

Alexander Kern



Nutzungsmanagement für sichere digitale Wertschöpfungsnetze

**SHAKER
VERLAG**

Nutzungsmanagement für sichere digitale Wertschöpfungsnetze

Vom Fachbereich Maschinenbau
an der Technischen Universität Darmstadt
zur

Erlangung des akademischen Grades eines Doktor-Ingenieurs (Dr.-Ing.)
genehmigte

DISSERTATION

vorgelegt von

Alexander Marco Kern, M.Sc.

aus Köln, Deutschland

Berichterstatter:	Prof. Dr.-Ing. Reiner Anderl
Mitberichterstatter:	Prof. Dr.-Ing. Matthias Weigold
Tag der Einreichung:	06. August 2020
Tag der mündlichen Prüfung:	03. November 2020

Darmstadt 2020

D17

Forschungsberichte aus dem Fachgebiet
Datenverarbeitung in der Konstruktion

Band 69

Alexander Kern

**Nutzungsmanagement für sichere
digitale Wertschöpfungsnetze**

D 17 (Diss. TU Darmstadt)

Shaker Verlag
Düren 2020

Bibliografische Information der Deutschen Nationalbibliothek

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

Zugl.: Darmstadt, Techn. Univ., Diss., 2020

Copyright Shaker Verlag 2020

Alle Rechte, auch das des auszugsweisen Nachdruckes, der auszugsweisen oder vollständigen Wiedergabe, der Speicherung in Datenverarbeitungsanlagen und der Übersetzung, vorbehalten.

Printed in Germany.

ISBN 978-3-8440-7746-9

ISSN 1435-1129

Shaker Verlag GmbH • Am Langen Graben 15a • 52353 Düren

Telefon: 02421 / 99 0 11 - 0 • Telefax: 02421 / 99 0 11 - 9

Internet: www.shaker.de • E-Mail: info@shaker.de

Geleitwort des Herausgebers

Die moderne Informations- und Kommunikationstechnologie (IKT) bietet vielfältige Innovations- und Leistungspotentiale, die im Entstehungsprozess neuer Produkte auszuschöpfen sind. Dies setzt jedoch voraus, dass die wissenschaftlichen Grundlagen zum Einsatz der modernen IKT in der Produktentstehung vorliegen und neue Methoden wissenschaftlich abgesichert sind. Darüber hinaus stellen die wissenschaftliche Durchdringung und die Bereitstellung wissenschaftlicher Forschungsergebnisse eine abgestimmte Kooperation zwischen Forschung und Industrie dar.

Vor diesem Hintergrund informiert diese Schriftenreihe über aktuelle Forschungsergebnisse des Fachgebiets Datenverarbeitung in der Konstruktion (DiK) des Fachbereichs Maschinenbau an der Technischen Universität Darmstadt.

Ziel der Forschungsarbeiten ist die wissenschaftliche Durchdringung innovativer, interdisziplinärer und integrierter Produktentstehungsprozesse und darauf aufbauend die Konzeption neuer Methoden für die Entwicklung, Konstruktion, Arbeitsvorbereitung und Herstellung neuer innovativer Produkte.

Die wachsende Digitalisierung und Vernetzung industrieller Wertschöpfungsprozesse ist ein fundamentaler Eckpfeiler der horizontalen und vertikalen Integration bestehender Wertschöpfungsketten hin zu digitalen Wertschöpfungsnetzen. Diese sind Voraussetzung für die Entwicklung neuer Geschäftsmodelle und damit für den Erhalt der zukünftigen Wettbewerbsfähigkeit von industriellen Unternehmen. Die größte Herausforderung für diese Unternehmen besteht heute darin, die Vernetzung und Kommunikation zwischen den an den Wertschöpfungsprozessen beteiligten Systemen hinreichend in Bezug auf die Vertraulichkeit, Integrität und Verfügbarkeit abzusichern. Insbesondere die Anforderungen an die Leistungsfähigkeit und Flexibilität stehen heutigen Schutzkonzepten entgegen und stellen ein ungeklärtes Forschungsfeld dar.

Herr Kern nimmt sich dieser Problemstellung in seiner Dissertation an und entwickelt neue Grundlagen für ein durchgängiges Schutzkonzept für den informationstheoretischen Kommunikationsprozess in industriellen Wertschöpfungsnetzen. Den wissenschaftlichen Kern bildet das Nutzungsmanagement für die Umsetzung eines sicheren digitalen Wertschöpfungsnetzes. Dieses besteht aus einem Berechtigungsmanagement, einem Identitätsmanagement und einem Attributmanagement, die jeweils den Anforderungen eines modernen digitalen Wertschöpfungsnetzes gerecht werden. Die Integration der drei Teilkomponenten führt zu einem Schutzkonzept, welches sowohl leistungsfähig als auch flexibel ist und gleichzeitig die Vertraulichkeit, Integrität und Verfügbarkeit der Vernetzung und Kommunikation schützt. Damit leistet die vorliegende Dissertation einen wesentlichen Beitrag für die Weiterentwicklung und Absicherung heutiger und zukünftiger Wertschöpfungsprozesse.

Darmstadt, November 2020

Reiner Anderl

Vorwort des Autors

Die vorliegende Dissertation entstand während meiner Tätigkeit als wissenschaftlicher Mitarbeiter am Fachgebiet Datenverarbeitung in der Konstruktion (DiK) im Fachbereich Maschinenbau an der Technischen Universität Darmstadt.

Mein besonderer Dank gilt meinem Doktorvater Herrn Prof. Dr.-Ing. Reiner Anderl, Leiter des Fachgebiets DiK. Seine wertvollen Anregungen und Empfehlungen, die vielen fachlichen Diskussionen, sowie die gewährten wissenschaftlichen Freiräume haben meine Zeit am DiK geprägt und so einen wichtigen Beitrag zur Entstehung und Fertigstellung dieser Dissertation geleistet. Durch seine wertschätzende Betreuung und wohlwollende Förderung durfte ich viele industrielle und politische Erfahrungen sammeln und habe mich in meiner Zeit am DiK nicht nur wissenschaftlich, sondern auch persönlich weiterentwickeln können.

Herrn Prof. Dr.-Ing. Matthias Weigold, Leiter des Instituts für Produktionsmanagement, Technologie und Werkzeugmaschinen, danke ich herzlich für die kritische Durchsicht meiner Dissertation, die hilfreichen Rückmeldungen und insbesondere für die Übernahme des Korreferats.

Ich bedanke mich bei allen ehemaligen und aktuellen Kolleg*innen des Fachgebiets DiK für die freundschaftliche und kreative Arbeitsatmosphäre. Die zahlreichen fachlichen Diskussionen und stets konstruktive Kritik haben einen wesentlichen Anteil zur Fertigstellung dieser Dissertation beigetragen.

Besonderer Dank gilt meinen Freund*innen Lars Niemczick, Stefan Kugler, Thiago Weber Martins, Erdal Tantik, Katharina Warncke, Marco Grimm und Benedikt Sierck, die mich in dieser besonderen Zeit sowohl fachlich als auch zwischenmenschlich entscheidend geprägt haben.

Ganz herzlich möchte ich mich abschließend bei meiner Familie bedanken, die mich auf meinem Weg zu dieser Dissertation stets unterstützt und treu begleitet hat. Insbesondere meine Mama Silvia Kern und mein Papa Theo Kern sowie meine Schwester Tamara Kern haben mich auf meinem Weg zum Gelingen dieser Dissertation immer unterstützt.

Mein größter Dank gilt meiner Ehefrau Marlene. Ihre uneingeschränkte Geduld hat mir die Motivation und Ausdauer geschenkt, um diese Dissertation zu vollenden. Ihre liebevolle Unterstützung war mir zudem stets eine Quelle der Freude und Inspiration. Ihr und meiner Familie ist diese Arbeit gewidmet.

Darmstadt, November 2020

Alexander Kern

Inhaltsverzeichnis

Abbildungsverzeichnis	VII
Tabellenverzeichnis	IX
Abkürzungsverzeichnis	XI
1 Einleitung	1
1.1 Motivation.....	2
1.2 Zielsetzung der Dissertation.....	5
1.3 Aufbau der Dissertation.....	6
2 Stand der Technik und Forschung	9
2.1 Digitalisierung und Vernetzung der Industrie.....	9
2.2 Digitale Kommunikation.....	11
2.2.1 Die Geschichte des Internets.....	12
2.2.2 TCP/IP-Referenzmodell und OSI-Schichtenmodell.....	13
2.2.3 Leistungskenngrößen für Kommunikationsnetzwerke.....	18
2.2.4 Entwicklung der digitalen Kommunikation.....	19
2.3 Software-definierte Vernetzung.....	22
2.3.1 SDN Ebenenmodell.....	22
2.3.2 OpenFlow.....	26
2.4 Sicherheit in der Informations- und Kommunikationstechnik.....	30
2.4.1 Schutzziele.....	31
2.4.2 Risiko- und Bedrohungsanalyse.....	32
2.4.3 Technische Schutzmaßnahmen.....	34
2.4.4 Genutzte Normen und Standards.....	37
2.5 Berechtigungsmanagement.....	38
2.5.1 Definition wichtiger Konzepte und Begrifflichkeiten.....	38
2.5.2 Klassische Berechtigungsmodelle.....	41
2.5.3 Moderne Berechtigungsmodelle.....	43
2.6 Identitätsmanagement.....	48
2.6.1 Identität.....	48
2.6.2 Authentifizierungsmechanismen.....	50
2.7 Aktuelle Forschungsansätze und industrielle Umsetzungen.....	52
2.8 Fazit.....	53
3 Anforderungsprofil	55
3.1 Handlungsbedarf.....	55
3.2 Bedrohungsanalyse.....	59
3.2.1 Angreifermodellierung.....	59

3.2.2	Bedrohungsmodellierung.....	60
3.3	Zieldefinition	62
3.4	Anforderungen.....	63
3.4.1	Anforderungen an das Nutzungsmanagement	63
3.4.2	Anforderungen an die Implementierung	68
3.5	Fazit zum Anforderungsprofil.....	69
4	Konzept für das Attribut-basierte Nutzungsmanagement in Software- definierten Wertschöpfungsnetzen	71
4.1	Begriffsdefinitionen.....	72
4.2	Konzeptioneller Ansatz.....	75
4.3	Konzeptstruktur	77
4.4	Gesamtkonzept	78
4.4.1	Aufbau des Nutzungsmanagements.....	78
4.4.2	Berechtigungsmanagement für Wertschöpfungsnetze	87
4.4.3	Identitätsmanagement für Wertschöpfungsnetze	107
4.4.4	Berechtigungsorientiertes Attributmanagement.....	121
4.4.5	Integration der Teilkonzepte in eine Nutzungsmanagementarchitektur für Software-definierte Wertschöpfungsnetze	128
4.5	Fazit zum Konzept.....	129
5	Prototypische Implementierung	133
5.1	Aufbau des Swan-Demonstratorsystems	133
5.2	Implementierung der ABUC-Berechtigungsarchitektur.....	134
5.3	Implementierung des Identitätsmanagements.....	139
5.4	Implementierung des Attributmanagements	142
5.5	Implementierung der graphischen Benutzungsoberfläche	143
5.6	Integration der Teilkonzepte zum Swan-Demonstratorsystem	149
5.7	Fazit zur Implementierung	151
6	Validierung und Verifikation	153
6.1	Validierung	154
6.1.1	Anwendungsfall für die Validierung	154
6.1.2	Bewertung der Sicherheit	162
6.1.3	Bewertung der Leistungsfähigkeit	163
6.1.4	Bewertung der Flexibilität	167
6.2	Verifikation des Anforderungsprofils.....	170
6.3	Fazit zur Validierung und Verifikation	176
7	Ausblick	179
8	Zusammenfassung	183
Literatur		187
Anhang		233
A.1	Internet-Referenzmodelle	234
A.2	Kommentierter XACML-Politik-Satz	236
A.3	Public-Key-Infrastruktur.....	241