garantiekosten. Für diese Ansprüche wird der Originalhersteller kontaktiert, nicht der Imitator [Nee07].

[11] 213 deutsche Unternehmen nahmen an der Umfrage teil [GSS15].

[12] Beim Reverse Engineering wird ein bestehendes System in seine Bestandteile zerlegt und dadurch Know-how und Wissen extrahiert [PS02].

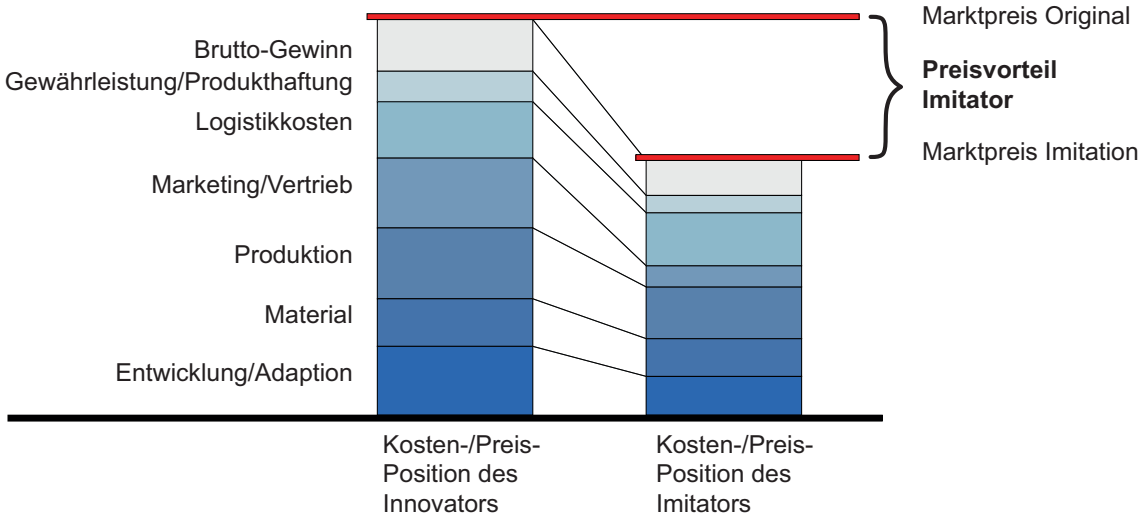


Bild 2-6: Bestandteile der Produktkosten von Innovator und Imitator [Nee07, S.51]

Aufgrund der illegal kopierten Produkte sowie des entwendeten Know-hows entsteht insbesondere bei den betroffenen Unternehmen ein großer **Schaden**. Die Schäden sowie die unterschiedlichen Auswirkungen von Produktpiraterie werden in Kapitel 2.3.1 erläutert. In Kapitel 2.3.2 werden Möglichkeiten zum Schutz vor Produktpiraterie vorgestellt. Für den Schutz Intelligenter Technischer Systeme ergeben sich neue Herausforderungen. Bedingt werden diese durch die Weiterentwicklung der Systeme. Die Herausforderungen werden in Kapitel 2.3.3 beschrieben.

2.3.1 Schaden durch Produktpiraterie

Bei den Unternehmen des deutschen Maschinen- und Anlagenbaus entstehen erhebliche Schäden durch Produktpiraterie [VDM16]. Der Maschinen- und Anlagenbau war im Jahr 2014 der größte industrielle Arbeitgeber in Deutschland mit ca. einer Mio. Beschäftigten in rund 6.400 Unternehmen. Diese erwirtschafteten zusammen einen Umsatz von 212 Mrd. Euro. 151,5 Mrd. Euro wurden durch den Warenexport erzielt [VDM15].

Für den deutschen Maschinen- und Anlagenbau sind Innovationen einer der wichtigsten Erfolgsfaktoren im Wettbewerb [VDM14b]. Insbesondere für verwandte Wirtschaftszweige wie die Automobil- oder die Chemieindustrie wird die Branche als wesentlicher Innovationstreiber gesehen [MWS06].

Mit Hilfe der Befragung von Unternehmen des Maschinen- und Anlagenbaus entwickelt der Verband Deutscher Maschinen- und Anlagenbau (VMDA) alle zwei Jahre eine Studie zum Thema Produktpiraterie. Aus dieser geht hervor, dass seit einigen Jahren mehr als **zwei Drittel** aller befragten Unternehmen[13] **Opfer von Produktpiraterie** sind. Bei

[13] An der Studie im Jahr 2014 beteiligten sich insgesamt 337 Mitglieder des VDMA [VDM14a]. Im Jahr 2016 waren es 193 Mitglieder [VDM16].

großen Unternehmen mit mehr als 1000 Mitarbeitern waren es sogar **94 Prozent**. Der entstandene Schaden wird auf 7,3 Mrd. Euro beziffert. Der Schaden entsteht, da gefälschte Produkte den Umsatz verringern und Kosten für Rechtsstreitigkeiten oder Schutzmaßnahmen anfallen. Ließe sich dieser Schaden minimieren und könnte in den Umsatz der Unternehmen einfließen, würden dadurch jedes Jahr mehr als 30.000 neue Arbeitsplätze geschaffen [VDM14a], [VDM16].

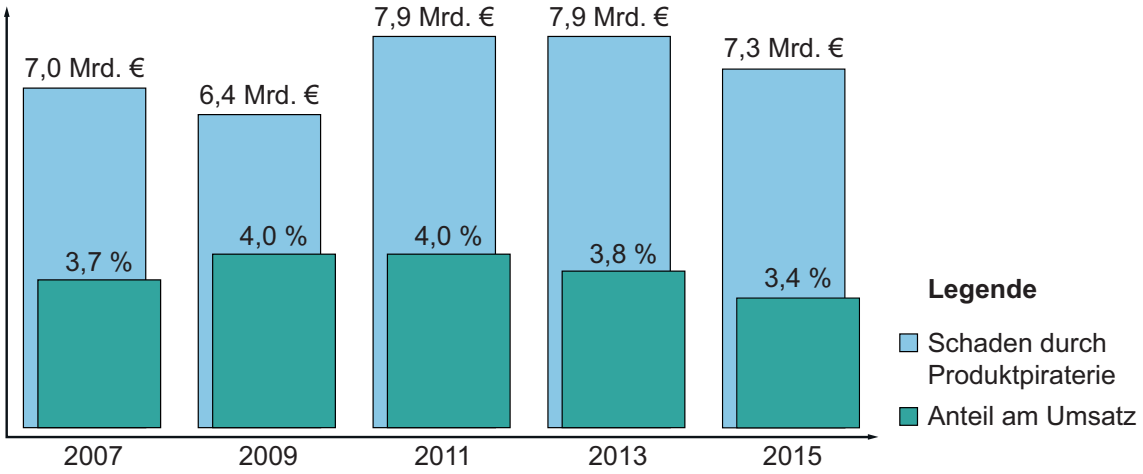


Bild 2-7: Schaden durch Produktpiraterie im Maschinen- und Anlagenbau [VDM16]

Die Entwicklung des Schadens durch Produktpiraterie in den letzten Jahren ist in Bild 2-7 dargestellt. Hier wird auch der Anteil am Gesamtumsatz der Branche aufgezeigt. Demnach beträgt der Schaden seit 2007 konstant zwischen drei und vier Prozent des Gesamtumsatzes. Die gravierendste Aussage aus der VDMA-Studie ist, dass der Schaden durch Produktpiraten nicht nennenswert zurückgegangen ist, obwohl 2008 vom BMBF die Forschungsoffensive „Innovationen gegen Produktpiraterie“ gestartet wurde. Diese ist mittlerweile ausgelaufen.

Der VDMA-Studie entsprechend schützen sich **82 Prozent** der befragten Unternehmen durch **juristische Maßnahmen** vor Imitationen. Diese Schutzmaßnahmen stellen einen wichtigen Baustein im Kampf gegen Produktpiraten dar, allerdings wirken juristische Maßnahmen **reaktiv**. Das bedeutet, die Maßnahmen greifen erst, nachdem der Schaden eingetreten ist (vgl. Kap. 2.3.2). Darüber hinaus machen viele Unternehmen von ihrem Recht keinen Gebrauch und gehen nicht gegen Imitatoren vor. Zusätzlich sind gerichtliche Verfahren oft sehr langwierig und kostspielig. Zudem ist die Durchsetzung der Rechte nicht in allen Ländern ohne Weiteres möglich. Eines der besten Beispiele hierfür ist die Volksrepublik China [VDM16]. Es gibt kaum Möglichkeiten das Recht an seinem **geistigen Eigentum in China** juristisch durchzusetzen. Daher untersuchen KEUPP ET AL., welche Strategien zum Schutz des geistigen Eigentums in China in der Praxis angewendet werden. Sie stellen fest, dass viele Unternehmen Strategien wie technologische Spezialisierung oder Geheimhaltung verwenden. Zusätzlich wird deutlich, dass ein vertrauensvolles Verhältnis zu den Angestellten und zu öffentlichen Amtsträgern in China eine Voraussetzung für den Schutz des geistigen Eigentums ist [KBG09].

Die von KEUPP ET AL. vorgestellten Strategien sind nicht ausreichend. Dies beweist das Ergebnis der VDMA-Studie, wonach 83 Prozent aller Unternehmen des deutschen Maschinen- und Anlagenbaus China als Herkunftsland für Plagiate sehen. Aber auch in Deutschland werden zahlreiche Imitate hergestellt. Insgesamt 24 Prozent der Unternehmen konnten Plagiate identifizieren, die in Deutschland produziert wurden [VDM16].

Durch Imitationen entsteht für Unternehmen eine Vielzahl an leistungswirtschaftlichen **Risiken**. So sieht knapp die Hälfte der vom VDMA befragten Unternehmen Produktpiraterie als die größte Gefahr für deren Maschinen und Anlagen [VDM16, S.15]. Nach KUSKE betreffen die Risiken primär die Wertschöpfung des Unternehmens. Beispiele sind die Substitution des Originals, der Verlust des Know-hows, Imageschäden, Kundenverlust, Preisverfall etc. Nicht nur für Unternehmen entstehen Risiken durch Imitationen, auch für Volkswirtschaften entstehen Risiken und Schäden. Diese können z. B. durch Steuermindereinnahmen, Arbeitsplatzverluste oder den Rückgang der Innovationsbereitschaft entstehen [Kus13, S.12ff.]. Ebenso bestehen für Konsumenten und Anwender Risiken. Hierzu zählen Risiken für Leib und Leben (z. B. durch Fehlfunktion) oder der Verlust von Gewährleistungs- und Garantieansprüchen. So sehen 39 Prozent in Plagiaten eine große Gefährdung des Menschen. Darüber hinaus erkennt GLOBERMANN, dass durch Produktpiraterie nicht nur die Originalhersteller und Käufer die Leidtragenden sind, sondern auch die Verkäufer und die Herkunftsländer der gefälschten Waren. Zwar wird durch die Imitate kurzfristig ein Mehrwert erzeugt, langfristig betrachtet wird es zur Reduktion von ausländischen Investments und damit zu negativen Effekten für die Wirtschaft kommen [Glo88].

2.3.2 Schutz vor Produktpiraterie

Mit Hilfe von Schutzmaßnahmen kann der Schaden durch Produktpiraterie reduziert und bestenfalls vollständig verhindert werden. Hierfür müssen die unternehmensspezifischen Bedrohungen identifiziert und anschließend wirksame Maßnahmen zum Schutz eingesetzt werden [LMP+12b, S.105ff.], [Mei11, S.98ff.].

Schutzmaßnahmen lassen sich generell in reaktive und präventive Schutzmaßnahmen einteilen [Mei10, S.44]. **Reaktive Maßnahmen** sind z. B. rechtliche Maßnahmen wie Schutzrechte. Bei der Verletzung der Rechte müssen diese durchgesetzt werden. Dieses Vorgehen ist fast ausschließlich reaktiv. Der Schutz wirkt erst, nachdem der Schaden eingetreten ist und Imitate entwickelt wurden. Nur wenn Schutzrechte eine abschreckende Wirkung entfalten, können diese auch präventiv wirken. Der Vorteil für Unternehmen besteht darin, dass die Durchsetzung mit externen Akteuren (Anwalt, Gericht, Zoll) geschehen kann. Jedoch ist dies zum Teil mit hohem Aufwand verbunden (vgl. Kap. 2.3.1). **Präventive Maßnahmen** haben das Ziel, bereits vor Schadenseintritt wirksam zu sein. Bei der Prävention wird die Produktion von Imitaten verhindert, indem Strategien bzw. Maßnahmen zum Schutz der Produkte umgesetzt werden. So kann

bspw. die Attraktivität ein Produkt zu kopieren, durch hohe Komplexität, kurze Lebenszyklen, hohe Fixkosten etc. reduziert werden [Kok13], [Mei08], [Mei10].

Es existieren zahlreiche reaktive sowie präventive Schutzmaßnahmen gegen Produktpiraterie. In einschlägigen Veröffentlichungen sind jeweils ca. 80 Maßnahmen gesammelt (z. B. [LMP+12a], [GGL12]). Die Sammlungen werden in Kapitel 3.1 näher vorgestellt. KOKOSCHKA unterteilt Schutzmaßnahmen in sieben Kategorien. Er definiert drei Oberkategorien: strategische, produktbezogene und prozessbezogene Schutzmaßnahmen. Zudem gibt es vier Querschnittskategorien: kommunikative, kennzeichnende, informationstechnische (IT) und rechtlichen Schutzmaßnahme [Kok12a]. Die Querschnittskategorien können in eine oder mehrere Hauptkategorien eingeteilt werden. Die Kategorien und deren Zuordnung sind in Bild 2-8 abgebildet und im Folgenden beschrieben.

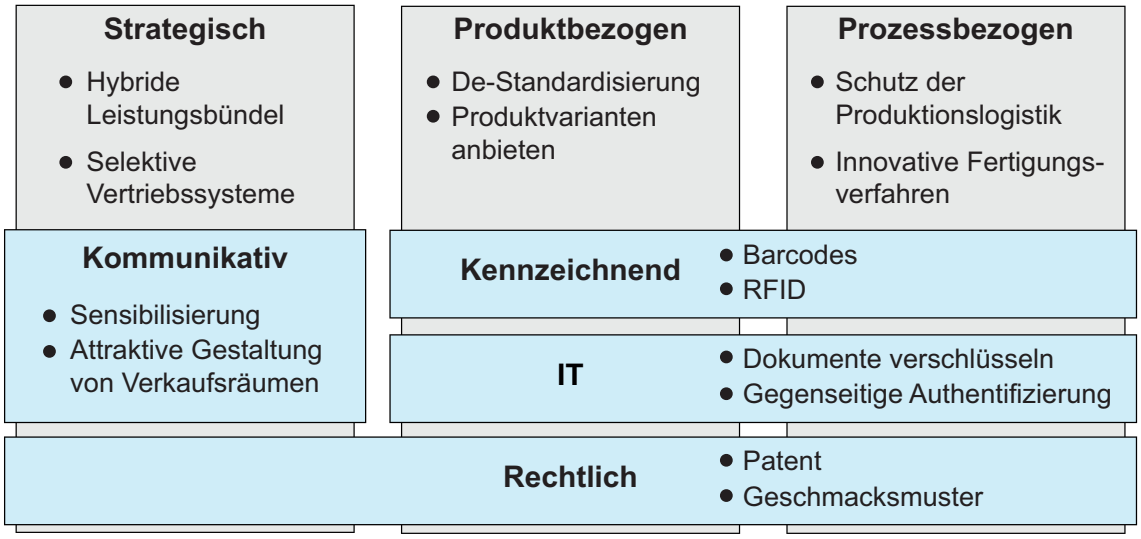


Bild 2-8: Kategorien für Schutzmaßnahmen nach KOKOSCHKA [Kok12a]

Strategische Schutzmaßnahmen: Diese Maßnahmen beziehen sich nicht ausschließlich auf ein bestimmtes Produkt oder Produktionssystem. Die strategischen Schutzmaßnahmen sind langfristig orientiert und setzen in der frühen Phase der Produktentstehung an. Daher bilden sie das Grundgerüst für die Produkt- und Produktionssystementwicklung unter Berücksichtigung der Gesichtspunkte des Systemschutzes. Bei strategischen Maßnahmen muss berücksichtigt werden, dass diese nicht nur in der Unternehmensstrategie, sondern auch in allen Substrategien untergebracht werden [Kok12b].

Ein Beispiel für strategische Schutzmaßnahmen ist das *Anbieten von hybriden Leistungsbündeln*. Auf Basis dieser Maßnahme werden Produktergänzungen und Services bereits bei der Produktentstehung berücksichtigt. Ein weiteres Beispiel sind *selektive Vertriebssysteme*. Mit Hilfe dieser wird eine kontrollierte Distribution der Produkte durchgeführt. So werden die Gefahren vor Imitationen und Know-how-Verlust verringert [Kok12b].

Produktbezogene Schutzmaßnahmen: Diese Maßnahmen sind in der Regel technisch geprägt. Das Ziel ist die Erstellung eines imitationsgeschützten Produktes. Um dies zu

erreichen müssen nicht zwangsläufig gesamte Produkte geschützt werden, die Maßnahmen lassen sich auch auf einzelne Komponenten herunterskalieren. Denkbar sind auch Ansätze, bei denen ein gesamtes Produkt dadurch geschützt wird, indem bei einzelnen Komponenten verschiedene Schutzmaßnahmen zur Anwendung kommen. Der Imitationsschutz kann z. B. durch die Senkung der Nachahmungsattraktivität des Produktes oder den Schutz ausgewählter Produkttechnologien realisiert werden [Kok12c].

Eine beispielhafte Maßnahme ist die *De-Standardisierung*. Bei dieser werden für wichtige Elemente eines Produktes nicht standardisierte Komponenten eingesetzt. Ein weiteres Beispiel ist das *Anbieten von Produktvarianten*. Hier wird ein Gesamtsystem aus funktionalen Modulen auf einer Modulplattform zusammengesetzt. Somit entsteht eine große Auswahl an Varianten und die Produkte können individualisiert für den jeweiligen Kundenkreis hergestellt werden. So wird das Kopieren der Leistung des Produktes erschwert, da die Imitation einer einzelnen Produktvariante nur einen kleinen Kundenkreis anspricht [Sch11], [Mei11].

Prozessbezogene Schutzmaßnahmen: Diese kommen vor allem bei Fertigungsprozessen zum Einsatz. Bei prozessbezogenen Maßnahmen ist die Aufteilung in die vier Aspekte Arbeitsablaufplanung, Arbeitsmittelplanung, Arbeitsstättenplanung und Produktionslogistik sinnvoll. Zur Verankerung der Schutzmaßnahmen in den betrieblichen Abläufen ist schützenswertes Know-how im Fertigungsprozess zu identifizieren und die Schutzmaßnahmen sind im Voraus zu planen [BK12a], [BK12b].

Ein Beispiel für prozessbezogene Schutzmaßnahmen ist der *Schutz der Produktionslogistik*. Durch diese Maßnahme findet eine Überwachung des gesamten Produktionsprozesses statt. Ein weiteres Beispiel für prozessbezogene Schutzmaßnahmen sind *innovative Fertigungsverfahren*. Diese erhöhen den Schutz vor Produktpiraterie durch die Herstellung von Bauteilen mit speziellen Eigenschaften und Gestaltungsformen. Die Imitation dieser Bauteile erfordert z. B. spezielles Know-how oder innovative Fertigungstechnologien [Mei11], [Kok13].

Kennzeichnende Schutzmaßnahmen: Sie ermöglichen Herstellern, Händlern, Konsumenten und auch staatlichen Behörden wie dem Zoll die Identifizierung eines Originalproduktes. Zu diesem Zweck versehen die Hersteller Originalprodukte und ggf. auch deren Verpackungen mit einer Markierung. Anhand der Kennzeichnungen kann ein Originalprodukt eindeutig identifiziert werden. Diese Identifizierung kann zusätzlich im Falle eines Rechtsstreits hinsichtlich der Beweisführung dienen [MS05], [Gue10], [Fuc06].

Eine kennzeichnende Schutzmaßnahme ist z. B. ein *Barcode*. Dieser ermöglicht die Identifikation der Produkte. Eine andere kennzeichnende Schutzmaßnahme wird durch *RFID* (radio-frequency-identification) realisiert. RFID dient zur Kennzeichnung und Rückverfolgung physischer Objekte [Mei11], [FD06].

Informationstechnische Schutzmaßnahmen: Durch diese Maßnahmen wird die gesamte IT-Infrastruktur wie Computer- oder Netzwerkverbindungen, Daten (CAD-Zeichnungen, Anforderungslisten), Anwendungssoftware und Systeme geschützt. Informationstechnik gewinnt zunehmend an Bedeutung, da der Softwareanteil in maschinenbaulichen Produkten stetig steigt. Dies bringt einen vermehrten Einsatz von informationstechnischen Schutzmaßnahmen gegen Produktpiraterie mit sich [PZ12].

Beispielhaft für IT-Maßnahmen ist die *Verschlüsselung vertraulicher Dokumente* beschrieben. Diese Schutzmaßnahme verhindert die Einsicht unbefugter Personen. Auch die *gegenseitige Authentifizierung von Komponenten* zählt zu den informationstechnischen Schutzmaßnahmen. Hierbei wird eine Austauschkomponente von der Steuereinheit eines Systems auf ihre Originalität überprüft [AAA+10], [Mei11], [Kok13].

Rechtliche Schutzmaßnahmen: Der Inhaber einer Erfindung erhält durch diese Maßnahmen das Recht, seine Erfindung für eine festgesetzte Dauer zu nutzen und Anderen die Nutzung zu verbieten. Das Schutzrecht bietet national wie international Möglichkeiten, Neuentwicklungen vor Nachahmungen zu schützen. Die Maßnahmen können sich auf die Technik beziehen (Patente, Gebrauchsmuster), auf die ästhetische Gestalt (Geschmacksmuster, Urheberrecht) oder auf die Kennzeichnung (Marken) [Lor12].

Ein Beispiel für rechtliche Schutzmaßnahmen ist das *Patent*. Durch die Anmeldung eines Patentes werden technische Erfindungen geschützt. Ein anderes Beispiel ist das *Geschmacksmuster*. Dieses bezweckt den Schutz der äußeren Form eines Erzeugnisses [Lor12].

Kommunikative Schutzmaßnahmen: Kommunikative Schutzmaßnahmen regeln den unternehmensinternen und -externen Umgang mit schützenswerten Informationen über Produkte und Prozesse. Zusätzlich legen sie fest, wie das Unternehmen beim Auftreten illegaler Imitate der eigenen Produkte reagiert [BK12c].

Eine kommunikative Schutzmaßnahme ist *Sensibilisierung* z. B. durch das Veranstalten von Aufklärungskampagnen über Produktpiraterie von Unternehmen oder Verbänden. Eine weitere Maßnahme ist das *attraktive Gestalten von Verkaufsräumen*. Durch solche Alleinstellungsmerkmale setzen sich Originalhersteller von Imitatoren ab. So nimmt der Kunde den Verkaufsvorgang als wertsteigernde Leistung wahr [BK12a], [WG07].

Im Rahmen der vorliegenden Arbeit sind technische, präventive Schutzmaßnahmen von größter Relevanz. Durch diese kann das systeminhärente Know-how gesichert und die Systeme können vor unerlaubtem Nachbau geschützt werden. Diese Maßnahmen werden hauptsächlich in der Oberkategorie produktbezogen einsortiert. Daher fokussiert sich die Arbeit auf die die **produktbezogenen Schutzmaßnahmen**. Zu dieser Kategorie zählen die Querschnittskategorien kennzeichnend, informationstechnisch und rechtlich (vgl. Bild 2-8). Rechtliche Maßnahmen werden jedoch nicht betrachtet, da diese in der Regel reaktiv wirken.

Zusammenfassend kann festgehalten werden, dass eine große Bandbreite an technischen Schutzmaßnahmen existiert. Diese sind in Form von Steckbriefen dargestellt (vgl. Kap. 3.1). Jedoch nutzen lediglich ein Drittel der Unternehmen des Maschinen- und Anlagenbaus solche technischen Schutzmaßnahmen. 42 Prozent der befragten Unternehmen gaben an, dass derzeitige technische Schutzmaßnahmen ungeeignet sind. Weiterhin wurden die Maßnahmen von 39 Prozent als zu kostenintensiv und von einem Viertel der Befragten als unbekannt deklariert [VDM16].

Gründe dafür, dass die Unternehmen keine wirksamen Schutzmaßnahmen finden, sind:

- Es sind keine geeigneten Schutzmaßnahmen bekannt.
- Die textbasierte Beschreibung der Schutzmaßnahmen ist nicht ausreichend, da sie nicht von allen Fachdisziplinen gleichermaßen verstanden wird und so die passenden Schutzmaßnahmen nicht identifiziert werden können.
- Die Unternehmen befassen sich zu spät mit dem Thema Systemschutz. Die bestehenden Maßnahmen können nicht mehr in das fertige System integriert werden.

Anhand dieser Ursachen ergeben sich **Verbesserungspotentiale für den präventiven Schutz Intelligenter Technischer Systeme**, die in der vorliegenden Arbeit aufgegriffen werden:

- Bestehende Schutzmaßnahmen müssen auf ihre Wirkung für ITS untersucht und wirksame Schutzmaßnahmen aufgezeigt werden.
- Für die Identifikation wirksamer Schutzmaßnahmen sind innovative Technologien zu berücksichtigen, da diese zum Systemschutz beitragen können.
- Der spätere Schutz sollte bestenfalls bereits bei der Produktkonzeption berücksichtigt werden [Gru10, S.112].
- Die Anwendung der Maßnahmen bereits während des Systementwurfs ist zu vereinfachen.
- Hierfür müssen die Schutzmaßnahmen so beschrieben werden, dass alle beteiligten Fachdisziplinen ein einheitliches Verständnis erlangen.
- Darüber hinaus muss die Wiederverwendung von bereits vorhandenem Wissen berücksichtigt werden.

Durch die Evolution von mechatronischen hin zu Intelligenten Technischen Systemen ergeben sind neue Herausforderungen beim Systemschutz. Diese werden im Folgenden beschrieben.

2.3.3 Herausforderungen beim Schutz Intelligenter Technischer Systeme

Wie in Kapitel 2.2.3 herausgearbeitet, werden sich zukünftige technische Systeme von bislang bekannten Produkten unterscheiden. Bedingt durch den Technologiesprung von mechatronischen hin zu intelligenten, vernetzen Systemen findet eine zunehmende Integration von disziplinübergreifenden Methoden, Techniken, Verfahren und Schnittstellen in die Systeme statt. Diese zukünftigen Systeme werden auf einem engen Zusammenwirken der Disziplinen Mechanik, Elektrotechnik, Regelungstechnik und Softwaretechnik beruhen. Da diese Systeme durch eine über die Mechatronik hinausgehende inhärente Intelligenz charakterisiert sind, werden sie als ITS bezeichnet [GTD13].

Für ITS entstehen unbekannte **Angriffsmöglichkeiten** und **Herausforderungen** beim Schutz dieser Systeme. Aufgrund des hohen Marktpotentials sowie des gesteigerten systeminternen Know-hows besteht bei Intelligenten Technischen Systemen die Gefahr vor Imitaten und Know-how-Abfluss durch **Reverse Engineering**. Laut VDMA ist das Reverse Engineering seit Jahren die am häufigsten angewandte Methode zur Extraktion des Produkt-Know-hows [VDM14a, S.14], [VDM16, S.18]. Hierbei kann das Know-how bzw. die Funktionsweise des Systems durch die physische Zerlegung abfließen.

Bedingt durch die ausgeprägten Kommunikationsfähigkeiten vernetzter Systeme (vgl. Kap. 2.2.3) müssen diese darüber hinaus gegen eine für technische Erzeugnisse, neue Angriffsform geschützt werden. Böswillige Angriffe über Kommunikationsschnittstellen werden als **Cyberattacken oder -angriffe** bezeichnet. Die Imitatoren nutzen die Vernetzung der Systeme als neue Angriffsmöglichkeit aus (vgl. Kap. 2.1) [BSI14a], [BRW15]. Mit Hilfe dieser Angriffe kann das systeminhärente Know-how in Form von Daten oft unbemerkt extrahiert und gestohlen werden [VDM13]. Mit dem gestohlenen Know-how vereinfacht sich die Imitation der Systeme, sodass der Imitationsprozess deutlich verkürzt wird. So kann das Plagiat kurz nach Markteinführung des Originals oft mit sehr ähnlichen Funktionen angeboten werden. Auf diese Weise versuchen Produktpiraten am Markterfolg der Originalhersteller zu partizipieren. [Kle13, S.88ff.].

Weltweit verursachen Cyberattacken bereits heute beträchtlichen Schaden und bedingen den Verlust von IP. 65 Prozent der Unternehmensführer sind der Ansicht, dass böswillige Angriffe aus externen oder auch internen Quellen am ehesten eine Gefahr darstellen und negative Auswirkungen auf das Geschäft haben werden. Dies wurde in einer gemeinsamen Studie von dem World Economic Forum und McKinsey in 2014 untersucht. Demnach sind mehr als die Hälfte der Befragten[14] der Meinung, das Risiko von Cyberattacken werde in den nächsten Jahren ein wichtiges Thema sein. Darüber hinaus prognostizieren 69 Prozent, dass die Weiterentwicklung der Angriffe schneller voranschreiten wird, als die Entwicklung der Gegenmaßnahmen [WEF14].

[14] An der Studie nahmen über 500 Führungskräfte und Experten teil [WEF14].

In einer Studie vom Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (Bitkom) wurden Geschäftsführer und Sicherheitsverantwortliche zum Thema digitale Angriffe befragt[15]. Das Ergebnis war, dass 51 Prozent der befragten Unternehmen, in den vergangenen zwei Jahren Opfer von digitaler Wirtschaftsspionage, Sabotage oder Datendiebstahl waren [Bit15-ol].

Aktuelle Ereignisse verdeutlichen den Bedarf an der Verbesserung des Schutzes für ITS. Zahlreiche Beispiele liefert der Automobilsektor. Es sind mehrere Hersteller betroffen. Ein Beispiel ist Fiat Chrysler Automobiles, dessen Jeep Cherokee in voller Fahrt gehackt wurde [Ber15-ol]. Auch Tesla Motors musste einen erfolgreichen Angriff verzeichnen, da sich die Fahrzeuge bei voller Fahrt ausschalten ließen [Tho15-ol].

Aber auch der Maschinen- und Anlagenbau muss sich mit neuen Angriffen auseinandersetzen. So berichtet das Bundesamt für Sicherheit in der Informationstechnik (BSI) über einen gezielten und erfolgreichen Angriff auf ein Stahlwerk in Deutschland. Dieser Angriff führte dazu, dass ein geregeltes Herunterfahren eines Hochofens nicht möglich war. Die Folge waren massive Beschädigungen der Anlage [BSI14a, S.31].

Für ITS hat die geographische Lage der Systeme keine Bedeutung. Entwicklung, Steuerung und Wartung erfolgen dynamisch und standortunabhängig. Im Umkehrschluss bringt die steigende Vernetzung **neue Möglichkeiten für Produktpiraten** mit sich. Die Imitatoren können sich ohne physischen Kontakt in das System hacken und Know-how stehlen. So können lokale Angriffe eine Bedrohung für weltweit vernetzte Systeme darstellen [Her15]. Zusätzlich können neue Arten von Imitaten, wie gefälschter Steuercode, kopierte Apps oder imitierte Software entstehen. Die neuen Angriffsmöglichkeiten sowie die Kompetenzen der Imitatoren müssen für den Einsatz wirksamer Schutzmaßnahmen bekannt sein und berücksichtigt werden.

Ferner ist für den Systemschutz zu beachten, dass einfache Schutzmaßnahmen nicht ausreichend sind, um das Gesamtsystem zu schützen. In Bild 2-9 ist aufgezeigt, dass mit steigender Produktkomplexität sowie Intelligenz der Systeme auch deren Schutz intensiviert werden muss. Demnach ist für hoch komplexe Systeme mit inhärenter Intelligenz das Gesamtsystem als Infrastruktur für Schutzmaßnahmen zu benutzen. Zusätzlich ist die erweiterte Informationsverarbeitung und somit die Intelligenz des Systems auszunutzen, um einen effektiven Schutz sicherzustellen. Hierdurch wird die autonome Adaption insbesondere informationstechnischer Schutzmaßnahmen ermöglicht. Voraussetzung ist die Integration der Schutzmaßnahmen in das Gesamtsystem. Daher werden auch die Schutzmaßnahmen für ITS komplexer, interdisziplinär und wissensintensiver [KA11].

[15] Für die Studie wurden Geschäftsführer und Sicherheitsverantwortliche von 1.074 Unternehmen repräsentativ befragt [Bit15-ol].

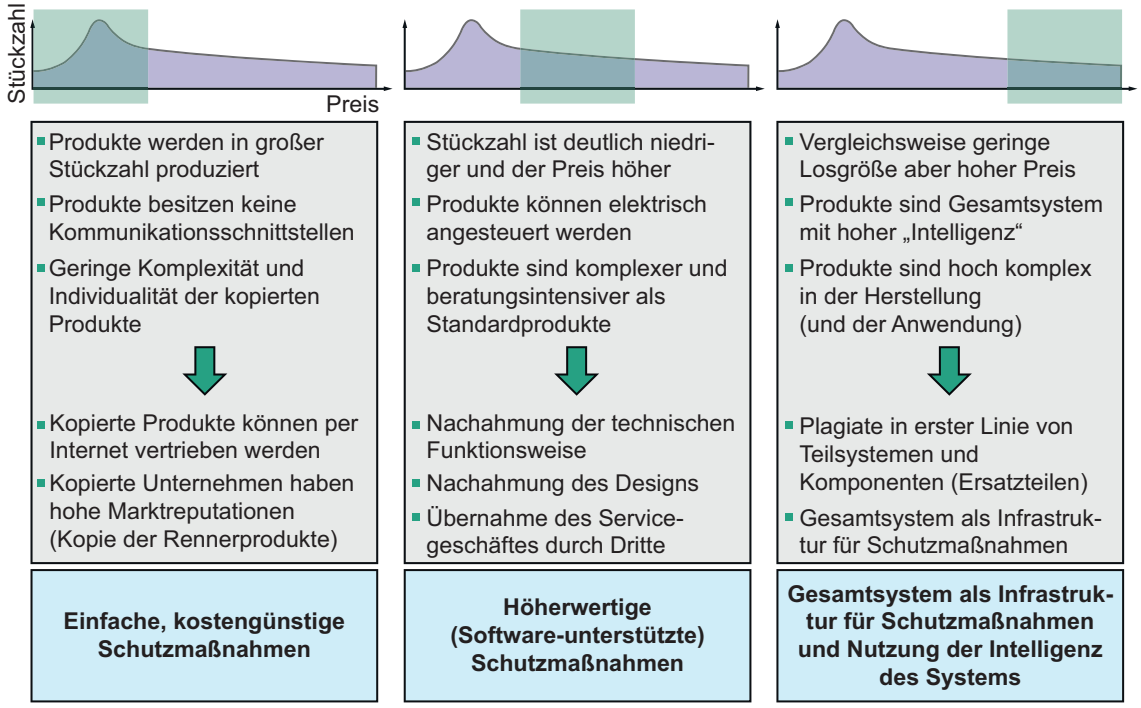


Bild 2-9: Art der Betroffenheit und mögliche Schutzmaßnahmen nach [AKL11, S.19]

Es zeigt sich, dass neue Herausforderungen an den Schutz Intelligenter Technischer Systeme entstehen. Dies liegt in der – in Kapitel 2.2.3 beschriebenen – Entwicklung von mechatronischen, hin zu Intelligenten Technischen Systemen begründet. Der gestiegene Anteil an integrierten Funktionen, Sensoren und Schnittstellen muss direkt von Beginn der Systementwicklung an berücksichtigt werden, um eine effektive Umsetzung der Aspekte des Systemschutzes sicherzustellen. Um den Herausforderungen begegnen zu können müssen die **Schutzanforderungen Intelligenter Technischer Systeme** (vgl. Kap. 2.1) bekannt sein. Bestehende Schutzmaßnahmen sind auf deren Wirkung zu überprüfen. Ggf. müssen anhand der Schutzanforderungen neue Maßnahmen für den wirkungsvollen Schutz identifiziert werden.

Zusammenfassend ergeben sich **Verbesserungspotentiale speziell für den Schutz Intelligenter Technischer Systeme**, die in der vorliegenden Arbeit aufgegriffen werden:

- Die Schutzanforderungen der ITS müssen identifiziert werden. Bestehende Schutzmaßnahmen sind auf deren Wirkung zu überprüfen und ggf. werden neue Maßnahmen und Ansätze zum Systemschutz benötigt.
- Neue Angriffsmöglichkeiten sind ebenso wie die zugehörigen Kompetenzen der Angreifer zu identifizieren und darzustellen.
- Durch die Komplexität der Systeme ist eine nachträgliche Integration der Schutzmaßnahmen in die Systeme nicht möglich. Die Aspekte des Schutzes müssen in den Entwurf der Systeme eingegliedert werden.

- Zukünftige Schutzmaßnahmen können oft nicht mehr nur einer Fachdisziplin zugeteilt werden. Die voranschreitende Entwicklung wird zu einer Verbindung zwischen den Schutzmaßnahmen und den Funktionen der zu schützenden Systeme führen [AIS15-ol], [KA11]. Daher wird das Wissen unterschiedlicher Fachdisziplinen für den Systemschutz benötigt. Dies hat zur Folge, dass die Schutzmaßnahmen bereits im Systementwurf von allen beteiligten Disziplinen gleichermaßen betrachtet werden müssen, da hier ein interdisziplinäres Lösungskonzept festgelegt wird.
- Hierfür sind die Schutzmaßnahmen so zu beschreiben, dass ein disziplinübergreifendes Verständnis sichergestellt wird.
- Darüber hinaus ist die Wiederverwendung von bereits erfolgreich eingesetztem Lösungswissen anhand der Darstellung der Schutzmaßnahmen zu unterstützen.

Nur wenn die Imitatoren sowie Fälscher und damit der illegale Know-how-Abfluss gestoppt wird, bleibt der Wettbewerbsvorsprung durch Innovationen erhalten. So kann die Entwicklung und Produktion in Deutschland gesichert werden. Um die Erforschung Intelligenter Technischer Systeme voranzutreiben und die Innovationslust der Unternehmen hochzuhalten, muss die Rentabilität der Neuentwicklungen sichergestellt werden. Hierfür müssen die Systeme wirksam geschützt werden. Damit dies gelingt, sind ein ganzheitliches Verständnis der Systeme sowie deren Schutzanforderungen unumgänglich. Insbesondere die Berücksichtigung von wirksamen Schutzmaßnahmen im Systementwurf verspricht ein hohes Erfolgspotential. Der Entwurf birgt an sich zahlreiche Herausforderungen (vgl. Kap 2.2.3). Die zusätzliche Berücksichtigung des Schutzes intensiviert diese Herausforderungen und verlangt nach neuen Ansätzen. Um den Schutz der Systeme frühzeitig zu berücksichtigen, muss deren Entstehungsprozess bekannt sein. Daher werden die Grundlagen des Systementwurfs im Folgenden erläutert.

2.4 Fachdisziplinübergreifender Systementwurf

Mechatronische Systeme entstehen durch ein stark ausgeprägtes Zusammenwirken unterschiedlicher Disziplinen und Technologien. Der Wandel zu Intelligenten Technischen Systemen wird vollzogen durch eine Erweiterung der klassischen Disziplinen der Mechatronik um eine Reihe neuer, teilweise nichttechnischer Fachbereiche wie den Kognitionswissenschaften [GTD13]. Dies hat Auswirkungen auf die Entstehung dieser Systeme. Um ein grundlegendes Verständnis für die fachdisziplinübergreifende Systementwicklung zu schaffen, wird das 3-Zyklen-Modell nach GAUSEMEIER erläutert. Die vorliegende Arbeit wird in dieses Modell eingeordnet (Kap. 2.4.1).

Die Entwicklung Intelligenter Technischer Systeme ist ein komplexer und wissensintensiver Prozess. Daher ergeben sich eine Reihe neuer Herausforderungen z. B. die Beherrschung der zunehmenden Komplexität oder die Schaffung eines einheitlichen Systemverständnisses [GDS13]. Nach BOUCHER und HOULIHAN sind die sechs größten Herausforderungen in der Entwicklung komplexer interdisziplinärer Systeme [BH08]:

- Erfahrene Systemingenieure sind schwer zu finden/Mangel an funktionsübergreifendem Know-how
- Frühzeitige Ermittlung von Problemen auf Systemebene
- Sicherstellung der Erfüllung sämtlicher Anforderungen im Endprodukt
- Hoher Aufwand bei der Simulation bzw. Modellierung des Produktverhaltens bis zum eigentlichen Prototypenbau
- Schwierigkeiten bei der Implementierung einer integrierten Lösung zur Produktentwicklung für alle an der Entwicklung beteiligten Disziplinen
- Auswirkungen von Änderungen auf andere Disziplinen sind kaum nachvollziehbar

Die etablierten Methoden zur Systementwicklung müssen den aufgezeigten Herausforderungen gerecht werden, damit die Entwicklung erfolgreich ist. In Kapitel 2.4.2 wird die VDI-Richtlinie 2206 „Entwicklungsmethodik für mechatronische Systeme“ [VDI2206] vorgestellt. Diese bildet die Grundlage in der Entwicklung komplexer Systeme. Anschließend werden in den Kapiteln 2.4.3 und 2.4.4 die Ansätze des Systems Engineering und des Model-Based Systems Engineering dargestellt. Der Denkansatz des SE fördert das Systemdenken und hilft so den aufgezeigten Herausforderungen gerecht zu werden [INC10]. Mit Hilfe der Nutzung abstrakter Modelle ermöglicht das MBSE eine ganzheitliche und gleichzeitig interdisziplinäre Abbildung sowie Herangehensweise für die Entwicklung Intelligenter Technischer Systeme [FMS12]. Zum MBSE gehörige Modellierungstechniken werden in Kapitel 3.3 untersucht. Das Kapitel 2.4.5 befasst sich mit dem Wissensmanagement. Die ausgewählten Ansätze sind im Folgenden näher beschrieben.

2.4.1 Produktentstehung nach GAUSEMEIER

Die **Produktentstehung** ist Teil des Produktlebenszyklus und beschreibt nach GAUSEMEIER den Prozess von der Produkt- bzw. Geschäftsidee bis zum Serienanlauf. Sie umfasst drei Hauptaufgabenbereiche: **Strategische Produktplanung, Produktentwicklung** und **Produktionssystementwicklung**. Diese sind im 3-Zyklen-Modell in Bild 2-10 dargestellt. Die Zyklen sind im Folgenden beschrieben [GP14].

Erster Zyklus: Hier wird durch die strategische Produktplanung der Entwicklungsauftrag erarbeitet. Der erste Zyklus gliedert sich in Potentialfindung, Produktfindung und Geschäftsplanung. Die Identifikation der Erfolgspotentiale der Zukunft und der Handlungsoptionen ist der zentrale Punkt der Potentialfindung. Während der Produktfindung werden Produkt- und Dienstleistungsideen zusammengetragen und Anforderungen formuliert. Im Rahmen der Geschäftsplanung ist eine Geschäftsstrategie festzulegen, ein Produktportfolio zu erarbeiten und ein Geschäftsplan aufzustellen.

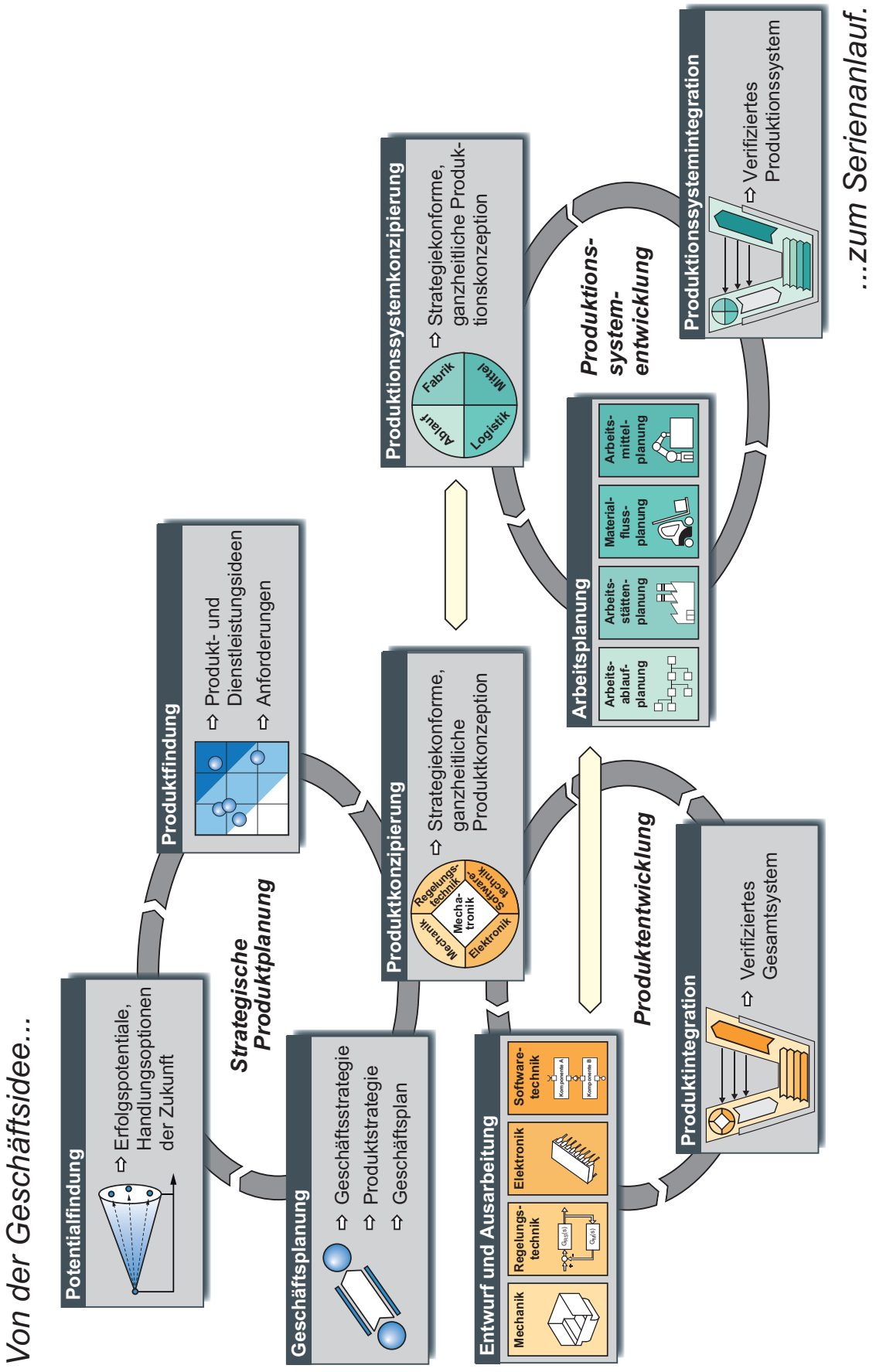


Bild 2-10: Das 3-Zyklen-Modell der Produktentstehung [GP14]

Zweiter Zyklus: Der zweite Zyklus ist die Produktentwicklung. Sie umfasst die Produktkonzipierung, den fachdisziplinspezifischen Entwurf sowie die Ausarbeitung. Darüber hinaus wird die Integration der Ergebnisse zu einer Gesamtlösung betrachtet. In der Phase Produktkonzipierung wird ein Produktkonzept, z. B. bestehend aus dem Funktionsnachweis und einer Prinziplösung, erstellt. Diese Phase bildet die Schnittstelle zu den Zyklen strategische Produktplanung und Produktionssystementwicklung. Nachdem eine prinzipielle Lösung erarbeitet wurde, folgen der disziplinspezifische Entwurf und die entsprechende Ausarbeitung. In der Phase Produktintegration werden die einzelnen Lösungen zu einem verifizierten Gesamtsystem integriert.

Da die Entwicklung von Produkt- und Produktionssystem parallel und in enger Abstimmung zu betrachten ist, gibt es definierte Schnittstellen zwischen dem zweiten und dritten Zyklus. Diese sind die Produkt- und Produktionssystemkonzipierung sowie Entwurf und Ausarbeitung. Die Schnittstellen sind durch die waagerechten Pfeile dargestellt (vgl. Bild 2-10) [GP14].

Dritter Zyklus: Dieser Zyklus ist die Produktionssystementwicklung. Die enge Abstimmung zum zweiten Zyklus ist notwendig, da die Fertigungstechnologien das Produkt beeinflussen und dessen Funktionen einschränken. In der Produktionssystementwicklung wird zunächst eine strategiekonforme und ganzheitliche Produktionskonzeption erstellt. Darauf folgend sind die Arbeitsablauf- und Arbeitsstättenplanung abzuleiten sowie eine Produktionslogistik und Arbeitsmittelplanung zu erarbeiten. Im Zuge der Produktionssystemintegration werden diese Aspekte integriert. Das Ergebnis ist ein verifiziertes Produktionssystem.

Die dargestellten drei Zyklen der Produktentstehung sind als ganzheitliches Wechselspiel zu betrachten. Aus diesem Wechselspiel ergeben sich Überschneidungen. Diese können als integratives Zusammenwirken der Bereiche aufgefasst werden und spiegeln sich ebenfalls in der Grundidee des **SE** wider [AES+12].

Der zu entwickelnden Systematik liegt das 3-Zyklen-Modell der Produktentstehung zugrunde. Um zusätzlich den präventiven Systemschutz zu ermöglichen sind die Schutzanforderungen Intelligenter Technischer Systeme zu identifizieren und zu berücksichtigen (vgl. Kap. 2.3.3). Die Produktanforderungen werden im ersten Zyklus, der Produktfindung, formuliert. Zusätzlich sind die Aspekte des Systemschutzes im Systementwurf zu verankern. Unter Entwurf verstehen DAENZER und HUBER die Erahnung eines Ganzen oder eines Lösungskonzepts. Dies beinhaltet das Erkennen bzw. Finden der dazu erforderlichen Lösungselemente sowie das gedankliche, modellhafte Zusammenbauen und Verbinden dieser Elemente zu einem Ganzen [DH02]. Lösungselemente werden von GAUSEMEIER ET AL. wie folgt definiert:

> *„Lösungselemente sind realisierte und bewährte Lösungen – Baugruppen, Module, Softwarebibliotheken etc. – zur Erfüllung einer Funktion des Gesamtsystems“ [GAC+13, S.11].*

Der Systementwurf ist grundlegender Bestandteil der vorliegenden Arbeit. Dieser wird im zweiten Zyklus, der Produktentwicklung, erarbeitet. Die Entwicklung prinzipieller Lösungen für das angestrebte Produkt wird in der Produktkonzipierung erarbeitet. Bereits während der Entwicklung der prinzipiellen Lösungen sind die Aspekte des Systemschutzes zu berücksichtigen. Aus den genannten Gründen ordnet sich die vorliegende Arbeit in die Produktfindung sowie maßgeblich in die Schnittstelle des ersten und zweiten Zyklus, die Produktkonzipierung, ein.

2.4.2 Entwicklungsmethodik für mechatronische Systeme – VDI 2206

Ein Ansatz der Produktentwicklung ist die Entwicklungsmethodik für mechatronische Systeme – VDI 2206. Der Fokus der Methodik liegt auf der frühen Phase der Entwicklung und auf Systemen mit kontrolliertem Bewegungsverhalten (Klasse 2, Kap. 2.2.2). Der Kern der Methodik ist das in Bild 2-11, rechts gezeigte V-Modell. Dieses wurde aus der Softwareentwicklung übernommen und angepasst [VDI2206].

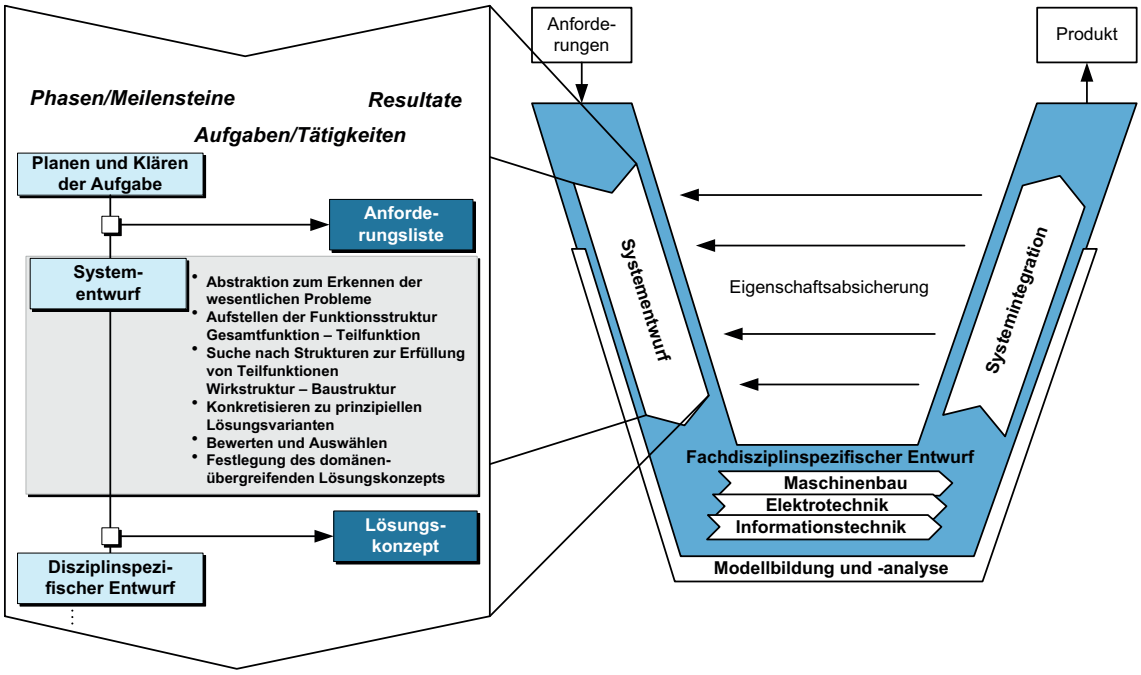


Bild 2-11: Das V-Modell der Entwicklungsmethodik für mechatronische Systeme (rechts) und die Tätigkeiten im Systementwurf (links) [VDI2206, S.32]

Die VDI-Richtlinie 2206 schlägt ein flexibles Vorgehensmodell vor, das die Erfahrungen der industriellen Praxis und die empirische Konstruktionsforschung berücksichtigt. Der Leitfaden besteht im Wesentlichen aus drei Elementen: allgemeiner Problemlösungszyklus auf der Mikroebene, V-Modell auf der Makroebene und vordefinierte Prozessbausteine zur Bearbeitung wiederkehrender Arbeitsschritte bei der Entwicklung mechatronischer Systeme. Die Elemente werden nachfolgend beschrieben [VDI2206].

Problemlösungszyklus auf der Mikroebene: Dieser sieht eine Strukturierung des Vorgehens im Entwicklungsprozess vor. Sie soll unterstützend bei der Produktentwicklung wirken. Der Zyklus staffelt sich in folgende Schritte: Situationsanalyse/Zielformulierung bzw. Zielübernahme/Situationsanalyse, Analyse und Synthese, Bewertung, Entscheidung und Planung des weiteren Vorgehens bzw. Lernen. Der fließende Übergang in weitere Problemlösungszyklen schafft einen effizienten und situationsangepassten Prozessverlauf. Die Dokumentation des gewonnenen Wissens soll zur Optimierung zukünftiger Prozessabläufe beitragen.

V-Modell: Das V-Modell beschreibt das allgemeine Vorgehen zum Entwurf mechatronischer Systeme (Bild 2-11, rechts). Im Folgenden werden die einzelnen Bestandteile und Prozessschritte detailliert erläutert. Der Fokus wird auf den interdisziplinären Systementwurf gelegt. Die **Anforderungen** bilden den Ausgangspunkt der Entwicklung, indem sie einen konkreten Entwicklungsauftrag darstellen. In der Phase *Planen und Klären der Aufgabe* werden die Anforderungen spezifiziert (vgl. Bild 2-11, links). Des Weiteren werden die Anforderungen als Maßstab genutzt, um das entwickelte Produkt zu einem späteren Zeitpunkt zu bewerten.

Das Ziel des **Systementwurfs** ist die Erarbeitung eines disziplinübergreifenden Lösungskonzeptes, welches die zentralen physikalischen und logischen Wirkungsweisen des Systems darstellt. Dazu ist die Aufgabenstellung zunächst zu abstrahieren, um das Problemverständnis zu fördern. Das Aufstellen der Funktionsstruktur aus der Gesamtfunktion ist der nächste Schritt. Hierfür werden notwendigen Teilfunktionen zur Erfüllung der Gesamtfunktion abgeleitet. Die jeweilige Funktion[16] ist lösungsneutral durch eine Kombination aus einem Substantiv und einem Verb zu beschreiben, um die darauf folgende Suche nach Strukturen zur Erfüllung von Teilfunktionen zu vereinfachen (vgl. Bild 2-11, links) [Ana15].

Während dieser Suche wird stets auf das vorhandene Wissen und bereits verfügbare Lösungen zurückgegriffen, eine „*Auswahl wiederverwendbarer Baugruppen*“ ist zu treffen [FG13, S.243]. Die Wiederverwendung der Lösungen wird durch die Dokumentation in ihrer abstrakten Form ermöglicht. Das Ergebnis der Zuordnung von Wirkprinzipien[17] bzw. Lösungselementen zu den Teilfunktionen sind **Prinziplösungen**. Diese werden zunächst bewertet. Durch die Auswahl der besten Lösungsvariante wird ein disziplinübergreifendes Lösungskonzept festgelegt (vgl. Bild 2-11, links).

Nach dem disziplinübergreifenden Entwurf erfolgt der **fachdisziplinspezifische Entwurf**. Dieser charakterisiert die Stufe der Konkretisierung im V-Modell. Sie erfolgt meist getrennt in den beteiligten Fachdisziplinen. Das Ziel ist es, mittels detaillierter

---

[16] Nach PAHL/BEITZ ist eine Funktion ein: *"[…] gewollter Zusammenhang zwischen Eingang und Ausgang eines Systems mit dem Ziel, eine Aufgabe zu erfüllen" [PBF+07, S.783].*

[17] *„Das Wirkprinzip stellt den Lösungsgedanken für eine Funktion auf erster konkreter Stufe dar“ [PBF+07, S.54].*

Auslegung und Berechnung den Funktionsnachweis zu erbringen. Im Rahmen der **Systemintegration** werden die ausgearbeiteten Lösungen zusammengeführt. Daraus resultiert der Gesamtentwurf des mechatronischen Systems. Während der Integration werden die Eigenschaften anhand der Anforderungen abgeglichen und somit abgesichert. Das Ergebnis ist das fertig entwickelte **Produkt** (vgl. Bild 2-11, rechts).

Prozessbausteine für wiederkehrende Tätigkeiten: Die Prozessbausteine werden für regelmäßig wiederkehrende Tätigkeiten im Rahmen der Entwicklung definiert. Die Suche nach vorhandenen Lösungen in den unterschiedlichen Disziplinen steht im Fokus des Systementwurfs. Die Ausarbeitung der Lösungen erfolgt in den einzelnen Disziplinen. Erst bei der Überprüfung der Funktionserfüllung wird ersichtlich, ob eine Kombination der einzelnen Lösungen möglich ist. Somit werden Unstimmigkeiten erst am Ende des Systementwurfs festgestellt.

VDI 2206 im Hinblick auf den Systemschutz

Die Forschung im Bereich Produktpiraterie stellt ein relativ junges und stark interdisziplinäres Forschungsfeld dar [STF09]. Dementsprechend wird nach passenden Methoden und Ansätzen gesucht, um den Systemschutz in die Entwicklung zu integrieren. Die Notwendigkeit dieser Integration wurde vor allem im Kapitel 2.3.3 herausgearbeitet. Die VDI 2206 berücksichtigt in keiner Weise den Schutz der Systeme und wird den aufgezeigte Herausforderungen nicht gerecht. Dies bestätigt die Notwendigkeit der Integration der Aspekte des Systemschutzes in etablierte Standards des Systementwurfs.

VDI 2206 im Hinblick auf den Entwurf Intelligenter Technischer Systeme

Bedingt durch den Innovationssprung von mechatronischen hin zu intelligenten, vernetzten Systemen reichen klassische Entwurfsmethodiken wie die VDI 2206 nicht mehr aus. Zur Beherrschung der Komplexität dieser Systeme sind die stark ausgeprägten Grenzen zwischen den einzelnen Fachdisziplinen aufzuheben und eine Methodik, die eine ganzheitliche und systemorientierte Herangehensweise fördert, einzuführen [GTD13]. Herausforderungen aufgrund steigender Vernetzung, Einbindung zahlreicher Disziplinen in den Entwurf und der Notwendigkeit, das System als Ganzes zu betrachten, zu beherrschen, zu entwickeln sowie zu vermarkten, lassen die VDI 2206 an ihre Grenzen stoßen [Ana15].

Den Herausforderungen wie steigende Komplexität, Berücksichtigung verschiedener fachspezifischer Begrifflichkeiten oder ein unterschiedliches Verständnis des Gesamtsystems, bestehend aus Produkt und Produktionssystem, kann insbesondere durch **SE** begegnet werden [Kai13]. SE versteht sich als durchgängige, fachdisziplinübergreifende Methodik zur Entwicklung technischer Systeme, die alle Aspekte ins Kalkül zieht [INC10].

2.4.3 Systems Engineering

Mechatronische Produkte sind charakterisiert durch das enge Zusammenspiel der Disziplinen Mechanik, Elektrotechnik, Regelungstechnik und Softwaretechnik. Durch ITS kommen noch weitere, teilweise fachfremde Disziplinen hinzu. Ein Grund hierfür ist die Integration von Methoden und Technologien aus nichttechnischen Bereichen z. B. den Kognitionswissenschaften. Mit der Vielzahl an beteiligten Disziplinen steigt auch die Anzahl an involvierten Experten während des Entwicklungsprozesses. Entscheidungen und Aktivitäten in der Entwicklung komplexer Systeme können dementsprechend nicht aus der Sicht einer einzigen Disziplin getroffen werden. Zahlreiche Probleme entstehen aufgrund der ineffizienten Zusammenarbeit der Disziplinen [Hel13, S.22]. Aus diesem Grund erfordert die Systementwicklung – zusätzlich zu den disziplinspezifischen Herausforderungen – die frühzeitige Sicherstellung eines einheitlichen Verständnisses des Gesamtsystems. Daher gewinnt die Abstimmung zwischen den einzelnen Fachdisziplinen bereits im Systementwurf zusehends an Bedeutung [Kai13].

Der Wandel von klassischen Produkten hin zu Systemen ist zudem durch den immer stärker werdenden Softwareanteil und eingebettete Elektronik gekennzeichnet. Die Systeme weisen Charakteristiken auf, die sich grundlegend von den Merkmalen der klassischen Produkte unterscheiden. SENDLER abstrahiert diesen Unterschied auf die Tatsache, dass Produkte aus Bauteilen zusammengebaut, während Systeme in eine Systemlandschaft integriert werden. Die logische Konsequenz ist der Wandel der klassischen Produktentwicklung zum SE [Sen13].

SE ist eine Sichtweise, Herangehensweise bzw. ein Ansatz, der Methoden und Prozesse zur Realisierung von erfolgreichen Systemen zur Verfügung stellt [INC12]. Eine einzige offizielle Definition von SE existiert nicht, jedoch wird in Fachkreisen zumeist die Definition von HITCHINS herangezogen:

> *„Systems Engineering is the art and science of creating whole solutions to complex problems“[Hit07, S.91].*

HABERFELLNER ET AL. strukturieren SE in zwei übergeordnete Bereiche: Die **SE-Denkweise** und den **Problemlösungsprozess**. Dieses Konzept nach HABERFELLNER ET AL. ist in Bild 2-12 dargestellt und wird im Folgenden beschrieben [HWF+12].

Zur SE-Denkweise gehören das **Systemdenken** und das **Vorgehensmodell** des SE. Im Problemlösungsprozess findet die Lösungsfindung statt. Hierbei erfolgt in der Systemgestaltung die eigentliche konstruktive Tätigkeit, während das Projektmanagement das Rahmenwerk für die Organisation darstellt. Das **Systemdenken** fördert den Verstehens- und Gestaltungsprozess von komplexen Systemen. Die dazugehörigen Denkansätze forcieren die ganzheitliche Betrachtung des Systems. Diese soll nach HABERFELLNER ET AL. umgebungsorientiert, wirkungsorientiert und strukturorientiert erfolgen.

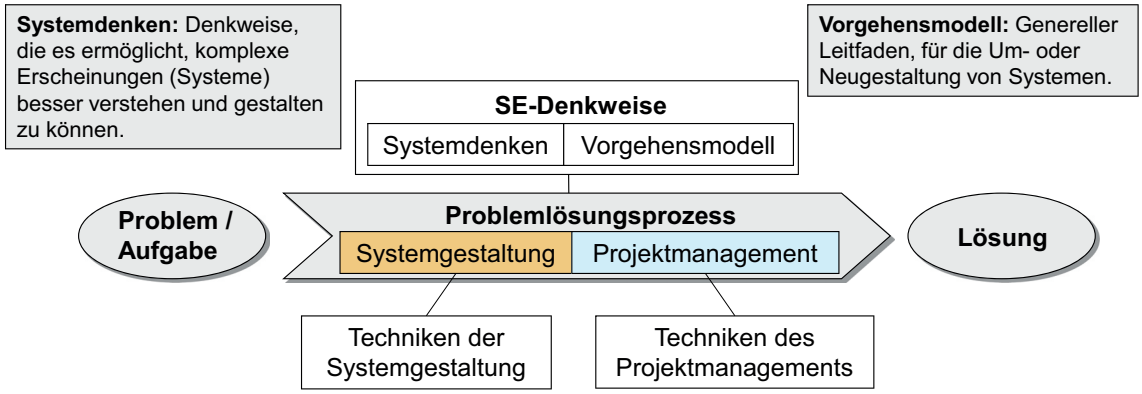


Bild 2-12: Konzept des Systems Engineering [HWF+12]

Das **SE-Vorgehensmodell** liefert vier Grundprinzipien, die im Systementwicklungsprozess kombinierbar sind. Das Ziel des *Top-Down-Vorgehens* ist es, das Betrachtungsfeld, zu Beginn mit hohem Abstraktionsniveau, schrittweise einzuengen und Lösungen für die abschließende Synthese zu erarbeiten. Das *Variantendenken* soll eine möglichst große Bandbreite an Lösungsvarianten bereitstellen. Ein *Phasenablauf* gliedert den Systementwicklungsprozess in zeitlich aufeinander folgende Abschnitte, während im *Problemlösungszyklus* ein Vorgehen definiert wird, das bei der Problemlösung unterstützt.

SE liefert die Basis für den interdisziplinären Entwurf Intelligenter Technischer Systeme. Die Integration der Aspekte des Systemschutzes in den Entwurf ist Betrachtungsgegenstand der vorliegenden Arbeit. Daher ist ein passender Ansatz für den Systementwurf zu identifizieren. Die Beherrschung der Komplexität auf Gesamtsystemebene ist im SE Gegenstand aktueller Forschungsarbeiten. Die Effizienzsteigerung des SE durch die Nutzung abstrakter Modelle (z. B. zur Systembeschreibung) und Förderung des Systemdenkens findet sich im MBSE wieder [Ana15].

2.4.4 Model-Based Systems Engineering

Nach INCOSE ist MBSE das zukünftige Paradigma der Produktentwicklung. MBSE ist ein Ansatz, den neuen Herausforderungen im interdisziplinären Systementwurf effektiv zu begegnen [INC07]. Es liefert die Idee einer ganzheitlichen Systembeschreibung anhand eines Systemmodells, welches bereits in den frühen Phasen der Entwicklung initial angefertigt und während der gesamten Entwicklungszeit fortlaufend aktualisiert wird. Die Reduktion des realen Systems auf ein abstraktes Systemmodell unterstützt das ganzheitliche und für alle Disziplinen gleiche Verständnis des Systems [Rop09].

Das MBSE ordnet sich zwischen der Systemspezifikation anhand von Anforderungen und den Methoden der einzelnen Fachdisziplinen ein. Dies ist in Bild 2-13 aufgezeigt.

MBSE hat das Ziel, den fachdisziplinübergreifenden Entwurf und die Analyse komplexer Systeme mit Hilfe von Modellen sicherzustellen. Im Fokus des MBSE steht das **Systemmodell**, das eine abstrakte und fachdisziplinunabhängige Systembetrachtung

ermöglicht. Dieses bildet die Basis für die Kommunikation und Koordination der verschiedenen Stakeholder in der Entwicklung. Mit der Erstellung des Systemmodells im Rahmen des Systementwurfs wird ein Paradigmenwechsel angestrebt. Somit wird das dokumentenbasierte Vorgehen durch ein modellbasiertes Vorgehen ersetzt [Kai13].

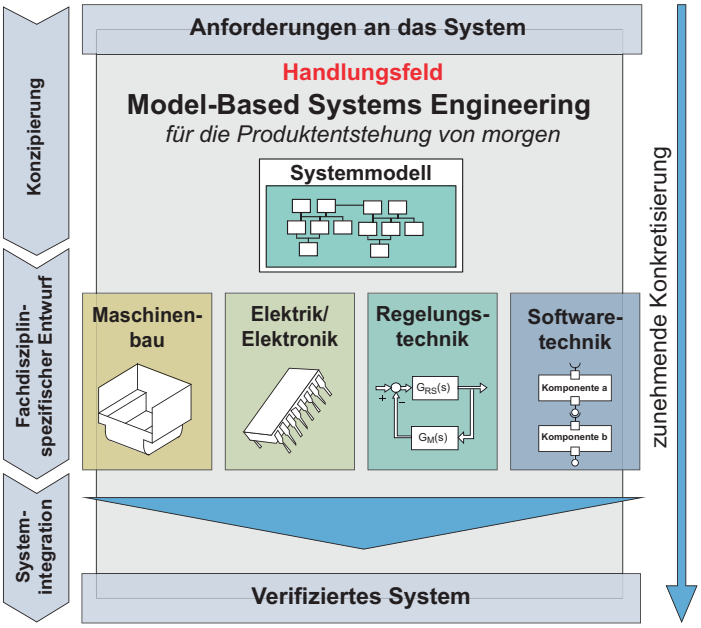


Bild 2-13: Handlungsfelder des Model-Based Systems Engineerings [Ana15] nach [FMS12]

Drei Aspekte sind bei der Erstellung des Systemmodells wesentlich: Anforderungen, Systemarchitektur und Verhalten [Alt12, S.9].

Die **Anforderungen** werden meist in Textform formuliert und spiegeln die zuvor festgelegten Ziele, die von dem fertigen Produkt erreicht werden sollen, wieder [Alt12, S.10]. Werden die Anforderungen nicht eindeutig formuliert oder nicht konsequent verfolgt, werden die Ziele verfehlt. Das Ergebnis stellen kostspielige Änderungen dar, deren Kosten im Produktlebenszyklus exponentiell ansteigen. Je später ein Fehler während der Produktentstehung entdeckt wird, umso höher werden die Kosten zur Behebung dieses Fehlers („rule of ten“) [BGJ+09]. Dieser Zusammenhang lässt sich auf den Systemschutz durch den Einsatz technischer Schutzmaßnahmen übertragen.

KAISER definiert die **Systemarchitektur** als eine Beschreibung der Funktionen, Elemente und deren Wechselwirkungen untereinander. Die Wechselwirkungen umfassen die Beziehungen und die Schnittstellen zwischen den Systemelementen. Unter Systemelementen versteht man physische Bauteile, die sich zu Modulen bzw. Baugruppen zusammenfassen lassen sowie Softwarekomponenten. Die Systemarchitektur bildet also den statischen Aufbau eines Systems als vernetzte Struktur ab, die vielfach auch als Wirkstruktur bezeichnet wird [Kai13], [Ana15].

Die Beschreibung des dynamischen **Verhaltens** vervollständigt das Systemmodell. Neben Funktionen werden Zustände und Zustandsänderungen als abstrakte Darstellungsformen des Verhaltens genutzt [Kai13].

Das Systemmodell stellt das primäre Artefakt im MBSE dar. Es ist als integriertes Rahmenwerk der interdisziplinären Systementwicklung zu betrachten [FMS12]. Die Einsatzmöglichkeiten des Systemmodells sind in Bild 2-14 dargestellt.

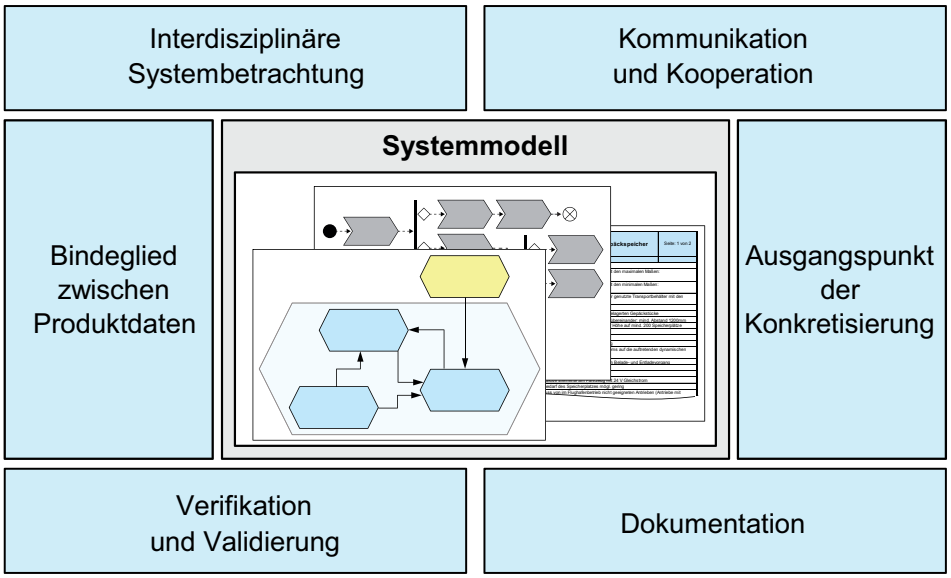


Bild 2-14: Einsatzbereiche des Systemmodells [Kai13, S.27]

Das Systemmodell ermöglicht vor allem die ganzheitliche und interdisziplinäre Betrachtung des Systems. Es kann zusätzlich als Plattform für die Kommunikation der an der Entwicklung beteiligten Fachdisziplinen genutzt werden. So wird ein einheitliches Verständnis des Systems gefördert. Auch die Dokumentation der disziplinübergreifenden Informationen erfolgt im Systemmodell. Zusätzlich fungiert es als Ausgangspunkt der Konkretisierung. Die einzelnen Fachdisziplinen beginnen mit dem Entwurf und der Ausarbeitung des Systems auf Basis der Informationen des Systemmodells. Darüber hinaus wird es als Bindeglied zwischen den Produktdaten sowie zur Validierung eingesetzt (vgl. Bild 2-14) [Kai13, S.26ff.].

Eine weitere Einsatzmöglichkeit des Systemmodells ist die Reduzierung der Komplexität einer Entwicklungsaufgabe. Dies wird mittels der Bildung von Sichten ermöglicht. So können durch die Anwendung von Filtern z. B. nur einzelne Betriebssituationen, Elemente, Elementklassen oder bestimmte Beziehungen dargestellt werden. Die Filterung erfolgt z. B. über den Typ der Beziehung. Nur die Elemente, die in Beziehungen zum gefilterten Typ stehen, werden angezeigt, alle anderen Elemente werden optisch in den Hintergrund gerückt. Je nach Zweck und Anwendung können verschiedene Sichten auf das Modell generiert werden z. B. die energiespezifische, stoffspezifische, informationsspezifische, messtechnische oder gestaltorientierte Sicht [Kai13], [GLL12].

SE und MBSE im Hinblick auf den Systemschutz

Weder SE noch MBSE berücksichtigen die Aspekte des Systemschutzes. Jedoch kann die Denkweise des SE als Grundlage für die Betrachtung des Systemschutzes bereits während des Systementwurfs herangezogen werden. Die modellbasierte Entwicklung des MBSE bietet die Möglichkeit, die im Kapiteln 2.3.3 aufgezeigten Verbesserungspotentiale umzusetzen. Insbesondere für die fachdisziplinübergreifende Beschreibung der Maßnahmen werden die Ansätze des MBSE berücksichtigt und weiterentwickelt.

SE und MBSE im Hinblick auf den Entwurf Intelligenter Technischer Systeme

SE kann die Forderung nach einer ganzheitlichen Denkweise erfüllen. Die einfache Handhabung und das leichte Verständnis der graphischen Modelle des MBSE ermöglichen ein einheitliches und fachdisziplinunabhängiges Verständnis des Gesamtsystems.

Mit Hilfe des MBSE wird die Zusammenarbeit der einzelnen Disziplinen unterstützt und die Komplexität der Systeme beherrschbar. Allerdings nimmt die Anzahl an zu berücksichtigenden Schnittstellen im Systementwurf stetig zu. Die eindeutige Beschreibung, kontinuierliche Pflege und die Kommunikation bei Änderungen sind entscheidend für den Erfolg der gesamten Entwicklung. Die Beschreibung des Systems, Sammlung der Informationen und durchgehende Aktualisierung der Daten in einem übergeordneten Systemmodell bietet derzeit das größte Potential für eine erfolgreiche Entwicklung [Ana15]. Für den Entwurf komplexer, intelligenter Systeme bietet das MBSE einen vielversprechenden Ansatz, der in der vorliegenden Arbeit berücksichtigt wird.

Für die Entwicklung Intelligenter Technischer Systeme ist ein interdisziplinäres Wissensmanagement erforderlich. Diese Thematik wird im Folgenden vorgestellt.

2.4.5 Wissensmanagement mit Lösungsmustern

ITS sind bereits während des Entwurfs durch das Zusammenwirken unterschiedlicher Fachdisziplinen charakterisiert. Durch die gestiegene Anzahl involvierter Experten ist die Entwicklung dieser Systeme ein höchst wissensintensiver Prozess. Dementsprechend wird die Wiederverwendung bereits existierender Lösungen immer bedeutender. Nicht zuletzt durch den demografischen Wandel, ist ein geeignetes Wissensmanagement als fester Bestandteil eines jeden Unternehmens zu sehen [GLL12], [AG12].

Aus diesem Grund erfordert die Systementwicklung zusätzlich zu den disziplinspezifischen Herausforderungen noch eine geeignete Herangehensweise zum Speichern und Kombinieren relevanten Wissens. Diese zeichnet sich dadurch aus, dass die Aufbereitung und Nutzung des Wissens vereinfacht, der zeitliche Aufwand für die Wissensaufbereitung so gering wie möglich gehalten und eine proaktive Unterstützung während des Entwurfs ermöglicht wird [GDS13], [Ana15].

Wissensformen

Wie bereits in Kapitel 2.1 angesprochen, soll mit der angestrebten Systematik vor allem das **produktgebundene, systeminhärente Know-how** geschützt werden. Um einen effektiven Schutz zu gewährleisten, soll das bereits erfolgreich eingesetzte Wissen zum Systemschutz wiederverwendet werden. Der Begriff Wissen wurde allgemein in Kapitel 2.1 eingeführt. An dieser Stelle wird auf die weitere Unterteilung des Begriffs eingegangen. Es ist zwischen implizitem und explizitem Wissen zu unterschieden.

Implizites Wissen: Unter impliziertem Wissen versteht POLANYI nicht formalisiertes Wissen, welches nicht vollständig mit Worten ausgedrückt werden kann. Implizites Wissen ist als eine Art Reflex zu verstehen, den Personen in bestimmten Situationen abrufen [Pol66, S.4ff.]. ANACKER überarbeitet diese Definition von implizitem Wissen und versteht es vielmehr als stillschweigend verfügbares Wissen, welches z. B. in den Köpfen der Experten vorhanden ist [Ana15].

Explizites Wissen: Das explizite Wissen ist formalisiertes Wissen, welches in einer abstrakten Form vorliegt. Die abstrakte Form kann bspw. eine Sprache sein. Diese Art des Wissens lässt sich sowohl transferieren als auch kommunizieren, z. B. durch die Weitergabe von Wissen anhand von Lehrbüchern [Ana15, S.29].

SECI-Modell

Zur Erklärung des Ablaufs der Wissenserzeugung in Unternehmen, eignet sich das SECI-Modell. Das Modell besteht aus den vier Phasen *Sozialisation* (Socialisation), *Externalisierung* (Externalization), *Kombination* (Combination) und *Internalisierung* (Internalization) (SECI). Diese Phasen werden kontinuierlich durchlaufen. So wird das individuelle Wissen innerhalb eines Unternehmens auf höhere Organisationsstufen wie Personengruppen oder die gesamte Organisation gehoben. Das SECI-Modell ist in Bild 2-15 abgebildet. Die Phasen werden im Folgenden beschrieben [NT97, S.84ff.].

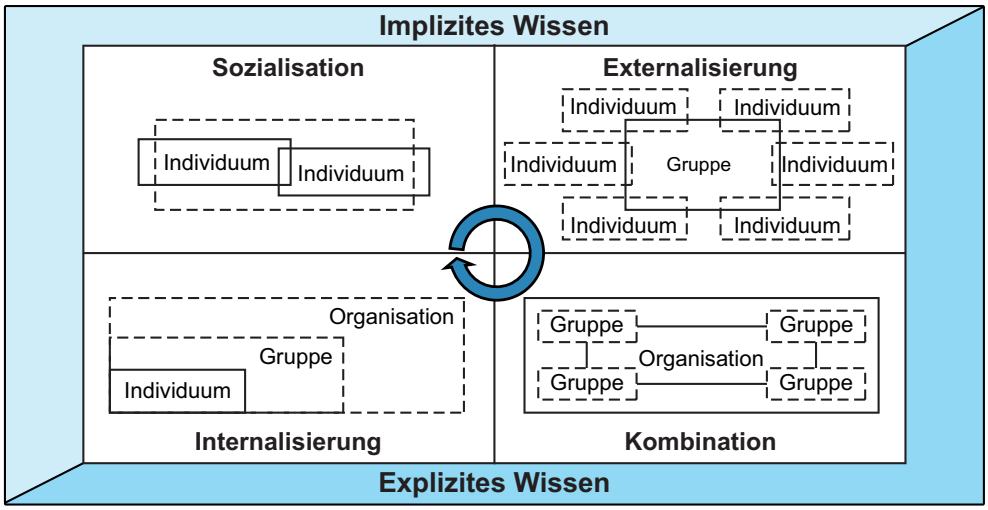


Bild 2-15: SECI-Modell nach NONAKA und TAKEUCHI [NT97, S.84]

Sozialisation (Austausch von implizitem Wissen): In der ersten Phase entsteht ein Austausch von implizitem Wissen zwischen Individuen. Dieser Austausch kann durch gemeinsame Erfahrungen, Beobachtungen oder Nachahmung von bestimmten Handlungen erfolgen. Aufgrund der Tatsache, dass der Wissensaustausch überwiegend stillschweigend verläuft, ist es nur begrenzt möglich, vorhandenes Wissen zu übertragen. Die Integration eines neuen Mitarbeiters in die Denk- und Arbeitsroutinen einer Abteilung kann als ein Beispiel für diesen Prozess gesehen werden.

Externalisierung (implizites Wissen wird zu explizitem Wissen): In dieser Phase findet die Umwandlung von implizitem in explizites Wissen statt. Voraussetzung ist, dass schwer beschreibbare Zusammenhänge allgemeinverständlich wiedergegeben werden. Analogien zu bekannten Sachverhalten wirken hierbei unterstützend. Ebenso bieten sich Visualisierungen in Form von Modellen und Diagrammen an. Durch die Zusammenarbeit von Individuen in Gruppen kann das Wissen aufgezeichnet und übertragen werden. Die Beteiligten der Gruppe erreichen den gleichen Stand an explizitem Wissen.

Kombination (Austausch von explizitem Wissen): Durch die Kombination wird das in der Externalisierung gewonnene Wissen erweitert. Dies geschieht maßgeblich durch den Zusammenschluss der verschiedenen Gruppen. Die Nutzung von Informationstechnologie ermöglicht den Zugang zu Wissen für alle Mitarbeiter der Organisation.

Internalisierung (explizites Wissen wird zu implizitem Wissen): Das im Kombinationsprozess generierte Wissen wird nun von den einzelnen Mitarbeitern in ihren Fachabteilungen angewendet. Das explizite Wissen wird durch den Bezug auf individuelle Sachverhalte teilweise wieder in implizites Wissen der Individuen umgewandelt.

Die Analyse des SECI-Modells verdeutlicht, dass sich die Experten der Fachdisziplinen über spezifische Sachverhalte und ihr Zusammenwirken nur dann austauschen können, wenn eine übergreifende Plattform für die Dokumentation und Pflege von Wissen existiert. Eine solche Plattform kann in Form von Lösungsmustern realisiert werden.

Lösungsmuster

Das in Unternehmen vorhandene Wissen sollte effektiv eingesetzt werden. In der Literatur finden sich zahlreiche Ansätze des Wissensmanagements. Nach ANACKER sind Muster der geeignetste Ansatz für das Wissensmanagement in Bezug auf die Produktentstehung von fortgeschrittenen mechatronischen Systemen (vgl. Kap. 3.4.3).

Muster beschreiben die Zusammenfassung einer Problemstellung in ihrer Umgebung und der dazugehörigen Lösung. Somit stellt ein Muster eine Lösung für ein spezifisches Problem dar. Diese Lösung bezieht sich auf einen bestimmten Kontext [Bar98], [Has05]. Die Wissensrepräsentation eines Musters unterteilt sich in die Kategorien Name, Problem, Lösung und Kontext. Der Kern ist somit eine verallgemeinerte Problem- und Lösungsbeschreibung. Muster tragen zur Lösung eines übergeordneten Gesamtproblems bei, indem zuerst das Problem in einzelne Teilprobleme zerlegt wird. An-

schließend wird für die Teilprobleme eine Lösung erarbeitet. Durch das Zusammenführen der Teilprobleme wird das übergeordnete Gesamtproblem gelöst [AIS+95].

ANACKER definiert für die Produktentstehung den Begriff **Lösungsmuster** wie folgt:

> *„[…] Ein Lösungsmuster umfasst eine explizite und generalisierte Beschreibung eines Problems sowie der zugehörigen Lösung (Problem-Lösungs-Paar). Lösungsmuster unterstützen den Menschen bei der Erzeugung von Artefakten. Artefakte in der Produktentstehung sind u. a. Objekte (Organisationsstruktur, CAD-Modell, Systemmodell, Softwarecode, Arbeitsplan etc.) oder Prozesse (Ablauforganisation, Vertriebsprozess, Entwicklungsprozess etc.)“ [Ana15, S.91].*

Demnach werden Lösungsmuster den Anforderungen an ein durchgängiges Wissensmanagement gerecht. Diese Anforderungen sind z. B. die Unterstützung des fachdisziplinübergreifenden Entwurfs sowie seine Einbettung in die Produktentstehung. Darüber hinaus bieten Muster eine Kombination aus den Stärken der Konstruktionswissenschaft und des Systems Engineering [Ana15].

Zusätzlich sind Lösungsmuster in der Lage, die **Forderungen aus der Industrie** zur Weiterentwicklung und Anwendbarkeit des SE zu erfüllen. Diese Forderungen beziehen sich hauptsächlich auf drei Aspekte. Der erste Aspekt ist die *Interdisziplinarität* der Wissensrepräsentation und -präsentation. Durch Lösungsmuster ist die disziplinübergreifende Verständlichkeit für alle an der Produktentwicklung beteiligten Fachdisziplinen gleichermaßen gegeben. Die Forderung der *Modellbasiertheit* kann durch Muster in Form von Modellen und der damit einhergehenden Möglichkeit zur Integration in die Entwicklung erfüllt werden. Zur Erfüllung der *Durchgängigkeit* muss die kontinuierliche Anwendung von nur einem Konzept über alle Phasen der Produktentwicklung hinweg sichergestellt sein. Lösungsmuster erfüllen diese Forderung, indem sie den nahtlosen Übergang zwischen den einzelnen Disziplinen ermöglichen [GDS13], [Ana15].

ANACKER fasst auf Basis eines umfangreichen Literaturüberblicks ([Ris98], [Ris00], [Dei09], [SZ03], [Suh93]) folgende Vorteile von Lösungsmustern zusammen [Ana15]:

- **Übertragbarkeit:** Lösungsmuster ermöglichen die sprachenunabhängige Wiederverwendung sowie Repräsentation von Wissen. Aufgrund der einheitlichen Struktur ist die Übertragbarkeit auf alle an der Produktentstehung beteiligten Fachdisziplinen sichergestellt.
- **Verbesserung der Kommunikation:** Lösungsmuster sind in der Lage die Kommunikation innerhalb eines Unternehmens zu verbessern und bilden folglich eine Plattform, um abgeschlossene Entwicklungstätigkeiten und entwicklungsrelevantes Wissen zu reflektieren.
- **Langfristige Dokumentation:** Das implizite Wissen, welches z. B. durch die über Jahre aufgebaute Erfahrung einzelner Mitarbeiter vorliegt, kann mit Lösungsmus-

tern externalisiert und somit übersichtlich und langfristig Dritten zur Verfügung gestellt werden.

- **Komplexitätsreduktion:** Mit der Zerteilung des komplexen Gesamtproblems in einzelne Probleme kann die Komplexität besser beherrscht werden. Die Teillösungen werden durch die Lösungsmuster repräsentiert.
- **Effizienzsteigerung:** Die Effizienz in Problemlösungsprozessen lässt sich mit Lösungsmustern steigern. Diese bieten die Möglichkeit, Erfahrungswissen zu externalisieren und anschließend zielgerichtet in neue Entwicklungen einzubringen.
- **Förderung der Kreativität:** Lösungsmuster unterstützen die Kreativität, da die enthaltenen Informationen spezifisch an die jeweilige Aufgabe angepasst werden müssen. Im Vergleich zu detaillierten Lösungen bieten Lösungsmuster abstrahierte (generalisierte) Informationen, die mit dem eigenen Wissen abgeglichen und anhand der Denkmuster reflektiert werden müssen.

Lösungsmuster im Hinblick auf den Systemschutz

Trotz offenkundiger Vorteile der modellbasierten Darstellung fand bis dato kein Einzug des Systemschutzes in modellbasierte Ansätze statt. Bisherige Schutzmaßnahmen sind textbasiert in Form von Steckbriefen beschrieben (vgl. Kap. 3.1). Allgemein stellen auch Steckbriefe eine Art Muster dar [Dum10]. Aus diesem Grund wird die strukturierte Beschreibung von Schutzmaßnahmen (z. B. durch Steckbriefe) als **Schutzmuster** definiert. Die textbasierte Beschreibung der Schutzmuster erschwert das interdisziplinäre Verständnis, da zahlreiche Schutzmaßnahmen mechatronische Funktionen darstellen. So wird die disziplinübergreifende Berücksichtigung der Maßnahmen im Systementwurf erschwert. Die Vermutung, dass das notwendige Lösungswissen für die Schutzmaßnahmen von Unternehmen zum Teil nicht identifiziert werden kann, wird von ANACKER bestärkt (vgl. [Ana15, S.27ff.]). Insbesondere das implizite Unternehmenswissen, das z. B. personengebunden gespeichert ist, lässt sich durch textbasierte Steckbriefe nicht allgemein verständlich abbilden.

Damit der Systemschutz sichergestellt werden kann, ist die Darstellung von Schutzmaßnahmen für ITS zu modifizieren. Hierdurch muss ihre Zugänglichkeit vereinfacht und die Anwendung verbessert werden. Als möglicher Ansatz hierfür sind Lösungsmuster geeignet und vielversprechend.

Lösungsmuster im Hinblick auf den Entwurf Intelligenter Technischer Systeme

Der Entwurf intelligenter Systeme ist durch Herausforderungen wie die steigende Komplexität der Systeme, die zunehmende Interdisziplinarität sowie die Intensivierung des Know-hows geprägt (vgl. Kap. 2.2.3, 2.4). Um diesen Herausforderungen effektiv zu begegnen, sind geeignete Herangehensweisen zum Explizieren, Speichern und Kombinieren von relevantem Wissen erforderlich [GDS13].

Lösungsmuster erfüllen alle Anforderungen für die Unterstützung der Systementwicklung und bilden eine Kombination aus den Stärken der Konstruktionswissenschaft und des SE. Insbesondere in den frühen Phasen der Entwicklung Intelligenter Technischer Systeme bieten Lösungsmuster einen vielversprechenden Ansatz zur Steigerung der Entwicklungseffizienz und werden als eine sinnvolle Erweiterung des MBSE angesehen. So lassen sich Lösungsmuster z. B. bei der Erstellung des Systemmodells verwenden. Hierdurch wird die Anwendung des MBSE unterstützt. Darüber hinaus wird das Lösungswissen unterschiedlicher Disziplinen gleichwertig behandelt, allgemeinverständlich beschrieben und kann somit miteinander kombiniert werden [Ana15].

2.5 Problemabgrenzung

In der vorliegenden Problemanalyse wurden Herausforderungen für den Schutz Intelligenter Technischer Systeme beschrieben. Zusammenfassend lässt sich festhalten, dass die Erhaltung des Wettbewerbsvorsprungs durch Innovationen die größte und zugleich wichtigste Herausforderung im Zuge der Weiterentwicklung von mechatronischen hin zu Intelligenten Technischen Systemen darstellt. Dies belegt auch die von acatech[18] postulierte Kausalkette: Wohlstand braucht Beschäftigung braucht Innovation braucht Bildung [GW11]. Damit sich der angestrebte Innovationssprung für die Unternehmen rentiert, müssen die innovativen Systeme wirkungsvoll vor unerlaubtem Nachbau und illegalem Know-how-Abfluss geschützt werden. Hierfür sind aus der beschriebenen Problemanalyse fünf grundsätzliche **Herausforderungen** besonders hervorzuheben:

Effektiver und wirkungsvoller Systemschutz: Aufgrund der neuen Fähigkeiten der Systeme ergeben sich neue Möglichkeiten für Produktpiraten. Daher stellen ITS neue Herausforderungen an den angestrebten Systemschutz. Die aus den Herausforderungen resultierenden Schutzanforderungen sind beim Schutz der Systeme zwingend zu berücksichtigen (Kap. 2.3.3). Bestehende Schutzmaßnahmen müssen auf ihre Wirkung überprüft und ggf. müssen neue Maßnahmen gesichtet werden, um die Schutzanforderungen bestmöglich zu erfüllen.

Systemschutz während des Systementwurfs: Gleichzeitig steigt die Komplexität der Systeme, wodurch neue Entwicklungsmethoden benötigt werden (vgl. Kap. 2.2, Kap. 2.4). Bedingt durch die Komplexität ist eine nachträgliche Ausstattung der Systeme mit Schutzmaßnahmen oft nicht mehr möglich (Kap. 2.3.3). Dementsprechend müssen Schutzmaßnahmen bereits im Systementwurf berücksichtigt werden.

Integration des Schutzes in bestehende Entwurfsmethoden: Ein wirksamer Systemschutz ist nur möglich, wenn die Facetten des Schutzes in moderne Methoden für den interdisziplinären Systementwurf integriert werden. So wird der Systemschutz bereits in den frühen Entwicklungsphasen sowie durchgängig während des gesamten Entwick-

[18] Deutsche Akademie der Technikwissenschaften

lungsprozesses berücksichtigt. Die interdisziplinäre Systementwicklung wird insbesondere durch die fachdisziplinübergreifende, modellbasierte Erstellung eines Systemmodells sowie die Wiederverwendung von Lösungswissen geprägt (Kap. 2.4).

Interdisziplinäre Anwendung von Schutzmaßnahmen: Um eine Integration des Systemschutzes in Entwurfsmethodiken sicherzustellen, ist die Darstellung der Schutzmaßnahmen zu überarbeiten. Die klassische, textbasierte Beschreibung von Maßnahmen in Form von Steckbriefen ist nicht mehr ausreichend, nicht zuletzt, da der Systemschutz nicht mehr nur von einer Fachdisziplin betrachtet wird. Die Aspekte der Schutzmaßnahmen sind modellbasiert z. B. mit semiformalen Modellen zu beschreiben (Kap. 2.3.3). Hierdurch erlangen alle Fachdisziplinen sowie fachfremde Disziplinen ein einheitliches Verständnis der Schutzmaßnahmen.

Wiederverwendung von Lösungswissen bei Schutzmaßnahmen: Sowohl ITS als auch deren Schutzmaßnahmen entwickeln sich fortlaufend weiter. Zukünftige Maßnahmen werden von zahlreichen Disziplinen gleichermaßen entwickelt und eingesetzt. Die Intensität des benötigten Know-hows zur Entwicklung, Implementierung und Umsetzung einer Schutzmaßnahme steigt stetig an (Kap. 2.4.5). Daher muss auch für Schutzmaßnahmen die Wiederverwendung von bereits erfolgreich eingesetztem Lösungswissen ermöglicht werden.

Es besteht entsprechender Bedarf für eine *Entwurfssystematik für den präventiven Schutz Intelligenter Technischer Systeme vor Produktpiraterie*. Die zu entwickelnde Systematik nimmt sich den aufgezeigten Herausforderungen an und lässt sich in einen Wissensbereich (Wissen über Schutzanforderungen und wirksame Schutzmaßnahmen für ITS) sowie einen Entwurfsbereich (Vorlagen und Vorgehen für den Entwurf geschützter ITS) unterteilen. Die Systematik gliedert sich in die in Bild 2-16 abgebildeten drei Handlungsfelder (HF).

HF 1: Identifikation wirksamer Schutzmaßnahmen

Das erste Handlungsfeld resultiert aus der Herausforderung *effektiver und wirkungsvoller Systemschutz.* Um wirksame Schutzmaßnahmen für ITS bereitzustellen, sind in einem ersten Schritt die **Schutzanforderungen Intelligenter Technischer Systeme** zu identifizieren. Anhand dieser Schutzanforderungen sind zunächst bekannte Schutzmaßnahmen auf ihre Wirkung für den Systemschutz zu überprüfen.

Zum einen sind die Schutzanforderungen der Systeme größtenteils unbekannt, zum anderen werden die Angriffe auf die Systeme vielfältiger. Auf Basis des gestiegenen systeminhärenten Know-hows, der Teilintelligenz sowie zahlreicher Schnittstellen der Systeme (z. B. durch Netzwerkfähigkeiten), ergeben sich neue Möglichkeiten einen Angriff zu platzieren. Zusätzlich wird die Anzahl der Angriffe weiter zunehmen. Darüber hinaus ist der Fortschritt bei der Weiterentwicklung der Angriffe größer, als bei der Entwicklung neuer Schutzmaßnahmen [WEF14]. Aus diesem Grund sind wirksame

Schutzmaßnahmen für ITS zu identifizieren. Diese müssen die Schutzanforderungen bestmöglich erfüllen, also einen hohen Wirkungsgrad aufweisen.

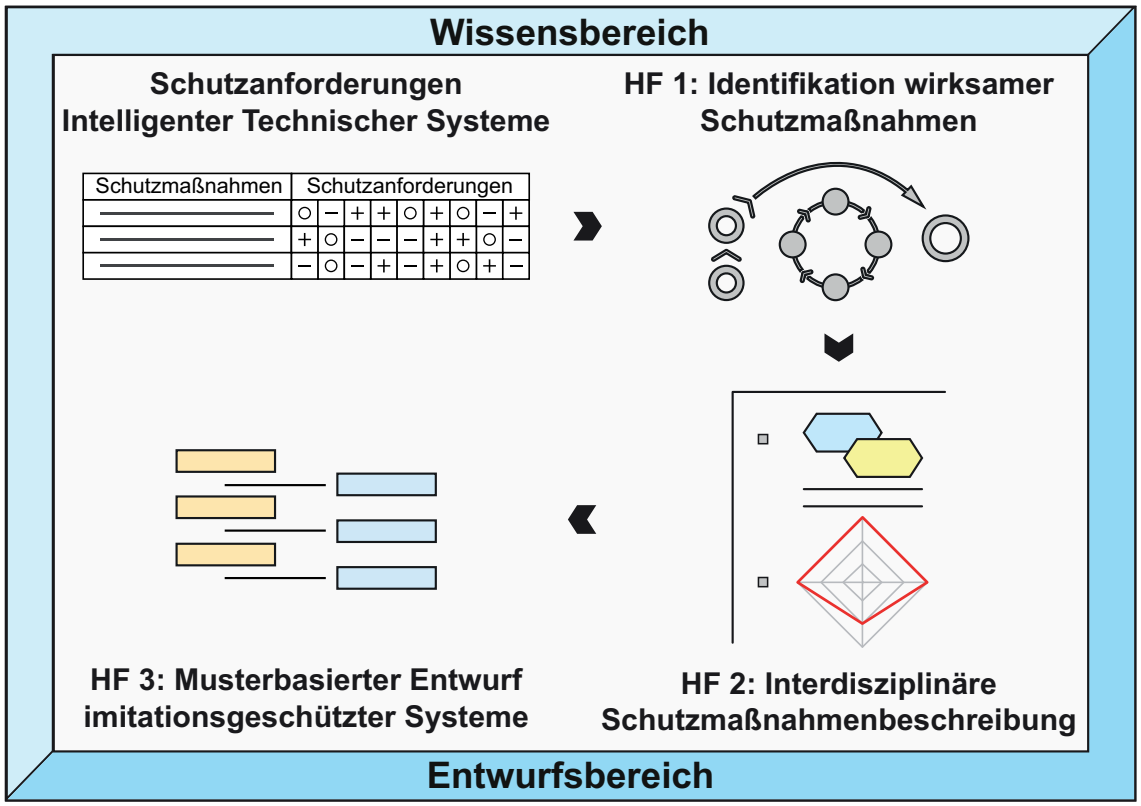


Bild 2-16: Identifizierte Handlungsfelder

HF 2: Interdisziplinäre Schutzmaßnahmenbeschreibung

Das zweite Handlungsfeld vereint die Herausforderungen *Systemschutz während des Systementwurfs, interdisziplinäre Anwendung von Schutzmaßnahmen* sowie *Wiederverwendung von Lösungswissen bei Schutzmaßnahmen*. Die Systementwicklung wird zunehmend durch die hohe Anzahl involvierter Fachdisziplinen und einer daraus resultierenden Steigerung der Komplexität geprägt. Der modellbasierte Entwurf beschreibt das System ganzheitlich in einer Art und Weise, die jede Fachdisziplin gleichermaßen lesen und nachvollziehen kann (Kap 2.4.4). Bereits während des Entwurfs sind die Aspekte des Schutzes zu berücksichtigen. Damit Schutzmaßnahmen von allen Disziplinen gleichermaßen verstanden und eingesetzt werden, muss dessen Beschreibung adaptiert werden. Die aktuell textbasiert beschriebenen Maßnahmen müssen in eine modellbasierte, fachdisziplinübergreifende Darstellungsform überführt werden (Kap. 2.3.3).

Ein weiterer zu berücksichtigender Aspekt ist die Wiederverwendung von bereits erfolgreich eingesetztem Lösungswissen. Hierfür sind die Strukturierung und Abstraktion der Lösungsmuster auf die Darstellung der Schutzmaßnahmen zu adaptieren. Durch den Einsatz von Lösungsmustern wird die Möglichkeit geschaffen, kollektives Erfahrungswissen zielgerichtet in neue Entwicklungsprojekte einzubringen. Dies steigert die Effizienz in Problemlösungsprozessen signifikant.

HF 3: Musterbasierter Entwurf imitationsgeschützter Systeme

Das dritte Handlungsfeld ergibt sich aus der Herausforderung *Integration des Schutzes in bestehende Entwurfsmethoden* und baut auf den anderen beiden Handlungsfeldern auf. Es beschreibt die Integration der Aspekte des Systemschutzes in den Entwurf Intelligenter Technischer Systeme. Die beste Methode zum Systemschutz ist zwecklos, wenn sie in der Praxis nicht angewendet wird. Daher wird größter Wert auf die Verankerung der Aspekte des Schutzes in bestehende Ansätze gelegt. Somit soll es den Entwicklern mit überschaubarem zusätzlichem Aufwand möglich sein, den Schutz der Systeme bereits während des Entwurfs zu berücksichtigen.

Als Grundlage für die Integration in bestehende Entwurfsmethoden dienen die ersten beiden Handlungsfelder. Nur so können wirkungsvolle Schutzmaßnahmen in das modellbasierte Entwicklungsvorgehen integriert und eine effektive Entwicklung präventiv geschützter Intelligenter Technischer Systeme sichergestellt werden.

2.6 Anforderungen an die Arbeit

Aus der Problemanalyse resultieren folgende Anforderungen an eine *Entwurfssystematik für den präventiven Schutz Intelligenter Technischer Systeme vor Produktpiraterie*:

A1) Charakterisierung ITS-spezifischer Schutzanforderungen: ITS stellen neue, besondere Herausforderungen an ihren Schutz. Bedingt durch die steigende Anzahl an Schnittstellen, die Durchdringung der Systeme mit Informationstechnologie sowie die Vernetzung mit anderen Systemen ergeben sich für einen wirksamen Schutz zahlreiche neue Schutzanforderungen. Der wirksame Schutz für ITS ist eine zentrale Herausforderung, die es zu lösen gilt. Daher müssen für den Systemschutz die charakteristischen Anforderungen bekannt sein und berücksichtigt werden (vgl. HF 1, Kap. 2.3.2, 2.3.3).

A2) Bereitstellung passender Schutzmaßnahmen für ITS: Durch neue Funktionen und innovative Eigenschaften stellen ITS neue Anforderungen an ihren Schutz, sog. Schutzanforderungen. Auf dieser Grundlage sind bisherige Schutzmaßnahmen auf ihre Wirkung zu überprüfen. Neue Schutzmaßnahmen sind zu identifizieren und bestehende Maßnahmen weiterzuentwickeln. Aus allen Maßnahmen sind die für ITS wirkungsvollsten zu bestimmen (vgl. HF 1, Kap. 2.3.3).

A3) Darstellung der Kompetenzen der Imitatoren und der Angriffsmöglichkeiten: Um die Wirkung einer Maßnahme entsprechend darzustellen, muss aufgezeigt werden, gegen welche Angriffe und Imitatoren die Maßnahme Schutz bietet. Zusätzlich ist die Kenntnis sowohl über die Kompetenzen der Imitatoren als auch über mögliche Angriffe entscheidend, um passende Schutzmaßnahmen auszuwählen (vgl. HF 1, Kap. 2.3.3).

A4) Interdisziplinarität und Ganzheitlichkeit: Ebenso wie ITS selber zeichnen sich auch innovative Schutzmaßnahmen dadurch aus, dass sie die Expertise unterschiedlicher Fachdisziplinen vereinen. Aus diesem Grund ist für die Schutzmaßnahmen ein ein-

heitliches und ganzheitliches Verständnis über sämtliche Fachdisziplinen hinweg zu schaffen. Dieser Herausforderung wird mit Hilfe einer geeigneten Wissensdarstellung begegnet. Diese stellt sicher, dass der Einsatz der Schutzmaßnahmen über sämtliche Fachdisziplinen hinweg gleichermaßen ermöglicht wird (vgl. HF 2, Kap. 2.3.3, 2.4.5).

A5) Modellbasierte Maßnahmenbeschreibung zur Verwendung im Systementwurf: Um eine frühzeitige Berücksichtigung der Schutzmaßnahmen sicherzustellen, sind die Maßnahmen zum Schutz von ITS zu adaptieren. Graphische Modelle, im Kontext des MBSE, verfolgen das Ziel der Effizienzsteigerung sowie der Kostenminimierung in der Entwicklung. Schutzmaßnahmen müssen darauf adaptiert werden und sind generalisiert sowie modellbasiert darzustellen. Hierdurch kann der Systemschutz bereits im Entwurf beachtet werden (vgl. HF 2, Kap. 2.3.3).

A6) Wiederverwendung von Lösungswissen: Ebenso wie ITS und deren Entwicklung werden auch die Schutzmaßnahmen für ITS zunehmend komplexer und wissensintensiver. Dies liegt darin begründet, dass an der Entwicklung und dem Einsatz der Schutzmaßnahmen für ITS zahlreiche Fachdisziplinen involviert sind. Die Verwendung modellbasierter Lösungsmuster bietet die Möglichkeit, bereits bekanntes und einst erfolgreich eingesetztes Lösungswissen zu externalisieren, allen Disziplinen gleichermaßen zur Verfügung zu stellen und es somit erneut erfolgreich einzusetzen. Hierfür ist die textbasierte Beschreibungsform von Schutzmaßnahmen in eine modellbasierte Form zu überführen (vgl. HF 2, Kap. 2.3.3, 2.4.5).

A7) Frühzeitige und durchgängige Berücksichtigung des Systemschutzes: Die Aspekte des Systemschutzes für ITS sind bereits frühzeitig, das bedeutet in den frühen Phasen der Produktentwicklung, zu planen [Kok13, S.7], [Gru10, S.112]. Bedingt durch die steigende Anzahl an Fachdisziplinen sowie die größer werdende Komplexität der Systeme, nimmt die Bedeutung der frühzeitigen Berücksichtigung der Aspekte des Systemschutzes immer weiter zu. Der Systemschutz muss bereits im Entwurf betrachtet werden, da hier ein interdisziplinäres Lösungskonzept festgelegt wird. So wird ebenfalls die durchgängige Betrachtung sichergestellt (vgl. HF 3, Kap. 2.3.3, 2.4.4).

A8) Integration in etablierte Standards des Systementwurfs: Die Berücksichtigung des Systemschutzes soll möglichst geringen Mehraufwand für die Entwickler erzeugen. Aus diesem Grund sollen die Aspekte des Schutzes in ein etabliertes Vorgehen zum Entwurf von ITS integriert werden. Der Systemschutz wird so automatisch beim Systementwurf mitberücksichtigt und durchgängig betrachtet (vgl. HF 3, Kap. 2.3.3, 2.4).

A9) Präventiver Schutz auf Basis technischer Maßnahmen: Der Schutz für ITS soll präventiv wirken, das bedeutet, dass die Wirkung der Schutzmaßnahmen eintritt bevor ein Schaden entstehen kann. Dies soll durch technische Schutzmaßnahmen realisiert werden (vgl. HF 3, Kap. 2.1, 2.3.3).

3 Stand der Technik

Dieses Kapitel gibt einen Überblick über den Stand der Technik. Aus der Problemanalyse wird deutlich, dass der Schutz für ITS aktuell nicht ausreichend gewährleistet werden kann. Hieraus resultiert das erste Handlungsfeld: Wirksame Schutzmaßnahmen für ITS müssen identifiziert werden. Um diese These zu überprüfen befasst sich der Stand der Technik mit **bestehenden Schutzmaßnahmen und deren Darstellung**. Diese sind in Kapitel 3.1 beschrieben. Kapitel 3.2 gibt einen Überblick über den **Entwurf präventiv imitationsgeschützter Systeme**. Um die Forderung des zweiten Handlungsfeldes nach einer interdisziplinären Beschreibung von Schutzmaßnahmen zu erfüllen, werden in Kapitel 3.3 **Modellierungstechniken** und in Kapitel 3.4 Strukturierungen **interdisziplinärer Entwurfsmuster** untersucht. Durch die Auswahl einer geeigneten Modellierungstechnik sowie einer passenden Struktur wird die Grundlage für die modellbasierte Beschreibung der Schutzmaßnahmen geschaffen. Um den in Handlungsfeld 3 behandelten musterbasierten Entwurf imitationsgeschützter Systeme zu realisieren, wird in Kapitel 3.5 der **musterbasierte Entwurf Intelligenter Technischer Systeme** untersucht. Der Stand der Technik wird komplettiert durch die Bewertung der Ansätze anhand der Anforderungen aus Kapitel 2. Die Reihenfolge der Ansätze stellt keine Bewertung dar.

3.1 Bestehende Schutzmaßnahmen und deren Darstellung

Dieses Kapitel gibt einen Überblick über bestehende Schutzmaßnahmen gegen Produktpiraterie sowie deren Darstellung als Schutzmuster (vgl. Kap. 2.4.5). Untersucht werden Sammlungen von Schutzmaßnahmen nach ABELE ET AL. (Kap. 3.1.1), LINDEMANN ET AL. (Kap. 3.1.2) sowie GAUSEMEIER ET AL. (Kap. 3.1.3). Bei der Untersuchung wird auf die Anzahl, Kategorisierung, Beschreibung und Darstellung der Maßnahmen sowie auf individuelle Besonderheiten der Autoren eingegangen.

3.1.1 Schutz vor Produktpiraterie nach ABELE ET AL.

ABELE ET AL. beschreiben die Herausforderungen für den Schutz des Know-hows. Ferner zeigen sie eine Methodik auf, mit der das unternehmensspezifische Risiko ermittelt wird. Die zahlreichen beschriebenen Maßnahmen zur Abwehr von Produktpiraterie werden kategorisiert als: Kennzeichnungstechnologien, Maßnahmen der Produktgestaltung, Maßnahmen der Unternehmensprozessgestaltung, juristische Absicherung zum erfolgreichen Produktschutz sowie Mehrwertstrategien zur Verhinderung von Produktpiraterie [AKL11]. Aufgrund der Abgrenzung der vorliegenden Arbeit (vgl. Kap. 2.1) werden hauptsächlich die Maßnahmen der Produktgestaltung untersucht.

Schutzmaßnahmen, die sowohl die Entwicklung als auch die Konstruktion eines Produktes beeinflussen, werden als **Maßnahmen der Produktgestaltung** kategorisiert. Sie dienen dem Schutz des Know-hows, welches in den Produkten vorhanden ist. Die Maß-

nahmen haben als maßgebliches Ziel, die Möglichkeit des Reverse Engineering zu unterbinden. Sie werden untergliedert in [Sch11]:

Konstruktive Maßnahmen: Die Berücksichtigung konstruktiver Schutzmaßnahmen erschwert das Reverse Engineering. Werden konstruktive Maßnahmen im Entwicklungsprozess berücksichtigt, so wird der Umgang mit dem Produkt-Know-how während der Entwicklung erleichtert. Beispiele sind Kapselung[19] und De-Standardisierung.

Methoden der Produktgestaltung: Hier liegt der Fokus auf der Erfüllung von Kundenwünschen. Bestehende Methoden der Produktgestaltung werden angepasst, damit sowohl gegen illegale Imitatoren als auch legale Wettbewerber ein Schutz realisiert werden kann. Beispiele sind Erhöhung der Variantenvielfalt und Verkürzung von Innovationszyklen.

Integration von Sicherheitssystemen: In dieser Unterkategorie werden IT-basierte Sicherheitssysteme vorgestellt. Diese stammen aus der Softwaretechnik und werden für den Einsatz gegen Produktpiraterie angepasst. Beispielhafte Maßnahmen sind die Produktaktivierung, die gegenseitige Identifizierung der Komponenten durch IT sowie der Einsatz von Dongles[20].

Darstellung als Schutzmuster

Die Schutzmaßnahmen sind in Textform beschrieben. Eine einheitliche Strukturierung der Maßnahmenbeschreibung ist nicht auszumachen.

Bewertung

ABELE ET AL. kategorisieren bestehende Schutzmaßnahmen und beschreiben die einzelnen Kategorien. Weiterhin sind zahlreiche Unterkategorien beschrieben und die jeweils zugehörigen Schutzmaßnahmen aufgeführt. Die Beschreibung der Maßnahmen ist sehr oberflächlich und verlässt die Ebene der allgemeinen Beschreibung nur selten. Die Schutzmaßnahmen sind in Textform beschrieben, konkrete Beispiele sind nur bei wenigen Maßnahmen hinterlegt. Ein intuitives sowie disziplinübergreifendes Verständnis der Schutzmaßnahmen kann nicht sichergestellt werden. Produktspezifische Herausforderungen für den Schutz, je nach Komplexität und Intelligenz eines Produktes, werden aufgezeigt (vgl. Bild 2-9). Jedoch wird in der Beschreibung der Schutzmaßnahmen nicht näher darauf eingegangen. Somit kann auch der Schutz Intelligenter Technischer Systeme nicht hinreichend sichergestellt werden.

---

[19] Die Schutzmaßnahme Kapselung integriert in das Produkt einen Selbstzerstörungsmechanismus. Bei der Demontage wird die gekapselte Produktkomponente zerstört und kann nicht mehr untersucht und nachgebaut werden [Sch11].

[20] Dongles haben ihren Ursprung in der Softwaretechnik und waren dafür gedacht, das Kopieren von Software zu verhindern. Die Dongles wurden angepasst und dienen z. B. auch dem Schutz von Maschinensteuerungen [Sch11, S.54].

3.1.2 Know-how-Schutz im Wettbewerb nach LINDEMANN ET AL.

LINDEMANN ET AL. greifen auf die Ergebnisse der Forschungsoffensive „Innovationen gegen Produktpiraterie“ zurück und entwickeln einen Leitfaden, um Wissensschutz zu ermöglichen und Produktpiraterie zu bekämpfen. Sie analysieren die Aspekte des Systemschutzes und diskutieren typische Herausforderungen im Kontext von Produktpiraterie. Darüber hinaus wird der ungewollte Know-how-Verlust analysiert und Wissensschutzmechanismen aufgezeigt. Es werden 72 Schutzmaßnahmen beschrieben. LINDEMANN ET AL. beschreiben ein generisches Vorgehen um Schutzkonzepte zu erarbeiten. Diese Konzepte bestehen aus mehreren, aufeinander abgestimmten Schutzmaßnahmen. So wird ein breiter Schutz vor Produktpiraterie ermöglicht [LMP+12a].

Darstellung als Schutzmuster

Die Schutzmaßnahmen sind textbasiert in Form eines **Steckbriefs** dargestellt. Beispielhaft ist ein Steckbrief im Anhang A1.1 abgebildet.

Der Steckbrief zur Darstellung der Schutzmaßnahmen beinhaltet eine *Maßnahmenbeschreibung* und nennt die *Vor- und Nachteile der Schutzmaßnahme*. Die Beschreibungen sind stichpunktartig dargestellt. Zusätzlich werden die *Einsatz- und Randbedingungen* beschrieben. Hier werden die Aspekte Wirkung (präventiv oder reaktiv), der zeitliche Einsatz der Wirkung (sofort, weniger als ein Monat, weniger als ein Jahr oder mehr als ein Jahr) und die Anwendbarkeit im Produktentstehungsprozess (PEP) unterschieden. In der Kategorie Anwendbarkeit wird die für den Einsatz der Maßnahme passende Phase des PEP (Produktkonzeption, -entwicklung, Zulieferkonzeption, Fertigungsplanung, Fertigung, Vertrieb oder Service) vorgeschlagen [LMP+12a].

Ferner wird eine *Klassifizierung der Imitatoren* erarbeitet. Durch diese wird aufgezeigt, gegen welche Imitatoren die Schutzmaßnahme am wirkungsvollsten ist. Die Klassifizierung wird anhand der folgenden Merkmale bestimmt [LMP+12a, S.104].

Fertigungskompetenz: Die Fertigungskompetenz beschreibt die Fähigkeiten, Fertigkeiten sowie das Wissen, welches die Imitatoren über die Herstellung von Materialien, Erzeugnissen und Produkten besitzen.

Entwicklungskompetenz: Hier werden die Fähigkeiten, Fertigkeiten sowie das Wissen dargestellt, um die Lösung eines technischen Problems zu erarbeiten.

Kundenzugang: Dieser beschreibt den Grad der Erreichbarkeit des Kundenkreises.

Finanzstärke: Stellt die Höhe der zur Verfügung stehenden finanziellen Mittel dar.

Beziehung zwischen Originalhersteller und Nachahmer: Auf Grundlage dieses Merkmals wird unterschieden, ob mögliche Imitatoren z. B. Kunden, Lieferanten, Lizenznehmer oder unabhängige Dritte sind.

Zuletzt wird auf die *Hebel* eingegangen, durch welche die Wirkung erzielt wird. Es wird zwischen drei Hebeln unterschieden: Reduzierung des Angebots der Imitatoren, Redu-

zierung der Nachfrage nach Nachahmungen sowie Minimierung des Know-how-Verlusts. Die Reduzierung des Angebots der Imitatoren kann z. B. durch die Verminderung der Kostenvorteile des Plagiators, die Erhöhung des rechtlichen Risikos oder die Erschwerung des Know-how-Zugangs erreicht werden. Möglichkeiten um die Nachfrage nach Nachahmungen zu reduzieren, sind z. B. die Verkürzung der Innovationszyklen, die Sensibilisierung der Kunden gegenüber Produktpiraterie oder die Verbesserung der Originalprodukte im Vergleich zu den Plagiaten. Indem die legale oder illegale Informationsweitergabe unterbunden wird, kann der Know-how-Verlust minimiert werden. Eine Schutzmaßnahme kann mehrere Hebel gleichzeitig bedienen. Ebenso können mehrere Möglichkeiten zur Nutzung des Hebels vorhanden sein [LMP+12a].

Bewertung

Die Anzahl der aufgeführten Schutzmaßnahmen ist mit 72 sehr hoch. Die Maßnahmen sind übersichtlich, jedoch oberflächlich in Form von textbasierten Steckbriefen dargestellt. Konkrete Anwendungsbeispiele für den praktischen Einsatz der Schutzmaßnahmen fehlen. Die gewählte Darstellung erschwert die Integration der Schutzmaßnahmen in den modellbasierten Systementwurf, da die textbasierte Beschreibung hierfür in die modellbasierte Spezifikation des Systems zu überführen ist. Hervorzuheben ist die direkte Verortung der Schutzmaßnahmen im PEP, wenngleich dies nur sehr generisch geschieht. Auf eine Kategorisierung der Schutzmaßnahmen wird nicht eingegangen, dafür werden die Wirkungen der Maßnahmen ausführlich beschrieben. Insbesondere die Klassifizierung der Imitatoren ist anzusprechen. Sie zeigt auf, gegen welche Kompetenzen die Schutzmaßnahme wirkungsvoll ist und zwingt die Originalhersteller zeitgleich, sich mit den Imitatoren auseinanderzusetzen. Die Klassifizierung bildet eine gute Ausgangsbasis, muss jedoch für den Schutz Intelligenter Technischer Systeme angepasst werden.

3.1.3 Präventiver Produktschutz nach GAUSEMEIER ET AL.

GAUSEMEIER ET AL. zeigen eine Übersicht der Ergebnisse der Forschungsoffensive „Innovationen gegen Produktpiraterie“ auf. Es werden 85 Schutzmaßnahmen vorgestellt, kategorisiert und beschrieben. Darüber hinaus präsentieren sie ein generisches Vorgehensmodell zur Entwicklung von Schutzkonzeptionen. Auf Basis des Bündelns einzelner Schutzmaßnahmen lassen sich Schutzkonzepte entwickeln. So wird die Wirkung der einzelnen Maßnahmen verstärkt und ein ganzheitlich angelegter Schutz realisiert. Die Schutzmaßnahmen werden anhand der Kategorisierung nach KOKOSCHKA eingeordnet (vgl. Kap. 2.3.2, Bild 2-8). Diese Darstellung erlaubt die Zuordnung der Maßnahmen zu den jeweiligen Kategorien. Es ist anzumerken, dass die Kategorien untereinander abhängig sind und sich die Schutzmaßnahmen nicht immer eindeutig zuordnen lassen [GGL12].

Darstellung als Schutzmuster

Die Schutzmaßnahmen sind in Steckbriefen textbasiert beschrieben (vgl. Bild 3-1).

Gegenseitige Authentifizierung von Komponenten

Kurzbeschreibung

Bei der gegenseitigen Authentifizierung wird eine Austauschkomponente von einer Steuerungseinheit einer Anlage/Maschine auf ihre Originalität überprüft.

© Paul Fleet - Fotolia.com

Anwendungen / Vorgehen

Beim Einbau eines Ersatzteils in eine Anlage/Maschine wird das Bauteil durch die Maschinensteuerung authentifiziert, indem sie von der Austauschkomponente zuvor definierte Daten abfragt (z. B. über RFID-Chips). Nur wenn die Komponente über die geforderten Daten verfügt, wird sie von der Anlage für ihre Funktion zugelassen. Damit wird seitens des Originalherstellers angestrebt, dass durch den Kunden Originalteile verwendet werden. Bei Verwendung von Originalteilen werden dem Kunden beispielsweise verlängerte Garantiezeiträume oder bestimmte Verfügbarkeiten der Maschine zugesichert. Erweist sich bei der Authentifizierung ein Ersatzteil als Fälschung, erhält der Benutzer eine Meldung darüber, die quittiert werden muss. Somit entsteht eine Absicherung gegen Schadensansprüche durch Versagen von Anlagen aufgrund gefälschter Ersatzteile. Eine Abschaltung der Maschine bei Verwendung von Nichtoriginalteilen ist nach deutschem Recht nicht zulässig. Die gegenseitige Authentifizierung von Komponenten erfolgt entweder durch in der Komponente eingebettete Steuerungssoftware oder durch Sensoren, die Austauschkomponenten ohne eigene Steuerungs- oder Produktsoftware erkennen.

Unternehmensbereiche

- ☐ Produktplanung
- ■ Entwicklung / Konstruktion
- ☐ Einkauf
- ☐ Arbeitsvorbereitung
- ☐ Fertigung
- ☐ Vertrieb
- ■ Service

Kategorie Schutzmaßnahme

- ☐ Strategische Maßnahme
- ■ Produktbezogene Maßnahme
- ■ Prozessbezogene Maßnahme
- ☐ Kennzeichnende Maßnahme
- ■ IT-Maßnahme
- ☐ Rechtliche Maßnahme
- ☐ Kommunikationsmaßnahme

Anwendungsbeispiel

Im Projekt ProOriginal wurde ein Fräsbearbeitungszentrum vom Typ DMC 65 H duoBLOCK® der Firma Deckel Maho Gildemeister (DM… Komponenten von Festo ausgestattet. Die Authentifizierung… läuft nach deren Einbau automatisiert ab. D…

Bild 3-1: Steckbrief für die gegenseitige Authentifizierung von Komponenten [GGL12, S.263] (Auszug)

Zuerst wird die Schutzmaßnahme in einer *Kurzbeschreibung* erläutert. Anschließend werden existierende *Anwendungen bzw. Vorgehen* aufgezeigt, welche den Schutz ermöglichen. Hierdurch wird die Maßnahme detaillierter beschrieben und ein erster Bezug zur Umsetzung in der Praxis hergestellt. Zusätzlich kann im Ansatz so bereits erfolgreich eingesetztes Wissen wiederverwendet werden. Die für die Maßnahme passenden *Unternehmensbereiche* sowie die *Kategorie der Schutzmaßnahme* sind ebenfalls aufgelistet. Die Unternehmensbereiche werden unterschieden in Produktplanung, Entwicklung/Konstruktion, Einkauf, Arbeitsvorbereitung etc. [GGL12].

Um den Bezug zur Praxis zu intensivieren, werden *Anwendungsbeispiele* für den Maßnahmeneinsatz dargestellt. Anschließend werden *Vor- und Nachteile* beschrieben. Zuletzt werden noch *Quellen bzw. Experten* für die jeweilige Schutzmaßnahme genannt. Beispielhafte Steckbriefe sind vollständig im Anhang A1.2 dargestellt.

Bewertung

GAUSEMEIER ET AL. zeigen 85 Schutzmaßnahmen auf und beschreiben sie textbasiert in Steckbriefen. So werden die Beschreibung, Anwendungen, Einsatzbereiche, der Nutzen sowie die Vor- und Nachteile der Schutzmaßnahmen dargestellt. Allerdings werden z. B. die Funktionsweise sowie die die technische Umsetzung nicht so beschrieben, dass sie von allen am Entwurf beteiligten Fachdisziplinen gleichermaßen verstanden werden können. Zusätzlich kann die Integration der Schutzmaßnahmen in den Entwurf Intelligenter Technischer Systeme nicht sichergestellt werden, da hierfür die modellbasierte Spezifikation der Maßnahmen erforderlich ist. Hervorzuheben ist der konkrete Bezug zu bereits existierenden Vorgehen sowie die zahlreichen Anwendungsbeispiele aus der industriellen Praxis. In Ansätzen kann bereits erfolgreich eingesetztes Wissen wiederverwendet werden, da für jede Maßnahme Anwendungen beschrieben werden. Mit Hilfe der Kategorisierung können die Schutzmaßnahmen leicht zugeordnet werden. Dies hilft zudem bei der Suche nach passenden Maßnahmen. Eine Klassifizierung der Imitatoren ist nicht zu finden. Aufgrund der textbasierten Beschreibungen kann das disziplinübergreifende Verständnis nicht ausreichend sichergestellt werden.

3.2 Entwurf präventiv imitationsgeschützter Systeme

Arbeiten zum Thema Systemschutz sind keinesfalls nur in jüngster Vergangenheit entstanden. Ebenfalls gehören Maßnahmen außerhalb juristischer Strategien bereits seit den achtziger Jahren zum Stand der Technik. HARVEY und RONKAINEN entwickelten 1985 Strategien zum Produktschutz. Diese basieren zwar im Wesentlichen auf juristischen Strategien, dennoch werden auch organisatorische Ansätze aufgezeigt. Als technische Maßnahme wird die Kennzeichnungstechnologie Labeling beschrieben [HR85].

Die im Folgenden aufgezeigten Arbeiten gehen über das Sammeln von Schutzmaßnahmen (vgl. Kap 3.1) hinaus und liefern Ansätze für den Entwurf präventiv imitationsgeschützter Systeme. In Kapitel 3.2.1 ist die Methodik zum Schutz gegen Produktimitationen beschrieben. Kapitel 3.2.2 zeigt den präventiven Nachahmungsschutz von technischen Produkten. Im Kapitel 3.2.3 liegt der Fokus auf dem Know-how-Schutz von virtuellen Produktmodellen. Die in Kapitel 3.2.4 vorgestellte Arbeit entwickelt ein Schutzkonzept für Investitionsgüter. Abschließend wird in Kapitel 3.2.5 ein Verfahren zur Konzipierung imitationsgeschützter Produkte und Produktionssysteme untersucht.

3.2.1 Methodik zum Schutz gegen Produktimitationen nach NEEMANN

Zum Schutz gegen Produktimitationen entwickelt NEEMANN ein sieben-stufiges Vorgehensmodell. Dieses ist in Bild 3-2 dargestellt. Die einzelnen Phasen werden im Folgenden erläutert [Nee07].

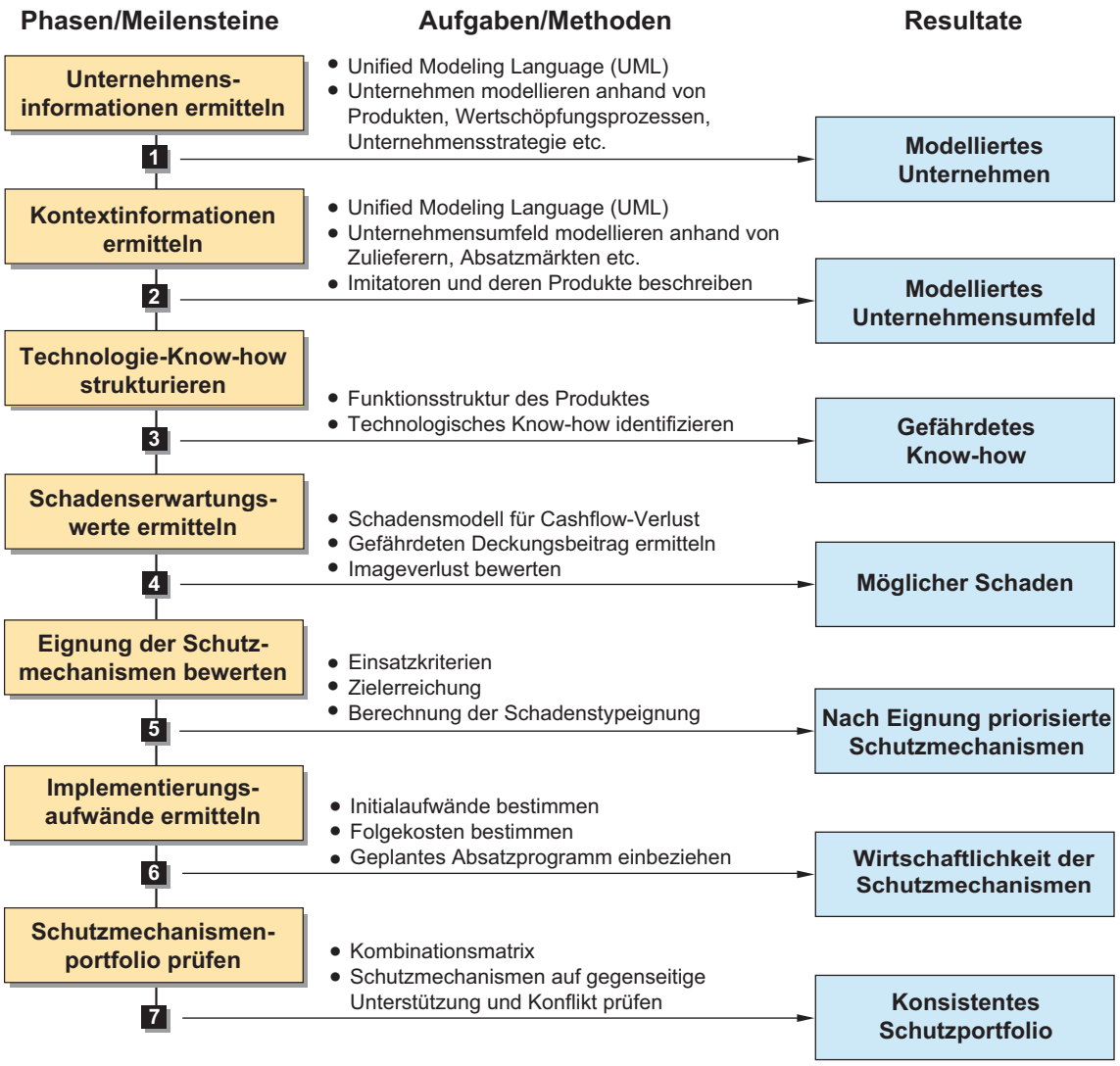


Bild 3-2: Vorgehensmodell der Methodik zum Schutz gegen Produktimitationen nach NEEMANN *[Nee07, S.150]*

Unternehmensinformationen ermitteln: In der ersten Stufe wird das Unternehmen mit der UML modelliert. Durch die Abbildung des Produktportfolios, der Unternehmensstrategie, des Produkt- und Prozess-Know-hows sowie des Schutzmaßnahmenportfolios werden die Unternehmensinformationen und deren Zusammenhänge ermittelt.

Kontextinformationen ermitteln: Mit Hilfe der UML wird das Unternehmensumfeld modelliert. In diesem werden Kontextinformationen über Kunden, Zulieferer und Absatzmärkte erfasst. Für die jeweiligen Absatzmärkte wird untersucht, welche Originalprodukte und welche Imitate angeboten werden.

Technologie-Know-how strukturieren: In dieser Phase wird das technologische Know-how identifiziert und bewertet. Die Identifikation geschieht mit der systematischen Zerlegung ausgewählter Produkte. Die Produkt- und Funktionsstruktur werden analysiert. Anschließend erfolgt die Zuordnung der einzelnen Produktkomponenten zu sog. Technologie-Know-how-Elementen. Zur Ermöglichung der Bewertung des techno-

logischen Know-hows untersucht NEEMANN die Produkte und Prozesse. Die Beiträge zum Erreichen von Wettbewerbsvorteilen stehen im Fokus. Auf Basis der Untersuchung werden Produktfunktionen aufgezeigt, die im besonderen Maße zur Produktdifferenzierung am Markt beitragen. Diesen werden die Technologien zur Funktionserfüllung zugeordnet. Zu den Technologien werden sog. Produkt-Know-how-Elemente eingeteilt.

Die Prozesse werden auf den Beitrag zur Erreichung von wertschöpfungsbedingten Wettbewerbsvorteilen untersucht. Diesen Prozessschritten werden sog. Prozess-Know-how-Elemente zugeteilt. Resultat ist das gefährdete Produkt- und Prozess-Know-how.

Schadenserwartungswerte ermitteln: Die Schadenserwartungswerte ermitteln sich aus der Multiplikation der Schadenswerte für ein Schutzobjekt und der Auftretenswahrscheinlichkeit von Produktpiraterie. Die Schadenswerte werden anhand von Einflussfaktoren wie Cashflow-Verlust, Imageverlust und Kosten für Produkthaftungsprozesse bestimmt. Die Auftretenswahrscheinlichkeit von Produktpiraterie wird anhand von Einflussfaktoren wie Marktgröße, Produktpreis sowie dem Technologieniveau der eingesetzten Produkt- und Produktionstechnologie abgeschätzt.

Eignung der Schutzmechanismen bewerten: Die Bewertung der sog. Schutzmechanismen (geeignete Schutzmaßnahmen) erfolgt anhand der Einsatzkriterien, der Schadenstypeignung und der Zielrichtung. Die Einsatzkriterien wurden maßnahmenspezifisch von NEEMANN erarbeitet. Die Schadenstypeignung bezieht sich auf die Art der Imitation (Markenpiraterie, Überproduktion, sklavische Kopie oder Konzeptkopie). Die Zielrichtung bewertet, ob eine Maßnahme gegen die oben genannten Schadenserwartungen (Cash-Flow-Verlust, Imageverlust, Kosten für Produkthaftungsprozesse) wirkt. Resultierend ergeben sich anhand ihrer Eignung priorisierte Schutzmechanismen.

Implementierungsaufwände ermitteln: In dieser Phase werden die Implementierungsaufwände bestimmt. Diese setzen sich zusammen aus den Initialaufwänden und den jährlichen Folgekosten. So kann die Wirtschaftlichkeit der identifizierten Schutzmechanismen ermittelt werden.

Schutzmechanismenportfolio auf Konsistenz prüfen: Abschließend wird das Portfolio der Schutzmechanismen geprüft. Die Prüfung erfolgt in Form einer Konsistenzprüfung mit einer Kombinationsmatrix. Diese gibt Auskunft darüber, ob sich Schutzmechanismen gegenseitig unterstützen oder behindern.

Die aufgezeigte Methodik wird durch das auf Microsoft-Excel basierende Tool TeknoPro (Technology Know-how Protection) unterstützt. Insbesondere bei der Ermittlung der Erwartungswerte des Schadens (Phase 4), der Eignungsbewertung (Phase 5) und der Ermittlung der Implementierungsaufwände (Phase 6) ist das Werkzeug hilfreich.

Bewertung

NEEMANN beschreibt eine Methodik zum Schutz gegen Imitationen von Produkten. Er unterscheidet Schutzmaßnahmen nach deren Wirkung auf bestimmte oder alle Produkte

des Unternehmens. Zusätzlich kategorisiert er die vorhandenen Schutzmaßnahmen. Im Vorgehensmodell wird die UML verwendet, um das Unternehmen und sein Umfeld zu modellieren. Er ordnet den einzelnen Produktkomponenten Technologie-Know-how-Elemente zu. Jedoch werden diese nicht explizit definiert. Anhand einer detaillierten Untersuchung der Produkte und Prozesse identifiziert er schützenswertes Produkt- und Prozess-Know-how. Zum Schutz des schützenswerten Know-hows werden Schutzmaßnahmen auf deren Eignung und Wirtschaftlichkeit hin analysiert und bewertet.

Die Methodik geht nicht im Detail auf die Produktentwicklung ein und ordnet sich ebenfalls nicht in bestehende Entwicklungsansätze ein. Daher muss die recht komplexe Methodik losgelöst von der Entwicklung durchlaufen werden. Zudem fehlt es an einer disziplinübergreifenden und ganzheitlichen Betrachtung.

3.2.2 Präventiver Nachahmungsschutz bei technischen Produkten nach SCHNAPAUFF

SCHNAPAUFF schlägt ein fünf-stufiges Modell zur Gestaltung eines präventiven Nachahmungsschutzes von technischen Produkten vor. Das Vorgehensmodell ist in Bild 3-3 abgebildet. Die fünf Phasen werden nachfolgend detailliert beschrieben [Sch09].

Gefährdungsanalyse: In der ersten Phase werden relevante Daten mit dem Fokus auf Produktpiraterie erhoben. Diese Daten werden mit Hilfe von Befragungen, Messebesuchen, Recherchen und Beobachtungen von Schutzrechtsanmeldungen Dritter gesammelt. In die sich anschließende Risikobewertung fließen verschiedene Analysen ein. Diese Analysen betreffen die aktuelle Situation, mögliche Schäden, Nachahmungsattraktivität und Nachahmungswahrscheinlichkeit sowie bereits bestehende Nachahmungshürden. Für jedes Produkt wird so der Handlungsbedarf abgeleitet.

Eingrenzung des Schutzgegenstands: In diesem Schritt wird zunächst kritisches Know-how identifiziert. Die Identifikation ist angelehnt an das Prozessmodell zur Identifikation von Kernkompetenzen nach ROGULIC[21] und unterteilt sich in vier Phasen: Vorbereitung, Wissensentwicklung, Lokalisierung und Beurteilung. Die Identifikation des kritischen Know-hows stellt einen Teil der Lokalisierung dar und beinhaltet eine Analyse der Produkte und Wertschöpfungsprozesse. Bei der Analyse der Produkte werden vorausgewählte relevante Komponenten und Baugruppen bzgl. Markt- und Know-how-Kriterien bewertet. Komponenten, die ein relevantes Kaufkriterium aufweisen, werden mit einer hohen Marktbedeutung eingestuft. Hingegen werden Zukaufteile eher mit einer geringen Know-how-Intensität bewertet. Die priorisierten Baugruppen, die als besonders Know-how-kritisch eingestuft wurden, bilden die Basis für die Schutzsystemgestaltung. Die zu schützenden Know-how-Komponenten der Wertschöpfungspro-

[21] Für weitere Informationen sei auf [Rog99] und [Rog00] verwiesen.

zesse werden anhand der Wertkettenanalyse nach PORTER[22] ermittelt. Dadurch werden die Arbeitsschritte mit besonders hohem Know-how-Niveau ermittelt.

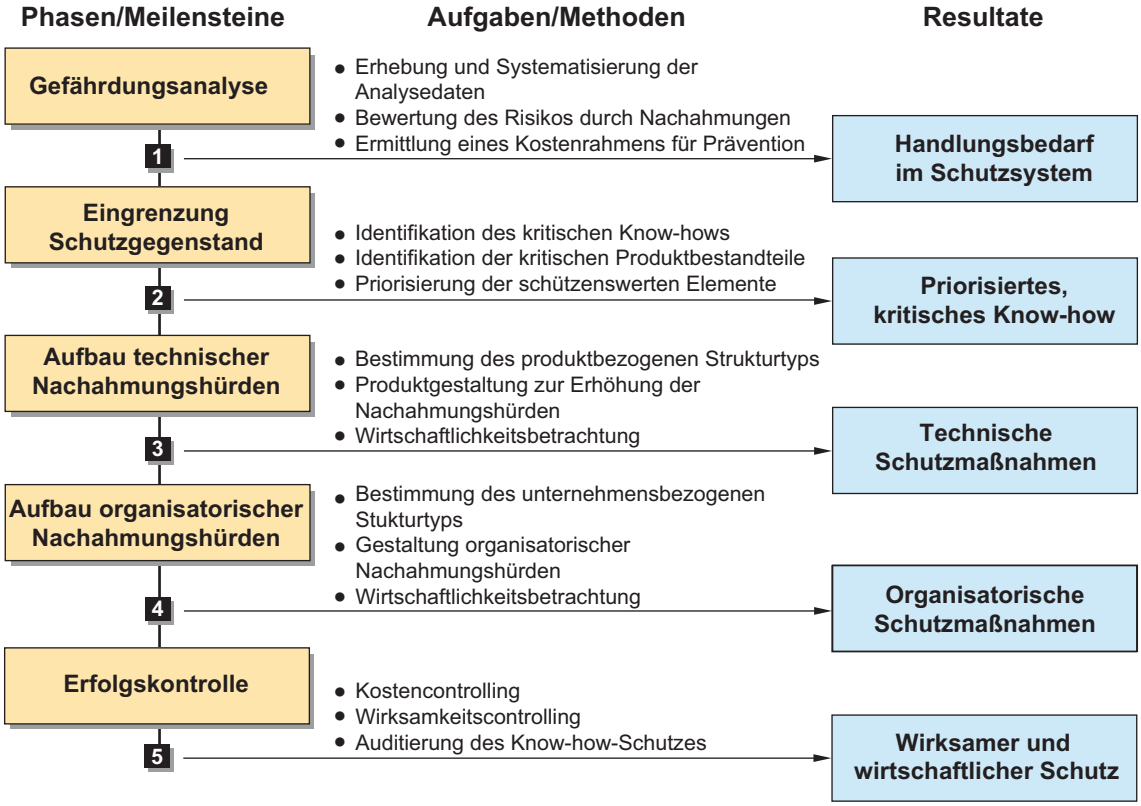


Bild 3-3: Vorgehensmodell für die Gestaltung eines präventiven Schutzes vor Nachahmungen nach SCHNAPAUFF [Sch09, S.205]

Aufbau technischer Nachahmungshürden: In dieser Phase werden technische Produkte so gestaltet, dass ein möglichst hoher Aufwand zur Nachahmung erforderlich wird. Die dafür benötigten Schutzmaßnahmen werden in Abhängigkeit der Einteilung der Produkte in sog. produktbezogene Strukturtypen definiert. Die vier Strukturtypen sind: Einfaches Produkt, mechanisch komplexes Produkt, elektronisch komplexes Produkt und hochkomplexes Produkt [Sch09, S.197ff.]. Sie werden anhand der Komplexität der mechanischen und elektrischen Produktelemente gebildet (vgl. Bild 3-4).

Anhand der Einteilung in die Strukturtypen werden verschiedene Schutzmaßnahmen vorgeschlagen. So kann ein mechanisch einfaches und elektronisch komplexes Produkt durch Produktkennzeichnungen geschützt werden. Bei mechanisch komplexen Produkten eignet sich z. B. die Schutzmaßnahme De-Standardisierung. Hochkomplexe Produkte benötigen individuelle Maßnahmen und sind daher gesondert zu betrachten. Der Abschluss der Phase ist eine Wirtschaftlichkeitsbetrachtung. Hier werden Sach- und Personalkosten sowie indirekte Kosten (Kosten zur Umsetzung der Maßnahmen) betrachtet.

[22] Für weitere Informationen sei auf [Por00, S.67ff.] verwiesen.

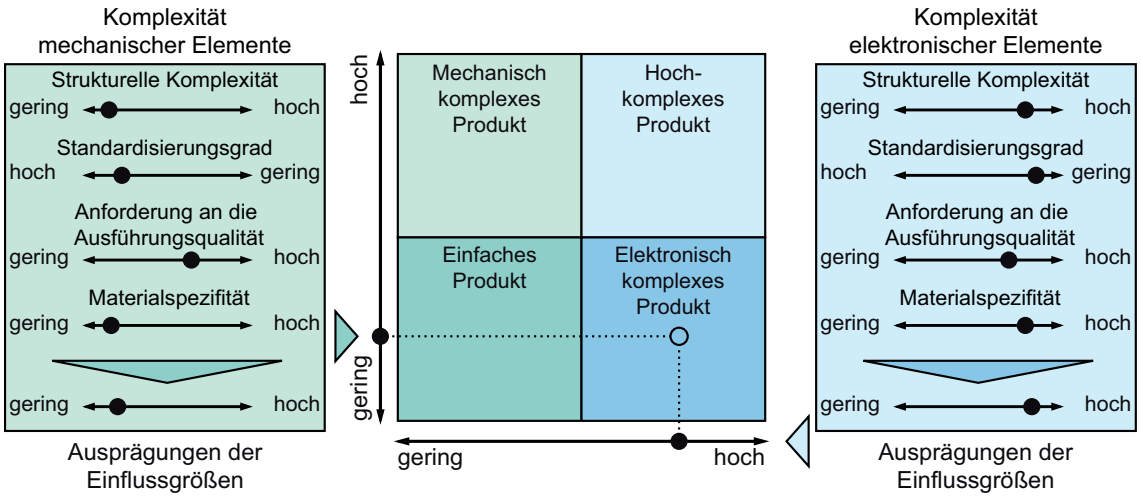


Bild 3-4: Bestimmung des produktbezogenen Strukturtyps [Sch09, S.237]

Aufbau organisatorischer Nachahmungshürden: Hier wird der Schutz des kritischen Know-hows fokussiert. Als Basis für die Auswahl organisatorischer Maßnahmen dienen die unternehmensbezogenen Strukturtypen: Lokaler Outsourcer, Lokaler Wertschöpfer, Globaler Outsourcer und Globaler Wertschöpfer [Sch09, S.199ff.]. Die Strukturtypen werden anhand der Komplexität der Standortstruktur und der Wertschöpfungstiefe ermittelt. Auf Grundlage der Zuordnung der unternehmensbezogenen Strukturtypen zu den jeweils passenden Schutzmaßnahmenbündeln können die relevanten Schutzmaßnahmen individuell für jeden Strukturtypen identifiziert werden. Abschließend erfolgt eine Wirtschaftlichkeitsbetrachtung der organisatorischen Schutzmaßnahmen.

Erfolgskontrolle: In der letzten Phase wird die Wirtschaftlichkeit überwacht. Dies geschieht durch eine Gegenüberstellung der tatsächlich anfallenden Kosten für die Maßnahmen mit den Kennzahlen z. B. der Entwicklung von Umsatz, Preis oder Rendite der geschützten Produkte. Die so ermittelten Ergebnisse werden mit den Werten der Wirtschaftlichkeitsbetrachtung aus den Phasen 3 und 4 verglichen. Die Durchführung von regelmäßigen Audits stellt die andauernde Kontrolle des Know-how-Schutzes sicher.

Bewertung

SCHNAPAUFF entwickelt ein Verfahren zur Gestaltung eines präventiven Nachahmungsschutzes für technische Produkte. Hervorzuheben ist die erarbeitete Identifikation von schützenswertem Know-how. Dieses bezieht sich auf das gesamte Unternehmen und nicht nur auf einzelne Produkte. So wird eine Informationsgrundlage darüber geschaffen, welches Know-how in zukünftigen Entwicklungen besonders schützenswert ist. Zusätzlich werden Strukturtypen unterschieden. Diese kategorisieren die Komplexität der Produktelemente. Die Zuordnung von Schutzmaßnahmen zu den Strukturtypen ist jedoch schwer nachvollziehbar. Eine durchgängige Systematik lässt sich nicht erkennen.

Das Verfahren von SCHNAPAUFF bietet mit der Gefährdungsanalyse die Möglichkeit, Angriffspunkte für Produktpiraterie frühzeitig zu erkennen. Eine interdisziplinäre Be-

trachtungsweise wird jedoch nicht aufgezeigt. Ebenfalls fehlt die Integration in ein vorhandenes Entwicklungsvorgehen. Das entwickelte Vorgehen betrachtet lediglich die Entwicklung von Nachahmungshürden. Der passende Zeitpunkt im Produktentstehungsprozess für das Durchlaufen des Vorgehens wird nicht näher spezifiziert.

3.2.3 Beitrag zum ganzheitlichen Know-how-Schutz von virtuellen Produktmodellen nach MEIMANN

MEIMANN befasst sich mit dem ganzheitlichen Know-how-Schutz von virtuellen Produktmodellen während der Produktentwicklung. Nach MEIMANN besteht für einen Originalhersteller die einzige Strategie gegen Produktpiraten darin, das Kopieren der Produkte zu erschweren und dieses so für Imitatoren unwirtschaftlich zu machen. Er entwickelt ein Konzept zum Know-how-Schutz der Produktmodelle in der virtuellen Produktentwicklung. Das Konzept besteht im Wesentlichen aus zwei Methodiken und einem IT-Konzept für die Implementierung der Know-how-Schutz-Methodik in das firmenspezifische Product Lifecycle Management (PLM)-System. Die beiden Methodiken sind die Methodik zur Integration von Know-how-Schutz-Merkmalen in virtuelle Produktmodelle und die Methodik für kontrollierte Modellverfremdung [Mei10].

Im Fokus der vorliegenden Arbeit steht der *präventive Schutz Intelligenter Technischer Systeme vor Produktpiraterie*. Zur Sicherstellung des Schutzes wird eine *Entwurfssystematik* angestrebt. Daher wird die erstgenannte Methodik im Folgenden detailliert untersucht. Die Verfremdung von Produktmodellen dient dem Schutz des Unternehmenswissens. Dies liegt in der vorliegenden Arbeit außerhalb des Betrachtungsbereichs (vgl. Kap. 2.1). Die Methodik zur Modellverfremdung wird daher nur grob beschrieben.

Die entwickelte **Methodik zur Integration von Know-how-Schutz-Merkmalen in virtuelle Produktmodelle** erweitert die VDI-Richtlinie 2221. Die VDI 2221 beschreibt die Methodik zum Entwickeln und Konstruieren technischer Systeme und Produkte [VDI2221], [Mei10, S.90ff.]. Ein wesentliches Merkmal des Konzeptes zum Know-how-Schutz ist die Berücksichtigung der Know-how-relevanten Aspekte in den frühen Phasen der Produktentwicklung. Als frühe Phasen betrachtet MEIMANN die Produktplanung, Funktionsfindung und Prinziperarbeitung und die damit verbundenen Tätigkeiten der Anforderungsdefinition, Funktionsfindung sowie Wirkstrukturmodellierung (vgl. [VDI2221]). Das generelle Vorgehen beim Entwickeln und Konstruieren startet nach der VDI-Richtlinie 2221 mit der Phase *Klären und Präzisieren der Aufgabenstellung*. Das Ergebnis ist die Anforderungsliste. Diese Phase wird nicht betrachtet. Die Integration der Aspekte des Know-how-Schutzes findet hauptsächlich in den Phasen *Funktionsfindung* und *Prinziperarbeitung* statt. Die Identifikation der zu schützenden Produktfunktionen spielt eine zentrale Rolle beim Know-how-Schutz. Das resultierende Vorgehensmodell ist in Bild 3-5 dargestellt. Im Folgenden werden die Phasen beschrieben, der Fokus liegt auf den Erweiterungen (diese sind grün hinterlegt) [Mei10], [VDI2221].

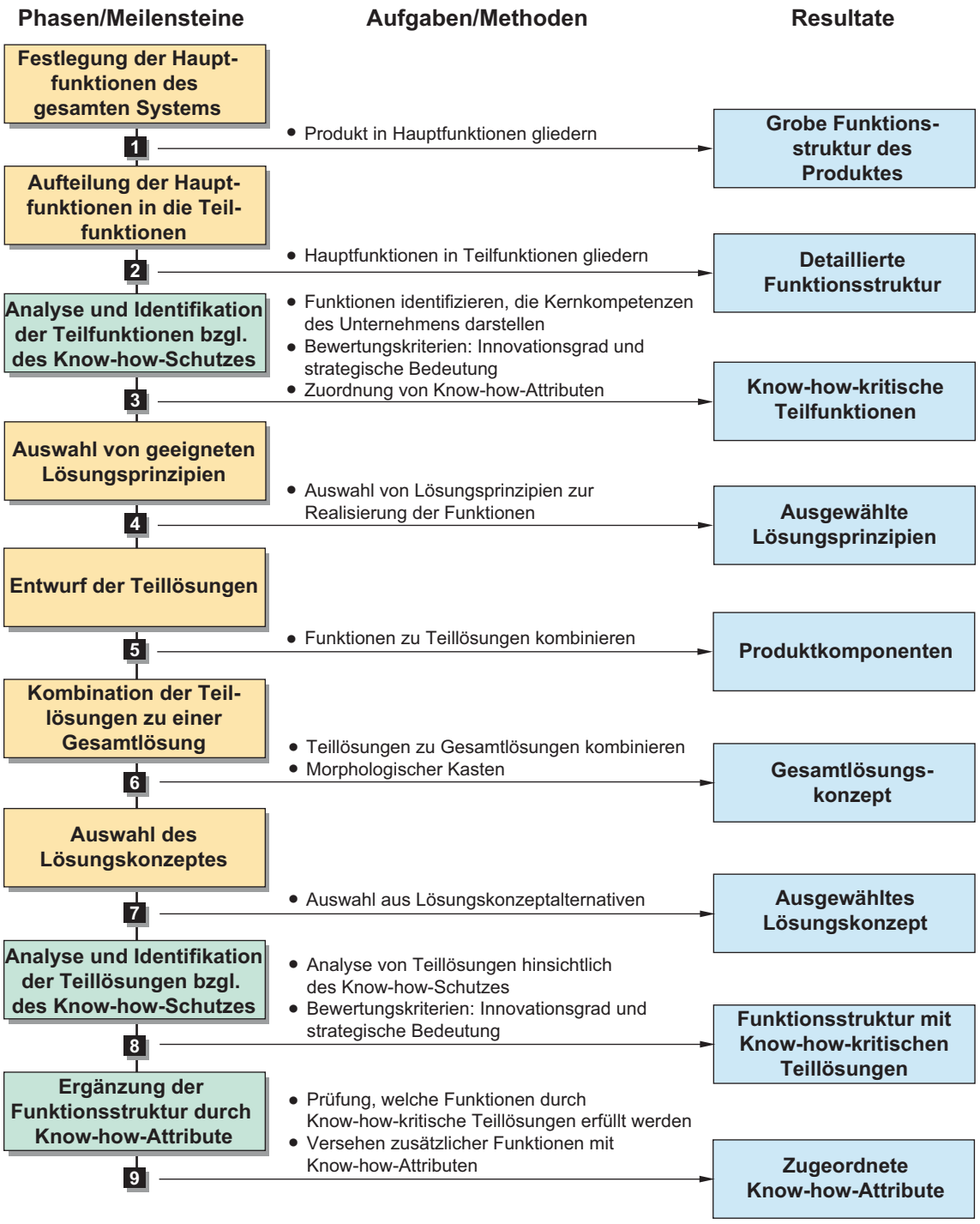


Bild 3-5: Vorgehensmodell zur Identifikation Know-how-kritischer Produktfunktionen in den frühen Entwicklungsphasen nach MEIMANN [Mei10, S.92]

Festlegung der Hauptfunktionen des gesamten Systems: In dieser Phase erfolgt analog zur VDI-Richtlinie 2221 die Festlegung der Hauptfunktionen.

Aufteilung der Hauptfunktionen in die Teilfunktionen: Zur Erstellung der detaillierten Funktionsstruktur werden die Hauptfunktionen in Teilfunktionen gegliedert.

Analyse und Identifikation der Teilfunktionen bzgl. des Know-how-Schutzes: Der Fokus der Methodik liegt auf der Erweiterung der Funktionsstruktur durch sog. Know-how-Attribute. Hierfür müssen diese Attribute zu den schützenswerten Funktionen zugeordnet werden. In dieser Phase werden die schützenswerten, Know-how-kritischen Produktfunktionen analysiert und identifiziert. Die Analyse und Identifikation dieser Funktionen erfolgt in drei Schritten: Zunächst werden die Produktfunktionen identifiziert, die Kernkompetenzen des Unternehmens darstellen. Weiter werden die Produktfunktionen anhand der Bewertungskriterien Innovationsgrad und strategische Bedeutung analysiert. Eine detaillierte Beschreibung dieser Analyse ist in Phase 8 dargestellt. Zum Abschluss werden die Know-how-Attribute den schützenswerten Produktfunktionen in der Funktionsstruktur zugeordnet.

Auswahl von geeigneten Lösungsprinzipien: Hier werden nun nach der VDI 2221 die geeigneten Lösungsprinzipien zur Realisierung der ermittelten Funktionen ausgewählt.

Entwurf der Teillösungen: In dieser Phase werden durch die Kombination der einzelnen Funktionen und deren Lösungsprinzipien Produktkomponenten spezifiziert.

Kombination der Teillösungen zu einer Gesamtlösung: Hier werden nun die Teillösungen zu einer Gesamtlösung kombiniert. Mithilfe des morphologischen Kastens werden die einzelnen Funktionen der Teillösungen zu Gesamtlösungskonzepten vereint.

Auswahl des Lösungskonzeptes: Aus den ermittelten Alternativen wird in dieser Phase ein Lösungskonzept zur weiteren Konkretisierung ausgewählt.

Analyse und Identifikation der Teillösungen bzgl. des Know-how-Schutzes: In dieser Phase werden die verwendeten Teillösungen in zwei Schritten hinsichtlich des Know-how-Schutzes untersucht. Die Teillösungen werden im ersten Schritt angelehnt an EHRENSPIEL[23] anhand ihres Innovationsgrades bewertet. Hierbei haben neue Lösungsprinzipien tendenziell eine höhere Bedeutung für Unternehmen. Da diese These für Unternehmen individuell zu überprüfen ist, wird im zweiten Schritt die strategische Bedeutung der Lösungsprinzipien überprüft. Die Aspekte des möglichen Wettbewerbsvorteils, der Eignung zur Patentanmeldung sowie Möglichkeiten zur Übertragung von Innovationen in andere Bereiche werden berücksichtigt. Ergebnis der Phase ist eine Funktionsstruktur mit Know-how-kritischen Teillösungen.

Ergänzung der Funktionsstruktur durch Know-how-Attribute: In der abschließenden Phase wird geprüft, welche Funktionen durch die in der vorherigen Phase identifizierten Know-how-kritischen Teillösungen erfüllt werden. Diese Funktionen werden zusätzlich als Know-how-kritische Funktionen identifiziert. Analog zur Phase 3 werden auch diese Funktionen mit Know-how-Attributen gekennzeichnet. So ergibt sich als Ergebnis des Vorgehensmodells eine Funktionsstruktur, bei der die identifizierten Know-how-kritischen Teillösungen passenden Know-how-Attributen zugeordnet sind.

[23] Für weitere Informationen sei auf [Ehr07] verwiesen.

Die **Methodik für kontrollierte Modellverfremdung** konzentriert sich auf die Anpassung der virtuellen Produktmodelle. Aufgrund des zunehmenden Informationsgehalts in den Produktmodellen sowie des elektronischen Datenaustauschs über Computernetze wird es Angreifern ermöglicht, leicht an fremdes Know-how zu gelangen. Daher ist die entsprechende Anpassung der virtuellen Modelle nötig. Mit der Verfremdung werden Informationen entfernt. Hierbei werden die Anforderungen interner und externer Stakeholder berücksichtigt. Die Modellverfremdung wird z. B. durch das Entfernen von Informationen aus den CAD-Modellen erreicht [Mei10, S.104ff.].

Bewertung

Die Arbeit von MEIMANN gliedert sich in zwei Kernbestandteile. Diese sind Integration des Know-how-Schutzes in virtuelle Produktmodelle und die kontrollierte Modellverfremdung. Hervorzuheben ist die Integration in die frühen Phasen der Produktentwicklung. Hierfür bildet die VDI-Richtlinie 2221 die Grundlage. MEIMANN erweitert diese mit Prozessbausteinen der Know-how-Schutz-Methodik. Durch die Erweiterung wird die Identifikation von schützenswerten Produktfunktionen ermöglicht. Da die VDI-Richtlinie 2221 nur auf einzelne Fachdisziplinen ausgerichtet ist, fehlt die interdisziplinäre Betrachtung über sämtliche Fachdisziplinen hinweg.

Bei der kontrollierten Modellverfremdung wird auf Grundlage des Weglassens von Informationen der Know-how-Abfluss verhindert. Der Einsatz von Schutzmaßnahmen beschränkt sich jedoch auf die Verfremdung von virtuellen Produktmodellen z. B. CAD-Zeichnungen. Eine Verbindung zwischen den schützenswerten Funktionen und den Schutzmaßnahmen durch Modellverfremdung wird nicht aufgezeigt.

3.2.4 Ganzheitliches, präventives Schutzkonzept für Investitionsgüter (PROTACTIVE)

Im BMBF-Projekt „Präventives Schutzkonzept für Investitionsgüter durch einen ganzheitlichen Ansatz aus Organisation, Technologie und Wissensmanagement“ (PROTACTIVE) wurde ein Lösungsansatz bestehend aus drei voneinander unabhängigen Lösungskonzepten entwickelt. Die Lösungskonzepte beziehen sich auf die Aufbau- und Ablauforganisation, den Technologieschutz und auf das Wissensflussmanagement. Jedoch wird der bestmöglichste Schutz nur über eine Verzahnung der drei Lösungskonzepte erreicht [SN10, S.23f.].

Das Ziel der vorliegenden Arbeit ist, Produkte technisch vor Produktpiraterie und Nachahmung zu schützen. Dies deckt sich mit dem Ziel des Lösungskonzeptes **Technologieschutz** (vgl. [SSM10, S.31f.]). Aus diesem Grund wird ausschließlich das Lösungskonzept Technologieschutz detailliert untersucht.

Technologieschutz: Der Technologieschutz besteht aus zwei aufeinander aufbauenden Phasen, der Diagnose-Phase (Ganzheitliche-Piraterie-Diagnose) und der Synthese Phase (Design-for-Anti-Piracy) [SSM10, S.33ff.].

In der **Diagnose-Phase** wird eine ganzheitliche Untersuchung zum Piraterierisiko durchgeführt. Sie wird als Ganzheitliche-Piraterie-Diagnose (GPD) bezeichnet und besteht aus fünf Phasen. Die GPD basiert auf einer modifizierten FMEA (Fehler-Möglichkeits-und-Einfluss-Analyse) und der Differentialdiagnose. In dieser werden die Ursache-Wirkungs-Beziehungen untersucht[24]. Die vorliegende Arbeit fokussiert den präventiven Schutz für ITS. Die Analyse der Gefahrenlage spielt eine untergeordnete Rolle. Aus diesem Grund ist sowohl das Vorgehensmodell der GPD als auch die Beschreibung der einzelnen Phasen lediglich im Anhang A2 dargestellt. Die Ergebnisse der GPD sind ein qualitatives Piraterie-Bedrohungsprofil sowie die Piraterie-Risiko-Zahl. Mit diesen lässt sich das Risiko vor Produktpiraterie bestimmen.

In der darauf folgenden **Synthese-Phase** wird der technisch-konstruktive Schutz vor Produktpiraterie als zusätzliches Ziel in der Produktentwicklung definiert. Die Design-for-Anti-Piracy-Methodik (DfAP) basiert auf den Grundlagen, dass sowohl das Ziel (Konstruktionsaufgabe) als auch der Weg (Konstruktionsschritte) beim Systemschutz zu berücksichtigen sind. Die Produktintegrität (Sicherheit, Schutz, Berechtigung) ist das oberste Ziel. Als Konstruktionsweg wird der Prozess nach PAHL/BEITZ (vgl. [PBF+07]) zugrunde gelegt [SSM10]. Die DfAP besteht ebenfalls aus fünf Schritten. Diese sind in Bild 3-6 dargestellt und werden im Folgenden beschrieben [SSM10, S.38ff.].

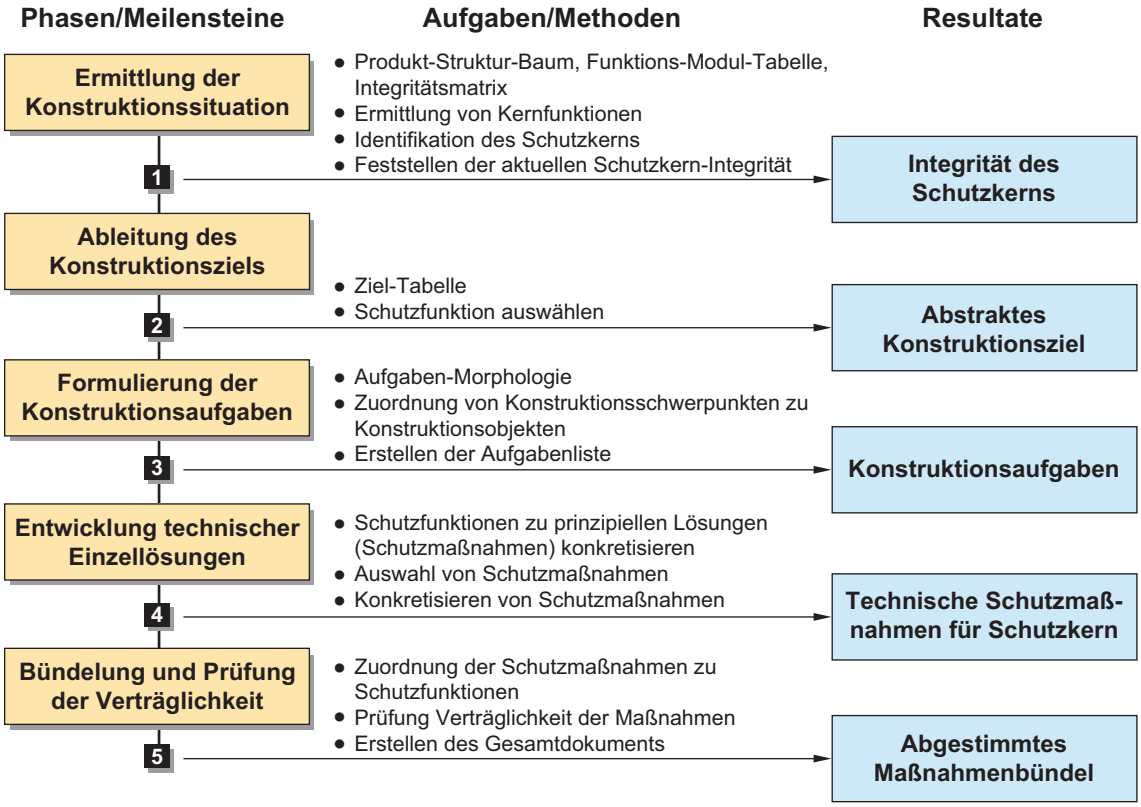


Bild 3-6: Vorgehensmodell für die DfAP nach SCHALLNUS ET AL. [SSM10, S.38]

[24] Für weitere Informationen sei auf [SSM10, S.34ff.] verwiesen.

Ermittlung der Konstruktionssituation: Hier wird festgestellt, wie hoch die aktuelle Integrität des zu schützenden Produktes ist. Dazu wird das Produkt in seine Module und Bestandteile zerlegt. Dies erfolgt mittels eines Produkt-Struktur-Baums. Die Identifikation von Kernfunktionen erfolgt durch das Aufstellen einer Funktions-Modul-Tabelle. Weiterhin wird überprüft, welche Module diese Kernfunktionen sicherstellen. Anhand der identifizierten Module wird der sog. Schutzkern beschrieben. Dieser wird abschließend bezüglich seiner Zerlegbarkeit und Verständlichkeit untersucht.

Ableitung des Konstruktionsziels: In dieser Phase wird für die Module des Schutzkerns festgelegt, ob ihre Integrität erhöht werden soll. Dies kann durch die beiden Schutzfunktionen Verstecken und/oder Verfremden realisiert werden.

Formulierung der Konstruktionsaufgaben: Hier wird das Konstruktionsziel präzisiert. Dies erfolgt anhand der Zuordnung eines Konstruktionsschwerpunktes zu einem Konstruktionsobjekt. Für die Zuordnung wird ein morphologischer Kasten verwendet.

Entwicklung technischer Einzellösungen: Diese Phase hat das Ziel, die Integrität des Schutzkerns zu erhöhen. Dazu werden technische Lösungen entwickelt. Zu unterscheiden sind die Teilschritte Konzipieren und Entwerfen. Beim Konzipieren findet die Konkretisierung der Schutzfunktionen verstecken und verfremden zu prinzipiellen Lösungen statt. So werden geeignete Schutzmaßnahmen identifiziert. Im Teilschritt Entwerfen findet eine Konkretisierung und Bewertung der ausgewählten Schutzmaßnahmen statt.

Bündelung und Prüfung der Verträglichkeit: Abschließend werden die entwickelten Einzellösungen den jeweiligen Schutzfunktionen zugeordnet. Weiterhin wird die Verträglichkeit der Lösungen überprüft [SSM10, S.44].

Bewertung

In dem Projekt PROTACTIVE wird ein Vorgehen entwickelt, das aufbauend auf der Diagnose des Risikos von Produktpiraterie eine Methodik zum Systemschutz beschreibt. Mit Hilfe der Diagnose können ansatzweise auch neue Angriffe berücksichtigt werden. Hervorzuheben ist insbesondere, dass bei der DfAP-Methodik die Aspekte des Systemschutzes in die Konstruktionsschritte nach PAHL/BEITZ (vgl. [PBF+07]) integriert werden. Beim Konzipieren des Produktes werden schützenswerte Module identifiziert. Für diese werden jeweils die beiden Schutzfunktionen Verstecken und Verfremden auf deren Eignung untersucht. Ziel der Schutzfunktionen ist es, die Module vor unerlaubtem Nachbau zu schützen und den Know-how-Abfluss zu verhindern.

Die Integration der Aspekte des Produktschutzes in die Konstruktion kann als beispielhaftes Vorgehen für die vorliegende Arbeit betrachtet werden. Der Prozess nach PAHL/BEITZ ist jedoch nicht weitreichend genug, da dieser sich zu sehr auf die einzelnen Fachdisziplinen fokussiert ist (vgl. [PBF+07]). Für die moderne Systementwicklung wird ein disziplinübergreifendes Systemmodell benötigt. Die Arbeiten der einzelnen Disziplinen müssen in diesem Modell zusammenfließen (vgl. Kap. 2.4).

3.2.5 Verfahren zur Konzipierung imitationsgeschützter Produkte und Produktionssysteme nach KOKOSCHKA

KOKOSCHKA entwickelt ein Vorgehen zum Schutz von Produkten und Produktionssystemen. Dieses ist in Bild 3-7 gezeigt. Die Phasen sind im Folgenden erläutert [Kok13].

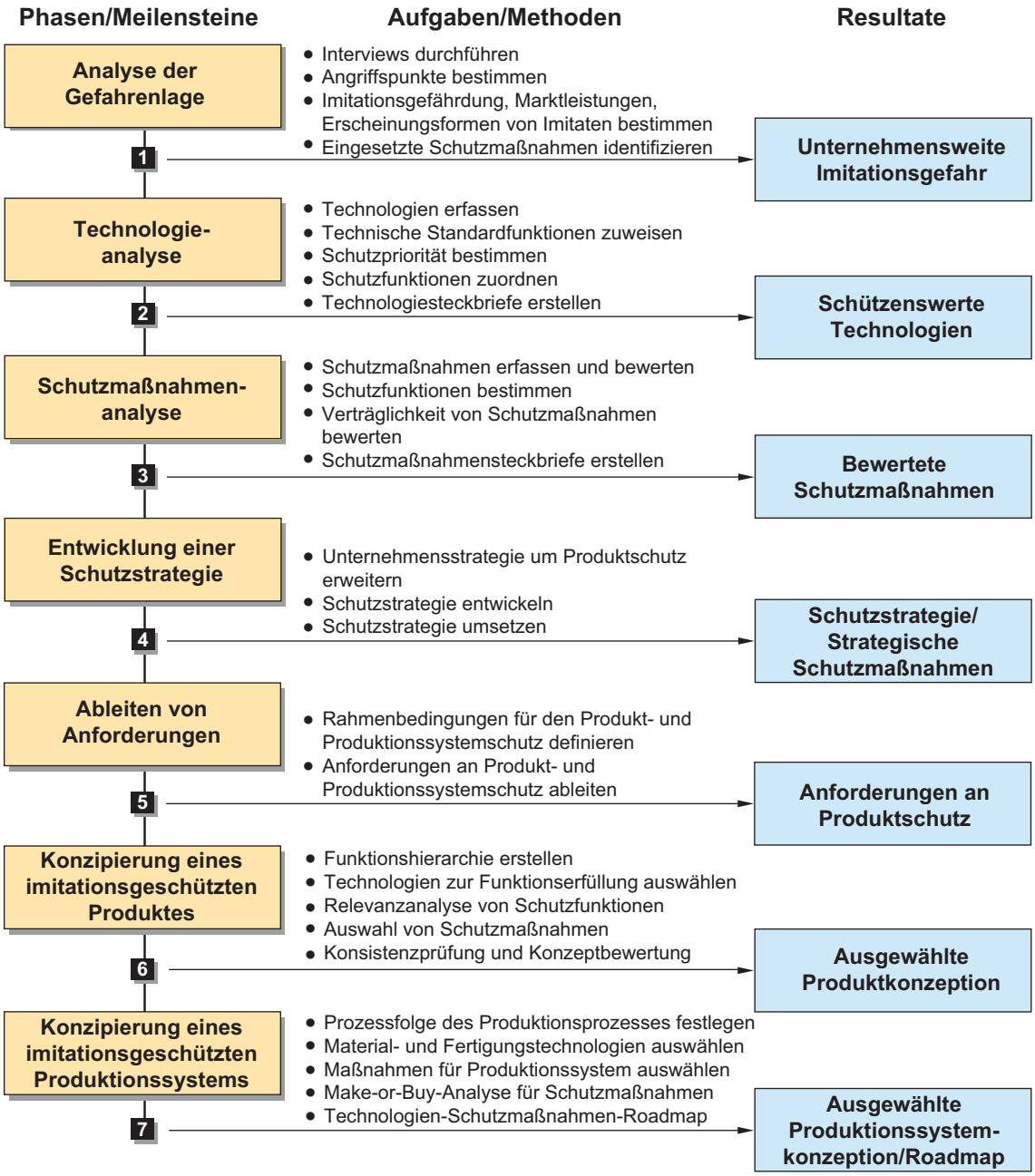


Bild 3-7: Vorgehensmodell zur Konzipierung imitationsgeschützter Produkte und Produktionssysteme nach KOKOSCHKA [Kok13, S.88]

Das entwickelte Vorgehensmodell beschreibt ein sieben-stufiges Verfahren um imitationsgeschützte Produkte und Produktionssysteme zu konzipieren. Bei diesem steht die Phase der Produktkonzipierung im Fokus (vgl. Kap. 2.4.1, Bild 2-10). Die ersten vier

Phasen sind unabhängig von einem bestimmten Produkt oder Produktionssystem. In diesen Phasen wird die unternehmensweite Gefahr vor Imitationen initial bestimmt.

Analyse der Gefahrenlage: In der ersten Phase wird die Imitationsgefahr ermittelt. Dies geschieht in Anlehnung an die im Rahmen der Forschungsoffensive „Innovationen gegen Produktpiraterie“ entwickelte Bedarfsanalyse Produktschutz[25]. Es werden Interviews durchgeführt, um Angriffspunkte zu ermitteln. Zusätzlich werden imitationsgefährdete Marktleistungen und -regionen identifiziert. So wird ein Überblick erstellt, welche Marktleistungen des Unternehmens am häufigsten imitiert werden und in welchen Marktregionen dies geschieht. Zum Abschluss werden darüber hinaus die im Unternehmen bereits eingesetzten Schutzmaßnahmen untersucht.

Technologieanalyse: Hier steht die Identifikation schützenswerter Technologien im Fokus. Es werden zunächst die Produkt-, Fertigungs-, Material- und Informationstechnologien des betrachteten Unternehmens erfasst. Diesen Technologien werden unternehmensspezifische, technische Standardfunktionen zugeordnet. Diese sind in der Sprache des Entwicklers mit einer Nomen-Verb-Kombination beschrieben. Beispiele für unternehmensspezifische Standardfunktionen sind in Tabelle 3-1 dargestellt.

Tabelle 3-1: Beispiele für unternehmensspezifische Standardfunktionen [Kok13, S.99]

Nr.	Technologie	Unternehmensspezifische Standardfunktionen			
		Nomen 1	Verb 1	Nomen 2	Verb 2
1	3-Wege-Ventil	Durchfluss	kontrollieren		
2	Mechanische Waage	Material	wiegen		
3	Programmierbare Wägeelektronik	Material	wiegen	Information	verarbeiten
4	Steuerungssoftware	Information	speichern	Information	verarbeiten
5	Clinchen	Material	fügen		
6	Fräsen	Material	abtragen		
7	Lasersintern	Material	auftragen		

Die identifizierten Technologien werden anschließend hinsichtlich ihrer Schutzpriorität (Relevanz für das Unternehmen und Imitationsgefährdung) bewertet. Für die schützenswerten Technologien werden Funktionen zu ihrem Schutz, sog. Schutzfunktionen, definiert. Sie ermöglichen eine Verknüpfung von Schutzmaßnahmen mit Technologien. Beispiele für Schutzfunktionen sind Informationsfluss steuern, Funktionalität verschleiern, Kompatibilität beschränken und Manipulation verhindern [Kok13, S.105f.].

[25] Für eine detaillierte Beschreibung der Bedarfsanalyse Produktschutz sei auf LINDEMANN ET AL. [LMP+12b, S.105ff.] und MEIWALD [Mei11, S.98ff.] verwiesen.

Abschließend werden strukturierte Technologiesteckbriefe erstellt und in einer Innovations-Datenbank abgelegt. Diese enthalten produktschutzrelevante Informationen wie Schutzpriorität und Schutzfunktion.

Schutzmaßnahmenanalyse: In dieser Phase werden alle verfügbaren Schutzmaßnahmen erfasst und bewertet. Es werden die gesammelten Schutzmaßnahmen von MEIWALD [Mei11], LINDEMANN ET AL. [LMP+12a] und GAUSEMEIER ET AL. [GGL12] berücksichtigt. Die unternehmensspezifische Bewertung einer Schutzmaßnahme basiert auf den Aspekten: Implementierungsaufwand, Einsatzpotential sowie Schutzwirkung. Im Fokus dieser Phase steht die anschließende Bestimmung der Schutzfunktionen. Jede Schutzmaßnahme erfüllt bestimmte Schutzfunktionen. Durch diese Verbindung wird eine systematische Kombination von Technologien und Schutzmaßnahmen ermöglicht.

Damit ein wirksamer Schutz erzielt wird, müssen sich die eingesetzten Schutzmaßnahmen in ihrer Wirkung unterstützten. Aus diesem Grund wird eine Verträglichkeitsanalyse der Schutzmaßnahmen erarbeitet. Alle Schutzmaßnahmeninformationen werden analog zu den Technologien als Steckbriefe abgelegt.

Entwicklung einer Schutzstrategie: In der vierten Phase wird die Schutzstrategie entwickelt. Diese wird in der Strategie des Unternehmens verankert. Dazu muss die Unternehmensstrategie um Aspekte des Produktschutzes sowie die Definition einer Schutzstrategie für das Gesamtunternehmen erweitert werden. Die Schutzstrategie schafft die Basis zur Beachtung des Produktschutzes im Unternehmen.

Ableiten von Anforderungen: In dieser Phase findet der Übergang vom produktunabhängigen (Phasen 1-4) zum produktspezifischen Teil (Phasen 4-7) des Verfahrens statt. Hierbei schaffen die abzuleitenden Anforderungen die Grundlage für die Produkt- und Produktionssystemkonzipierung unter Berücksichtigung des Produktschutzes. Im ersten Schritt sind Rahmenbedingungen für den Produkt- und Produktionssystemschutz zu definieren. Anschließend werden die Produkt- und Produktionssystemschutzanforderungen abgeleitet und in einer Anforderungsliste gesammelt. Dem Grundgedanken des 3-Zyklen-Modells der Produktentstehung (vgl. Kap. 2.4.1) folgend werden Produkt und Produktionssystem parallel konzipiert. Zugunsten der Übersichtlichkeit werden diese Tätigkeiten im Vorgehensmodell als zwei aufeinander folgende Phasen dargestellt.

Konzipierung eines imitationsgeschützten Produktes: Die sechste Phase basiert auf der Konstruktionssystematik nach PAHL/BEITZ (vgl. [PBF+07]). Zunächst wird eine Funktionshierarchie erstellt. Die Gesamtfunktion bildet die erste Ebene der Struktur. Sie wird zergliedert in Haupt- und Teilfunktionen. Die Beschreibung der Funktionen erfolgt in der eigenen Beschreibungsweise des Entwicklers. Für die Auswahl von Technologien wird die Funktionshierarchie in definierte, unternehmensspezifische Standardfunktionen übersetzt. Mit Hilfe eines morphologischen Kastens werden anschließend Technologien zur Erfüllung der Funktionen ausgewählt. Den schützenswerten Technologien werden anhand der Schutzfunktionen relevante Schutzmaßnahmen zugeordnet.

Zur Identifikation von Schutzfunktionen mit höchster Priorität wird eine Relevanzanalyse durchgeführt. Anschließend werden Schutzmaßnahmen ausgewählt, die möglichst viele dieser Schutzfunktionen erfüllen. Die ausgewählten Kombinationen der Technologien und Schutzmaßnahmen werden auf ihre Verträglichkeit untereinander untersucht.

An dieser Stelle liegen nun mehrere prinzipielle Lösungen für das Produkt vor. Diese bestehen aus Technologien zur Erfüllung der Funktion sowie aus einer konsistenten Kombination von Schutzmaßnahmen. Abschließend werden die erstellten imitationsgeschützten Produktkonzeptionen hinsichtlich ihrer Schutzwirkung und des Implementierungsaufwandes analysiert, bewertet und in einem Portfolio dargestellt.

In die Bestimmung der Schutzwirkung fließen Kriterien wie Durchschnittsbeitrag zur Erfüllung von Schutzfunktionen, Nachahmungs-/Manipulationsrobustheit, Zugangsbeschränkungen etc. ein. Der Implementierungsaufwand wird anhand der Investitionsrisiken und der Verfügbarkeit im Unternehmen bzw. bei Anbietern bewertet. Im weiteren Verlauf der Konzipierung ist die festgelegte Lösungsvariante zu konkretisieren. Dazu verweist KOKOSCHKA auf die Partialmodelle Wirkstruktur, Verhalten und Gestalt der Spezifikationstechnik CONSENS (vgl. Kap. 3.3.1).

Konzipierung eines imitationsgeschützten Produktionssystems: Die abschließende Phase umfasst das Festlegen einer Prozessfolge. Zur Bestimmung der Prozessfolge wird die Prinziplösung des Gesamtproduktes in einzelne Baugruppen unterteilt und die Baustruktur des Produktes ermittelt. Anschließend wird untersucht, welche Systemelemente vom Unternehmen selbst gefertigt werden müssen. Für diese Entscheidung wird auf die Schutzpriorität der in den Systemelementen eingesetzten Technologien zurückgegriffen. Darauf aufbauend erfolgen die Planung der Material- und Fertigungstechnologien sowie die Auswahl relevanter Schutzmaßnahmen für das Produktionssystem. Diese erfolgt analog zur Maßnahmenauswahl für das Produkt (siehe Phase 6).

Darauf folgend wird eine Make-or-Buy-Analyse durchgeführt. Bei dieser wird entschieden, welche Schutzmaßnahmen selbst entwickelt und welche zugekauft werden sollen. Als nächstes ist die Integration ausgewählter Schutzmaßnahmen in den Produktionsprozess durchzuführen. Dafür sind Prozessschritte zum Einbringen von Schutzmaßnahmen in die Prozessfolge zu integrieren.

Abschließend wird eine Technologien-Schutzmaßnahmen-Roadmap erstellt. Aus dieser geht hervor, welche Technologien und Schutzmaßnahmen für eine imitationsgeschützte Produkt- und Produktionssystemkonzeption eingesetzt werden müssen.

Bewertung

Hervorzuheben ist die von KOKOSCHKA vorgenommene Kategorisierung der Schutzmaßnahmen in sieben Kategorien (vgl. Kap. 2.3.2 und Bild 2-8). Diese ermöglicht eine Charakterisierung der Maßnahmen und verbessert die Übersichtlichkeit. Hierdurch wird auch die Suche nach relevanten Schutzmaßnahmen unterstützt. Weiterhin wird ein Vorgehensmodell zur imitationsgeschützten Konzipierung von Produkten und zugehörigem

Produktionssystem erarbeitet. Hier wird zunächst die Imitationsgefahr analysiert. Anschließend wird die Konzipierung unter Berücksichtigung der Aspekte des Produktschutzes durchgeführt. Die Berücksichtigung von Schutzmaßnahmen bereits im Entwurf von Produkten wird angesprochen. Zudem wird der Produktschutz in die Produktkonzipierung integriert. KOKOSCHKA nutzt die Konzipierung nach PAHL/BEITZ und ergänzt diese um Aspekte des Imitationsschutzes. Der Prozess nach PAHL/BEITZ ist jedoch nicht weitreichend genug, da dieser zu sehr auf die einzelnen Fachdisziplinen fokussiert ist (vgl. [PBF+07]). Auf die weiteren, interdisziplinären Schritte der Konzipierung, welche mit der Spezifikationstechnik CONSENS durchgeführt werden sollen, wird lediglich verwiesen. Somit kann den Herausforderungen der interdisziplinären Entwicklung nicht begegnet werden.

Darüber hinaus werden schützenswerte Technologien identifiziert. Diese werden über Schutzfunktionen zu passenden Schutzmaßnahmen zugeordnet. Damit wird eine Verbindung von Technologien und Schutzmaßnahmen hergestellt. Die Ausnutzung neuer Technologien zur Verbesserung des Schutzes wird nicht angesprochen.

3.3 Modellierungstechniken

Die in Kapitel 3.1 untersuchten Schutzmaßnahmen haben gemein, dass sie textbasiert beschrieben sind. Zukünftige Schutzmaßnahmen müssen jedoch so dargestellt werden, dass sie von allen Disziplinen gleichermaßen verstanden werden. Zusätzlich ist zu berücksichtigen, dass die Schutzmaßnahmen für den Einsatz im modernen Systementwurf ausgelegt sein müssen. Zentraler Aspekt des Entwurfs ist das Systemmodell, welches eine abstrakte und ganzheitliche Systembetrachtung ermöglicht (vgl. Kap. 2.4.4). Zur interdisziplinären Beschreibung des Systemmodells sind eine Modellierungssprache, eine -methode und ein -werkzeug nötig [Alt12], [Ana15], [Kai13].

Im Folgenden wird auf Modellierungstechniken eingegangen, die eine **Sprache** sowie eine **Methode** erhalten. Zunächst wird CONSENS vorgestellt. Anschließend ist die SysML und SYSMOD dargestellt. Zusätzlich wird die Modellierungstechnik METUS beschrieben. Auf die detaillierte Beschreibung von Werkzeugen wird verzichtet, da sich die vorliegende Arbeit auf die Spezifikation des Systems fokussiert[26]. Die virtuelle Darstellung sowie Pflege der Artefakte des Systemmodells wird nicht explizit betrachtet.

3.3.1 CONSENS

Die Spezifikationstechnik CONSENS (CONceptual design Specification technique for the Engineering of complex Systems) wurde im Zuge des Sonderforschungsbereichs 614 am Heinz Nixdorf Institut entwickelt [ADG+09]. CONSENS basiert auf den Arbei-

[26] Für einen Überblick über bestehende Software-Tools zur Modellierung des Systemmodells sei auf KAISER verwiesen [Kai13, S.59ff.].

ten von KALLMEYER, FRANK und GAUSEMEIER ET AL. [Kal98], [Fra06], [GEK01]. Sie enthält eine **Modellierungssprache** sowie eine **Vorgehensweise zur Systemmodellerstellung**. Zusätzlich werden unterschiedliche Sichten auf das Systemmodell ermöglicht. Das Ziel von CONSENS ist die ganzheitliche und fachdisziplinübergreifende Beschreibung des Systems im Rahmen der Konzipierung.

Sprache: Die Darstellung des Systems wird durch Elemente und Beziehungen zwischen den Elementen ermöglicht. Bei den Elementen wird zwischen System- und Umfeldelementen differenziert. Systemelemente befinden sich innerhalb der Systemgrenze, während Umfeldelemente außerhalb des Systems liegen. Die Beziehungen bzw. Wechselwirkungen zwischen den Systemelementen sind durch Flussbeziehungen dargestellt. Einen Überblick über die Modellkonstrukte und deren graphische Notation gibt die Tabelle 3-2 [PBF+07], [GLL12], [Kai13].

Tabelle 3-2: Notation der Beziehungen und Elemente in CONSENS [Kai13, S.76]

Modellkonstrukte	Graphische Notation	Beschreibung
Umfeldelement		Elemente außerhalb der Systemgrenze
System/ Systemelement		Das System entspricht dem zu entwickelnden Produkt und besteht aus Systemelementen
Energiefluss		Mechanische, thermische und elektrische Energien sowie Kenngrößen werden festgelegt [PBF+07, S.43]
Stofffluss		Beschreiben den Transport und den Austausch von Gasen, Flüssigkeiten oder festen Körpern [PBF+07, S.43]
Informationsfluss		z. B. Austausch von Messgrößen, Daten oder Informationen zwischen elektronischen Einheiten [PBF+07, S.43]
Logische Beziehung		Semantik ergibt sich durch die Bezeichnung der Beziehung
Störfluss		Störende Beziehung zwischen zwei Elementen

Methode: CONSENS ist in Aspekte, sog. Partialmodelle, unterteilt. Die sieben Partialmodelle ermöglichen eine interdisziplinäre Beschreibung des Systems. Diese werden im Folgenden näher beschrieben und sind in Bild 3-8 dargestellt [DGO+14].

Umfeld: In diesem Partialmodell werden das Umfeld sowie dessen Interaktion mit dem zu entwickelnden System beschrieben. So wird die Systemgrenze festgelegt. Auf das System haben unterschiedliche Bereiche Einfluss wie übergeordnete Systeme, der Benutzer oder die Umwelt des Systems. Darüber hinaus werden Wechselwirkungen einzelner Einflüsse untersucht [Kai13], [Ana15].

Anwendungsszenarien: Anwendungsszenarien beschreiben, in welcher Art und Weise sich das System in einem Zustand oder in einer bestimmten Situation verhalten soll. Sie

enthalten also für ein bestimmtes Problem eine mögliche Lösung. Ein Anwendungsszenario besteht aus der Charakterisierung einer möglichen Betriebssituation des Systems und dem in dieser Situation erforderlichen Verhalten [GLL12], [Ana15].

Anforderungen: Aus den Partialmodellen Umfeld und Anwendungsszenarien sowie aus der Aufgabenstellung ergeben sich Anforderungen an das System. In einer Anforderungsliste werden diese gesammelt. Sie werden verbal beschrieben und mit Attributen und Ausprägungen konkretisiert [PBF+07].

Funktionen: Aus den Anforderungen werden Funktionen abgeleitet. Das Ziel der Funktion ist, eine spezifische Aufgabe zu erfüllen. Die Darstellung der Funktionen erfolgt hierarchisch [PBF+07].

Wirkstruktur: Das zentrale Partialmodell in CONSENS ist die Wirkstruktur. Hier wird das Zusammenwirken der Elemente des Systems gezeigt. Zur Erfüllung der beschriebenen Teilfunktionen werden Lösungen gesucht. Diese werden dann in der Wirkstruktur zueinander in Beziehung gesetzt. Ziel ist die Abbildung der grundsätzlichen Struktur und der prinzipiellen Wirkungsweise des Systems. Mit Hilfe von Systemelementen kann die Modellierung erfolgen [GLL12].

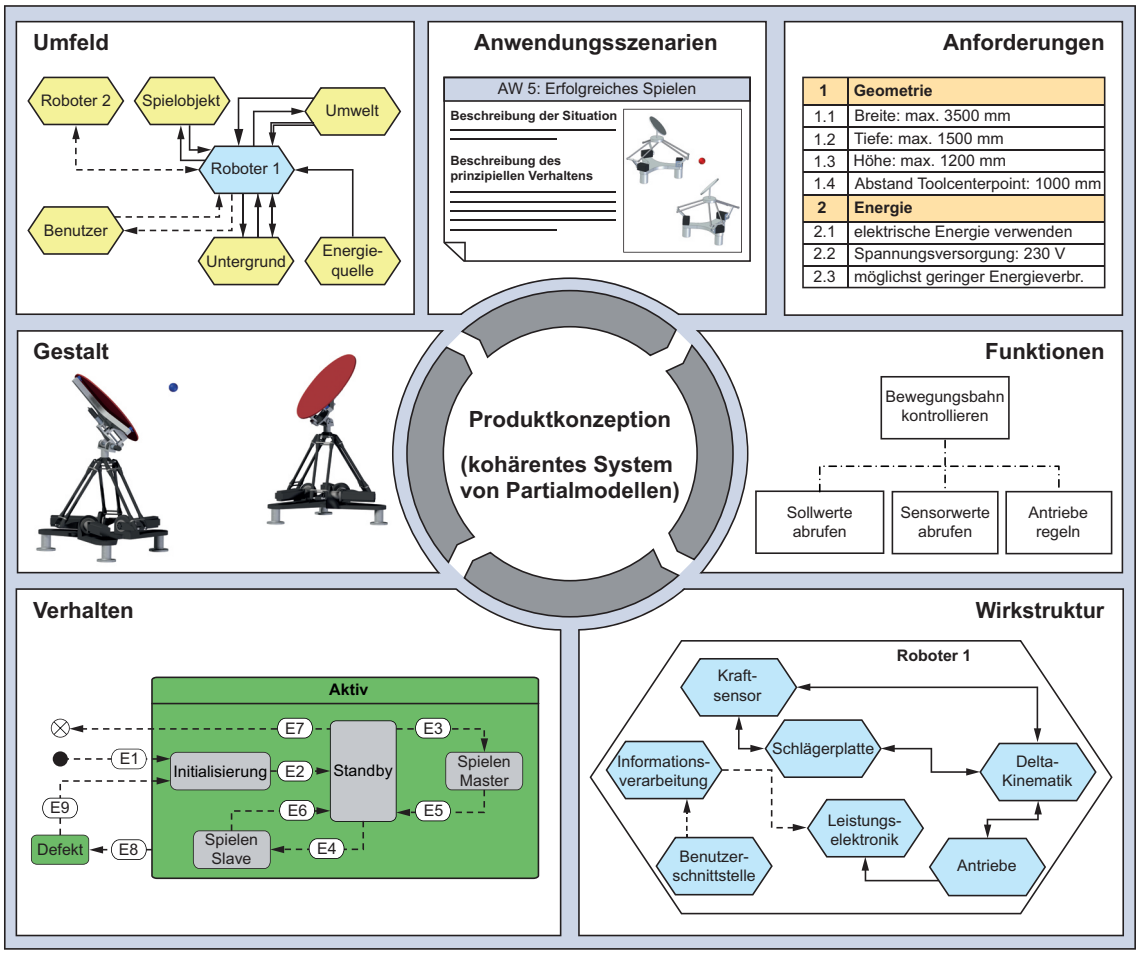


Bild 3-8: Partialmodelle zur Beschreibung des Systemmodells [DGO+14, S.38]

Verhalten: Das Partialmodell Verhalten wird in drei Arten gegliedert: Zustände, Aktivitäten und Sequenz [Kai13], [Ana15].

- Systemzustände und Zustandsübergänge werden durch das Modell Verhalten – Zustände abgebildet.
- Mit dem Aspekt Verhalten – Aktivitäten werden Ablaufdiagramme erstellt. Diese spezifizieren die Reihenfolge der Funktionsausführung eines Systemelements.
- Die Wechselwirkungen zwischen den Systemelementen werden im Modell Verhalten – Sequenzen beschrieben.

Gestalt: Hier werden aufbauend auf der Wirkstruktur alle gestaltbehafteten Systemelemente durch eine Form abgebildet. Das Gestaltmodell enthält Angaben über Anzahl, Form, Lage, Anordnung sowie Art der Wirkflächen und -orte des Systems.

Zu Beginn der Entwicklung wird mit CONSENS ein disziplinübergreifendes Systemmodell aus den aufgeführten Partialmodellen erstellt. Die Systemmodellierung lässt sich in zwei Phasen aufteilen. In der Workshop-Phase werden die relevanten Systeminformationen zusammengetragen. An den Workshops müssen alle relevanten Stakeholder teilnehmen, um alle wichtigen Systeminformationen zusammenzustellen sowie um ein einheitliches und disziplinübergreifendes Systemverständnis zu erlangen. In der zweiten Phase werden die Ergebnisse der Workshops aufbereitet. Hierfür stehen zur Digitalisierung der Modelle diverse Software-Tools zur Verfügung (vgl. [Kai13, S.59ff.]).

Je nach Zweck und Anwendung können verschiedene Sichten auf das Systemmodell generiert werden. So wird die Komplexität einer Entwicklungsaufgabe beherrschbar.

Bewertung

CONSENS dient der disziplinübergreifenden, modellbasierten Beschreibung mechatronischer Systeme. Hierdurch werden ein intuitives Verständnis und eine leichte Erlernbarkeit erreicht. CONSENS bietet gute Voraussetzungen für den ganzheitlichen und disziplinübergreifenden Entwurf von ITS. Jedoch wird die Pflege und Aktualisierung der Modelle nicht angesprochen. Die Aspekte des Systemschutzes werden nicht adressiert. CONSENS bildet mit den beschriebenen modellbasierten Partialmodellen eine gute Ausgangsbasis, um den Schutz der Systeme in deren Entwurf zu integrieren.

3.3.2 SysML/SYSMOD

Die SysML basiert auf der Unified Modeling Language (UML)[27], adressiert jedoch die ganzheitliche und disziplinübergreifende Modellierung technischer Systeme.

[27] Für detaillierte Informationen zur UML sei auf die Arbeit von FORBRIG verwiesen [For07].

Sprache: Durch die Anwendung verschiedener Diagramme ermöglicht die SysML die Beschreibung der Aspekte Struktur, Anforderungen und Verhalten [Wei06]. Die individuellen Diagramme werden nachfolgend beschrieben [Ana15].

Struktur: Die Struktur wird mit Blöcken beschrieben. Blockdefinitionsdiagramme beschreiben die Beziehungen zwischen den verschiedenen Blöcken. Interne Blockdiagramme legen die Beziehungen zwischen den Bestandteilen eines Blocks fest. Die Beziehungen zwischen den Eigenschaften verschiedener Blöcke können mit Hilfe von Zusicherungsdiagrammen definiert werden.

Anforderungen: Diese werden mit Anforderungsdiagrammen beschrieben. So können bestehende Beziehungen zwischen den Anforderungen spezifiziert werden.

Verhalten: Für die Modellierung des Verhaltens stehen vier Diagrammtypen zur Auswahl. Mit Anwendungsfalldiagrammen lassen sich die Interaktionen der Benutzer oder externen Geräte mit dem System beschreiben. Mögliche Systemzustände werden durch Zustandsdiagramme dargestellt. In Sequenzdiagrammen werden Szenarien abgebildet. Systemabläufe werden mit Aktivitätsdiagrammen visualisiert.

Methode: Die zur SysML gehörige Methode ist SYSMOD und beschreibt ein Vorgehen zur Modellierung komplexer Systeme. Das Vorgehen unterteilt sich in sechs übergeordnete Schritte: Anforderungen ermitteln, Systemkontext modellieren, Anwendungsfälle modellieren, Fachwissen modellieren, Glossar erstellen und Anwendungsfälle realisieren [Wei06].

Zu jedem übergeordneten Schritt existiert ein detaillierteres Vorgehen, das in einem Aktivitätsdiagramm dargestellt wird (vgl. Anhang A3, Bild A-6). In Steckbriefen sind die Beschreibungen der einzelnen detaillierten Schritte festgehalten (vgl. Anhang A3, Bild A-7). Die Steckbriefe enthalten eine Erläuterung sowie die ein- und ausgehenden Daten. Zusätzlich sind Leitfragen aufgeführt. Das mit SYSMOD erstellte Systemmodell stellt eine abstrakte Lösung der Struktur und des Systemverhaltens dar [Wei06].

In der SysML wird ebenfalls die Bildung von Sichten ermöglicht. Je nach Zweck und Anwendung können verschiedene Sichten auf das Modell generiert werden [Alt12].

SysML in Kombination mit SYSMOD ermöglichen die ganzheitliche und disziplinübergreifende Modellierung technischer Systeme. SysML bildet den Entwurf technischer Systeme über die drei Aspekte Struktur, Anforderungen und Verhalten ab. Die Vorgehensschritte der Methode SYSMOD sind am Verhalten des Systems orientiert, sodass der Fokus auf der Software liegt. Aus einem Konstrukt aus Systembausteinen wird die Systemstruktur beschrieben. Ein Baustein kann eine Software, Hardware, Person oder eine beliebige andere Einheit sein.

Bewertung

SysML in Kombination mit SYSMOD ermöglichen die ganzheitliche und disziplinübergreifende Modellierung technischer Systeme. SysML bildet den Entwurf techni-

scher Systeme über die drei Aspekte Struktur, Anforderungen und Verhalten ab. Diese beinhalten einen enormen Umfang an Diagrammen und Konstrukten, deren Verwendung nicht immer eindeutig definiert ist. Die Sprache der SysML bietet durch den Bezug zur UML Vorteile durch die Standardisierung und die weite Verbreitung. Fachdisziplinübergreifend ergeben sich hierdurch jedoch Herausforderungen, da die Vielzahl an Elementen und die Darstellung außerhalb der Softwaretechnik nicht bekannt sind. Somit werden die disziplinübergreifende Erstellung des Systementwurfs und das Gesamtverständnis erschwert. Ferner werden die Aspekte des Systemschutzes nicht berücksichtigt.

3.3.3 METUS

Die Modellierungstechnik METUS wurde von der ID-Consult GmbH in einer Forschungskooperation mit der Daimler AG entwickelt. METUS dient zur Entwicklung und Optimierung von Produktarchitekturen und besteht aus sieben Teilschritten, die in der METUS-Raute in Bild 3-9 dargestellt sind [TGH08], [IDC15-ol].

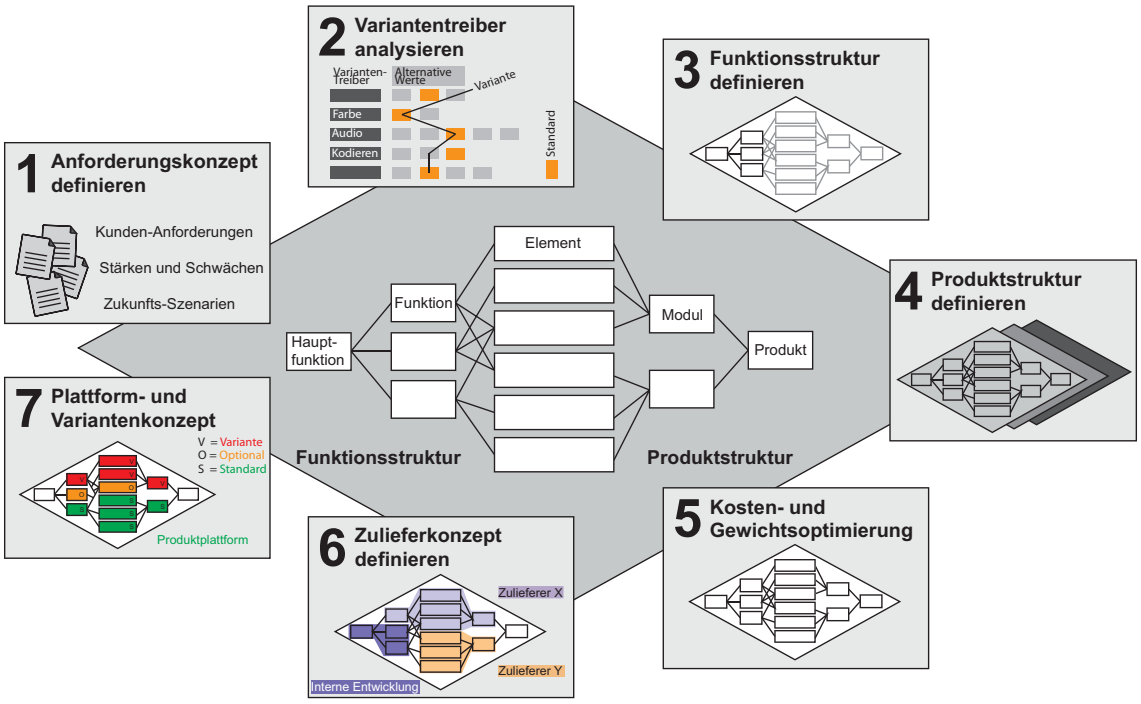


Bild 3-9: Darstellung von Funktions- und Produktstruktur sowie der METUS-Methode nach [TGH08], [TG10]

Sprache: Eine Modellierungssprache wird nicht explizit genannt, die darzustellenden Elemente und deren graphische Notation lassen sich jedoch aus der Methode und dem Werkzeug ableiten [Kai13]. Die Sprache unterteilt sich in die Aspekte Anforderungen, Funktionen und die Systemstruktur. Die Anforderungen werden in einer Liste verwaltet. Es werden z. B. funktionale Anforderungen, Anforderungen an die Produkteigenschaft oder Umgebungsbedingungen unterschieden [TG10].

Die Hauptfunktion wird in ihre Teilfunktionen zerlegt, sodass die Funktionsstruktur hierarchisch dargestellt wird. Ebenso wird die Produktstruktur hierarchisch dargestellt (vgl. Bild 3-9, Hintergrund). Die Systemelemente werden mit den entsprechenden Funktionen verknüpft. Die Elemente können zusätzlich mit Attributen (Standard-, Varianz- oder optionales Element) und Parametern (Gewicht oder Kosten) versehen werden. Durch die Verknüpfung von Elementen entstehen die Module des Systems [Kai13].

Methode: Mit METUS wird in sieben Schritten das Produktkonzept erstellt (vgl. Bild 3-9, Vordergrund). Die Schritte sind im Folgenden erläutert [TGH08], [TG10].

Anforderungskonzept definieren: Mit Hilfe einer Anforderungsanalyse werden die Anforderungen aus Sicht der Kunden und des Unternehmens erfasst.

Variantentreiber analysieren: Für jedes Element werden die Varianten beschrieben. Anhand der geeigneten Kombination der Varianten erfolgt die Produktkonfiguration.

Funktionsstruktur definieren: Die Teilfunktionen des Systems werden aus den Hauptfunktionen gebildet und in der Funktionsstruktur dargestellt.

Produktstruktur definieren: Die Produktstruktur wird aus der Funktionsstruktur abgeleitet. Die Realisierung der Funktionen erfolgt durch Elemente. Die Elemente können zu Modulen zusammengefasst werden.

Kosten- und Gewichtsoptimierung: Die Funktionsverknüpfung mit den Elementen und Modulen wird genutzt, um die Zielkosten sowie das -gewicht zu optimieren.

Zulieferkonzept definieren: Das Zulieferkonzept beschreibt die Zuordnung der Elemente und Module zu internen Abteilungen wie der Entwicklung, Fertigung oder Montage. Auch die Lieferanten werden den Elementen und Modulen zugeordnet.

Plattform- und Variantenkonzept: Hier wird auf Basis der vorangegangenen Schritte die Plattform inklusive der Produktvarianten definiert.

Bei METUS steht die Modularisierung im Fokus. Die Elemente können dargestellt und zu Modulen verknüpft werden. Die einzelnen Teilfunktionen der Hauptfunktion werden hierarchisch betrachtet.

Bewertung

Bei METUS steht die Modularisierung im Fokus. Die Elemente können dargestellt und zu Modulen verknüpft werden. Die einzelnen Teilfunktionen der Hauptfunktion werden hierarchisch betrachtet. Jedoch werden weder die Wirkungsweise noch die Interaktion der Elemente adressiert. Zudem bleibt eine Umfeldbetrachtung aus, sodass die Interaktion mit dem Umfeld nicht ersichtlich wird. Der Systemschutz wird nicht berücksichtigt.

3.4 Interdisziplinäre Entwurfsmuster

Insbesondere der Entwurf komplexer, vernetzter Systeme stellt einen extrem wissensintensiven Prozess dar. Um diesen Prozess effizienter zu gestalten und vorhandenes Wissen besser aufbereiten und nutzen zu können, müssen bereits entwickelte und erprobte Ansätze sowie Lösungen wiederverwendet werden. Darüber hinaus hat die Problemanalyse gezeigt, dass aufgrund der steigenden Interdisziplinarität ein fachdisziplinübergreifender Systementwurf unerlässlich ist (vgl. Kap. 2.4).

Lösungsmuster sind eine Möglichkeit, um den Herausforderungen effektiv zu begegnen. Sie beschreiben bekanntes Wissen, um ein Problem zu lösen oder um zu der Problemlösung beizutragen. So kann das Wissen, welches oft personengebunden ist, in Artefakten beschrieben und gespeichert werden. Lösungsmuster werden als Erweiterung der Methoden des MBSE gesehen. Insbesondere im Systementwurf helfen Lösungsmuster die Entwicklung zu optimieren. Angelehnt an die bereits beschriebenen Informationen des Systemmodells können Lösungsmuster z. B. Anforderungsmuster, Architekturmuster oder mechatronische Systementwurfsmuster sein. Ein Beispiel für ein Lösungsmuster ist z. B. der im Maschinenbau bekannte Hebeleffekt [Ana15] (vgl. Kap. 2.4.5).

Vor diesem Hintergrund werden in Kapitel 3.4.1 Lösungsmuster für selbstoptimierende Systeme untersucht. In Kapitel 3.4.2 stehen Systementwurfsmuster im Fokus. Abschließend werden in Kapitel 3.4.3 Lösungsmuster für fortgeschrittene mechatronische Systeme analysiert.

3.4.1 Lösungsmuster für selbstoptimierende Systeme nach DUMITRESCU

DUMITRESCU erarbeitet eine einheitliche Spezifikation für Lösungsmuster zur Unterstützung der Externalisierung und Wiederverwendung von Wissen. Er fokussiert den Einsatz der Lösungsmuster für den Entwurf mechatronischer Systeme und speziell die Integration kognitiver Funktionen. Die Lösungsmuster werden in sechs Aspekte unterteilt, deren Inhalte mit der Spezifikationstechnik CONSENS (vgl. Kap. 3.3.1) erstellt werden. Die Aspekte sind in Bild 3-10 dargestellt und werden im Folgenden beschrieben [Dum10, S.129ff.].

Merkmale: Die für ein Muster charakteristischen Eigenschaften werden als Merkmale definiert. Diese erlauben Rückschlüsse auf die Anforderungen an das Lösungsmuster. DUMITRESCU empfiehlt Merkmale für die Informationsverarbeitung und für das (physikalische) Grundsystem zu unterscheiden. Charakteristische Merkmale für das Grundsystem sind: *Einsatzbedingungen, Geometrie, Stoffliche Merkmale, Kinematik, Montage, Normung*. Die Merkmale für die Informationsverarbeitung werden benannt als: *Einsatzbedingungen, Zeitpunkt der Aktivität, Echtzeitfähigkeit, Modellierbarkeit, Art der Berechnung, Entität, Signalart, Modellierungs-/Programmiersprache, Datenstruktur*[28].

[28] Für eine detaillierte Erläuterung der einzelnen Merkmale sei auf [Dum10, S.131f.] verwiesen.

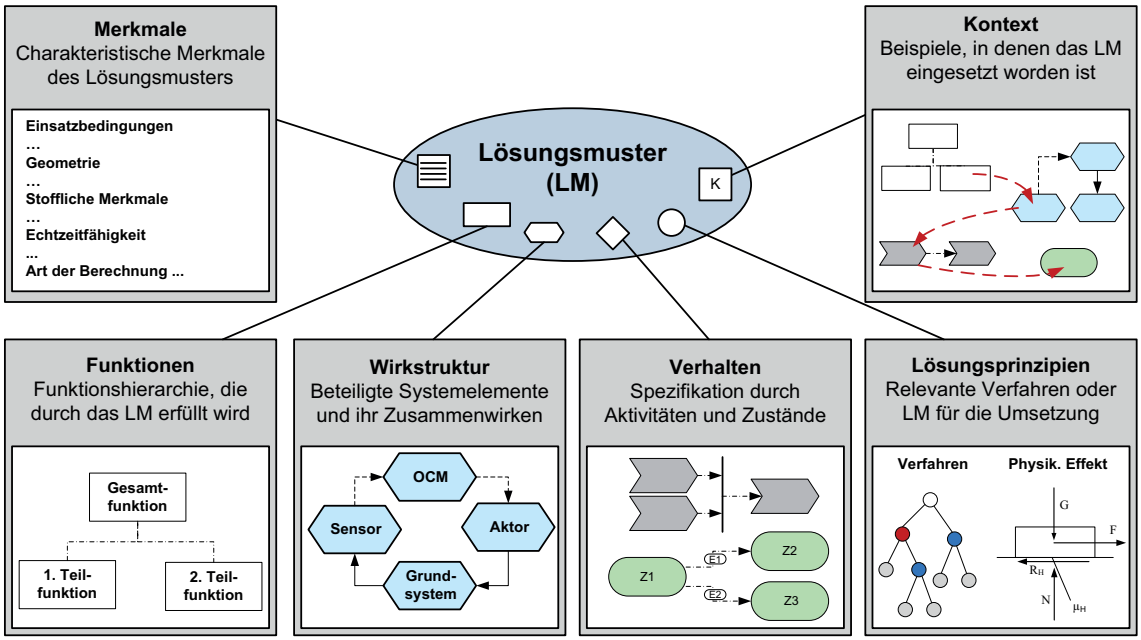


Bild 3-10: Spezifikation eines Lösungsmusters nach DUMITRESCU [Dum10, S.130]

Funktionen: Funktionen beschreiben die Aufgabe eines Lösungsmusters und repräsentieren so das zu lösende Problem. Besteht die Aufgabe aus mehreren Funktionen, so werden diese in einer Funktionshierarchie dargestellt. In Anlehnung an die prinzipiellen Flussarten mechatronischer Systeme (vgl. Kap. 3.3.1, Tabelle 3-2) wird zwischen stoff-, energie- und informationsbestimmten Funktionen differenziert. Die Aspekte Merkmale und Funktionen bilden die Problembeschreibung des Musters.

Wirkstruktur: Lösungsmuster besitzen neben einer Problem- auch eine Lösungsbeschreibung. Die Wirkstruktur bildet den Kern der Lösungsbeschreibung indem alle funktionserfüllenden Systemelemente dargestellt werden. Durch die Spezifikation der Interaktionen zwischen den Systemelementen wird die prinzipielle Wirkungsweise des Lösungsmusters beschrieben.

Verhalten: Die Lösungsbeschreibung des Musters wird neben der Wirkstruktur durch den Aspekt Verhalten komplettiert. Dieser wird in die Bereiche *Verhalten – Aktivitäten* und *Verhalten – Zustände* unterteilt.

Lösungsprinzipien: Die spezifizierte Lösung eines Musters beruht auf Lösungsprinzipien, welche die Basis für die Umsetzung der Lösung darstellen. Die Lösungsprinzipien beruhen wiederum auf Verfahren[29].

Kontext: Zur Vervollständigung eines Lösungsmusters muss dies über mindestens ein Beispiel verfügen. So wird der Kontext der Umsetzung beschrieben und auf zurücklie-

[29] Aufbauend auf den Arbeiten von SAUER [Sau06, S.74] definiert DUMITRESCU ein Verfahren als Abfolge von physikalisch-technischen, chemischen, biologischen oder informationstechnischen Wirkungsabläufen, die zur Funktionsrealisierung notwendig sind [Dum10, S.134].

gende Projekte verwiesen. Zur Beschreibung des Kontexts sind im Idealfall die Aspekte Funktionen, Wirkstruktur und Verhalten zu dokumentieren. Zusätzlich betont DUMITRESCU die Bedeutung von Querverweisen zwischen den Aspekten. Diese geben wichtige Hinweise für eine erneute Verwendung der Lösungsmuster.

Bewertung

Anhand der einheitlichen Spezifikation von Lösungsmustern nach DUMITRESCU können kognitive Funktionen in mechatronische Systeme integriert werden. Mit Hilfe der modellbasierten Beschreibung von Informationen durch Nutzung der Spezifikationstechnik CONSENS wird das interdisziplinäre Verständnis sichergestellt. So wird die Darstellung von Lösungsansätzen über mehrere Disziplinen hinweg ermöglicht. Die Schnittstellen und wechselseitigen Abhängigkeiten zu anderen Lösungsmustern werden hauptsächlich im Aspekt Kontext beschrieben. Diese Beschreibung basiert auf Beispielen. Insbesondere für ITS ist dies nicht ausreichend. Bedingt durch die Entwicklung von mechatronischen zu vernetzen Systemen wird die Vernetzung der einzelnen Systemelemente deutlich ansteigen. Weiterhin wird auch die Komplexität in den Beziehungen zwischen den Lösungsmustern zunehmen. Aus diesem Grund muss die Darstellung der Abhängigkeiten der Lösungsmuster untereinander sowie zu den Fachdisziplinen vereinfacht und transparent abgebildet werden.

3.4.2 Systementwurfsmuster-Metamodell nach PFISTER

Für PFISTER sind Lösungsmuster (Systementwurfsmuster) eine Möglichkeit, um unveränderliches Wissen und Erfahrungen zu repräsentieren. Er hebt die Notwendigkeit hervor, dass dieses Wissen mit Hilfe abstrakter Modelle repräsentiert wird. Hierbei ist nach PFISTER die Modellierungssprache nicht entscheidend. Durch die zusätzliche Identifikation der relevanten Lösungsmuster können diese darüber hinaus beim Lösen von Problemen helfen.

Der Einsatz von Lösungsmustern bietet zahlreiche Vorteile z. B. die Leistungssteigerung (in Form von Umfang und Relevanz), die Verbesserung der Funktionssicherheit (durch etablierte Lösungen, welche mehrmals kontextbezogen eingesetzt und geprüft werden), die Effizienzsteigerung (durch Zeitersparnis von der Produktidee bis zum Serienanlauf) sowie die Förderung von gemeinschaftlichem Arbeiten durch Austausch von Wissen auf einer gemeinsamen Plattform [PCH+11].

PFISTER beschreibt Lösungsmuster in UML und SysML (vgl. Kap. 3.3.2), bei denen er unterschiedliche Klassen und Objekte definiert. Ebenfalls werden die Rollen und Beziehungen spezifiziert. Die Systementwurfsmuster sind durch Angaben wie Name, Autor und Datum spezifiziert und direkt mit den Klassen Funktion und Bestandteil verbunden (vgl. Bild 3-11).

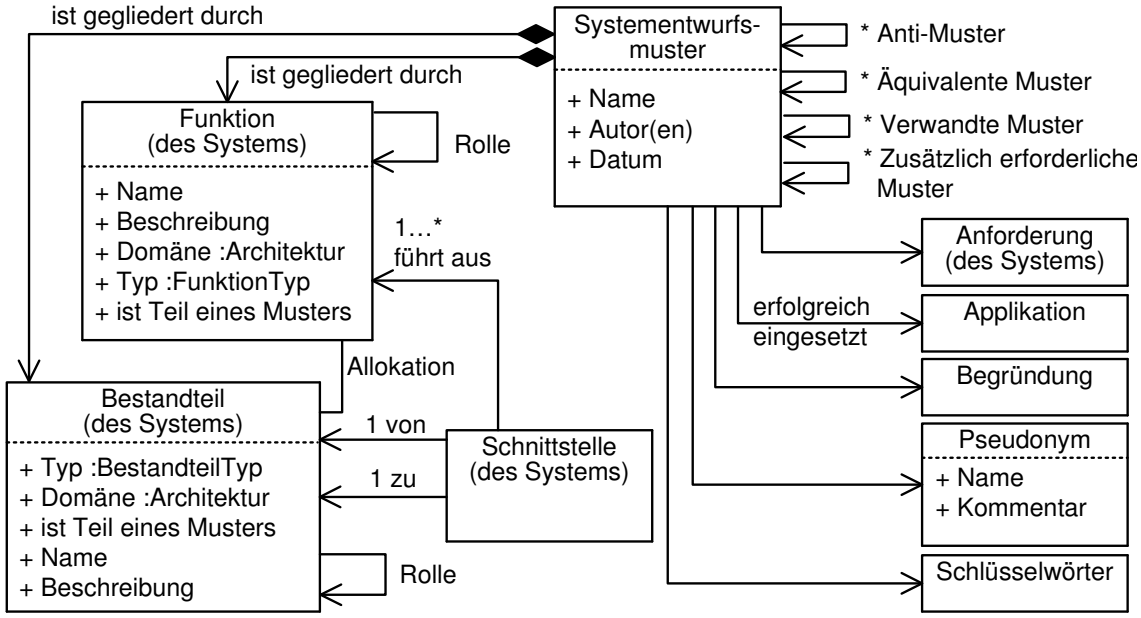


Bild 3-11: Systementwurfsmuster-Metamodell nach PFISTER [PCH+11]

Die Lösungsmuster von PFISTER können Beziehungen zu weiteren Mustern aufweisen. Neben den internen Informationen (Name, Autor und Datum) existieren weitere externe Angaben zur Beschreibung eines Lösungsmusters. Dazu zählen z. B. Angaben über die zugrundeliegenden Anforderungen oder Applikationen, in denen es erfolgreich eingesetzt wurde. Diese Angaben helfen dem Entwickler bei der Suche nach Lösungsmustern in einer Datenbank. Zur Gliederung werden Funktionen und Bestandteile eingesetzt [PCH+11].

Bewertung

PFISTER beschreibt Lösungsmuster mit der Modellierungssprache UML und SysML und betont die Notwendigkeit der modellbasierten Repräsentation sowohl der Problem- als auch der Lösungsbeschreibung. Ebenfalls betont er die Relevanz der Beziehungen zu weiteren Lösungsmustern. Die Sprachen SysML und UML bieten Vorteile durch die Standardisierung und die weite Verbreitung. Fachdisziplinübergreifend ergeben sich jedoch Herausforderungen, da die Vielzahl an Elementen und die Darstellung außerhalb der Softwaretechnik nicht bekannt sind. Somit werden die disziplinübergreifende Erstellung des Systementwurfs und das Gesamtverständnis erschwert. Für die Beschreibung der Lösungsmuster lässt er daher auch weitere Modellierungssprachen zu, jedoch mangelt es an allgemeinverständlichen Beispielen. Den Ansatz auf die modellbasierte Beschreibung von Schutzmustern zu überführen ist aufwändig. Dies liegt in dem hohen Formalisierungsgrad und der gewählten Detailtiefe begründet.

3.4.3 Lösungsmuster für fortgeschrittene mechatronische Systeme nach ANACKER

ANACKER schlägt einen Ansatz zur Beherrschung der Komplexität und Steigerung der Effizienz in der Entwicklung fortgeschrittener mechatronischer Systeme[30] vor. Er erarbeitet Lösungsmuster zur Wiederverwendung von Wissen für den Systementwurf. In seiner Arbeit erweitert ANACKER die Ansätze von DUMITRESCU und verallgemeinert sie. Hierdurch sind die Ansätze allgemeingültig für mechatronische Systeme anwendbar. ANACKER erarbeitet eine einheitliche Strukturierung von Lösungsmustern für den Systementwurf fortgeschrittener mechatronischer Systeme (vgl. Bild 3-12).

Als Systementwurfsmuster definiert ANACKER Lösungswissen, welches fachdisziplinübergreifend beschrieben und allgemeinverständlich ist sowie bei der Erstellung des Systementwurfs unterstützt. Beispielhafte Lösungsmuster für den Systementwurf sind Zusammenarbeit synchronisieren oder Informationsaustausch initiieren[31] [Ana15].

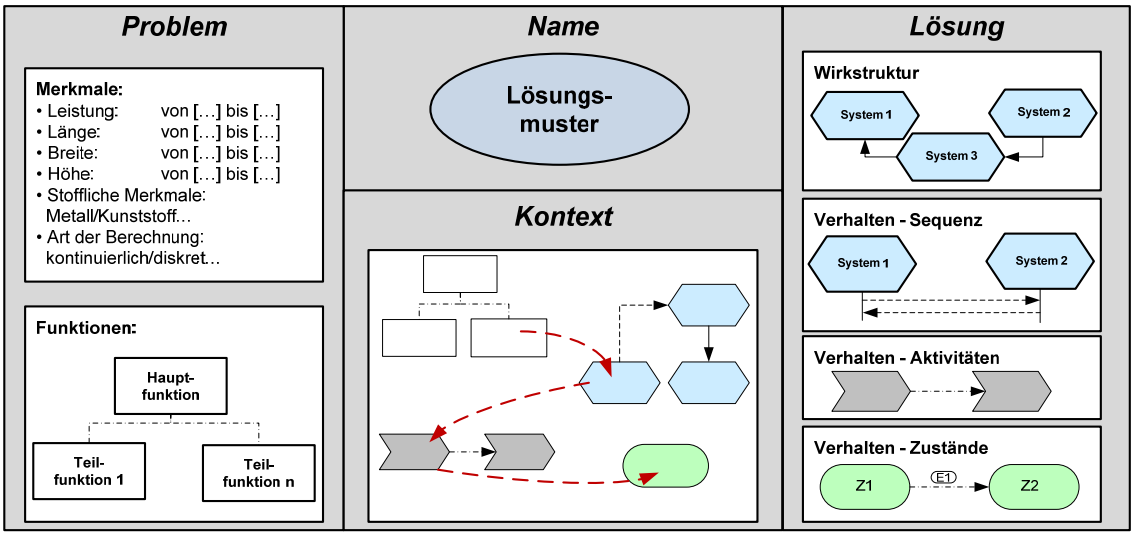


Bild 3-12: Einheitliche Strukturierung von Lösungsmustern für den Systementwurf mechatronischer Systeme nach ANACKER [Ana15, S.106]

Die Lösungsmuster sind durch die Kategorien Name, Problem, Lösung und Kontext spezifiziert. Mit dieser Struktur und der modellbasierten Darstellung der einzelnen Kategorien mit CONSENS (vgl. Kap. 3.3.1) wird das Lösungsmuster fachdisziplinübergreifend und allgemeinverständlich repräsentiert und kann im Systementwurf eingesetzt werden. Die einzelnen Kategorien werden im Folgenden beschrieben [Ana15].

---

[30] Fortgeschrittene mechatronische Systeme werden als zunehmend intelligenter werdende, technische Systeme definiert. Diese basieren auf dem synergetischen Zusammenwirken technischer Fachdisziplinen wie Maschinenbau, Elektrotechnik und Informationstechnik sowie nichttechnischer Disziplinen wie höhere Mathematik, Biologie und Kognitionswissenschaft [VDI2206, S.14], [ADG+09, S.5].

[31] Für weitere Beispiele von Lösungsmustern sei hier auf [Ana15, S.108ff.] verwiesen.

Name: Jedes Muster bekommt einen eindeutigen Namen. So bekommt der Entwickler bei der Suche eines passenden Musters einen Anhaltspunkt für den Inhalt.

Problem: Das zu lösende Problem wird möglichst lösungsneutral mit Hilfe der Aspekte Merkmale und Funktionen beschrieben. Merkmale umfassen sämtliche Eigenschaften, die für das Lösungsmuster charakteristisch sind. Diese können Angaben zur Geometrie, Drehzahl (z. B. in einem Antriebssystem), Bewegungsart, Echtzeitfähigkeit oder zur Art der Berechnung (Informationsverarbeitung) enthalten. Ein Lösungsmuster kann genau eine, oder bei komplexen Mustern auch mehrere Funktionen erfüllen. Diese werden dann in einer Funktionshierarchie abgebildet.

Lösung: Für die Abbildung der Lösung dienen die CONSENS-Partialmodelle Verhalten und Wirkstruktur (vgl. Kap. 3.3.1). Je nach Komplexität müssen nicht zwangsläufig alle Partialmodelle erstellt werden. Die Wirkstruktur bildet den Kern der Lösungsbeschreibung. Es werden die Systemelemente sowie deren Beziehungen untereinander abgebildet. Durch die Verhaltensmodelle wird die Lösungsbeschreibung komplettiert. Die Spezifikation des Verhaltens ist insbesondere für Lösungsmuster mit Schwerpunkt Softwaretechnik relevant. Aktivitäten, Zustände und Sequenzdiagramme bilden erforderliche Informationen je nach Verhalten ab. Den Kern bildet hier die zeitliche Abfolge der Kommunikation. ANACKER erweitert CONSENS um das Partialmodell Verhalten – Sequenz, damit die Anknüpfung an Lösungsmuster aus der Softwaretechnik gewährleistet werden kann.

Kontext: Hier sind Anwendungsbeispiele aufgeführt, in denen das Lösungsmuster bereits erfolgreich eingesetzt wurde. Für die Spezifikation eines Lösungsmusters muss mindestens ein Anwendungsbeispiel angegeben werden.

Besonders hervorzuheben ist die von ANACKER vorgenommene Charakterisierung von Lösungsmustern für den Systementwurf. Lösungsmuster für den Systementwurf besetzen die Schnittstellen zwischen fachdisziplinspezifischen Ansätzen und vereinen diese. Für die Charakterisierung werden folgende drei Dimensionen benutzt [Ana15, S.116ff.].

Art der Wissensrepräsentation: Lösungsmuster dienen in erster Linie zur Repräsentation von Lösungswissen. Dieses kann textbasiert oder modellbasiert dargestellt werden. Insbesondere werden Lösungsmuster in der modernen Entwicklung mechatronischer Systeme durch Modelle abgebildet. Diese unterscheiden sich in ihrem Formalisierungsgrad. Hier wird zwischen formalen und semiformalen Modellen unterschieden.

Spezialisierung des Lösungswissens: Eine Unterscheidung im Grad der Spezialisierung des Lösungswissens ist notwendig, damit sich der Entwickler zu Beginn einer Produktentwicklung nicht in unnötigen Details verliert. Die Spezialisierung nimmt mit fortschreitender Konkretisierung des Entwurfs immer weiter zu.

Aggregation des Lösungswissens: Hier werden die Zusammenhänge zwischen der Spezialisierung (generalisiert zu spezialisiert) und der Aggregation (elementar zu komplex) von Lösungswissen beschrieben.

Auf Grundlage der Charakterisierung der Lösungsmuster und der aufgezeigten Zusammenhänge zwischen den Mustern entwickelt ANACKER einen multidimensionalen **Wissensraum**. Dieser beinhaltet Lösungsmuster für die Produktentwicklung und bildet deren wechselseitige Beziehungen ab (vgl. Anhang A4, Bild A-8, links und Kap. 3.5.4). Der definierte Wissensraum unterscheidet die Spezialisierung des Lösungswissens (generalisiert zu spezialisiert), die Aggregation des Lösungswissens (elementar zu komplex) sowie die Art der Wissensrepräsentation (modellbasiert und textbasiert). Die modellbasierte Wissensrepräsentation wird weiter zwischen formalen und semiformalen Ansätzen unterschieden [Ana15, S.120ff.]. Der Wissensraum stellt somit eine Plattform dar, welche die Kommunikation und Kooperation im Rahmen der fachdisziplinübergreifenden Entwicklung verbessert.

Bewertung

Durch die Arbeit von ANACKER wird eine einheitliche Strukturierung für Lösungsmuster erarbeitet. Die Strukturierung von Lösungsmustern ist geeignet, um multidisziplinäre Lösungsansätze darzustellen. Darüber hinaus wird das personengebundene Wissen externalisiert und fließt so für alle Disziplinen gleichermaßen zugänglich in die Entwicklung ein. Die Lösungsmuster werden in einem Wissensraum eingeordnet und so für die Wiederverwendung gespeichert. Die genannten Vorteile von Lösungsmustern (Hilfsmittel zur Beherrschung von Komplexität, Anregung der Kreativität) bieten einen geeigneten Ansatz, um die Entwicklung intelligenter Systeme effizienter zu gestalten. Die Lösungsmuster werden mit CONSENS beschrieben, so dass sie im Entwurf intelligenter, vernetzter Systeme berücksichtigt werden können. Die Aspekte des Systemschutzes werden jedoch nicht beachtet, jedoch bietet die Spezifikationstechnik CONSENS eine gute Ausgangsbasis, zur Berücksichtigung dieser. Der von ANACKER beschriebene Einsatz von Lösungsmustern im Systementwurf kann als ein Ansatz für die Integration des Systemschutzes in die frühen Phasen der Systementwicklung gesehen werden.

3.5 Musterbasierter Entwurf Intelligenter Technischer Systeme

Der musterbasierte Entwurf komplexer und vernetzter Systeme erfordert ein geeignetes Vorgehen. Die Problemanalyse hat gezeigt, dass ein geeignetes Vorgehen den frühzeitigen, interdisziplinären Systementwurf unterstützen muss (vgl. Kap. 2.4.4). Zusätzlich ist insbesondere die Berücksichtigung von erfolgreich eingesetztem Lösungswissen entscheidend (vgl. Kap. 2.4.5). Aus diesen Gründen wird in Kapitel 3.5.1 der musterbasierte Entwurf selbstoptimierender Systeme untersucht. In Kapitel 3.5.2 wird ein SE Entwurfsmuster-Metamodell fokussiert betrachtet. In Kapitel 3.5.3 wird ein Ansatz zur Identifizierung von Systemarchitekturmustern aufgezeigt. Abschließend ist in Kapitel 3.5.4 ein Ansatz zum lösungsmusterbasierten Entwurf fortgeschrittener mechatronischer Systeme beschrieben.

3.5.1 Musterbasierter Entwurf der selbstoptimierenden Informationsverarbeitung nach DUMITRESCU

DUMITRESCU erarbeitet eine Strukturierung für Lösungsmuster der Selbstoptimierung (vgl. Kap. 3.4.1) und beschreibt den musterbasierten Entwurf der selbstoptimierenden Informationsverarbeitung. Als Grundlage dient ein Vorgehensmodell zur Integration kognitiver Funktionen in mechatronische Systeme. Dies ist in Bild 3-13 dargestellt.

Das Vorgehensmodell berücksichtigt die Vorgehensweise für den Systementwurf nach der VDI-Richtlinie 2206. Der Entwurf der intelligenten Informationsverarbeitung liegt im Fokus der Betrachtung. Das Vorgehensmodell gibt einen Überblick über die wesentlichen Tätigkeiten und zu erarbeitenden Resultate. Es gliedert sich in Phasen und Meilensteine und legt die Reihenfolge zur Durchführung der Phasen fest. Sowohl die Darstellung als auch die Reihenfolge ist idealtypisch. Die reale Anwendung ist geprägt durch Iterationen und Rücksprünge in vorangegangene Phasen. DUMITRESCU nennt als Ausgangspunkt für das Vorgehensmodell ein nicht vollständig konzipiertes mechatronisches System. Das zu entwickelnde System enthält keine spezifizierte Informationsverarbeitung. Diese wird mittels des Vorgehens erarbeitet. Die einzelnen Phasen des Vorgehensmodells sind im Folgenden beschrieben [Dum10].

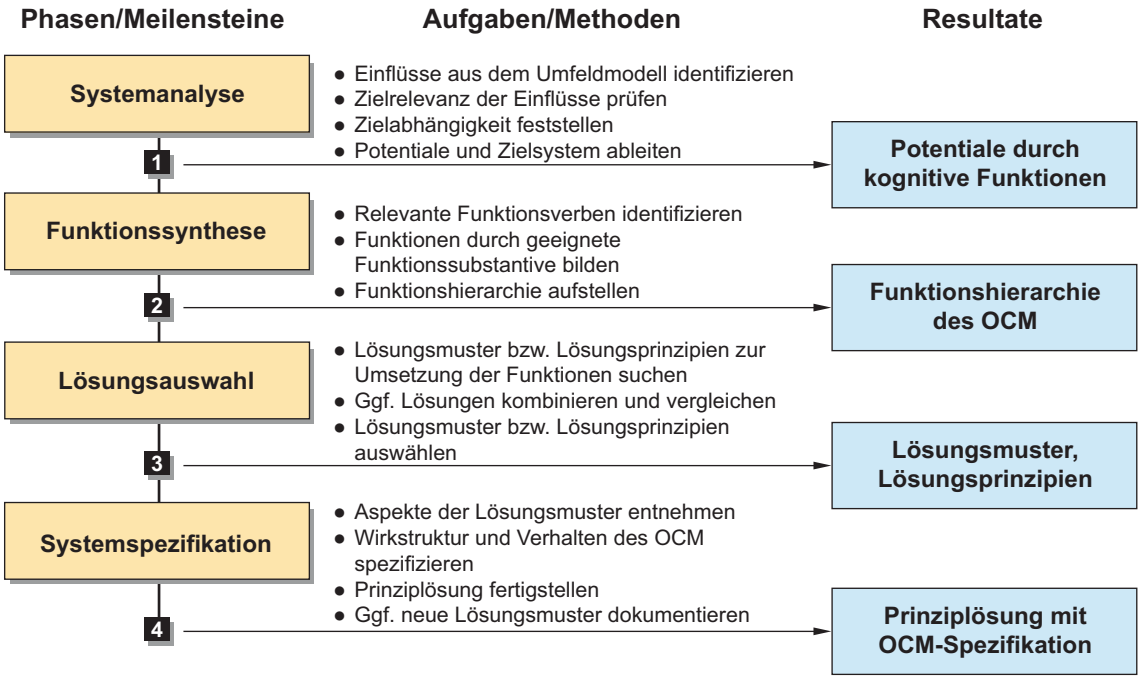


Bild 3-13: Vorgehensmodell für den lösungsmusterbasierten Entwurf mechatronischer Systeme nach DUMITRESCU [Dum10, S.100]

Systemanalyse: In der ersten Phase des Vorgehensmodells werden die bisher erarbeiteten Entwicklungsresultate gesichtet. Darauf aufbauend erfolgt eine Analyse des mechatronischen Systems hinsichtlich der zu erwartenden Nutzenpotentiale durch die Integration kognitiver Funktionen. Demnach klärt diese Phase den Bedarf für die Integration kognitiver Funktionen. Zur Untersuchung der Nutzenpotentiale erarbeitet DUMITRESCU

die Methode zur Zielabhängigkeitsanalyse[32] und schlägt die weitere Ausarbeitung des mechatronischen Systems mit CONSENS (vgl. Kap. 3.3.1) vor. Werden so Nutzenpotentiale identifiziert, wird das Vorgehensmodell weiter durchlaufen. Hat die Analyse ergeben, dass keine Nutzenpotentiale vorliegen, ist das Vorgehensmodell beendet. Hier kann mit klassischen Entwurfsmethoden (z. B. VDI 2206) fortgefahren werden.

Funktionssynthese: Die zweite Phase hat das Ziel, eine Funktionshierarchie des zu entwickelnden Systems (hier Operator-Controller-Modul (OCM)) aufzustellen. Der Fokus liegt auf der Spezifikation der notwendigen kognitiven Funktionen. Diese können abstrakt mit Hilfe eines Funktionsverbenkatalogs[33] von Entwicklern unterschiedlicher Disziplinen beschrieben werden. Eine von DUMITRESCU entwickelte Entwurfsschablone für die Funktionshierarchie erleichtert die Spezifikation des Systems.

Lösungsauswahl: In dieser Phase werden auf Basis der zuvor erarbeitenden Funktionshierarchie geeignete Lösungen (Lösungsmuster) gesucht und ausgewählt. Die Suche erfolgt durch die Zuordnung der Teilfunktionen der untersten Gliederungsebene mit dem Aspekt Funktionen der einheitlichen Spezifikation eines Lösungsmusters (vgl. Kap. 3.4.1). So wird der Rückschluss auf ein passendes Lösungsmuster ermöglicht.

Systemspezifikation: In der letzten Phase wird die Komplettierung der Prinziplösung des mechatronischen Systems angestrebt. Durch die Informationen der ausgewählten Lösungsmuster kann das System mit der Spezifikationstechnik CONSENS ganzheitlich beschrieben werden. Der Schwerpunkt liegt auf der Konzipierung der Informationsverarbeitung. Zur Unterstützung der Entwickler erarbeitet DUMITRESCU eine Entwurfsschablone für die Wirkstruktur mechatronischer Systeme sowie eine Übersicht über ausgewählte Systemelemente der Informationsverarbeitung[34].

Bewertung

DUMITRESCU beschreibt ein Vorgehensmodell für den musterbasierten Entwurf mechatronischer Systeme. Dieses versetzt Dritte in die Lage, die kognitive Informationsverarbeitung zu spezifizieren. Der Fokus liegt auf dem Entwurf der intelligenten Informationsverarbeitung mit dem Ziel der Integration von Kognition in den Systementwurf. Aspekte des Systemschutzes finden keine Berücksichtigung. Der allgemeine Ansatz zur Integration kann als Grundlage für die vorliegende Arbeit genutzt werden.

---

[32] Mit der Methode wird die Notwendigkeit des Einsatzes kognitiver Funktionen in mechatronischen Systemen festgestellt. Für weitere Details sei auf [Dum10, S.102ff.] verwiesen.

[33] Der Katalog definiert wesentliche Funktionsverben zur Beschreibung informationsverarbeitender Funktionen für mechatronische Systeme. Für weitere Informationen sei auf [Dum10, S.118ff.] verwiesen.

[34] Für weitere Informationen sei auf [Dum10, S.111ff.] verwiesen.

3.5.2 Lösungsmusterbasiertes Systems Engineering nach PFISTER

PFISTER schlägt einen Ansatz zur Anwendung von Lösungsmustern im SE vor. Dieser basiert auf Lösungsmustern aus der Softwaretechnik und verfolgt zwei Ziele. Erstens sollen Entwickler unterstützt werden, benötigtes Wissen zu externalisieren und erneut einzusetzen. PFISTER geht speziell auf disziplinübergreifendes Wissen ein. Zweitens soll den Entwicklern ermöglicht werden, relevante Lösungsmuster zu identifizieren und diese anzuwenden [PCH+11].

Damit Lösungsmuster im modellbasierten Systementwurf eingesetzt werden können, sind diese mit einer formalisierten Sprache zu beschreiben und in einer Datenbank abzulegen. Zusätzlich müssen die Modelle in eine Entwicklungsumgebung einzubinden sein. PFISTER entwickelt ein Metamodell zur Verwendung im SE, das primär den Anspruch hat, die Lösungsmuster in das übergeordnete SE einzubetten. Das Metamodell ist in Bild 3-14 als UML-Diagramm dargestellt.

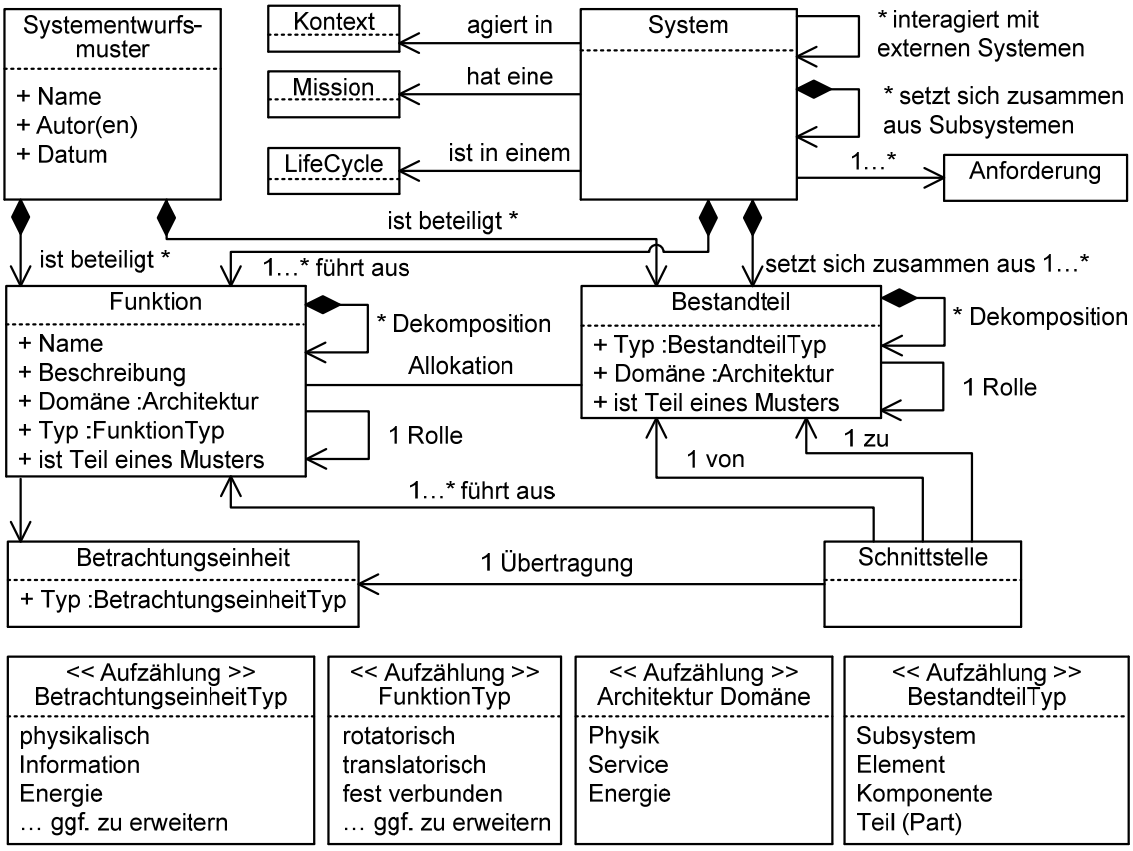


Bild 3-14: Metamodell für ein lösungsmusterbasiertes Systems Engineering nach PFISTER (vgl. [PCH+11])

Die definierten Lösungsmuster für das SE werden als Systementwurfsmuster bezeichnet und in das Metamodell eingeordnet. Die Systementwurfsmuster sind direkt mit den Klassen *Funktion* und *Bestandteil* verbunden. Aufgrund dieser direkten Verbindung sind die Lösungsmuster indirekt ebenfalls mit der Klasse *System* verbunden. Innerhalb einer Klasse kann auf Typen verwiesen werden, für die Auswahllisten existieren oder

ggf. definiert werden müssen. So wird in der Klasse *Bestandteil* auf den Typ *:BestandteilTyp* verwiesen. In diesem Typ ist eine Auswahlliste bestehend aus Subsystem, Element, Komponente und Teil (Part) hinterlegt. Ein Lösungsmuster definiert das Zusammenwirken von Komponenten und Funktionen eines Systems in generalisierter Art und Weise. Das relevante Lösungswissen wird in einem Lösungsmuster mit Hilfe abstrakter physikalischer oder funktionaler Modelle dargestellt. Daher bietet sich die Anwendung von Lösungsmustern im SE bei der Synthese von funktionalen und physikalischen Architekturen an. Jedoch sollten Lösungsmuster nicht individuell, sondern im Zusammenhang betrachtet werden [PCH+11].

Bewertung

Pfister beschreibt mit der UML die allgemeine Einbettung von Lösungsmustern im Systems Engineering. Hierbei betrachtet er den Entwurf eines technischen Systems. Die Wiederverwendung von Lösungswissen wird angesprochen, allerdings kann die Durchgängigkeit im Sinne der ganzheitlichen Produktentstehung nach GAUSEMEIER nicht sichergestellt werden.

3.5.3 Identifizierung von Systemarchitekturmustern nach KALAWSKY

KALAWSKY benutzt Systemarchitekturmuster, um komplexe Systeme zu entwerfen und zu analysieren. Dafür untersucht er die Erstellung von Systemarchitekturen mit Lösungsmustern. Zusätzlich beschreibt er ein Vorgehen zur Identifikation von Systemarchitekturmustern auf Basis bestehender Systeme. Das erarbeitete Vorgehensmodell zur Definition von Systemarchitekturmustern ist in Bild 3-15 gezeigt und wird im Folgenden beschrieben [KJT+13].

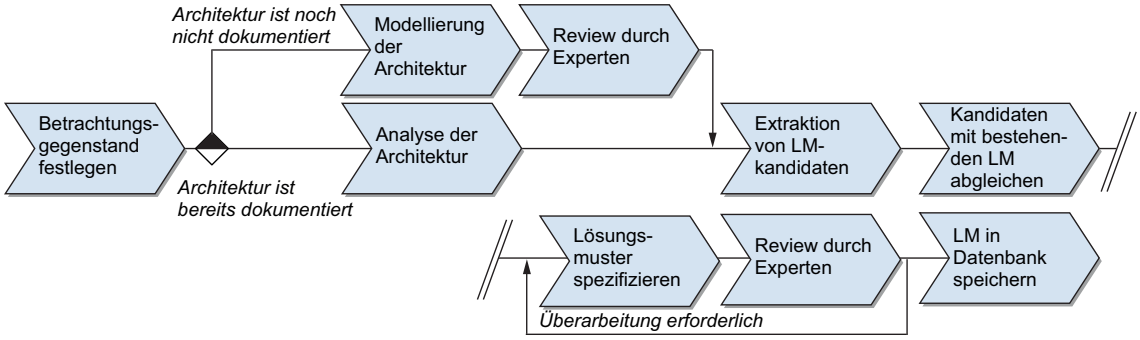


Bild 3-15: Vorgehensmodell zur Definition von Systemarchitekturmustern nach KALAWSKY [KJT+13, S.289]

Das Vorgehensmodell stellt nach KALAWSKY die Zusammenfassung des iterativen Identifikationsprozesses dar. Der Prozess beinhaltet Diskussionen und Abstimmungen zwischen einem Systemarchitekten und den Experten der an der Systementwicklung beteiligten Fachdisziplinen. Da der Systemarchitekt für die Identifikation der fachdisziplinübergreifenden Zusammenhänge zwischen den einzelnen Teilsystemen verantwortlich ist, ordnet ihm KALAWSKY die Schlüsselrolle für einen erfolgreichen Prozess zu.

In dem Vorgehensmodell zur Definition von Systemarchitekturmustern ist der erste Schritt die Festlegung des zu betrachtenden Gegenstands. Auf diesem Schritt bauen alle folgenden Tätigkeiten auf. Das weitere Vorgehen hängt davon ab, ob bereits eine modellbasierte Spezifikation des Betrachtungsgegenstands vorliegt. Ist eine Spezifikation vorhanden, so wird diese im nächsten Schritt analysiert. Für den Fall, dass keine Spezifikation vorliegt, ist die Architektur entsprechend zu modellieren.

Die folgenden zwei Schritte extrahieren erste Anhaltspunkte für potentielle Kandidaten innovativer Lösungsmuster. Falls der potentielle Kandidat ein neuartiges Lösungsmuster (LM) darstellt, so wird dieses entsprechend spezifiziert. Die Spezifikation ist vom Systemarchitekten durchzuführen. Anschließend muss das erarbeitete Lösungsmuster mit Experten besprochen werden. Solch ein Review ist notwendig, da an einem Systemarchitekturmuster zahlreiche Fachdisziplinen beteiligt sind. Die Schritte der Spezifikation des Lösungsmusters sowie des Reviews sind solange zu wiederholen, bis alle erforderlichen Informationen im Lösungsmuster spezifiziert sind. Auf Grundlage der abschließenden Speicherung der Lösungsmuster in einer Datenbank wird die langfristige Sicherung des Wissens gewährleistet.

Die Analyse der Spezifikation eines Systems beschreibt KALAWSKY gesondert. Demnach können Lösungsmuster auf allen hierarchischen Ebenen der Systemarchitektur gefunden werden. Anhand der Analyse möglicher Veränderungen der Systemarchitektur können Verbesserungspotentiale oder vorhandene Probleme aufgezeigt werden. Damit alternative Systemarchitekturen verglichen werden können, müssen Vorhersagemodelle und Simulationen erstellt und genutzt werden [KJT+13].

Bewertung

Das Vorgehensmodell von KALAWSKY beschreibt die durchzuführenden Tätigkeiten zur Identifizierung von Systemarchitekturmustern hauptsächlich generisch. Der Systemarchitekt wird hervorgehoben. Ihm kommt die Schlüsselrolle zu. Voraussetzung ist jedoch, dass der Systemarchitekt über fachdisziplinübergreifendes Know-how verfügt. In dem Vorgehen werden keine Hinweise auf die Verwendung einer bestimmten Spezifikationstechnik gegeben. Ferner wird nicht auf die Strukturierung der Lösungsmuster eingegangen. Ebenso mangelt es an Details zur Verwendung von Werkzeugen für die Analyse der Systemarchitektur. Darüber hinaus fehlt der Bezug auf ITS. Zusammenfassend bleibt festzuhalten, dass das Vorgehen nach KALAWSKY lediglich einen groben Rahmen liefern kann.

3.5.4 Lösungsmusterbasierter Entwurf fortgeschrittener mechatronischer Systeme nach ANACKER

ANACKER erarbeitet eine einheitliche Strukturierung von Lösungsmustern für fortgeschrittene mechatronische Systeme (vgl. Kap. 3.4.3) und entwickelt zusätzlich ein Vorgehensmodell für einen lösungsmusterbasierten Systementwurf. In Anlehnung an die

Strukturierung nach GAUSEMEIER definiert ANACKER die Erkenntnisse aus der strategischen Produktplanung (vgl. Kap. 2.4.1) als Eingangsinformationen für das Vorgehen. Das Vorgehensmodell ist in Bild 3-16 dargestellt. Es unterteilt sich in fünf aufeinanderfolgende Phasen, welche im Weiteren beschrieben werden [Ana15, S.131ff.].

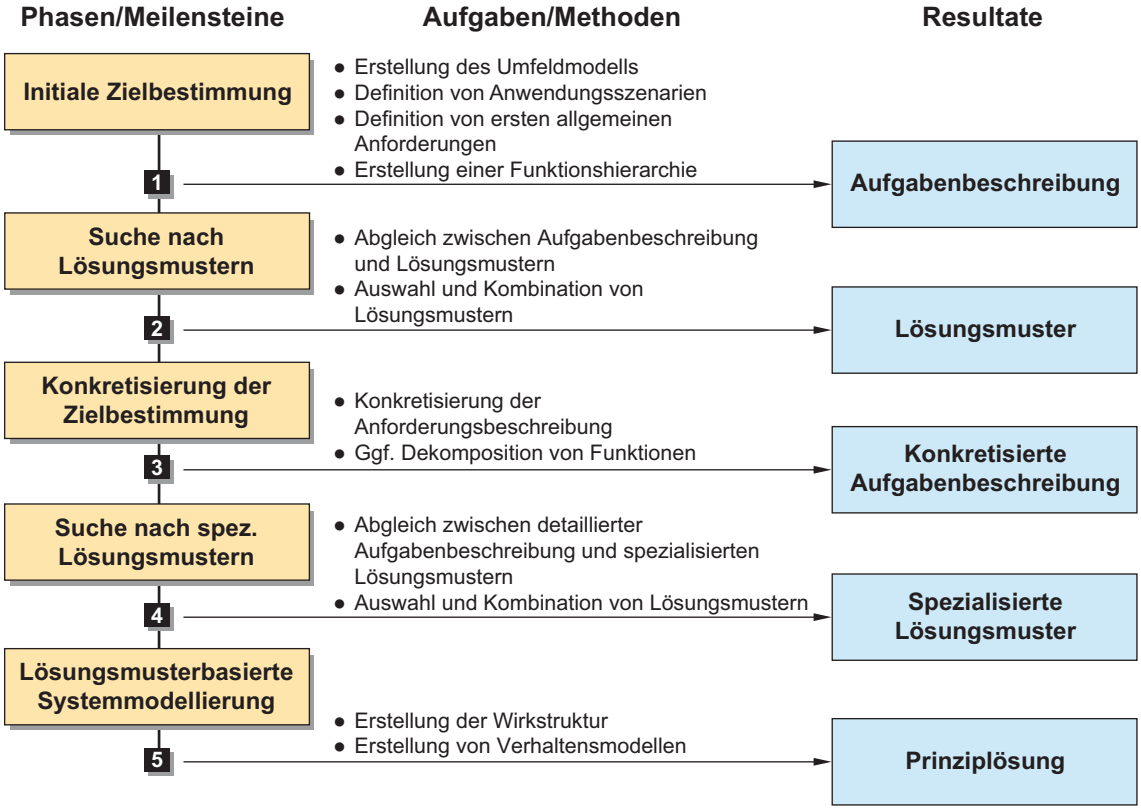


Bild 3-16: Vorgehensmodell für einen lösungsmusterbasierten Systementwurf nach ANACKER [Ana15, S.131]

Initiale Zielbestimmung: Das Ziel dieser Phase ist die Schaffung einer ersten Grundlage, auf der ein interdisziplinäres Entwicklerteam nach potentiellen Lösungsmustern suchen kann. Diese Phase umfasst die klassischen Tätigkeiten Aufgabenbeschreibung, Zielbestimmung, Synthese und Analyse. Hierfür werden ein Modell des Systemumfelds, erste Anwendungsszenarien und Anforderungen sowie die Funktionshierarchie spezifiziert. Für die entsprechenden Modelle der Spezifizierung wird die Spezifikationstechnik CONSENS angewendet.

Suche nach Lösungsmustern: Das Ziel dieser Phase ist eine erste Einschränkung des Suchraums. Hier steht die Analyse der Funktionshierarchie im Fokus der Betrachtung. ANACKER unterscheidet bei der Funktionshierarchie zwischen der Top-Down und der Bottom-Up Suchstrategie. Der Top-Down Ansatz beginnt die Suche bei der Hauptfunktion und durchläuft die einzelnen Ebenen der Hierarchie solange, bis eine Lösung gefunden wird. Es wird das Ziel verfolgt, möglichst schnell Lösungsmuster mit einem hohen Aggregationsgrad für die vorliegende Entwicklungsaufgabe zu identifizieren. Die Bottom-Up Suche beginnt auf der untersten Hierarchieebene. Durch diese Suchstrategie

werden Lösungsalternativen für die einzelnen Teilfunktionen fokussiert. Beide Suchen basieren darauf, dass die Anforderungen und Funktionen aus der ersten Phase mit der Problembeschreibung der Lösungsmuster verglichen werden. Sollte für Funktionen kein Lösungsmuster gefunden werden, so sind neuartige Konzepte zur Erfüllung der Funktion zu erarbeiten. Das Ergebnis der Phase ist ein morphologischer Kasten mit einer Gegenüberstellung von potentiellen Lösungsmustern und den in der initialen Zielbestimmung ermittelten Funktionen.

Konkretisierung der Zielbestimmung: In dieser Phase wird die bestehende Spezifikation aus Phase 1 (im Kern Anforderungen und Funktionshierarchie) konkretisiert. Dies ist nötig, da die in Phase 2 durchgeführte Auswahl und Kombination von Lösungsmustern in der Regel zu neuen Erkenntnissen bei den Entwicklern führt. Somit ist das Ergebnis dieser Phase eine konkretisierte Aufgabenbeschreibung, bestehend aus einer konkretisierten Anforderungsliste sowie einer Funktionshierarchie.

Suche nach spezialisierten Lösungsmustern: Die Suche in dieser Phase verläuft analog zur Suche nach Lösungsmustern in Phase 2. Ausgehend von den bereits ausgewählten generalisierten Lösungsmustern, werden nun spezialisierte Lösungsmuster gesucht. Mit diesen ist es möglich, den Systementwurf weiter zu konkretisieren. ANACKER weist darauf hin, dass insbesondere die Phasen 3 und 4 ggf. iterativ zu durchlaufen sind.

Lösungsmusterbasierte Systemmodellierung: In der letzten Phase des Vorgehensmodells werden die Wirkstruktur und die Verhaltensmodelle auf fachdisziplinübergreifender Ebene aufgebaut. Für die Erstellung der Wirkstruktur werden aufbauend auf den Lösungsmustern die Systemelemente und deren interne Beziehungen innerhalb der Muster dargestellt. Die Systemelemente werden zu einem verträglichen Gesamtsystem kombiniert. Analog zur Wirkstruktur werden die Verhaltensmodelle mit der Spezifikationstechnik CONSENS erarbeitet. Das von ANACKER entwickelte Partialmodell Verhalten – Sequenz beinhaltet detaillierte Informationen zu einer bidirektionalen Kommunikation zwischen mindestens zwei Systemelementen. Diese Anteile des Verhaltens werden direkt in die Wirkstruktur integriert. Somit liegt als abschließendes Ergebnis eine fachdisziplinübergreifende Spezifikation für das mechatronische System vor.

Besonders hervorzuheben ist das aufgezeigte **Zusammenspiel zwischen dem Wissensraum** (vgl. Anhang A4, Bild A-8, links sowie Kap. 3.4.3) **und den Ebenen im Systementwurf** (Anhang A4, Bild A-8, rechts) von mechatronischen Systemen. Der definierte Wissensraum beinhaltet notwendige Lösungsmuster für eine Produktentwicklung. Diese werden anhand der drei Achsen Spezialisierung des Lösungswissens (X-Achse), Art der Wissensrepräsentation (Y-Achse) sowie Aggregation des Lösungswissens (Z-Achse) charakterisiert.

Im Systementwurf werden die Entwurfsebenen **disziplinübergreifende System-Ebene** und **disziplinorientierte Mechatronik-Ebene** unterschieden (vgl. Anhang A4, Bild A-8, rechts). Hier verläuft die Konkretisierung von links nach rechts [Ana15, S.123ff.].

Disziplinübergreifende System-Ebene: Zu Beginn des Entwurfs wird die Zielbestimmung durchgeführt, mit dem Fokus, alle Anforderungen an das zu entwickelnde System zu ermitteln. Auf Basis der Anforderungen wird anschließend die Funktionshierarchie definiert. Auf dieser Basis erfolgt nun die Suche nach Lösungsmustern im Wissensraum. Nach der Auswahl und Kombination der Lösungsmuster werden deren Informationen (Wirkstruktur und Verhalten) genutzt, um das System auf Gesamtsystemebene semiformal zu spezifizieren. Nun erfolgt die Konkretisierung der Struktur- und Verhaltensmodelle indem auf zusätzliche, fachdisziplinspezifische Informationen zurückgegriffen wird. Dieser Prozess ist als iterativ zwischen der disziplinübergreifenden System-Ebene und der disziplinorientierten Mechatronik-Ebene anzusehen.

Disziplinorientierte Mechatronik-Ebene: Hier wird die Ausarbeitung in den einzelnen Fachdisziplinen fokussiert. Der Übergang in die disziplinorientierte Mechatronik-Ebene beruht auf zwei Aspekten. Zum einen werden die bereits spezifizierten, disziplinübergreifenden Informationen in die Mechatronik-Ebene transformiert. Zum anderen wird der Übergang maßgeblich durch die Verbindungen im Wissensraum sichergestellt. Hierbei sind insbesondere die Informationen zu den Schnittstellen zwischen den Fachdisziplinen von hoher Bedeutung. Zusätzlich werden die Informationen zu den ausgewählten fachdisziplinspezifischen Lösungsmustern übermittelt. Nach der disziplinspezifischen Bearbeitung muss der aktuelle Stand in das übergeordnete Systemmodell eingepflegt werden, damit Änderungen und Aktualisierungen von allen Disziplinen gleichermaßen verfolgt werden können.

Nach ANACKER genügt es im Entwurf fortgeschrittener mechatronischer Systeme nicht mehr, zu Beginn eine Prinziplösung zu erstellen und nach der Übergabe des Entwurfs in die Fachdisziplinen die Entwicklung losgelöst zu betreiben. Auch eine regelmäßige Abstimmung der beteiligten Disziplinen ist nicht weitreichend genug. Vielmehr muss ein zentrales Modell initial erstellt und über die gesamte Entwicklung hinweg aktualisiert und erweitert werden (vgl. Anhang A4, Bild A-8, rechts). So wird die Komplexität beherrscht und nachträgliche Änderungen basierend auf Missverständnissen werden vermieden [Ana15].

Bewertung

Zur Nutzung der Lösungsmuster im Entwurf fortgeschrittener mechatronischer Systeme beschreibt ANACKER ein Vorgehensmodell. Er entwickelt einen interdisziplinären und ganzheitlichen Ansatz. Durch dieses Vorgehen wird der Entwurf fortgeschrittener mechatronischer Systeme mit Hilfe von Lösungsmustern ermöglicht. Mit der Verknüpfung des Systementwurfs und den Lösungsmustern des Wissensraums wird das Zusammenspiel zwischen den Entwurfsebenen und den Disziplinen beschrieben. Zusätzlich wird die Verwendung der Lösungsmuster im Systementwurf dargestellt.

Der Systemschutz wird nicht betrachtet. Jedoch bieten das erarbeitete Vorgehen zum Systementwurf sowie die Strukturierung der Lösungsmuster geeignete Ansätze für die Erweiterung des lösungsmusterbasierten Entwurfs um die Aspekte des Systemschutzes.

3.6 Bewertung und Handlungsbedarf

Ein Vergleich des Stands der Technik mit den abgeleiteten Anforderungen aus Kapitel 2 führt zu folgender Bewertung. Diese ist in Bild 3-17 zusammengefasst.

Bewertung der untersuchten Ansätze hinsichtlich der gestellten Anforderungen.

Bewertungsskala:

○ = nicht erfüllt
◐ = teilweise erfüllt
● = voll erfüllt

Legende: s.o. = selbstoptimierenden
mech. = mechatronischer

			Anforderungen								
			Charakterisierung ITS-spezifischer Schutzanforderungen	Bereitstellung passender Schutzmaßnahmen für ITS	Darstellung der Kompetenzen der Imitatoren und der Angriffsmöglichkeiten	Interdisziplinarität und Ganzheitlichkeit	Modellbasierte Maßnahmenbeschreibung zur Verwendung im Systementwurf	Wiederverwendung von Lösungswissen	Frühzeitige und durchgängige Berücksichtigung des Systemschutzes	Integration in etablierte Standards des Systementwurfs	Präventiver Schutz auf Basis technischer Schutzmaßnahmen
			A1	A2	A3	A4	A5	A6	A7	A8	A9
Schutz für Intelligente Technische Systeme	Schutzmaßnahmenkataloge	Schutz vor Produktpiraterie nach Abele et al.	○	◐	○	○	○	○	○	○	◐
		Know-how Schutz im Wettbewerb nach Lindemann et al.	○	◐	●	◐	○	○	○	○	◐
		Präventiver Produktschutz nach Gausemeier et al.	○	◐	○	◐	○	◐	○	○	◐
	Entwurf präventiv imitationsgeschützter Systeme	Methodik zum Schutz gegen Produktimitationen nach Neemann	○	○	◐	○	○	○	◐	○	◐
		Präventiver Nachahmungsschutz bei technischen Produkten nach Schnapauff	○	○	○	○	○	○	◐	○	◐
		Beitrag zum ganzheitlichen Know-how-Schutz nach Meimann	○	○	○	◐	○	○	◐	●	○
		Präventives Schutzkonzept für Investitionsgüter - PROTACTIVE	○	○	◐	○	◐	○	◐	●	●
		Konzipierung geschützter Produkte und Produktionssysteme nach Kokoschka	○	○	◐	○	○	○	◐	●	●
Entwurf Intelligenter Technischer Systeme	Modellierungstechniken	CONSENS	○	○	○	●	●	◐	○	○	○
		SysML/SYSMOD	○	○	○	◐	◐	◐	○	○	○
		METUS	○	○	○	○	○	◐	○	○	○
	Entwurfsmuster	Lösungsmuster für selbstoptimierende Systeme nach Dumitrescu	○	○	○	◐	◐	●	○	●	○
		Systementwurfsmuster-Metamodell nach Pfister	○	○	○	◐	○	◐	○	◐	○
		Lösungsmuster für fortgeschrittene mechatronische Systeme nach Anacker	○	○	○	●	●	●	○	●	○
	Musterbasierter Entwurf	Musterbasierter Entwurf der s.o. Informationsverarbeitung nach Dumitrescu	○	○	○	◐	○	●	○	●	○
		Lösungsmusterbasiertes Systems Engineering nach Pfister	○	○	○	◐	○	◐	○	○	○
		Identifizierung von Systemarchitekturmustern nach Kalawsky	○	○	○	◐	○	◐	○	○	○
		Lösungsmusterbasierter Entwurf fortgeschrittener mech. Systeme nach Anacker	○	○	○	●	○	●	○	●	○

Bild 3-17: Bewertung des untersuchten Stands der Technik anhand der Anforderungen

A1) Charakterisierung ITS-spezifischer Schutzanforderungen: Anforderungen bilden den Ausgangspunkt des Systementwurfs. Die Identifikation und Berücksichtigung von Anforderungen wird in erster Linie mit Modellierungstechniken (vgl. Kap. 3.3) ermöglicht. Insbesondere die Ansätze zur Systementwicklung nach ANACKER, NEEMANN und KOKOSCHKA berücksichtigen die Anforderungen des Systems. Hierbei handelt es sich jedoch um allgemeine Anforderungen der Systeme. Die Schutzanforderungen Intelligenter Technischer Systeme werden nicht betrachtet.

A2) Bereitstellung passender Schutzmaßnahmen für ITS: In Kapitel 3.1 sind Sammlungen bestehender Schutzmaßnahmen aufgezeigt. Eine Analyse dieser Schutzmaßnahmen soll klären, ob sie für ITS geeignet sind. Hierfür müssen die Schutzmaßnahmen mit den Schutzanforderungen abgeglichen werden. So kann die Wirkung der Schutzmaßnahmen (Grad der Erfüllung der Schutzanforderungen) bestimmt werden. Nur wenige der aufgezeigten Ansätze zur Entwicklung geschützter Systeme berücksichtigen neue Ansätze für den Systemschutz. Meist wird auf vorhandene Maßnahmen verwiesen. Der Ansatz, die Systeme insbesondere mit Hilfe innovativer Schutzmaßnahmen abzusichern, muss intensiver berücksichtigt werden. Daher sind erste innovative Ansätze aufzuzeigen.

A3) Darstellung der Kompetenzen der Imitatoren und der Angriffsmöglichkeiten: Einige der aufgezeigten Ansätze zur Entwicklung geschützter Systeme bestimmen die aktuelle Bedrohungslage. Durch diese werden mögliche Angriffspunkte und Bedrohungen aufgezeigt. LINDEMANN ET AL. klassifizieren die Imitatoren anhand ihrer Kompetenzen. Die Angriffspunkte sowie die Kompetenzen der Imitatoren sind für die Auswahl passender Schutzmaßnahmen von entscheidender Bedeutung. Daher müssen die Identifikation potentieller Bedrohungen sowie insbesondere die Klassifizierung der Imitatoren nach LINDEMANN ET AL. in der angestrebten Systematik berücksichtigt werden.

A4) Interdisziplinarität und Ganzheitlichkeit: Zur Modellierung komplexer technischer Systeme eignet sich in erster Linie CONSENS. Hierdurch kann ein ganzheitlicher Systementwurf auf Basis eines zentralen Systemmodells erfolgen. So wird ein einheitliches Systemverständnis sichergestellt. Für die Darstellung des interdisziplinären Lösungswissens sind Muster geeignet. Insbesondere eignet sich die Strukturierung von Lösungsmustern für den Systementwurf mechatronischer Systeme nach ANACKER.

A5) Modellbasierte Maßnahmenbeschreibung zur Verwendung im Systementwurf: Damit die Möglichkeit geschaffen wird, Schutzmaßnahmen im Systementwurf zu berücksichtigen, ist ihre Darstellung zu adaptieren. Grundlage hierfür sind die Lösungsmuster nach ANACKER. Diese nutzen die modellbasierte Spezifikation mit CONSENS. Die aktuelle textbasierte Darstellung von Schutzmaßnahmen ist grundlegend zu überarbeiten. Mit der modellbasierten Beschreibung durch CONSENS ist die Integration der Schutzmaßnahmen in den Systementwurf möglich.

A6) Wiederverwendung von Lösungswissen: Aufgrund des intensivierten Wissens während der Entwicklung ist für Schutzmaßnahmen die Möglichkeit zu schaffen, bereits

erfolgreich eingesetztes Lösungswissen wiederzuverwenden. Die einheitliche Strukturierung von Lösungsmustern nach ANACKER ist hierfür besonders geeignet. Diese ist allgemeingültig für komplexe technische Systeme und berücksichtigt die Vielzahl involvierter Fachdisziplinen. Der Ansatz ist auf Schutzmaßnahmen zu übertragen.

A7) Frühzeitige und durchgängige Berücksichtigung des Systemschutzes: Alle untersuchten Ansätze zur Entwicklung geschützter Systeme postulieren entweder die frühzeitige oder die ganzheitliche Berücksichtigung von Aspekten des Systemschutzes. Vollumfänglich kann diese Anforderung jedoch von keinem Ansatz erfüllt werden, da insbesondere die fortlaufende Berücksichtigung des Schutzes während der Entwicklung oft vernachlässigt wird.

A8) Integration in etablierte Standards des Systementwurfs: Diese Anforderung wird gleich von mehreren Ansätzen voll erfüllt. Für den Systementwurf Intelligenter Technischer Systeme eignen sich insbesondere modellbasierte Entwurfsansätze. Zur Steigerung der Effizienz müssen diese zusätzlich die Wiederverwendung von Lösungswissen ermöglichen. Diese Kombination wird vollumfänglich durch das Vorgehensmodell für den lösungsmusterbasierten Entwurf fortgeschrittener mechatronischer Systeme nach ANACKER erfüllt.

A9) Präventiver Schutz auf Basis technischer Maßnahmen: Insbesondere das Schutzkonzept für Investitionsgüter (PROTACTIVE) sowie der Ansatz von KOKOSCHKA erfüllen diese Anforderung in vollem Umfang. Durch diese Ansätze wird der präventive Schutz durch technische Maßnahmen ermöglicht. Die erzielten Ergebnisse sind aufzugreifen und für die Entwicklung der Entwurfssystematik zu berücksichtigen.

Keiner der untersuchten Ansätze und auch keine Kombination bestehender Ansätze erfüllt alle Anforderungen in vollem Umfang. Eine bedeutende Schwäche ist die unzureichende Charakterisierung der Schutzanforderungen sowie Schutzmaßnahmen Intelligenter Technischer Systeme. Speziell für ITS wirksame Schutzmaßnahmen werden nur unzureichend bereitgestellt. Darüber hinaus fehlt es an einer geeigneten Darstellungsweise der Schutzmaßnahmen. Mit dieser soll sowohl die Interdisziplinarität als auch die Wiederverwendung von Lösungswissen berücksichtigt werden. Die Ansätze zum interdisziplinären Entwurf unter Berücksichtigung von Lösungswissen sind mit Vorgehen für den imitationsgeschützten Entwurf zu vereinen. Es besteht demnach dringender Handlungsbedarf für eine *Entwurfssystematik für den präventiven Schutz Intelligenter Technischer Systeme vor Produktpiraterie.*

4 Entwurfssystematik für den präventiven Schutz Intelligenter Technischer Systeme

In diesem Kapitel wird die *Entwurfssystematik für den präventiven Schutz Intelligenter Technischer Systeme vor Produktpiraterie* vorgestellt. In Kapitel 4.1 wird ein Überblick über die Systematik und deren wesentliche Bestandteile gegeben.

4.1 Überblick über die Systematik

ITS beruhen auf einer Symbiose von Ingenieurswissenschaften, Informatik sowie fachfremden Disziplinen. Aus dieser Symbiose ergeben sich Möglichkeiten für neue Funktionen. Mit diesen Funktionen kann z. B. das Bedienerlebnis für den Nutzer gesteigert werden. Allerdings entstehen durch die Vernetzung der Systeme neue Angriffsmöglichkeiten, um an das systeminhärente Know-how zu gelangen. Den daraus resultierenden Herausforderungen an den Schutz dieser Systeme kann mit Hilfe der entwickelten Systematik begegnet werden. Diese umfasst vier Bestandteile (Bild 4-1):

- Als Grundlage dient die umfangreiche Betrachtung der **Schutzanforderungen Intelligenter Technischer Systeme**. Ausgehend von den Erkenntnissen der Problemanalyse werden allgemeine Anforderungen an den Systemschutz identifiziert. Diese dienen der Schaffung eines grundlegenden Verständnisses für die Bedarfe der Industrie beim Thema Systemschutz. Zusätzlich werden die ITS-spezifischen Schutzanforderungen herausgearbeitet. Diese bilden die Basis der angestrebten Systematik. Durch die Identifikation dieser Anforderungen werden die neuen Herausforderungen beim Schutz Intelligenter Technischer Systeme verdeutlicht.
- Aufbauend auf den ermittelten Schutzanforderungen folgt die Identifikation **wirksamer Schutzmaßnahmen**. Bestehende Schutzmaßnahmen sowie neue Ansätze zur Verbesserung des Schutzes werden mit den Schutzanforderungen abgeglichen. So können die wirksamsten Maßnahmen für den Schutz Intelligenter Technischer Systeme herausgearbeitet werden. Diese bilden den ersten Grundpfeiler für den präventiven Schutz Intelligenter Technischer Systeme.
- Die **Darstellung von Schutzmaßnahmen** bildet den zweiten Grundpfeiler der Systematik. Hier dient die Strukturierung der Lösungsmuster nach ANACKER (vgl. Kap. 3.4.3) als Basis. Die Strukturierung wird um spezifische Gesichtspunkte ergänzt und angepasst. Darauf aufbauend erfolgt die Überarbeitung der Darstellung der Schutzmaßnahmen. Diese werden von textbasierten Steckbriefen in die modellbasierte Repräsentation als Lösungsmuster übertragen. Für die Spezifikation der Schutzmaßnahmen wird CONSENS (vgl. Kap. 3.3.1) verwendet.
- Das Vorgehensmodell zur **Integration des präventiven Schutzes in den musterbasierten Entwurf Intelligenter Technischer Systeme** bildet den dritten Grund-

pfeiler und den Kern der vorliegenden Arbeit. Anhand des strukturierten Vorgehens wird die Integration des Schutzes in den Systementwurf sichergestellt. Insbesondere die Prinziplösung eines Systems im Sinne der VDI 2206 steht als Ergebnis der Konzipierung bzw. des Systementwurfs im Fokus. Ziel ist die Integration der Aspekte des Systemschutzes in den Entwurf, also die frühzeitige, abstrakte und fachdisziplinübergreifende Spezifikation des Systems. Als Grundlage für den Entwurf Intelligenter Technischer Systeme dient der bestehende lösungsmusterbasierte Systementwurf nach ANACKER (vgl. Kap. 3.4.4). Dieser wird angepasst und um die Aspekte des Systemschutzes ergänzt, damit die gestellten Anforderungen erfüllt werden. Die erarbeiteten Bestandteile ergeben in Kombination eine Systematik für den Entwurf präventiv geschützter Intelligenter Technischer Systeme.

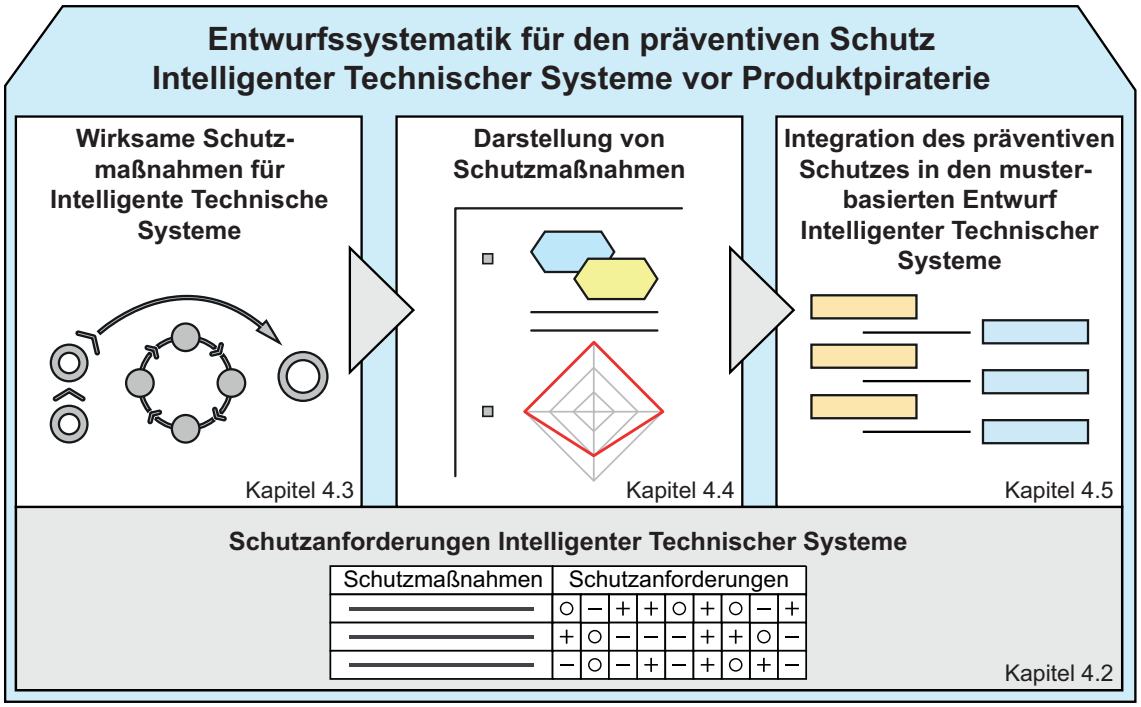


Bild 4-1: Entwurfssystematik für den präventiven Schutz Intelligenter Technischer Systeme vor Produktpiraterie

4.2 Schutzanforderungen Intelligenter Technischer Systeme

Die Anforderungen an den Schutz eines Systems werden als **Schutzanforderungen** bezeichnet (vgl. Kap. 2.1). Diese spiegeln die Bedarfe der Industrie wider und sind darüber hinaus wesentlich für das Verständnis des Schutzes, insbesondere für ITS. Die Schutzanforderungen Intelligenter Technischer Systeme resultieren aus den neuen Herausforderungen beim Systemschutz. Diese Herausforderungen entstehen z. B. durch die steigende Anzahl an Schnittstellen oder aufgrund der Vernetzung der Systeme. Diese bieten den potentiellen Angreifern eine Vielzahl an Angriffsmöglichkeiten. So ist es z. B. mit Cyberattacken möglich, das Know-how der Systeme zu entwenden, ohne physischen Kontakt zum System herzustellen (vgl. Kap. 2.3.3).

Zur Aufnahme der Schutzanforderungen müssen Unternehmen befragt werden, die einen Bezug zu diesen innovativen Systemen besitzen. Hierfür eignen sich insbesondere die 25 Kernunternehmen[35] des Spitzenclusters it‘s OWL. Die Kernunternehmen wurden mit Hilfe eines eigens entwickelten Fragenkatalogs befragt. Aus den gegebenen Antworten können die Herausforderungen an den Systemschutz sowie spezielle Herausforderungen beim Schutz Intelligenter Technischer Systeme abgeleitet werden. Anhand dieser Herausforderungen ist es möglich, Schutzanforderungen abzuleiten. Die detaillierte Beschreibung zur Erhebung der Herausforderungen und Ableitung der Anforderungen ist im Anhang A5 dargestellt. Hier sind ebenfalls der Fragenkatalog sowie die identifizierten Herausforderungen abgebildet. Zusätzlich ist hier eine Übersicht aller Schutzanforderungen aufgelistet.

Insgesamt können aus der Befragung **37 Schutzanforderungen** identifiziert und kategorisiert[36] werden. Davon sind **sechs Schutzanforderungen** speziell für ITS bedeutsam. Diese Schutzanforderungen werden im Folgenden detailliert analysiert.

Vertraulichkeit sensibler Daten: Diese Anforderung an den Schutz Intelligenter Technischer Systeme wurde am häufigsten genannt. Die befragten Unternehmen gaben die Kommunikations- und Netzwerkfähigkeiten der Systeme als Grund an, weshalb dem Schutz für den Datenaustausch eine besondere Bedeutung zugutekommt. Darüber hinaus werden die Daten eines vernetzten Systems in der Cloud gespeichert. Der Schutz dieser Daten muss unter allen Umständen gewährleistet werden. Folgerichtig ist die Vertraulichkeit sensibler Daten sicherzustellen.

Überwachung des Systemverhaltens: Die Schutzanforderung legt die Ausnutzung der Kommunikationseigenschaften der Systeme zugrunde. Wenn ein System angegriffen wird, registriert und meldet es den Angriff automatisch. Durch die Meldung wird der Originalhersteller oder der Systembetreiber über den Angriff informiert und hat die Möglichkeit zu reagieren. Darüber hinaus können weitere vernetzte Systeme vor dem Angriff gewarnt werden.

Eindeutige Authentifizierung: Diese Schutzanforderung zielt auf die charakteristischen Eigenschaften eines intelligenten, vernetzten Systems ab (vgl. Kap. 2.2.2). Wie bei der vorherigen Schutzanforderung bereits beschrieben, können die Eigenschaften der Systeme wie die Kommunikationsfähigkeiten, ausgenutzt werden, um den Systemschutz zu verbessern. Auf Basis der Intelligenz eines Systems lassen sich z. B. Ersatzteile, Komponenten oder neue Softwareversionen identifizieren und eindeutig authentifizieren.

---

[35] Die Kernunternehmen prägen die Entwicklungsstrategie des Spitzenclusters maßgeblich z. B. aufgrund der Bearbeitung von Innovationsprojekten [its12].

[36] Der Fragenkatalog wurde in Anlehnung an die Schutzmaßnahmenkategorien nach KOKOSCHKA (vgl. Kap. 2.3.2) strukturiert. So können die identifizierten Schutzanforderungen zu den Kategorien der Schutzmaßnahmen zugeordnet werden.

Integrität in Netzwerken: Es besteht eine enge Verknüpfung mit der Schutzanforderung Vertraulichkeit sensibler Daten. Die Netzwerkeigenschaften vernetzter Systeme ermöglichen neue Funktionen und erhöhen das Bedienerlebnis signifikant. Jedoch entstehen so auch neue Angriffsmöglichkeiten für Imitatoren. Diese können durch das Abgreifen der Daten an systeminternes Know-how gelangen. Darüber hinaus besteht die Möglichkeit, sich über diese Schnittstelle unerlaubten Zugriff auf die Systeme zu verschaffen. Um die Systeme wirksam zu schützen, ist die Integrität in Netzwerken sicherzustellen.

Generierung einzigartiger kryptographischer Schlüssel und deren sicherer Speicherung: Wie in Kapitel 2.2.3 beschrieben, ist insbesondere der gestiegene Anteil an Software in den Systemen eine Voraussetzung für die Entwicklung mechatronischer Systeme hin zu vernetzten Systemen mit inhärenter Teilintelligenz. Im Maschinen- und Anlagenbau werden aktuell zahlreiche Innovationen mit Hilfe fachfremder Disziplinen wie der Softwaretechnik realisiert. Aus diesen Gründen muss dem Schutz der Software besondere Beachtung geschenkt werden. Durch die Generierung einzigartiger kryptographischer Schlüssel und deren sicherer Speicherung besteht die Möglichkeit, Soft- und Firmware sowie sensible Daten wirksam zu verschlüsseln und somit vor Angriffen zu schützen.

Selbstoptimierung der Schutzmaßnahmen: Die Fähigkeit zur Selbstoptimierung ist keine direkte charakteristische Eigenschaft Intelligenter Technischer Systeme. Selbstoptimierende Systeme nutzen Regel- und Adaptionsstrategien, um das Verhalten des Systems auf sich verändernde Einflüsse und künftige Ereignisse anzupassen. Die autonome Anpassung der Systeme wird durch inhärente Teilintelligenz ermöglicht [ADG+09, S.5]. Anhand der Selbstoptimierung der Schutzmaßnahmen bleiben ITS auch gegen neue, nicht berücksichtigte Angriffe resistent, indem sie unbekannte Angriffe identifizieren (Selbstdiagnose) und abwehren (Selbstheilung) (vgl. [GB12]).

Die identifizierten Schutzanforderungen Intelligenter Technischer Systeme zeigen die neuen Anforderungen sowie die Möglichkeiten für ihren Schutz auf. Insbesondere müssen Aspekte aus der Informationstechnik berücksichtigt werden, um einen wirksamen Schutz zu ermöglichen.

Ein Auszug der identifizierten Schutzanforderungen ist in Tabelle 4-1 abgebildet. Um die identifizierten Schutzanforderungen bereits im Systementwurf zu berücksichtigen, müssen sie im Lastenheft verankert sein. Zur Unterstützung der Entwickler dient die Checkliste für die Schutzanforderungen Intelligenter Technischer Systeme. Diese ist für die Auswahl und Spezifikation der Schutzanforderungen als Vorlage zu verwenden. Die Checkliste fließt als Hilfsmittel in das Vorgehen zur Integration des präventiven Schutzes in den Systementwurf ein (vgl. Kap. 4.5). Die vollständige Checkliste ist im Anhang A5.4 abgebildet.

Tabelle 4-1: Checkliste für die identifizierten Schutzanforderungen (Auszug)

Checkliste Schutzanforderungen			Version Datum
Nr.	**R/I**	**Schutzanforderungskategorie/Schutzanforderung**	**Bearbeiter**
1		**Strategische Schutzanforderungen**	
1.1		Internationale Wirksamkeit	
1.2		Einfache und kostengünstige Umsetzung	
1.3		Überwachbarkeit	
1.4		Anpassbarkeit und Optimierbarkeit im Lebenszyklus	
1.5		Erhalt der Differenzierung	
1.6		Erhalt der Produktivität und Nachhaltigkeit	
1.7		Vereinbarkeit mit dem Wissensmanagement	
2		**Produktbezogene Schutzanforderungen**	
2.1		Minimale Änderung von Kosten und Design	
8		**ITS-spezifische Schutzanforderungen**	
8.1		Vertraulichkeit sensibler Daten	
8.2		Überwachung des Systemverhaltens	
8.3		Eindeutige Authentifizierung	
8.4		Integrität in Netzwerken	
8.5		Einzigartige kryptographische Schlüssel generieren und sicher speichern	
8.6		Selbstoptimierung der Schutzmaßnahmen	

R: Relevant I: Irrelevant

4.3 Wirksame Schutzmaßnahmen für Intelligente Technische Systeme

Die in Kapitel 4.2 identifizierten Schutzanforderungen belegen, dass ITS besondere Kriterien an ihren Schutz stellen. Es werden wirksame Schutzmaßnahmen benötigt, welche die aufgezeigten Schutzanforderungen erfüllen. Um zu analysieren, wie wirksam eine Maßnahme ist, sind die Schutzmaßnahmen mit den Schutzanforderungen gegenüber zu stellen. Anhand der Anforderungserfüllung werden die wirksamsten Schutzmaßnahmen für ITS identifiziert. Um herauszufinden, ob ein Bedarf an neuen Schutzmaßnahmen[37] besteht, werden zunächst die im Stand der Technik behandelten Maßnahmen (vgl. Kap. 3.1) den Schutzanforderungen gegenüber gestellt.

[37] Als neue Schutzmaßnahmen werden Maßnahmen definiert, die in den Veröffentlichungen im Rahmen der Forschungsoffensive „Innovationen gegen Produktpiraterie“ keine Berücksichtigung fanden.

4.3.1 Analyse bekannter Schutzmaßnahmen

In diesem Abschnitt werden die identifizierten Schutzanforderungen mit den bekannten Schutzmaßnahmen aus dem Stand der Technik abgeglichen. Hierbei werden drei Stufen der Anforderungserfüllung unterschieden. Diese charakterisieren die Wirkung der jeweiligen Schutzmaßnahme bei den einzelnen Schutzanforderungen.

- Keine Erfüllung (−): Die Schutzmaßnahme erfüllt die Schutzanforderung nicht.
- Teilweise Erfüllung (○): Die Schutzmaßnahme kann teilweise zur Erfüllung der Schutzanforderung beitragen.
- Erfüllt (+): Die Schutzanforderung erfüllt die Schutzmaßnahme voll.

Mit der Gegenüberstellung können Rückschlüsse auf die Wirksamkeit der Schutzmaßnahmen im Allgemeinen und für den Schutz Intelligenter Technischer Systeme im Besonderen gezogen werden. Die allgemeine Wirksamkeit einer Schutzmaßnahme lässt sich durch die Gegenüberstellung der zur Kategorie der Schutzmaßnahmen zugehörigen Schutzanforderungen ermitteln. So passen z. B. zu den strategischen Schutzmaßnahmen die strategischen Schutzanforderungen. Anhand dieser Gegenüberstellung kann festgestellt werden, welche strategische Schutzmaßnahme die jeweiligen strategischen Schutzanforderungen am besten erfüllt. Ebenso dient die Untersuchung als Basis, um Maßnahmenkombinationen zu finden, die möglichst viele Schutzanforderungen erfüllen. Da für ITS keine Schutzmaßnahmen kategorisiert sind, werden die Schutzanforderungen Intelligenter Technischer Systeme (ITS-spezifisch) mit allen Schutzmaßnahmen abgeglichen. So werden die wirkungsvollsten Maßnahmen für ITS identifiziert.

Schutzmaßnahmen nach GAUSEMEIER ET AL.

Zunächst werden die Schutzmaßnahmen nach GAUSEMEIER ET AL. (vgl. Kap. 3.1.3) untersucht. Die Übersicht der Gegenüberstellung aller Schutzmaßnahmen ist im Anhang A6 dargestellt. In Tabelle 4-2 sind die strategischen sowie die informationstechnischen Schutzmaßnahmen mit den zugehörigen Schutzanforderungen abgebildet. Die Gegenüberstellung zeigt, dass die Schutzmaßnahmen nach GAUSEMEIER ET AL. die zugehörigen Schutzanforderungen der jeweiligen Kategorie überwiegend erfüllen. So sind z. B. die strategischen Schutzmaßnahmen für die Erfüllung der strategischen Schutzanforderungen größtenteils geeignet. Die Schutzmaßnahme *Überwachung des Marktes* erfüllt fast alle strategischen Schutzanforderungen voll. Lediglich die Forderung nach einfacher und kostengünstiger Umsetzung (1.2) kann nur zum Teil erfüllt werden (vgl. Tabelle 4-1). Auch die informationstechnischen Schutzmaßnahmen erfüllen große Teile der zugehörigen Schutzanforderungen. Mit Hilfe *sicherer Kommunikationsverbindungen* lassen sich zwei Drittel der Schutzanforderungen voll erfüllen. Einzig die Forderung nach lückenloser Identifikation von Angriffen (5.3) wird nur zum Teil erfüllt.

Tabelle 4-2: Gegenüberstellung der Schutzmaßnahmen nach GAUSEMEIER ET AL. [GGL12] mit den zugehörigen Schutzanforderungen

Abgleich Schutzmaßnahmen mit Schutzanforderungen																
Schutzanforderungen	strategisch							IT			ITS-spezifisch					
Schutzmaßnahmen	1.1	1.2	1.3	1.4	1.5	1.6	1.7	5.1	5.2	5.3	8.1	8.2	8.3	8.4	8.5	8.6
Strategische Schutzmaßnahmen																
Mitarbeiterbindung verstärken	+	+	−	−	+	+	+				−	−	−	−	−	−
Wissensmanagement einführen	+	○	+	−	+	+	+				−	−	−	−	−	−
Beschränkung von schützenswertem Know-how auf ausgewählte Personen	+	+	○	+	+	○	+				−	−	−	−	−	−
Sensibilisierung der Mitarbeiter für Social Engineering	+	+	−	−	+	+	+				−	−	−	−	−	−
Abteilungsübergreifende Kooperation in puncto Produktschutz	+	+	○	○	+	+	+				−	−	−	−	−	−
Innovationsprozesse optimieren	+	−	+	+	+	+	+				−	−	−	−	−	−
Target Costing	+	○	○	+	−	○	+				−	−	−	−	−	−
Kooperation mit Zulieferern	○	○	○	−	○	+	+				−	−	−	−	−	−
Zuliefererintegration	○	○	○	−	○	+	+				−	−	−	−	−	−
After-Sales-Management/ Hybride Leistungsbündel	+	−	○	+	○	○	+				−	−	−	−	−	−
Release Management	+	○	+	+	○	○	+				−	−	−	−	−	−
Marken- und Produktpreis-differenzierung	+	−	○	+	○	+	+				−	−	−	−	−	−
Selektive Vertriebssysteme	+	−	+	○	+	+	+				−	−	−	−	−	−
Shadow Placement	+	−	○	+	+	○	+				−	−	−	−	−	−
Quersubventionierung von leicht imitierbaren Produkten	−	−	−	+	○	+	+				−	−	−	−	−	−
Überwachung des Marktes	+	○	+	+	+	+	+				−	−	−	−	−	−
Umarmungsstrategie	○	○	○	○	+	+	+				−	−	−	−	−	−
Informationstechnische Schutzmaßnahmen																
Biometrische Zugangskontrolle								−	+	○	−	−	−	−	−	−
Rollenbasierte Zugangskontrolle installieren								−	+	○	−	−	−	−	−	−
Dokumente verschlüsseln								+	−	−	○	−	−	−	○	−
Informationen aus CAD-Modellen entfernen								+	−	−	○	−	−	−	−	−
Sichere Kommunikationsverbindungen								+	+	○	+	−	−	○	○	−
Gegenseitige Authentifizierung von Komponenten								○	−	−	○	○	+	−	○	−
Produktaktivierung								−	−	−	−	−	−	−	−	−
Auslagerung von sicherheitsrelevanten Rechenoperationen								−	○	−	−	−	−	−	○	−
Schutz von eingebetteter Software								+	○	−	+	○	−	−	+	−

Ein ganz anderes Ergebnis zeigt sich jedoch für die ITS-spezifischen Schutzanforderungen. Wie in Tabelle 4-2 visualisiert, erfüllt keine der strategischen Maßnahmen eine ITS-spezifische Schutzanforderung. Ähnlich verhält es sich mit den Schutzmaßnahmen der anderen Kategorien. Auf Basis der Gegenüberstellung wird festgehalten, dass die informationstechnischen Schutzmaßnahmen – von allen Schutzmaßnahmen nach GAUSEMEIER ET AL. – die Schutzanforderungen Intelligenter Technischer Systeme am besten erfüllen. Obwohl die informationstechnischen Schutzmaßnahmen zur Erfüllung der Schutzanforderungen Intelligenter Technischer Systeme am besten geeignet sind, ist die Anforderungserfüllung nicht zufriedenstellend. Lediglich die Schutzmaßnahmen *sichere Kommunikationsverbindungen, gegenseitige Authentifizierung von Komponenten* sowie *Schutz von eingebetteter Software* können wenigstens eine ITS-spezifische Schutzanforderung voll erfüllen (vgl. Tabelle 4-2).

Durch *sichere Kommunikationsverbindungen* kann die ITS-spezifische Schutzanforderung Vertraulichkeit sensibler Daten (8.1) erfüllt werden. Die Schutzanforderungen Integrität in Netzwerken (8.4) sowie die Generierung einzigartiger kryptographischer Schlüssel und deren sichere Speicherung (8.5) können teilweise erfüllt werden. Der Steckbrief der Schutzmaßnahme *sichere Kommunikationsverbindungen* ist im Anhang A1.2 in Bild A-2 gezeigt.

Auf Grundlage der *gegenseitigen Authentifizierung von Komponenten* lässt sich die Forderung nach eindeutiger Authentifizierung (8.3) voll erfüllen. Weiterhin kann die Vertraulichkeit sensibler Daten (8.1) sowie die Generierung einzigartiger kryptographischer Schlüssel und deren sichere Speicherung (8.5) unterstützt werden. Der Steckbrief der Schutzmaßnahme *gegenseitige Authentifizierung von Komponenten* ist im Anhang A1.2 in Bild A-3 gezeigt.

Mit Hilfe des *Schutzes eingebetteter Software* kann die Generierung einzigartiger kryptographischer Schlüssel und deren sichere Speicherung (8.5) voll erfüllt und zusätzlich die Vertraulichkeit sensibler Daten (8.1) unterstützt werden. Der Steckbrief dieser Schutzmaßnahme ist im Anhang A1.2 in Bild A-4 gezeigt.

Insgesamt kann festgehalten werden, dass keine der untersuchten Schutzmaßnahmen nach GAUSEMEIER ET AL. die Schutzanforderungen Intelligenter Technischer Systeme ausreichend erfüllt.

Schutzmaßnahmen nach LINDEMANN ET AL.

Zusätzlich werden die Schutzmaßnahmen nach LINDEMANN ET AL. (vgl. Kap. 3.1.2) untersucht. Es ist auffällig, dass es Redundanzen zu den bei GAUSEMEIER ET AL. aufgeführten Schutzmaßnahmen gibt. Der Fokus der Analyse liegt somit auf den technischen Maßnahmen, die bei GAUSEMEIER ET AL. nicht beschrieben sind. Die Gegenüberstellung dieser Schutzmaßnahmen ist in Tabelle 4-3 dargestellt.

Die untersuchten Schutzmaßnahmen nach LINDEMANN ET AL. werden in die Kategorien strategisch, produktbezogen und informationstechnisch unterteilt. Vergleichbar mit den

Schutzmaßnahmen nach GAUSEMEIER ET AL. werden die zugehörigen Schutzanforderungen überwiegend erfüllt. Insbesondere die strategischen Schutzmaßnahmen erfüllen nahezu alle strategischen Schutzanforderungen.

Tabelle 4-3: Gegenüberstellung der Schutzmaßnahmen nach LINDEMANN ET AL. [LMP+12a] mit den zugehörigen Schutzanforderungen

Abgleich Schutzmaßnahmen mit Schutzanforderungen																						
Schutzanforderungen	strategisch							produktbezogen							IT			ITS-spezifisch				
Schutzmaßnahmen	1.1	1.2	1.3	1.4	1.5	1.6	1.7	2.1	2.2	2.3	2.4	2.5	2.6	2.7	5.1	5.2	5.3	8.1	8.2	8.3	8.4	8.5	8.6
Strategische Schutzmaßnahmen																							
"Ein-Haus"-Strategie verfolgen	○	○	+	+	○	−	+											−	−	−	−	−	−
Know-how-Abfluss aus der Produktion unterbinden	+	+	○	○	+	+	○											−	−	−	−	−	−
Produkt-Service Systeme (PSS) anbieten	+	○	○	+	+	+	○											−	−	−	−	−	−
Produktbezogene Schutzmaßnahmen																							
High-Tech-Strategie verfolgen								−	−	+	+	○	○	+				−	−	−	−	−	−
Neue, schützbare Technologien für alte Produkte nutzen								−	○	+	+	−	○	+				−	−	−	−	−	−
Produkte anpassungs- und upgradegerecht gestalten								−	○	+	+	−	+	+				−	−	−	−	−	−
Selbstzerstörende Kernkompetenzbauteile gestalten								−	−	○	+	−	○	○				−	−	−	−	−	−
Informationstechnische Schutzmaßnahmen																							
Struktur der Steuerungssoftware zentralisieren															−	○	○	○	○	−	−	−	−
Zugang zu IT-Systemen schützen															○	○	−	○	○	−	○	−	−

Die ITS-spezifischen Schutzanforderungen werden mit allen Schutzmaßnahmen abgeglichen (vgl. Tabelle 4-3). Hier zeigt sich, dass die informationstechnischen Schutzmaßnahmen die Schutzanforderungen Intelligenter Technischer Systeme am besten erfüllen können. Allerdings erfüllt keine Schutzmaßnahme eine ITS-spezifische Schutzanforderung voll. Die Forderungen nach der Vertraulichkeit sensibler Daten (8.1) und nach der Überwachbarkeit des Systemverhaltens (8.2) können von beiden untersuchten informationstechnischen Schutzmaßnahmen teilweise erfüllt werden. Durch den Schutz der Zugänge zu IT-Systemen wird zusätzlich die Integrität in Netzwerken (8.4) unterstützt.

Die vorangegangene Untersuchung beweist, dass bestehende Schutzmaßnahmen nur unzureichend für den Schutz Intelligenter Technischer Systeme geeignet sind. Die wirksamsten Schutzmaßnahmen beinhaltet die Kategorie informationstechnische Schutzmaßnahmen. Aus dieser stechen lediglich die Schutzmaßnahmen *sichere Kommunikationsverbindungen, gegenseitige Authentifizierung von Komponenten* sowie *Schutz von eingebetteter Software* heraus (vgl. Anhang A1.2).

Die Gegenüberstellung bestehender Schutzmaßnahmen mit den identifizierten Schutzanforderungen zeigt die bestehende Lücke für den Systemschutz auf und unterstreicht den Forschungs- und Handlungsbedarf zur Verbesserung des Schutzes für ITS. Zum effektiven Systemschutz müssen neue Schutzmaßnahmen identifiziert werden. Diese sollten die ITS-spezifischen Schutzanforderungen besser erfüllen, als die bekannten Maßnahmen. Aus diesem Grund befasst sich der nächste Abschnitt mit neuen Ansätzen zur Verbesserung des Schutzes Intelligenter Technischer Systeme.

4.3.2 Neue Ansätze zur Verbesserung des Schutzes Intelligenter Technischer Systeme

ITS stellen besondere Anforderungen an ihren Schutz (vgl. Kap. 4.2). Diese Schutzanforderungen können von bekannten Schutzmaßnahmen nur unzureichend erfüllt werden (vgl. Kap. 4.3.1). Für eine Verbesserung des Systemschutzes sind im ersten Schritt innovative Ansätze zu identifizieren. Diese müssen daraufhin analysiert und mit den Schutzanforderungen abgeglichen werden. Hierfür sind zunächst Technologien[38] zur Realisierung des Systemschutzes zu analysieren.

Die Technologien können anhand einer Literaturrecherche identifiziert werden. Eine exemplarische Quelle ist der „Gartner Hype Cycle for Emerging Technologies 2015“. Dieser enthält eine repräsentative Gruppe von noch reifenden Technologien, die zum Systemschutz beitragen könnten [Gar15-ol]. Zur Visualisierung der identifizierten Technologien ist eine sog. Technologie-Roadmap erarbeitet worden. Diese bildet eine grafische Repräsentation von Technologien und ihren Verknüpfungen über die Zeit ab [MI08, S.3]. Die Technologie-Roadmap ist in Bild 4-2 dargestellt.

In der Roadmap sind auf der linken Seite die Kategorien der **Technologien** sowie deren Ausprägungen dargestellt. Darunter sind die **ITS-spezifischen Schutzanforderungen** aufgelistet. Die vertikalen Balken repräsentieren ausgewählte **Veröffentlichungen**. Balken visualisieren die **Entwicklungsphase** der Technologien in Bezug auf die Marktreife. Ein weißer Balken bedeutet, dass die Technologie noch nicht entwickelt ist. Je mehr sich der Balken verfärbt, desto weiter ist die Entwicklung fortgeschritten. Ein farblich gesättigter Balken steht für eine marktreife Technologie. Die Veröffentlichungen werden den Technologien zugeordnet. Die Zuordnung wird mittels schwarzer Punkte visualisiert. Ferner werden so die Schutzanforderungen mit den Veröffentlichungen verlinkt. Hierdurch kann direkt überblickt werden, welche Technologien zur Anforderungserfüllung beitragen.

---

[38] SCHUH ET AL. definieren auf Grundlage der Arbeiten von BINDER und KANTOWSKY Technologie als: *„[…] Wissen, Kenntnisse und Fertigkeiten zur Lösung technischer Probleme sowie Anlagen und Verfahren zur praktischen Umsetzung naturwissenschaftlicher Erkenntnisse“ [SKS+11, S.34] basierend auf [BK96].*

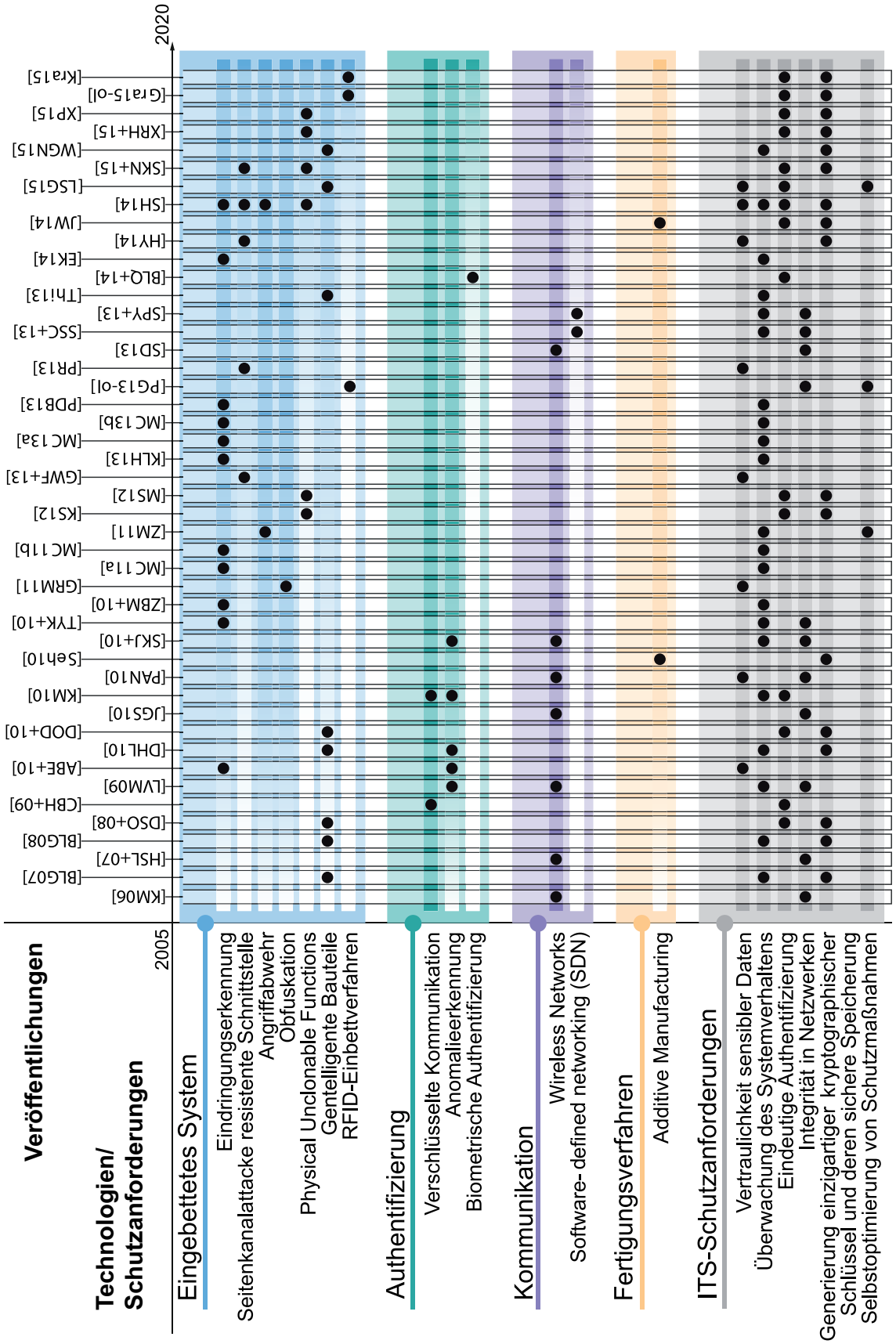


Bild 4-2: Technologie-Roadmap zur Identifikation neuer Schutzansätze

Insbesondere für **eingebettete Systeme** konnte eine Vielzahl an Veröffentlichungen ermittelt werden. Zahlreiche Publikationen befassen sich mit individuellen technologischen Ausprägungen wie Eindringungserkennung, Angriffsabwehr oder Obfuskation (Verschleierung). Vereinzelt werden auch kategorieübergreifende Ansätze vorgestellt.

ASFAW ET AL. beschreiben eine Möglichkeit zur Eindringungserkennung in eingebetteten medizinischen Systemen. Diese basiert auf der Identifikation von Anomalien im Systemverhalten. Für diese wird eine entsprechende Authentifizierungstechnologie benötigt [ABE+10].

Häufig bieten Ansätze zur Einbettung von Systemen die Möglichkeit, bestehende Maßnahmen weiterzuentwickeln. So können z. B. mit einem Einbettverfahren RFID-Module in Leiterplatten eingebettet werden. Der integrierte RFID-Chip enthält eine weltweit eindeutige Identität und kann ohne Sichtverbindung ausgelesen oder auch mit Daten beschrieben werden. Somit wird die Sicherheit der Kennzeichnung erhöht, da der RFID-Chip nicht entfernt werden kann, ohne die Leiterplatte zu zerstören und damit die Daten unbrauchbar zu machen [PG13-ol], [Gra15-ol], [Kra15].

Eine große Anzahl der Technologien eingebetteter Systeme werden von SCHIMMEL und HENNIG angesprochen. Sie beschreiben **Ansätze zum Kopier- und Manipulationsschutz eingebetteter Systeme** [SH14]. Diese weisen Potential zum Schutz Intelligenter Technischer Systeme auf, da sie vier Schutzanforderungen zugeordnet werden können. Die Technologien zum Schutz eingebetteter Systeme stellen den ersten Ansatz zur Verbesserung des Systemschutzes dar. Sie werden in Kapitel 4.3.2.1 detailliert untersucht.

Als Fertigungstechnologie zur Herstellung Intelligenter Technischer Systeme hat das **Additive Manufacturing** hohes Potential, den Systemschutz zu verbessern. Aus dieser Technologie ergeben sich neue Schutzmaßnahmen und zusätzlich können bestehende Maßnahmen erweitert bzw. verbessert werden. JAHNKE und WIGGE beschreiben das Potential additiver Fertigungsverfahren, Systeme präventiv gegen Produktpiraterie zu schützen [JW14]. Additive Fertigungsverfahren stellen den zweiten innovativen Ansatz zum Schutz Intelligenter Technischer Systeme dar. Das Kapitel 4.3.2.2 beschreibt die Technologie detailliert und untersucht die resultierenden Schutzmaßnahmen.

Ein dritter Ansatz mit Potential zur Weiterentwicklung des Systemschutzes sind sog. **gentelligente Bauteile**. Diese ermöglichen die Verschmelzung eines Bauteils mit zugehörigen Informationen. Ferner werden inhärente Funktionen, die bislang nur mit Sensoren realisiert werden konnten, verwirklicht. Somit sind gentelligente Bauteile in der Lage ihren Zustand selbst zu überwachen und Daten inhärent und dadurch sicher zu speichern. Dementsprechend können gentelligente Bauteile im weitesten Sinne als eingebettete Systeme definiert werden. Sie können insgesamt mehreren ITS-spezifischen Schutzanforderungen zugeordnet werden und weisen daher großes Potential zur Verbesserung des Schutzes Intelligenter Technischer Systeme auf. In Kapitel 4.3.2.3 werden sie analysiert. Die Ansätze zur Authentifizierung werden hauptsächlich in Verbindung mit Schutzmaßnahmen auf Basis gentelligenter Bauteile untersucht (vgl. Kap. 4.3.2.3).

Bei den Kommunikationstechnologien hat der Ansatz **Software-defined networking** großes Potential zum Aufbau sicherer Netzwerke. Daher wird dieser Ansatz zur Vernetzung von Intelligenten Technischen Systemen aufgegriffen und in Kapitel 4.3.2.4 vorgestellt.

Die innovativen Ansätze zur Verbesserung des Systemschutzes zeichnen sich u. a. durch die Verbindung mehrerer Technologien sowie eine Vielzahl an zugeordneten Schutzanforderungen aus. Die einzelnen Ansätze sowie daraus resultierende neue Schutzmaßnahmen werden im Folgenden beschrieben.

4.3.2.1 Ansätze zum Kopier- und Manipulationsschutz eingebetteter Systeme

Auf Basis der Kooperation mit dem Fraunhofer-Institut für Angewandte und Integrierte Sicherheit (AISEC) konnten neue informationstechnische Schutzmaßnahmen identifiziert und analysiert werden.

Protecting Electronic Products: Diese Schutzmaßnahme ermöglicht einen physikalischen Hardwareschutz. Hierfür wird eine Schutzfolie über die Leiterplatinen gezogen. Diese Schutzmaßnahme wird nach der Auflistung der Maßnahmen detailliert beschrieben und in Kapitel 4.4.3 in Bild 4-7 mit Hilfe eines modellbasierten Steckbriefs dargestellt.

Seitenkanalresistente Hardware Designs: Die Hardware wird so ausgelegt, dass sie vor Seitenkanalangriffen[39] geschützt ist.

Seitenkanalresistente Programmierung: Bei dieser Maßnahme wird die Soft- und Firmware so programmiert, dass sie vor Seitenkanalangriffen sicher ist. Dies gelingt z. B. durch die Verwendung von programmierbaren logischen Schaltungen (FPGAs). Diese erschweren das Auslesen von Informationen über Seitenkanäle [FS11, S.33ff.].

Obfuskation zum Schutz vor Reverse-Engineering: Hier wird der Quellcode eines Programms so abgeändert, dass er sehr schwer verständlich ist [FS11, S.31].

Secure Firmware: Zum Schutz vor Reverse-Engineering und IP-Diebstahl wird der Code der Firmware verschlüsselt. Mit einer spezifischen Schnittstelle – der secure-In-System-Programming-Schnittstelle (sISP)[40] – kann die verschlüsselte Firmware nicht ausgelesen werden [SH14].

---

[39] Mit Seitenkanalangriffen lassen sich z. B. durch Beobachtung des Stromverbrauchs, des zeitlichen Verhaltens oder der elektromagnetischen Abstrahlung Rückschlüsse auf chip-interne Geheimnisse ziehen [MS12].

[40] Eine sISP ist so konzipiert, dass die Bereiche des Flashspeichers, auf denen sich der Bootloader befindet, nicht erreichbar sind. Nach einer erfolgreichen Authentifizierung können bestimmte Speicherbereiche beschrieben, jedoch nicht ausgelesen werden. Auf diese Weise wird die Software optimal geschützt [SH14].

Secure Firmware Update: Diese Schutzmaßnahme verschlüsselt die Firmware während der Distribution über unsichere Kanäle.

Verified Boot: Diese Maßnahme gewährleistet, dass nur originale Firmware ausgeführt wird. Durch ein Zusammenspiel aus Soft- und Hardware wird die Firmware erst dann entschlüsselt und in den Arbeitsspeicher geladen, wenn die Originalität der Hardware nachgewiesen wurde.

Hardware Binding: Hierdurch wird sichergestellt, dass die Firmware nur auf originaler Hardware ausgeführt wird. Zur Verhinderung einer Analyse des Systems werden Sicherheitsabfragen in die Software integriert. So wird die Bindung der Software an die Hardware sichergestellt. Die Erzeugung einer Systemkopie wird erschwert [SH14].

Secure Memory Device: Diese Speicher ermöglichen die sichere Datenhaltung. Sie funktionieren ähnlich wie ein kryptographischer Dongle. Da Secure Memory Devices nicht an einer externen Schnittstelle angeschlossen, sondern im Hardwaredesign als Baustein mit integriert werden, bieten diese Bausteine nützliche kryptographische Grundfunktionen, die zur Absicherung des Gesamtsystems dienen [FS11, S.33].

Beispielhaft für die Maßnahmen des Fraunhofer AISEC wird die Schutzmaßnahme *Protecting Electronic Products* beschrieben (vgl. Kap. 4.4.3, Bild 4-7). Diese wurde speziell für den Schutz eingebetteter Systeme entwickelt und bietet somit großes Potential für die Anwendung bei Intelligenten Technischen Systemen (vgl. Kap. 2.2.3, 4.3.1).

Eingebettete Systeme sind aufgrund ihrer anwendungsspezifischen Optimierung anfällig für Produktpiraterie. Oftmals kann das Produkt ohne großen Aufwand nachgeahmt oder als exakte Kopie nachgebaut werden. Mittels Reverse Engineering wird ein Imitator das System Stück für Stück in seine Einzelteile zerlegen. Die verwendeten Bauteile werden identifiziert, daraufhin das System analysiert und mit gleichen oder äquivalenten Bauteilen nachgebaut. Die benötigte Firmware kann aus dem Original ausgelesen und in den Nachbau eingespielt werden. Erst durch sie wird das Produkt individualisiert und zum Leben erweckt. Die Firmware ist demnach das eigentliche Herzstück des Systems. Zusätzlich beinhaltet sie in der Regel den Großteil des Know-hows. Folgerichtig muss der Schutz der Firmware im Vordergrund stehen [AIS15-ol], [SH14].

Für den Schutz eingebetteter Systeme und insbesondere deren Firmware wird mit der Schutzmaßnahme *Protecting Electronic Products* ein Kopier- und Manipulationsschutz für Soft- und Hardwarekomponenten realisiert. Die Maßnahme vereint unterschiedliche Schutzmaßnahmen und Technologien im Themenfeld eingebetteter Systeme. Auf dieser Grundlage trägt sie zur Erfüllung mehrerer ITS-spezifischer Schutzanforderungen bei.

Zur Realisierung des Hardwareschutzes wird eine spezielle Folie zum Schutz von elektronischen Bauteilen über die Leiterplatinen des Systems gezogen. Diese Schutzmaß-

nahme wird als *Shielding*[41] bezeichnet. Wird die Folie geöffnet oder beschädigt, löscht das System die sensiblen Daten. Dies kann als eine Art Selbstzerstörungsmechanismus betrachtet werden. In Kombination mit sog. PUFs[42] wird der Systemschutz in allen Betriebsmodi (Aus/Boot/An) sichergestellt. Im ausgeschalteten Zustand sind die sensiblen Daten verschlüsselt. Der Schlüssel wird durch fertigungstoleranzbedingte Eigenschaften der Folie generiert. Ohne den Schlüssel sind die Daten nutzlos. Erst durch den Start des Systems werden die Daten entschlüsselt. Die Schutzfolie verschließt als elektronisches Siegel die Gehäuse elektronischer Geräte manipulationssicher und deaktiviert die Funktionalität bei Siegelbruch. Die Schnittstelle sISP ist die einzige Verbindung der Komponenten, die sich unterhalb der Folie befinden. Somit kann der Schutz während des Bootens sichergestellt werden, da die Speicherbereiche zur Ver- und Entschlüsselung nicht erreichbar sind. Mit der Kombination der einzelnen Maßnahmen bietet die Schutzmaßnahme *Protecting Electronic Products* Kopier- und Manipulationsresistenz für eingebettete Systeme. Ferner wird die Detektion und Reaktion auf Angriffe ermöglicht [AIS15-ol], [Sh14].

Die Bewertung der Schutzmaßnahmen wurde in Zusammenarbeit mit dem Fraunhofer AISEC durchgeführt. Die Maßnahmen werden mit den informationstechnischen und den ITS-spezifischen Schutzanforderungen abgeglichen. Das Ergebnis der Bewertung ist in Tabelle 4-4 gezeigt.

Die beschriebene Schutzmaßnahme ist in der obersten Zeile dargestellt. Sie ist die wirksamste der dargestellten Schutzmaßnahmen zum Kopier- und Manipulationsschutz eingebetteter Systeme, da sie vier der ITS-spezifischen Schutzanforderungen voll erfüllt. Dazu gehören Vertraulichkeit sensibler Daten (8.1), Überwachbarkeit des Systemverhaltens (8.2), eindeutige Authentifizierung (8.3) sowie die Generierung einzigartiger kryptographischer Schlüssel und deren sichere Speicherung (8.5). Insbesondere die Forderung nach Integrität in Netzwerken (8.4) wird von der Maßnahme nicht erfüllt. Ebenso wird eine selbstständige Optimierung der Schutzmaßnahme (8.6), z. B. anhand erlernter Erfahrungen von vorangegangenen Angriffen, aktuell nicht berücksichtigt.

---

[41] Beim Shielding wird ein Schutzgitter aus Leiterbahnen über einen Chip oder eine Leiterkarte aufgespannt, um Manipulationsversuche zu detektieren. Durch einen unter dem Gitter liegenden Sensor wird ein Durchtrennen des Netzes erkannt. Dann wird ein Löschvorgang ausgelöst, der die auf dem Chip laufende Firm- oder Software entfernt. Die Schutzmaßnahme ist jedoch nur im eingeschalteten Zustand wirksam, da die Auswerteelektronik nur reagiert, wenn sich das System im Betrieb befindet [SH14].

[42] Physical Unclonable Functions (PUFs) basieren auf unkontrollierbaren und nicht reproduzierbaren Fertigungstoleranzen. Das Prinzip basiert auf der Erzeugung von Challenge/Response-Paaren. Durch die Anregung (Challenge) reagieren die PUFs mit einem analogen oder digitalen Signal (Response). Dieses sieht zufällig aus, ist aber reproduzierbar. So wird ein kryptographischer Schlüssel oder eine Identifikationsnummer abgeleitet. So wird eine Lösung für sichere Haltung der Identifikationsmerkmale realisiert, da der Schlüssel nicht abgespeichert werden muss, sondern aus den einzigartigen Toleranzen des Produktes reproduziert wird [KS12], [Mer14], [SH14].

Tabelle 4-4: Gegenüberstellung der Maßnahmen zum Kopier- und Manipulationsschutz eingebetteter Systeme mit den zugehörigen Schutzanforderungen

Abgleich Schutzmaßnahmen mit Schutzanforderungen									
Schutzanforderungen	IT			ITS-spezifisch					
Schutzmaßnahmen	5.1	5.2	5.3	8.1	8.2	8.3	8.4	8.5	8.6
Informationstechnische Schutzmaßnahmen									
Protecting Electronic Products	−	+	+	+	+	+	−	+	−
Seitenkanalresistente Hardware Designs	−	+	○	○	−	−	−	−	−
Seitenkanalresistente Programmierung	○	○	−	○	−	−	−	−	−
Obfuskation zum Schutz vor Reverse-Engineering	−	○	−	○	−	−	−	−	−
Secure Firmware	−	+	○	+	−	−	○	−	−
Secure Firmware Update	−	+	○	+	−	−	○	−	−
Verified Boot	−	+	−	−	−	○	−	−	−
Hardware Binding	−	+	○	−	−	○	−	−	−
Secure Memory Device	−	+	−	+	−	−	−	○	−

Insgesamt können ebenso die Schutzmaßnahmen des Fraunhofer AISEC zum Kopier- und Manipulationsschutz eingebetteter Systeme die Schutzanforderungen Intelligenter Technischer Systeme nur partiell erfüllen. Hervorzuheben ist die Schutzmaßnahme *Protecting Electronic Products*. Sie erfüllt eine Vielzahl der informationstechnischen, als auch der ITS-spezifischen Schutzanforderungen und sollte daher für den Schutz Intelligenter Technischer Systeme berücksichtigt werden.

4.3.2.2 Direct Manufacturing als Technologie zum Systemschutz

Additive Manufacturing (AM) bezeichnet Verfahren zur schichtweisen Herstellung von Bauteilen ohne formgebendes Werkzeug [ZA13]. Das direkte Fertigen von Endprodukten mittels dieser Verfahren wird als Direct Manufacturing bezeichnet. Grundsätzlich wird bei additiven Fertigungsverfahren ein dreidimensionales Fertigungsproblem in Schichten zerlegt. Hierdurch kann die gewünschte Geometrie Schicht für Schicht hergestellt werden. Die Bauteilherstellung basiert auf einer Zugabe von Material – im Gegensatz zu abtragenden Verfahren z. B. dem Fräsen. So wird mit Hilfe dieser Fertigungstechnologien die Herstellung von Bauteilen ermöglicht, die mit konventionellen Fertigungsverfahren nicht ohne Weiteres herstellbar wären. Ferner besteht die Möglichkeit, individuelle Bauteile mit nur einer Anlage zu fertigen, ohne Beeinflussung des Fertigungsprozesses durch die Bauteilkomplexität. Im Vergleich mit konventionellen Fertigungsverfahren ergibt sich somit ab einer gewissen Komplexität und in Abhängigkeit zur Stückzahl sowie Bauteilgröße eine höhere Wirtschaftlichkeit. Anwendungsbeispiele für Direct Manufacturing sind hochfeste, komplexe, aber dennoch sehr leichte Bauteile. Diese werden u. a. in der Luftfahrt, für individuell geformten Zahnersatz sowie Spritz-

gusswerkzeuge mit integrierten Kühlkanälen eingesetzt [GEK11], [GLG08]. Weitere Ausführungen zur Unterscheidung additiver Verfahren sind im Anhang A7 beschrieben.

Schutzmaßnahmen basierend auf AM bieten Potential für den wirksamen Schutz von ITS. Die Ausnutzung innovativer Fertigungsverfahren wird bereits bei GAUSEMEIER ET AL. angesprochen (vgl. [BK12a]). Jedoch wird hier das Direct Manufacturing per se als Beispiel der Schutzmaßnahme innovative Fertigungsverfahren genannt.

Vergleicht man additive und herkömmliche (subtraktive) Herstellungsverfahren können drei Potentiale abgeleitet und als elementare Potentiale für den Schutz definiert werden.

Herstellung ohne Werkzeug: Wirtschaftliche Vorteile ergeben sich für kleine Losgrößen.

Geometrische Gestaltungsfreiheit: Schichtweiser Prozess von 1D über 2D zu 3D ermöglicht die Herstellung hochkomplexer Geometrien.

Freiheit der mechanischen Eigenschaften: Schichtweiser Prozess ermöglicht die lokale und heterogene Einstellung von mechanischen Eigenschaften.

Unter Berücksichtigung dieser elementaren Potentiale wurden Schutzmaßnahmen entwickelt. Einige sind innovative Maßnahmen während andere Weiterentwicklungen von bereits bestehenden Schutzmaßnahmen sind. Im Folgenden werden die entwickelten Schutzmaßnahmen auf Basis additiver Fertigung vorgestellt und beschrieben.

Lokale Änderung der Dichte: Mit AM können bis zu drei verschiedene Materialstrukturen innerhalb eines Produktes realisiert werden. Diese sind festes Material, Tragstrukturen und loses Pulver bzw. Hohlräume. Auf Grundlage der Variation dieser Materialstrukturen kann die Dichteverteilung einer Komponente sehr leicht beeinflusst werden.

Individuelle und lokale Anpassung des Materials: Bei pulverbasierten Verfahren (wie dem LS-Verfahren) ist es möglich, unterschiedlich poröse Strukturen zu schaffen (funktionale Porosität). Hierdurch können die mechanischen Eigenschaften individuell und lokal angepasst werden. Darüber hinaus ist es möglich, die Mikrostruktur anzupassen, indem materialspezifische Prozessparameter variiert werden [Seh10, S.105ff.]

Freiform Design: Basierend auf dem Potential der geometrischen Gestaltungsfreiheit ermöglicht diese Maßnahme nahezu unbegrenzte Möglichkeiten beim Design. So können z. B. Freiformflächen hergestellt werden, die konventionell nur unwirtschaftlich oder gar nicht herstellbar sind.

Innere Strukturen: Anhand von inneren Strukturen sind innerhalb der Bauteile nahezu unbegrenzte Möglichkeiten des Designs realisierbar. Einschränkungen entstehen lediglich durch überschüssiges Material oder Trägermaterial, das nach der Herstellung entfernt werden muss.

Ausreizen der technologischen Grenzen von AM: Additive Fertigung wird oft als benutzbar für jedermann beschrieben. Nähert man sich den technologischen Grenzen,

entstehen zahlreiche Potentiale, um ein Produkt zu schützen. Hierfür ist ein umfassendes Wissen über den Herstellungsprozess erforderlich.

Individuelle Anpassung: AM erfordert keine spezielle Ausrüstung oder Werkzeuge, um Produktvarianten oder maßgeschneiderte Produkte herzustellen. Daher können Produkte z. B. einzeln markiert oder individuell, den jeweiligen Kundenanforderungen entsprechend, entwickelt und gefertigt werden. So bleiben die Produktionskosten stabil.

Diese Schutzmaßnahmen können weiter untergliedert werden. So kann eine Ausprägung der Schutzmaßnahme *Freiform Design* z. B. die Funktionsintegration sein. Mit Hilfe additiver Fertigung wird die Integration verschiedener Funktionen in eine Komponente bzw. einen Arbeitsschritt ermöglicht. Bei konventionellen Verfahren werden diese Funktionen von mehreren Bauteilen in einer Baugruppe erfüllt. Durch die Funktionsintegration erhöht sich die Komplexität einzelner Komponenten. Hierdurch wird das Reverse Engineering erschwert, da die Geometrie sowie die mechanischen Eigenschaften einer physikalischen Komponente schwerer nachvollziehbar sind [JW14].

Additive Schutzmaßnahmen stellen oft nur einen Teil einer übergeordneten Schutzmaßnahe dar. So ist z. B. für eine Originalitätsüberprüfung die Kombination aus additiver Fertigung, geeigneter Identifikationsverfahren und informationstechnischer Auswertung notwendig. ITS vereinen die aufgezählten Technologien miteinander und bieten so die Möglichkeit, einen präventiven Schutz basierend auf AM umzusetzen. Um festzustellen, inwieweit sich dieser Schutz für ITS wirksam ist, wird die Wirkung der Schutzmaßnahmen überprüft. Das Ergebnis ist in Tabelle 4-5 dargestellt.

Tabelle 4-5: Gegenüberstellung der Schutzmaßnahmen basierend auf Additive Manufacturing mit den zugehörigen Schutzanforderungen

Abgleich Schutzmaßnahmen mit Schutzanforderungen													
Schutzanforderungen	produktbezogen							ITS-spezifisch					
Schutzmaßnahmen	2.1	2.2	2.3	2.4	2.5	2.6	2.7	8.1	8.2	8.3	8.4	8.5	8.6
Produktbezogene Schutzmaßnahmen													
Lokale Änderung der Dichte	○	−	○	+	−	+	+	○	○	+	−	+	−
Individuelle und lokale Anpassung des Materials	○	−	○	+	−	+	+	○	○	+	−	+	−
Freiform Design	○	−	○	+	−	+	+	−	−	○	−	○	−
Innere Strukturen	○	−	○	+	−	+	+	○	○	+	−	○	−
Ausreizen der technologischen Grenzen von AM	−	−	○	+	−	+	○	−	−	○	−	−	−
Individuelle Anpassung	−	−	+	+	−	+	○	−	−	+	−	○	−

Die abstrakten Schutzmaßnahmen basierend auf AM erfüllen die meisten der produktbezogenen und zudem einige der ITS-spezifischen Schutzanforderungen. Durch *innere Strukturen* sowie *individueller Anpassung* lassen sich Bauteile eindeutig authentifizie-

ren (8.3). Dies ist möglich, da die Bauteile individuell und einzigartig erzeugt werden. Hierdurch wird die Identifikation sichergestellt, z. B. kann mit hinterlegten Fertigungsmerkmalen das Bauteil eindeutig authentifiziert werden.

Hervorzuheben sind die Schutzmaßnahmen, welche sich mit den Materialeigenschaften befassen. Anhand der *lokalen Änderung der Dichte* oder der *individuellen und lokalen Anpassung des Materials* lassen sich bauteilinhärente Kennzeichnungen realisieren. So kann z. B. ein QR-Code durch die lokale Dichteänderung erzeugt werden. Dieser ist direkt im Bauteil integriert und kann die Forderungen nach eindeutiger Authentifizierung (8.3) sowie nach Generierung einzigartiger kryptographischer Schlüssel und deren sicherer Speicherung (8.5) erfüllen.

4.3.2.3 Gentelligente Bauteile zur Verbesserung des Systemschutzes

In der Natur sind Lebewesen nur dann existenzfähig, wenn sie mit der Umwelt interagieren und auf externe Einflüsse reagieren können. Damit sie äußere Einflüsse wahrnehmen können, besitzen Lebewesen biologische Strukturen, sog. Rezeptoren. Die Wahrnehmung besteht aus zwei Teilprozessen. Zunächst wird der äußere Einfluss vom Rezeptor aufgenommen. Das aufgenommene Signal wird anschließend zum Zentralnervensystem – dem Gehirn und Rückenmark – weitergeleitet. Hier entsteht der Sinneseindruck, welcher sich als Wahrnehmung oder Empfindung äußert. Technisch können diese Prozesse imitiert werden. Die Rezeptoren werden mit künstlichen **Sensoren** nachgeahmt. Die Sensoren dienen zur Erfassung von Größen und ermöglichen Systemen, eigenständig auf Zustände zu reagieren und ihr Verhalten zu kontrollieren [HS12a, S.1f.].

Der Sonderforschungsbereich 653 „Gentelligente Bauteile im Lebenszyklus“ hat das Ziel, die physikalische Trennung von Bauteil und dazugehörigen Informationen aufzuheben. Hierfür werden nach dem Vorbild der Natur sog. **gentelligente Bauteile** entwickelt. Diese werden durch **Genetik** dazu befähigt, gespeicherte Informationen an folgende Generationen zu vererben. Die **Intelligenz** ermöglicht das Detektieren von Informationen und Belastungen während des gesamten Produktlebenszyklusses [DHL05].

Bspw. bieten gentelligente Sinterbauteile die Möglichkeit einer inhärenten und somit manipulationssicheren Datenspeicherung. Zusätzlich ist es mit integrierten Funktionselementen möglich, eine im Bauteil enthaltene Kennzeichnung sowie Zustandsüberwachung zu realisieren [BLB+06], [BLG07], [BLG08].

Eine weitere Möglichkeit zum Datenschutz besteht in der Qualifizierung der Bauteilrandzone als inhärenter Informationsspeicher. Mit Mikrostrukturen können gezielt Informationen in die Bauteiloberfläche eingebracht werden. Hierdurch kann das Bauteil eindeutig identifiziert werden [DSO+08].

Ebenfalls ist es möglich, dass Belastungen vom Bauteil selbst detektiert werden. Ultrakurz gepulste Laserstrahlen ermöglichen die Herstellung der erforderlichen Strukturen auf der Bauteiloberfläche [DSB+11], [DSK+12].

Eine weitere Form gentelligenter Bauteile stellen **sensitive Werkstoffe** dar. Mit Hilfe dieser Werkstoffe können Belastungen und Veränderungen eines Bauteils ohne zusätzliche Sensorik detektiert werden. Auf Grundlage verschiedener Messprinzipien kann z. B. der Zustand oder die Beanspruchung eines Bauteils gemessen werden. Die Messprinzipien werden im Folgenden kurz vorgestellt [Thi13, S.23ff.].

Magnetische Flussdichte: Dieses Messprinzip beruht auf magnetischen Magnesiumlegierungen. Basierend auf dem Villari-Effekt[43] kann mit einem Wirbelstromsignal die magnetische Flussdichte und damit die Beanspruchung des Werkstoffs kontinuierlich detektiert werden [DHL10].

Eigenspannung: Die Eigenspannungen in der Bauteiloberfläche ändern sich, sobald die effektive Spannung aus Eigenspannung und aufgebrachter Spannung die Dehngrenze des Werkstoffs überschreitet. Anhand der messbaren Veränderung der Eigenspannung ist das direkte Detektieren von Bauteilüberbeanspruchungen möglich [DKB+11].

Martensitgehalt: Bei Beanspruchungen oberhalb der Dehngrenze des Werkstoffs ändert sich der Martensitgehalt in metastabilen austenitischen Stählen[44]. Dies wird ausgenutzt, um eine kontinuierliche Überwachung des Bauteils zu ermöglichen.

Aus den beschriebenen innovativen Eigenschaften und Funktionen ergeben sich neue Möglichkeiten für den Schutz Intelligenter Technischer Systeme und insbesondere deren Komponenten. Die **Schutzmaßnahmen basierend auf gentelligenten Bauteilen** sind im Folgenden aufgelistet und beschrieben.

Bauteilinhärente Datenspeicherung: Gentelligente Bauteile sind in der Lage, Daten und Informationen zu speichern. Die Speicherung erfolgt nicht auf externen Datenträgern, sondern bauteilinhärent. Dies kann z. B. mit eingebrachten Fremdkörpern realisiert werden [BLG07], [BLG08] oder durch die Ausnutzung von Mikrostrukturen [DSO+08]. Die inhärent gespeicherten Daten können z. B. zur Identifikation von Originalteilen verwendet werden.

Angriffserkennung: Anhand sensitiver Werkstoffe ist eine kontinuierliche Zustandsüberwachung sowie Belastungserkennung möglich [Thi13, S.23ff.]. Hieraus ergeben sich große Potentiale zum Plagiatsschutz, welcher z. B. in Form einer Angriffserkennung realisiert werden kann. Für diese sind keine externen Sensoren erforderlich. Das Bauteil erkennt mit der Zustands- und Belastungsüberwachung selbst, ob und wann es angegriffen wird.

---

[43] Der Villari-Effekt ist ein magnetostriktiver Effekt. Er bewirkt, dass sich bei einer Änderung der Werkstofflänge das magnetische Feld ändert [HS12b, S.22f.].

[44] Stähle mit mehr als 18 Prozent Chrom- und 8 Prozent Nickelanteil weisen eine austenitische Kristallstruktur auf. Dies wirkt sich besonders positiv auf die Kombination von Verarbeitbarkeit, mechanischen Eigenschaften und Korrosionsbeständigkeit aus [Dil05, S.146f.].

Zustandsüberwachung: Mit der kontinuierlichen Zustandsüberwachung sind gentelligente Bauteile in der Lage, ihren Wartungszeitpunkt selbst zu bestimmen [Thi13], [WGN15]. Die Wartung bzw. der Austausch einer Komponente kann somit ausschließlich zu dem Zeitpunkt zugelassen werden, an dem Ermüdungserscheinungen auftreten. Auf diese Weise können Komponenten nicht beliebig ausgebaut und durch möglicherweise gefälschte Teile ersetzt werden.

Authentifizierung auf Basis gentelligenter Bauteile: Klassischerweise funktioniert Authentifizierung mittels eines Datenabgleichs. So kann z. B. eine entsprechend gekennzeichnete Komponente von einer Maschine als Originalkomponente erkannt werden. Hierfür müssen die Daten bereits im Vorfeld auf der Maschine oder in einer Cloud hinterlegt werden. Mit Hilfe gentelligenter Bauteile können diese Daten ebenfalls auf der Komponente gespeichert werden. Für diese Authentifizierung wird eine einzigartige Oberflächenstruktur auf die Komponente aufgebracht. Diese Struktur kann in digitale Daten konvertiert und auf der Oberfläche des Werkstoffs gespeichert werden. Die individuellen Daten werden somit aus der einzigartigen Oberfläche erzeugt. Die Maschine kann bei der Authentifizierung diese Daten ebenfalls aus der Oberflächenstruktur erzeugen und in einem weiteren Schritt mit den in der Komponente gespeicherten Daten abgleichen [DOD+10].

Vererbung von Informationen: Informationen können von gentelligenten Bauteilen generationsübergreifend vererbt werden [LSG15]. Durch eine Authentifizierung wird sichergestellt, dass die Informationen einer ausgetauschten Komponente ausschließlich an Originalkomponenten vererbt werden. Somit verfügen Originalteile über ein weiteres Alleinstellungsmerkmal gegenüber gefälschten Bauteilen. So können zudem z. B. erlernte Informationen über Anwendungsszenarien weitergegeben werden, wodurch eine kontinuierliche Verbesserung des Schutzes ermöglicht wird.

Bauteilinhärente Kennzeichnung: Mit dieser Schutzmaßnahme ist es möglich, eine von außen unsichtbare, nicht manipulierbare Kennzeichnung innerhalb von Bauteilen zu erstellen. Für diese werden Fremdpartikel in das Bauteil eingebracht. Diese inhärente Kennzeichnung verknüpft das Bauteil mit den zugeordneten Informationen (z. B. Werkstücknummer, Herstellungsparameter, Chargennummer etc.) [Lan07].

Viele der entwickelten Maßnahmen beruhen auf bestehenden Schutzmaßnahmen und erweitern diese. Gentelligente Bauteile können demnach als ein Teil von Schutzmaßnahmen gesehen werden. So sind bspw. für eine Authentifizierung eine Lese-/Empfangseinheit sowie eine Informationseinheit erforderlich.

Um zu überprüfen, inwieweit sich die neuen Schutzmaßnahmen basierend auf gentelligenten Bauteilen zum Schutz Intelligenter Technischer Systeme eignen, werden sie den relevanten Schutzanforderungen gegenübergestellt. Die Einordnung der Schutzmaßnahmen erfolgt in die Kategorien produktbezogen und kennzeichnend. Das Ergebnis ist in Tabelle 4-6 dargestellt. Die vorgestellten Schutzmaßnahmen basierend auf gentelligenten Bauteilen erfüllen insgesamt fünf der sechs Schutzanforderungen Intelligenter

Technischer Systeme. Lediglich die Forderung nach Integrität in Netzwerken kann von keiner Schutzmaßnahme voll erfüllt werden.

Tabelle 4-6: Gegenüberstellung der Schutzmaßnahmen basierend auf gentelligenten Bauteilen mit den zugehörigen Schutzanforderungen

Abgleich Schutzmaßnahmen mit Schutzanforderungen																	
Schutzanforderungen	produktbezogen							kenn-zeichnend				ITS-spezifisch					
Schutzmaßnahmen	2.1	2.2	2.3	2.4	2.5	2.6	2.7	4.1	4.2	4.3	4.4	8.1	8.2	8.3	8.4	8.5	8.6
Produktbezogene Schutzmaßnahmen																	
Bauteilinhärente Datenspeicherung	+	−	+	+	○	+	+					+	−	○	−	+	−
Angriffserkennung	+	−	+	+	○	+	+					○	+	−	○	−	−
Zustandsüberwachung	+	−	+	+	○	+	+					○	+	−	○	−	○
Authentifizierung auf Basis gentelligenter Bauteile	+	−	+	+	○	+	+					+	○	+	−	+	−
Vererbung von Informationen	○	−	+	+	−	+	+					+	−	○	−	○	+
Kennzeichnende Schutzmaßnahmen																	
Bauteilinhärente Kennzeichnung								○	○	+	+	−	−	○	−	+	−

Die *bauteilinhärente Datenspeicherung* stellt die Vertraulichkeit sensibler Daten (8.1) sicher. Zusätzlich können so einzigartige kryptographische Schlüssel generiert und sicher gespeichert werden (8.5). Mit der *Authentifizierung auf Basis gentelligenter Bauteile* kann ebenfalls die Forderung nach Vertraulichkeit sensibler Daten (8.1) und darüber hinaus die Schutzanforderung eindeutige Authentifizierung (8.3) erfüllt werden. Die Ausnutzung der Eigenschaften gentelligenter Bauteile ermöglicht zudem die Generierung einzigartiger kryptographischer Schlüssel und deren sichere Speicherung (8.5).

Besonders hervorzuheben ist die Schutzmaßnahme *Vererbung von Informationen*. Diese erfüllt als einzige die Forderung nach Selbstoptimierung der Schutzmaßnahmen (8.6). Auf Grundlage der Vererbung können erlerntes Wissen sowie Erfahrungswerte an andere Systeme oder neue Generationen weitergegeben werden. Hierdurch kann der Systemschutz kontinuierlich mit Hilfe selbstoptimierender Systeme verbessert werden.

4.3.2.4 Software-defined networking

Die Vernetzung der Systeme sowie die Auslagerung von Daten in eine Cloud sind wesentliche Unterscheidungsmerkmale Intelligenter Technischer zu mechatronischer Systeme (vgl. Kap. 2.2.3). Da Angriffe über die Kommunikationsschnittstellen der Systeme (Cyberattacken) zunehmen, ist der Schutz der Kommunikationsverbindungen von entscheidender Bedeutung (vgl. Kap. 2.3.3).

Ein Ansatz zum Aufbau von Kommunikationsnetzwerken ist *Software-defined networking (SDN)*. Mit *SDN* werden die Dynamik der Netzwerkfunktionen sowie intelligente

Anwendungen im Betrieb ermöglicht. Dies geschieht in Verbindung mit sinkenden Kosten durch vereinfachte Hard- und Software sowie ein einfaches Management [SSC+13].

In traditionellen Netzwerken sind die Kontroll- und Datenebene in einem Netzwerkknoten verbunden. *SDN* zeichnet sich insbesondere durch die Trennung der Kontroll- und der Datenebene aus. Die Steuerung (Kontrollebene) übernimmt ein externer Controller [SSC+13]. Dies wird in der Definition der OPEN NETWORKING FOUNDATION deutlich:

> *„In the SDN architecture, the control and data planes are decoupled, network intelligence and state are logically centralized, and the underlying network infrastructure is abstracted from the applications" [ONF12-ol].*

Anhand von *SDN* können insbesondere die Schutzanforderungen Überwachung des Systemverhaltens (8.2) sowie Integrität in Netzwerken (8.4) erfüllt werden (vgl. Tabelle 4-7). Dies wird ermöglicht, da die SDN-Architektur verschiedene Sicherheitsüberwachungen und Analysen unterstützt. So können z. B. Bedrohungen auf Basis forensischer Netzwerkuntersuchungen identifiziert werden. Ferner existieren acht Sicherheitsprinzipien, mit deren Hilfe die Netzwerkintegrität sichergestellt wird [ONF15-ol], [SSC+13].

Kommunikationsverbindungen sind ein essentieller Bestandteil Intelligenter Technischer Systeme (vgl. Kap. 2.2.3). Die Vernetzung der Systeme ist Voraussetzung für die Kommunikationseigenschaften und muss bestmöglich gesichert werden. *SDN* ist ein potentieller Ansatz zum Aufbau von sicheren Netzwerken und sollte für die Systemkommunikation berücksichtigt werden.

4.3.2.5 Übersicht über wirksame Schutzmaßnahmen

In den vorherigen Abschnitten wurden bekannte Schutzmaßnahmen sowie innovative Ansätze zum Systemschutz untersucht und mit den Schutzanforderungen abgeglichen. Besonderes Augenmerk lag auf den ITS-spezifischen Schutzanforderungen. Mit Hilfe der Gegenüberstellung wurde die Wirkung der Schutzmaßnahmen in Bezug auf ITS überprüft. Sowohl von den bekannten Schutzmaßnahmen, als auch aus den innovativen Ansätzen konnten wirksame Maßnahmen identifiziert und hervorgehoben werden. Eine Übersicht über die zehn wirksamsten Schutzmaßnahmen für den Schutz Intelligenter Technischer Systeme ist in Tabelle 4-7 abgebildet.

Auf die einzelnen Schutzmaßnahmen wurde bereits in den vorherigen Kapiteln detailliert eingegangen, daher sind sie hier zusammenfassend beschrieben. Die Technologie der **Authentifizierung** kommt in zwei Maßnahmen vor. Die *Authentifizierung auf Basis gentelligenter Bauteile* kann als Erweiterung bzw. Spezialisierung der *gegenseitigen Authentifizierung von Komponenten* verstanden werden. Im Kern bleibt die Authentifizierung gleich, jedoch ändert sich die Generierung und Speicherung der Authentifizierungsdaten (vgl. Kap. 4.3.2.3).

Tabelle 4-7: Übersicht der zehn wirksamsten Schutzmaßnahmen für Intelligente Technische Systeme

Abgleich Schutzmaßnahmen mit Schutzanforderungen																
Schutzanforderungen	produktbezogen							IT			ITS-spezifisch					
Schutzmaßnahmen	2.1	2.2	2.3	2.4	2.5	2.6	2.7	5.1	5.2	5.3	8.1	8.2	8.3	8.4	8.5	8.6
Produktbezogene Schutzmaßnahmen																
Lokale Änderung der Dichte	○	−	○	+	−	+	+				○	○	+	−	+	−
Individuelle und lokale Anpassung des Materials	○	−	○	+	−	+	+				○	○	+	−	+	−
Bauteilinhärente Datenspeicherung	+	−	+	+	○	+	+				+	−	○	−	+	−
Authentifizierung auf Basis gentelligenter Bauteile	+	−	+	+	○	+	+				+	○	+	−	+	−
Vererbung von Informationen	○	−	+	+	−	+	+				+	−	○	−	○	+
Informationstechnische Schutzmaßnahmen																
Sichere Kommunikationsverbindungen								+	+	○	+	−	−	○	○	−
Gegenseitige Authentifizierung von Komponenten								○	−	−	○	○	+	−	○	−
Schutz von eingebetteter Software								+	○	−	+	○	−	−	+	−
Protecting Electronic Products								−	+	+	+	+	+	−	+	−
Software-defined networking (SDN)								+	+	+	+	○	○	+	○	−

Hervorzuheben sind an dieser Stelle die Schutzmaßnahmen *Vererbung von Informationen, SDN* sowie *Protecting Electronic Products*. Mit der *Vererbung von Informationen* kann die Forderung nach Selbstoptimierung der Schutzmaßnahmen (8.6) erfüllt werden. Dies ist für die Entwicklung wirksamer Schutzmaßnahmen für ITS wesentlich und sollte stets berücksichtigt werden. Durch *SDN* kann die Integrität in Netzwerken (8.4) sichergestellt werden. Auch diese Maßnahme ist für den wirksamen Schutz vernetzter Systeme zwingend zu beachten. Die Schutzmaßnahme mit den meisten voll erfüllten ITS-spezifischen Schutzanforderungen ist *Protecting Electronic Products*. Sie erfüllt vier der sechs Schutzanforderungen Intelligenter Technischer Systeme (vgl. Tabelle 4-7). Sie vereint zahlreiche Ansätze für den Schutz eingebetteter Systeme und ist die wirksamste Maßnahme für den präventiven Schutz Intelligenter Technischer Systeme.

Die Übersicht der wirksamen Schutzmaßnahmen für ITS in Tabelle 4-7 dient zur Unterstützung der Entwickler. Anhand dieser Übersicht können die wirksamsten Schutzmaßnahmen identifiziert und deren Erfüllung der Schutzanforderungen überprüft werden. Insbesondere die Kombination der Schutzmaßnahmen zu Maßnahmenbündeln bietet die Möglichkeit, einen wirksamen Schutz umzusetzen. Die Übersicht stellt eine Vorauswahl an wirksamen, möglichen Lösungen für den Entwurf präventiv geschützter Intelligenter Technischer Systeme dar. Sie kann beliebig erweitert werden und fließt als Hilfsmittel in das Vorgehensmodell in Kapitel 4.5 ein.

In diesem Kapitel wurden innovative Ansätze für den Schutz Intelligenter Technischer Systeme vorgestellt. Vor allem durch die Kombination der vorgestellten Schutzmaßnahmen ergeben sich zahlreiche Einsatzmöglichkeiten. Um eine effiziente Kombination und Umsetzung der Maßnahmen sicherzustellen, müssen diese während der Entwicklung frühzeitig berücksichtigt werden. Hierfür muss die Darstellung der Schutzmaßnahmen überarbeitet werden, um sie für alle Fachbereiche verständlich zu machen und die Integration in moderne Entwurfsmethoden zu ermöglichen. Die Überarbeitung der Darstellung ist im folgenden Abschnitt beschrieben.

4.4 Darstellung von Schutzmaßnahmen

In diesem Kapitel werden die Grundlagen für den Einsatz von Schutzmaßnahmen als Lösungsmuster erarbeitet. Wie in Kapitel 2.4 beschrieben, ist der fachdisziplinübergreifende Entwurf Intelligenter Technischer Systeme ein Prozess, der insbesondere durch die Vielzahl an beteiligten Disziplinen sowie die hohe Wissensintensität geprägt ist. Die modellbasierte Darstellung von Schutzmaßnahmen sowie die Wiederverwendung von Lösungswissen bieten Möglichkeiten, den daraus resultierenden Herausforderungen bei der Berücksichtigung des Systemschutzes zu begegnen. Darüber hinaus trägt die Wiederverwendung von Lösungswissen zur Steigerung der Effizienz in Problemlösungsprozessen bei (vgl. Kap 2.4.5). Die Grundlage bieten die Lösungsmuster nach ANACKER. Da diese die Spezifikationstechnik CONSENS nutzen, wird diese ebenfalls für die modellbasierte Beschreibung der Maßnahmen verwendet. Um die Vorteile der Lösungsmuster zu nutzen, wird in den kommenden Abschnitten die schrittweise Überführung der textbasierten in eine modellbasierte Darstellung von Schutzmaßnahmen aufgezeigt. Das Ziel ist die Repräsentation der Schutzmaßnahmen als Lösungsmuster zur nahtlosen Integration in den Entwurf Intelligenter Technischer Systeme.

4.4.1 Transfer textbasierter in modellbasierte Beschreibungen

Bestehende Schutzmaßnahmen sind in der Regel textbasiert, in Form von Steckbriefen beschrieben (vgl. Kap. 3.1). Die modellbasierte Darstellung mit CONSENS bietet wesentliche Vorteile (in Anlehnung an [Kai13, S.23ff.], [Ana15, S.105ff.]):

- Unabhängigkeit der Darstellung der Schutzmaßnahmen von einzelnen Disziplinen
- Sicherstellung eines eindeutigen und einheitlichen Verständnisses der Maßnahmen
- Sprachenunabhängige Darstellung
- Vereinfachung der Berücksichtigung im Systementwurf
- Unterstützung der Wiederverwendung von bereits vorhandenem Lösungswissen

Ein Vergleich der text- und modellbasierten Beschreibung ist in Tabelle 4-8 dargestellt. Bei der textbasierten Beschreibung ermöglichen verschiedene Aspekte die Spezifizie-

rung der Schutzmaßnahmen. So werden u. a. die Aspekte: Maßnahmenbeschreibung, Einsatz-/Randbedingungen, Wirkung/Hebel der Schutzmaßnahme und Anwendungsbeispiel zur Beschreibung genutzt.

Tabelle 4-8: Vergleich der text- und modellbasierten Maßnahmenbeschreibung

Aspekte von Schutzmaßnahmen	Partialmodelle von CONSENS
Maßnahmenbeschreibung	• Funktionen • Verhalten
Vor- und Nachteile	
Einsatz-/Randbedingungen	• Umfeld • Verhalten
Klassifizierung der Imitatoren	
Wirkung/Hebel der Schutzmaßnahme	• Umfeld • Wirkstruktur (Nutzen von Sichten)
Anwendung/Vorgehen	• Anwendungsszenarien • Wirkstruktur
Anwendungsbeispiel	• Wirkstruktur

Die meisten dieser Aspekte können modellbasiert mit den Partialmodellen von CONSENS dargestellt werden (vgl. Tabelle 4-8). Bspw. ist es möglich, die Maßnahmenbeschreibung mit den Partialmodellen Funktionen und Verhalten abzubilden. Die Einsatz-/Randbedingungen können mit den Partialmodellen Umfeld und Verhalten spezifiziert werden. Lediglich die Darstellung der Vor- und Nachteile sowie die Klassifizierung der Imitatoren kann nicht modellbasiert beschrieben werden.

Exemplarisch wird im Folgenden die für ITS wirksamste Schutzmaßnahme *Protecting Electronic Products* schrittweise in eine modellbasierte Darstellung überführt. Die Funktionsableitung ist in Bild 4-3 gezeigt. Die textbasierten Beschreibung der Maßnahme ist in Kapitel 4.3.2.1 zu finden. Anhand dieser Beschreibung wird das Funktionsprinzip erarbeitet. Die textbasierten Informationen der Maßnahmenbeschreibung werden modellbasiert mit CONSENS abgebildet (vgl. Tabelle 4-8).

Die Schutzmaßnahme *Protecting Electronic Products* ist anhand der **Wirkstruktur** dargestellt. Die Maßnahme besteht aus den Systemelementen: Folie, Messschaltung, Datenverarbeitung (bestehend aus Filterung und Steuerung), RAM[45] (bestehend aus Software und Manipulationsüberwachung) und Flash (bestehend aus Bootlader und verschlüsselter Firm-/Software). Über die sISP Schnittstelle des Bootladers kann die Software initial aufgespielt bzw. aktualisiert werden. Der Service über diese Schnittstelle ist als **Umfeldelement** dargestellt, da er nicht direkt zum System gehört.

[45] Random-Access Memory (RAM) ist ein Datenspeicher. In der vorliegenden Arbeit wird er als flüchtiger Speicher definiert.

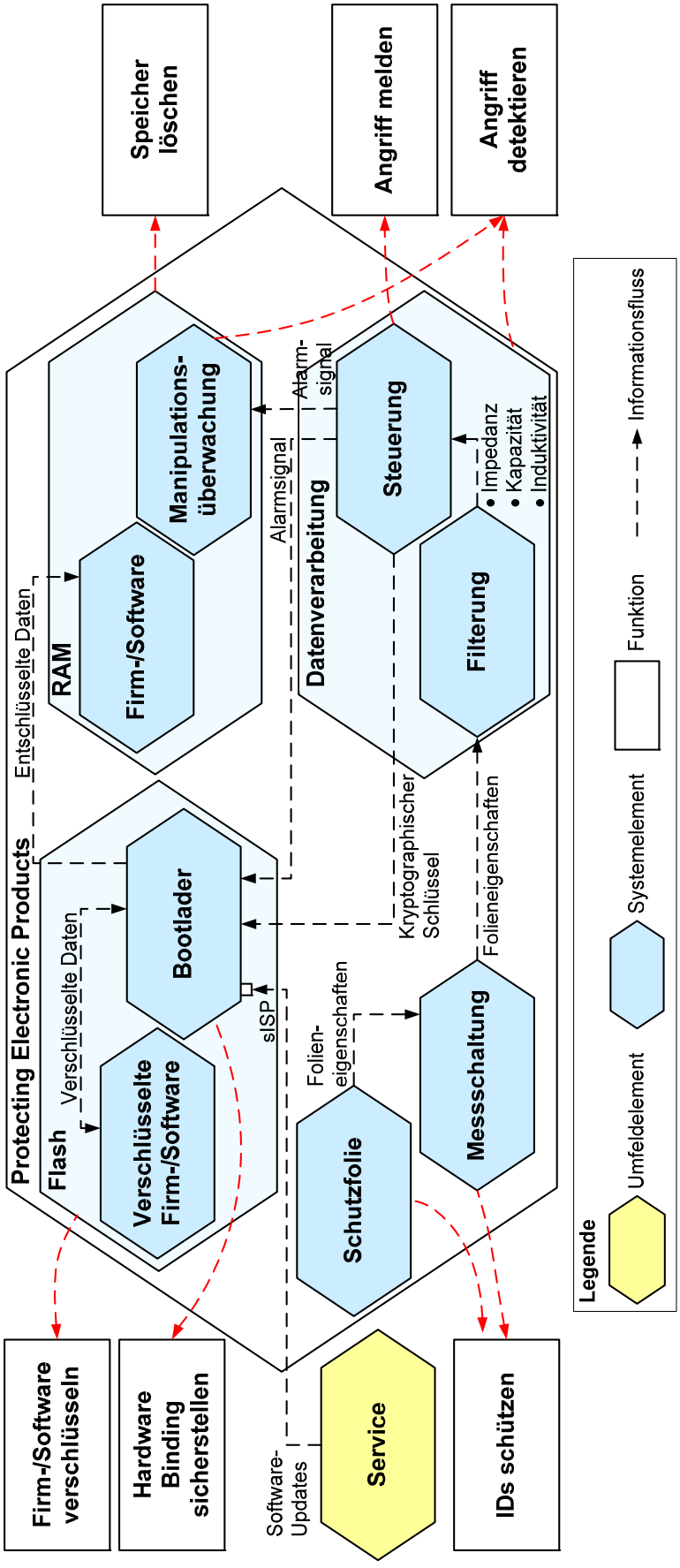


Bild 4-3: Funktionsableitung der Schutzmaßnahme Protecting Electronic Products

Mit der in Bild 4-3 gezeigten Darstellung lassen sich die Beziehungen der internen Elemente untereinander abbilden. So kann die Entschlüsselung der Firm-/Software nachvollzogen werden. Die Folieneigenschaften werden zunächst von der Messschaltung aufgenommen und von der Datenverarbeitung gefiltert. Passen die Daten überein, so wird der kryptographische Schlüssel genutzt, um die Firm-/Software zu entschlüsseln. Diese wird in den RAM geladen und kann nun ausgeführt werden (vgl. Kap. 4.3.2.1).

Ausgehend von der Strukturierung können die **Funktionen** des Systems abgeleitet werden. So wird z. B. die Funktion *Software verschlüsseln* aus den Elementen des Flash-Speichers ermittelt. Die Funktionen fließen in die Erarbeitung der **Übersicht der Schutzfunktionen** für die Schutzmaßnahme Protecting Electronic Products in Bild 4-4 ein.

Die abgeleiteten Funktionen gehören zur zweiten Spezialisierungssebene der Schutzfunktionen. Sie spezialisieren somit nach dem Bottom-Up Prinzip die übergeordneten Funktionen. Die Funktionen können nach dem Top-Down Prinzip um weitere Ebenen ergänzt werden. So kann z. B. die Funktion *Angriff detektieren* in drei weitere Funktionen unterteilt werden (vgl. Bild 4-4). Die Funktionen sollten nur bis zu einem gewissen Grad spezialisiert werden, da sonst die Neutralität der Lösungen nicht mehr sichergestellt werden kann. Insbesondere dann, wenn es zu einer Funktion genau eine Lösung gibt. Die Hauptfunktion der Schutzmaßnahme ist der Schutz eines eingebetteten Systems. Diese Funktion wird spezialisiert durch die Teilfunktionen *Manipulation verhindern*, *Kompatibilität beschränken* und *sensible Daten schützen*. Zur Verhinderung von Manipulationen müssen Angriffe detektiert und gemeldet werden. Im Falle eines erfolgreichen Angriffs muss der Speicher gelöscht werden, damit die Software nicht entwendet werden kann. Die Angriffsdetektion setzt die Manipulationsüberwachung voraus, diese wird durch die Messung der Kapazität, Induktivität und Impedanz realisiert. Die Beschränkung der Kompatibilität wird auf Grundlage des Hardware Bindings sichergestellt.

Der Schutz sensibler Daten teilt sich in die Funktionen *Software verschlüsseln* und *IDs*[46] *schützen* auf. Die Software wird verschlüsselt bevor das System in den Betriebszustand „Aus“ wechselt, so ist sie bei Diebstahl unbrauchbar. Die IDs können mit nicht reproduzierbaren Schlüsseln (PUFs) verschlüsselt und sicher gespeichert werden.

Die gewählte Spezialisierung stellt keinesfalls die abschließende Spezialisierungsebene dar. So kann z. B. die Generierung der PUFs in weitere Funktionen aufgeteilt werden. Die Spezialisierung ist individuell, unter Berücksichtigung der Lösungsneutralität zu wählen.

[46] Identifikationsmerkmale

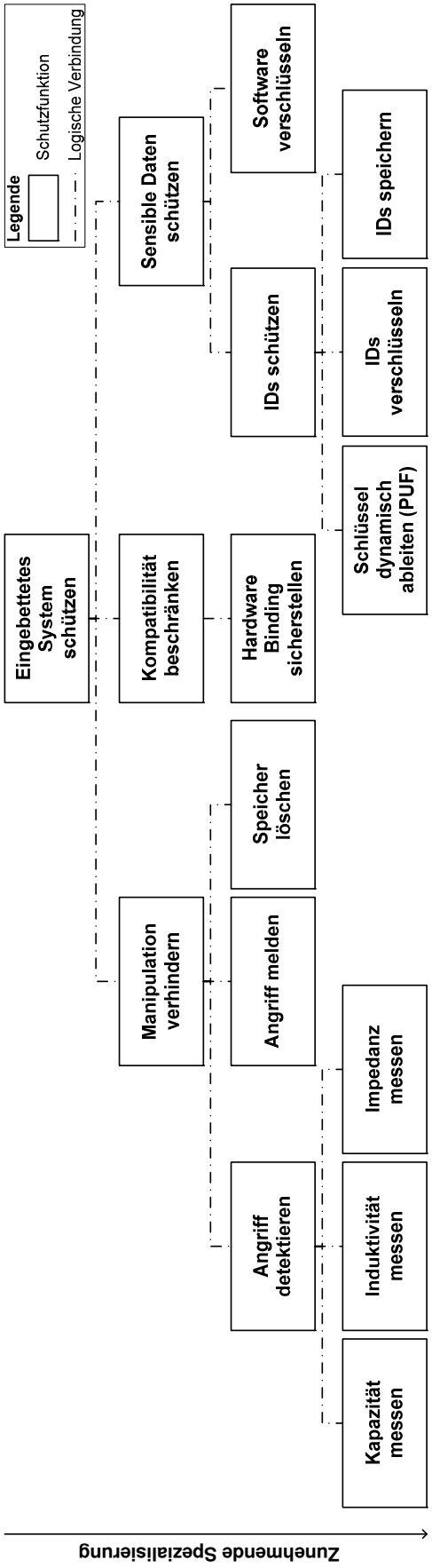


Bild 4-4: Schutzfunktionen der Schutzmaßnahme Protecting Electronic Products

Mit dem Modell Verhalten – Aktivitäten wird die Maßnahmenbeschreibung finalisiert. Dieses ist in Bild 4-5 abgebildet und visualisiert die Abfolge der Aktivitäten.

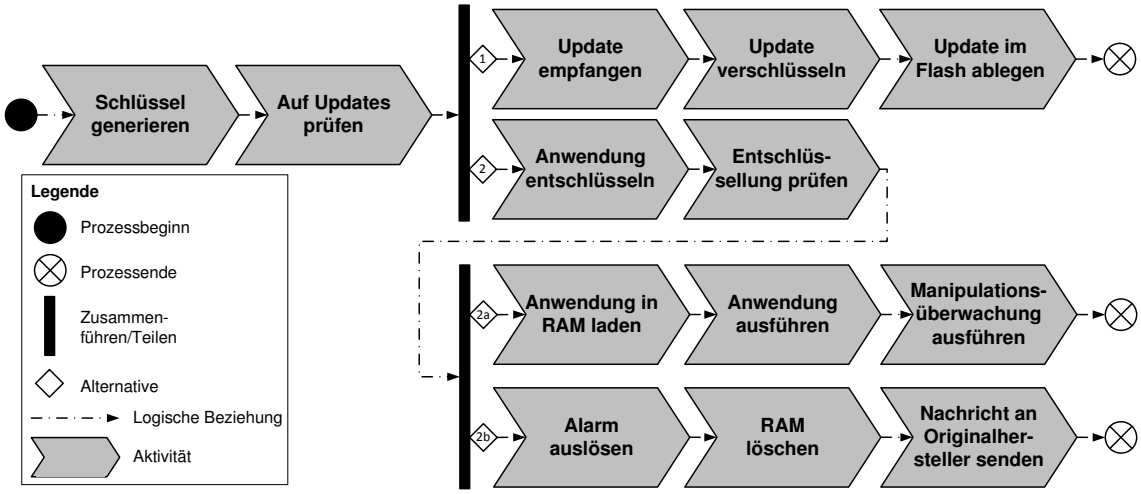


Bild 4-5: Verhaltensmodell der Schutzmaßnahme Protecting Electronic Products

Beim Start des Systems wird ein nicht reproduzierbarer Schlüssel aus den Eigenschaften der Schutzfolie (PUF) generiert. Anschließend wird nach Updates gesucht. Im Falle von vorhandenen Updates werden diese empfangen, verschlüsselt und im Flash-Speicher abgelegt (Alternative 1). Sonst wird die auszuführende Anwendung entschlüsselt und überprüft (Alternative 2). Sollte die Entschlüsselung korrekt sein, wird die Anwendung in den RAM geladen und ausgeführt. Zusätzlich wird die Manipulationsüberwachung gestartet (Alternative 2a). War die Entschlüsselung nicht korrekt, wird ein Alarm ausgelöst. So wird der RAM gelöscht, damit die Anwendung nicht gestohlen werden kann. Darüber hinaus wird der Originalhersteller benachrichtigt (Alternative 2b).

Zusammenfassend lässt sich festhalten, dass anhand der modellbasierten Systemspezifikation eine hinreichend detaillierte Beschreibung der Schutzmaßnahme ermöglicht wird. Damit ebenfalls die Aspekte Vor- und Nachteile sowie die Klassifizierung der Imitatoren modellbasiert dargestellt werden können (vgl. Tabelle 4-8), wird im folgenden Abschnitt die Adaption der Schutzmaßnahmendarstellung untersucht.

4.4.2 Adaption musterbasierter Darstellung

Schutzmaßnahmen müssen allgemeinverständlich und hinreichend abstrakt beschrieben werden, damit sie im Systementwurf berücksichtigt werden können. Aus diesem Grund wurde im vorherigen Abschnitt der Transfer von textbasierten in modellbasierte Beschreibungen erarbeitet. Es zeigte sich, dass die Aspekte Vor- und Nachteile sowie die Klassifizierung der Imitatoren nicht in CONSENS beschrieben werden können (vgl. Tabelle 4-8). Für diese Aspekte sind alternative Darstellungen zu entwickeln.

Zunächst wird die **Klassifizierung der Imitatoren** untersucht. Diese zeigt zum einen, gegen welche Kompetenzen der Imitatoren eine Schutzmaßnahme wirksam ist (vgl.

Bild 4-6). Die Einschätzung der Wirkung der Schutzmaßnahme muss von Experten vorgenommen werden. Zum anderen können mit der Klassifizierung die Kompetenzen der relevanten Imitatoren dargestellt werden (vgl. Bild 5-3). Die Klassifizierung nach LINDEMANN ET AL. zeigt die Charakterisierung der Imitatoren, welche mit der vorliegenden Maßnahme bekämpft werden können [LMP+12a, S.163]. Demnach wirken Schutzmaßnahmen, die gegen eine hoch ausgeprägte Kompetenz wirken, auch bei den Ausprägungen mittel oder gering. Die Kompetenzen der Imitatoren werden durch fünf Aspekte charakterisiert. Diese wurden im Kapitel 3.1.2 beschrieben [LMP+12a, S.104].

Da sich die vorliegende Arbeit auf den Schutz Intelligenter Technischer Systeme fokussiert, spielt die Beziehung zwischen dem Originalhersteller und dem Imitatoren keine Rolle. Lediglich die Kompetenzen der Imitatoren haben Einfluss auf die Maßnahmenauswahl. Ebenso ist der Kundenzugang vernachlässigbar, da er die Auswahl von technischen Schutzmaßnahmen – insbesondere in der frühen Phase des Systementwurfs – nicht beeinflusst. Ein bislang nicht berücksichtigter Aspekt ist für den Schutz vernetzter Systeme von besonderer Bedeutung. Cyberattacken stellen ein Risiko für Intelligente Technische Systeme dar und verursachen immensen Schaden [WEF14]. Daher ist die Kenntnis über das Know-how der Imitatoren auf diesem Gebiet relevant und wird als **Cyberkompetenz** definiert. Sie charakterisiert die Fähigkeiten der Imitatoren für die Nutzung von Informationstechnologie zur illegalen Beschaffung von Know-how. Aus diesem Grund wird der Aspekt Cyberkompetenz in die Klassifizierung aufgenommen.

Die **Charakterisierung der Imitatoren** erfolgt anhand verschiedener Indikatoren und deren Ausprägung (vgl. [LMP+12a], [Gri14], [STF12], [BSI12b]). Diese sind in der Tabelle 4-9 aufgeführt. Sowohl die aufgeführten Indikatoren als auch deren Ausprägungen sind Hilfestellungen zur Beurteilung der Kompetenzen. Sie erheben keinen Anspruch auf Vollständigkeit. Aufgrund der Tatsache, dass Reverse Engineering die meist angewandte Methode zur Extraktion des Produkt-Know-hows ist [VDM16], sind die Entwicklungskompetenzen der Imitatoren besonders relevant. Für den Schutz Intelligenter Technischer Systeme sind ebenso die neu hinzugefügten Cyberkompetenzen ausschlaggebend. Beide Kompetenzen werden im Folgenden näher beschrieben. Zur Beschreibung der Kompetenzen sei zudem auf das Kapitel 3.1.2 verwiesen.

Entwicklungskompetenz: Dieser Aspekt lässt sich z. B. anhand der funktionalen Qualität oder verwendeter Produktkomponenten von Imitaten abschätzen. Ist die funktionale Qualität mit der des Originalproduktes vergleichbar, so ist dies ein Argument für eine hohe Entwicklungskompetenz des Imitators. Reverse Engineering bedarf bestimmter Analysewerkzeuge. So werden für das Analysieren eingebetteter Systeme wie Röntgengeräte, Signal-Generatoren, Logikanalysatoren, Oszilloskope, Laser oder Mikroskope gebraucht [FS11]. Die Ausstattung der Imitatoren mit diesen Werkzeugen ist dementsprechend relevant für die Bewertung der Kompetenzen.

Cyberkompetenzen: Für die Abschätzung der Cyberkompetenzen sind bekannte Angriffe zu analysieren. Dies stellt jedoch eine Herausforderung dar. Einerseits ist der Ur-

sprung einer Cyberattacke schwer zu lokalisieren (da viele Angriffe auf Schwarzmärkten käuflich erworben werden können). Andererseits ist das Ausmaß eines Angriffs schwer einzugrenzen (da die Menge entwendeter Informationen häufig nicht beziffert werden kann) [BSI12b], [Gon12]. Aus diesem Grund wird die Einschätzung anhand der Indikatoren Angriffsdimension und -art vorgenommen. Die Ausprägungen der Angriffsart sind in Anlehnung an die Grundwerte der Informationssicherheit[47] definiert.

Tabelle 4-9: Indikatoren zur Bewertung der Kompetenzen von Imitatoren

Kompetenzen	Indikatoren	Ausprägung
Fertigungs-kompetenz	Fertigungsqualität	hochwertig, minderwertig, aufwendig, toleranztreu
	Herstellungs-Know-how	komplexer Prozess, Spezialwissen, Standardfertigung
	Produktkernelemente	Kostentreiber, individuelle Komponenten, besondere Funktionen
Finanzstärke	Ressourcenausstattung	aufwändige Prozesse, Sondermaschinen, Standardfertigung
	Rendite	Gewinn bei Anwendung einer Produktionstechnologie, Investitionen in Produktionsanlagen und Organisation
Entwicklungs-kompetenz	funktionale Qualität	fehlerhaft, präzise, Vergleichbarkeit der Originalfunktionen, Produktkomplexität
	Produktkomponente	Originalteil, Sonderfertigung, Standardteil, Zweitmarke, Nachbau
	Wettbewerberbeteiligung	Übereinstimmung mit Konkurrenzprodukten, Spezialisierung bei Produkt- und Markenauswahl
Cyber-kompetenz	Angriffsdimension	Endgerät, Cloud, Netzwerk, gezielt, großflächig
	Angriffsart	Angriff auf Verfügbarkeit, Vertraulichkeit, Integrität

Die Kompetenzen der Imitatoren werden nach LINDEMANN ET AL. als **Polaritätsprofile** dargestellt. In Bild 4-6 ist die Klassifizierung der Imitatoren für die Schutzmaßnahme *Protecting Electronic Products* (vgl. Kap. 4.3.2.1) dargestellt. Die Klassifizierung zeigt auf, gegen welche Kompetenzen die Schutzmaßnahme wirksam ist.

Ein Imitator braucht eine sehr hohe Cyberkompetenz um die Schutzmaßnahme *Protecting Electronic Products* zu umgehen. Es bestehen zahlreiche Schutzmechanismen, um Cyberattacken abzuwehren (Verschlüsselung auf Basis einzigartiger kryptographischer Schlüssel, Manipulationsüberwachung etc.). Ebenso kann die Wirkweise der Maßnahme nicht im ausgeschalteten Zustand mittels Reverse Engineering identifiziert werden. Daher sind hohe Fertigungskompetenzen und große finanzielle Stärke nutzlos.

[47] Die Grundwerte der Informationssicherheit werden vom BSI charakterisiert als: Vertraulichkeit, Verfügbarkeit und Integrität. Die Vertraulichkeit adressiert zu definierende Zugriffsrechte von Personen sowie die Verschlüsselung von Daten. Die Verfügbarkeit charakterisiert die Erreichbarkeit von Services, Funktionen oder Informationen eines IT-Systems. Die Robustheit der Daten gegen Manipulation wird durch die Integrität beschrieben [BSI12a].

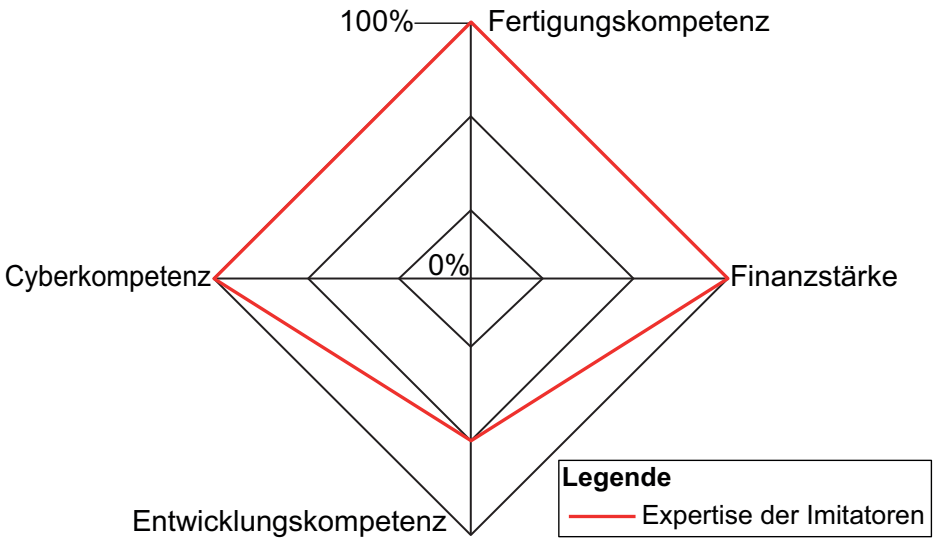


Bild 4-6: Klassifizierung der Imitatoren der Schutzmaßnahme Protecting Electronic Products

Bedingt durch die Erweiterung der Klassifizierung um den Aspekt Cyberkompetenzen, werden die Angriffe auf vernetzte Systeme berücksichtigt. So ist die Klassifizierung für den Schutz Intelligenter Technischer Systeme geeignet. Relevante **Vor- und Nachteile** werden unter dem Aspekt Merkmale eines Schutzmusters vermerkt. Ebenfalls sind hier die Quellen anzugeben, auf denen das Schutzmuster beruht.

Die modellbasierte Darstellung der Schutzmaßnahmen unter Berücksichtigung von bereits erfolgreich eingesetztem Lösungswissen wird als **Schutzmuster** bezeichnet. Die Schutzmuster basieren auf der einheitlichen Strukturierung von Lösungsmustern nach ANACKER. Diese Lösungsmuster sind für die Entwicklung fortgeschrittener mechatronischer Systeme ausgelegt und erhöhen die Effizienz in Problemlösungsprozessen (vgl. Kap. 2.4.5 und 3.4.3). Allgemein beschreiben Muster ein Problem und die zugehörige Lösung. Sie bestehen basierend auf der Definition von ALEXANDER aus den Kategorien: Name, Problem, Lösung und Kontext [AIS+77] (vgl. Bild 3-12). Da sich Schutzmuster auf eine bestimmte Lösung (eine bestimmte Schutzmaßnahme) beziehen, beschreiben sie weniger das allgemeine Problem als vielmehr die Aufgabe der Maßnahme. Aus diesem Grund wird die Problembeschreibung der Lösungsmuster als Beschreibung der **Entwurfsaufgabe** angepasst. Im folgenden Abschnitt wird das Schutzmuster Protecting Electroinic Products detailliert beschrieben.

4.4.3 Darstellung des Schutzmusters Protecting Electronic Products

Schutzmuster wurden als strukturierte, modellbasierte Beschreibung von Schutzmaßnahmen (z. B. durch Steckbriefe) definiert. Beispielhaft ist die Schutzmaßnahme *Protecting Electronic Products* (vgl. Kap. 4.3.2.1) im Bild 4-7 als Schutzmuster modellbasiert dargestellt. Die Aspekte sind im Folgenden beschrieben.

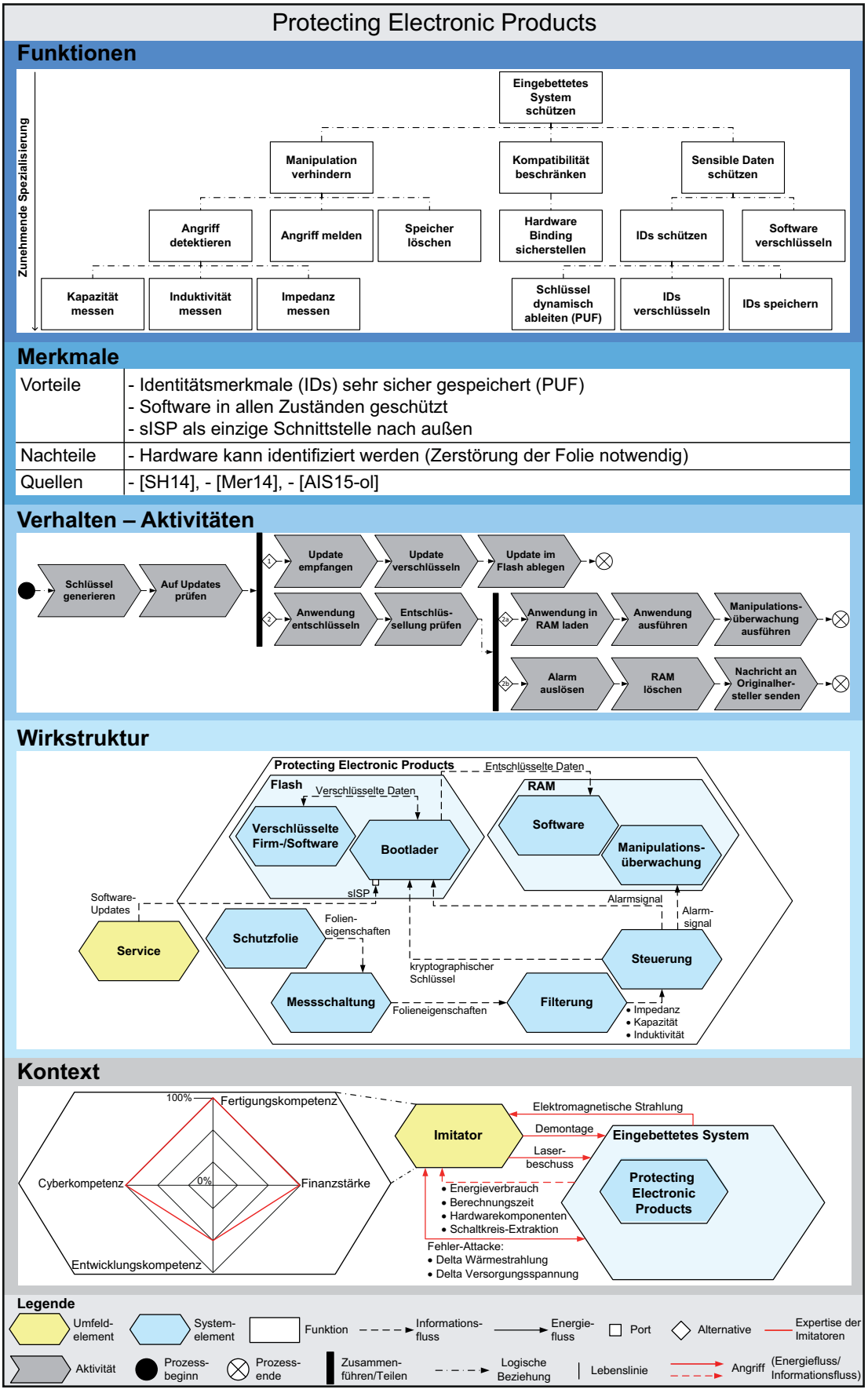


Bild 4-7: Schutzmuster Protecting Electronic Products

Name: Genau wie die Schutzmaßnahmen wird auch das Schutzmuster als *Protecting Electronic Products* definiert. Der Name des Schutzmusters sollte mit dem Namen der Schutzmaßnahme übereinstimmen.

Entwurfsaufgabe: Die Entwurfsaufgabe wird durch Funktionen und Merkmale beschrieben. Im Aspekt Funktionen wird die Übersicht der Schutzfunktionen der Schutzmaßnahme aufgezeigt. Hier wird die Gesamtfunktion solange durch Teilfunktionen spezialisiert, bis sich für diese Teilfunktionen Lösungen finden lassen [VDI2221]. Die Hauptfunktion ist der Schutz des eingebetteten Systems. Diese wird in die Teilfunktionen Manipulation verhindern, Kompatibilität beschränken und sensible Daten schützen untergliedert. Diese werden weiter aufgegliedert (vgl. Kap. 4.4.1, Bild 4-4).

In der modellbasierten Aufgabenbeschreibung besteht mit dem Aspekt Merkmale die Möglichkeit, Informationen (Eigenschaften des Schutzmusters) textbasiert darzustellen. In Bild 4-7 sind Vor- und Nachteile sowie relevante Quellen aufgelistet. Ebenso werden Hinweise zur Umsetzung des Schutzmusters gegeben (vgl. Anhang A8, Bild A-20).

Lösung: Das Lösungswissen wird anhand der Partialmodelle Verhalten und Wirkstruktur dargestellt[48]. Das Verhalten wird mit den Modellen Zustände, Aktivitäten und Sequenz beschrieben (vgl. Kap. 3.3.1). Im Beispiel in Bild 4-7 ist das Modell Verhalten – Aktivitäten visualisiert. In diesem werden die ablaufenden Prozesse abgebildet. So können Prozessfolgen wie die Entschlüsselung der Anwendung und deren Überprüfung sowie nachfolgende Prozesse, abgebildet werden (vgl. Kap. 4.4.1, Bild 4-5).

Die Wirkstruktur dient der Darstellung von Beziehungen zwischen Systemelementen. Hier kann z. B. nachvollzogen werden, auf welche Weise die Folieneigenschaften genutzt werden, um daraus mit der Datenverarbeitung einen einzigartigen kryptographischen Schlüssel zu generieren (vgl. Kap. 4.3.2.1, 4.4.1, Bild 4-3).

Kontext: Dieser Aspekt besteht im Wesentlichen aus der Klassifizierung der Imitatoren. Anhand dieser wird aufgezeigt, gegen welche Kompetenzen die Maßnahme wirkungsvoll ist. Die Klassifizierung der Imitatoren wird kombiniert mit Ausschnitten aus dem Umfeldmodell sowie der Wirkstruktur des Systems. Auf diese Weise können die Einsatz-/Randbedingungen einer Schutzmaßnahme visualisiert werden (vgl. Kap. 4.4.2). Ebenso sind im Kontext mögliche Angriffsarten eines Imitators visualisiert. Zudem sind die Informationen, die ein Angreifer sich beschaffen kann, aufgeführt. So könnte ein Imitator ein eingebettetes System z. B. durch Demontage, Laserbeschuss oder eine Fehler-Attacke angreifen. Dann wären Rückschlüsse auf elektromagnetische Strahlung, Energieverbrauch, Wärmestrahlung etc. möglich. Durch diese sind Imitatoren in der Lage, die Funktionsweise eines Systems zu imitieren. Das Schutzmuster *Protecting*

[48] Bei weniger komplexen Sachverhalten können die Partialmodelle auch einzeln genügen. Wenn kein Softwareanteil vorhanden ist, kann das Verhalten vernachlässigt werden [Ana15, S.107].

Electronic Products schützt ein eingebettetes System vor diesen Angriffen und sorgt so dafür, dass die Imitation deutlich erschwert wird.

In CONSENS werden die Wechselwirkungen zwischen den Systemelementen mit Flussbeziehungen dargestellt. Störflüsse sind rot markiert (vgl. Kap. 3.3.1). So lassen sich Angriffe visualisieren. Störende Energieflüsse eignen sich z. B. zur Abbildung von Angriffen unter Krafteinwirkung. Durch diese Angriffe werden Systemelemente (wie RFID-Chips) freigelegt. Störende Informationsflüsse bieten sich an um z. B. Cyberattacken darzustellen. Chemische Angriffe (zur Freilegung von Systemelementen) werden anhand störender Stoffflüssen abgebildet. Einen Überblick gibt die *Tabelle 4-10*.

Tabelle 4-10: Darstellung von Angriffen mit Hilfe von Flussbeziehungen

Flussbeziehungen	Angriffsarten
Energiefluss (störend)	• Angriffe unter Krafteinwirkung (z. B. Schleifen) • Physikalische Angriffe (z. B. Entnehmen und Hinzufügen von Hardware) • Strahlung (elektromagnetische, Wärme- oder Röntgenstrahlung) • Energieverbrauch durch das System • Laserbeschuss
Informationsfluss (störend)	• Cyberattacken (Remote-Zugriff oder durch physikalische Verbindung mit dem System) • Manipulation der Firmware • Angriffe auf Kommunikationsnetze
Stoffffluss (störend)	• Chemische Angriffe (z. B. Säure)

Beispielhaft wird ein Seitenkanalangriff auf ein eingebettetes System untersucht. Durch einen solchen Angriff kann z. B. ein geheimer Schlüssel anhand der Abstrahlung physikalischer Informationen ermittelt werden. Zunächst werden die elektronischen Bauteile freigelegt. Diese Angriffe können in Form von störenden Energie- oder Stoffflüssen dargestellt werden (z. B. Schleifen oder Ätzen). Anschließend werden mit einer Korrelationsleistungsanalyse Informationen extrahiert. Hierzu werden die elektromagnetische Strahlung und der Energieverbrauch gemessen. Dies kann anhand störender Energieflüsse visualisiert werden. Ebenfalls wird die benötigte Zeit für die Signalverarbeitung bestimmt. Hier dienen störende Informationsflüsse zur Visualisierung (vgl. [FS11], [MKP12]). Die so dargestellten Angriffe sowie die dazugehörigen Schutzmuster können in unterschiedlichen Abstraktionsebenen beschrieben werden. Auf die unterschiedlichen Ebenen wird im folgenden Abschnitt näher eingegangen.

4.4.4 Abstraktionsebenen von Schutzmustern

Für die Visualisierung der unterschiedlichen Abstraktionsebenen eignen sich die Schutzmaßnahmen auf Basis der Authentifizierung im Besonderen. Die Maßnahme *gegenseitige Authentifizierung von Komponenten* ist bei GAUSEMEIER ET AL. beschrieben (vgl. Kap. 4.3.1). In dem textbasierten Steckbrief wird sie mit einer Kurzbeschreibung erläutert (vgl. Bild 3-1):

> *„Bei der gegenseitigen Authentifizierung wird eine Austauschkomponente von einer Steuerungseinheit einer Anlage/Maschine auf ihre Originalität überprüft" [GGL12, S.263].*

Im Aspekt Anwendung/Vorgehen wird die Kurzbeschreibung detailliert. Hier wird das Funktionsprinzip der Schutzmaßnahme wie folgt beschrieben:

> *„Beim Einbau eines Ersatzteils in eine Anlage/Maschine wird das Bauteil durch die Maschinensteuerung authentifiziert, indem sie von der Austauschkomponente zuvor definierte Daten abfragt (z. B. über RFID-Chips) […]" [GGL12, S.263].*

Ebenfalls ist die Schutzmaßnahme bei LINDEMANN ET AL. unter der Bezeichnung „gegenseitige Bauteilauthentifizierung vorsehen" beschrieben (vgl. Anhang A1.1, Bild A-1). Die Unterschiede in den Beschreibungen sind äußert gering und werden daher vernachlässigt.

In beiden Beschreibungen wird übereinstimmend erwähnt, dass ein RFID-Chip als mögliches Speicher- und Sendeelement für Identifikationsinformationen dienen kann. Die Informationen werden demnach **sensorbasiert** übertragen. Mit eingebetteter Steuerungssoftware ist es möglich, den Austausch von Informationen zwischen Systemelementen über ein **Kommunikationsmodul**[49] zu gestalten. Nach LINDEMANN ET AL. ist die Maßnahme ebenfalls abstrahiert auf mechanische Bauteile übertragbar und somit **gestaltbasiert** anwendbar, z. B. anhand einer Passwelle. In den vorliegenden textbasierten Beschreibungen werden verschiedene Abstraktionsebenen vermischt. Dies ist für die zunächst abstrakte Anwendung im Entwurf und die spätere Konkretisierung nachteilig.

Die Schutzmaßnahme wird allgemeingültig beschrieben, jedoch werden gleichzeitig verschiedene Beispiele und Umsetzungen der Maßnahme dargestellt. Somit ist auch der Name der Schutzmaßnahmen nicht eindeutig. Eine gegenseitige Authentifizierung setzt einen bidirektionalen Datenaustausch voraus. Während der Informationsfluss über ein Kommunikationsmodul bidirektional stattfindet, werden sensorbasierte Messgrößen in der Regel unidirektional transportiert. Für eine bidirektionale Kommunikation sind ak-

[49] In der Elektrotechnik werden fertige Transceiver-Baugruppen und die zugehörigen Komponenten zur Ansteuerung (Mikrocontroller) als Kommunikationsmodul bezeichnet. Über dieses findet die Kommunikation mit externen Systemen statt. Darüber hinaus dient es als zentrale, interne Schnittstelle zur Weiterleitung von Daten bzw. Informationen [Dum10, S.116].

tive RFID-Chips notwendig. Diese können Daten empfangen und speichern. Zur gegenseitigen Authentifizierung müssen die Daten allerdings ausgewertet werden. Dies kann der RFID-Chip an sich nicht leisten. Ebenso kann mit der Abstraktion die Einschränkung der Authentifizierung auf Komponenten vernachlässigt werden. So ist auch die Authentifizierung anderer Systeme denkbar.

Durch die Überführung der textbasieren in die modellbasierte Maßnahmenbeschreibung können Abstraktionsebenen vereinfacht dargestellt werden. Die Ebenen finden sich im **multidimensionalen Wissensraum** nach ANACKER wieder (vgl. Kap 3.4.3 und Anhang A4). Demnach werden die Spezialisierung des Lösungswissens (generalisiert zu spezialisiert), die Aggregation des Lösungswissens (elementar zu komplex) sowie die Art der Wissensrepräsentation (modellbasiert und textbasiert) unterschieden. In Bild 4-8 sind Spezialisierungsebenen für den Schutz durch Authentifizierung dargestellt.

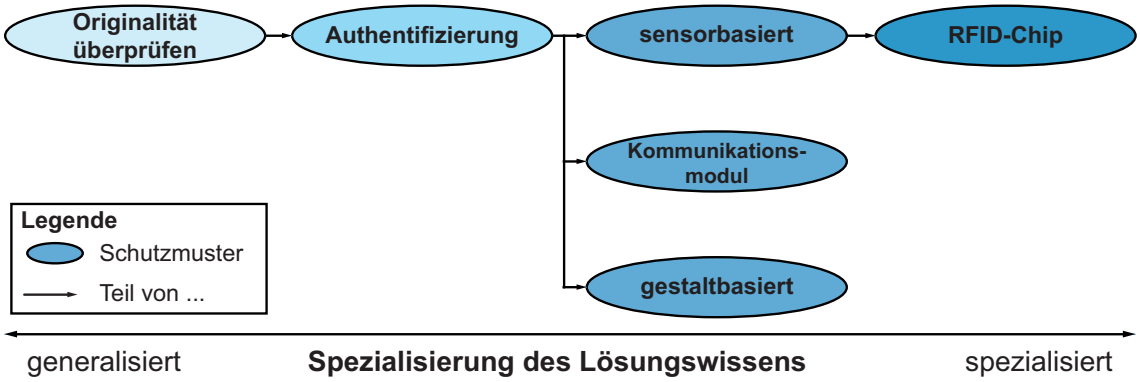


Bild 4-8: Spezialisierungsebenen von Schutzmustern auf Basis der Authentifizierung

Das im Schutzmuster enthaltene Lösungswissen kann generalisiert oder spezialisiert sein. Ein sehr generelles Schutzmuster ist *Originalität überprüfen* (vgl. Anhang A8, Bild A-20). Hierbei wird das übergeordnete Ziel der Überprüfung der Originalität lösungsneutral und abstrakt beschrieben. Dieses Ziel kann z. B. anhand einer *Authentifizierung* erreicht werden. Die Authentifizierung kann wiederum *sensorbasiert* (vgl. Schutzmuster *Authentifizierung über Sensorik* Anhang A8, Bild A-21), über ein *Kommunikationsmodul* (vgl. Schutzmuster *Gegenseitige Authentifizierung über Kommunikationsmodul* Anhang A8, Bild A-22) oder über die *Gestalt* stattfinden. Als Sensor kann u. a. ein *RFID-Chip* dienen (vgl. Schutzmuster *Authentifizierung von Komponenten durch RFID* Anhang A8, Bild A-23). Hiermit wird die stärkste Spezialisierung des Lösungswissens erreicht. Mit Hilfe der unterschiedlichen Abstraktionsebenen wird die kontinuierliche Anwendung der Schutzmuster während der gesamten Entwicklung sichergestellt. So können im Systementwurf zunächst generalisierte Schutzmuster berücksichtigt werden. Mit fortschreitender Konkretisierung der Entwicklung können auch die Schutzmuster weiter spezialisiert werden.

Die verschiedenen Ausprägungen der Aggregation des Lösungswissens sowie die Unterschiede bei der Art der Wissensrepräsentation sind in Bild 4-9 visualisiert. Die Dimension für die Aggregation des Lösungswissens verläuft vom elementaren zum kom-

plexen. Elementare Lösungen sind z. B. grundlegende Prinzipien wie die Datenübertragung oder messtechnische Prinzipien. Diese bilden die Basis für komplexere Lösungen.

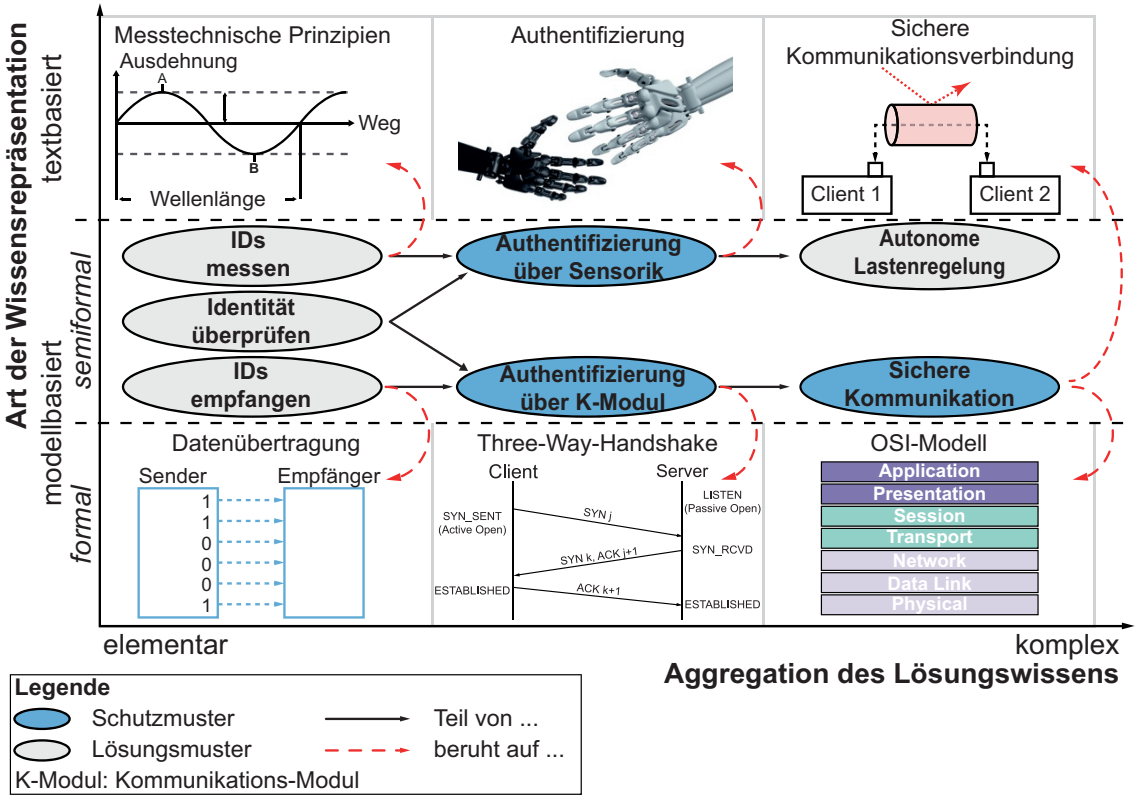


Bild 4-9: Spezialisierung von Schutzmustern in Anlehnung an [Ana15, S.117], basierend auf [ISO7498], [Bue01], [Har02], [Stef04]

Bei der Art der Wissensrepräsentation wird zwischen modellbasierter und textbasierter Darstellung unterschieden. Die modellbasierte Darstellung wird weiter in formale und semiformale Modelle unterteilt. Die semiformalen Modelle bilden die Lösungs- und Schutzmuster. Diese stehen in Verbindung miteinander und beruhen auf Lösungsprinzipien. Bspw. beruht das Lösungsmuster *IDs empfangen* auf dem Prinzip der Datenübertragung. Das Lösungsmuster ist ein Teil des Schutzmusters *gegenseitige Authentifizierung über Kommunikationsmodul* (vgl. Anhang A8, Bild A-22), welches wiederum auf dem *Three-Way-Handshake* beruht. Das Schutzmuster ist ein Teil des komplexeren Schutzmusters *sichere Kommunikation* (vgl. Anhang A8, Bild A-24). In diesem werden die Modelle und Prinzipien der Informationssicherheit (vgl. Kap. 4.4.2) zusammengefasst. Sichere Kommunikationsverbindungen stellen die Voraussetzung für den Austausch sensibler Informationen zwischen Systemen dar. Dieser beruht auf dem standardisierten *OSI-Modell* (vgl. [ISO7498], [Bue01], [Har02], [Stef04]). Schutzmuster können ebenfalls auf komplexeren Lösungsmustern beruhen. So ist die *Authentifizierung über Sensorik* (vgl. Anhang A8, Bild A-21) Teil der *autonomen Lastenregelung*.

Mit Schutzmustern kann die Effizienz in Problemlösungsprozessen wesentlich verbessert werden. Schutzmuster schaffen die Möglichkeit, kollektive Erfahrungen und Wis-

sen über den Schutz der Systeme in neue Entwicklungsprojekte einzubringen. Um den wirksamen Schutz für ITS zu gewährleisten, muss dieser im Systementwurf beachtet werden. So können zur effektiven Umsetzung von Schutzmustern bereits entsprechende Komponenten berücksichtigt oder Verhaltensmodelle entwickelt werden. Für die Integration der Aspekte des Systemschutzes in den Entwurf Intelligenter Technischer Systeme ist die modellbasierte Darstellung der Schutzmuster eine grundlegende Voraussetzung. Zur Integration der Aspekte des Systemschutzes im Systementwurf wird im folgenden Kapitel ein Vorgehen entwickelt und vorgestellt.

4.5 Integration des präventiven Schutzes in den musterbasierten Entwurf Intelligenter Technischer Systeme

Die *Entwurfssystematik für den präventiven Schutz Intelligenter Technischer Systeme vor Produktpiraterie* wird durch das folgende Vorgehensmodell komplettiert. So wird ein funktionsorientierter Systementwurf im Sinne der VDI 2206 unter Berücksichtigung des Systemschutzes ermöglicht. Ziel ist die Integration der Aspekte des präventiven Systemschutzes in den lösungsmusterbasierten Entwurf Intelligenter Technischer Systeme. Die disziplinübergreifende Berücksichtigung des Systemschutzes in den frühen Phasen der Entwicklung soll erleichtert werden. Das Vorgehen gliedert sich in vier aufeinanderfolgende Phasen. Bild 4-10 verdeutlicht den Ablauf der Phasen, Aufgaben und Methoden sowie Resultate.

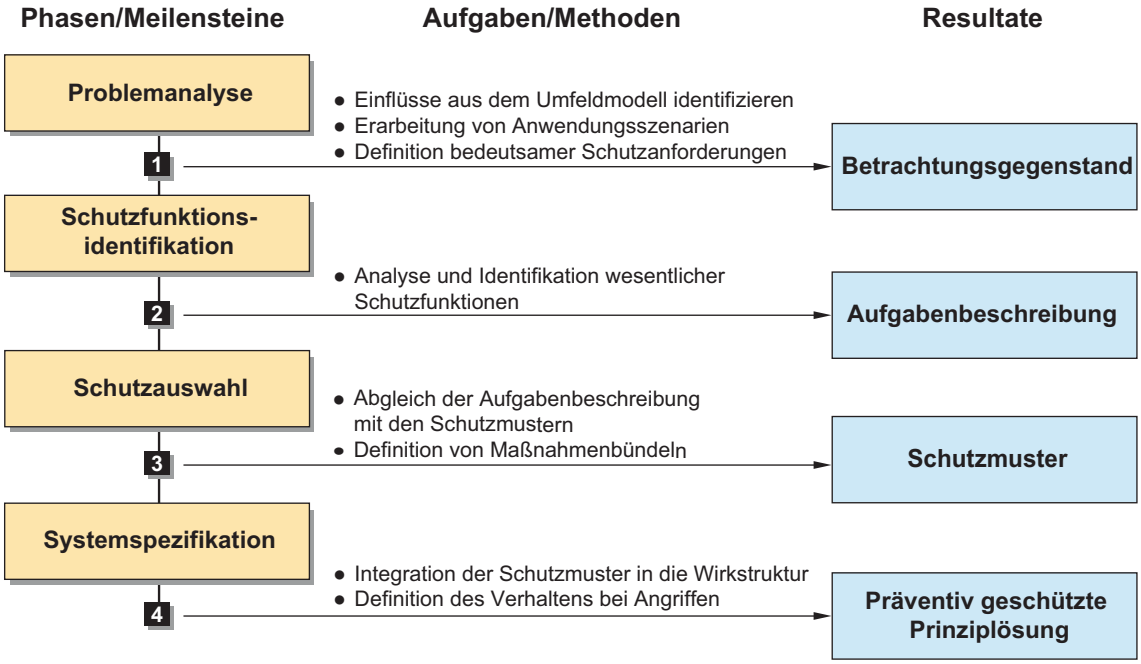


Bild 4-10: Vorgehensmodell zur Integration des Schutzes in den musterbasierten Entwurf Intelligenter Technischer Systeme

In Anlehnung an die Strukturierung nach GAUSEMEIER sind die Erkenntnisse aus der strategischen Produktplanung zugrunde liegende Eingangsinformationen für das Vorge-

hen (vgl. Kap. 2.4.1). Das Vorgehensmodell wird in einzelne Phasen und Meilensteine unterteilt und gibt einen Überblick über die wesentlichen Tätigkeiten und zu erarbeitenden Resultate. Zudem wird die Reihenfolge der Durchführung der einzelnen Phasen festgelegt. Hier handelt es sich um eine sequentielle und idealtypische Darstellung, deren tatsächliche Anwendung Iterationen und Rücksprünge zulässt. Das Vorgehen wird zunächst losgelöst von den übrigen Aufgaben im Systementwurf vorgestellt. Der Fokus liegt auf den Schritten zur Integration der Aspekte des Systemschutzes in den Entwurf. Die Einordnung des Vorgehens in den übergeordneten Systementwurf erfolgt in Kapitel 4.5.5.

4.5.1 Phase 1: Problemanalyse

Das Ziel der ersten Phase ist die Festlegung des Betrachtungsgegenstandes. Dieser bildet im Kern die **Bedrohungslage** für das zu entwickelnde System ab. Es wird angenommen, dass es sich bei dem Entwicklungsgegenstand um eine Neuentwicklung handelt und demzufolge die Modelle und Analysen neu erarbeitet werden müssen.

Zur Identifizierung von Bedrohungen existieren bereits eine Vielzahl an Analysen (vgl. z. B. [LMP+12b, S.105ff.], [Mei11, S.98ff.], [Gri14, S.72ff.], [Kok13, S.90ff.] und [SSM10, S.34ff.]). Alle diese Analysen haben gemein, dass sie relativ aufwändig sind und nicht auf bestehenden Artefakten aufbauen. Darüber hinaus beziehen sie sich meist allgemein auf die Bedrohungssituation eines ganzen Unternehmens. Zusätzlich entwickelt GRIGORI eine präventive Risikoanalyse und nennt Bewertungskriterien zur Identifikation potentieller Angriffspunkte am Originalprodukt (vgl. [Gri14, S.73ff.]). Allerdings beziehen sich diese Kriterien auf bereits fertig entwickelte Produkte.

Mit geringem Aufwand lässt sich bereits während der Erstellung der ersten Partialmodelle die individuelle Bedrohungslage eines Systems identifizieren. Die Modelle zur Analyse des Systems sind für den Produktschutz zu verwenden. So können relevante Aspekte untersucht und beschrieben werden. In dieser Phase werden die Partialmodelle Umfeld, Anwendungsszenarien und Anforderungen zur Unterstützung des präventiven Systemschutzes verwendet.

Zur Übersicht potentieller Imitatoren werden zunächst die Einflüsse aus dem **Umfeldmodell** identifiziert. Ziel ist die Analyse der externen Einwirkungen auf das System. Zur Zielerreichung wird das Umfeldmodell um Imitatoren (wie Produktpiraten, Wettbewerber) sowie offene Schnittstellen erweitert. In der Darstellung werden die Elemente hervorgehoben, die mit den Imitatoren in Kontakt stehen. Dies wird als *Imitationssicht* definiert (vgl. Kap. 5.1.1, Bild 5-2). Mit Flussbeziehungen werden die Wechselwirkungen (z. B. Angriffsmöglichkeiten auf das System) dargestellt. Die Kompetenzen der Angreifer werden durch die Klassifizierung der Imitatoren (vgl. Kap. 4.4.2) visualisiert. Auf Basis von **Anwendungsszenarien** sind Angriffs- sowie Abwehrszenarien zu erstellen. Diese beschreiben das gewünschte Systemverhalten im Falle eines Angriffs. Abschließend werden die **Anforderungen** erweitert. Auf Grundlage der abgeleiteten Er-

kenntnisse werden die bedeutsamen Schutzanforderungen an das System spezifiziert. Grundlage für die Identifikation sind die in Kapitel 4.2 erarbeiteten Schutzanforderungen Intelligenter Technischer Systeme. Zur Unterstützung der Entwickler wurde eine Checkliste erarbeitet (vgl. Kap. 4.2). Diese kann als Vorlage für die Auswahl und Spezifikation der relevanten Schutzanforderungen verwendet werden.

Zusammenfassend werden in der ersten Phase folgende **Hilfsmittel** eingesetzt:

- Checkliste für die Schutzanforderungen Intelligenter Technischer Systeme (vgl. Kap. 4.2, Tabelle 4-1). Die vollständige Checkliste ist im Anhang A5.4 abgebildet.
- Spezifikationstechnik CONSENS (vgl. Kap. 3.3.1)

Das **Resultat** der Phase *Problemanalyse* ist die Bestimmung des Betrachtungsgegenstands. Dieser umfasst im Kern die individuelle Bedrohungslage des zu entwickelnden Systems. Die Ansprüche und Erwartungen an den Schutz des Systems werden in Form einer Anforderungsbeschreibung dokumentiert.

4.5.2 Phase 2: Schutzfunktionsidentifikation

Hier werden die **Schutzfunktionen** des zu entwickelnden Systems identifiziert. Schutzfunktionen sind Nebenfunktionen des Systems und für den Schutz notwendig. Sie schützen das System vor Angriffen und erschweren so den Imitationsprozess. Die Funktionsbeschreibung stellt den Übergang der Analyse zur Synthese des zu entwickelnden Systems dar und ermöglicht die erste Konkretisierung der Schutzaspekte.

Die relevanten Schutzfunktionen sind in die Funktionshierarchie des Gesamtsystems zu integrieren. Die Schutzfunktionen spezialisieren die Hauptfunktion *System schützen* mit Hilfe von Teilfunktionen. Die Spezialisierung ist solange fortzusetzen, bis für die Schutzfunktionen auf der untersten Ebene Lösungen in Form von Schutzmustern gefunden werden können. Die Übersicht der Schutzfunktionen beinhaltet keine Aussagen über die Zusammenhänge zwischen den Funktionen. Dies ermöglicht eine lösungsneutrale Dokumentation. Auf dieser Grundlage kann das volle Innovationspotential in der anschließenden Lösungsfindung ausgenutzt werden.

Zur Unterstützung der Erarbeitung der Schutzfunktionen wird eine entsprechend vorstrukturierte Übersicht der Standard-Schutzfunktionen präventiv geschützter Intelligenter Technischer Systeme entwickelt (vgl. Kap. 5.1.2, Bild 5-5). Diese erleichtert den Entwicklern die Identifikation der wesentlichen Schutzfunktionen. Basierend auf den Schutzfunktionen werden in der folgenden Phase passende Schutzmuster identifiziert.

Die Schutzfunktionsbeschreibung ist für die Suche nach relevanten Lösungen in Form von Schutzmustern von entscheidender Bedeutung, da während der nachfolgenden Schutzauswahl (Phase 3) die Suche nach erfolgsversprechenden Lösungen auf Basis der Schutzfunktionsbeschreibung realisiert wird.

Zusammenfassend werden in der zweiten Phase folgende **Hilfsmittel** eingesetzt:

- Übersicht der Standard-Schutzfunktionen präventiv imitationsgeschützter Intelligenter Technischer Systeme (vgl. Kap. 5.1.2, Bild 5-5)
- Spezifikationstechnik CONSENS (vgl. Kap. 3.3.1)

Das **Resultat** der Phase *Schutzfunktionsidentifikation* ist die Erarbeitung der Aufgabenbeschreibung. Diese besteht hauptsächlich aus den Schutzfunktionen. Für die Auswahl der Schutzmuster wird diese durch die bereits erstellte Checkliste für die Schutzanforderungen Intelligenter Technischer Systeme ergänzt.

4.5.3 Phase 3: Schutzauswahl

In der dritten Phase wird die Suche und Auswahl von Schutzmustern forciert. Ausgehend von den Schutzanforderungen werden wirksame Schutzmuster identifiziert. Die Übersicht der wirksamsten Schutzmuster definiert die zur Verfügung stehenden Lösungen und bilden die Grundlage der Auswahl (vgl. Kap 4.3.2.5).

In der Funktionshierarchie des Gesamtsystems werden Lösungen für die einzelnen Funktionen gesucht. Den Schutzfunktionen werden Lösungen in Form von Schutzmustern zugeordnet. Für die Suche werden zwei generelle Suchstrategien unterschieden – Top-Down oder Bottom-Up. Die **Top-Down-Strategie** verfolgt das Ziel, möglichst schnell Schutzmuster für die übergeordneten Schutzfunktionen zu finden. So soll effizient der wirksame Schutz für die vorliegende Entwicklungsaufgabe identifiziert werden. Dementsprechend startet die Suche bei der Hauptschutzfunktion. Wird kein passendes Schutzmuster gefunden, wird die Suche auf die weiteren Spezialisierungsebenen der Funktion erweitert. Diese werden nacheinander durchlaufen. Die **Bottom-Up-Strategie** verfolgt das Ziel, elementare Schutzmuster zu identifizieren. Dies bietet sich an, wenn für ein System alternative Lösungen für den Schutz betrachtet werden sollen. Folgerichtig startet die Suche auf der untersten Ebene der Spezialisierung und fokussiert Lösungsalternativen für die einzelnen Teilschutzfunktionen [ABG+14, S.157].

Basierend auf den Schutzfunktionen werden Lösungen in Form wirksamer Schutzmuster für die einzelnen Funktionen identifiziert. Einzelne Schutzmuster reichen häufig für den Systemschutz nicht aus. In dieser Phase sind daher auch alternative oder ergänzende Schutzlösungen zu identifizieren. Daher ist die Bottom-Up-Strategie die geeignete Suchmethode. Durch diese werden verschiedene Schutzmuster identifiziert. Die Expertise der Entwickler ermöglicht die Auswahl der Schutzmuster, die am wirksamsten für die jeweilige Bedrohungslage sind. Dies kann z. B. durch die Klassifizierung der Imitatoren und die Erfüllung der Schutzanforderungen analysiert werden.

Kann für eine Schutzfunktion kein Schutzmuster gefunden werden, sind neue Ansätze zu erarbeiten. Die Phasen 1-3 können beliebig oft iterativ durchlaufen werden. Pro

Durchlauf ist der Betrachtungsgegenstand und die Aufgabenbeschreibung zu konkretisieren, umso zunehmend detailliertere Lösungen zu identifizieren (vgl. Kap 4.4.4).

Zusammenfassend werden in der dritten Phase folgende **Hilfsmittel** eingesetzt:

- Übersicht der wirksamsten Schutzmaßnahmen für ITS (vgl. Kap 4.3.2.5)
- Schutzmuster für ITS (vgl. Kap. 4.4)
- Morphologischer Kasten [PBF+07]

Das **Resultat** der Phase *Schutzauswahl* ist ein morphologischer Kasten, der wirksame Schutzmuster beinhaltet. Diese werden den Schutzfunktionen gegenübergestellt.

4.5.4 Phase 4: Systemspezifikation

Die Partialmodelle Wirkstruktur und Verhalten beschreiben die Spezifikation des zu entwickelnden Systems und ermöglichen eine erste Konkretisierung. Während der Erstellung der **Wirkstruktur** müssen die ausgewählten Schutzmuster berücksichtigt werden, um so die Integration der Aspekte des Schutzes in das System sicherzustellen. Die Erweiterung der Wirkstruktur durch die Schutzmuster stellt eine konkrete Spezifikation des präventiv geschützten Systems dar. Mit Hilfe der Flussbeziehungen werden die Wechselwirkungen zwischen den Schutzmustern und den Systemelementen sowie der Schutzmuster untereinander dargestellt. Hierbei bietet es sich an, die Wirkstruktur in Kombination mit den Umfeldelementen darzustellen. Die so entstandene Systemstruktur ermöglicht die Visualisierung der Auswirkungen von Angriffen. Die Sichtenbildung lässt die gefilterte Darstellung zu, z. B. auf die Auswirkungen einzelner Angriffe. So wird die Komplexität verringert und der Systemschutz fokussiert.

Im Partialmodell **Verhalten** wird das Systemverhalten im Falle eines Angriffs modelliert. Das Modell Gestalt dient zur Entwicklung der äußeren Form, welche in der Regel mittels CAD-Systemen erstellt wird. Da der Systemschutz unabhängig von der äußeren Gestalt des Systems wirken soll und diese in den frühen Phasen der Entwicklung oft noch unbekannt ist, wird das Partialmodell bei der weiteren Betrachtung vernachlässigt.

Zusammenfassend werden in der vierten Phase folgende **Hilfsmittel** eingesetzt:

- Spezifikationstechnik CONSENS (vgl. Kap. 3.3.1)
- Informationen aus den Schutzmustern

Das **Resultat** der abschließenden Phase *Systemspezifikation* ist eine disziplinübergreifende Spezifikation der Prinziplösung eines präventiv geschützten Intelligenten Technischen Systems. Dieses Vorgehen ist nun während der Entwicklung immer wieder zu durchlaufen. Die Lösungen sollten kontinuierlich konkretisiert werden.

4.5.5 Einordnung in den Systementwurf

Das Vorgehen zur Integration des Schutzes in den musterbasierten Entwurf Intelligenter Technischer Systeme ist ergänzend zum klassischen Systementwurf im Sinne der VDI 2206 anzuwenden.

Für den Entwurf Intelligenter Technischer Systeme hat sich das lösungsmusterbasierte Vorgehen nach ANACKER als besonders geeignet erwiesen (vgl. Kap. 3.5.4). Aus diesem Grund ordnet sich das Vorgehensmodell aus Bild 4-10 in den lösungsmusterbasierten Systementwurf ein.

In Bild 4-11 ist auf der linken Seite der lösungsmusterbasierte Entwurf nach ANACKER vereinfacht dargestellt (vgl. Bild 3-16). Die vier Phasen des Vorgehensmodells zur Integration des Schutzes in den musterbasierten Entwurf Intelligenter Technischer Systeme und deren Methoden bzw. Hilfsmittel sind auf der rechten Seite abgebildet. Mit den roten Pfeilen wird die Integration visualisiert. Folgend ist die Einordnung für jede Phase des Vorgehens beschrieben.

Problemanalyse: In dieser Phase wird der Betrachtungsgegenstand erweitert. Entstehende Artefakte werden genutzt, um die Bedrohungslage des zu entwickelnden Systems abzubilden. Aus dem Umfeldmodell können Angriffsmöglichkeiten auf das System identifiziert und abgebildet werden. Hieraus ergeben sich Anwendungsszenarien. Mit diesen kann das gewünschte Verhalten des Systems z. B. bei einem Angriff, beschrieben werden. Darüber hinaus werden die Anforderungen durch die Schutzanforderungen Intelligenter Technischer Systeme ergänzt (vgl. Kap. 4.2, Tabelle 4-1).

Schutzfunktionsidentifikation: Durch die Integration von Schutzfunktionen in die Funktionshierarchie des zu entwickelnden Systems, wird die funktionale Systembeschreibung erweitert.

Schutzauswahl: Nun werden den Funktionen Lösungen zugeordnet. Für die Schutzfunktionen werden Lösungen in Form von Schutzmustern gesucht. Die Auswahl der Lösungen wird mit einem morphologischen Kasten vorgenommen.

Systemspezifikation: Auf Grundlage der Wirkstruktur und des Systemverhaltens wird der Schutz des Systems in die Prinziplösung integriert. Die Prinziplösung ist das Ergebnis des Entwurfs und dient als Ausgangspunkt für die fachdisziplinspezifische Ausarbeitung.

Die Validierung der erarbeiteten *Entwurfssystematik für den präventiven Schutz Intelligenter Technischer Systeme vor Produktpiraterie* ist Gegenstand des folgenden Kapitels. Anhand eines praktischen Beispiels wird das Vorgehensmodell durchlaufen und angewendet.

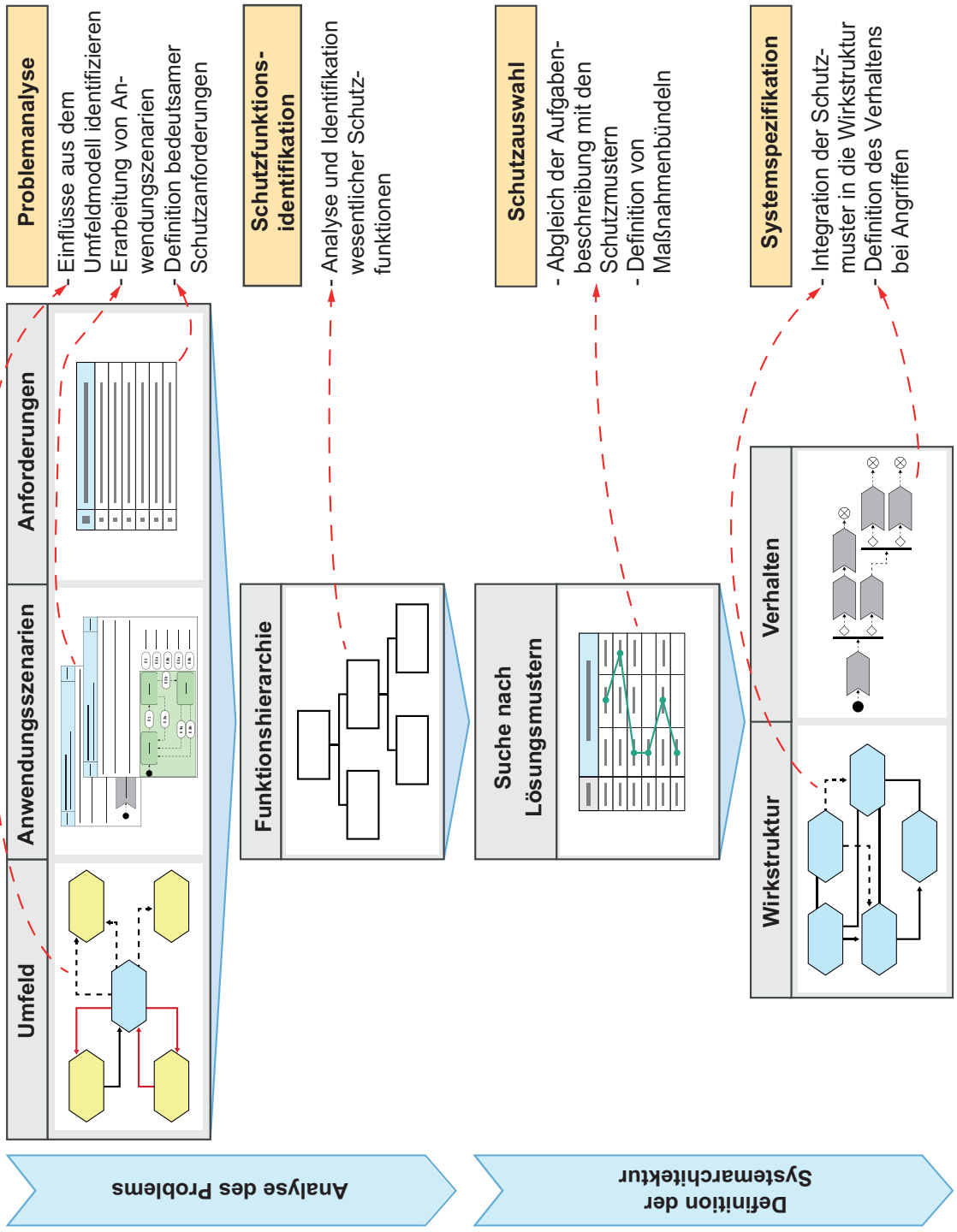


Bild 4-11: Integration des Schutzes in den musterbasierten Entwurf nach ANACKER

5 Anwendung und Bewertung

In diesem Kapitel wird die entwickelte *Entwurfssystematik für den präventiven Schutz Intelligenter Technischer Systeme vor Produktpiraterie* anhand eines Anwendungsbeispiels validiert. Kern der Systematik ist das erarbeitete *Vorgehensmodell zur Integration des Schutzes in den musterbasierten Entwurf Intelligenter Technischer Systeme* (vgl. Kap. 4.5). Dieses Vorgehen greift die Ergebnisse der vorherigen Kapitel auf. In Kapitel 5.1 wird es beispielhaft durchlaufen und somit validiert. In Kapitel 5.2 findet der Abgleich der Entwurfssystematik mit den in Kapitel 2.6 aufgestellten Anforderungen statt.

5.1 Anwendung des Vorgehens am Beispiel eines Mähdreschers

Die Validierung des Vorgehens wird in Zusammenarbeit mit CLAAS durchgeführt. Die von der CLAAS Gruppe produzierten Landmaschinen entwickeln sich zunehmend zu intelligenten und vernetzten Systemen. Mit Hilfe der Digitalisierung werden Landmaschinen zu mobilen Rechensystemen weiterentwickelt, mit Sensoren ausgestattet und mit Informationen weiterer Systeme verknüpft. So werden in Echtzeit Ernteerträge gemessen, Kraftstoffverbräuche optimiert, Unkraut erkannt und darüber hinaus, basierend auf Daten des Ackers, Düngeempfehlungen ausgesprochen. Die Kommunikation erfolgt von Maschine zu Maschine (M2M). Zusätzliche Daten wie Getreidequalität und -menge oder Wetterdaten und Kraftstoffverbrauch werden von den Systemen untereinander ausgetauscht, um so den optimalen Einsatz der Maschinen zu gewährleisten und den Bediener größtmöglich zu unterstützen [Wil14-ol], [IKT16-ol].

Laut VDMA sind 90 Prozent der Unternehmen im Bereich der Landtechnik von Produktpiraterie betroffen [VDM16, S.16]. Insbesondere einzelne Komponenten[50] stehen seit Jahren im Fokus von Imitatoren und Wettbewerbern und werden am häufigsten plagiiert [VDM16, S.17]. Das Geschäft mit Komponenten, wie Ersatz- und Verschleißteile, ist für CLAAS besonders ertragreich. Aus diesem Grund ist das Ziel der Validierung der präventive Schutz der originalen Komponenten und damit die Sicherstellung des unternehmerischen Erfolgs von CLAAS.

Innerhalb der CLAAS Gruppe ist die CLAAS Service and Parts GmbH (CSP) für Komponenten verantwortlich. Das Ziel der CSP ist die hohe Qualität und Zuverlässigkeit der Produkte auch im Bereich After-Sales sicherzustellen. Die CSP beschäftigt sich daher neben dem Servicegeschäft auch mit dem ganzheitlichen Ansatz der Entwicklung von After-Sales-Produkten und -Lösungen. Die CSP vertritt bereits bei der Entwicklung der Maschinen ihre relevanten Interessen.

---

[50] CLAAS definiert eine Komponente wie folgt: *„Eine Komponente stellt in Bezug auf die Produktstruktur einen Teil des Produktes (Hard- oder Software) dar. Eine Komponente kann sowohl ein Teil als auch eine Baugruppe sein. In Bezug auf die Softwarekomponenten wird nicht weiter unterschieden."*

Bild 5-1: Schnittbild des CLAAS Mähdreschers LEXION 780 mit VARIO Schneidwerk [Cla16]

Im Rahmen der Validierung soll der Schutz von Komponenten einer neuen Generation eines Mähdreschers umgesetzt werden. Ein Mähdrescher ist eine landwirtschaftliche Maschine, welche die Ernte der Körnerfrüchte von Nutzpflanzen (z. B. Getreide) ermöglicht. Der Mähdrescher ist in der Lage mehrere Verfahrensschritte in einem Arbeitsgang zu erledigen, insbesondere das Mähen, Dreschen und Separieren der Körnerfrüchte. Der CLAAS Mähdrescher LEXION 780 ist beispielhaft in Bild 5-1 im Schnittbild dargestellt. Der Mähdrescher wird immer in Kombination mit einem Vorsatzgerät (hier einem Schneidwerk) betrieben, da dieser seine Funktion sonst nicht erfüllen kann. Das Schneidwerk wird zur Ernte vor dem Mähdrescher angebracht, damit das Erntegut geschnitten, in den Mähdrescher befördert und dort weiterverarbeitet werden kann. Das Vorsatzgerät wird als Subsystem integrativ zum Mähdrescher entwickelt. Die grundlegende Funktion des Schneidwerks ist das Schneiden, Aufnehmen und Zusammenführen des Erntegutes (vgl. [Ren95, S.782f.], [BW06]).

Für die Validierung der vorliegenden Arbeit wird ein VARIO Schneidwerk betrachtet (vgl. Bild 5-1). Im Folgenden werden die einzelnen Phasen des Vorgehensmodells aus Kapitel 4.5 durchlaufen.

5.1.1 Phase 1: Problemanalyse

In der Problemanalyse werden zunächst die Einflüsse aus dem **Umfeldmodell** des CLAAS Mähdreschers untersucht. Ein Mähdrescher ist als Verbund mehrerer Subsysteme zu verstehen. So ist z. B. das Schneidwerk ein individuelles System, das mit unterschiedlichen Mähdreschertypen gekoppelt werden kann. Das Umfeldmodell wird während der Erarbeitung um Imitatoren erweitert. Das Ziel ist die Identifikation von Bedrohungen und Angriffsmöglichkeiten. Die Sichtenbildung unterstützt die Fokussierung auf den Systemschutz. Relevante Elemente sowie deren Beziehungen stehen im Vordergrund. Die für den Schutz weniger wichtigen Elemente werden optisch in den Hintergrund gerückt. So bleibt die Vollständigkeit des Modells erhalten, zugleich wird die Übersichtlichkeit deutlich erhöht. Das Umfeldmodell des Mähdreschers in der Imitationssicht ist in Bild 5-2 dargestellt.

Aus den Informationen des Umfeldmodells sowie aus bisherigen Erfahrungen konnte das zu entwickelnde Schneidwerk als das System identifiziert werden, welches die größte Imitationsgefahr aufweist. Dies liegt an der hohen Anzahl von Ersatz- und Verschleißteilen. Die Teile und Komponenten entlang des Gutflusses müssen regelmäßig gewartet und getauscht werden. Somit ist das Schneidwerk sehr wartungsintensiv und muss einfach zugänglich sein. Die Wartung wird oft von Servicepartnern durchgeführt. Darüber hinaus ist das Service- und Wartungsgeschäft sehr profitabel, weshalb hier ein großer Konkurrenzkampf herrscht. Zusätzlich sind zahlreiche Komponenten des Schneidwerks verhältnismäßig einfache Produkte wie die Schneidmesser. Diese sind leicht zu imitieren, haben eine hohe Absatzmenge und versprechen somit einen großen Gewinn für die Imitatoren. Deshalb ist es naheliegend, dass das Schneidwerk sowie dessen Komponenten einer hohen Imitationsgefahr ausgesetzt sind. Daher wird dieses System für die Validierung detailliert betrachtet.

Das Schneidwerk erfasst mittels Sensoren seine Umgebung, kommuniziert mit anderen Systemen (wie dem Mähdrescher), passt sich den aktuellen Begebenheiten autonom an und stellt Informationen über aktuelle Betriebsbedingungen bereit. Die Unterstützung des Fahrers steht im Fokus. So ist über eine Laserabtastung unterstützt durch GPS-Daten ein elektronisch-optisches Lenksystem entwickelt worden. Mit diesem wird die automatische Lenkung entlang der Bestandskante realisiert. Die Fahrerunterstützung wird weiter durch das Selbstoptimierungssystem CEMOS AUTOMATIC verbessert. Dieses stellt eine den jeweiligen Erntebedingungen angepasste Maschinenoptimierung sicher. So werden optimale Ernteergebnisse und Maschineneffizienz erreicht. Es werden bis zu 50 verschiedene Parameter wie Rotordrehzahl, Rotorklappenstellung, Gebläsedrehzahl, Obersieb- und Untersieböffnung sowie die dazu passende Fahrgeschwindigkeit den aktuellen Gegebenheiten angepasst. Das System nutzt Informationen, die vom Mähdrescher, vom Schneidwerk und anderen Subsystemen aufgenommen werden, und passt die Parameter des gesamten Erntesystems optimal und kontinuierlich an. Es können unterschiedliche Optimierungsstrategien gefahren werden: Maximaler Durchsatz, minimaler Kraftstoffeinsatz, hohe Druschqualität etc. [Cla16].

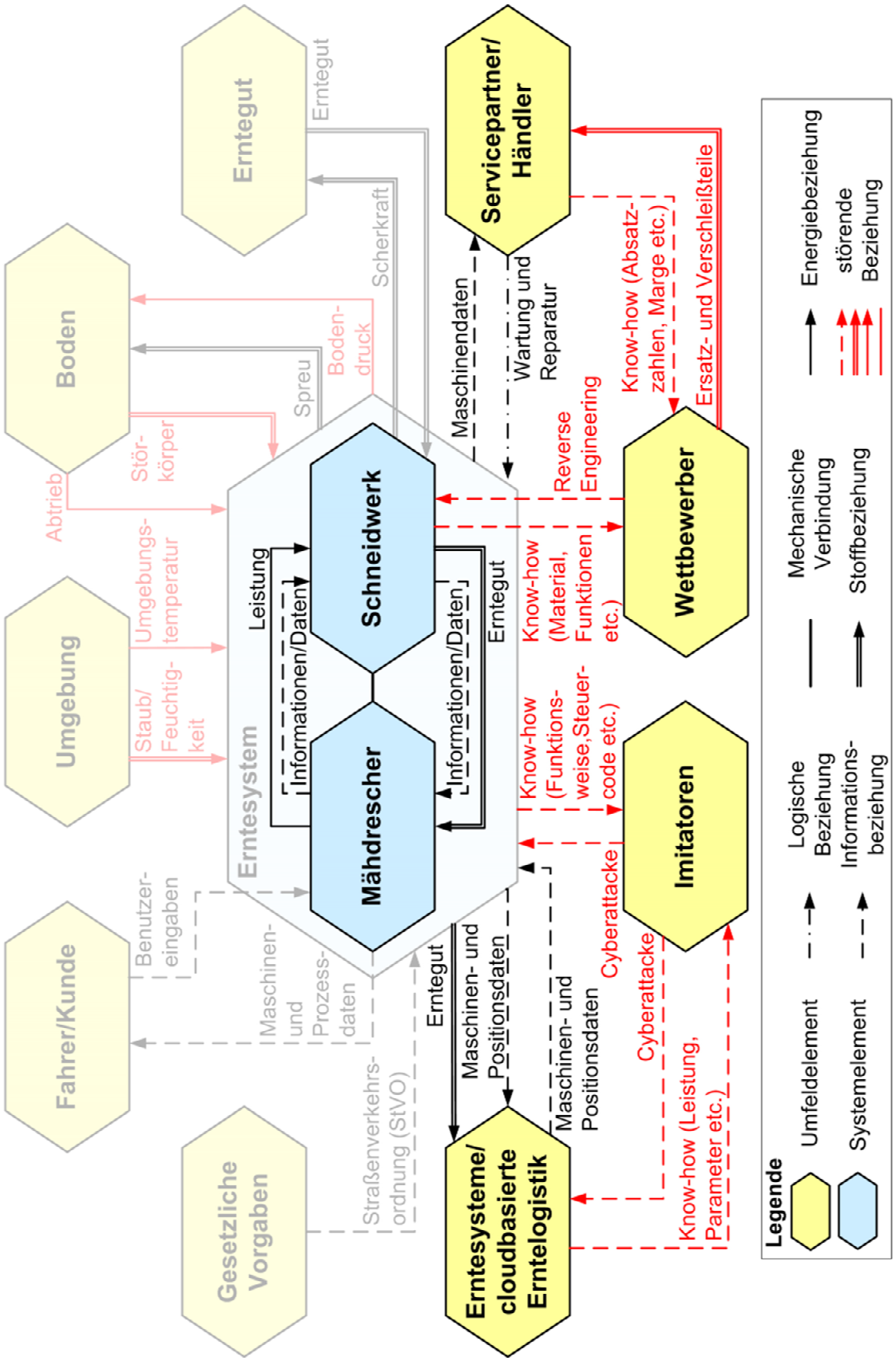


Bild 5-2: Imitationssicht auf das Umfeldmodell eines Erntesystems bestehend aus Mähdrescher und Schneidwerk

Das Erntesystem kommuniziert darüber hinaus mit der cloudbasierten Erntelogistik. So wird ein effizientes und intelligentes Flottenmanagement erreicht. Hierdurch kann bspw. das Zusammenspiel des Mähdreschers und des Traktors mit Überladewagen beim Entleeren des Korntanks optimiert werden [Tel16-ol].

In der Steuerung des Schneidwerks laufen die Informationen zusammen, werden ausgewertet und an den Mähdrescher kommuniziert. Die Steuerung ist demnach für die Umsetzung innovativer Funktionen besonders wichtig und ermöglicht einen Wettbewerbsvorsprung. Gelangen die Imitatoren z. B. an den Quellcode der Steuerung, können die Alleinstellungsmerkmale des Originalherstellers schnell imitiert werden. Aus diesem Grund ist die Steuerung des Schneidwerks besonders durch Angriffe bedroht.

Auf Grundlage des Umfeldmodells konnten zwei potentielle Gruppen von Imitatoren identifiziert werden. Hierzu zählen die legalen Wettbewerber sowie die illegalen Imitatoren. In Workshops mit Experten von CLAAS konnten die Indikatoren zur Bewertung der Kompetenzen ermittelt sowie deren Ausprägungen eingestuft werden. Hieraus werden die Kompetenzen abgeleitet (vgl. Tabelle 4-9). Diese sind durch die **Klassifizierung der Imitatoren** in Bild 5-3 visualisiert.

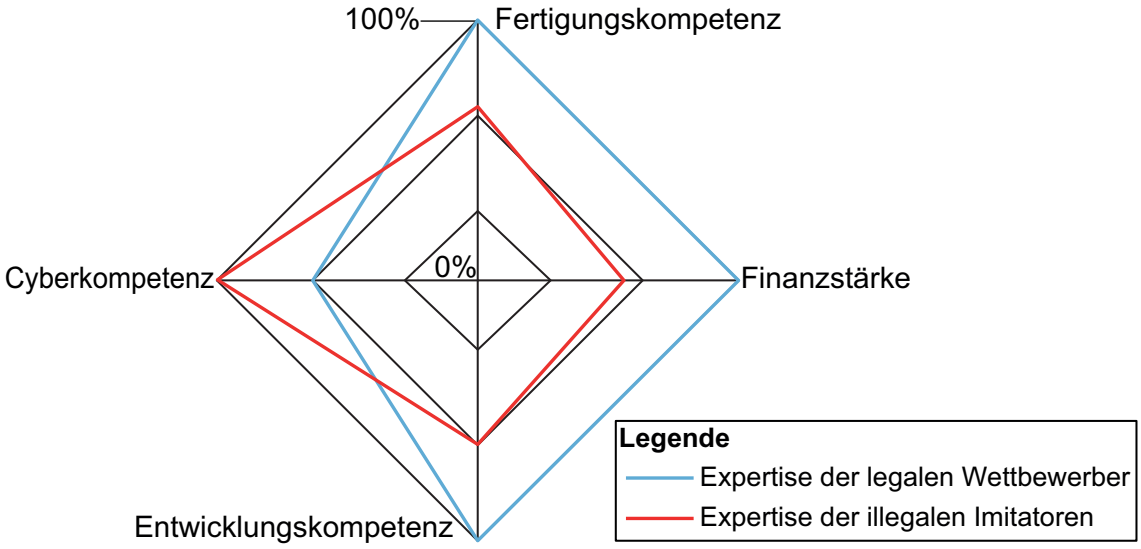


Bild 5-3: Klassifizierung der Wettbewerber und Imitatoren

Auf Basis der Klassifizierung kann ausgeschlossen werden, dass **legale Wettbewerber** die Steuerungssoftware angreifen und imitieren. Dieser Angriff könnte z. B. über den Angriff auf die Kommunikationsschnittstellen erfolgen. Hierfür muss ausreichend Cyberkompetenz vorhanden sein und zusätzlich erhebliche kriminelle Energie aufgebracht werden. Die Wettbewerber entwickeln eigene Lösungen und konzentrieren sich auf den Verkauf der ertragreichen Ersatzteile und Komponenten entlang des Gutflusses.

Die **illegalen Imitatoren** wie Produktpiraten imitieren die Ersatzteile und versuchen so einen größtmöglichen Gewinn zu erzielen. Unter der mangelnden Qualität leidet vor

allem der Kunde, da er mit erhöhten Stillstandzeiten der Maschine rechnen muss. Kann der Kunde die Imitate nicht vom Original unterscheiden, so leidet auch das Image des Originalherstellers (vgl. Kap. 2.3). Darüber hinaus haben die Imitatoren großes Interesse an dem Know-how, welches in der Steuerung vorhanden ist. Durch die sehr hohe Cyberkompetenz besitzen sie die Möglichkeit diese anzugreifen und auszulesen. Aus den extrahierten Informationen können die Imitatoren zusätzliches Know-how erlangen und haben die Möglichkeit Komponenten oder in Zukunft ganze Maschinen zu imitieren und sich zum legalen Wettbewerber zu entwickeln.

Anhand der Informationen aus dem Umfeldmodell können denkbare Angriffe und mögliche Abwehrmaßnahmen in Form von **Anwendungsszenarien** dokumentiert werden. Beispielhaft sind die Szenarien *Cyberattacke auf die Steuerungssoftware* und *Verwendung von Originalkomponenten* in Bild 5-4 abgebildet.

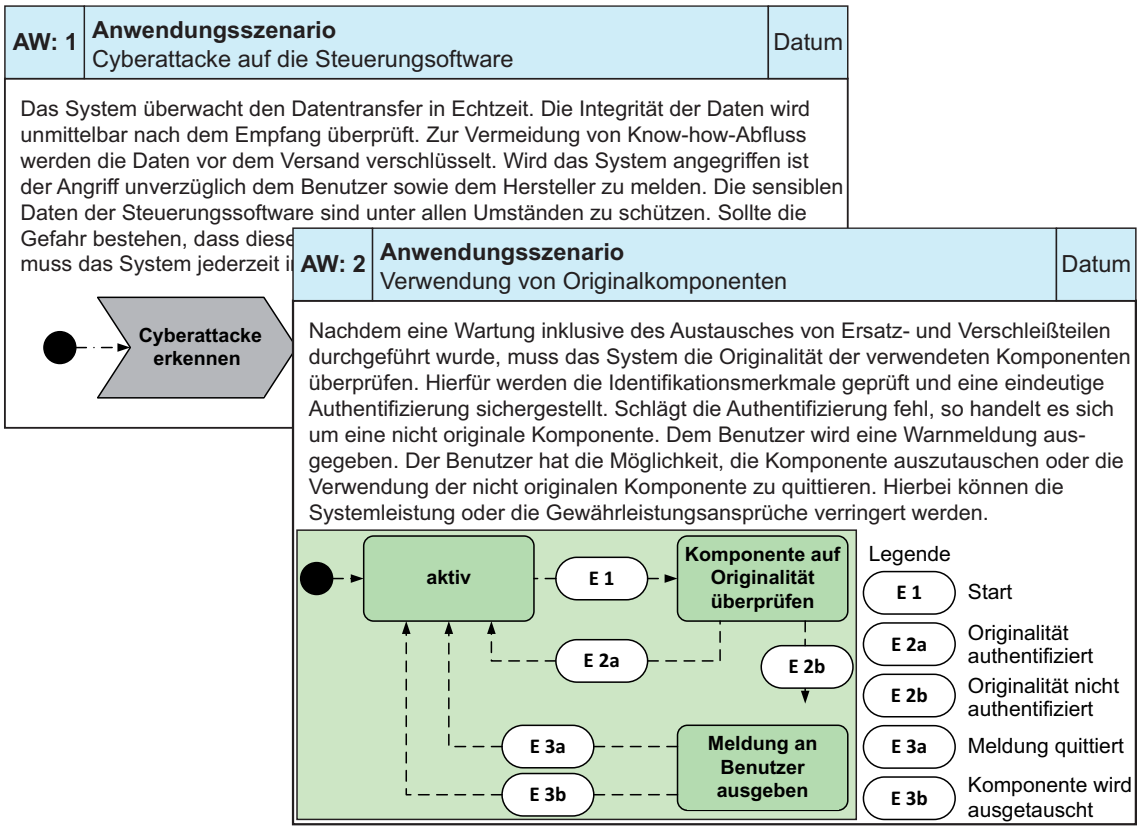


Bild 5-4: Beispielhafte Anwendungsszenarien des Schneidwerks für Angriffs- und Abwehrsituationen

Ein Anwendungsszenario ist eine Cyberattacke auf die Steuerungssoftware des Schneidwerks. Durch Servicezugänge, Schnittstellen zum Mähdrescher oder ungesicherte Kommunikationsverbindungen können Angreifer die Funktionalität der Software auslesen. Für einen wirksamen Schutz muss der Know-how-Abfluss durch Cyberattacken verhindert werden. Eine mögliche Lösung ist die Überwachung des Systems. So werden Angriffe erkannt und Gegenmaßnahmen eingeleitet. Ein weiteres Anwendungs-

szenario ist die ausschließliche Verwendung originaler Ersatzteile und Komponenten. Diese Anwendung kann mit der gegenseitigen Authentifizierung realisiert werden.

Auf Grundlage der Informationen aus dem Umfeld und den Anwendungsszenarien können die Anforderungen des Mähdreschers ergänzt werden. Hierbei unterstützt die erarbeitete Checkliste der Schutzanforderungen Intelligenter Technischer Systeme (vgl. Kap. 4.2, Tabelle 4-1).

Auf Basis der erarbeiteten Checkliste wurden die Schutzanforderungen diskutiert und zahlreiche für relevant erachtet. Bis auf die Selbstoptimierung der Schutzmaßnahmen (8.6) wurden alle ITS-spezifischen Schutzanforderungen in die Anforderungsliste übernommen. Die Weiterentwicklung der Fähigkeit zur Selbstoptimierung des Schneidwerks ist für CLAAS relevant, jedoch wird die autonome Optimierung des Schutzes nicht weiter verfolgt. Eine mögliche Selbstoptimierung der eingesetzten Schutzmuster wird ggf. in zukünftigen Entwicklungen aufgegriffen.

5.1.2 Phase 2: Schutzfunktionsidentifikation

In dieser Phase stehen die Schutzfunktionen des Systems im Vordergrund. Aufbauend auf den Informationen aus der ersten Phase wird eine Übersicht der Standard-Schutzfunktionen präventiv geschützter Intelligenter Technischer Systeme erarbeitet. Diese ist in Bild 5-5 visualisiert und steht exemplarisch für die Spezifikation der Schutzfunktionen eines präventiv geschützten Intelligenten Technischen Systems.

Aufgrund der abstrakten Beschreibung der Schutzfunktionen können die Standard-Schutzfunktionen ebenso auf andere Systeme übertragen werden. Die Hauptfunktion ist *System schützen*. Diese wird spezialisiert durch die Teilfunktionen *Rechtsschutz sicherstellen, Herkunftsnachweis erbringen* und *Imitation erschweren*.

Das Thema Rechtsschutz wird in der vorliegenden Arbeit nicht weiter betrachtet (vgl. Kap. 2.1). Der Herkunftsnachweis ist sowohl für die Steuerung des Schneidwerks (insbesondere für den Quellcode) als auch für die bedrohten Ersatzteile und Komponenten relevant. Die Funktion *Herkunftsnachweis erbringen* spezialisiert sich in zwei weitere Teilfunktionen: *Originalität kennzeichnen* und *Originalität überprüfen*. Für die Originalitätskennzeichnung ist zu beachten, dass sie imitationssicher zu gestalten ist. Darüber hinaus soll das System in der Lage sein, die Originalität der Komponenten zu überprüfen und ggf. Fremdkomponenten abzuweisen. So können Imitate abgewiesen oder zumindest als solche identifiziert werden. Auf dieser Grundlage kann die Systemleistung gedrosselt oder der Benutzer auf den Verfall der Garantieansprüche hingewiesen werden.

Die Zulässigkeit solcher Schutzmuster ist bereits frühzeitig zu überprüfen. Je nach geltendem Recht sind Gesetze gegen unlauteren Wettbewerb und gegen Wettbewerbsbeschränkungen sowie Kartellbestimmungen zu berücksichtigen.

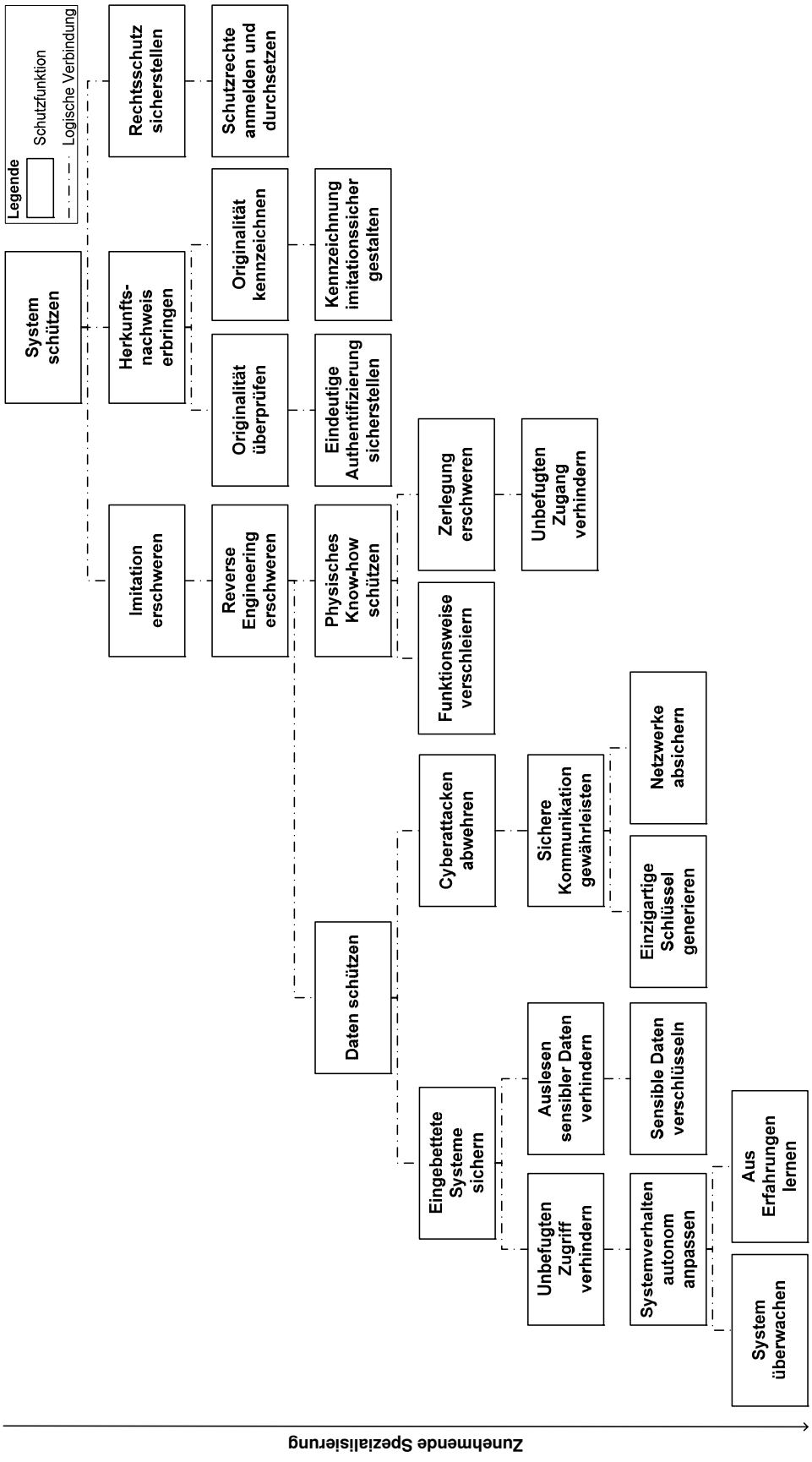


Bild 5-5: Übersicht der Standard-Schutzfunktionen präventiv geschützter Intelligenter Technischer Systeme

Zur Abwehr von Imitationen muss die Funktion *Reverse Engineering erschweren* erfüllt werden. Diese ist insbesondere für die Ersatzteile und Komponenten relevant. Die Funktion unterteilt sich weiter in *physisches Know-how schützen* und *Daten schützen* (vgl. Kap. 2.3.3). Um das physische Know-how des Systems (hier insbesondere der Ersatzteile und Komponenten) zu schützen, sind die Unterfunktionen *Funktionsweise verschleiern* und *Zerlegung erschweren* zu erfüllen. Die Zerlegung des Systems wird erschwert, indem der Zugang für Unbefugte verhindert wird. Am Beispiel des Schneidwerks dürfen die Zugänge zu sensiblen Komponenten nur durch autorisiertes Personal geöffnet werden.

Die Funktion *Daten schützen* ist besonders relevant für den Schutz der Steuerung. Zum Schutz der Daten ist die Funktion Cyberattacken abwehren zu erfüllen. Hierfür ist *sichere Kommunikation gewährleisten* eine wichtige Funktion. Zur Erfüllung der Funktion müssen einzigartige Schlüssel generiert und Netzwerke abgesichert werden. Der Datenschutz wird weiter verfeinert in die Funktion *Eingebettete Systeme sichern*. Eingebettete Systeme (hier die Steuereinheit) bilden den Kern Intelligenter Technischer Systeme. Daher muss das Auslesen sensibler Daten verhindert werden.

Dies wird mit der Funktion *sensible Daten verschlüsseln* realisiert. Darüber hinaus müssen die Systeme vor unbefugtem Zugriff geschützt werden. Voraussetzung ist die autonome Anpassung des Systemverhaltens. Hierfür sind die Funktionen *System überwachen* und *aus Erfahrungen lernen* zu verwirklichen.

Die Übersicht der Standard-Schutzfunktionen dient als Vorlage für präventiv geschützte ITS. Sie erhebt keinen Anspruch auf Vollständigkeit und ist individuell anzupassen. Die relevanten Schutzfunktionen müssen zusätzlich zur Funktionshierarchie des Gesamtsystems betrachtet werden und sind in diese als Nebenfunktionen zu integrieren. Zusammen mit den Anwendungsszenarien sowie den Schutzanforderungen bilden die Schutzfunktionen die Grundlage zur Auswahl der Schutzmuster. Dies ist Gegenstand der folgenden Phase.

5.1.3 Phase 3: Schutzauswahl

Für das Gesamtsystem werden in der dritten Phase passende Lösungen auf Basis der Funktionen gesucht. In der vorliegenden Arbeit steht die Auswahl passender Schutzmuster im Fokus. Grundlage sind die identifizierten wirksamen Schutzmaßnahmen für den präventiven Schutz Intelligenter Technischer Systeme (vgl. Kap 4.3.2.5). Den Schutzfunktionen (Bild 5-5) werden Lösungen in Form von Schutzmustern zugeordnet. Die Suche startet bei der untersten Spezialisierungsebene. Aufgrund der Tatsache, dass die Schutzanforderung Selbstoptimierung der Schutzmaßnahmen (8.6) von CLAAS als nicht relevant betrachtet wurde, werden die Schutzfunktion *Systemverhalten autonom anpassen* sowie die zugehörigen Teilfunktionen nicht weiter berücksichtig. Beispielhaft sind für die Schutzfunktion *sensible Daten verschlüsseln* die Schutzmuster *Vererbung von Informationen, Schutz von eingebetteter Software* sowie *Protecting Electronic Pro-*

ducts als mögliche Lösungen identifiziert. Der Entwickler wird bei der Suche nach Lösungen durch die Darstellung als Schutzmuster unterstützt. Diese gibt einen Überblick über die Schutzfunktionen der Maßnahme. So erfüllt z. B. das Schutzmuster *Protecting Electronic Products* die Schutzfunktion *sensible Daten schützen*. Der Schutz wird mit der Verschlüsselung der Software realisiert (vgl. Bild 4-7). Alle Lösungsalternativen des Gesamtsystems werden im morphologischen Kasten gesammelt. Ein Auszug aus dem morphologischen Kasten mit Fokus auf dem Systemschutz ist in Bild 5-6 dargestellt.

Anhand des morphologischen Kastens können die passenden Schutzmuster übersichtlich zu den Schutzfunktionen zugeordnet werden. Generell kann ein Schutzmuster auch mehrere Schutzfunktionen erfüllen. Der morphologische Kasten wird nun von oben nach unten durchlaufen und jeweils ein Schutzmuster für die Erfüllung einer Schutzfunktion ausgewählt. So kann eine Kombination an Schutzmustern identifiziert werden, die alle Schutzfunktionen erfüllt. Dies ist in Bild 5-6 durch die grüne Linie visualisiert.

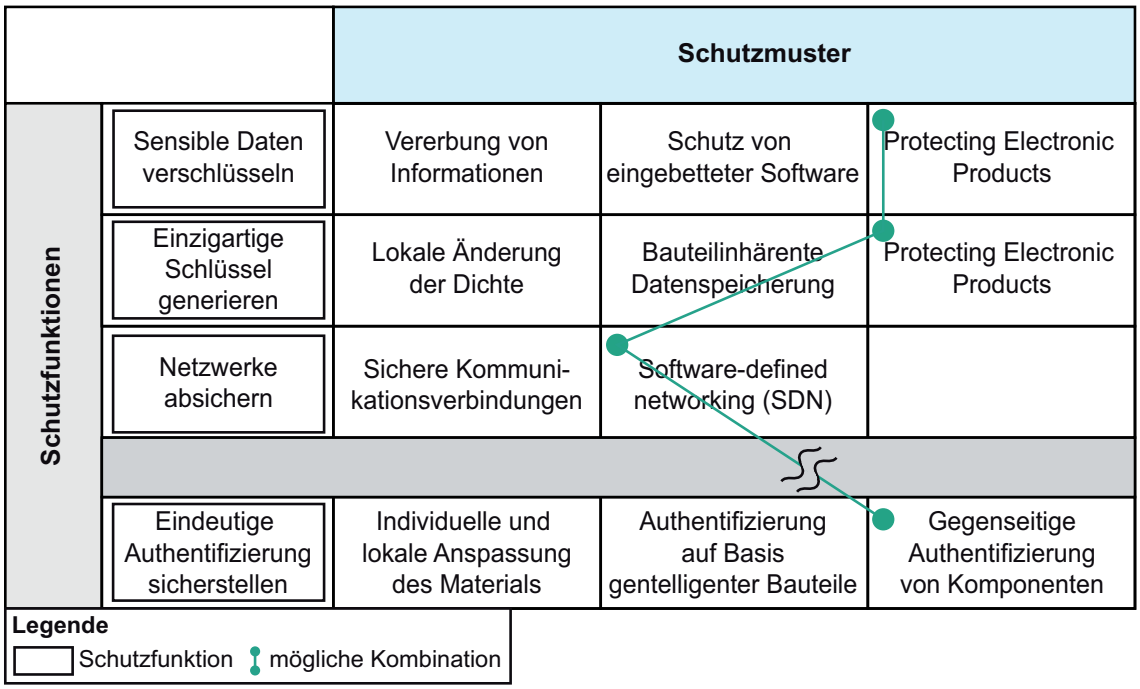


Bild 5-6: Morphologischer Kasten für den Schutz des Schneidwerks (Auszug)

Es ist zu überprüfen, gegen welche Kompetenzen die Maßnahmen wirkungsvoll sind. Dies wird im Schutzmuster durch die Klassifizierung der Imitatoren aufgezeigt (vgl. Kap. 4.4.2). Die für die Bedrohungslage wirksamsten Maßnahmen sind auszuwählen. Hierfür sind die Schutzmuster mit den Kompetenzen der Imitatoren abzugleichen (vgl. Bild 5-3). Für den weiteren Verlauf der Validierung ist die Kombination der Schutzmuster *Protecting Electronic Products*, *SDN* sowie *gegenseitige Authentifizierung von Komponenten* ausgewählt. Diese Kombination erfüllt alle ausgewählten Schutzanforderungen Intelligenter Technischer Systeme (vgl. Kap. 5.1.1).

5.1.4 Phase 4: Systemspezifikation

In dieser Phase werden die ausgewählten Schutzmuster in die Spezifikation des Systems integriert. Dies geschieht während der Erarbeitung der Gesamtsystemspezifikation. Im Fokus stehen die ausgewählten Schutzmuster *Protecting Electronic Products, SDN* sowie *gegenseitige Authentifizierung von Komponenten*. Diese werden nachfolgend in die Prinziplösung des Schneidwerks integriert. Hierfür werden die Partialmodelle Wirkstruktur und Verhalten erweitert. Im Vordergrund der Betrachtung steht die Integration der Schutzmuster. Diese sind als rot umrandete Systemelemente dargestellt. Die Prinziplösung dient der Anschauung und ist vereinfacht dargestellt.

In Bild 5-7 ist die Steuerung des Schneidwerks abgebildet. Diese besteht vereinfacht aus einem Steuergerät, der Datenverarbeitung, einem Kommunikationsmodul sowie der Energieversorgung. Das Steuergerät ist für die interne Kommunikation zuständig. Es tauscht Daten mit der Gutaufnahme aus (wie Drehzahl und Position der Haspel) und sendet Maschinenparameter für die Einstellung der Mäheinrichtung. Für die externe Kommunikation ist das Kommunikationsmodul verantwortlich. Es kommuniziert mit dem System, an welches das Schneidwerk gekoppelt ist (hier der Mähdrescher). Sämtliche relevante Daten des Schneidwerks werden mit dem Mähdrescher ausgetauscht. Dies ist für die Synchronisation der Parameter von entscheidender Bedeutung. Für eine Erhöhung des Durchsatzes sind sowohl die Parameter des Mähdreschers als auch die des Schneidwerks anzupassen.

Für die Kommunikation ist der *SDN-Ansatz* zu berücksichtigen. Das bedeutet, dass für den Aufbau der Kommunikationsnetzwerke die Kontroll- und Datenebene getrennt betrachtet und ausgeführt werden müssen (vgl. Kap. 4.3.2.4).

Sowohl das Kommunikationsmodul als auch das Steuergerät bekommen die Anweisungen von der Datenverarbeitung. Hier laufen alle Daten des Systems zusammen und werden verarbeitet. Für den Schutz der sensiblen Daten, in diesem Fall der Firm- bzw. Software der Datenverarbeitung, wird das Schutzmuster *Protecting Electronic Products* (vgl. Kap 4.3.2.1) integriert. Dieses umschließt das eingebettete System mit einer Schutzfolie und sichert den Schutz der sensiblen Daten. Durch die Schutzfolie wird der Nachbau durch Reverse Engineering verhindert, da die Daten unbrauchbar sind, sollte die Folie entfernt werden. Weiterhin wird der kryptographische Schlüssel zur Entschlüsselung der Software aus den Folieneigenschaften generiert. Er muss somit nicht gespeichert werden und ist zudem nicht reproduzierbar. Auf die entschlüsselte Software kann die Datenverarbeitung zugreifen und die gewünschten Operationen ausführen. In diesem Zustand sorgt die Manipulationsüberwachung dafür, dass Angriffe detektiert werden und die Software gelöscht wird. Updates oder Wartungen der Steuerung können erst nach der erfolgreichen Authentifizierung über die sISP-Schnittstelle erfolgen. Bestimmte Speicherbereiche können beschrieben, jedoch nicht ausgelesen werden. So wird der Schutz der Software auch während der Wartung oder eines Updates sichergestellt.

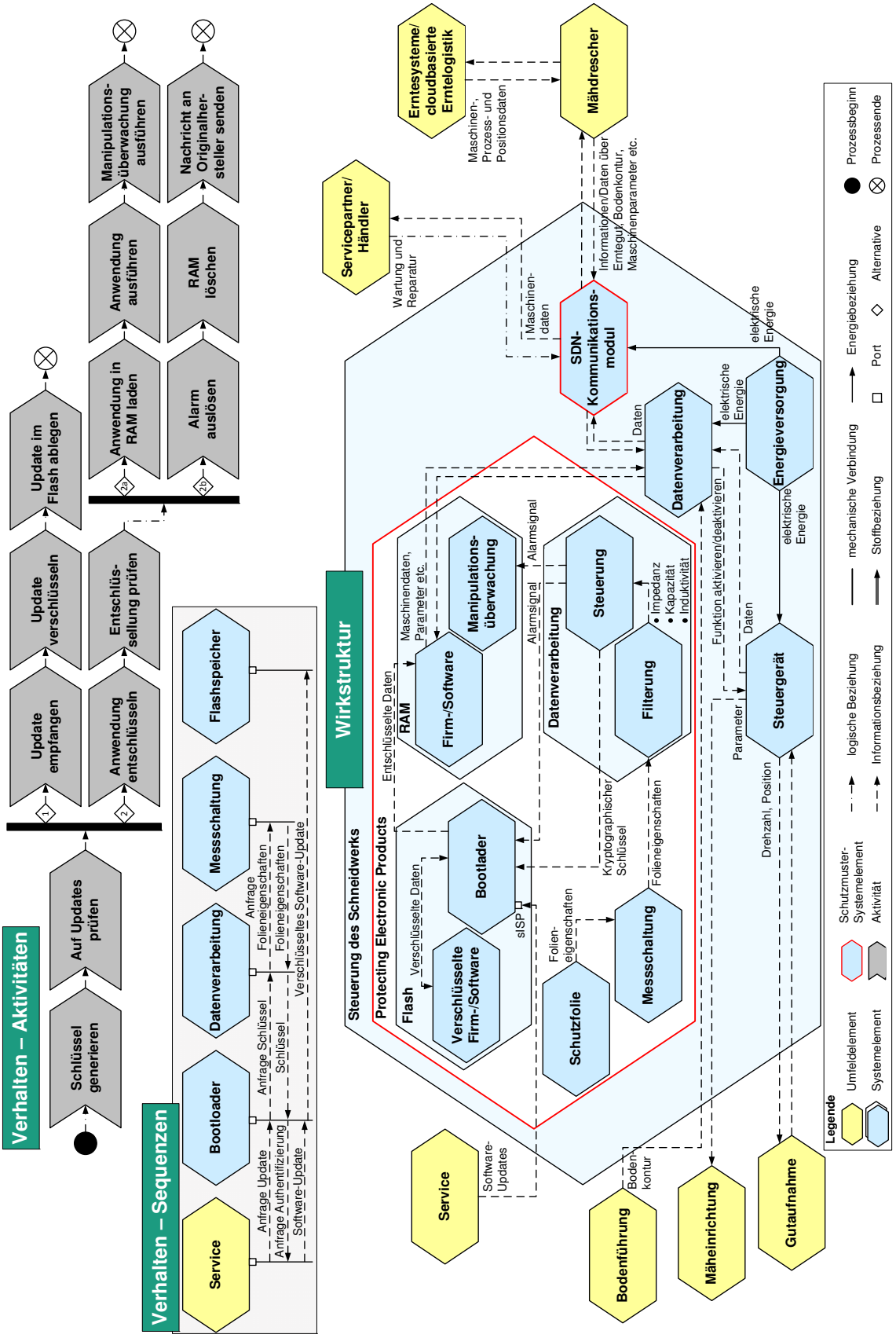


Bild 5-7: Prinziplösung der präventiv geschützten Steuerung des Schneidwerks

Für die Maßnahme *Protecting Electronic Products* sind in Bild 5-7 zusätzlich Verhaltensdiagramme dargestellt. Aus dem Schutzmuster ist das Modell Verhalten – Aktivitäten entnommen. Dies beschreibt das Systemverhalten nach der Aktivierung (vgl. Bild 4-7). Darüber hinaus ist das Modell Verhalten – Sequenz visualisiert, damit die Wechselwirkungen zwischen den Systemelementen abgebildet werden. Die Verhaltensmodelle komplettieren die Prinziplösung, indem sie erforderliche Informationen je nach Verhalten darstellen.

Die Integration des Schutzes auf Basis der Authentifizierung ist in Bild 5-8 veranschaulicht. Hierbei sind unterschiedliche Spezialisierungen der Authentifizierung integriert (vgl. Bild 4-8). Zur gegenseitigen Authentifizierung des Schneidwerks und des Mähdreschers wird das Schutzmuster *gegenseitige Authentifizierung über Kommunikationsmodul* (vgl. Bild A-22) verwendet. Nach einer Wartung oder Reparatur muss sich zudem das Schnittsystem am Schneidwerk authentifizieren. Dies ist mit der *Authentifizierung von Komponenten über Sensorik* (vgl. Bild A-21) realisiert. Die Elemente der Schutzmuster sind rot umrandet.

Damit sich das Schneidwerk und der Mähdrescher gegenseitig authentifizieren können, muss in den Steuerungen der Systeme ein Kommunikationsmodul vorhanden sein. Dieses sendet und empfängt die jeweiligen IDs. Die Datenverarbeitung überprüft die empfangenen IDs. Bei erfolgreicher Authentifizierung ist das System betriebsbereit.

Stimmen die IDs überein, so kann davon ausgegangen werden, dass es sich jeweils um originale Systeme handelt (hier Mähdrescher und Schneidwerk). Falls die IDs nicht übereinstimmen, wird ein Fehler ausgegeben. Für das weitere Systemverhalten sind die Gesetze gegen unlauteren Wettbewerb sowie Kartellbestimmungen zu berücksichtigen (vgl. Kap. 5.1.2). Das Verhalten der jeweiligen Steuerungen ist im Aktivitätsdiagramm in Bild 5-8 visualisiert. Dieses ist aus dem Schutzmuster *gegenseitige Authentifizierung über Kommunikationsmodul* entnommen (vgl. Bild A-22).

Um den Schutz der Ersatz- und Verschleißteile wie Messer oder Doppelfinger sicherzustellen, wurde die Authentifizierung des gesamten Schnittsystems am Schneidwerk entwickelt. Zunächst müssen alle Systemelemente, die für das Schneiden zuständig sind, zu einem übergeordneten Schnittsystem zusammengefasst werden. Dieses System wird um einen Sender erweitert. Der Sender überträgt die IDs an einen Sensor. Dieser ist in die Steuerung des Schneidwerks integriert. So kann die Originalität des Schnittsystems überprüft und abgesichert werden.

Die Zustände der Datenverarbeitung sind im Verhaltensdiagramm in Bild 5-8 dargestellt. Während der Wartungsarbeiten ist die Datenverarbeitung im Zustand *Service*. Vom Sensor werden die IDs empfangen. Die IDs werden ausgewertet. Enthalten sie die erforderlichen Erkennungsmerkmale, wird der Service beendet und das Schneidwerk aktiviert. Es ist somit betriebsbereit. Stimmen die IDs nicht überein, wird ein Fehler gemeldet. Das System verbleibt im Wartungszustand.

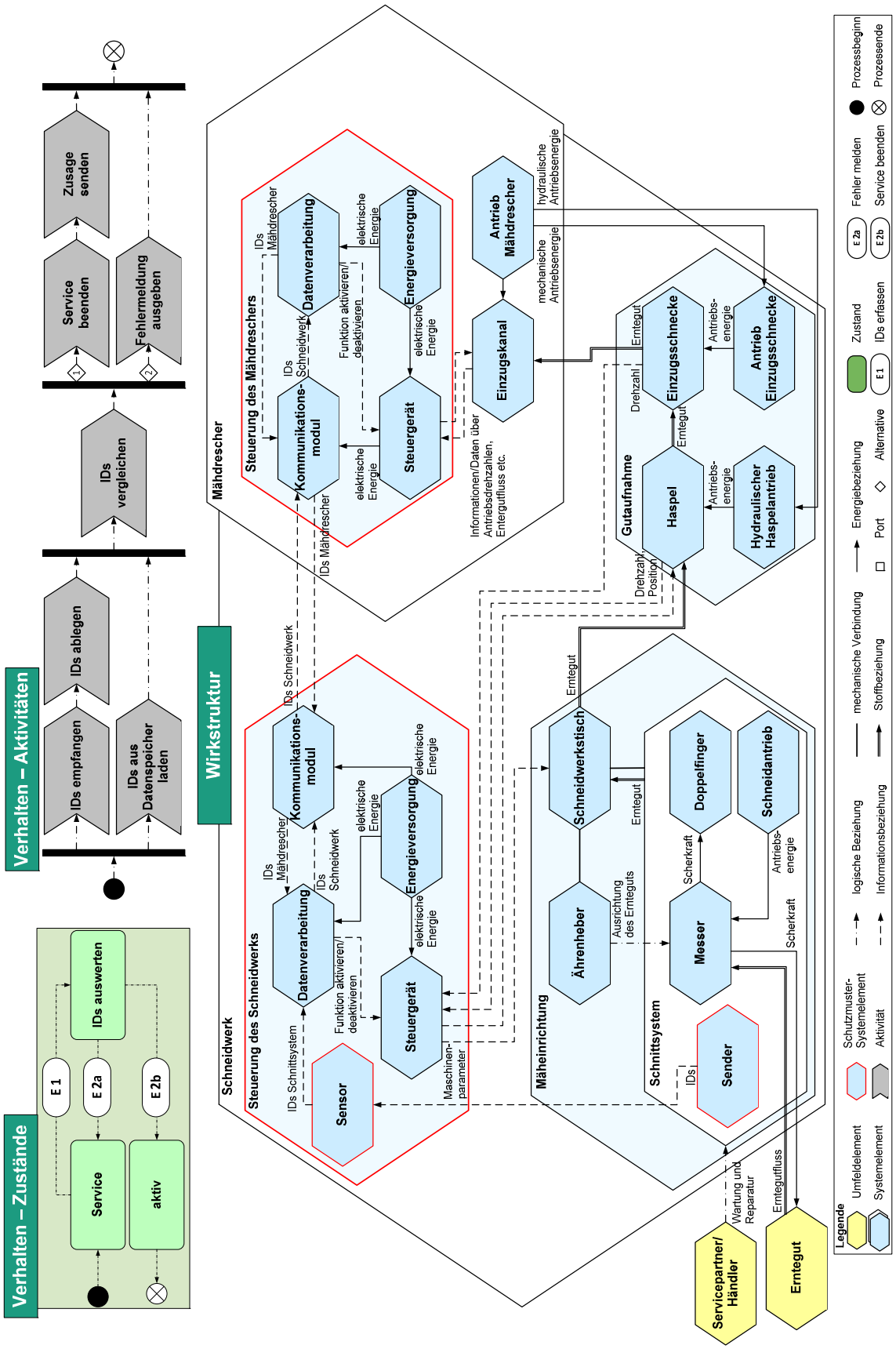


Bild 5-8: Prinziplösung des präventiv geschützten Schneidwerks

Die Kombination der Wirkstruktur und der Verhaltensdiagramme zeigt die Prinziplösung des präventiv geschützten Schneidwerks. Durch die ausgewählten Schutzmuster werden die Steuerung sowie deren sensible Daten geschützt. Zusätzlich sind die Kommunikationsverbindungen abgesichert (vgl. Bild 5-7). Darüber hinaus wird die Authentifizierung der Originalkomponenten ermöglicht. So können sich die Systeme untereinander (Schneidwerk und Mähdrescher) wie auch die Ersatz- und Verschleißteile am Schneidwerk authentifizieren (vgl. Bild 5-8).

5.2 Bewertung der Arbeit anhand der Anforderungen

Im Anschluss an die beispielhafte Anwendung wird die erarbeitete *Entwurfssystematik für den präventiven Schutz Intelligenter Technischer Systeme vor Produktpiraterie* anhand der Anforderungen aus Kapitel 2.6 abschließend bewertet. Hierzu wird zu jeder Anforderung eine Erläuterung gegeben, inwieweit die Entwurfssystematik oder deren Bestandteile zur Erfüllung der Anforderung beiträgt.

A1) Charakterisierung ITS-spezifischer Schutzanforderungen: Das Fundament der erarbeiteten *Entwurfssystematik* besteht aus der Identifikation der charakteristischen Schutzanforderungen Intelligenter Technischer Systeme. In Kapitel 4.2 wurden die Herausforderungen für den Systemschutz aufgenommen. Darauf aufbauend wurden die ITS-spezifischen Schutzanforderungen identifiziert und analysiert. Diese dienen als Grundlage für die Überprüfung der Wirksamkeit der Schutzmaßnahmen.

A2) Bereitstellung passender Schutzmaßnahmen für ITS: Aufbauend auf den Schutzanforderungen wurde die Wirkung bestehender Schutzmaßnahmen überprüft. Innovative Ansätze wurden aufgezeigt sowie resultierende Maßnahmen identifiziert und beschrieben. Die neuen Schutzmaßnahmen wurden ebenfalls auf ihre Wirkweise überprüft (vgl. Kap. 4.3).

A3) Darstellung der Kompetenzen der Imitatoren und der Angriffsmöglichkeiten: Mit der Klassifizierung der Imitatoren wurden die ITS-relevanten Kompetenzen der Imitatoren visualisiert (vgl. Kap. 4.4). Hierzu wurde die Klassifizierung nach LINDEMANN ET AL. überarbeitet. Zur Darstellung der Angriffsmöglichkeiten wurden verschiedene Partialmodelle aus CONSENS benutzt (z. B. Umfeld und Anwendungsszenarien). So wurden unterschiedliche Angriffe übersichtlich und individuell dargestellt und analysiert.

A4) Interdisziplinarität und Ganzheitlichkeit: Der Entwurf Intelligenter Technischer Systeme wird durch ein fachdisziplinübergreifendes Team von Experten erarbeitet. Die interdisziplinäre sowie ganzheitliche Abbildung von Schutzmaßnahmen ist daher von hoher Priorität. Die Entwurfssystematik stützt sich in diesem Zusammenhang auf die einheitliche Darstellung von Lösungsmustern nach ANACKER und überführt die Maßnahmen in eine musterbasierte Darstellung (vgl. Kap. 4.5.1).

A5) Modellbasierte Maßnahmenbeschreibung zur Verwendung im Systementwurf: Die Darstellung von Schutzmaßnahmen wurde in Kapitel 4.4 grundlegend überarbeitet. Mit Hilfe graphischer Modelle des MBSE wurden die textbasierten Steckbriefe der Schutzmaßnahme in eine modellbasierte Darstellung überführt. Diese stellt das interdisziplinäre Verständnis sicher und vereinfacht die Anwendung der Maßnahmen in den frühen Phasen der Entwicklung Intelligenter Technischer Systeme – dem Systementwurf.

A6) Wiederverwendung von Lösungswissen: Die einheitliche Strukturierung von Lösungsmustern für den Systementwurf nach ANACKER dient als Grundlage für die Struktur der modellbasierten Beschreibung von Schutzmaßnahmen. Nach ANACKER beschreibt ein Lösungsmuster in Anlehnung an die Arbeiten von ALEXANDER ein Problem (hier die Entwurfsaufgabe) und die zugehörige Lösung. Mit Beispielen sowie unterschiedlichen Abstraktionsebenen kann bereits erfolgreich eingesetztes Lösungswissen für den Produktschutz externalisiert und gespeichert werden (vgl. Kap. 4.4).

A7) Frühzeitige und durchgängige Berücksichtigung des Systemschutzes: Zur Sicherstellung der frühzeitigen Beachtung des Schutzes für ITS wurde in Kapitel 4.5 ein Vorgehensmodell entwickelt. Dieses erweitert den Entwurf Intelligenter Technischer Systeme, indem es die Aspekte des Systemschutzes integriert. Somit werden diese in den frühen Phasen der Entwicklung berücksichtigt. Diese Erweiterung ist gleichzeitig die Basis für die durchgängige Berücksichtigung des Systemschutzes. Darüber hinaus wurde anhand der unterschiedlichen Abstraktionsebenen die durchgängige Anwendung der Schutzmuster sichergestellt.

A8) Integration in etablierte Standards des Systementwurfs: Die Aspekte des Systemschutzes wurden in den lösungsmusterbasierten Systementwurf nach ANACKER integriert. Dieser greift die Herangehensweise eines funktionsorientierten Entwurfs im Sinne der VDI 2206 auf und erweitert die etablierten Entwurfsschritte unter Berücksichtigung von bereits erfolgreich eingesetztem Lösungswissen. In Kapitel 4.5 wurde der lösungsmusterbasierte Systementwurf angepasst und ergänzt, damit zusätzlich der Systemschutz berücksichtigt wird.

A9) Präventiver Schutz auf Basis technischer Maßnahmen: Mit der entwickelten Entwurfssystematik wurde ein präventiver Schutz für ITS auf Grundlage technischer Schutzmaßnahmen realisiert und exemplarisch angewendet (vgl. Kap. 4 und 5).

Die erarbeitete *Entwurfssystematik für den präventiven Schutz Intelligenter Technischer Systeme vor Produktpiraterie* erfüllt damit alle gestellten Anforderungen in vollem Umfang. Die Systematik fokussiert den präventiven Schutz Intelligenter Technischer Systeme. Die Wiederverwendung von bereits erfolgreich eingesetztem Lösungswissen wird ermöglicht. Anhand des Validierungsbeispiels in Kapitel 5 wurde dies unter realen Bedingungen erprobt und unter Beweis gestellt.

6 Zusammenfassung und Ausblick

Geprägt durch die fortschreitende Digitalisierung entwickeln sich mechatronische Produkte zu vernetzten Systemen mit inhärenter Teilintelligenz. Folgerichtig werden sie als **ITS** bezeichnet. Diese Systeme verbinden die physische und die virtuelle Welt. Sie haben die Fähigkeit, mit anderen Maschinen zu kommunizieren und berücksichtigen darüber hinaus die Wünsche des Benutzers. Zusätzlich sind sie in der Lage, sich ihrer Umwelt autonom anzupassen [GDJ+14].

Auf Basis dieser Entwicklung eröffnen sich für die Hersteller dieser Systeme neue Perspektiven. Anhand der fortschreitenden Durchdringung maschinenbaulicher Erzeugnisse mit Informations- und Kommunikationstechnik ergeben sich zahlreiche Innovationspotentiale. Auf der Grundlage von Innovationen können Unternehmen ihren Wettbewerbsvorsprung und damit ihre Marktführerschaft sicherstellen. Jedoch entstehen auch Begehrlichkeiten bei Wettbewerbern und Imitatoren. **Produktpiraterie** bedroht den Markterfolg vieler Unternehmen und bringt sie um die Rendite ihrer Investitionen in Forschung und Entwicklung. Insbesondere mit Reverse Engineering und Cyberattacken gelingt es den Imitatoren, das Know-how aus den Systemen bzw. deren Komponenten zu extrahieren. Die Aspekte des Schutzes müssen insbesondere in den frühen Phasen der Entwicklung – dem sog. **fachdisziplinübergreifenden Systementwurf** – berücksichtigt werden. So wird der wirksame und effiziente Systemschutz sichergestellt.

Daraus resultierend liegt die zentrale Herausforderung der vorliegenden Arbeit im *präventiven Schutz Intelligenter Technischer Systeme*. Um dieser zu begegnen, müssen drei **Handlungsfelder** erschlossen werden. Für einen wirkungsvollen, präventiven Schutz müssen **wirksame Schutzmaßnahmen** für ITS identifiziert werden. Hierfür sind zunächst die Schutzanforderungen der intelligenten, vernetzten Systeme aufzunehmen. Weiterhin muss die **interdisziplinäre Schutzmaßnahmenbeschreibung** erarbeitet werden. Dies ist grundlegende Voraussetzung, damit die Maßnahmen bereits im Systementwurf berücksichtigt werden können. Darüber hinaus ist der Systemschutz in etablierte Standards des Systementwurfs zu integrieren. So wird der **musterbasierte Entwurf imitationsgeschützter Systeme** ermöglicht.

Im Rahmen dieser Arbeit wurden bestehende Schutzmaßnahmen untersucht und deren Darstellung überarbeitet. Weiterhin wurden Möglichkeiten zum Entwurf präventiv imitationsgeschützter Systeme, interdisziplinäre Modellierungstechniken, Entwurfsmuster zur Wiederverwendung von Lösungswissen und Ansätze für den musterbasierten Entwurf Intelligenter Technischer Systeme analysiert. Die Analysen liefern jedoch nur partielle Ergebnisse, die genutzt und erweitert werden können. Eine ganzheitliche Systematik, die alle Handlungsfelder abdeckt, existiert nicht.

Zahlreiche Schutzmaßnahmen sind bei *ABELE ET AL.*, *LINDEMANN ET AL.* und *GAUSEMEIER ET AL.* aufgeführt. Alle Werke haben gemein, dass sie die Schutzmaßnahmen textbasiert darstellen. Hierdurch kann das disziplinübergreifende Verständnis nicht ausreichend

sichergestellt werden. Die Berücksichtigung der Maßnahmen im Systementwurf ist nur bedingt möglich. Die Verfahren zum Entwurf präventiv imitationsgeschützter Systeme sind insgesamt nicht auf den Schutz Intelligenter Technischer Systeme ausgelegt. So spezialisieren sich z. B. der *Beitrag zum ganzheitlichen Know-how-Schutz von virtuellen Produktmodellen nach MEIMANN,* das *ganzheitliche und präventive Schutzkonzept für Investitionsgüter (PROTACTIVE)* sowie das *Verfahren zur Konzipierung imitationsgeschützter Produkte und Produktionssysteme nach KOKOSCHKA* zu sehr auf fachdisziplinspezifische Entwicklungen. Hierdurch sind sie für die Entwicklung geschützter Intelligenter Technischer Systeme ungeeignet. Im Hinblick auf die Darstellung von Schutzmaßnahmen wurden die Themenfelder Modellierungstechniken und Wissensmanagement mit Lösungsmustern analysiert. Als Grundlage für die Adaption der Schutzmaßnahmen wird eine geeignete Musterstruktur benötigt. Von den untersuchten Strukturierungen modellbasierter Entwurfsmuster in der Produktentstehung besticht die *einheitliche Strukturierung von Lösungsmustern für den Systementwurf nach ANACKER.* Sie eignet sich insbesondere zur Externalisierung und Darstellung von multidisziplinärem Lösungswissen. Darüber hinaus sind die Lösungsmuster so beschrieben, dass sie im Entwurf Intelligenter Technischer Systeme berücksichtigt werden können. Die Beschreibung der Muster nach ANACKER erfolgt mit der Spezifikationstechnik CONSENS. Sie ist sowohl als Sprache zur modellbasierten Beschreibung technischer Artefakte als auch zur Erstellung des Systemmodells im Rahmen des Entwurfs geeignet. Zusätzlich werden Ansätze für den musterbasierten Entwurf Intelligenter Technischer Systeme untersucht. Bei den Ansätzen des musterbasierten Entwurfs zeigte sich der *Lösungsmusterbasierte Entwurf fortgeschrittener mechatronischer Systeme nach ANACKER* als der Ansatz, welcher die gestellten Anforderungen am besten erfüllt. Hierbei gab die ganzheitliche, interdisziplinäre sowie durchgängige Verwendung der Lösungsmuster bei komplexen Systementwürfen den Ausschlag. Insgesamt besteht **Handlungsbedarf** für eine *Entwurfssystematik für den präventiven Schutz Intelligenter Technischer Systeme vor Produktpiraterie*.

Die erarbeitete Systematik greift Inhalte der untersuchten Ansätze auf, überträgt sie auf die Gegebenheiten der modernen Produktentstehung, erweitert und ergänzt sie, um den Anforderungen des Schutzes Intelligenter Technischer Systeme gerecht zu werden. Das erarbeitete **Ergebnis** setzt sich aus den folgenden vier Bestandteilen zusammen:

- Der Aufnahme sowie Analyse der **Schutzanforderungen Intelligenter Technischer Systeme**. Diese dienen als Grundlage für die Überprüfung der Wirksamkeit von Schutzmaßnahmen.
- Der Identifikation **wirksamer Schutzmaßnahmen für Intelligente Technische Systeme** zur bestmöglichen Erfüllung der Schutzanforderungen. Hierfür werden sowohl bestehende als auch neue Schutzmaßnahmen auf Grundlage innovativer Technologien untersucht.

- Der Überarbeitung der **Darstellung der Schutzmaßnahmen** zur Sicherstellung eines interdisziplinär einheitlichen Verständnisses. So wird ebenfalls die Wiederverwendung von bereits erfolgreich eingesetztem Lösungswissen im Bereich Systemschutz ermöglicht.
- Der Entwicklung des Vorgehensmodells zur **Integration des präventiven Schutzes in den musterbasierten Entwurf Intelligenter Technischer Systeme**. Dieses versetzt die Entwickler in die Lage, gemeinsam mit einem interdisziplinären Entwicklungsteam ein Systemkonzept für präventiv geschützte ITS zu erstellen.

Die **Validierung** der Systematik erfolgte anhand der exemplarischen Entwicklung eines Mähdreschers. Im Zuge der Validierung wurde das entwickelte Vorgehensmodell vollständig durchlaufen und die erarbeiteten Hilfsmittel eingesetzt. So konnten die einzelnen Phasen des Vorgehensmodells inklusive der erarbeiteten Resultate vorgestellt werden. Die Validierung zeigt, dass die entwickelte *Entwurfssystematik für den präventiven Schutz Intelligenter Technischer Systeme vor Produktpiraterie* die gestellten Anforderungen in vollem Umfang erfüllt.

Im Hinblick auf die stetige Weiterentwicklung technischer Erzeugnisse besteht weiterer Forschungsbedarf. Neuartige Anforderungen der Systeme von morgen müssen identifiziert und beim Systemschutz berücksichtigt werden. Damit auch zukünftige Angriffe wirksam abgewehrt werden können, sind eine kontinuierliche Weiterentwicklung bestehender Schutzmaßnahmen sowie die Suche nach neuen Ansätzen zum Systemschutz unabdingbar.

Die entwickelte Systematik betrachtet schwerpunktmäßig die frühen Phasen des modellbasierten Systementwurfs. Daher sind die Auswirkungen der eingesetzten Schutzmaßnahmen auf die weitere System- und Produktionssystementwicklung zu untersuchen.

Insbesondere die Reaktion auf nicht berücksichtigte Ereignisse muss für den Schutz der Systeme weiterentwickelt werden. Das Forschungsfeld der Resilienz bietet Ansätze, um z. B. auch bei nicht berücksichtigten Angriffen den Schutz zu gewährleisten.

Die vorliegende Arbeit betrachtet den Schutz der Systeme vor Produktpiraterie. Die erarbeitete Systematik ist allgemeingültig und kann abstrahiert ebenso für andere Bereiche eingesetzt werden. Durch die Systematik können die Aspekte des Systemschutzes, z. B. im Bereich Betriebssicherheit, bereits in den frühen Phasen der Entwicklung betrachtet und so wirksame Maßnahmen berücksichtigt werden.

7 Abkürzungsverzeichnis

3P	Prävention gegen Produktpiraterie – Innovationen schützen
acatech	Deutsche Akademie der Technikwissenschaften
AISEC	Fraunhofer-Institut für Angewandte und Integrierte Sicherheit
AM	Additive Manufacturing
AW	Anwendungsszenarien
Bitkom	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.
BMBF	Bundesministerium für Bildung und Forschung
BSI	Bundesamt für Sicherheit in der Informationstechnik
bspw.	beispielsweise
bzw.	beziehungsweise
ca.	circa
CAD	computer-aided design
CONSENS	CONceptual design Specification technique for the Engineering of complex Systems
CPS	Cyber-Physical Systems
CSP	CLAAS Service and Parts GmbH
DfAP	Design-for-Anti-Piracy-Methodik
DNA	deoxyribonucleic acid
e. V.	eingetragener Verein
et al.	et alii
etc.	et cetera
f.	folgend
ff.	folgenden
FLM	Fused Layer Modeling
FMEA	Fehler-Möglichkeits-und-Einfluss-Analyse
FPGA	Field Programmable Gate Array

ggf.	gegebenenfalls
GPD	Ganzheitliche-Piraterie-Diagnose
GPS	Global Positioning System
HF	Handlungsfeld
IEM	Fraunhofer-Institut Entwurfstechnik Mechatronik
IDs	Identifikationsmerkmale
IP	Intellectual Property
IT	Informationstechnik/Informationstechnisch
ITS	Intelligente Technische Systeme
it’s OWL	Intelligente Technische Systeme OstWestfalenLippe
Kap.	Kapitel
LM	Lösungsmuster
LS	Laser Sintern
M2M	Maschine zu Maschine
MBSE	Model-Based Systems Engineering
mech.	mechatronischer
Mio.	Millionen
Mrd.	Milliarden
OCM	Operator-Controller-Modul
OSI	Open Systems Interconnection
PEP	Produktentstehungsprozess
PLM	Product Lifecycle Management
PLZ	Produktlebenszyklus
PSS	Produkt-Service-Systeme
PUF	Physical Unclonable Functions
PwC	PricewaterhouseCoopers
QR-Code	Quick Response Code
RAM	Random-Access Memory

RFID	radio-frequency-identification
S.	Seite
SDN	Software-defined networking
SE	Systems Engineering
SECI	Socialization, Externalization, Combination, Internalization
sISP	secure-In-System-Programming-Schnittstelle
s.o.	selbstoptimierenden
StVO	Straßenverkehrsordnung
SLM	Selective Laser Melting
sog.	sogenannte
u. a.	unter anderem
UML	Unified Modeling Language
VDI	Verein Deutscher Ingenieure
VDMA	Verband Deutscher Maschinen- und Anlagenbau
vgl.	vergleiche
WIPO	World Intellectual Property Organization
z. B.	zum Beispiel

8 Literaturverzeichnis

[AAA+10] ABELE, E.; ALBERS, A.; AURICH, J. C.; GÜNTHNER, W. A. (Hrsg.): Wirksamer Schutz gegen Produktpiraterie im Unternehmen – Piraterierisiken erkennen und Schutzmaßnahmen umsetzen. Band 3 der Reihe „Innovationen gegen Produktpiraterie“, VDMA Verlag GmbH, Frankfurt am Main, 2010

[ABE+10] ASFAW, B.; BEKELE, D.; ESHETE, B.; VILLAFIORITA, A.; WELDEMARIAM, K.: Host-based Anomaly Detection for Pervasive Medical Systems. In: Proceedings of the 5th International Conference on Risks and Security of Internet and Systems, Montreal, 2010, S.1-8

[ABG+14] ANACKER, H.; BAUER, F.; GAUSEMEIER, J.; SCHIERBAUM, T.: Systementwurf mit Hilfe von Lösungsmustern aus dem Semantic Web. In: GAUSEMEIER, J.; TRÄCHTLER, A.; SCHÄFER, W. (Hrsg.): Semantische Technologien im Entwurf mechatronischer Systeme – Effektiver Austausch von Lösungswissen in Branchenwertschöpfungsketten. Carl Hanser Verlag, München, 2014

[aca11] ACATECH BEZIEHT POSITION: Nanoelektronik als künftige Schlüsseltechnologie der Informations- und Kommunikationstechnik in Deutschland. Berlin 2011

[ADG+09] ADELT, P.; DONOTH, J.; GAUSEMEIER, J.; GEISLER, J.; HENKLER, S.; KAHL, S.; KLOPPER, B.; KRUPP, A.; MUNCH, E.; OBERTHUR, S.; PAIZ, C.; PORRMANN, M.; RADKOWSKI, R.; ROMAUS, C.; SCHMIDT, A.; SCHULZ, B.; VÖCKING, H.; WITKOWSKI, U.; WITTING, K.; ZNAMENSHCHYKOV, O.: Selbstoptimierende Systeme des Maschinenbaus – Definitionen, Anwendungen, Konzepte. HNI-Verlagsschriftenreihe, Band 234, Paderborn, 2009

[AES+12] ANDERL, R.; EIGNER, M.; SENDLER, U.; STARK, R. (Hrsg.): acatech DISKUTIERT. Smart Engineering – Interdisziplinäre Produktentstehung. Springer-Verlag, 2012

[AG12] ALBERS, A.; GAUSEMEIER, J.: Von der fachdisziplinorientierten Produktentwicklung zu vorausschauenden und systemorientierten Produktentstehung. In: ANDERL, R.; EIGNER, M.; SENDLER, U.; STARK, R. (Hrsg.): Smart Engineering – Interdisziplinäre Produktentstehung. acatech DISKUSSION, 2012

[AIS+77] ALEXANDER, C.; ISHIKAWA, S.; SILVERSTEIN, M.; JACOBSON, M.; FIKSDAHLKING, I.; ANGEL, S.: A Pattern Language. Oxford University Press, 1st Edition, New York, 1977

[AIS+95] ALEXANDER, C.; ISHIKAWA, S.; SILVERSTEIN, M.; JACOBSON, M.; FIKSDAHLKING, I.; ANGEL, S.; CZECH, H.(Hrsg.): Eine Muster-Sprache – Städte, Gebäude, Konstruktion. Löcker Verlag, Wien, 1995

[AIS15-ol] FRAUNHOFER INSTITUTE FOR APPLIED AND INTEGRATED SECURITY (AISEC). Unter: http://www.aisec.fraunhofer.de/de/fields-of-expertise/product-protection/pep-protecting-electronic-products.html, am 28. März 2015

[AKL11] ABELE, E.; KUSKE, P.; LANG, H.: Schutz vor Produktpiraterie – Ein Handbuch für den Maschinen- und Anlagenbau. Springer-Verlag, Berlin, 2011

[Alk11-ol] ALKATEB, S.: 5 Things You Need to Know About Deep Packet Inspection (DPI). 4/2011, Unter: http://www.cavium.com/pdfFiles/CSS-DPI-White-Paper.pdf, am 20. März 2016

[Alt12] ALT, O.: Modell-basierte Systementwicklung mit SysML – In der Praxis. Carl Hanser Verlag, München, 2012

[Ana15] ANACKER, H.: Instrumentarium für einen lösungsmusterbasierten Entwurf fortgeschrittener mechatronischer Systeme. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Band 354, Paderborn, 2015

[Bar98] BARTER, R.H.: A Systems Engineering Pattern Language. In: Proceedings of 8th Annual International Symposium on the International Council on Systems Engineering, Vancouver, Juli 1998

[BBB+10] BAKHKHAT, S.; BÖDE, F.; BRUCKE, M.; DEGEN, K.; EBERT, C.; EINSIEDLER, I.; GOUMA, C.; GRUNERT, F.; MÖLLERS, R.; NIEHAUS, J.; RENGER, K.; RICHTER, S.; RUPP, S.; SALECKER, J.; STEIN, R.; WINZENRIED, O.; ZIEGLER, S.; BITKOM (Hrsg.): Eingebettete Systeme - Ein strategisches Wachstumsfeld für Deutschland. BITKOM, Berlin, 2010

[BD06] BORTZ, J.; DÖRING, N.: Forschungsmethoden und Evaluation für Human- und Sozialwissenschaftler. Springer-Verlag, Berlin, 4. Auflage, 2006

[Ber15-ol] BERGERT, D.: Jeep Cherokee – Auto in voller Fahrt gehackt. Unter: http://www.computerbild.de/artikel/cb-News-Connected-Car-Jeep-Cherokee-gehackt-12287345.html, am: 23. November 2015

[BGJ+09] BERTSCHE, B.; GOHNER, P.; JENSEN, U.; SCHINKOTHE, W.; WUNDERLICH, H.-J.: Zuverlässigkeit mechatronischer Systeme. Springer-Verlag, Berlin, 2009

[BH08] BOUCHER, M.; HOULIHAN, D.: Systems Design: New Product Development for Mechatronics. The Aberdeen Group, 2008

[BHL07-ol] BRAUN, S.; HELLENBRAND, D.; LINDEMANN, U.: Kostentransparenz in der Mechatronik – Eine Studie über Komplexitäts- und Kostentreiber mechatronischer Produkte. Unter: http://www.shaker.de/de/content/catalogue/index.asp?lang=&ID=8&ISBN=OND-00000-0000004, am 22. November 2015

[Bib15-ol] BIBLIOGRAPHISCHES INSTITUT GMBH - DUDEN VERLAG (Hrsg.); unter: http://www.duden.de/rechtschreibung/Systematik#Bedeutung1, am 24. November 2015

[Bit15-ol] BUNDESVERBAND INFORMATIONSWIRTSCHAFT, TELEKOMMUNIKATION UND NEUE MEDIEN E. V. (BITKOM): Digitale Angriffe auf jedes zweite Unternehmen. Unter: https://www.bitkom.org/Presse/Presseinformation/Pressemitteilung_5253.html, am 2 Mai 2016

[BK96] BINDER, V., KANTOWSKY, J.: Technologiepotentiale: Neuausrichtung der Gestaltungsfelder des strategischen Technologiemanagements. DUV, Wiesbaden (1996)

[BK12a] BAUER, W.; KOKOSCHKA, M.: Schutzmaßnahmen in der Produktionssystementwicklung. In: GAUSEMEIER, J.; GLATZ, R.; LINDEMANN, U. (Hrsg.): Präventiver Produktschutz – Leitfaden und Anwendungsbeispiele. Carl Hanser Verlag, München, 2012

[BK12b] BAUER, W.; KOKOSCHKA, M.: Produktschutz von der Fertigung bis zur Rücknahme. In: GAUSEMEIER, J.; GLATZ, R.; LINDEMANN, U. (Hrsg.): Präventiver Produktschutz – Leitfaden und Anwendungsbeispiele. Carl Hanser Verlag, München, 2012

[BK12c] BAUER, W.; KOKOSCHKA, M.: Kommunikative Schutzmaßnahmen. In: GAUSEMEIER, J.; GLATZ, R.; LINDEMANN, U. (Hrsg.): Präventiver Produktschutz – Leitfaden und Anwendungsbeispiele. Carl Hanser Verlag, München, 2012

[BLB+06] BEHRENS, B.-A.; LANGE, F.; BOUGECHA, A.; GASTAN, E: Verschlüsselte Sinterbauteile – Fremdpartikel liefern kodierte Informationen um sicherheitsrelevante Teile zu identifizieren. In: Konstruktionspraxis Spezial, Sonderheft 5, November 2006, S.18-20

[BLG07] BEHRENS, B.-A.; LANGE, F.; GASTAN, E.: Ansatz zur manipulationssicheren Markierung von pulvermetallurgisch hergestellten Bauteilen. In: UTF Science, Meisenbach Verlag, Bamberg, Ausgabe 4, 2007, S.1-4

[BLG08] BEHRENS, B.-A.; LANGE, F.; GASTAN, E.: Plagiatschutz sicherheitsrelevanter Sinterbauteile – Verfahrensprinzip und Betrachtung erreichbarer Bauteilfestigkeiten und Risssicherheiten. In: wt Werkstattstechnik online, Ausgabe 10, 2008, S.880-884

[BLQ+14] BAO, S. H.; LI, M.; QIN, Y.; SU, Z.; WEN, L.; ZHANG, S. L.: Voice Based Biometric Authentication Method and Apparatus. Patent, Nr.: US2014/0359739 A1, Dezember 2014

[Bro10] BROY, M. (Hrsg.): Cyber-Physical Systems – Innovation durch softwareintensive eingebettete Systeme. acatech DISKUTIERT, Springer-Verlag, Berlin, 2010

[Bru08] BRÜSEMEISTER, T.: Qualitative Forschung - Ein Überblick. VS Verlag, Wiesbaden, 2. Auflage, 2008

[BRW15] BOSSERT, O.; RICHTER, W.; WEINBERG, A.: Protecting the enterprise with cybersecure IT architecture, McKinsey & Company, März 2015

[BSI12a] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK (Hrsg.): Leitfaden Informationssicherheit – IT-Grundschutz kompakt, 2012

[BSI12b] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK (Hrsg.): Sensibilisierung Cyber-Bedrohungen – ein Einstieg, 2012

[BSI14a] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK (Hrsg.): Die Lage der IT-Sicherheit in Deutschland 2014, 2014

[BSI14b] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK (Hrsg.): Industrial Control System Security – Top 10 Bedrohungen und Gegenmaßnahmen 2014, 2014

[Bue01] BÜSCHKES, R.: Angriffserkennung in Kommunikationsnetzen. Dissertation. Fakultät für Mathematik, Informatik und Naturwissenschaften, Rheinisch-Westfälische Technische Hochschule Aachen, Aachen, 2001

[BW06] BÖTTINGER, S., WACKER, P.: Aktuelle Entwicklung und Stand der Mähdruschtechnik. In: Landtechnik, Ausgabe 61, April 2006, S.202-203

[CBH+09] CHALKIAS, K.; BALDIMTSI, F.; HRISTU-VARSAKELIS, D.; STEPHANIDES, G.: Two Types of Key-Compromise Impersonation Attacks against One-Pass Key Establishment Protocols. In: Communications in Computer and Information Science, Vol. 23, 2009, S.227-238

[Cla16] CLAAS: Produktpräsentation 2016 – LEXION 780 / 770 / 760 / 750 / 740 HRC (higher regulated countries) / Stage IV (Tier 4)

[DAB+10] DAMM, W.; ACHATZ, R.; BEETZ, K.; BROY, M.; GRIMM, K.; LIGGESMEYER, P.: Nationale Roadmap Embedded Systems. In: BROY, M. (Hrsg.): Cyber-Physical Systems – Innovation durch softwareintensive eingebettete Systeme. acatech DISKUTIERT, Springer-Verlag, Berlin, 2010

[Dei09] DEIGENDESCH, T.: Kreativität in der Produktentwicklung und Muster als methodisches Hilfsmittel. Dissertation, Fakultät für Maschinenbau, Karlsruher Institut für Technologie (KIT), Forschungsbericht Band 41, Institut für Produktentwicklung (IPEK), Karlsruhe, 2009

[DGO+14] DZIWOK, S.; GAUSEMEIER, J.; OESTERSÖTEBIER, F.; POHLMANN, U.; RIEKE, J.; SCHÄFER, W.; SCHIERBAUM, T.; TRÄCHTLER, A.: Modellbasierter Entwurf mechatronischer Systeme. In: GAUSEMEIER, J.; TRÄCHTLER, A.; SCHÄFER, W. (Hrsg.): Semantische Technologien im Entwurf mechatronischer Systeme – Effektiver Austausch von Lösungswissen in Branchenwertschöpfungsketten. Carl Hanser Verlag, München, 2014

[DH02] DAENZER, W. F.; HUBER, F. (Hrsg.): Systems Engineering – Methodik und Praxis, Verlag Industrielle Organisation, Zürich, 11. Auflage, 2002

[DHL05] DENKENA, B; HASENFUß, K.; LIEDTKE, C.: Gentelligente Bauteile – Genetik und Intelligenz in der Produktionstechnik. In: Zeitschrift für wirtschaftlichen Fabrikbetrieb ZWF, Carl Hanser Verlag, München, Ausgabe 10, 2005, S.569-572

[DHL10] DENKENA, B.; HENNING, H.; LORENZEN, L.: Genetics and intelligence: new approaches in production engineering. In: Production Engineering – Research and Development, Vol. 4, Issue 1, Februar 2010, S.65-73

[Dil05] DILTHEY, U.: Schweißtechnische Fertigungsverfahren 2 – Verhalten der Werkstoffe beim Schweißen. Springer-Verlag Berlin, 2005

[DIN19226] DEUTSCHES INSTITUT FÜR NORMUNG E. V. (DIN): Leittechnik – Regelungstechnik und Steuerungstechnik – Allgemeine Grundbegriffe. DIN 19226 Teil 1, Beuth-Verlag, Berlin, 1995

[DKB+11] DENKENA, B.; KÖHLER, J.; BREIDENSEIN, B.; MÖRKE, T.: Elementary studies on the inducement and relaxation of residual stress. In: Procedia Engineering Vol: 19, 2011, S.88-93

[DOD+10] DRAGON, R., OSTERMANN, J., DENKENA, B., BREIDENSTEIN, B., MÖRKE, T.: Data Storage in Gentelligent Components: A New Way for Self-Authentication. In: Self-X in Engineering: 2nd Workshop on „Self-X in Engineering“ within the 33rd Annual German Conference on Artificial Intelligence, Karlsruhe, September 2010, S.1-13

[DSB+11] DÜSING, J. F.; SUTTMANN, O.; BANDORF, R.; GERDES, H.: Oberflächen-Dünnschichtsensorik erschließt neue Anwendungen, In: Laser Magazin, Ausgabe 3, 2011, S.11-12

[DSK+12] DÜSING, J. F.; SUTTMANN, O.; KOCH, J.; SUTE, U.; OVERMEYER, L.: Laser Thin Film Patterning of Embedded Strain Sensors on Non-Planar Surfaces. In: Proceedings of the 1st Joint Symposium on System-integrated Intelligence: New Challenges for Product and Production Engineering (SysInt), Juni 2012, S.198-200

[DSO+08] DRAGON, R.; STEINBRENNER, I.; OSTERMANN, J.; DENKENA, B.: Inherent Mechanical Data Storage on Micro-Structured Surfaces. In: 4th. IPROMS Virtual International Conference, Juli 2008, S.466-471

[Dum10] DUMITRESCU, R.: Entwicklungssystematik zur Integration kognitiver Funktionen in fortgeschrittene mechatronische Systeme. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Band 286, Paderborn, 2010

[EBD+15] EMMRICH, V.; BAUERNHANSL, T.; DOBELE, M.; PAULUS-ROHMER, D.; SCHATZ, A.; WESKAMP, M.: Geschäftsmodell-Innovation durch Industrie 4.0 – Chancen und Risiken für den Maschinen- und Anlagenbau. Studie, Fraunhofer IPA, Dr. Wieselhuber & Partner GmbH, München, 2015

[Ehr07] EHRLENSPIEL, K.: Integrierte Produktentwicklung – Denkabläufe, Methodeneinsatz, Zusammenarbeit. Carl Hanser Verlag, München, 3. Auflage, 2007

[EK14] EYISI, E.; KOUTSOUKOS, X.: Energy-Based Attack Detection in Networked Control Systems. In: HiCoNS '14 Proceedings of the 3rd international conference on High confidence networked systems, New York, 2014, S.115-124

[FD06] FRANKE, W.; DANGELMAIER, W. (Hrsg.): RFID – Leitfaden für die Logistik: Anwendungsgebiete, Einsatzmöglichkeiten, Integration, Praxisbeispiele, Gabler Verlag, 2006

[FG13] FELDHUSEN, J.; GROTE, K.-H. (Hrsg.): Pahl/Beitz Konstruktionslehre – Methoden und Anwendungen erfolgreicher Produktentwicklung. Springer-Verlag Berlin, 8. Auflage, 2013

[FMS12] FRIEDENTHAL, S.; MOORE, A.; STEINER, R.: A practical guide to SysML – The systems modeling language. Morgan Kaufmann, Waltham, 2. Auflage, 2012

[For07] FORBRIG, P.: Objektorientierte Softwareentwicklung mit UML. Carl Hanser Verlag, München, 3. Auflage, 2007

[Fra06] FRANK, U.: Spezifikationstechnik zur Beschreibung der Prinziplösung selbstoptimierender Systeme. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Band 175, Paderborn, 2006

[FS11] FILIPOVIC, B.; SCHIMMEL, O.: Schutz eingebetteter Systeme vor Produktpiraterie – Technologischer Hintergrund und Vorbeugemaßnahmen. Fraunhofer AISEC, Garching, 2011

[Fuc06] FUCHS, H. J. (Hrsg.): Piraten, Fälscher und Kopierer – Strategien und Instrumente zum Schutz geistigen Eigentums in der Volksrepublik China, Betriebswirtschaftlicher Verlag Dr. Th. Gabler, Wiesbaden, 2006

[GAC+13] GAUSEMEIER, J.; ANACKER, H.; CZAJA, A.; WASSMANN, H.; DUMITRESCU, R.: Auf dem Weg zu intelligenten technischen Systemen. In: 9. Paderborner Workshop Entwurf mechatronischer Systeme, HNI-Verlagsschriftenreihe, Band 310, 18.-19. April, Paderborn, 2013

[Gar15-ol] GARTNER, INC.: Gartner's 2015 Hype Cycle for Emerging Technologies. Unter: http://www.gartner.com/newsroom/id/3114217, am 3. Januar 2016

[GB12] GEISBERGER, E.; BROY, M. (Hrsg.): agendaCPS – Integrierte Forschungsagenda Cyber-Physical Systems. acatech STUDIE, März 2012

[GDS13] GAUSEMEIER, J.; DUMITRESCU, R.; STEFFEN, D. (Hrsg.): Systems Engineering in der industriellen Praxis. Studie, Wentker Druck GmbH, 2013

[GDJ+14] GAUSEMEIER, J.; DUMITRESCU, R.; JASPERNEITE, J.; KÜHN, A.; TRSEK, H.: Auf dem Weg zu Industrie 4.0: Lösungen aus dem Spitzencluster it‘s OWL, April 2014

[Geb13] GEBHARDT, A.: Generative Fertigungsverfahren. Additive Manufacturing und 3D Drucken für Prototyping - Tooling - Produktion. Hanser Verlag, München, 4. Auflage, 2013

[GEK01] GAUSEMEIER, J.; EBBESMEYER, P.; KALLMEYER, F.: Produktinnovation – Strategische Planung und Entwicklung der Produkte von morgen. Carl Hanser Verlag, München, 2001

[GEK11] GAUSEMEIER, J.; ECHTERHOFF, N.; KOKOSCHKA, M.: Direct Manufacturing – innovative Fertigungsverfahren für die Produkte von morgen. In: GAUSEMEIER, J. (Hrsg.): Vorausschau und Technologieplanung. 7. Symposium für Vorausschau und Technologieplanung Heinz Nixdorf Institut, HNI-Verlagsschriftenreihe, Band 300, Paderborn, 2011

[GGL12] GAUSEMEIER, J.; GLATZ, R.; LINDEMANN, U. (Hrsg.): Präventiver Produktschutz – Leitfaden und Anwendungsbeispiele. Carl Hanser Verlag, München, 2012

[GL06] GLÄSER, J. LAUDEL, G.: Experteninterviews und qualitative Inhaltsanalyse, VS Verlag, Wiesbaden, 2. Auflage, 2006

[GLG08] GRIESSBACH, S.; LACH, R.; GRELLMANN, W.: Kleinserienfertigung hochfester Kunststoffbauteile, Kunststoffe 98 (2008) 5, Carl Hanser Verlag, München, 2008, S.29-32

[GLL12] GAUSEMEIER, J.; LANZA, G.; LINDEMANN, U.: Produkte und Produktionssysteme integrativ konzipieren – Modellbildung und Analyse in der frühen Phase der Produktentstehung. Hanser Verlag, München, 2012

[Glo88] GLOBERMANN, S.: Adressing International Product Piracy, Journal of International Business Studies, Palgrave Macmillan, Vol. 19, September 1988, S.497-504

[Gon12] GONCHAROV, M.: Russian Underground 101. Trend Micro Incorporated, Research Paper, 2012

[GP14] GAUSEMEIER, J.; PLASS, C.: Zukunftsorientierte Unternehmensgestaltung – Strategien, Geschäftsprozesse und IT-Systeme für die Produktion von morgen. Carl Hanser Verlag, München, 2. Auflage, 2014

[Gra15-ol] GRASER, F.: Industrie 4.0 beginnt bei der Leiterplatte. Unter: http://www.elektronikpraxis.vogel.de/iot/industrie40/articles/506183/, am 17. März 2016

[Gri14] GRIGORI, K. M.: Prävention und Bekämpfung von Marken- und Produktpiraterie – Leitfäden für Analysen, Ermittlungen und Schutzstrategien. Springer Gabler Verlag, Wiesbaden, 2014

[GRM11] GAMAGE, T. T.; ROTH, T. P.; MCMILLIN, B. M.: Confidentiality Preserving Security Properties for Cyber-Physical Systems. 35th IEEE Annual Computer Software and Applications Conference, 2011, S.28-37

[Gro15] GRONAU, N.: Der Einfluss von Cyber-Physical Systems auf die Gestaltung von Produktionssystemen. Industrie Management, GITO Verlag, März 2015

[GRS03] GORZ, G.; ROLLINGER, C.-R.; SCHNEEBERGER, J. (Hrsg.): Handbuch der Künstlichen Intelligenz. Oldenbourg Wissenschaftsverlag, München, 4. Auflage, 2003

[Gru10] GRÜNEIS, B.: Produktpiraterie in China – Durchsetzung geistiger Eigentumsrechte vs. Wirtschaftlicher Entwicklung. Dissertation, Fakultät für Wirtschaftswissenschaften, Technische Universität München, München, 2010

[GSS15] GACKSTATTER, S.; SPIELER, A.; STEPHAN, J.: Innovation – Deutsche Wege zum Erfolg. Studie der PricewaterhouseCoopers AG, Stuttgart, 2015

[GTD13] GAUSEMEIER, J.; TSCHIRNER, C.; DUMITRESCU, R.: Der Weg zu Intelligenten Technischen Systemen. Industrie Management, GITO Verlag, Januar 2013

[Gue10] GÜNTHER, W.A. (Hrsg.): Integrierter Produktpirateriesschutz durch Kennzeichnung und Authentifizierung kritischer Bauteile im Maschinen- und Anlagenbau – Leitfaden zum Schutz vor Produktpiraterie durch Bauteilkennzeichnung. Technische Universität München, München, 2010

[GW11] GAUSEMEIER, J.; WIENDAHL, H.-P. (Hrsg.): acatech DISKUTIERT, Wertschöpfung und Beschäftigung in Deutschland. Springer-Verlag, Berlin, 2011

[GWF+13] GOPAL, V.; WOLRICH, G. M.; FEGHALI, W. K.; GUILFORD, J. D.; OZTURK, E.; DIXON, M. G.: Method and apparatus for performing efficient side-channel attack resistant reduction using montgomery or barrett reduction. U.S. Patent No. 8.392.494 B2, März 2013

[Han55] HANSEN, F.: Konstruktionssystematik – Eine Arbeitsweise für fortschrittliche Konstrukteure. VEB Verlag Technik, Berlin, 2. Auflage, 1955

[Har02] HARTMANN, J.: Sichere Kommunikation im Internet – Vertraulichkeit, Integrität und Authentizität in einem anonymen Netzwerk. Dissertation, Philosophische Fakultät, Rheinische Friedrich-Wilhelm-Universität Bonn, Bonn, 2002

[Has05] HASKINS, C.: Application of Patterns and Pattern Languages to Systems Engineering. In: Proceedings of 15th Annual International Symposium of the International Council on Systems Engineering, Rochester, Juli 2005

[Hel13] HELLENBRAND, D.: Transdisziplinäre Planung und Synchronisation mechatronischer Produktentwicklungsprozesse. Dissertation, Fakultät für Maschinenwesen, Technische Universität München, Garching, 2013

[Her15] HERTEL, M.: Risiken der Industrie 4.0 – Eine Strukturierung von Bedrohungsszenarien der Smart Factory. In: HMD Praxis der Wirtschaftsinformatik, Vol. 52, Issue 5, Oktober 2015, S.724–738

[Hit07] HITCHINS, D. K.: Systems engineering – A 21st century systems methodology. John Wiley, West Sussex, 2007

[HR85] HARVEY, M.; RONKAINEN, I.A.: International Counterfeiters: Marketing Success without the Cost and the Risk. In: Columbia Journal of World Busines 20 (3), 1985

[HS09] HERZOG, O.; SCHILDHAUER, T. (Hrsg.): acatech DISKUTIERT, Intelligente Objekte: Technische Gestaltung – Wirtschaftliche Verwertung – Gesellschaftliche Wirkung. Springer-Verlag, Berlin, 2009

[HS12a] HESSE, S.; SCHNELL, G.: Sensoren für die Prozess- und Fabrikautomation. Funktion – Ausführung – Anwendung. Vieweg+Teubner Verlag, Wiesbaden, 5. Auflage, 2012

[HS12b] HERING, E.; SCHÖNFELDER, G.: Sensoren in Wissenschaft und Technik – Funktionsweise und Einsatzgebiete. Vieweg+Teubner Verlag, Wiesbaden, 1. Auflage, 2012

[HSL+07] HAN, J.; SHAH, A.; LUK, M.; PERRIG, A.: Don't sweat your privacy: Using humidity to detect human presence. In: Proceedings of 5th International Workshop on Privacy in UbiComp, 2007

[HWF+12] HABERFELLNER, R.; De WECK, O.; FRICKE, E.; VÖSSNER, S. (Hrsg.): Systems Engineering – Grundlagen und Anwendung. Orell füssli Verlag, Zürich, 12. Auflage, 2012

[HY14] HISAKADO, T.; NORITAKA Y.: Device for evaluating side-channel attack resistance, method for evaluating side-channel attack resistance, and program for evaluating side-channel attack. U.S. Patent No. 8.848.903 B2, 2014

[IDC15-ol] ID-CONSULT GMBH: METUS Methodik. Unter: http://id-consult.com/metus/metus-methodik, am 3. Dezember 2015

[IKT16-ol] CLUSTER INFORMATIONS- UND KOMMUNIKATIONSTECHNOLOGIE NRW: Industrie 4.0 steigert die Erträge in der Landwirtschaft. Unter: http://ikt.nrw.de/iktnrw-staerken-sichtbar-machen/nrw-zeigt-profil/portraet-claas-telekom, am 16. Mai 2016

[INC07] INTERNATIONAL COUNCIL ON SYSTEMS ENGINEERING (INCOSE): Systems Engineering Vision 2020, INCOSE, San Diego, 2007

[INC10] INTERNATIONAL COUNCIL ON SYSTEMS ENGINEERING (INCOSE): Systems Engineering Handbook – A Guide for System life cycle processes and activities. International council on Systems Engineering (INCOSE), Version 3.2, 2010

[INC12] INTERNATIONAL COUNCIL ON SYSTEMS ENGINEERING (INCOSE): INCOSE Systems Engineering Handbuch – Deutsche Übersetzung. GfSE, 2012

[ISO7498] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO): Information technology – Open Systems Interconnection – Basic Reference Modell: The Basic Model – ISO/IEC 7498-1, Genève, 1994

[its12] ITSOWL: Intelligente Technische Systeme OstwestfalenLippe … für die Märkte von Morgen – Strategie, Mai 2012

[JGS10] JIANG, W.; GUO, W.; SANG, N.: Periodic Real-Time Message Scheduling for Confidentiality-Aware Cyber-Physical System in Wireless Networks. In: 5th International Conference on Frontier of Computer Science and Technology, 2010, S.355-360

[JW14] JAHNKE, U.; WIGGE, F.: Potenzial additiver Fertigungsverfahren zur Prävention gegen Produktpiraterie, in CNC-Arena eMagazine März 2014

[KA11] KUSKE, P.; ABELE, E.: Produktpiraterie im Maschinenbau – Herausforderung im 21. Jahrhundert. In: ABELE, E.; KUSKE, P.; LANG, H.: Schutz vor Produktpiraterie – Ein Handbuch für den Maschinen- und Anlagenbau. Springer-Verlag, Berlin, 2011

[Kai13] KAISER, L.: Rahmenwerk zur Modellierung einer plausiblen Systemstruktur mechatronischer Systeme. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Band 327, Paderborn, 2013

[Kal98] KALLMEYER, F.: Eine Methode zur Modellierung prinzipieller Lösungen mechatronischer Systeme. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Band 42, Paderborn, 1998

[KBG09] KEUPP, M. M.; BECKENBAUER, A.; GASSMANN, O.: How managers protect intellectual property rights in China using de facto strategies. In: R&D Management, Vol. 39, Issue 2, März 2009, S.211–224

[KFG07] KRAUSE, F.-L.; FRANKE, H.-J.; GAUSEMEIER, J. (Hrsg.): Innovationspotenziale in der Produktentwicklung, Carl Hanser Verlag, München, 2007

[KJT+13] KALAWSKY, R. S.; JOANNOU, D.; TIAN, Y.; FAYOUMI, A.: Using architecture patterns to architect and analyze systems of systems. In: Procedia Computer Science, Vol. 16, 2013, S.283-292

[Kle13] KLEINE, O.: Planung von Strategien gegen industrielle Produktpiraterie, Springer-Gabler Verlag, Heidelberg, 2013

[KLH13] KWON, C.; LIU, W.; HWANG, I.: Security Analysis for Cyber-Physical Systems against Stealthy Deception Attacks. In: American Control Conference (ACC), Washington, DC, Juni 2013, S.3344-3349

[KM06] KAO, J.-C.; MARCULESCU, R.: Eavesdropping Minimization via Transmission Power Control in Ad-Hoc Wireless Networks. In: 2006 3rd Annual IEEE Communications Society on Sensor and Ad Hoc Communications and Networks, Vol. 2, 2006, S.707-714

[KM10] KILLOURHY, K.; MAXION, R.: Why Did My Detector Do That?! – Predicting Keystroke-Dynamics Error Rates. In: Proceedings of Recent Advances in Intrusion Detection – 13th International Symposium, 2010, S.256-276

[Koe12a] KÖSTER, O.: Folgen der Produktpiraterie – Welche Konsequenzen zieht Produktpiraterie nach sich? In: GAUSEMEIER, J.; GLATZ, R.; LINDEMANN, U. (Hrsg.): Präventiver Produktschutz – Leitfaden und Anwendungsbeispiele. Carl Hanser Verlag, München, 2012

[Koe12b] KÖSTER, O.: Imitat, Plagiat, Fälschung – Was ist was und was ist (il)legal? In: GAUSEMEIER, J.; GLATZ, R.; LINDEMANN, U.: Präventiver Produktschutz – Leitfaden und Anwendungsbeispiele, Carl Hanser Verlag, München, 2012

[Kok12a] KOKOSCHKA, M.: Kategorisierung von Schutzmaßnahmen. In: GAUSEMEIER, J.; GLATZ, R.; LINDEMANN, U. (Hrsg.): Präventiver Produktschutz – Leitfaden und Anwendungsbeispiele. Carl Hanser Verlag, München, 2012

[Kok12b] KOKOSCHKA, M.: Strategische Schutzmaßnahmen. In: GAUSEMEIER, J.; GLATZ, R.; LINDEMANN, U. (Hrsg.): Präventiver Produktschutz – Leitfaden und Anwendungsbeispiele. Carl Hanser Verlag, München, 2012

[Kok12c] KOKOSCHKA, M.: Schutzmaßnahmen in der Produktentwicklung. In: GAUSEMEIER, J.; GLATZ, R.; LINDEMANN, U. (Hrsg.): Präventiver Produktschutz – Leitfaden und Anwendungsbeispiele. Carl Hanser Verlag, München, 2012

[Kok13] KOKOSCHKA, M.: Verfahren zur Konzipierung imitationsgeschützter Produkte und Produktionssysteme. Dissertation, Universität Paderborn, HNI-Verlagsschriftenreihe, Band 313, Paderborn, 2013

[Kra15] KRAUTZ, V.: Beta Layout erhält europäisches Patent für RDID-Einbettverfahren. In: Produktion von Leiterplatten und Systemen (PLUS), Eugen G. Leuze Verlag, Bad Saulgau, Ausgabe 10, 2015, S.1920

[KS12] KATZENBEISSER, S.; SCHALLER, A.: Physical Unclonable Functions – Sicherheitseigenschaften und Anwendungen. In: DuD Datenschutz und Datensicherheit, Ausgabe 12, 2012, S.881-885

[Kus13] KUSKE, P.: Methode zur Gestaltung einer Know-how-Schutzstrategie für den Maschinen- und Anlagenbau. Dissertation, Technische Universität Darmstadt, Shaker Verlag, Aachen, 2013

[Laa93] LAATZ, W.: Empirische Methoden – Ein Lehrbuch für Sozialwissenschaftler. Harri Deutsch, Frankfurt am Main, 1993

[Lam10] LAMNEK, S.: Qualitative Sozialforschung, Beltz Verlag, Weinheim, 5. Auflage, 2010

[Lan07] LANGE, F.: Der Bauplan im Innern – Plagiatschutz durch Werkstückkennzeichnung innerhalb des Bauteils. In: phi – Produktionstechnik Hannover informiert, Ausgabe 2, 2007, S.10-11

[Len02] LENZEN, M.: Natürliche und künstliche Intelligenz – Einführung in die Kognitionswissenschaft. Campus Verlag, Frankfurt am Main, 2002

[Lik32] LICKERT, R.: A Technique for the Measurement of Attitudes. Virginia, 1932

[LJK+13] LINDEMANN, C.; JAHNKE, U.; KLEMP, E.; KOCH, R.: Additive Manufacturing als serienreifes Produktionsverfahren. Industrie Management, GITO Verlag, Februar 2013

[LL06] LECOINTRE, G; LE GUYADER, H.: Biosystematik: Alle Organismen im Überblick. Springer-Verlag, Berlin 2006

[LMP+12a] LINDEMANN, U.; MEIWALD, T.; PETERMANN.; SCHENKL, S.: Know-how-Schutz imWettbewerb – Gegen Produktpiraterie und unerwünschten Wissenstransfer. Springer-Verlag, Berlin, 2012

[LMP+12b] LINDEMANN, U.; MEIWALD, T.; PETERMANN.; SCHENKL, S., KOKOSCHKA, M.: Bedarfsanalyse Produktschutz. In: GAUSEMEIER, J.; GLATZ, R.; LINDEMANN, U. (Hrsg.): Präventiver Produktschutz – Leitfaden und Anwendungsbeispiele. Carl Hanser Verlag, München, 2012

[Lor12] LORENZEN, B.: Rechtliche Schutzmaßnahmen. In: GAUSEMEIER, J.; GLATZ, R.; LINDEMANN, U. (Hrsg.): Präventiver Produktschutz – Leitfaden und Anwendungsbeispiele. Carl Hanser Verlag, München, 2012

[LSG15] LACHMAYER, R.; SAUTHOFF, B.; GOTTWALD, P.: Technische Vererbung in der Produktentwicklung. In: Konstruktion, Springer-VDI-Verlag, Ausgabe 7-8, 2015, S.69

[LVM09] LINDA, O.; VOLLMER, T.; MANIC, M.: Neural Network based Intrusion Detection System for critical infrastructures. In: International Joint Conference on Neural Networks, 2009, S.1827-1834

[MC11a] MITCHELL, R.; CHEN, I.-R.: A Hierarchical Performance Model for Intrusion Detection in Cyber-Physical Systems. In: IEEE Wireless Communications and Networking Conference (WCNC), 2011, S.2095-2100

[MC11b] MITCHELL, R.; CHEN, I.-R.: Survivability Analysis of Mobile Cyber-Physical Systems with Voting-based Intrusion Detection. 7th International Wireless Communications and Mobile Computing Conference (IWCMC), 2011, S.2256-2261

[MC13a] MITCHELL, R.; CHEN, I.-R.: Effect of Intrusion Detection and Response on Reliability of Cyber Physical Systems. In: IEEE Transactions on Reliability, Vol. 62, Nr. 1, März 2013, S.199-210

[MC13b] MITCHELL, R.; CHEN, I.-R.: Behavior-Rule Based Intrusion Detection Systems for Safety Critical Smart Grid Applications. In: IEEE Transactions on Smart Grid, Vol. 4, Nr. 3, September 2013, S.1254-1263

[Mei08] MEIER, H.; VÖLKER, O.; BINNER, S. M.: Ein ganzheitlicher aktiver Ansatz zum Schutz gegen Produktpiraterie. Industrie Management, GITO Verlag, Juni 2008

[Mei10] MEIMANN, V.: Ein Beitrag zum ganzheitlichen Know-how-Schutz von virtuellen Produktmodellen in Produktentwicklungsnetzwerken. Dissertation, Ruhr-Universität Bochum, Bochum, 2010

[Mei11] MEIWALD, T.: Konzepte zum Schutz vor Produktpiraterie und unerwünschtem Knowhow-Abfluss. Dissertation, Fakultät für Maschinenwesen, Technische Universität München, München, 2011

[Mei90] MEISTER, H. E.: Leistungsschutz und Produktpiraterie – Fragmente zu einem Phänomen. Frankfurt am Main, 1990

[Mer14] MERLI, D.: Attacking and Protecting Ring Oscillator Physical Unclonable Functions and Code-Offset Fuzzy Extractors. Dissertation, Technische Universität München, München, 2014

[MI08] MÖHRLE, M.G.; ISENMANN, R.: Grundlagen des Technologie-Roadmapping. In: MÖHRLE, M. G.; ISENMANN, R (Hrsg.): Technologie-Roadmapping: Zukunftsstrategien für Technologieunternehmen. Springer-Verlag Berlin, 3. Auflage, 2008

[Mit09] MITTELSTAED A.: Strategisches IP-Management – mehr als nur Patente. Gabler, 2009

[MKP12] MORADI, A.; KASPER, M.; PAAR, C.: Black-Box Side-Channel Attacks Highlight the Importance of Countermeasures. In: DUNKELMANN (Hrsg.): Topics in Cryptology – CT-RSA 2012, Springer-Verlag, Berlin, 2012, S.1-18

[MS05] MAILIK, H.; SCHINDLER, S.: Fälschungssichere Verpackungen – Sicherheitstechnologien und Produktschutz. Hüthig Verlag, Heidelberg, 2005

[MS12] MERLI, D.; SIGL, G.: Physical Unclonable Functions – CMOS-Implementierungen und Hardware Attacken. In: Datenschutz und Datensicherheit, Ausgabe 12, 2012, S.876-880

[MWS06] MEYER, M.; WALBER, B.; SCHMIDT, C.: Produktionsplanung und -steuerung (PPS) in temporären Produktionsnetzwerken des Maschinen- und Anlagenbaus. In: SCHUH, G. (Hrsg.) Produktionsplanung und -steuerung – Grundlagen, Gestaltung und Konzepte. Springer-Verlag Berlin, 3. Auflage, 2006

[Nee07] NEEMANN, C. W.: Methodik zum Schutz gegen Produktimitationen, Dissertation Fraunhofer-Institut für Produktionstechnologie IPT, Aachen, Shaker Verlag, Band 13/2007, Aachen, 2007

[NT97] NONAKA, I.; TACKEUCHI, H.: Die Organisation des Wissens – Wie japanische Unternehmen eine brachliegende Ressource nutzbar machen. Campus Verlag, Frankfurt am Main, 1997

[OEC96] ORGANISATION FÜR WIRTSCHAFTLICHE ZUSAMMENARBEIT UND ENTWICKLUNG (OECD) (Hrsg.): The Knowledge-Based Economy, Paris, 1996

[ONF12-ol] OPEN NETWORKING FOUNDATION (ONF): Software-Defined Networking: The New Norm forNetworks. Unter: https://www.opennetworking.org/images/stories/downloads/sdn-resources/white-papers/wp-sdn-newnorm.pdf, am 13. März 2016

[ONF15-ol] OPEN NETWORKING FOUNDATION (ONF): Principles and Practices for Securing Software-Defined Networks. Unter: https://www.opennetworking.org/images/stories/downloads/sdn-resources/technical-reports/Principles_and_Practices_for_Securing_Software-Defined_Networks_applied_to_OFv1.3.4_V1.0.pdf, am 13. März 2016

[OWL15-ol] TECHNOLOGIE-NETZWERK IT'S OWL: Spitzencluster Intelligente Technische Systeme OstwestfalenLippe – it's OWL. Unter: http://www.its-owl.de/technologie-netzwerk/strategie/intelligente-technische-systeme, am 23. November 2015

[PAN10] PHAM, N.; ABDELZAHER, T.; NATH, S.: On Bounding Data Stream Privacy in Distributed Cyber-physical Systems. In: IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, 2010, S.221-228

[PBF+07] PAHL, G.; BEITZ, W.; FELDHUSEN, J.; GROTE, K.-H.: Konstruktionslehre – Grundlagen erfolgreicher Produktentwicklung – Methoden und Anwendung. Springer-Verlag, Berlin, 7. Auflage, 2007

[PCH+11] PFISTER, F.; CHAPURLAT, V.; HUCHARD, M.; NEBUT, C.: A Design Pattern meta model for Systems Engineering. In: Proceedings of 18th IFAC (International Federation of Automatic Control) World Congress, Mailand, 2011

[PDB13] PASQUALETTI, F.; DÖRFLER, F.; BULLO,F.: Attack Detection and Identification in Cyber-Physical Systems. In: IEEE Transactions on Automatic Control, Vol. 58, Nr. 11, November 2013, S.2715-2729

[PG13-ol] PFROMM, H.; GRASER, F.: Die Leiterplatte von morgen trägt ihre Identität immer bei sich. Unter: http://www.elektronikpraxis.vogel.de/leiterplattenfertigung/articles/403018/, am 17. März 2016

[Pol66] POLANYI, M.: The Tacit Dimension. The University of Chicago Press, Chicago, 1966

[Por00] PORTER, M.: Wettbewerbsvorteile – Spitzenleistungen erreichen und behaupten. Campus Verlag, Frankfurt, New York, 6. Auflage, 2000

[PR13] PROUFF, E.; RIVAIN, M.: Masking against Side-Channel Attacks: A Formal Security Proof. In: Advances in Cryptology – EUROCRYPT, Proceedings of 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Mai 2013, S.142-159

[PRR06] PROBST, G.; RAUB, S.; ROMHARDT, K.: Wissen managen – Wie Unternehmen ihre wertvollste Ressource optimal nutzen. Gabler Verlag, Wiesbaden, 2006

[PS02] SAMUELSON, P.; SCOTCHMER, S.: The law and economics of reverse engineering, Yale Law Journal, Vol 111, No. 7, Mai 2002, S.1575-1664

[PZ12] PLACZEK, M.; ZIMMERMANN, S.: Informationstechnische Schutzmaßnahmen. In: GAUSEMEIER, J.; GLATZ, R.; LINDEMANN, U.: Präventiver Produktschutz – Leitfaden und Anwendungsbeispiele. Carl Hanser Verlag, München, 2012

[Ren95] RENIUS, K. T.: Mähdrescher. In: HIERSIG, H. M. (Hrsg.): VDI-Lexikon Maschinenbau, Springer-Verlag, Berlin, 1995

[Ris98] RISING L.: The Patterns Handbook: Techniques, Strategies, and Applications. Cambridge University Press, 1998

[Ris00] RISING, L.: The Pattern Almanac. Cambridge University Press, 2000

[RN05] RUSSEL, S.-J.; NORVIG, P.: Artificial Intelligence – A Modern Approach. Pearson Education, New Jersey, 2005

[Rog99] ROGULIC, B.: Ein gesamthaftes Prozessmodell zur Identifikation von Kernkompetenzen. Dissertation, Hochschule für Wirtschafts-, Rechts- und Sozialwissenschaften (HSG), Universität St. Gallen, St. Gallen, 1999

[Rog00] ROGULIC, B.: Praxisorientiertes Wissensmanagement – Identifikation von Kernkompetenzen als Voraussetzung für erfolgreiches Wissensmanagement, Dr. Hermann Schindler, Bad Homburg, 2000

[Rop09] ROPOHL, G., „Allgemeine Technologie – Eine Systemtheorie der Technik. Third edition“, Universitaetsverlag Karlsruhe, Karlsruhe, 2009

[Sau06] SAUER, T.: Ein Konzept zur Nutzung von Lösungsobjekten für die Produktentwicklung in Lern- und Assistenzsystemen. VDI-Fortschritt-Berichte, VDI Reihe 1, Nr. 390, VDI Verlag, Düsseldorf, 2006

[SB89] SAUTER, N.; BUNTE, H.-J.: EG-Gruppenfreistellungsverordnung, München, 1989

[Sch09] SCHNAPAUFF, K.: Präventiver Nachahmungsschutz bei technischen Produkten – für industrielle oder professionelle Anwendungen. Dissertation, Fakultät Wirtschaftswissenschaften, Technische Universität München, München, 2009

[Sch11] SCHRÖDER, L.: Maßnahmen der Produktgestaltung. In: ABELE, E.; KUSKE, P.; LANG, H.: Schutz vor Produktpiraterie – Ein Handbuch für den Maschinen- und Anlagenbau. Springer-Verlag, Berlin, 2011

[Seh10] SEHRT, J.T.: Möglichkeiten und Grenzen bei der generativen Herstellung metallischer Bauteile durch das Strahlschmelzverfahren. Dissertation. Shaker, Aachen, 2010

[SD13] STELTE, B.; RODOSEK, G. D.: Assuring Trustworthiness of Sensor Data for Cyber-Physical Systems. In: IFIP/IEEE International Symposium on Integrated Network Management, Mai 2013, S.395-402

[Sen13] SENDLER, U. (Hrsg.): Industrie 4.0 – Beherrschung der industriellen Komplexität mit SysLM. Springer-Verlag, Berlin, 2013

[SH14] SCHIMMEL, O.; HENNING, M.: Kopier- und Manipulationsschutz für eingebettete Systeme. In: Datenschutz und Datensicherheit, Ausgabe 11, 2014, S.742-746

[SKJ+10] SHIN, S.; KWON, T.; JO, G.-Y.; PARK, Y.; RHY, H.: An Experimental Study of Hierarchical Intrusion Detection for Wireless Industrial Sensor Networks. In: IEEE Transactions on Industrial Informatics, Vol. 6, Nr. 4, November 2010, S.744–757

[SKN+15] SHIOZAKI, M.; KUBOTA, T.; NAKAI, T.; TAKEUCHI, A.; NISHIMURA, T.; FUJINO, T.: Tamper-Resistant Authentication System with Side-Channel Attack Resistant AES and PUF using MDR-ROM. In: IEEE International Symposium on Circuits and Systems (ISCAS), Mai 2015, S.1462-1465

[SKS+11] SCHUH, G.; KLAPPERT, S.; SCHUBERT, J.; NOLLAU, S.: Grundlagen zum Technologiemanagement. In: SCHUH, G.; KLAPPERT, S. (Hrsg.): Technologiemanagement – Handbuch Produktion und Management 2. Springer-Verlag, Berlin, 2011

[SN10] SIEBEL, C.; NAHR, M: Ganzheitliches und präventives Schutzkonzept für Investitionsgüter (PROTACTIVE). In: KLEINE, O.; KREIMEIER, D.; LIEBERKNECHT, N. (Hrsg.): Piraterierobuste Gestaltung von Produkten und Prozessen. Band 1 der Reihe „Innovationen gegen Produktpiraterie“, VDMA-Verlag, Frankfurt am Main, 2010

[Spr15-ol] SPRINGER GABLER VERLAG (Herausgeber), Gabler Wirtschaftslexikon, Stichwort: Geistiges Eigentum. Unter: http://wirtschaftslexikon.gabler.de/Archiv/634523991/geistiges-eigentum-v2.html, am 28. März 2015

[SPY+13] SHIN, S.; PORRAS, P.; YEGNESWARAN, V.; FONG, M.; GU, G.; TYSON, M.: FRESCO: Modular Composable Security Services for Software-Defined Networks. In: ISOC Network and Distributed System Security Conference, San Diego, Februar 2013

[SSC+13] SEZER, S.; SCOTT-HAYWARD, S.; CHOUHAN, P. K.; FRASER, B.; LAKE, D.; FINNEGAN, J.; VILJOEN, N.; MILLER, M. RAO, N.: Are We Ready for SDN? Implementation Challenges for Software-Defined Networks. IEEE Communications Magazine, Vol. 51, Issue 7, 2013, S.36-43

[SSM10] SCHALLNUS, R.; STEPHAN, R.; MEISSNER, K.: Technologieschutz. In: KLEINE, O.; KREIMEIER, D.; LIEBERKNECHT, N. (Hrsg.): Piraterierobuste Gestaltung von Produkten und Prozessen. Band 1 der Reihe „Innovationen gegen Produktpiraterie“, VDMAVerlag, Frankfurt am Main, 2010

[Stef04] STEFFEN, A.: Secure Communications in Embedded Systems. In: ZURAWSKI, R.: The Industrial Information Technology Handbook. CRC Press, Boca Raton, 2005, Kap. 91, S.1-12

[STF09] STAAKE, T.; THIESSE, F.; FLEISCH, E.: The Emergence of Counterfeit Trade – A Literature Review. In: European Journal of Marketing 32(3/4), 2009, S.320-349

[STF12] STAAKE, T.; THIESSE, F.; FLEISCH, E.: Business Strategies in the Counterfeit Market. In: Journal of Business Research. Vol. 65, Issue 5, Mai 2012

[Str96] STRUBE, G.: Wörterbuch der Kognitionswissenschaft. Klett-Cotta, 1996

[Str98] STRUBE, G.: Modelling Motivation and Action Control in Cognitive Systems. In: SCHMID, U.; KREMS, J. F.;WYSOCKII, F.: Mind Modelling. Pabst, Berlin, 1998

[Suh93] SUHM, A.: Produktmodellierung in wissensbasierten Konstruktionssystemen auf Basis von Lösungsmustern. Dissertation, Fakultät für Maschinenbau, Universität Karlsruhe, Reihe Konstruktionstechnik, Verlag Shaker, Aachen, 1993

[SW07] SCHÄFER, W.; WEHRHEIM, H.: The Challenges of Building Advanced Mechatronic Systems. In: FOSE ´07: 2007 Future of Software Engineering, IEEE Computer Society, 2007, S.72-84

[SZ03] SANZ, R.; ZALEWSKI, J.: Pattern Based Control Systems Engineering – Using Design Patterns to Document, Transfer and Exploit Design Knowledge. IEEE Control Systems Magazine, 2003, S.46-60

[Tel16-ol] TELEKOM Ein Netz im Kornfeld. Unter: https://www.telekom.com/innovation/industrie4.0/claas/245778, am 16. Mai 2016

[TG10] TRETOW, G.; GÖPFERT, J.: Systems-Engineering in der frühen Phase der Produktentwicklung. CAD-CAM Report April 2010, S.58-61

[TGH08] TRETOW, G.; GÖPFERT, J.; HEESE, C.: In sieben Schritten systematisch entwickeln. CAD-CAM Report August 2008, Hoppenstedt Publishing, S.36-39

[Thi13] van THIEL, B.: Entwicklung einer Methodik zur Zustandsüberwachung von Bauteilen aus sensitiven Werkstoffen. Dissertation, Fakultät für Maschinenbau, Gottfried Wilhelm Leibniz Universität Hannover, Garbsen, 2013

[Tho15-ol] THOMA, J.: Gehackte Teslas lassen sich bei voller Fahrt ausschalten. Unter: http://www.golem.de/news/auto-hacking-gehackte-teslas-lassen-sich-bei-voller-fahrt-ausschalten-1508-115641.html, am 23. November 2015

[Trä09] TRÄCHTLER, A.: Entwurf intelligenter mechatronischer Systeme – Regelungstechnische Konzepte für selbstoptimierendes Verhalten. In: Tagungsband des 6. Paderborner Workshop Entwurf mechatronischer Systeme, 2.-3. April, HNI-Verlagsschriftenreihe, Band 250, Paderborn, 2009

[TYK+10] TANG, L. A.; YU; X.; KIM; S.; HAN; J.; HUNG; C. C.; PENG, W. C.: Tru-Alarm: Trustworthiness Analysis of Sensor Networks in Cyber-Physical Systems. In: IEEE 10th International Conference on Data Mining (ICDM), 2010, S.1079-1084

[VBS08] VOIGT, K.-I.; BLASCHKE, M.; SCHEINER, C.W.: Einsatz und Nutzen von Innovationsschutzmaßnahmen im Kontext von Produktpiraterie. In: SPECHT, D. (Hrsg.): Produkt- und Prozessinnovationen in Wertschöpfungsketten, Gabler Verlag, Wiesbaden, 2008

[VDI2206] VEREIN DEUTSCHER INGENIEURE (VDI): Entwicklungsmethodik für mechatronische Systeme. VDI-Richtlinie 2206, Beuth Verlag, Berlin, 2004

[VDI2221] VEREIN DEUTSCHER INGENIEURE (VDI) 2221: Methodik zum Entwickeln und Konstruieren technischer Systeme und Produkte. Beuth Verlag, Berlin, 1993

[VDM13] VERBAND DEUTSCHER MASCHINEN- UND ANLAGENBAU e. V. (VDMA): Studie Status Quo der Security in Produktion und Automation 2013/14, Frankfurt am Main, 2013

[VDM14a] VERBAND DEUTSCHER MASCHINEN- UND ANLAGENBAU e. V. (VDMA): Studie Produktpiraterie 2014, Frankfurt am Main, 2014

[VDM14b] VERBAND DEUTSCHER MASCHINEN- UND ANLAGENBAU e. V. (VDMA); MCKINSEY & COMPANY: Zukunftsperspektive deutscher Maschinenbau – Erfolgreich in einem dynamischen Umfeld agieren, 2014

[VDM15] VERBAND DEUTSCHER MASCHINEN- UND ANLAGENBAU e. V. (VDMA): Maschinenbau in Zahl und Bild 2015, Frankfurt am Main, 2015

[VDM16] VERBAND DEUTSCHER MASCHINEN- UND ANLAGENBAU e. V. (VDMA): Studie Produktpiraterie 2016, Frankfurt am Main, 2016

[WAB+07] WILDEMANN, H.; ANN, C.; BROY, M.; GÜNTHNER, W.; LINDEMANN, U.: Plagiatschutz – Handlungsspielräume der produzierenden Industrie gegen Produktpiraterie. TCW Transfer-Centrum, München, 2007

[WEF14] WORLD ECONOMIC FORUM; MCKINSEY & COMPANY: Risk and Responsibility in a Hyperconected World – Insight Report, 2014

[Wei06] WEILKIENS, T.: Systems Engineering mit SysML/UML – Modellierung, Analyse, Design. dpunkt Verlag, Heidelberg, Germany, 2008

[Wil14-ol] WILLHARDT, R.: Smart Farming, Smart Factoring & Co. – Wo Bauern den Autofirmen was vormachen. Unter: http://www.handelsblatt.com/technik/vernetzt/smart-farming-smart-factoring-und-co-wo-bauern-den-autofirmen-was-vormachen/10708266-all.html, am 16. Mai 2016

[WIP08] WORLD INTELLECTUAL PROPERTY ORGANIZATION (WIPO); Understanding industrial property. WIPO publication no. 895(E), Geneva, 2008

[WG07] VON WELSER, M.; GONŹALES, A.: Marken- und Produktpiraterie – Strategien und Lösungsansätze zu ihrer Bekämpfung, WILEY-VCH Verlag, Weinheim, 2007

[WGN15] WINKENS, M.; GOERKE, M.; NYHUIS, P.: Use of Life Cycle Data for Condition-Oriented Maintenance. In: WORLD ACADEMY OF SCIENCE, ENGINEERING AND TECHNOLOGY (Hrsg.): International Science Index 100 – International Journal of Social, Behavioral, Educational, Economic, Business and Industrial Engineering. Vol. 9, Nr. 4, 2015, S.1216-1219

[XP15] XU, T.; POTKONJAK, M.: Stable and Secure Delay-based Physical Unclonable Functions Using Device Aging. In: IEEE International Symposium on Curcuits and Systems (ISCAS), Lissabon, Mai 2015, S.33-36

[XRH+15] XU, X.; RAHMATI, A.; HOLCOMB, D. E.; FU, K.; BURLESON, W.: Reliable Physical Unclonable Functions Using Data Retention Voltage of SRAM Cells. In: IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, Vol. 34, Issue 6, 2015, S.903-914

[ZA13] ZIMMER, D.; ADAM, G.: Konstruktionsregeln für Additive Fertigungsverfahren. In: Zeitschrift Konstruktion, Vol. 2013, Issue 7/8, 2013, S.77-82

[ZBM+10] ZIMMER, C.; BHAT, B.; MUELLER, F.; MOHAN, S.: Time-Based Intrusion Detection in Cyber-Physical Systems. In: ICCPS '10 Proceedings of the 1st ACM/IEEE International Conference on Cyber-Physical Systems, 2010, S.109-118

[ZM11] ZHU, M.; MARTÍNEZ, S.: Stackelberg-game analysis of correlated attacks in cyber-physical systems. In: American Control Conference (ACC), San Francisco, 2011, S.4063-4068

Anhang

Inhaltsverzeichnis Seite

A1 Ergänzung zu Kapitel 3.1 – Bestehende Schutzmaßnahmen und deren Darstellung

A1.1 Schutzmaßnahmensteckbrief nach LINDEMANN ET AL.

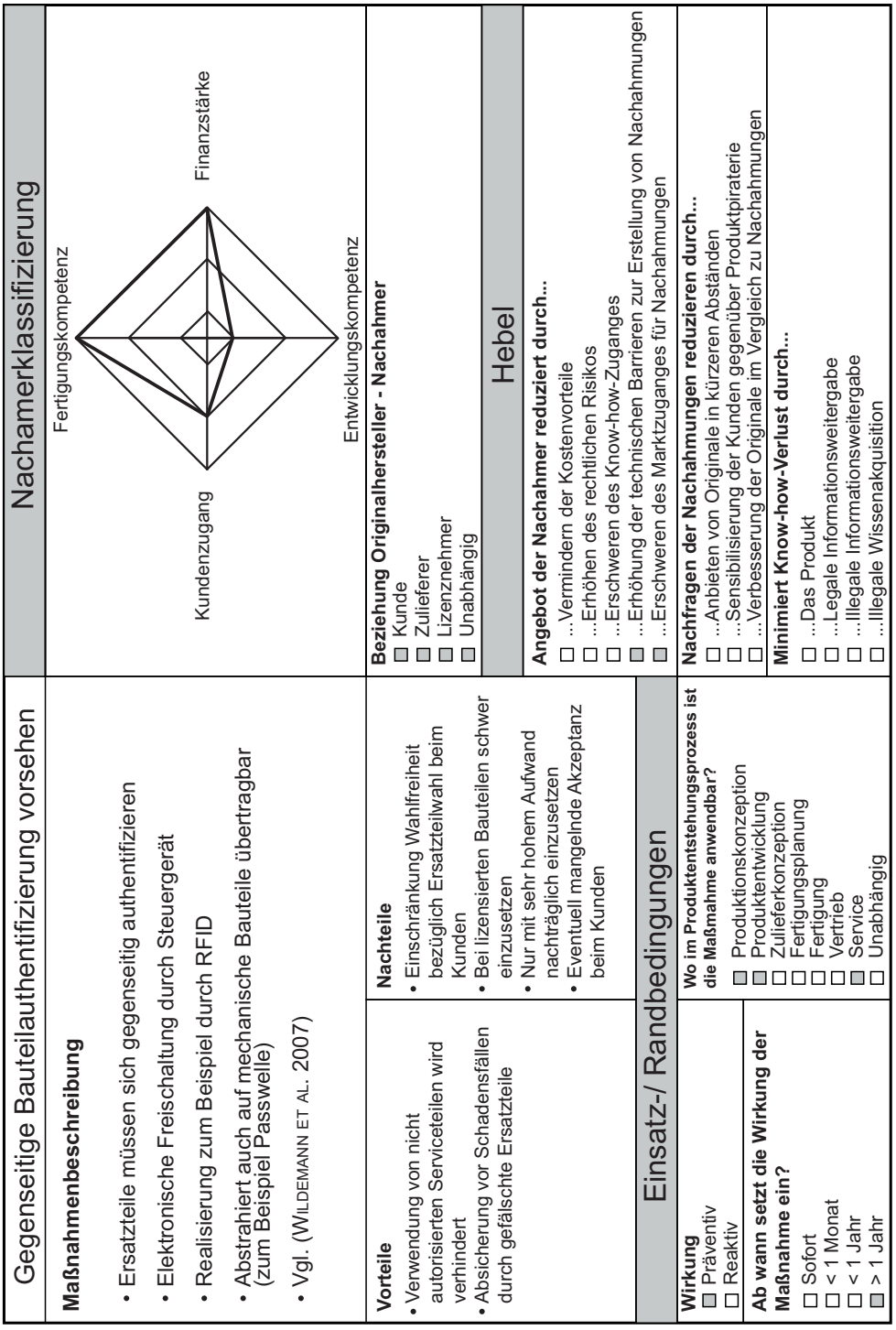


Bild A-1: Steckbrief Gegenseitige Bauteilauthentifizierung vorsehen [LMP+12a, S.196f.]

A1.2 Schutzmaßnahmensteckbrief nach GAUSEMEIER ET AL.

Sichere Kommunikationsverbindungen (sicherer Informationsfluss)

Kurzbeschreibung

Ziel der sicheren Kommunikationsverbindung ist es, Kommunikationswege so aufzubauen, dass unbefugte Dritte keine Möglichkeit haben, die Inhalte abzugreifen.

Anwendungen / Vorgehen

Es existieren mehrere Verfahren zum Aufbau sicherer Kommunikationsverbindungen. Bei der Verschlüsselung wird ein Klartext (die Information) mithilfe eines Verschlüsselungsverfahrens in einen Geheimtext umgewandelt. Ein Verfahren ist die Verschlüsselung von E-Mails mithilfe eines Zusatzprogramms. Dabei werden kryptographische Verfahren verwendet, um Informationen zu transformieren und so eine E-Mail mitlesesicher zu machen. Ein anderes Verfahren ist die Steganografie. Steganografie ist die Wissenschaft der verborgenen Speicherung oder Übermittlung. Dabei werden die Informationen verborgen, sodass sie als solche in der Mitteilung (dem Träger) nicht zu erkennen sind. Man tarnt geheime Informationen, während der Träger der Information (Medium bzw. Trägerdatei) keine weitere Funktion haben muss, jedoch haben kann.

Unternehmensbereiche

- [x] Produktplanung
- [x] Entwicklung / Konstruktion
- [x] Einkauf
- [x] Arbeitsvorbereitung
- [x] Fertigung
- [x] Vertrieb
- [ ] Service

Kategorie Schutzmaßnahme

- [ ] Strategische Maßnahme
- [ ] Produktbezogene Maßnahme
- [ ] Prozessbezogene Maßnahme
- [ ] Kennzeichnende Maßnahme
- [x] IT-Maßnahme
- [ ] Rechtliche Maßnahme
- [ ] Kommunikationsmaßnahme

Anwendungsbeispiele

Die Firma mirabyte bietet das Produkt FrontFace an, mit dem der interne Informationsfluss einer Firma, wie z. B. ein interner E-Mail-Dienst, abgewickelt werden kann. Zudem werden die IT-Systeme und die IT-Infrastruktur geschützt, indem z. B. Server überwacht werden. Anwender dieses Programms sind z. B. die Unternehmen BASF, Eastern Airways, Intel und Vedes [Mir11a-ol].

Vorteile

- „Unsichtbare“ Schutzmaßnahme

Nachteile

- Kompatibilitätsprobleme unterschiedlicher Programme
- Mangelnde Sensibilität führt zum Umgehen von definierten Schutzmechanismen
- Kommunikation mit Externen kann erschwert werden

Quellen / Experten

[Mir11a-ol] MIRABYTE: Business Messenger. Unter: http://www.mirabyte.com/de/produkte/business-messenger/, 5. Juli 2011

Bild A-2: Steckbrief für Sichere Kommunikationsverbindungen [GGL12, S.262]

Gegenseitige Authentifizierung von Komponenten

Kurzbeschreibung

Bei der gegenseitigen Authentifizierung wird eine Austauschkomponente von einer Steuerungseinheit einer Anlage/Maschine auf ihre Originalität überprüft.

© Paul Fleet - Fotolia.com

Anwendungen / Vorgehen

Beim Einbau eines Ersatzteils in eine Anlage/Maschine wird das Bauteil durch die Maschinensteuerung authentifiziert, indem sie von der Austauschkomponente zuvor definierte Daten abfragt (z. B. über RFID-Chips). Nur wenn die Komponente über die geforderten Daten verfügt, wird sie von der Anlage für ihre Funktion zugelassen. Damit wird seitens des Originalherstellers angestrebt, dass durch den Kunden Originalteile verwendet werden. Bei Verwendung von Originalteilen werden dem Kunden beispielsweise verlängerte Garantiezeiträume oder bestimmte Verfügbarkeiten der Maschine zugesichert. Erweist sich bei der Authentifizierung ein Ersatzteil als Fälschung, erhält der Benutzer eine Meldung darüber, die quittiert werden muss. Somit entsteht eine Absicherung gegen Schadensansprüche durch Versagen von Anlagen aufgrund gefälschter Ersatzteile. Eine Abschaltung der Maschine bei Verwendung von Nichtoriginalteilen ist nach deutschem Recht nicht zulässig. Die gegenseitige Authentifizierung von Komponenten erfolgt entweder durch in der Komponente eingebettete Steuerungssoftware oder durch Sensoren, die Austauschkomponenten ohne eigene Steuerungs- oder Produktsoftware erkennen.

Unternehmensbereiche

- ☐ Produktplanung
- ■ Entwicklung / Konstruktion
- ☐ Einkauf
- ☐ Arbeitsvorbereitung
- ☐ Fertigung
- ☐ Vertrieb
- ■ Service

Kategorie Schutzmaßnahme

- ☐ Strategische Maßnahme
- ■ Produktbezogene Maßnahme
- ■ Prozessbezogene Maßnahme
- ☐ Kennzeichnende Maßnahme
- ■ IT-Maßnahme
- ☐ Rechtliche Maßnahme
- ☐ Kommunikationsmaßnahme

Anwendungsbeispiel

Im Projekt ProOriginal wurde ein Fräsbearbeitungszentrum vom Typ DMC 65 H duoBLOCK® der Firma Deckel Maho Gildemeister (DMG) mit Komponenten von Festo ausgestattet. Die Authentifizierung der Komponenten läuft nach deren Einbau automatisiert ab. Dabei erkennt die Steuerungseinheit der Werkzeugmaschine die zuvor digital gekennzeichneten Komponenten selbstständig und prüft diese auf Echtheit. Mit einem Feldbus werden bestimmte Produktdaten an die Steuerungseinheit der Maschine übertragen und die Komponenten authentisiert. Das Ergebnis dieser Authentizitätsprüfung wird am Ausgabebildschirm angezeigt. Wird eine Komponente als Nichtoriginal erkannt, gibt die Maschine eine Warnung auf dem Bildschirm aus [AKL11].

© DECKEL MAHO Pfronten GmbH

Vorteile

- Gefälschte Ersatzteile werden erkannt
- Absicherung vor Schadensfällen durch gefälschte Ersatzteile [Mei11]

Nachteile

- Evtl. zusätzliche Schnittstelle erforderlich [AAA+10]
- Wahlfreiheit bei Ersatzteilwahl beim Kunden wird eingeschränkt [Mei11]
- Bei lizenzierten Bauteilen schwer einzusetzen [Mei11]
- Nur mit sehr hohem Aufwand nachträglich einzusetzen [Mei11]

Quellen / Experten

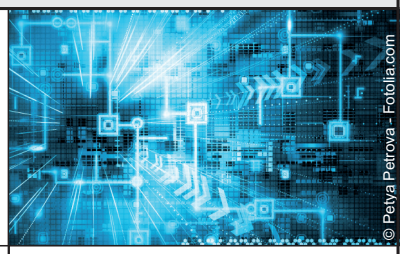
[AAA+10] Abele, E.; Albers, A.; Aurich, J.; Günthner, A. (Hrsg.): Wirksamer Schutz gegen Produktpiraterie im Unternehmen, 2010
[AKL11] Abele, E.; Kuske, P.; Lang, H.: Schutz vor Produktpiraterie. Springer-Verlag, Berlin, 2011
[Mei11] Meiwald, T.: Konzepte zum Schutz vor Produktpiraterie und unerwünschtem Know-how-Abfluss. Diss., TU München, 2011

Bild A-3: Steckbrief für die gegenseitige Authentifizierung von Komponenten [GGL12, S.263]

Schutz von eingebetteter Software

Kurzbeschreibung

Bei dem Schutz von eingebetteter Software geht es um ein durchgängiges Schutzsystem für Software in einer Maschine, digitale Produktionsdaten und Maschinendaten. Durch den stetigen Anstieg des Einsatzes von Maschinen mit hohem Softwareanteil und den Anstieg der Digitalisierung der Produktion steigt auch die Bedeutung der Absicherung der kompletten Entwurfs- und Fertigungsketten.



Anwendungen / Vorgehen

Immer höhere Anteile von Produktinnovationen hängen heutzutage unmittelbar mit Software und Elektronik zusammen. Dies macht einen Schutz dieser Software unumgänglich. Die zunehmende Digitalisierung führt zusätzlich zu einem erhöhten Volumen an digitalen Produktions- und Maschinendaten, die auch geschützt werden müssen.
Zum Schutz von Objekten mit eingebetteter Software können Lizenzinformationen und Schlüssel in einer verschlüsselten und digital signierten Lizenzdatei gespeichert werden. Diese Datei verhindert, dass der enthaltene Schlüssel missbräuchlich genutzt werden kann. Die Lizenzdatei kann genau an ein Rechensystem gebunden sein. Somit kann die Software nur so lange auf dem System genutzt werden, solange nichts an dem System verändert wird, z. B. durch den Austausch der Hardware.

Unternehmensbereiche

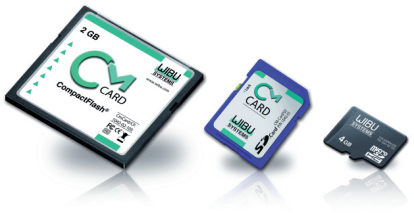
- ☐ Produktplanung
- ■ Entwicklung / Konstruktion
- ☐ Einkauf
- ☐ Arbeitsvorbereitung
- ■ Fertigung
- ☐ Vertrieb
- ☐ Service

Kategorie Schutzmaßnahme

- ☐ Strategische Maßnahme
- ☐ Produktbezogene Maßnahme
- ☐ Prozessbezogene Maßnahme
- ☐ Kennzeichnende Maßnahme
- ■ IT-Maßnahme
- ☐ Rechtliche Maßnahme
- ☐ Kommunikationsmaßnahme

Anwendungsbeispiel

Die Firma WIBU-SYSTEMS AG hat das CodeMeter-System entwickelt, das einen hardwarebasierten Schutz von Embedded Software bietet [Itp11-ol]. CodeMeter schützt die Stickmuster- und Produktionsdaten der Firma ZSK Stickmaschinen von der Erstellung im CAD-System bis zur Maschine gegen unerlaubtes Kopieren. Der Schutz der Steuerungssoftware der Maschinen durch Codeverschlüsselung erschwert auch den Nachbau der Maschine selbst – da die Steuerungssoftware nicht auf eine andere Steuerung kopiert werden kann bzw. diese dort nicht funktioniert [Win12].



© WIBU-SYSTEMS AG

Vorteile

- Kombiniertes Schutzverfahren mithilfe mehrerer Programme möglich
- Der Aufwand zur Erstellung von Imitaten ist für den Imitator schwer abschätzbar
- Keine unkontrollierte Weitergabe von Software-Kopien möglich [Mei11]

Nachteile

- Aktualisierungen der Software erfordern Zeitaufwand
- Gegebenenfalls fehlende Akzeptanz beim Kunden [Mei11]

Quellen / Experten

[Itp11-ol] IT-PRODUCTION: Innovationen gegen Imitate. Unter: http://www.it-production.com/index.php?seite=einzel_artikel_ansicht&id=39360, 22. Juni 2011
[Mei11] MEIWALD, T.: Konzepte zum Schutz vor Produktpiraterie und unerwünschtem Know-how-Abfluss, Diss., TU München, 2011
[Win12] WINZENRIED, O.: Einsatz des CodeMeter in Stickmaschinen. In: Gausemeier, J.; Glatz, R.; Lindemann, U. (Hrsg.): Präventiver Produktschutz – Leitfaden und Anwendungsbeispiele, Carl Hanser Verlag, München, 2012

Bild A-4: Steckbrief für Schutz von eingebetteter Software [GGL12, S.266]

A2 Ergänzung zu Kapitel 3.2.4 – Ganzheitliches, präventives Schutzkonzept für Investitionsgüter (PROTACTIVE)

Das Vorgehen der **Ganzheitliche-Piraterie-Diagnose (GPD)** ist im folgenden Bild dargestellt. Die einzelnen Phasen werden im nachfolgend erläutert [SSM10, S.34ff.].

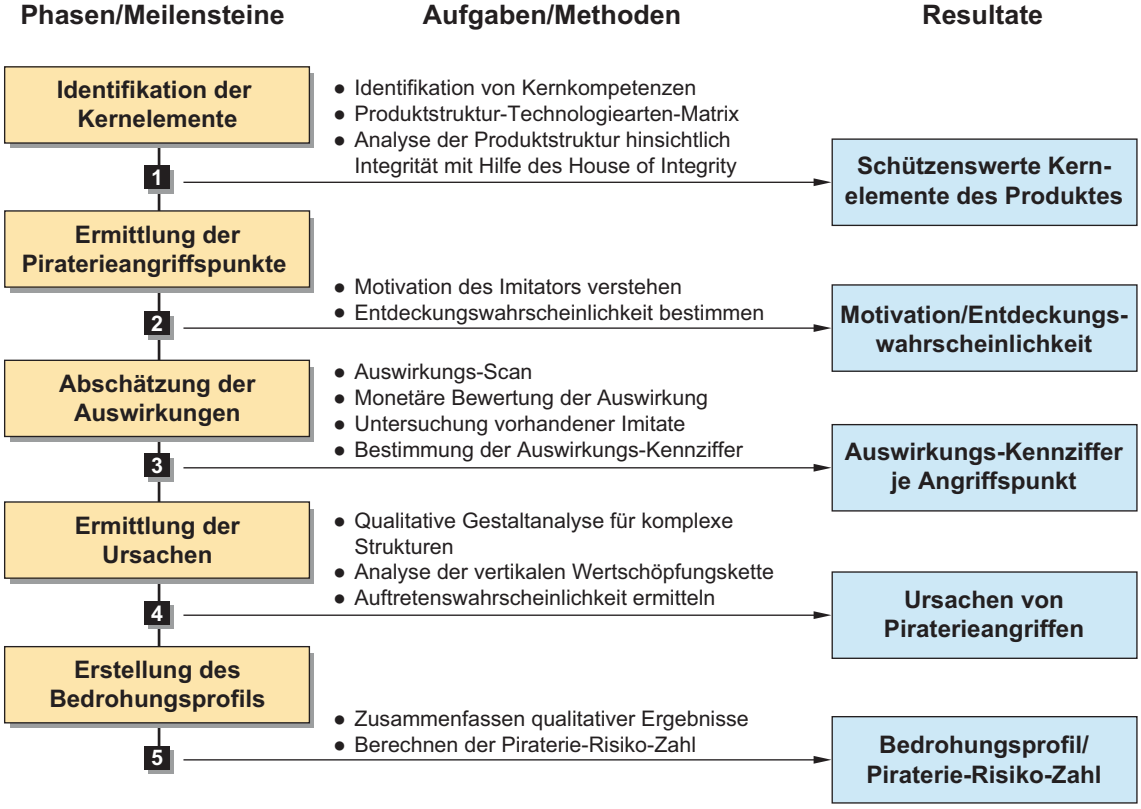


Bild A-5: Vorgehensmodell für die Ganzheitliche-Piraterie-Diagnose-Methodik nach SCHALLNUS ET AL. [SSM10, S.34]

Identifikation der Kernelemente: In der ersten Phase werden die Kernelemente identifiziert. Hierzu werden zunächst die Kernkompetenzen eines Unternehmens analysiert. Die Kernkompetenzen werden vom Unternehmen eingesetzt, um ein Produkt erfolgreich herzustellen und zu vermarkten. Anschließend wird die sog. Produktstruktur-Technologiearten-Matrix erstellt. In der Produktstruktur-Dimension werden die Kernbaugruppen des Produktes aufgelistet. Die Technologiearten-Dimension führt wesentliche Produkt- und Prozesstechnologien des Unternehmens auf. In den Feldern der Matrix werden die in den Kernbaugruppen eingesetzten Technologien eingetragen.

Zusätzlich wird die Struktur des Produktes hinsichtlich der Integrität der Bauteile und Funktionen untersucht. Die Produktintegrität ist definiert als:

> *„Maß für die Einbettung des Schutzkerns in seine konstruktive (unternehmensseitige) sowie anwendungsrelevante (kundenseitige) Umwelt“ [SSM10, S.32].*

Diese Untersuchung wird durch das House of Integrity ermöglicht. Das House of Integrity stellt eine Adaption des House of Quality dar und untersucht die Integrität des Produktes anhand von vier Kriterien [SSM10, S.32]:

- Zerlegbarkeit (Visibilität) bestimmt das Maß für den Aufwand zum Zerlegen eines Produktes in seine Bestandteile
- Verständlichkeit (Familiarität) bezeichnet das Maß für den Aufwand zur Identifikation der zugrunde liegenden Funktionen und Wirkprinzipien
- Austauschbarkeit wird als Maß für die Ersetzbarkeit einer geschützten Komponente durch eine andere Komponente bei gleicher Funktionalität und Kundennutzen eingesetzt
- Verzichtbarkeit bewertet, inwieweit auf Bauteile bei weitgehendem Erhalt der Produktfunktionalität verzichtet werden kann

Generell gilt: Je höher die Integrität eines Produktes ist, desto besser ist der technologische Schutz vor Produktpiraterie und Nachahmung.

Ermittlung der Piraterieangriffspunkte: In der zweiten Phase wird die Entdeckungswahrscheinlichkeit von Imitationen bestimmt. Hierzu nehmen Mitarbeiter des Unternehmens gedanklich die Rolle von Imitatoren ein, um deren Motivation nachzuvollziehen und so mögliche Angriffspunkte zu identifizieren.

Abschätzung der Auswirkungen: In dieser Phase werden mögliche Konsequenzen von Produktpiraterie analysiert. Hierzu werden Imitate (sofern verfügbar) durch Reverse Engineering untersucht. Weiterhin werden die Auswirkungen von Produktpiraterie monetär bewertet. Zum Abschluss der Phase wird die Auswirkungs-Kennziffer bestimmt.

Ermittlung der Ursachen: In der vierten Phase wird das Produkt mit Hilfe einer Quantitativen Gestaltanalyse für komplexe Strukturen untersucht. Hierbei wird ebenso die vertikale Wertschöpfungskette beleuchtet. Für die ermittelten Ursachen wird abschließend die Auftretenswahrscheinlichkeit abgeschätzt.

Erstellung des Bedrohungsprofils: In der abschließenden Phase werden die quantitativen Analyseergebnisse der vorherigen Phasen (Entdeckungswahrscheinlichkeit, Auswirkung und Auftretenswahrscheinlichkeit) zu einer sog. Piraterie-Risiko-Zahl aggregiert. Die qualitativen Analyseergebnisse (Kernkompetenzen oder Motive von Imitatoren) werden bei der Erstellung des Bedrohungsprofils berücksichtigt.

Die Ergebnisse der GPD sind ein qualitatives Piraterie-Bedrohungsprofil sowie die Piraterie-Risiko-Zahl. So lässt sich das individuelle Risiko vor Produktpiraterie bestimmen.

A3 Ergänzung zu Kapitel 3.3.2 – SysML/SYSMOD

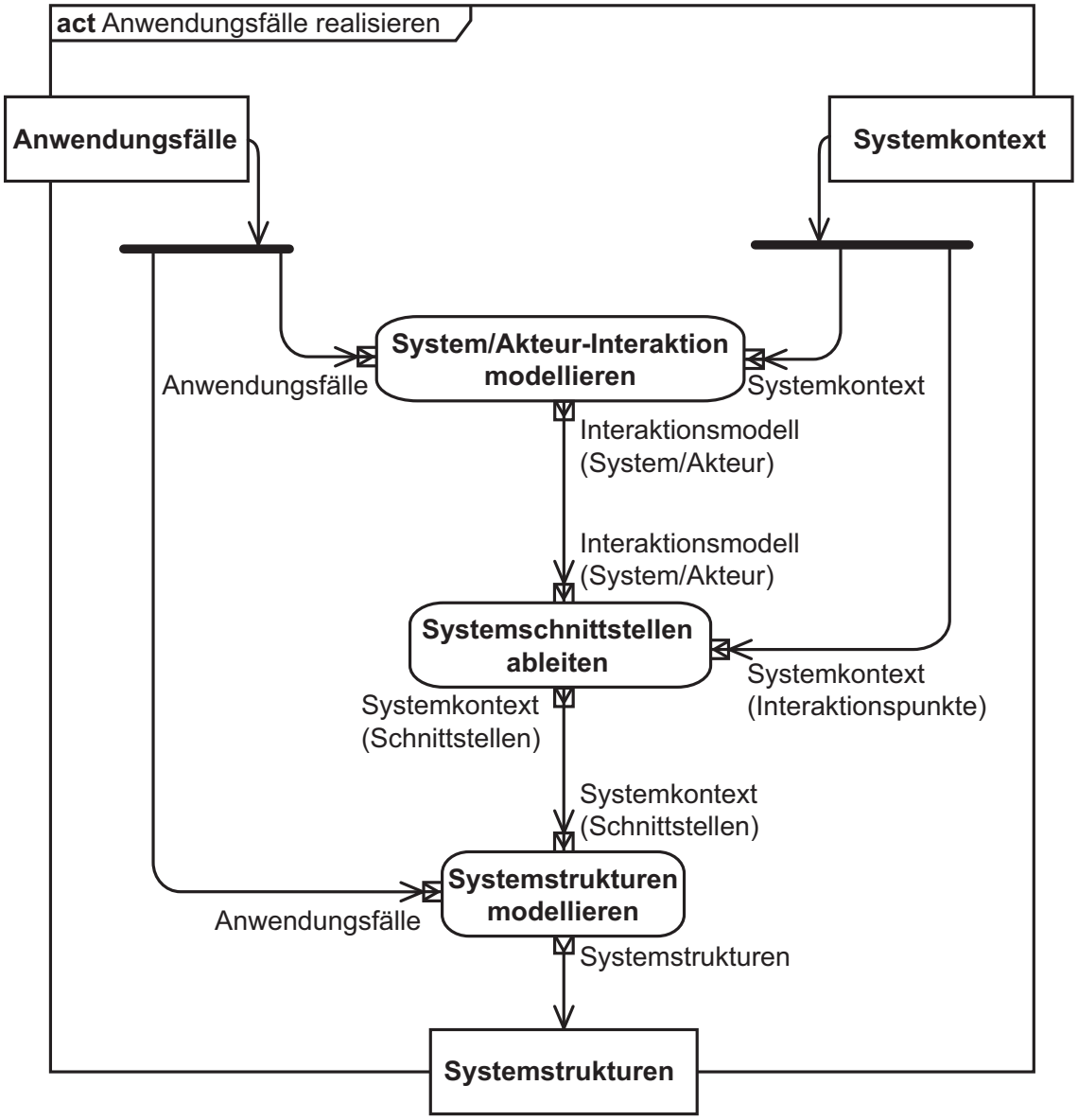
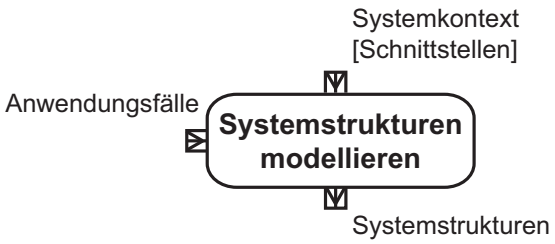


Bild A-6: Vorgehen für den übergeordneten Schritt „Anwendungsfälle realisieren“ nach [Wei06]

Steckbrief Systemstrukturen modellieren



Ein- und ausgehende Daten

Systemkontext [Schnittstellen]
System mit Schnittstellenbeschreibung der Interaktionspunkte
Anwendungsfälle
Dienstleistungen des Systems
Systemstrukturen
Beschreibung der statischen Strukturen des Systems

Beschreibung

Modellieren Sie die Systembausteine und ihre Zusammensetzung, die für das Gesamtsystem notwendig sind, um die Anfoderungen zu erfüllen

Leitfragen

- ☐ Welche Bausteine werden zur Umsetzung der Anwendungsfälle/ Anforderungen benötigt?
- ☐ Wie ist ein Baustein aufgebaut?
- ☐ Wie sind die Bausteine miteinander verbunden?
- ☐ Welche Interaktionspunkte und Schnittstellen haben die Bausteine?

Bild A-7: Beispiel eines Steckbriefs der SYSMOD Methode nach [Wei06]

A4 Ergänzung zu Kapitel 3.5.4 – Lösungsmusterbasierter Entwurf fortgeschrittener mechatronischer Systeme nach ANACKER

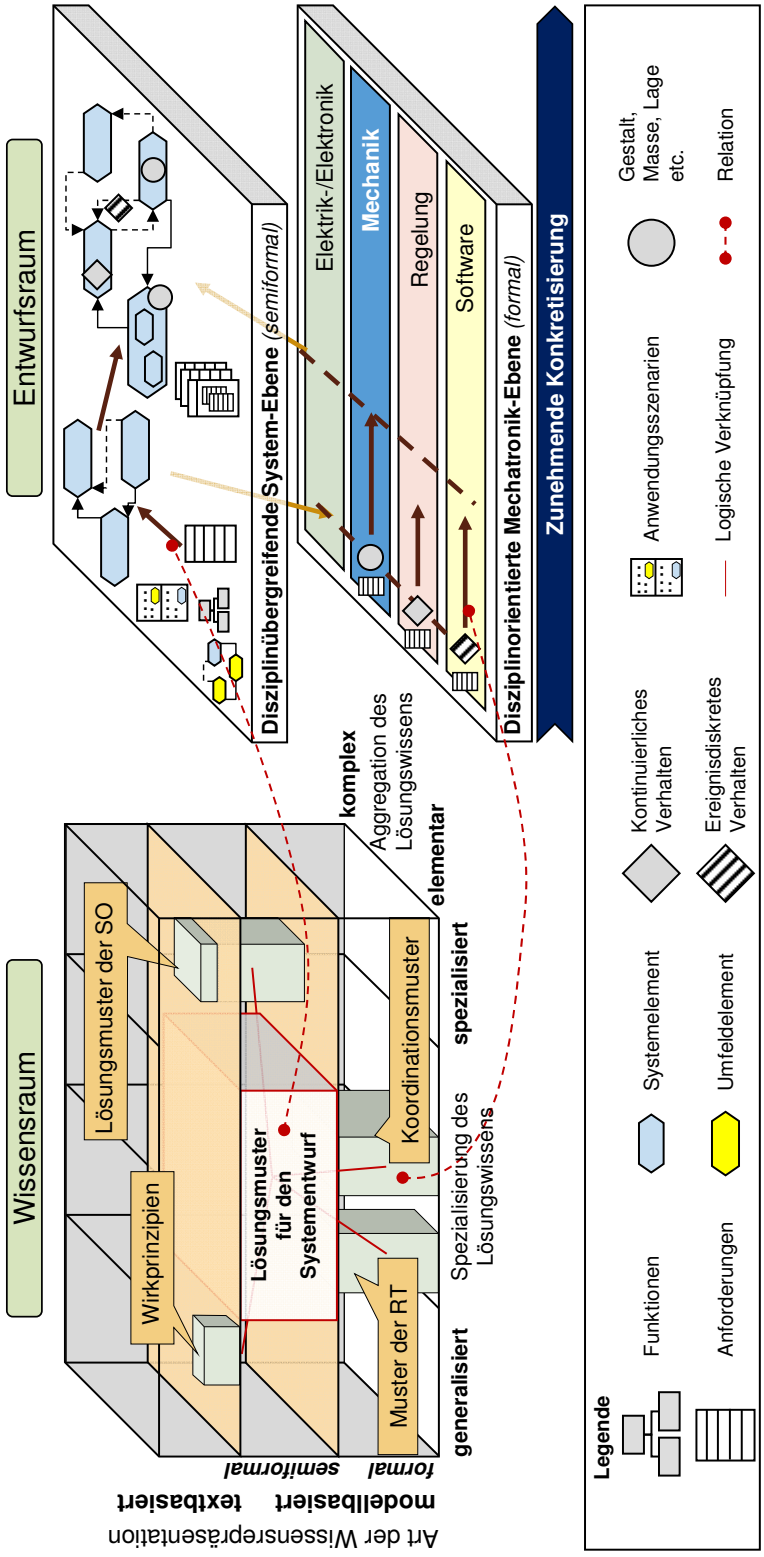


Bild A-8: Zusammenspiel zwischen den Lösungsmustern im Wissensraum und den Ebenen im Entwurfsraum mechatronischer Systeme [Ana15, S.124]

A5 Ergänzung zu Kapitel 4.2 – Schutzanforderungen Intelligenter Technischer Systeme

A5.1 Vorgehen zur Aufnahme von Schutzanforderungen

Aufgrund der geringen Anzahl verfügbarer Untersuchungsobjekte (25 Kernunternehmen) konnte eine quantitative Untersuchung ausgeschlossen werden[51]. Für die **qualitative Aufnahme der Herausforderungen** ist ein geeignetes Erhebungsverfahren zu wählen. Die existierenden Ansätze bieten ein breites Spektrum an Erhebungsmethoden wie Beobachtungen, Interviews oder schriftliche Befragung [Bru08, S.14ff.].

Unter **Beobachtung** versteht man:

> *„[…] das Sammeln von Erfahrungen in einem nicht kommunikativen Prozess mit Hilfe sämtlicher Wahrnehmungsmöglichkeiten“ aus [BD06, S.262] nach [Laa93, S.169].*

Um die Herausforderungen des Schutzes für ITS zu verstehen, ist die Kommunikation mit dem Untersuchungsobjekt erforderlich. Damit ist die Beobachtung zur Aufnahme der Herausforderungen als unbrauchbar zu betrachten.

Unter einem **Interview** versteht man eine qualitative Befragung mit einer gezielten Vorgehensweise, bei der ein verbaler Informationsaustausch mit der Versuchsperson veranlasst wird [Lam10, S.301f.]. Im Rahmen eines Interviews lassen sich Informationen über Meinungsstrukturen, Kausalzusammenhänge sowie subjektive Erfahrungen über das Thema Systemschutz einholen. Somit kann ein Interview dem Forscher neue und nicht erwartete Informationen aufzeigen.

Die erste Befragung im Rahmen der Aufnahme der Herausforderungen wurde in Form eines Interviews durchgeführt. Auf Basis des Interviews konnte das intuitive Verständnis der Fragen erhöht und deren Präzision verbessert werden. Aufgrund der beanspruchten Zeit sowohl vom Forscher als auch vom Experten wurde diese Methode für die weitere Befragung ausgeschlossen.

Die selbstständige Beantwortung von schriftlich vorgelegten Fragen in Form von Fragebögen nennt man eine **schriftliche Befragung** [BD06, S.252]. Bei dieser Form der Datenerhebung besteht keine direkte Interaktion zwischen dem Forscher und dem Befragten. Die Reihenfolge und Form der Fragen ist in einem standardisierten Fragenkatalog immer gleich. Häufig erfolgt die Beantwortung auf einer Bewertungsskala wie der Likert Skala [Lik32]. Darüber hinaus sind auch offene, also frei formulierbare Antworten möglich. Hier können die Befragten ihre Antworten eigenständig formulieren und so

[51] Für quantitative Untersuchungen wird eine große Anzahl an Fällen untersucht, sodass aufgrund der Häufigkeit bestimmte Merkmalskombinationen statistisch analysiert werden können (vgl. [GL06]).

neue Informationen für den Forscher generieren. Die schriftliche Befragung wurde im Rahmen der vorliegenden Arbeit ausgewählt.

Das Vorgehensmodell zur Aufnahme der Herausforderungen ist nachfolgend in Bild A-9 dargestellt. Die drei Phasen werden im Folgenden näher beschrieben.

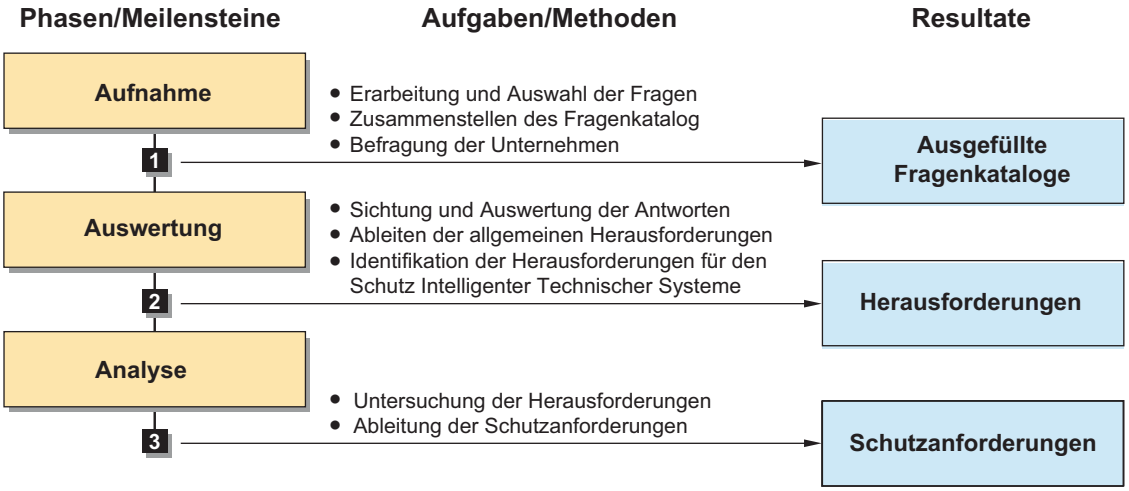


Bild A-9: Vorgehensmodell zur Aufnahme der Herausforderungen und Identifikation der Schutzanforderungen

Anhand der Antworten der Unternehmen konnten allgemeine Herausforderungen an den Schutz sowie die speziellen Herausforderungen Intelligenter Technischer Systeme abgeleitet werden. Die Herausforderungen werden anschließend analysiert, mit dem Ziel die Schutzanforderungen zu identifizieren.

Phase 1: Aufnahme

Im Fragenkatalog werden verschiedene Fragetypen eingesetzt. Geschlossene Fragen werden verwendet um die Relevanz eines Themas zu identifizieren und offene Fragen um die Herausforderungen der Unternehmen abzuleiten. Die Fragen werden in drei Hauptbereiche unterteilt:

Allgemeine Fragen über das Unternehmen: Diese betreffen z. B. die Größe oder die Branche des Unternehmens. Zusätzlich soll mit diesen Fragen ermittelt werden, wie sehr das Unternehmen von Produktpiraterie betroffen ist. Ferner wird der bisherige Einsatz von Schutzmaßnahmen hinterfragt.

Fragen zum allgemeinen Schutz von Systemen: In Anlehnung an die Kategorisierung nach KOKOSCHKA (vgl. Kap. 2.3.2) sind die Fragen in sieben Kategorien unterteilt. Zusätzlich werden hier Fragen zu unternehmensspezifischen Besonderheiten beim Systemschutz gestellt. Darüber hinaus wird die Akzeptanz von Schutzmaßnahmen untersucht. Diese Fragen dienen dazu herauszufinden, ob es beim Einsatz von Schutzmaßnahmen gesonderte Herausforderungen für die Sicherstellung der Akzeptanz zu berücksichtigen gibt.

Fragen zum Schutz von Intelligenten Technischen Systemen: Diese stehen im Fokus der Befragung. Sie betreffen u. a. die entstehenden Herausforderungen durch innovative Technologien z. B. im Zuge der vierten industriellen Revolution (Industrie 4.0) oder die Ausnutzung der charakteristischen Eigenschaften intelligenter Systeme für den Schutz.

Die Befragung wurde an die Kernunternehmen geschickt. Diese sollten den Fragebogen an den jeweiligen Mitarbeiter weiterleiten, der für das Thema Systemschutz verantwortlich ist. Die meisten Fragebögen wurden von der Rechtsabteilung ausgefüllt. Einige Antworten kamen aus der Abteilung für Forschung und Entwicklung sowie aus dem Bereich Technologieentwicklung. Die gegebenen Antworten sind signifikant unterschiedlich, je nach dem in welcher Abteilung die Fragen beantwortet wurden. Typische Antworten aus der Rechtsabteilung sind:

- Das ganzheitliche Patentmanagement ist aktuell eine Herausforderung.
- Bestehende Werkzeuge für die Suche nach Plagiaten sind nicht ausreichend.
- Das Bewusstsein für die durch Produktpiraterie ausgelösten Probleme ist nicht genügend ausgeprägt.

Die Antworten aus den Entwicklungs- bzw. Technologieabteilungen sind hingegen stärker auf technische Lösungen jenseits rechtlicher Maßnahmen ausgerichtet:

- Schutzmaßnahmen sind oft nicht überwachbar.
- Die Schutzmaßnahmen dürfen keinen negativen Einfluss auf das Design, die Leistung und die Kosten eines Systems ausüben.
- Oftmals leidet die Benutzerfreundlichkeit des Systems unter dem Einsatz von Schutzmaßnahmen.

Ein Ergebnis dieser Phase ist der entwickelte und ausgefüllte Fragenkatalog. Dieser ist im Anhang A5.2 abgebildet. 16 Unternehmen beantworteten den Fragebogen.

Phase 2: Auswertung

Die Auswertung ist individuell für jeden Fragenkatalog eines Unternehmens angefertigt worden. Die gegebenen Antworten aller Unternehmen wurden anhand ihres Inhalts gebündelt. Anschließend konnten die Herausforderungen aus den Antworten abgeleitet werden. Ebenso wurden die speziellen Herausforderungen für den Schutz Intelligenter Technischer Systeme identifiziert. Da der Fragenkatalog in Anlehnung an die Schutzmaßnahmen nach KOKOSCHKA (vgl. Kap. 2.3.2) kategorisiert wurde, konnte die Zuordnung der Herausforderungen zu den Kategorien der Schutzmaßnahmen erfolgen. Die unternehmensspezifischen Herausforderungen wurden individuell zu jeweils passenden Kategorien nach KOKOSCHKA zugeteilt. Die Herausforderungen zum Thema Akzeptanz von Schutzmaßnahmen wurden aufgrund hoher inhaltlicher Übereinstimmung bei der Kategorie strategische Schutzmaßnahmen eingeordnet.

Auf Grundlage der Anzahl der Nennungen ist die Relevanz der Herausforderungen ermittelt worden. Die meist genannten Herausforderungen sind:

- Mit Hilfe von Schutzmaßnahmen muss der Kunde, Mitarbeiter, Lieferant etc. für die Thematik Systemschutz sensibilisiert werden. Das Bewusstsein für das Vorhandensein von Produktpiraterie ist zu erhöhen (12 von 16 Nennungen).
- Durch die Schutzmaßnahmen müssen Imitationen und Originale einfach voneinander zu unterscheiden sein, sodass der Kunde informiert wird und Gewissheit besitzt, dass er ein originales Produkt verwendet (12 von 16 Nennungen).
- Auf Basis der Schutzmaßnahmen muss ein sicherer, zuverlässiger, schneller und kostenneutraler Datentransfer gewährleistet sein (12 von 16 Nennungen).

Für den **Schutz Intelligenter Technischer Systeme** konnten **sechs spezielle Herausforderungen** identifiziert werden**:**

- Anhand der Schutzmaßnahmen muss die Sicherheit beim Datenmanagement verbessert werden.
- Basierend auf den Schutzmaßnahmen muss die sichere Kommunikation von Intelligenten Technischen Systemen ermöglicht werden. Die Systeme müssen die Informationen automatisch weiterleiten, sobald die Gefahr einer Kopie entsteht.
- Die Schutzmaßnahmen müssen die Vorteile der Intelligenten Technischen Systeme unterstützen.
- Mit den Schutzmaßnahmen muss ein sicherer Datenaustausch in Netzwerken gewährleistet werden.
- Durch die Maßnahmen wird der Schutz von Softwarekomponenten erhöht.
- Die Eigenschaft der Selbstoptimierung muss verwendet bzw. ausgenutzt werden, um von Angriffen zu lernen.

Als Ergebnis dieser Phase konnten **37 Herausforderungen** aufgenommen und kategorisiert werden. Davon konnten **sechs Herausforderungen** dem Schutz Intelligenter Technischer Systeme zugeordnet werden. Diese Herausforderungen sind vollständig im Anhang A5.3 aufgelistet.

Phase 3: Analyse

In dieser Phase wurden die identifizierten Herausforderungen untersucht. Ziel war die Ableitung von Schutzanforderungen. Angelehnt an die Herausforderungen konnten 37 Schutzanforderungen identifiziert werden. Sechs dieser Schutzanforderungen beziehen sich speziell auf den Schutz Intelligenter Technischer Systeme. Die vollständige Auflistung der Schutzanforderungen ist im Anhang A5.4 dargestellt.

A5.2 Fragenkatalog zur Aufnahme von Schutzanforderungen

Prävention gegen Produktpiraterie 3P **Herausforderungen Systemschutz**

Das Technologie-Netzwerk: Intelligente Technische Systeme OstWestfalenLippe it's owl

1. Allgemeine Fragen zum Unternehmen:

1. Wie viele Mitarbeiter beschäftigt Ihr Unternehmen?
   - ☐ Großunternehmen (> 250 Mitarbeiter)
   - ☐ Mittelständisches Unternehmen (< 250 Mitarbeiter)
   - ☐ Kleinunternehmen (< 50 Mitarbeiter)
2. In welcher Branche ist Ihr Unternehmen einzuordnen?
   - ☐ Elektrotechnik
   - ☐ Maschinen- und Anlagenbau
   - ☐ Automobilindustrie
   - ☐ Möbelindustrie
   - ☐ Sonstige .....
3. Nennen Sie bitte die wichtigsten Produkte.

   .....
4. Bennen Sie bitte Ihr Kundenumfeld.
   - ☐ Endkunde (direkt an den Verbraucher)
   - ☐ Kunde (Unternehmen hat Zuliefererfunktion)
   - ☐ Sonstige .....
5. Wie stark ist Ihr Unternehmen von Produktpiraterie betroffen?
   - ☐ Produkte werden imitiert und sind qualitativ hochwertig.
   - ☐ Erste Imitate wurden entdeckt sind aber von niedriger Qualität.
   - ☐ Das Risiko von Produktpiraterie ist bekannt, Imitate sind noch nicht aufgetaucht.
   - ☐ Unser Unternehmen ist nicht von Produktpiraterie betroffen.
6. Welche Maßnahmen zum Produkt- und Know-how-Schutz setzen Sie ein?
   - ☐ Rechtliche Schutzmaßnahmen (Patente, Geschmacks-, Gebrauchsmuster)
   - ☐ Kennzeichnende Schutzmaßnahmen (Hologramme, RFID, DataMatrix-Code)
   - ☐ Präventive Schutzmaßnahmen (technische oder organisatorische Maßnahmen)
   - ☐ Keine
7. Wie groß ist die Sensibilität für das Thema Produktpiraterie in Ihrem Unternehmen?
   - ☐ Systemschutz ist in der Unternehmensstrategie verankert und wird gelebt.
   - ☐ Es erfolgt eine durchgängige Kommunikation durch alle Unternehmensbereiche.
   - ☐ Wir gehen mit dem Thema offen um, haben aber wenig Erfahrungen damit gemacht.
   - ☐ Das Thema wird im Unternehmen nicht kommuniziert.

Bild A-10: Fragenkatalog zur Aufnahme der Herausforderungen Seite 1/7

Prävention gegen Produktpiraterie 3P **Herausforderungen Systemschutz** Das Technologie-Netzwerk: Intelligente Technische Systeme OstWestfalenLippe it's owl

8. Nennen Sie bitte Ihre vier wichtigsten ausländischen Standorte und die Aktivitäten vor Ort. (Vertrieb, Fertigung, Entwicklung etc.)

Land	Vertrieb	Fertigung	Entwicklung	.....
.....	☐	☐	☐	☐
.....	☐	☐	☐	☐
.....	☐	☐	☐	☐
.....	☐	☐	☐	☐

2. Fragen zum Systemschutz:

unternehmensspezifisch
Jedes Unternehmen hat unternehmensspezifische Anforderungen an den Systemschutz, welche für die Entwicklung einer zugeschnittenen Schutzkonzeption für ein Unternehmen von großer Wichtigkeit sind.

9. Was hat Ihre Firma speziell für Anforderungen an den Systemschutz?

.....

10. Welche Voraussetzungen müssen erfüllt sein damit sie Systemschutz in ihrem Unternehmen einführen/ausbauen?

.....

11. Welche Eigenschaften würden als Ausschlusskriterium für das Einsetzten von Schutzmaßnahmen gelten?

.....

12. Nach welchen Kriterien beurteilen Sie die Tauglichkeit von Schutzkonzepten/-maßnahmen?
    - ☐ Wirkung
    - ☐ Akzeptanz
    - ☐ Kosten
    - ☐ .....

Bild A-11: Fragenkatalog zur Aufnahme der Herausforderungen Seite 2/7

Prävention gegen Produktpiraterie 3P **Herausforderungen Systemschutz**

Das Technologie-Netzwerk: Intelligente Technische Systeme OstWestfalenLippe it's owl

13. Inwieweit ist Ihnen eine Überwachung /Überwachbarkeit der Schutzmaßnahmen wichtig?
    Sehr wichtig ☐ wichtig ☐ mittel ☐ weniger wichtig ☐ unwichtig ☐
14. Wie wichtig ist die Optimierung und Anpassung der Schutzmaßnahmen im Laufe des Produktlebenszyklus?
    Sehr wichtig ☐ wichtig ☐ mittel ☐ weniger wichtig ☐ unwichtig ☐
15. Ab wann lohnt sich für Sie der Einsatz von Systemschutz in Bezug auf die relative Höhe des Schadens durch Produktpiraterie?

    ---

16. Wie viele Ressourcen (Mitarbeiter) dürfen für den Systemschutz in Anspruch genommen werden?

    ---

17. Wie viele Ressourcen (Mitarbeiter) können für Kontrolle der Maßnahmen eingesetzt werden?

    ---

18. Was würden Sie einsetzten, um Industriespionage und Abfluss von Informationen zu vermeiden/verringern (E-Mail Verschlüsselungen (IT-Sicherheit); keine Fotohandys im Betrieb; Zugangsbeschränkungen)?

Kategorie strategisch
Die Integration und Ausrichtung des Systemschutzes muss an die Strategie eines Unternehmens und seine Bedürfnisse angepasst werden (Selektive Vertriebswege, Wissensmanagement).

19. Sollen Systemschutzkonzepte/-maßnahmen auch für andere Unternehmensstandorte einsetzbar bzw. übertragbar sein oder individuell gestaltet werden?
    ☐ Ja ☐ Nein ☐ weiß ich nicht
20. Welche Punkte Ihrer Strategie müssen bei der Schutzkonzeption berücksichtigt werden?

Bild A-12: Fragenkatalog zur Aufnahme der Herausforderungen Seite 3/7

Prävention gegen Produktpiraterie 3P

Herausforderungen Systemschutz

Das Technologie-Netzwerk: Intelligente Technische Systeme OstWestfalenLippe it's owl

Kategorie produktbezogen
Der Schutz eines Produktes ist auf das Produkt selbst und seine Funktionen abzustimmen. Um ein Produkt zu schützen sind verschiedene Schutzmaßnahmen realisierbar und kombinierbar, es sind für das gegebene Produkt die geeignetsten Maßnahmen zu ermitteln (Funktionsintegration, De-Standardisierung).

21. Welche produktbezogenen Maßnahmen werden bereits in Ihrem Unternehmen eingesetzt?

---

22. Welche Bedingungen müssen erfüllt sein, damit Systemschutz bereits in der Entwicklung eines Produktes berücksichtigt wird?

---

23. Darf der Systemschutz Kosten oder Design des Produktes verändern? Wenn ja, inwieweit?
☐ Ja ---------- ☐ Nein

Kategorie prozessbezogen
In Bezug auf die ablaufenden Prozesse in einem Unternehmen kann es leicht zu einem Know-how-Abfluss kommen. Es gilt diesen ungewollten Know-how-Abfluss zu verhindern und die Wertschöpfungskette zu sichern (Innovative Fertigungsverfahren, Schutz der Logistikkette).

24. Würden Sie andere Fertigungsverfahren einsetzten, um den Systemschutz zu erhöhen?
☐ Ja ☐ Nein ☐ weiß ich nicht

25. Kennen Sie besondere Technologien, die in Zukunft zum Systemschutz beitragen können?

---

26. Durch welche Prozesse können komplexe Anlagen/Produktionssysteme geschützt werden?

Bild A-13: Fragenkatalog zur Aufnahme der Herausforderungen Seite 4/7

Prävention gegen Produktpiraterie 3P

Herausforderungen Systemschutz

Das Technologie-Netzwerk: Intelligente Technische Systeme OstWestfalenLippe

it's owl

Kategorie kennzeichnend
Zum Schutz vor Fälschung werden Produkte oft gekennzeichnet. Es gibt sichtbare und nicht sichtbare Kennzeichnungen, um ein Produkt auf dessen Echtheit zu überprüfen (Hologramme, RFID, DataMatrix-Code).

27. Ist Sichtbarkeit einer Schutzmaßnahme relevant?
    ☐ Ja ☐ Nein ☐ nicht zwingend
28. Hat die Sichtbarkeit des Schutzes Auswirkungen auf Kaufentscheidung des Kunden?
    ☐ Ja, positiv ☐ Ja, negativ ☐ Nein ☐ weiß ich nicht
29. Soll der Kunde eine Information bekommen, wenn er kein Originalteil verwendet?
    ☐ Ja ☐ Nein

Kategorie informationstechnisch
Ein ständiger Informationsaustausch zwischen den Systemen birgt einen weiteren Angriffspunkt für Produktpiraterie. Es ist die unbefugte Nutzung der Leistungen, Funktionen und Speicherinhalten von Dritten zu verhindern (Verschlüsselung, Authentifizierung von Komponenten).

30. Soll eine automatische Weitergabe von Informationen der ITS an das Unternehmen erfolgen, wenn Gefahr einer Kopie besteht?
    ☐ Ja ☐ Nein
31. Wie können Eingriffe von außen verhindert werden? Wie kann die Kommunikationssicherheit für die Vernetzung von Maschinen im Sinne von Industrie 4.0 sichergestellt werden?

    .....
32. Wie wichtig ist Schutz von Datenübermittlung? Welche Anforderungen muss dieser erfüllen?
    Sehr wichtig ☐ wichtig ☐ mittel ☐ weniger wichtig ☐ unwichtig ☐

    Anforderungen: .....

Bild A-14: Fragenkatalog zur Aufnahme der Herausforderungen Seite 5/7

Prävention gegen Produktpiraterie 3P

Herausforderungen Systemschutz

Das Technologie-Netzwerk: Intelligente Technische Systeme OstWestfalenLippe it's owl

Kategorie rechtlich
Um sich vor Produktpiraterie zu schützen, setzten viele Unternehmen bereits rechtliche Schutzmaßnahmen ein, welche jedoch erst greifen wenn der Schaden bereits eingetreten ist (Patente, Geschmacks-, Gebrauchsmuster).

33. Wie wichtig sind juristische Schutzmaßnahmen beim Systemschutz?
    Sehr wichtig ☐ wichtig ☐ mittel ☐ weniger wichtig ☐ unwichtig ☐
34. Welche Rolle werden Schutzrechte (Patente etc.) in Zukunft einnehmen?
    Sehr wichtig ☐ wichtig ☐ mittel ☐ weniger wichtig ☐ unwichtig ☐

Kategorie Akzeptanz
Damit technische Systeme am Markt erfolgreich sind, müssen diese von den Benutzern eingesetzt werden wollen. Manche Schutzmaßnahmen erschweren hingegen auch die Benutzung legal erworbener Produkte (beispielsweise Online-Zugang bei Software). Auch Mitarbeiter müssen die Maßnahmen einsetzten und akzeptieren.

35. Berücksichtigen Sie bei der bisherigen Implementierung von Schutzmaßnahmen auch die Auswirkungen auf die Benutzer? Wenn nicht, geben Sie hierfür bitte Gründe an.
    ☐ Ja ☐ Nein .....
36. Erläutern Sie bitte kurz, wie Ihrer Meinung nach eine hohe Akzeptanz bezogen auf eine bestimmte Schutzmaßnahme durch Mitarbeiter und Kunden erreicht werden kann.

    .....
37. Können Sie sich Gründe vorstellen, warum Sie eine Schutzmaßnahme als Benutzer oder Mitarbeiter ablehnen würden

    .....

Kategorie kommunikativ
Ein Plagiat kann das Image einer Marke bzw. eines Unternehmens beeinträchtigen, da für die Kunden Plagiate nicht immer leicht zu erkennen sind (Sensibilisieren, Messebesuche).

38. Wie wichtig ist es den Kunden über Plagiate aufzuklären?
    Sehr wichtig ☐ wichtig ☐ mittel ☐ weniger wichtig ☐ unwichtig ☐
39. Müssen Mitarbeiter auch über das Risiko von Produktpiraterie aufgeklärt werden?
    ☐ Ja ☐ Nein ☐ weiß ich nicht
40. Suchen Sie gezielt nach Plagiaten (Internet, Messen)?
    ☐ Ja ☐ Nein

Bild A-15: Fragenkatalog zur Aufnahme der Herausforderungen Seite 6/7

Prävention gegen Produktpiraterie 3P **Herausforderungen Systemschutz**

Das Technologie-Netzwerk: Intelligente Technische Systeme OstWestfalenLippe it's owl

3. Fragen in Bezug auf ITS:

Intelligente Technische Systeme beruhen auf einer Symbiose von Informatik und Ingenieurwissenschaften und zeichnen sich insbesondere durch vier zentrale Fähigkeiten aus: Sie sind adaptiv, robust, vorrausschauend und benutzerfreundlich. Durch die Systeme erhöhen sich Zuverlässigkeit, Sicherheit und Verfügbarkeit von Produkten und Produktionssystemen, außerdem werden Ressourcen effizienter eingesetzt.

41. Vor welche besonderen Herausforderungen wird der Systemschutz durch den Einsatz / die Entwicklung neuer Technologien / intelligenter Systeme (Industrie 4.0, ITS) gestellt?

---

42. Inwiefern ist die eigenständige Kommunikation von ITS in Bezug auf einen dadurch verbesserten Systemschutz relevant?
    Sehr wichtig ☐ wichtig ☐ mittel ☐ weniger wichtig ☐ unwichtig ☐
43. Wird sich der Lebenszyklus von ITS verändern (verlängern, verkürzen, keine Veränderung)? Ergeben sich dadurch neue Herausforderungen an den Systemschutz?

---

44. Wie kann die Intelligenz einer Maschine oder eines Produktes zum Systemschutz beitragen?

---

45. Welche Eigenschaften der ITS dürfen durch Schutzmaßnahmen auf keinen Fall beeinflusst werden?

---

46. Durch Selbstoptimierung können sich Maschinen eigenständig an sich ändernde Betriebsbedingungen anpassen. Ist für Sie hierdurch auch eine neue Art von Systemschutz möglich? Was für Eigenschaften sollte dieser haben?

---

47. Ist die Anpassung des Systemschutzes im Hinblick auf die Selbstoptimierung der Maschine in Zukunft relevant?

Bild A-16: Fragenkatalog zur Aufnahme der Herausforderungen Seite 7/7

A5.3 Auflistung der Herausforderungen an den Systemschutz

Prävention gegen Produktpiraterie 3P

Herausforderungen

Das Technologie-Netzwerk: Intelligente Technische Systeme OstWestfalenLippe
it's owl

Nummer	Zusammenfassung der Herausforderungen	Anzahl Nennungen (von 16)
1	Strategische Herausforderungen	
1.1	Die Schutzmaßnahmen müssen international wirksam sein, d.h. an verschiedenen Standorten des Unternehmens, auch außerhalb von Deutschland, ihre Wirksamkeit behalten.	10
1.2	Die Umsetzung der Schutzmaßnahmen muss relativ einfach und kostengünstig umsetzbar sein.	10
1.3	Die Schutzmaßnahmen müssen beobachtbar sein, der Nutzen der Maßnahmen muss erkennbar und auslesbar sein.	9
1.4	Die Anpassung und Optimierbarkeit der Maßnahmen im Produktlebenszyklus muss gegeben sein.	8
1.5	Das Alleinstellungsmerkmal zur Differenzierung von der Konkurrenz muss trotz des Einsatzes der Schutzmaßnahmen erhalten bleiben.	3
1.6	Die Schutzmaßnahmen stellen kein Hindernis für die Produktivität und Nachhaltigkeit dar.	1
1.7	Die Schutzmaßnahmen müssen mit dem Wissensmanagement vereinbar sein.	1
2	Produktbezogene Herausforderungen	
2.1	Der Einsatz der Schutzmaßnahmen darf nur eine minimale Änderung von Kosten und Design des Produktes hervorrufen.	10
2.2	Die Implementierung muss einfach und kostengünstig sein.	10
2.3	Die Benutzerfreundlichkeit (Usability) des Produktes muss trotz des Einsatzes der Schutzmaßnahmen gewährleistet werden.	9
2.4	Die Leistungsfähigkeit des Produktes muss erhalten bleiben.	5
2.5	Der Arbeitsaufwand/-ablauf für Mitarbeiter darf durch die Schutzmaßnahmen nicht erhöht werden.	3
2.6	Die Kompatibilität zu anderen Systemen muss erhalten bleiben.	1
2.7	Die Wartung des Produktes muss einfach bleiben.	1
3	Prozessbezogene Herausforderungen	
3.1	Die Umstellungsaufwände durch den Einsatz der Schutzmaßnahmen sollen gering wie möglich ausfallen. Eine Umstellung auf andere Fertigungsverfahren soll vermieden werden.	6
3.2	Die Schutzmaßnahmen sind im Produktentstehungsprozess fest verankert.	4
3.3	Der Schutz von komplexen Produktionssystemen wird durch die Maßnahmen gewährleistet.	4
3.4	Die Komplexität der Schutzmaßnahmen muss handhabbar sein.	2

Bild A-17: Auflistung der Herausforderungen Seite 1/2

Prävention gegen Produktpiraterie 3P

Herausforderungen

Das Technologie-Netzwerk: Intelligente Technische Systeme OstWestfalenLippe it's owl

4	Kennzeichnende Herausforderungen	
4.1	Durch die Schutzmaßnahmen müssen Imitationen und Originale einfach voneinander zu unterscheiden sein, so dass der Kunde informiert wird, dass er ein Original verwendet.	12
4.2	Die Schutzmaßnahmen sind sichtbar. Das Verstecken der Maßnahme ist nicht notwendig.	10
4.3	Die Schutzmaßnahmen werden vom Kunden akzeptiert. Der Kunde sieht sie als ästhetisch und notwendig an. Sie wird nicht als störend empfunden.	4
4.4	Die Schutzmaßnahmen sind Fälschungssicher. Es ist sehr schwer für den Imitator sie nachzuahmen.	2
5	Informationstechnische Herausforderungen	
5.1	Auf Basis der Schutzmaßnahmen muss ein sicherer, zuverlässiger, schneller und kostenneutraler Datentransfer gewährleistet sein.	12
5.2	Die Schutzmaßnahmen sind in der Lage eine Spionage im Unternehmensnetzwerk/auf dem Dienstrechner lückenlos zu verhindern.	2
5.3	Bei erfolgter Spionage muss diese lückenlos zu identifizieren sein.	2
6	Rechtliche Herausforderungen	
6.1	Durch den Einsatz der neuen Schutzmaßnahmen dürfen die patentrechtlichen Schutzmaßnahmen nicht außer Kraft gesetzt werden.	10
6.2	Die Schutzmaßnahmen gewährleisten ein ganzheitliches Patentmanagement, bedeutet sie verbessern die Schutzrechte weltweit.	4
6.3	Durch den Einsatz der Schutzmaßnahmen werden neue patentrechtliche Schutzmaßnahmen forciert bzw. erzwungen.	1
7	Kommunikative Herausforderungen	
7.1	Mit Hilfe von Schutzmaßnahmen muss der Kunde, Mitarbeiter, Lieferant etc. für die Thematik Systemschutz sensibilisiert werden. Das Bewusstsein für das Vorhandensein von Produktpiraterie ist zu erhöhen.	12
7.2	Eine gezielte Suche nach Plagiaten wird durch die Schutzmaßnahmen umgesetzt.	9
7.3	Die Schutzmaßnahmen tragen zur Geheimhaltung bei.	4
8	Herausforderungen Intelligenter Technischer Systeme	
8.1	Mit Hilfe der Schutzmaßnahmen muss ein sicherer Umgang mit Daten ermöglicht werden.	12
8.2	Auf Basis der Schutzmaßnahmen muss die sichere Kommunikation von Intelligenten Technischen Systemen ermöglicht werden. Die Systeme müssen die Informationen automatisch weiterleiten, sobald Gefahr entsteht.	9
8.3	Die Schutzmaßnahmen müssen die Vorteile der Intelligenten Technischen Systeme unterstützen.	7
8.4	Mit Hilfe der Schutzmaßnahmen muss ein sicherer Datenaustausch in Netzwerken gewährleistet werden.	6
8.5	Durch die Maßnahmen wird der Schutz von Softwarekomponenten erhöht.	2
8.6	Die Eigenschaft der Selbstoptimierung muss verwendet bzw. ausgenutzt werden, um von Angriffen zu lernen.	1

Bild A-18: Auflistung der Herausforderungen Seite 2/2

A5.4 Vollständige Auflistung allgemeiner sowie ITS-spezifischer Schutzanforderungen

Tabelle A-1: Auflistung der Schutzanforderungen 1/2

Checkliste Schutzanforderungen			Version Datum
Nr.	**R/I**	**Schutzanforderungskategorie/Schutzanforderung**	**Bearbeiter**
1		**Strategische Schutzanforderungen**	
1.1		Internationale Wirksamkeit	
1.2		Einfache und kostengünstige Umsetzung	
1.3		Überwachbarkeit	
1.4		Anpassbarkeit und Optimierbarkeit im Lebenszyklus	
1.5		Erhalt der Differenzierung	
1.6		Erhalt der Produktivität und Nachhaltigkeit	
1.7		Vereinbarkeit mit dem Wissensmanagement	
2		**Produktbezogene Schutzanforderungen**	
2.1		Minimale Änderung von Kosten und Design	
2.2		Einfache und kostengünstige Implementierung	
2.3		Keine Einschränkung der Benutzerfreundlichkeit (Usability)	
2.4		Erhalt der Leistungsfähigkeit des Systems	
2.5		Keine Erhöhung des Arbeitsaufwands/-ablaufs	
2.6		Erhalt der Kompatibilität zu anderen Systemen	
2.7		Einfache Wartung	
3		**Prozessbezogene Schutzanforderungen**	
3.1		Geringe Umstellungsaufwände	
3.2		Verankerung der Schutzmaßnahme im Produktentstehungsprozess	
3.3		Gewährleistung des Schutzes komplexer Produktionssysteme	
3.4		Handhabbarkeit der Komplexität	
4		**Kennzeichnende Schutzanforderungen**	
4.1		Einfache Unterscheidung zwischen Original und Imitation	
4.2		Information des Kunden, dass er ein originales Produkt verwendet	
4.3		Akzeptanz des Kunden	
4.4		Imitationssicher	

R: Relevant I: Irrelevant

Tabelle A-2: Auflistung der Schutzanforderungen 2/2

Checkliste Schutzanforderungen			Version Datum
Nr.	**R/I**	**Schutzanforderungskategorie/Schutzanforderung**	**Bearbeiter**
5		**Informationstechnische Schutzanforderungen**	
5.1		Sicherer, zuverlässigen, schnellen und kostenneutralen Datentransfer	
5.2		Verhinderung von Angriffen	
5.3		Lückenlose Identifikation von Angriffen	
6		**Rechtliche Schutzanforderungen**	
6.1		Verträglichkeit zu patentrechtlichen Schutzmaßnahmen	
6.2		Unterstützung des ganzheitlichen Patentmanagements	
6.3		Forcierung neuer rechtlicher Schutzmaßnahmen	
7		**Kommunikative Schutzanforderungen**	
7.1		Sensibilisierung und Erhöhung des Bewusstseins für das Vorhandensein von sowie für entstehende Probleme durch Produktpiraterie	
7.2		Unterstützung bei der Suche nach Plagiaten	
7.3		Verbesserung der Geheimhaltung	
8		**ITS-spezifische Schutzanforderungen**	
8.1		Vertraulichkeit sensibler Daten	
8.2		Überwachung des Systemverhaltens	
8.3		Eindeutige Authentifizierung	
8.4		Integrität in Netzwerken	
8.5		Einzigartige kryptographische Schlüssel generieren und sicher speichern	
8.6		Selbstoptimierung der Schutzmaßnahmen	

R: Relevant I: Irrelevant

A6 Ergänzung zu Kapitel 4.3.1 – Analyse bekannter Schutzmaßnahmen

Schutzmaßnahmen nach GAUSEMEIER ET AL.

Tabelle A-3: Gegenüberstellung der Maßnahmen mit den Schutzanforderungen 1/3

Abgleich Schutzmaßnahmen mit Schutzanforderungen																				
Schutzanforderungen	strategisch							produktbezogen							ITS-spezifisch					
Schutzmaßnahmen	1.1	1.2	1.3	1.4	1.5	1.6	1.7	2.1	2.2	2.3	2.4	2.5	2.6	2.7	8.1	8.2	8.3	8.4	8.5	8.6
Strategische Schutzmaßnahmen																				
Mitarbeiterbindung verstärken	+	+	–	–	+	+	+								–	–	–	–	–	–
Wissensmanagement einführen	+	○	+	–	+	+	+								–	–	–	–	–	–
Beschränkung von schützens-wertem Know-how auf ausgewählte Personen	+	+	○	+	+	○	+								–	–	–	–	–	–
Sensibilisierung der Mitarbeiter für Social Engineering	+	+	–	–	+	+	+								–	–	–	–	–	–
Abteilungsübergreifende Koope-ration in puncto Produktschutz	+	+	○	○	+	+	+								–	–	–	–	–	–
Innovationsprozesse optimieren	+	–	+	+	+	+	+								–	–	–	–	–	–
Target Costing	+	○	○	+	–	○	+								–	–	–	–	–	–
Kooperation mit Zulieferern	○	○	○	–	○	+	+								–	–	–	–	–	–
Zuliefererintegration	○	○	○	–	○	+	+								–	–	–	–	–	–
After-Sales-Management/ Hybride Leistungsbündel	+	–	○	+	○	○	+								–	–	–	–	–	–
Release Management	+	○	+	+	○	○	+								–	–	–	–	–	–
Marken- und Produktpreisdifferenzierung	+	–	○	+	○	+	+								–	–	–	–	–	–
Selektive Vertriebssysteme	+	–	+	○	+	+	+								–	–	–	–	–	–
Shadow Placement	+	–	○	+	+	○	+								–	–	–	–	–	–
Quersubventionierung von leicht immitierbaren Produkten	–	–	–	+	○	+	+								–	–	–	–	–	–
Überwachung des Marktes	+	○	+	+	+	+	+								–	–	–	–	–	–
Umarmungsstrategie	○	○	○	○	+	+	+								–	–	–	–	–	–
Produktbezogene Schutzmaßnahmen																				
Black-Box-Bauweise anwenden								–	○	+	○	–	–	–	–	–	–	–	–	–
De-Standardisierung								○	○	○	+	–	–	–	–	–	–	–	–	–
Funktionsintegration								○	○	+	+	–	+	○	–	–	–	–	–	–
Selbstzerstörungmechanismus								–	○	+	○	–	○	○	–	–	–	–	–	–
Erweiterungsmanagement								–	○	○	○	–	+	+	–	–	–	–	–	–
Produktvarianten anbieten								+	+	+	○	○	+	+	–	–	–	–	–	–
Mass Customization								○	–	+	+	–	+	+	–	–	–	–	–	–
Benchmarking von Imitaten								○	–	+	+	–	+	+	–	–	–	–	–	–

Tabelle A-4: Gegenüberstellung der Maßnahmen mit den Schutzanforderungen 2/3

Abgleich Schutzmaßnahmen mit Schutzanforderungen														
Schutzanforderungen	prozess-bezogen				kenn-zeichnend				ITS-spezifisch					
Schutzmaßnahmen	3.1	3.2	3.3	3.4	4.1	4.2	4.3	4.4	8.1	8.2	8.3	8.4	8.5	8.6
Prozessbezogene Schutzmaßnahmen														
Geheimhaltung während der Entwicklung	+	+	+	+					−	−	−	−	−	−
Aufteilung der Fertigung auf mehrere Standorte	−	+	+	−					−	−	−	−	−	−
Innovative Fertigungsverfahren	−	+	○	+					−	−	−	−	−	−
Kernkompetenzbauteile intern entwickeln und fertigen	○	+	+	+					−	−	−	−	−	−
Organisation der Lieferantenwertschöpfung	○	+	○	○					−	−	−	−	−	−
Schutz der Produktionslogistik	+	−	+	+					−	−	−	−	−	−
Schutz der Distributionslogistik	+	−	−	+					−	−	−	−	−	−
"Intelligente" Verpackungen	−	+	−	○					−	−	−	−	−	−
Sichere Sammlung und Entsorgung von Ausschussware	+	−	○	+					−	−	−	−	−	−
Kennzeichnende Schutzmaßnahmen														
2D-/3D-Barcodes					+	+	+	○	−	−	−	−	−	−
Clusterfolie					+	+	+	−	−	−	−	−	−	−
Echtfarbenelemente					○	○	○	−	−	−	−	−	−	−
EpiCode					+	+	+	+	−	−	−	−	−	−
Guillochendruck					+	+	+	○	−	−	−	−	−	−
Hologramm					+	+	+	−	−	−	−	−	−	−
Intagliodruck/Stichtiefdruck					○	+	+	○	−	−	−	−	−	−
Mikrotext					○	+	○	−	−	−	−	−	−	−
Rauschmustercodierung					−	+	−	+	−	−	−	−	−	−
RFID					+	+	+	−	+	○	+	−	−	−
Sicherheitsanstanzung					+	+	+	−	−	−	−	−	−	−
Sicherheitsetikett und Siegel					+	+	+	−	−	−	−	−	−	−
Sicherheitspapier					○	+	+	+	−	−	−	−	−	−
Sicherheitsstreifen					○	+	+	+	−	−	−	−	−	−
Siebdruck und Prägen					+	+	+	−	−	−	−	−	−	−
Spezialtinte					−	+	○	+	−	−	−	−	−	−
Chemische Marker					+	+	○	○	−	−	−	−	−	−
Digitale Wasserzeichen					−	−	−	○	−	−	−	−	−	−
DNA-Kennzeichnung					−	−	−	+	−	−	−	−	−	−
Farbcode					−	+	−	○	−	−	−	−	−	−
Isotope Kennzeichnung					−	+	−	+	−	−	−	−	−	−
Infrarot-/Ultraviolett-Farbpigmente					+	+	+	○	−	−	−	−	−	−
Materialmarker mit charakteristischer Fluoreszenz					○	+	○	+	−	−	−	−	−	−
Nanobiotech-Kennzeichnung					−	−	○	+	−	−	−	−	−	−
Oberflächenauthentifizierung					−	−	−	+	−	−	−	−	−	−
Röntgenfluoreszenz					−	−	−	+	−	−	−	−	−	−

Tabelle A-5: Gegenüberstellung der Maßnahmen mit den Schutzanforderungen 3/3

Abgleich Schutzmaßnahmen mit Schutzanforderungen															
Schutzanforderungen	IT			rechtlich			kommu-nikativ			ITS-spezifisch					
Schutzmaßnahmen	5.1	5.2	5.3	6.1	6.2	6.3	7.1	7.2	7.3	8.1	8.2	8.3	8.4	8.5	8.6
Informationstechnische Schutzmaßnahmen															
Biometrische Zugangskontrolle	–	+	○							–	–	–	–	–	–
Rollenbasierte Zugangskontrolle installieren	–	+	○							–	–	–	–	–	–
Dokumente verschlüsseln	+	–	–							○	–	–	–	○	–
Informationen aus CAD-Modellen entfernen	+	–	–							○	–	–	–	–	–
Sichere Kommunikationsverbindungen	+	+	○							+	–	–	○	○	–
Gegenseitige Authentifizierung von Komponenten	○	–	–							○	○	+	–	○	–
Produktaktivierung	–	–	–							–	–	–	–	–	–
Auslagerung von sicherheitsrelevanten Rechenoperationen	–	○	–							–	–	–	–	○	–
Schutz von eingebetteter Software	+	○	–							+	○	–	–	+	–
Rechtliche Schutzmaßnahmen															
Schutzrechtsstrategien entwickeln				+	+	+				–	–	–	–	–	–
Patent anmelden				+	+	–				–	–	–	–	–	–
Gebrauchsmuster anmelden				+	+	–				–	–	–	–	–	–
Geschmacksmuster anmelden				+	+	–				–	–	–	–	–	–
Kennzeichenrechte anmelden				+	+	–				–	–	–	–	–	–
Urheberrechte				+	+	–				–	–	–	–	–	–
Schutzrechte verwerten				○	+	○				–	–	–	–	–	–
Grenzbeschlagnahme				+	+	–				–	–	–	–	–	–
Unterstützung durch Verfassungsschutz				+	+	–				–	–	–	–	–	–
Kommunikative Schutzmaßnahmen															
Kommunikationsstrategien anwenden							+	–	+	–	–	–	–	–	–
Kunden für Originiale und Imitate sensibilise							+	○	–	–	–	–	–	–	–
Lobbyarbeit							+	○	–	–	–	–	–	–	–
Attraktive Gestaltung von Verkaufsräumen							○	–	–	–	–	–	–	–	–
Benchmarking von Imitaten							○	+	–	–	–	–	–	–	–
Messebesuche durchführen							+	+	–	–	–	–	–	–	–

A7 Ergänzung zu Kapitel 4.3.2.2 – Direct Manufacturing als Technologie zum Systemschutz

Additive Fertigungsverfahren unterscheiden sich sowohl in der Form und Art des Ausgangsstoffes als auch in der Fertigungstechnologie. Die Fertigung kann auf unterschiedliche Arten erfolgen: Laser-basiert, wie das **Laser Sintern** von Kunststoffpulver (LS) und das **Selective Laser Melting** von Metallpulver (SLM) oder spritzdüsen-basiert wie das **Fused Layer Modeling** mit einem thermoplastischen Materialstrang als Ausgangsmaterial (FLM). Im Folgenden werden die drei gängigsten Verfahren näher erläutert [Geb13], [ZA13].

Laser Sintern: Hier wird das thermoplastische Kunststoffpulver mit Hilfe eines Lasers schichtweise verfestigt. Der Bauprozess vom CAD-Datensatz bis zum fertigen Bauteil ist schematisch für das LS-Verfahren in Bild A-19 dargestellt.

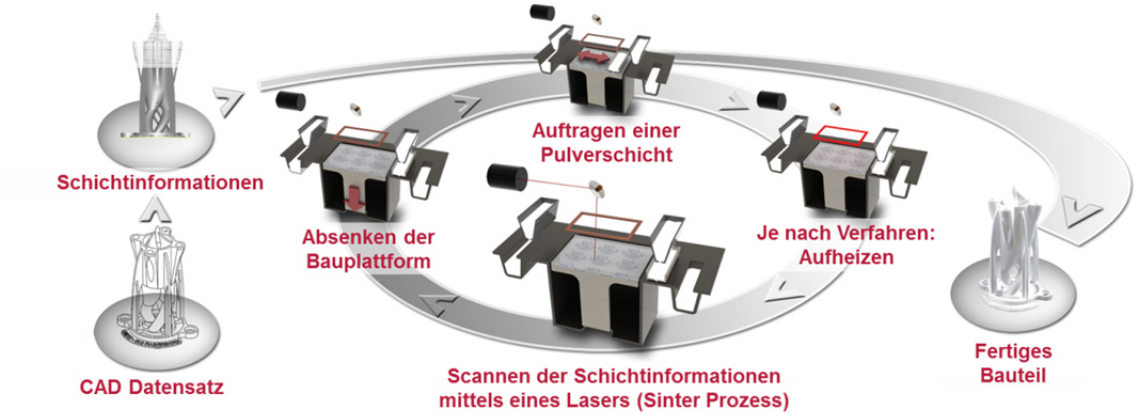


Bild A-19: Schematische Darstellung additiver Fertigungsverfahren am Beispiel des Laser Sintern Prozesses [LJK+13]

Zunächst wird eine Pulverschicht auf die Bauebene mittels eines Schiebers aufgetragen. Die Verschmelzung des Kunststoffpulvers erfolgt anschließend durch den Laser an den Konturen, die die jeweilige Schicht des Bauteils darstellen. Durch Wärmeleitung kommt es zur Abkühlung und so zu einer festen Schicht. Für den Auftrag einer neuen Pulverschicht muss die gesamte Bauplattform um die Schichtstärke abgesenkt werden. Ab hier beginnt der Bauvorgang erneut, zunächst mit dem partiellen Erhitzen der Schicht anhand des Lasers, anschließend mit dem Absenken der Bauplattform und dem Pulverauftrag. Am Ende der Bauphase, nachdem das Pulver möglichst gleichmäßig abgekühlt ist, wird das überschüssige Pulver entfernt.

Selective Laser Melting: Bei diesem Verfahren wird Metallpulver als Ausgangsstoff verwendet. Das Funktionsprinzip des SLM-Verfahrens ist vergleichbar mit dem Laser Sintern. Jedoch hat der Laser eine deutlich höhere Leistung, welche zum Aufschmelzen des Materials benötigt wird.

Fused Layer Modeling: Hierbei werden Bauteile durch lokales Anschmelzen und anschließendes Extrudieren drahtförmiger Thermoplaste erzeugt. Durch das schichtweise definierte Ablegen des aufgeschmolzenen Werkstoffs entstehen räumliche Strukturen aus Kunststoff.

A8 Ergänzung zu Kapitel 4.4.4 – Abstraktionsebenen von Schutzmustern

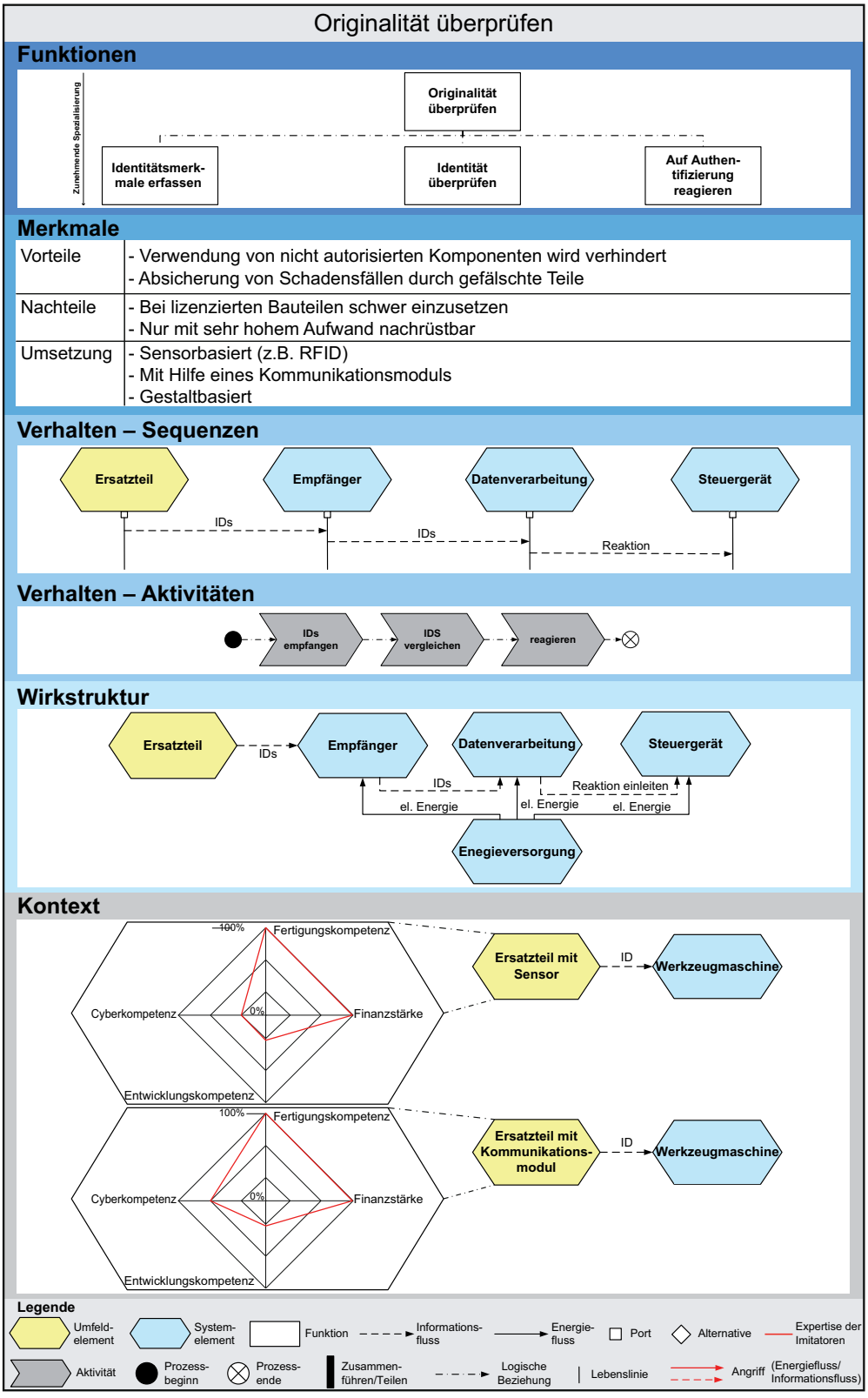


Bild A-20: Schutzmuster Originalität überprüfen

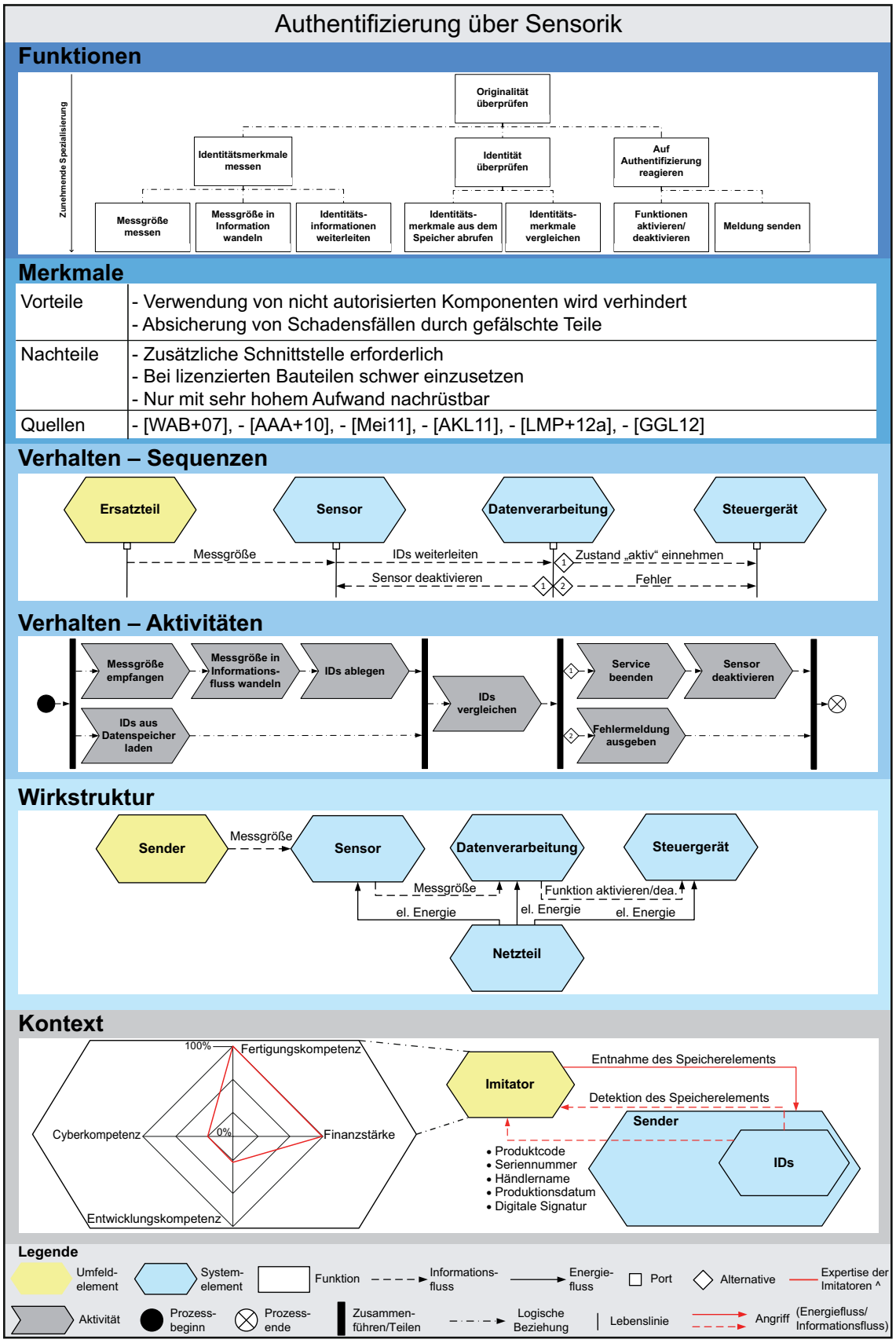


Bild A-21: Schutzmuster Authentifizierung über Sensorik

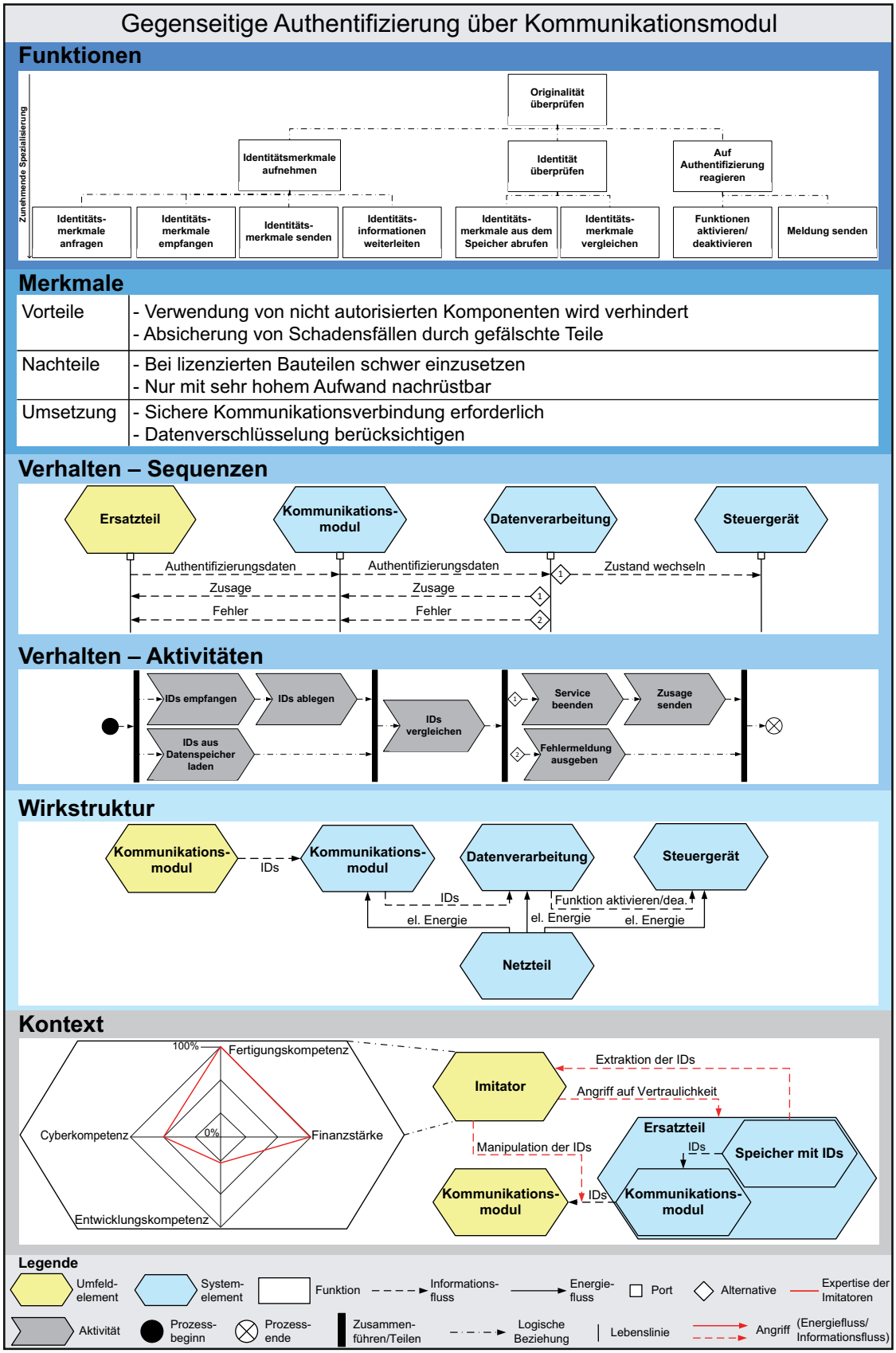


Bild A-22: Schutzmuster gegenseitige Authentifizierung über Kommunikationsmodul

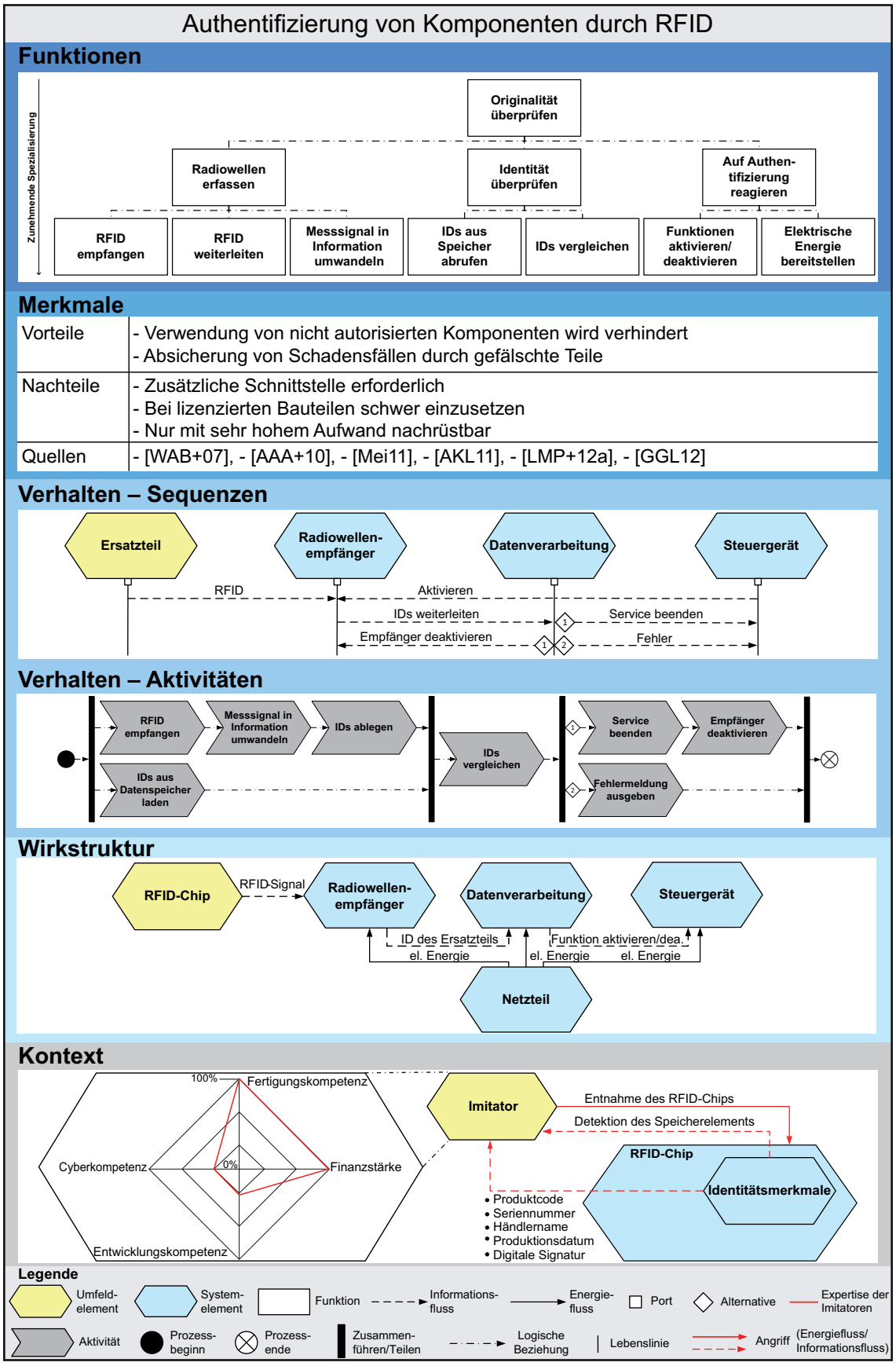
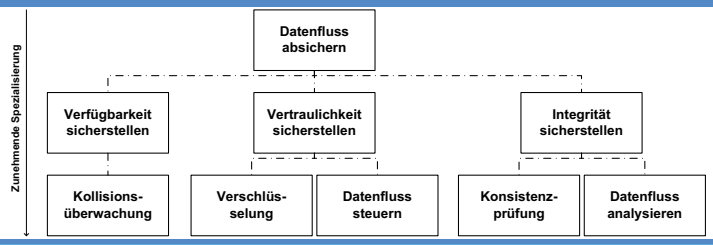


Bild A-23: Schutzmuster Authentifizierung von Komponenten durch RFID

Sichere Kommunikation

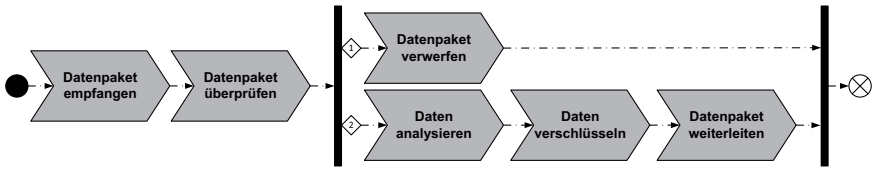
Funktionen



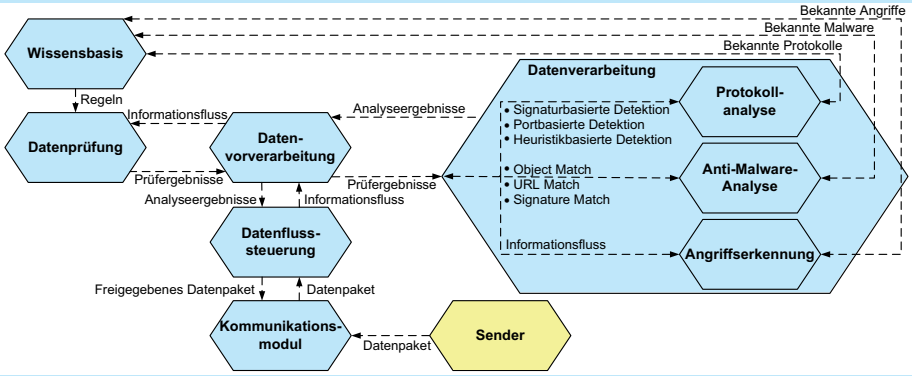
Merkmale

Vorteile	- Unbefugte Dritte haben keine Möglichkeit, die Daten abzugreifen - Schutz ist „unsichtbar“
Nachteile	- Kommunikation mit Externen wird ggf. erschwert - Kompatibilitätsprobleme bei unterschiedlichen Programmen/Systemen - Mitarbeiter müssen für den sensiblen Umgang mit Daten geschult werden
Umsetzung	- Es existieren unterschiedlich mächtige Verfahren zum Aufbau sicherer Kommunikationsverbindungen (Verschlüsselung, Steganografie, Turbo Deep Packet Inspection)
Quellen	- [Alk11-ol], - [GGL12]

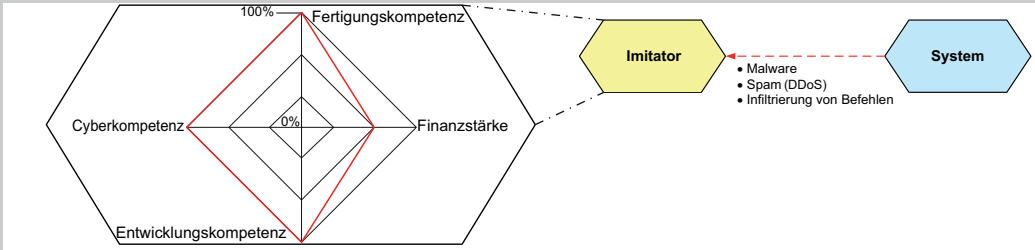
Verhalten – Aktivitäten



Wirkstruktur



Kontext



Legende

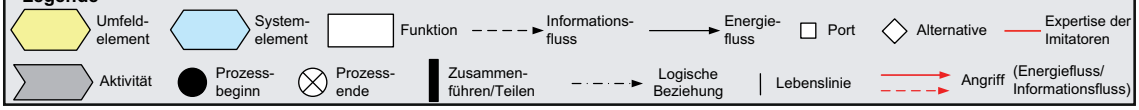


Bild A-24: Schutzmuster Sichere Kommunikation

Lebenslauf

Aus Gründen des Datenschutzes enthält diese online-Version keinen Lebenslauf.

Paderborn, 22. Dezember 2016

Das Heinz Nixdorf Institut – Interdisziplinäres Forschungszentrum für Informatik und Technik

Das Heinz Nixdorf Institut ist ein Forschungszentrum der Universität Paderborn. Es entstand 1987 aus der Initiative und mit Förderung von Heinz Nixdorf. Damit wollte er Ingenieurwissenschaften und Informatik zusammenführen, um wesentliche Impulse für neue Produkte und Dienstleistungen zu erzeugen. Dies schließt auch die Wechselwirkungen mit dem gesellschaftlichen Umfeld ein.

Die Forschungsarbeit orientiert sich an dem Programm „Dynamik, Mobilität, Vernetzung: Eine neue Schule des Entwurfs der technischen Systeme von morgen“. In der Lehre engagiert sich das Heinz Nixdorf Institut in Studiengängen der Informatik, der Ingenieurwissenschaften und der Wirtschaftswissenschaften.

Heute wirken am Heinz Nixdorf Institut neun Professoren mit insgesamt 150 Mitarbeiterinnen und Mitarbeitern. Pro Jahr promovieren hier etwa 20 Nachwuchswissenschaftlerinnen und Nachwuchswissenschaftler.

Heinz Nixdorf Institute – Interdisciplinary Research Centre for Computer Science and Technology

The Heinz Nixdorf Institute is a research centre within the University of Paderborn. It was founded in 1987 initiated and supported by Heinz Nixdorf. By doing so he wanted to create a symbiosis of computer science and engineering in order to provide critical impetus for new products and services. This includes interactions with the social environment.

Our research is aligned with the program “Dynamics, Mobility, Integration: Enroute to the technical systems of tomorrow.” In training and education the Heinz Nixdorf Institute is involved in many programs of study at the University of Paderborn. The superior goal in education and training is to communicate competencies that are critical in tomorrows economy.

Today nine Professors and 150 researchers work at the Heinz Nixdorf Institute. Per year approximately 20 young researchers receive a doctorate.

Zuletzt erschienene Bände der Verlagsschriftenreihe des Heinz Nixdorf Instituts

Bd. 334 GAUSEMEIER, J. (Hrsg.): Vorausschau und Technologieplanung. 10. Symposium für Vorausschau und Technologieplanung, Heinz Nixdorf Institut, 20. und 21. November 2014, Berlin-Brandenburgische Akademie der Wissenschaften, Berlin, HNI-Verlagsschriftenreihe, Band 334, Paderborn, 2014 – ISBN 978-3-942647-53-3

Bd. 335 RIEKE, J.: Model Consistency Management for Systems Engineering. Dissertation, Fakultät für Elektrotechnik, Informatik und Mathematik, Universität Paderborn, HNI-Verlagsschriftenreihe, Band 335, Paderborn, 2014 – ISBN 978-3-942647-54-0

Bd. 336 HAGENKÖTTER, S .: Adaptive prozessintegrierte Qualitätsüberwachung von Ultraschalldrahtbondprozessen. Dissertation, Fakultät für Elektrotechnik, Informatik und Mathematik, Universität Paderborn, HNI-Verlagsschriftenreihe, Band 336, Paderborn, 2014 – ISBN 978-3-942647-55-7

Bd. 337 PEITZ, C.: Systematik zur Entwicklung einer produktlebenszyklusorientierten Geschäftsmodell-Roadmap. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Band 337, Paderborn, 2015 – ISBN 978-3-942647-56-4

Bd. 338 WANG, R.: Integrated Planar Antenna Designs and Technologies for Millimeter-Wave Applications. Dissertation, Fakultät für Elektrotechnik, Informatik und Mathematik, Universität Paderborn, HNI-Verlagsschriftenreihe, Band 338, Paderborn, 2015 – ISBN 978-3-942647-57-1

Bd. 339 MAO, Y.: 245 GHz Subharmonic Receivers For Gas Spectroscopy in SiGe BiCMOS Technology. Dissertation, Fakultät für Elektrotechnik, Informatik und Mathematik, Universität Paderborn, HNI-Verlagsschriftenreihe, Band 339, Paderborn, 2015 – ISBN 978-3-942647-58-8

Bd. 340 DOROCIAK, R.: Systematik zur frühzeitigen Absicherung der Sicherheit und Zuverlässigkeit fortschrittlicher mechatronischer Systeme. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Band 340, Paderborn, 2015 – ISBN 978-3-942647-59-5

Bd. 341 BAUER, F.: Planungswerkzeug zur wissensbasierten Produktionssystemkonzipierung. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Band 341, Paderborn, 2015 – ISBN 978-3-942647-60-1

Bd. 342 GAUSEMEIER, J.; GRAFE, M.; MEYER AUF DER HEIDE, F. (Hrsg.): 12. Paderborner Workshop Augmented & Virtual Reality in der Produktentstehung. HNI-Verlagsschriftenreihe, Band 342, Paderborn, 2015 – ISBN 978-3-942647-61-8

Bd. 343 GAUSEMEIER, J.; DUMITRESCU, R.; RAMMIG, F.; SCHÄFER, W.; TRÄCHTLER, A. (Hrsg.): 10. Paderborner Workshop Entwurf mechatronischer Systeme. HNI-Verlagsschriftenreihe, Band 343, Paderborn, 2015 – ISBN 978-3-942647-62-5

Bd. 344 BRÖKELMANN, J.: Systematik der virtuellen Inbetriebnahme von automatisierten Produktionssystemen. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Band 344, Paderborn, 2015 – ISBN 978-3-942647-63-2

Bd. 345 SHAREEF, Z.: Path Planning and Trajectory Optimization of Delta Parallel Robot. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Band 345, Paderborn, 2015 – ISBN 978-3-942647-64-9

Bd. 346 VASSHOLZ, M.: Systematik zur wirtschaftlichkeitsorientierten Konzipierung Intelligenter Technischer Systeme. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Band 346, Paderborn, 2015 – ISBN 978-3-942647-65-6

Bd. 347 GAUSEMEIER, J. (Hrsg.): Vorausschau und Technologieplanung. 11. Symposium für Vorausschau und Technologieplanung, Heinz Nixdorf Institut, 29. und 30. Oktober 2015, Berlin-Brandenburgische Akademie der Wissenschaften, Berlin, HNI-Verlagsschriftenreihe, Band 347, Paderborn, 2015 – ISBN 978-3-942647-66-3

Bd. 348 HEINZEMANN, C.: Verification and Simulation of Self-Adaptive Mechatronic Systems. Dissertation, Fakultät für Elektrotechnik, Informatik und Mathematik, Universität Paderborn, HNI-Verlagsschriftenreihe, Band 348, Paderborn, 2015 – ISBN 978-3-942647-67-0

Bezugsadresse:
Heinz Nixdorf Institut
Universität Paderborn
Fürstenallee 11
33102 Paderborn

Zuletzt erschienene Bände der Verlagsschriftenreihe des Heinz Nixdorf Instituts

Bd. 349 MARKWART, P.: Analytische Herleitung der Reihenfolgeregeln zur Entzerrung hochauslastender Auftragsmerkmale. Dissertation, Fakultät für Wirtschaftswissenschaften, Universität Paderborn, HNI-Verlagsschriftenreihe, Band 349, Paderborn, 2015 – ISBN 978-3-942647-68-7

Bd. 350 RÜBBELKE, R.: Systematik zur innovationsorientierten Kompetenzplanung. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Band 350, Paderborn, 2016 – ISBN 978-3-942647-69-4

Bd. 351 BRENNER, C.: Szenariobasierte Synthese verteilter mechatronischer Systeme. Dissertation, Fakultät für Elektrotechnik, Informatik und Mathematik, Universität Paderborn, HNI-Verlagsschriftenreihe, Band 351, Paderborn, 2016 – ISBN 978-3-942647-70-0

Bd. 352 WALL, M.: Systematik zur technologieinduzierten Produkt- und Technologieplanung. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Band 352, Paderborn, 2016 – ISBN 978-3-942647-71-7

Bd. 353 CORD-LANDWEHR, A.: Selfish Network Creation - On Variants of Network Creation Games. Dissertation, Fakultät für Elektrotechnik, Informatik und Mathematik, Universität Paderborn, HNI-Verlagsschriftenreihe, Band 353, Paderborn, 2016 – ISBN 978-3-942647-72-4

Bd. 354 ANACKER, H.: Instrumentarium für einen lösungsmusterbasierten Entwurf fortgeschrittener mechatronischer Systeme. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Band 354, Paderborn, 2016 – ISBN 978-3-942647-73-1

Bd. 355 RUDTSCH, V.: Methodik zur Bewertung von Produktionssystemen in der frühen Entwicklungsphase. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Band 355, Paderborn, 2016 – ISBN 978-3-942647-74-8

Bd. 356 SÖLLNER, C.: Methode zur Planung eines zukunftsfähigen Produktportfolios. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Band 356, Paderborn, 2016 – ISBN 978-3-942647-75-5

Bd. 357 AMSHOFF, B.: Systematik zur musterbasierten Entwicklung technologieinduzierter Geschäftsmodelle. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Band 357, Paderborn, 2016 – ISBN 978-3-942647-76-2

Bd. 358 LÖFFLER, A.: Entwicklung einer modellbasierten In-the-Loop-Testumgebung für Waschautomaten. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Band 358, Paderborn, 2016 – ISBN 978-3-942647-77-9

Bd. 359 LEHNER, A.: Systematik zur lösungsmusterbasierten Entwicklung von Frugal Innovations. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Band 359, Paderborn, 2016 – ISBN 978-3-942647-78-6

Bd. 360 GAUSEMEIER, J. (Hrsg.): Vorausschau und Technologieplanung. 12. Symposium für Vorausschau und Technologieplanung, Heinz Nixdorf Institut, 8. und 9. Dezember 2016, Berlin-Brandenburgische Akademie der Wissenschaften, Berlin, HNI-Verlagsschriftenreihe, Band 360, Paderborn, 2016 – ISBN 978-3-942647-79-3

Bd. 361 PETER, S.: Systematik zur Antizipation von Stakeholder-Reaktionen. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Band 361, Paderborn, 2016 – ISBN 978-3-942647-80-9

Bd. 362 ECHTERHOFF, O.: Systematik zur Erarbeitung modellbasierter Entwicklungsaufträge. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Band 362, Paderborn, 2016 – ISBN 978-3-942647-81-6

Bd. 363 TSCHIRNER, C.: Rahmenwerk zur Integration des modellbasierten Systems Engineering in die Produktentstehung mechatronischer Systeme. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Band 363, Paderborn, 2016 – ISBN 978-3-942647-82-3

Bd. 364 KNOOP, S.: Flachheitsbasierte Positionsregelungen für Parallelkinematiken am Beispiel eines hochdynamischen hydraulischen Hexapoden. Dissertation, Fakultät für Maschinenbau, Universität Paderborn, HNI-Verlagsschriftenreihe, Band 364, Paderborn, 2016 – ISBN 978-3-942647-83-0

Bezugsadresse:
Heinz Nixdorf Institut
Universität Paderborn
Fürstenallee 11
33102 Paderborn