

Marco Grimm



Konzept zum durchgängigen
Schutz von Daten in der verteilten
additiven Fertigung

**SHAKER
VERLAG**

Konzept zum durchgängigen Schutz von Daten in der verteilten additiven Fertigung

Vom Fachbereich Maschinenbau
an der Technischen Universität Darmstadt
zur
Erlangung des Grades eines Doktor-Ingenieurs (Dr.-Ing.)
genehmigte

D I S S E R T A T I O N

vorgelegt von

Marco Grimm, M.Sc.

aus Frankfurt am Main

Berichterstatter: Prof. Dr.-Ing. Reiner Anderl
Mitberichterstatter: Prof. Dr.-Ing. Matthias Weigold
Tag der Einreichung: 21. Mai 2019
Tag der mündlichen Prüfung: 17. Juli 2019

Darmstadt 2019

D17

Forschungsberichte aus dem Fachgebiet
Datenverarbeitung in der Konstruktion

Band 67

Marco Grimm

**Konzept zum durchgängigen Schutz von Daten
in der verteilten additiven Fertigung**

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., 2019

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 978-3-8440-7409-3

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

Vorwort 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 Produkte.

Die vorliegende Dissertation befasst sich mit der digitalen Prozesskette zur verteilten additiven Fertigung. Diese ist gekennzeichnet durch einen globalen Austausch von Bauteil- und Fertigungsdaten. Im Rahmen dieses unternehmensübergreifenden Datenaustauschs werden von verschiedenen Prozessakteuren Bauteile für die additive Fertigung optimiert, zu Aufträgen zusammengefasst und schließlich am Bestimmungsort gefertigt. Die moderne Informations- und Kommunikationstechnologie bietet hierzu mit ihrer Flexibilität und Schnelligkeit wichtige Wertschöpfungsfaktoren. Andererseits entstehen durch den digitalen Datenaustausch auch Risiken bezüglich Datenverlust und Manipulation. Diese Missbrauchsrisiken werden von den industriell etablierten Prozessketten zur additiven Fertigung nicht gelöst. Es sind heute noch keine geeigneten Mechanismen für eine effektive Nutzungskontrolle in der additiven Fertigung verfügbar, die nicht zu wesentlichen Einschränkungen bezüglich der Flexibilität führen. Die Folge ist, dass Bauteildaten heute in der Industrie weitgehend ungeschützt und unkontrolliert verarbeitet werden.

Herr Grimm nimmt sich dieser Problematik an und entwickelt in seiner Dissertation neue Ansätze für einen durchgängigen kryptografischen Schutz von Bauteil- und Fertigungsdaten in der additiven Fertigung. Er erweitert dazu die Prozesskette zur additiven Fertigung um neue Datensegmentierungs-, Pseudonymisierungs- und Verschlüsselungsschritte. Darauf aufbauend führt er eine auf Fertigungsattributen basierte Autorisierung von Anwendern und Systemen ein. Die Basis hierfür sind Prozessparameter und Einstellungen, welche relevant für die Arbeitsvorbereitung und Fertigung sind. Mit den aus Fertigungsattributen gebildeten Berechtigungen

erhalten Anwender und Fertigungssysteme ausschließlichen Zugriff auf die jeweils benötigten und für sie vorgesehenen Daten. Somit ist es möglich, das zugrunde liegende Bauteil- und Fertigungswissen ortsunabhängig und über die gesamte Prozesskette wirksam vor unberechtigten Zugriffen zu schützen, ohne die Flexibilität der Fertigung einzuschränken.

Die vorgestellten Methoden werden in einem Assistenzsystem und einem additiven Produktionssystem prototypisch umgesetzt. Abschließend wird der Prototyp anhand des hergeleiteten Anforderungsprofils verifiziert und mit typischen Anwendungsfällen aus der Praxis validiert.

Reiner Anderl

Inhaltsverzeichnis

1	Einleitung	1
1.1	Motivation und Problemstellung	1
1.2	Zielsetzung der Dissertation	3
1.3	Aufbau der Dissertation	4
2	Stand der Technik und Wissenschaft	7
2.1	Additive Fertigung	7
2.1.1	Technologie der additiven Fertigungsverfahren	8
2.1.1.1	Strangablegeverfahren	9
2.1.1.2	Laser-Sintern und Strahlschmelzen	10
2.1.2	Prozesskette zur additiven Fertigung	11
2.1.3	Datenformate der additiven Fertigung	12
2.1.3.1	STL-Schnittstelle	13
2.1.3.2	Schichtdaten	14
2.1.3.3	NC-Daten	15
2.1.4	Verteilte additive Fertigung	16
2.2	Virtuelle Produktentstehung	18
2.2.1	Produkt- und Bauteildaten	18
2.2.2	Produktentstehungsprozess	19
2.3	Sicherheit in der Informationstechnik	20
2.3.1	Schutzziele	21
2.3.2	Sicherheitsmaßnahmen	22
2.3.2.1	Juristische Maßnahmen	22
2.3.2.2	Strategische Maßnahmen	22
2.3.2.3	Organisatorische Maßnahmen	23
2.3.2.4	Technische Maßnahmen	23
2.3.3	Sicherheitsnormen	24
2.4	Kryptologie	24
2.4.1	Verschlüsselung	25
2.4.2	Symmetrische Kryptografie	27
2.4.2.1	Strom- und Blockchiffren	28
2.4.2.2	AES-Algorithmus	31
2.4.3	Asymmetrische Kryptografie	32
2.4.3.1	RSA-Kryptosystem	33
2.4.3.2	Elliptische-Kurven-Kryptografie	35
2.4.3.3	Pairing-basierte Kryptografie	36
2.4.4	Kryptografische Hashfunktionen	36
2.4.5	Digitale Signaturen	37

2.4.6	Zertifikate	38
2.4.7	Zugriffskontrolle und Rechtemanagement	39
2.5	Existierende Forschungsansätze	40
2.6	Fazit	42
3	Anforderungsprofil	45
3.1	Handlungsbedarf	45
3.2	Betrachtete Anwendungsfälle	47
3.2.1	Systemakteure	47
3.2.2	Systemgrenze	49
3.3	Angreifermodellierung	49
3.3.1	Angriffsvektoren	52
3.4	Zieldefinition	53
3.5	Anforderungen	53
3.5.1	Anforderungen an die Methodenkonzeption	54
3.5.2	Anforderungen an die Implementierung der Methoden	58
3.6	Fazit	61
4	Konzeption zum durchgängigen Schutz von Daten in der verteilten additiven Fertigung	65
4.1	Konzeptioneller Ansatz	65
4.2	Struktur des Gesamtkonzepts	66
4.3	Entwicklung der erweiterten Prozesskette	68
4.3.1	Integration der Autorisierung in die Prozesskette	68
4.3.2	Übersicht über die erweiterte Prozesskette	70
4.4	Definition von fertigungsbezogenen Attributen	72
4.4.1	Attributkonvention	74
4.4.2	Berechtigungsrichtlinien	76
4.4.3	Struktur der Richtlinien	77
4.5	Repräsentation geschützter Bauteil- und Fertigungsdaten	79
4.5.1	Segmentierung der Fertigungsdaten	80
4.5.2	Symmetrische Verschlüsselung der Fertigungsdatensegmente	81
4.5.3	Pseudonymisierung	83
4.5.4	Randomisierung	85
4.5.4.1	Vorgehensweise	88
4.5.5	Authentizitätsschutz	89
4.6	Zugriffsautorisierung für Bauteil- und Fertigungsdaten	90
4.6.1	Zustandsbehaftete Autorisierung	91
4.6.2	Erzeugung der Inhaltsschlüssel	92
4.6.3	Verknüpfung der Teilschlüssel	94
4.6.4	Autorisierungsprotokoll	94
4.7	Attributbasierte Autorisierung der Segmentzuordnung	96
4.7.1	Auswahl der kryptografischen Parameter	97
4.7.2	Bilineare Abbildung	99
4.7.3	Infrastruktur zur Verwaltung von Schlüsseln und Berechtigungen	101

4.7.4	Schlüsselerzeugung	102
4.7.5	Verschlüsselung der Segmentzuordnungsdaten	103
4.7.6	Entschlüsselung der Segmentzuordnungsdaten	104
4.8	Präsentation von geschützten Bauteil- und Fertigungsdaten	105
4.8.1	Assoziation von Bauteilpräsentation und Fertigungsdaten	106
4.8.1.1	Geometrische Transformation	107
4.8.2	Geometrische Detailreduktion	109
4.8.3	Anbindung von Stützstrukturen	111
4.9	Fazit	112
5	Prototypische Implementierung	115
5.1	Architektur des Gesamtsystems	115
5.2	Randbedingungen der Implementierung	117
5.3	SIAM-Assistenzsystem	118
5.3.1	Grafische Benutzungsoberfläche	119
5.3.1.1	Bauteilpräsentation und Transformationen	120
5.3.2	Repräsentation der Transformationsmatrix	125
5.3.3	Generierung der Fertigungsattribute	125
5.3.4	Bauteilimport und Export	126
5.3.5	Segmentgenerierung und Randomisierung	127
5.3.6	Umsetzung der kryptografischen Funktionen mit der SIAMCrypto-Klasse	128
5.4	Datenaustauschformat SIAM-XML	132
5.4.1	Authentisierung der Fertigungsdatensätze	134
5.5	Autorisierungsinstanz	135
5.5.1	Hochladen von Teilschlüsseln	135
5.5.2	Abruf von Teilschlüsseln	136
5.5.3	Widerruf von Teilschlüsseln	137
5.5.4	Schutz der Schlüsselübertragung	138
5.5.5	Implementierung der Datenbank	138
5.6	Prozesssimulation	139
5.7	SIAM-Maschinensteuerung	143
5.7.1	Desktop-FDM-Maschine	144
5.7.2	Eingebettete Maschinensteuerung	145
5.7.3	Hardwarearchitektur	145
5.7.4	Software	147
5.8	Maschinenzertifizierung	148
5.8.1	Prüfbauteil	150
5.9	Fazit zur Implementierung	150
6	Verifikation und Validierung	153
6.1	Methodik zur Verifikation und Validierung	153
6.2	Beispielbauteile	154
6.3	Testfall	157
6.4	Bewertung der Sicherheit	159
6.4.1	Statistische Güte der SIAM-Datensätze	159

6.4.2	Kryptografische Sicherheit	163
6.4.2.1	Sicherheit der Nutzdaten	163
6.4.2.2	Sicherheit der Segmentzuordnung	164
6.4.2.3	Sicherheit der Schlüsselverteilung	164
6.4.3	Angriffsvektoren im SIAM-System	165
6.5	Bewertung der Datenbeschreibung und Funktionalitäten	167
6.6	Bewertung der Leistung	169
6.6.1	Produktivitätsverlust im In-Prozess	169
6.6.2	Verbindungslatenz	173
6.6.3	Skalierbarkeit	174
6.6.3.1	Speicherbedarf	174
6.6.3.2	Rechenaufwand	176
6.7	Validierung	177
6.8	Fazit	180
7	Ausblick	183
8	Zusammenfassung	185
	Literaturverzeichnis	187
A	Verwendete Schlüssel	199
B	Beispiel für einen SIAM-XML-Datensatz	201
C	Elektronische Schaltung der SIAM-Steuerung	203

Abbildungsverzeichnis

2.1	Klassifizierung der additiven Fertigungsverfahren	9
2.2	Verfahrensprinzip FDM	10
2.3	Verfahrensprinzip SLS und SLM	11
2.4	Prozesskette zur additiven Fertigung	12
2.5	STL-Repräsentation	14
2.6	Schematischer Satzaufbau und Beispielsätze nach DIN 66025	16
2.7	Architektur der verteilten Fertigung im Cloud Manufacturing	17
2.8	Produktlebenszyklus aus informationstechnischer Sicht	20
2.9	Symmetrische Verschlüsselung	28
2.10	Asymmetrische Verschlüsselung	33
2.11	Attributbasierte Zugriffskontrolle	40
3.1	Anwendungsfalldiagramm	48
4.1	Fokus des Konzepts	66
4.2	Struktur des Gesamtkonzepts	67
4.3	Datenzugriff autorisieren	69
4.4	Übersicht über die Konzeptbestandteile	71
4.5	Konzeptbestandteile am Beispiel der verteilten additiven Fertigung	72
4.6	Innerbetriebliche Verteilung von Aufträgen	73
4.7	Struktur der Berechtigungsrichtlinien	78
4.8	Berechtigungsrichtlinie des Anwendungsbeispiels als Baum	79
4.9	Segmentierungsstrategien	80
4.10	Segmentdatenverschlüsselung in SADT-Darstellung	82
4.11	Schematische Darstellung des zweistufigen Pseudonymisierungsprozesses	84
4.12	Aufbau des Universally Unique Identifier	85
4.13	Beispielfall Kreiskegel	86
4.14	Datenlänge je Schichtrepräsentation des Kegels	87
4.15	Prozess der Segmentrandomisierung	88
4.16	Größenverteilung für den Kegel nach der Randomisierung	89
4.17	Lösungsansatz zur zustandsbehafteten Autorisierung	92
4.18	Autorisierungsprotokoll	95
4.19	Schlüsselinfrastruktur in der verteilten additiven Fertigung	101
4.20	Assoziation von Bauteilpräsentation und Fertigungsdaten	106
4.21	Koordinatentransformation im Bauraum	107
4.22	Reduktion der Bauteilgeometrie	110
4.23	Anbindung von Stützstrukturen	111
4.24	Bodenanbindung in der Bauteil Bounding Box	112

5.1	Architektur des Gesamtsystems	116
5.2	Hauptansicht SIAM-Assistenzsystem	120
5.3	Bauteilpräsentation in SIAM	121
5.4	Methoden zur Vereinfachung der Geometriedarstellung	123
5.5	Vereinfachung der Bauteilpräsentation	123
5.6	Rotationswerkzeuge	125
5.7	Signaturprüfung in SIAM	131
5.8	Implementierte XML-Struktur zur Datenspeicherung	133
5.9	Hauptfenster des SIAM-Simulators	141
5.10	Anzeige nach dem Laden einer SIAM-Datei	142
5.11	Interaktive Code-Visualisierung eines Bauteils nach der Entschlüsselung	143
5.12	SIAM-Demonstrator	144
5.13	SIAM-Controller	146
5.14	Blockschaltbild SIAM-Steuerung	147
5.15	Softwarearchitektur der SIAM-Maschinensteuerung	148
5.16	Maschinenzertifizierungsprozess	149
5.17	Prüfbauteil zur Maschinenkalibrierung und Zertifizierung	150
6.1	Beispielbauteile 1 und 2	155
6.2	Beispielbauteile 3 und 4	156
6.3	Zeit-Segment-Abhängigkeit bei der SIAM-Nutzung	172
6.4	Chiffretextgrößen und Erzeugungsdauer der Zuordnungstabellen	175
6.5	Maschinenschlüsselgrößen und Erzeugungsdauer	175
6.6	Zeitmessungen des vollständigen Schutzprozesses in SIAM	177
6.7	Geladenes Bauteil und erfolgreicher Export in SIAM-XML	178
6.8	Auszug der exportierten Segmentdaten	178
6.9	Transformationen des geschützten Bauteils	179
6.10	Hergestelltes Verdichterrad	180

Tabellenverzeichnis

2.1	Äquivalenz der Schlüssellängen	35
3.1	Übersicht der Anforderungen	62
3.2	Fortsetzung Übersicht der Anforderungen	63
4.1	Definition der numerischen und alphabetischen Attribute	74
4.2	Übersicht Attributkonvention	75
4.3	Fortsetzung Übersicht Attributkonvention	76
5.1	Rollen und Werkzeuge der Systemakteure im SIAM-Assistenzsystem	119
5.2	Ein- und Ausgabeformate	126
5.3	Datenbank-Tabellenschema	139
6.1	Betrachtete Testbauteile	157
6.2	Betrachtete Bauteildatensätze	157
6.3	Bauteileingabedaten für die Zufallstests	160
6.4	Ergebnisse der Zufallstests	160
6.5	Verarbeitungszeiten für die Komponenten eines Triebwerk gondelscharniers	170
6.6	Aufschlüsselung der Zeiten der SIAM Nebenutzung	171
6.7	Ermittelte durchschnittliche Latenzen im SIAM-System	173

Symbolverzeichnis

a, b, c	Ganzzahlige Parameter in endlichen Körpern
A, B, H	Koordinatensysteme zur Vektortransformation
α, β	Geheime Schlüsselparameter als Exponenten für MK
AT	Autorisierungsdaten der Autorisierungsinstanz
B	Baum der Berechtigungsrichtlinie
$c_{a,m}$	Schlüsseltext der Segmentzuordnungstabelle
c_i	Segment-Schlüsseltext mit Index i
C_i	Schlüsseltextblöcke mit Index i
C_m	Geschützter Inhaltsschlüssel k_m
C_{Policy}	Über Attribute geschützter Schlüsseltext
ctr_i	Inkrementierbarer Zähler für Blockchiffre
ΔP_{BM}	Relative Differenz (Verlust) der Betriebsmittelproduktivität
D_k	Entschlüsselungsfunktion mit Schlüssel k
E_k	Verschlüsselungsfunktion mit Schlüssel k
$e(g, g)$	Bilineare Paarung der Generatoren g in zwei Gruppen \mathbb{G}_i
g, h	Erzeuger (Generatoren) im endlichen Körper \mathbb{Z}_p
$\mathbb{G}_0, \mathbb{G}_1, \mathbb{G}_2$	Endliche Gruppen der Ordnung p
\mathbb{G}_T	Endliche Zielgruppe einer bilinearen Paarung
$h_{SHA2}(m)$	Hashwert der Nachricht m mit der Hashfunktion SHA-2
ID	Identifikator
id_i	Segmentidentifikator mit Index i
IV	Initialisierungsvektor für die Blockchiffre
J_i	Teilmenge an Attributen

k	Einbettungsgrad
$k_{cA,i}, k_{cB,i}$	Teilschlüssel A und B
$k_{c,i}$	Inhaltsschlüssel für das Segment i
k_i	Symmetrischer Schlüssel mit Index i
k_m	Symmetrischer Schlüssel der Segmentzuordnungstabelle
m_i	Nachricht mit Index i
MK	Geheimer Generalschlüssel der Zertifizierungsstelle
M_m	Segmentzuordnungstabelle
\vec{n}	Normalenvektoren für Flächenfacetten
n_u	Nutzungszähler
p	Primzahl zur Festlegung der Ordnung einer Gruppe
${}^A\vec{p}$	Ortsvektor im Bezugssystem A
p_i	Klartext mit Index i
pk	Öffentlicher Schlüssel
ψ, θ, ϕ	Rotationswinkel im Koordinatensystem nach DIN 70000
PK	öffentlicher Schlüssel der attributbasierten Verschlüsselung
P, Q	Punkte auf einer elliptischen Kurve
P_i	Klartextblöcke mit Index i
r, h, q	Ganzzahlige Parameter für die Erzeugung von Paarungen
R	Wurzel des Berechtigungsbaums (Berechtigungsrichtlinie)
${}^A\mathbf{R}_B$	Rotationsmatrix des Bauteils im Bezugssystem A
s	Zufällige Parameter im Berechtigungsbaum
S	Im Schlüssel SK_i zugewiesene Attribute
S'_i	Bei der Zertifizierungsstelle gespeicherte Attribute
sig_m	Digitale Signatur der Nachricht m
sk	Privater geheimer Schlüssel
SK_M	Geheimer Schlüssel einer Maschine M

SK_N	Geheimer Schlüssel eines Nutzers N
SK_S	Geheimer Schlüssel eines Systems S
S_M	Menge an Attributen einer Maschine
T	Autorisierungstag
${}^A\mathbf{T}_B$	Homogene Transformationsmatrix im Bezugssystem A
t_a	Ablaufzeit
A_{tB}^{\rightarrow}	Bauteilverschiebungsvektor im Bezugssystem A
t_{BH}	Hauptzeit des Betriebsmittels
t_{BN}	Nebennutzungszeit des Betriebsmittels
$t_{BN,E}$	Nebennutzungszeitanteil Datenentschlüsselung
$t_{BN,S}$	Nebennutzungszeitanteil Schlüsselabruf
$t_{BN,Z}$	Nebennutzungszeitanteil Entschlüsselung der Segmentzuordnungstabelle
T_o	Eigentümertoken
t_{rv}	Entzugszeitpunkt (Revokation) der Berechtigungen
T_u	Anwendertoken
$t_{u,i}$	Authentisierungstoken mit Index i (z.B. Anwendertoken)
V, Y	Baumknoten V und Blätter Y
\vec{v}_i	Ortsvektoren für Eckpunkte
\mathbb{Z}_p	Endlicher Körper der Primordnung p

Abkürzungsverzeichnis

2D	zweidimensional
3D	dreidimensional
3MF	3D Manufacturing Format
AABB	Axis Aligned Bounding Box
ABE	Attribute Based Encryption
ADC	Analog-Digital Converter
AEAD	Authenticated Encryption with Associated Data
AES	Advanced Encryption Standard
AF	Additive Fertigung
AMF	Additive Manufacturing File Format
AM	Additive Manufacturing
API	Application Program Interface
AP	STEP Application Protocol
ARM	Advanced RISC Machines Architektur
ASCII	American Standard Code for Information Interchange
B-Rep	Boundary Representation
BPMN	Business Process Model and Notation
BSI	Deutsches Bundesamt für Sicherheit in der Informationstechnik
CAD	Computer Aided Design
CAM	Computer Aided Manufacturing
CAx	Computer Aided X
CA	Certificate Authority
CC	Common Criteria

CDH	Computational Diffie-Hellman Problem
CLI	Common Layer Interface
CNC	Computerized Numerical Control
CPU	Central Processing Unit
DBDH	Decisional Bilinear Diffie-Hellman Problem
DDH	Decisional Diffie-Hellman Problem
DES	Data Encryption Standard
DIN	Deutsche Industrie Norm
DLP	Discrete Logarithm Problem
DRM	Digital Rights Management
EAL	Evaluation Assurance Level
ECC	Elliptic Curve Cryptography
ECDLP	Elliptic Curve Discrete Logarithm Problem
ERM	Enterprise Rights Management
ERP	Enterprise Resource Planning
FDM	Fused Deposition Modeling
FLM	Fused Layer Modeling
GPL	GNU General Public License
GUI	Graphical User Interface
HMI	Human Machine Interface
HTTP	Hypertext Transport Protokoll
IBE	Identity Based Encryption
IC	Integrated Circuit
IDE	Integrated Development Environment
IKT	Informations- und Kommunikationstechnologie
IP	Intellectual Property
ISO	International Organization for Standardization

IT	Informationstechnologie
IV	Initialisierungsvektor
JSON	Javascript Object Notation
LAN	Local Area Network
LLM	Layer Laminated Manufacturing
MAC	Message Authentication Code
MCU	Microcontroller Unit
MPU	Microprocessor Unit
NC	Numerical Control
NDA	Non-Disclosure Agreement
NIST	National Institute of Standards and Technology
OMAP	Open Multimedia Application Platform
OMG	Object Management Group
OS	Operating System
PDM	Produktdatenmanagement
PEP	Produktentstehungsprozess
PGP	Pretty Good Privacy
PKI	Public Key Infrastructure
PLM	Product Lifecycle Management
PMI	Product Manufacturing Information
PRU	Programmable Realtime Unit
REFA	Verband für Arbeitsgestaltung, Betriebsorganisation und Unternehmensentwicklung
REST	Representational State Transfer
RIPED	RACE Integrity Primitives Evaluation Message Digest
RISC	Reduced Instruction Set Computer
RPT	Rapid Prototyping and Tooling
RSA	Rivest Shamir Adleman Cryptosystem

RTOS	Realtime Operating System
SADT	Structured Analysis and Design Technique
SBC	Single Board Computer
SHA	Secure Hash Algorithm
SIAM	Secure Information Exchange for Additive Manufacturing
SIM	Subscriber Identity Module
SLM	Selective Laser Melting
SLS	Selective Laser Sintering
SOA	Service-Oriented Architecture
SQL	Structured Query Language
STEP	Standard for the Exchange of Product Model Data
STL	Surface Triangulation Language
TCG	Trusted Computing Group
TLS	Transport Layer Security
TPM	Trusted Platform Module
UML	Unified Modeling Language
URL	Uniform Resource Locator
UUID	Universally Unique Identifier
VDI	Verein Deutscher Ingenieure
VM	Virtuelle Maschine
VPN	Virtual Private Network
XML	Extensible Markup Language
XOR	Exklusiv-Oder-Funktion
XrML	Extensible Rights Markup Language