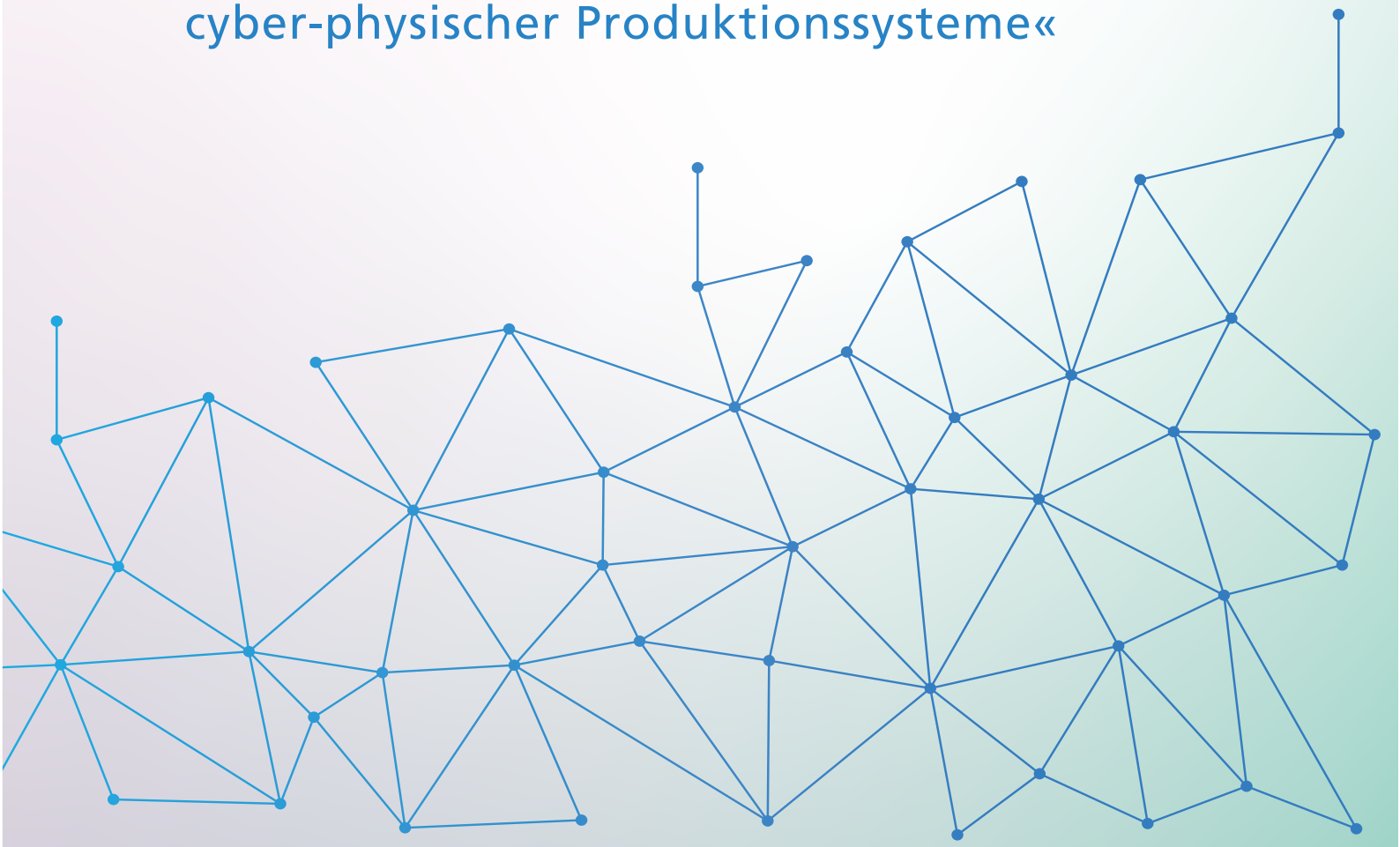
STUTTGARTER BEITRÄGE ZUR PRODUKTIONSFORSCHUNG

Daniel Stock

»Authentifizierungsverfahren auf Basis von Selbstbeschreibungsmerkmalen cyber-physischer Produktionssysteme«



Fraunhofer IPA

Universität Stuttgart

STUTTGARTER BEITRÄGE ZUR PRODUKTIONSFORSCHUNG BAND 138

Daniel Stock

»Authentifizierungsverfahren auf Basis von Selbstbeschreibungsmerkmalen cyber-physischer Produktionssysteme«

Kontaktadresse:

Fraunhofer-Institut für Produktionstechnik und Automatisierung IPA
Nobelstr. 12
70569 Stuttgart
Telefon 0711 970-1100
info@ipa.fraunhofer.de
www.ipa.fraunhofer.de

Bibliographische Information der Deutschen Nationalbibliothek

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

Zugl.: Stuttgart, Univ., Diss., 2022

D 93

2022

Druck und Weiterverarbeitung:

Fraunhofer Verlag, Mediendienstleistungen, 2022
Für den Druck des Buches wurde chlor- und säurefreies Papier verwendet.

Authentifizierungsverfahren auf Basis von Selbstbeschreibungsmerkmalen cyber-physischer Produktionssysteme

Von der Fakultät Konstruktions-, Produktions- und Fahrzeugtechnik
der Universität Stuttgart
zur Erlangung der Würde eines Doktor-Ingenieurs (Dr.-Ing.)
genehmigte Abhandlung

Vorgelegt von

Dipl.-Ing. Daniel Stock
aus Prag

Hauptberichter:	Prof. Dr.-Ing. Thomas Bauernhansl
Mitberichter:	Prof. Dr.-Ing. Michael Weyrich
Tag der mündlichen Prüfung:	27.04.2022

Institut für Industrielle Fertigung und Fabrikbetrieb (IFF)
der Universität Stuttgart
2022

Vorwort des Autors

Die vorliegende Arbeit entstand während meiner Arbeit als wissenschaftlicher Mitarbeiter am Fraunhofer-Institut für Produktionstechnik und Automatisierung IPA. Hier hatte ich die Möglichkeit in einer jungen Abteilung im spannenden Umfeld der digitalen Transformation seit der Geburtsstunde von Industrie 4.0 mitzuwirken.

Für die Möglichkeit der Promotion in diesem hochgradig anspruchsvollen Umfeld sowie die freundliche Hilfe und vielfältige Inspiration gilt mein Dank in erster Linie meinem Doktorvater Prof. Dr. Thomas Bauernhansl. Prof. Dr. Michael Weyrich danke ich für den fachlichen Austausch und die Übernahme des Mitberichts.

Mein Dank gilt zudem meinem Abteilungsleiter, Joachim Seidelmann, für die fachliche und umsichtige Unterstützung im Rahmen des vielfältigen und herausfordernden Alltags. Zudem danke ich vielen aktuellen und ehemaligen Kollegen, die mir in den vergangenen Jahren mit Rat und Tat zur Seite standen.

Meinem Kollegen Michael Oberle danke ich für den fachlichen Austausch und für die Durchsicht dieser Arbeit.

Ich danke zudem den Paten der in dieser Arbeit dargestellten Fallstudien für die Unterstützung bei der Erhebung der notwendigen Informationen: Ralf Kölle (scitis.io GmbH) und Christian Ehrmann (BÄR Automation GmbH).

Für die immerwährende Unterstützung und das mir entgegengebrachte Verständnis, danke ich meiner Frau Judith, meiner Familie, meiner Schwester Anna-Maria, meinen Großeltern und insbesondere meinen Eltern Rostislava und Angelo, die mich fortwährend unterstützt und gefördert haben.

Daniel Stock

Kurzfassung

Cybersicherheit und die hierfür notwendigen Authentifizierungsverfahren gewinnen in einer zunehmend vernetzten Produktion zwingend an Bedeutung. Diese Vernetzung führt zur Entstehung neuer Angriffsvektoren, die ein Risiko für die IT-Sicherheit im industriellen Umfeld und somit auch für die funktionale Sicherheit und Zuverlässigkeit technischer Systeme darstellen. Neben der Absicherung der Netzwerke und Zugriffs-beschränkter Bereiche stellt sich hier die Frage, ob ein cyber-physisches Produktionssystem als Entität, die Zugriff auf eine andere Ressource oder Zutritt zu einem geschützten Bereich einer Infrastruktur anfragt, auch diejenige ist, die sie mittels ihrer digitalen Identität vorgibt zu sein. Die Authentifizierung der Identität einer Entität kann mit aufwendigen technischen und organisatorischen Mitteln dargestellt werden. Jedoch besteht hier ein Zielkonflikt zwischen Funktionalität, Benutzbarkeit und Sicherheit. Die physischen Komponenten von CPPS werden durch den technischen Fortschritt getrieben immer leistungsfähiger und intelligenter. Ihre Fähigkeiten können durch zusätzliche Dienste im "Cyberspace" beliebig skalieren. Sie verfügen so über immer komplexere Self-X-Fähigkeiten, die ihren Autonomiegrad erhöhen.

Die vorliegende Arbeit geht der Frage nach wie eine CPPS-Selbstbeschreibung, also die Self-X-Fähigkeit Informationen über sich selbst zu übermitteln, dazu genutzt werden kann für dieses CPPS eine sichere Identität zu schaffen, die auf ihren Selbstbeschreibungsmerkmalen basiert. Der Beitrag der Arbeit liegt hierbei auf der Beschreibung eines ganzheitlichen Ansatzes zur Umsetzung von Authentifizierungsverfahren auf Grundlage von Selbstbeschreibungsmerkmalen, die als zusätzliche Maßnahmen im Rahmen einer „Defense-in-Depth"-Strategie eingesetzt werden können.

Abstract

Cybersecurity and the authentication procedures required for it are becoming imperatively more important in an increasingly networked production. This networking leads to the emergence of new attack vectors that pose a risk to IT security in the industrial environment and thus also to the functional safety and reliability of technical systems. In addition to securing networks and access-restricted areas, this raises the question of whether a cyber-physical production system, as an entity requesting access to another resource or access to a protected area of an infrastructure, is also the entity it claims to be by means of its digital identity. Authentication of an entity's identity can be represented by elaborate technical and organizational means. However, there is a conflict of objectives here between functionality, usability, and security. Driven by technological progress, the physical components of CPPS are becoming increasingly powerful and intelligent. Their capabilities can scale arbitrarily through additional services in "cyberspace". Thus, they have increasingly complex self-x capabilities that increase their degree of autonomy.

This thesis addresses the question of how a CPPS self-description, i.e., the Self-X capability to convey information about itself, can be used to create a secure identity for this CPPS based on its self-description characteristics. The contribution of the work here lies in the description of a holistic approach to the implementation of authentication procedures based on self-description features, which can be used as additional measures in the context of a "defense-in-depth" strategy.

Inhaltsverzeichnis

Abkürzungsverzeichnis

AC	Autonomic Computing
AGV	Automated Guided Vehicle
AI	Artificial Intelligence
API	Application Programming Interface (Programmierschnittstelle)
APT	Advanced Persistent Threat
BDE	Betriebsdatenerfassung
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certificate Authority (Zertifizierungsstelle)
CC	Secure Sockets Layer
CIA	Confidentiality, Integrity, Availability (Vertraulichkeit, Integrität, Verfügbarkeit)
CP	Cyber-physisch
CPDAL	Cyber-Physical Production System Self-Description-Based Data Access Layer
CPPS	Cyber-physisches Produktionssystem
CPS	Cyber-physisches System
DSM	Design Science Methodology
DSR	Design Science Research
DSRM	Design Science Research Methodology
EDA	Elektronischer Datenaustausch
EOL	End of Life (Lebensende)
ERP	Enterprise Resource Planning
ESB	Enterprise Service Bus

FAR	False Acceptance Rate
FRR	False Rejection Rate
FTA	Failure to Acquire (Fehlschlag der Erfassung)
FTE	Failure to Enroll (Fehlschlag der Erstanmeldung)
FTF	Fahrerloses Transportfahrzeug (vgl. AGV)
GPS	Global Positioning System
GSM	Global System for Mobile Communications
HMI	Human Machine Interface
HW	Hardware
ID	Identität (auch Identifikator)
IDM	Identitätsmanagement
IDMS	Identitätsmanagementsystem
IDP	Identitätsprovider
IDS	Intrusion Detection System (Angriffserkennungssystem)
IKT	Informations- und Kommunikationstechnik
IPC	Industrie PC
KI	Künstliche Intelligenz (vgl. AI)
MES	Manufacturing Execution System
MFA	Multi-Factor Authentication
ML	Maschinelles Lernen / Machine Learning
MQTT	Message Queuing Telemetry Transport
MSB	Manufacturing Service Bus
NIST	National Institute of Standards and Technology
OC	Organic Computing
OPC UA	OPC Unified Architecture

OS	Operating System (Betriebssystem)
OT	Operational Technology
PAD	Personal Authentication Device
PHY	Physical Layer
PIN	Persönliche Identifikationsnummer
PKI	Public-Key-Infrastruktur
PUF	Physical unclonable function
RA	Registration Authority
RAMI 4.0	Referenzarchitekturmodell Industrie 4.0
RBAC	Role Based Access Control
RFID	Radio-Frequency Identification
SCADA	Supervisory Control and Data Acquisition
SDN	Software-defined Networking
SDR	Software-defined Radio
SFA	Single-Factor Authentication
SID	Sichere Identität
SOA	Serviceorientierte Architektur
SPS	Speicherprogrammierbare Steuerung
SW	Software
UC	Ubiquitous Computing
UID	Eindeutige Identität (Unique Identity)
UML	Unified Modeling Language
URI	Uniform Resource Identifier
UUID	Universally Unique Identifier

Abbildungsverzeichnis

Abbildungen im Anhang

Tabellenverzeichnis

1 Einleitung

1.1 Ausgangssituation und Hintergrund

Durch die fortschreitende Vernetzung und Digitalisierung in allen Bereichen der Wirtschaft werden kontinuierlich neue Möglichkeiten zur Effizienzsteigerung geschaffen. So erlaubt beispielsweise der technische Fortschritt im Bereich der Informations- und Kommunikationstechnik (IKT) eine Datenintegration innerhalb der Wertschöpfungsnetze verschiedenster Industrien in Echtzeit. Diese Daten sind insbesondere dann wertvoll, wenn sie mit Kontext angereichert werden, sodass Informationen aus ihnen gewonnen werden können. Zudem können sie in einer anderen Form verarbeitet werden, um höherwertigen Nutzen oder Wissen aus ihnen zu gewinnen, wie es in Form einer sog. Wissenstreppe in Abbildung 1.1 anschaulich darstellt werden kann.

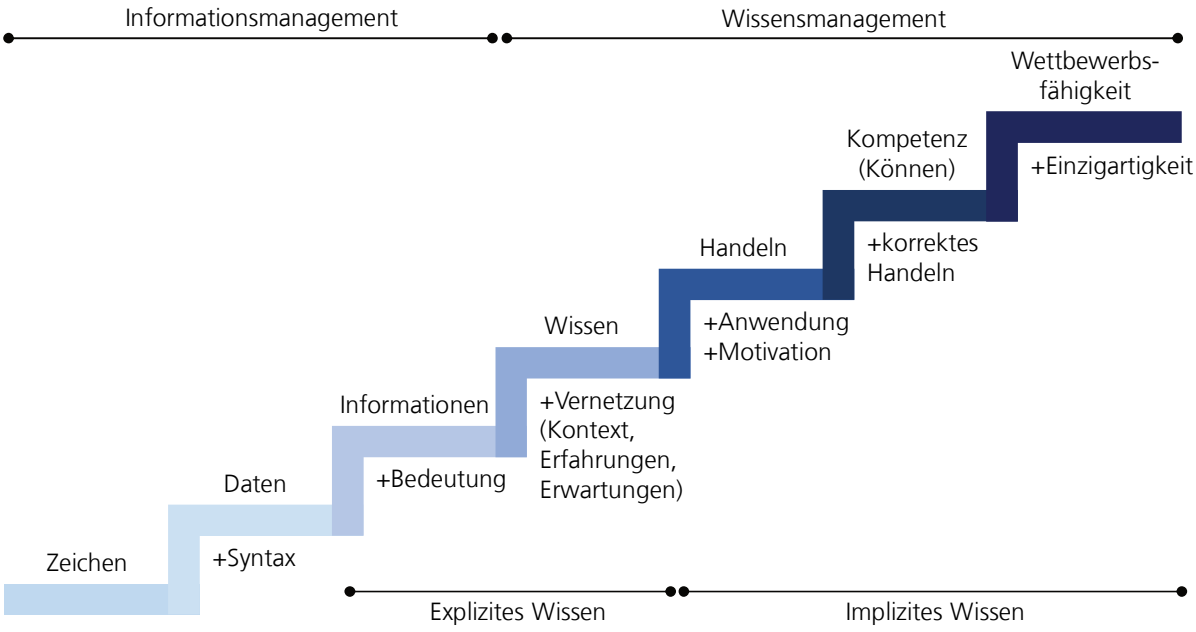


Abbildung 1.1 Die Wissenstreppe in Anlehnung an (North 2011, S. 36)

Die Vernetzung intelligenter Systeme hat einen zusätzlichen Einfluss auf die einzelnen Stufen der Wissenstreppe und ermöglicht so immer größere Sprünge zwischen den Stufen. Dies wiederum befähigt neue datengetriebene Ansätze und Anwendungen.

IT-geschichtlich betrachtet haben diese ihren Ursprung in Konzepten wie dem Ubiquitous Computing und dem Pervasive Computing, die sich damit befassen, wie sich die wachsende Allgegenwärtigkeit von Computern auswirkt. Bereits 1991 beschrieb Mark Weiser Ubiquitous Computing (UC) als einen allgemeinen Zustand bei dem Computer nahtlos in alltägliche Anwendungen integriert werden. Die Technik, die für UC benötigt wird, wurde von Weiser in drei Teilbereiche gegliedert: günstige, "low-power" Computer mit praktischem Display, ein Netzwerk, das sie verbindet und Softwaresysteme, die ubiquitäre (allgegenwärtige) Applikationen implementieren (Weiser 2002). Pervasive (durchdringendes) Computing (PC) wurde primär durch die von IBM gegen Ende der 90er-Jahre gegründete gleichnamige Sparte geprägt (IBM 2003). PC ist aus dem UC abgeleitet und beschreibt grundsätzlich ein verwandtes Konzept, allerdings nicht aus dem Blickwinkel eines idealisiert-akademischen Ansatzes, sondern im Kontext der kommerziellen Anwendung (Mattern 2004). Zudem wird der Umstand einbezogen, dass ein Computer im PC nicht mehr als solcher zu erkennen und für den Anwender praktisch unsichtbar ist. Miniaturisierung, Einbettung, Vernetzung, Allgegenwart und Kontextsensitivität werden in einer Studie zu den Auswirkungen des PC auf Gesundheit und Umwelt (Hilty et al. 2003) als seine kennzeichnenden Merkmale identifiziert. Ausgehend davon hat das BSI die Auswirkungen auf verschiedene Anwendungsfelder, Technologien und die volkswirtschaftliche Bedeutung des PC untersucht (BSI 2006). Während UC und PC hauptsächlich beschreiben, welche Formen Anwendungen annehmen und wie mit ihnen interagiert wird, gehen die Konzepte des Autonomic Computing (AC) und Organic Computing (OC) zusätzlich noch auf die Eigenschaften und das Verhalten informationstechnischer Systeme in Bezug auf Self-X-Fähigkeiten ein (Sterritt 2005; Wankhade et al. 2013). Die Differenzierung dieser beiden Ansätze findet ebenfalls in der Anwendung statt. AC ist mit dem architektonischen Design von Serversystemen befasst und zielt darauf ab die menschlichen Administratoren technischer Systeme durch Selbstorganisation selbiger zu entlasten (Kephart et al. 2003). Es wurde von IBM als Reaktion auf die ihrer Auffassung nach drohenden Krise der steigenden

Komplexität von Software in der IKT-Industrie formuliert, die man als Fortschrittshürde erkannt hatte (IBM 2001). OC wiederum bezieht sich auf die Interaktion des Menschen mit einer Menge von intelligenten Geräten. Diese stellen diesem Dienste bereit und passen sich an die augenblicklichen Bedarfe ihrer Umgebung zum Zeitpunkt der Ausführung an (Schmeck 2005).

Das "Wie" in Bezug auf die durch Vernetzung grundsätzlich ermöglichte lokale und globale Kommunikation wird in Bezug auf Geräte und Maschinen im betrieblichen und industriellen Einsatz als "Maschine zu Maschine"-Kommunikation (M2M) bezeichnet. Die erste Anwendung hatte Siemens mit dem Modul M1 Mitte der 90er-Jahre vorgestellt, das es Maschinen ermöglichte über das GSM-Netz Daten auszutauschen (Computerwoche 1996). M2M-Kommunikation betrachtet primär die direkte Kommunikation und den Datenaustausch zwischen zwei Maschinen, hat sich jedoch ebenfalls im Laufe der Zeit entsprechend funktional weiterentwickelt und beinhaltet neben drahtgebundener Technologien auch prinzipiell jede Art von drahtloser Kommunikation (Weyrich et al. 2014). Der Datentransfer zu einer übergeordneten Infrastruktur, die Anwendungen oder Diensten bereitstellt, wurde so Teil von M2M-Applikationen und darauf aufbauender Geschäftsmodelle (Viswanathan 2012).

Das Internet of Things (IoT – Internet der Dinge) ist in diesem Kontext die logische Konsequenz und die Ausweitung der M2M-Ansätze auf Alltags-Anwendungen (Minerva et al. 2015). Die Möglichkeit simple Geräte, beispielsweise Temperatursensoren, Kameras oder Bewegungsmelder, und nicht mehr nur komplexe Maschinen mit der Fähigkeit der Konnektivität auszustatten hat mit dem Aufkommen von Cloud-Technologien und den dadurch ermöglichten Plattformen ein massives Wachstum der Anzahl vernetzter Geräte ausgelöst. Schätzungen der Firma Cisco gingen ursprünglich von einer Anzahl von 50 Milliarden vernetzten intelligenten vernetzten Geräten bis zum Jahr 2020 aus (Evans 2011). Diese Zahl wurden mit im Jahr 2019 8 Milliarden geschätzten IoT-Geräten mittlerweile etwas relativiert. Jedoch ist der Trend einer fortschreitenden und durchgängigen Vernetzung konstant und wird voraussichtlich durch die globale Einführung von 5G-Infrastrukturen und den vermehrten Einsatz von Edge-Computing einen Schub erfahren

(Sachs et al. 2019). Die aktuelle Schätzung liegt bei ca. 15 Milliarden bei stetigem Wachstum, wie Abbildung 1.2 zu entnehmen ist.

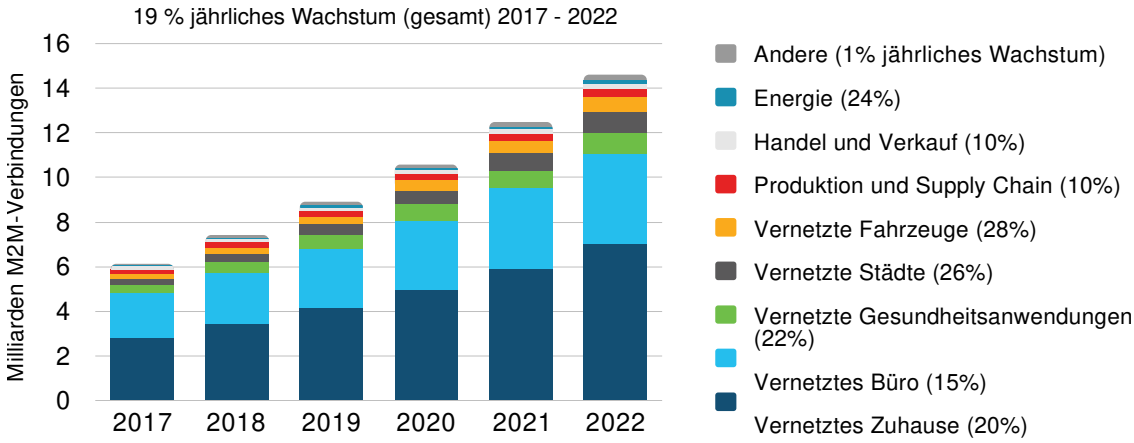


Abbildung 1.2 Prognose zur Anzahl vernetzter Geräte nach Anwendungsgebieten nach (Cisco 2019)

Die aktuelle Ausprägung in dieser fortlaufenden technischen Evolution sind cyber-physische Systeme (CPS) (Geisberger et al. 2012). Diese sind stark von den Prinzipien des Distributed Computing (DC) geprägt, was bedeutet, dass ihre Systemkomponenten in Form von Hard- und Softwarekomponenten örtlich verteilt sein können (Preden et al. 2009). Die Bundesregierung hat im Jahr 2011 das Zukunftsprojekt "Industrie 4.0" ins Leben gerufen, mit dem Ziel die Digitalisierung der Deutschen Industrie voranzutreiben (BMBF 2012). Im Rahmen dieser und folgender Aktivitäten wurden unter anderem CPS als die Grundlage für "Industrie 4.0" definiert und der Begriff als vierte industrielle Revolution international geprägt (Kagermann et al. 2013). CPS vereinen die Ansätze des UC/PC, OC/AC und IoT. In Verbindung mit Methoden des maschinellen Lernens (ML) als Teilgebiet Künstlicher Intelligenz (KI) können CPS zusätzlich befähigt werden und so Ansätze des Cognitive Computing (CC) (Weber 2015) adaptieren, um ihre Self-X-Fähigkeiten von einer Selbstbeschreibung, über Selbstkonfiguration bis hin zu Selbstoptimierung zu steigern (Weyrich et al. 2017, S. 185). Auf CPS und Self-X wird im Detail in Abschnitt 2.2 eingegangen. Einer Bitkom-Studie aus dem Jahr 2018 zufolge war im Jahr 2018 bereits jede

vierte Maschine vernetzt und jedes zweite Unternehmen in Deutschland nutzte Anwendungen für Industrie 4.0 (Bitkom et al. 2018). Die Möglichkeit der Vernetzung birgt neben den genannten Vorteilen allerdings auch Herausforderungen. Insbesondere IT-Sicherheit und Cyber-Sicherheit stellen Unternehmen vor die Herausforderung ihre Netzwerke, Computersysteme, oder Anlagen in Form von cyber-physischen Systemen vor unbefugten Zugriffen und Angriffen zu schützen. Dies äußert sich beispielsweise im Diebstahl privater oder sensitiver betrieblicher Daten, geistigen Eigentums oder sogar Beschädigung von Hard- und Software in Form angebotener Dienste und Funktionen. Ein steigendes Bewusstsein für diese Bedrohungen zeigt, dass im Jahr 2017 6 von 10 Unternehmen angaben sich von IT-Angriffen bedroht zu fühlen (Bitkom et al. 2017). 2018 waren es schon 8 von 10. Im Mai 2017 wurden global Unternehmen Opfer von Wannacry, einer Ransomware in Form eines Cryptowurms, der darauf abzielt betriebsrelevante Daten zu verschlüsseln (BSI 2017a, S. 26). Diese Verschlüsselung kann gegen ein Lösegeld wieder aufgehoben werden, falls die Täter wirtschaftliche Motive verfolgen. Allerdings gibt es auch Hinweise auf Sabotage, ideologisch motivierte Angriffe und sogar Cyber-Terrorismus (Bitkom 2018, S. 14; BSI 2018). Angriffe dieser Art sind hauptsächlich deswegen möglich, da viele der eingesetzten Systeme über veraltete Software verfügen, die entsprechende Schwachstellen aufweist (Ackerman 2017, S. 142). Die steigende Anzahl an vernetzten Geräten und menschliches Fehlverhalten oder organisatorische Mängel, wie das fehlende Wissen über die im Feld befindlichen Geräte, haben zudem die Situation verschärft (BSI 2019, S. 3). IT-Systeme im industriellen Umfeld waren in der Vergangenheit meist primär durch den Umstand geschützt, dass sie keinen Zugang zu externen bzw. globalen Netzwerk wie dem Internet hatten ((VDMA et al. 2016, S. 28)). Dieser Umstand wird als das "Air Gap" bezeichnet (Byres 2013). Somit konnten keine Angriffspunkte offengelegt werden, weshalb der erste Kurzbericht zur Industrial Control System Security des BSI aus dem Jahr 2012 „Internet-verbundene Steuerungskomponenten" noch nicht als Bedrohung listet, da Zwischenfälle hier noch eine Seltenheit waren und der Fokus auf der unverschlüsselten Kommunikation zwischen diesen lag (BSI 2012a). Aktuelle Berichte gehen jedoch explizit auf unmittelbar mit dem Internet verbundene Infrastruktur-Komponenten und mittelbar durch Cyber-Attacken angreifbare ein (BSI 2019).

1.2 Motivation und Problemstellung

Informationstechnische Systeme verfügen zum Zweck des Informationsaustauschs über eine Kommunikationsschnittstelle, sei es, um Daten bereitzustellen oder Fernzugriffe zu gewähren. Die Möglichkeit der Bereitstellung dieser Daten ist die Grundlage und der Treiber zahlreicher neuer digitaler Geschäftsmodelle, was die volkswirtschaftliche Bedeutung der Technologie und der darauf basierten Anwendungen hervorhebt (Dorst et al. 2019, S. 9). Insbesondere CPS sind definitionsgemäß und aufgrund ihrer intrinsischen Eigenschaften gefährdet, da ihre Systemkomponenten grundsätzlich verteilt sein können. Beliebige ihrer Softwarekomponenten können in Form eines Dienstes auf einer Cloud-Plattform oder sonstigen heterogenen Umgebungen ausgelagert sein. Dies stellt besondere Anforderungen an Cyber-Sicherheit und IT-Sicherheit, die mittels technischer und ggf. auch organisatorischer Maßnahmen sicherstellen, dass kein unbefugter Zugriff auf diese Systeme oder ihre Daten stattfinden kann.

IT-Sicherheit verfolgt ursprünglich die drei IT-Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit, wobei die Reihenfolge der Aufzählung auch die Priorisierung der Schutzziele darstellt (Dhillon 1997, S. 51). Dieses Prinzip ist auch als CIA-Triade (Confidentiality, Integrity, Availability) bekannt (Bedner et al. 2010) und wird im Detail in Anhang 3 diskutiert.

In industriellen Anwendungen liegt der Schwerpunkt dieser Schutzziele jedoch meist primär auf der Verfügbarkeit, ggf. auch auf der Integrität, da die Verfügbarkeit der Anlagen für die korrekte Ausführung ihrer technischen Funktion essenziell ist und Maschinendaten im Normalfall nicht personenbezogen sind (Norm IEC/TS 62443-1-1).

Unternehmen sind sich dieser Bedrohungen bewusst. Die IT-Sicherheit ist jedoch meist mit zusätzlichen Aufwänden verbunden, die Kleine und Mittelständische Unternehmen (KMU) im Besonderen vor eine oft schwere oder nicht zu bewältigende Herausforderung stellen, sei es aus finanziellen Gründen oder wegen Fachkräftemangel. Jede zusätzliche Maßnahme erhöht zwar die Sicherheit, löst aber einen Zielkonflikt zwischen Bedienbarkeit und Funktionalität eines Systems aus (Schumacher 2006, S. 32). Dieser kann in Anlehnung

an die CIA-Triade als Infosec-Triade (information security) wie in Abbildung 1.3 dargestellt werden kann (Waite 2010; Hilty et al. 2003, S. 255; Vacca 2013, S. 78).

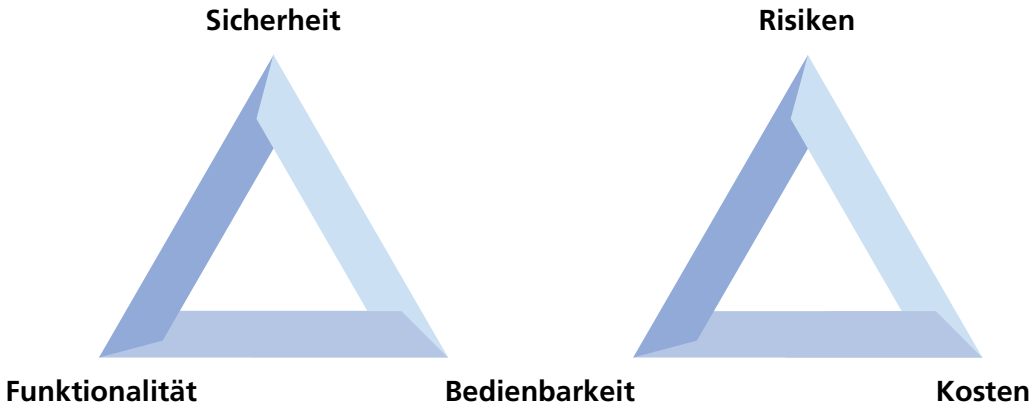


Abbildung 1.3 Infosec-Triaden in Anlehnung an (Waite 2010; Vacca 2013, S. 78)

Diese und weitere zahlreiche Komplexitätsfaktoren haben in verschiedenen Unternehmensbereichen Einfluss auf die innere Komplexität des Unternehmens, die sich wie in Abbildung 1.4 erkennbar ist aus verschiedenen Faktoren zusammensetzt. Die innere Komplexität in einem Unternehmen ist genau dann ideal, wenn sie der äußeren Komplexität des Marktes entspricht, welche wiederum durch zahlreiche Faktoren beeinflusst wird (Bauernhansl 2014). Der Drang zur Vernetzung und Digitalisierung ist somit nicht Selbstzweck, sondern die Reaktion auf die äußeren Komplexitätsfaktoren.

CPS werden immer leistungsfähiger, sowohl in Bezug auf die in ihnen eingesetzten Recheneinheiten als auch auf die von ihnen bereitgestellte fachliche Funktionalität. Damit geht auch eine Steigerung der Komplexität der Systeme einher. Hier ist die Herausforderung diese Komplexität dem Endanwender gegenüber möglichst zu kapseln, so dass sie für die Verwendung in einer produzierenden Umgebung keine oder zumindest kaum Einfluss hat. Dies gilt insbesondere für Funktionalitäten, die nicht direkt fachlich mit den Anforderungen des Anwenders in der Produktion zusammenhängen.

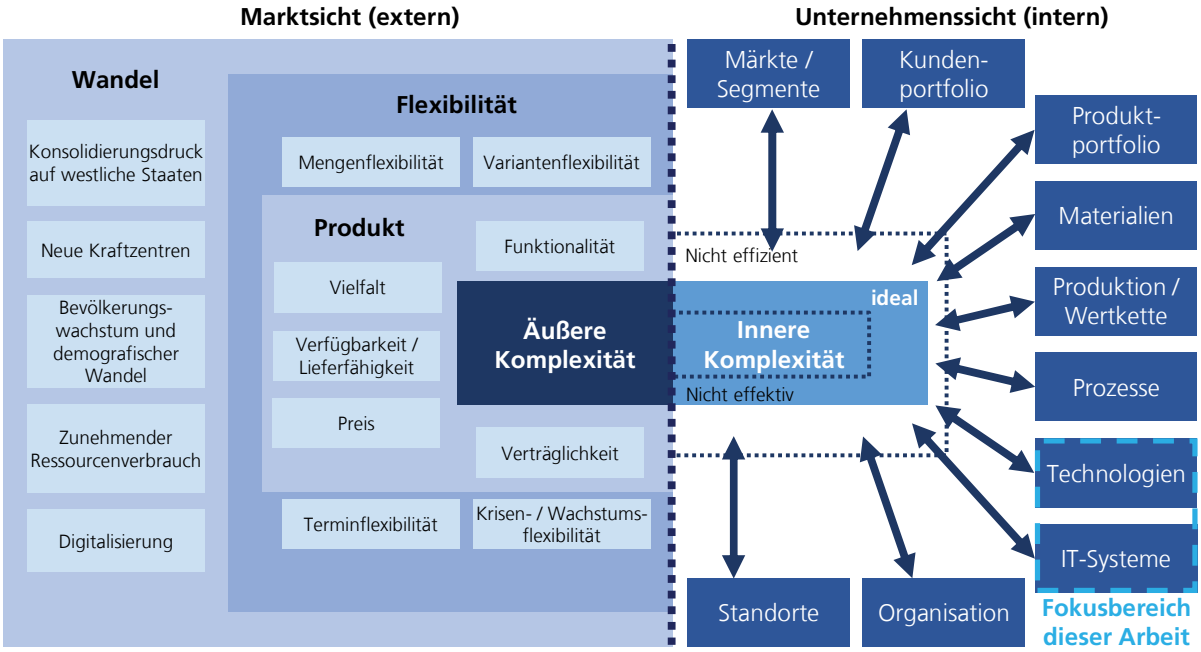


Abbildung 1.4 Übersicht verschiedener Komplexitätsfaktoren nach (Bauernhansl 2014)

Dies ist beispielsweise die Auswertung von Daten, die nicht unmittelbar prozessrelevant sind oder im Zuständigkeitsbereich des Anwenders liegen oder Funktionalitäten, die Maßnahmen zum Zweck der IT-Sicherheit betreffen. Diese Maßnahmen können vielfältig technisch oder organisatorisch umgesetzt werden und stehen einer Vielzahl von Bedrohungen entgegen. Das Themenfeld der IT-Sicherheit definiert hierzu eine Reihe von Angriffsvektoren, von denen insbesondere das Identity Spoofing (BSI 2011, S. 85), also das Vortäuschen einer Identität in Bezug auf CPS und im Kontext der IoT-Sicherheit eine wichtige Frage aufwirft: Wie kann sichergestellt werden, dass ein CPS oder eine Komponente eines CPS tatsächlich die ist, die sie vorgibt zu sein. Insbesondere wenn Komponenten nicht nur lokal, sondern auch global verteilt sein können und beispielsweise der physikalische Zugriff auf Komponenten nicht ausgeschlossen werden kann, ist eine technische Kompromittierung der Komponente möglich, die ihr definiertes und erwartetes Verhalten verändert, auch unbemerkt (Ray et al. 2017).

Ein Ergebnispapier der Plattform Industrie 4.0 aus dem Jahr 2016 befasst sich explizit mit der Frage nach sicheren Identitäten und definiert bereits die grundsätzlichen Anforderungen an sichere Identitäten. Die Implementierung sicherer Identitäten ist demnach technisch umsetzbar, jedoch sind diese Lösungen nachträglich in Form von Erweiterungen durch spezielle Security-Produkte wie z.B. Dongle, HW- Token oder SW-Token realisiert und nicht integraler Bestandteil des Systems (Jänicke et al. 2016). Eine mittels Informationen geschaffene Identität im Internet der Dinge wird bereits im Ansatz diskutiert, wirft jedoch im Vergleich zu einer Identität menschlicher Nutzer ungelöste organisatorische und technische Herausforderungen auf (Lam et al. 2016).

1.3 Zielsetzung und Forschungsfragen

Ziel dieser Arbeit ist zu untersuchen, ob eine eindeutige und sichere Identität mittels der Self-X-Fähigkeiten cyber-physischer Systeme geschaffen werden kann. Basierend auf der Selbstbeschreibung sollen Selbstbeschreibungsmerkmale, also charakteristische Merkmale eines CPS bzw. einzelner Bestandteile erfasst werden. Zudem soll betrachtet werden, wie diese sichere Identität durch ein Authentifizierungsverfahren geprüft werden kann, welches die Self-X-Eigenschaften von CPS nutzt, um nach einer Identifikation eine Authentifizierung zum Zweck einer Autorisierung durchzuführen.

Ein solches Authentifizierungsverfahren hat dabei nicht den Anspruch existierende und bewährte Sicherheitsmechanismen unmittelbar zu ersetzen, sondern soll nach dem Defense-in-Depth-Prinzip (vgl. Anhang 3.7) ergänzend eingesetzt werden, um die Sicherheit des Einsatzes vernetzter und verteilter Systeme in Form von cyber-physischen Systemen zu erhöhen.

Die primäre Forschungsfrage für die vorliegende Dissertation lautet somit wie folgt:

F1 - Wie können die Selbstbeschreibungsmerkmale eines CPS genutzt werden, um eine sichere Identität zur Identifikation und Authentifizierung eines CPPS zu schaffen?

Zusätzlich ergeben sich sekundäre Forschungsfragen, die die zusätzliche Problemstellung ergeben:

F1.1 - Biometrische Verfahren nutzen eindeutige Muster in physischen Merkmalen einer Person wie beispielsweise einen Fingerabdruck, um eine eindeutige Identifikation dieser Person durchzuführen. Maschinen besitzen per se keinen Fingerabdruck in diesem Sinne, jedoch soll in dieser Arbeit der Frage nachgegangen werden, ob und wie sich ein "künstlicher Fingerabdruck" mit Hilfe von Selbstbeschreibungsmerkmalen konstruieren lässt.

F1.2 - Welche Selbstbeschreibungsmerkmale eignen sich für die Konstruktion eines "künstlichen Fingerabdrucks" und somit einer sicheren Identität?

F1.3 - Können Authentifizierungsverfahren auf Grundlage der Selbstbeschreibungsmerkmale unter Nutzung der Self-X-Eigenschaften eines CPS geschaffen werden, ohne dass die Anwendbarkeit und Funktionalität der Anwendung beeinträchtigt wird?

1.4 Methodik und Gliederung der Arbeit

In den vorherigen Abschnitten wurden die Ausgangssituation, Problemstellung und Zielsetzung erörtert. Die sich daraus ergebende Forschungsfrage soll im Zuge dieser Arbeit methodisch beantwortet werden. Die vorliegende Arbeit ist aufgrund ihres Praxisbezugs und ihres Anspruchs Artefakte in Form eines Frameworks und einer prototypischen Umsetzung eines Authentifizierungsverfahrens auf Basis von Selbstbeschreibungsmerkmalen cyber-physischer Produktionssysteme zu schaffen den angewandten Wissenschaften bzw. präziser den Technik- und Ingenieurwissenschaften zuzuordnen. Anhang 1.1 beschreibt die Begründung der wissenschaftstheoretischen Positionierung im Detail. Die Auswahl der Vorgehensweise folgt den Prinzipien der Design Science (siehe Anhang 1.2), da diese sich mit der Erforschung und Entwicklung praxisorientierter Lösungen in Form von Artefakten befasst. Abbildung 1.5 stellt die Zusammenhänge der methodischen Design Science Research-Ansätze dar, an denen sich der Autor dieser Arbeit orientiert. Die Artefakte, die untersucht werden, sind so konzipiert, dass sie mit einem Problemkontext interagieren, um etwas in diesem Kontext zu verbessern. Sie können hierbei unterschiedlich ausgeprägt

sein, beispielsweise als Prozesse, Methodiken oder reine Software-Artefakte. Die Aspekte dieser unterschiedlichen Ausprägungen, auf denen der Fokus dieser Arbeit liegt, sind in Abbildung 1.5 rot markiert.

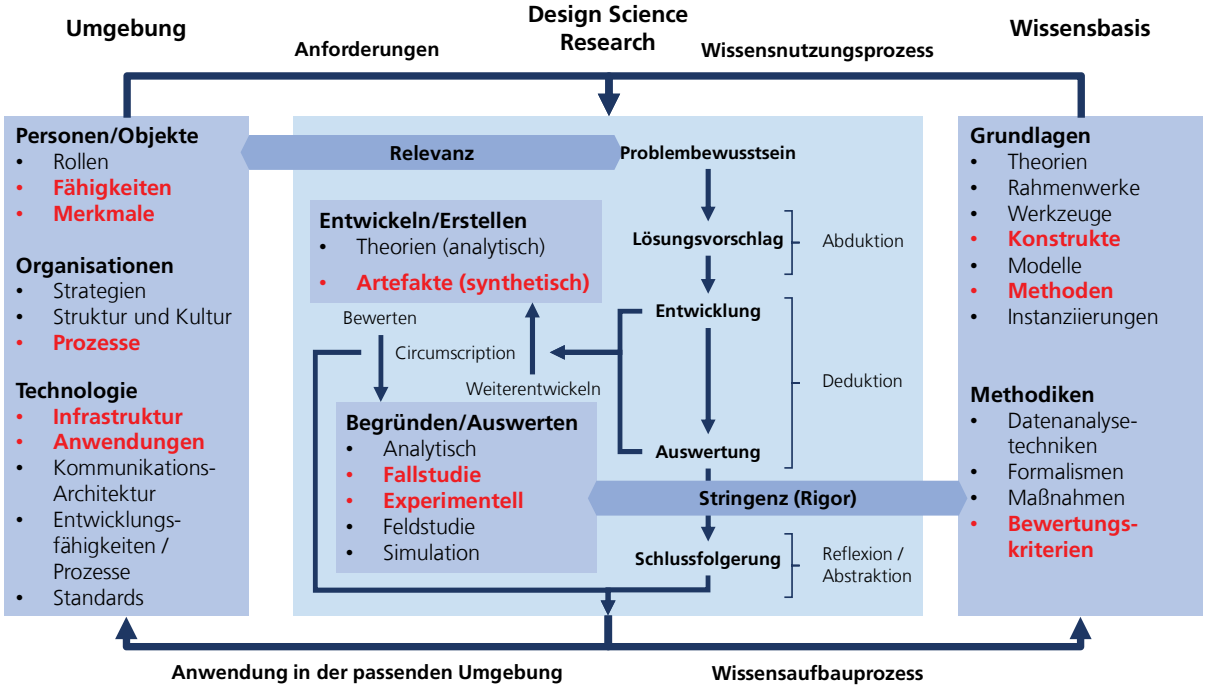


Abbildung 1.5 Vorgehen und Schwerpunkte nach Design Science Research in Anlehnung an (Hevner et al. 2004, S. 80; Owen 1998; Vaishnavi et al. 2015, S. 17)

Die Umgebung hat einen Fokus auf die Fähigkeiten und Merkmale von CPS (Objekten) und wie diese mittels der zum Einsatz kommenden Infrastruktur und Anwendungen im Rahmen eines Authentifizierungsprozesses genutzt werden können. Hierzu werden Artefakte entwickelt, die mittels Fallstudien und Experimenten ausgewertet werden. Der Beitrag zur Wissensbasis liegt hauptsächlich auf Konstrukten und Methoden zur Erstellung einer Authentifizierung auf Basis von Selbstbeschreibungsmerkmalen und einem methodischen Vorgehen zu Bestimmung der Bewertungskriterien.

Die Gliederung der Arbeit ergibt sich aus der Vorgehensweise zur Beantwortung der Forschungsfrage, die in Abbildung 1.6 dargestellt ist. Die Phasen basieren auf dem Design Research Methodology (DRM) Framework nach (Blessing et al. 2009, S. 15).

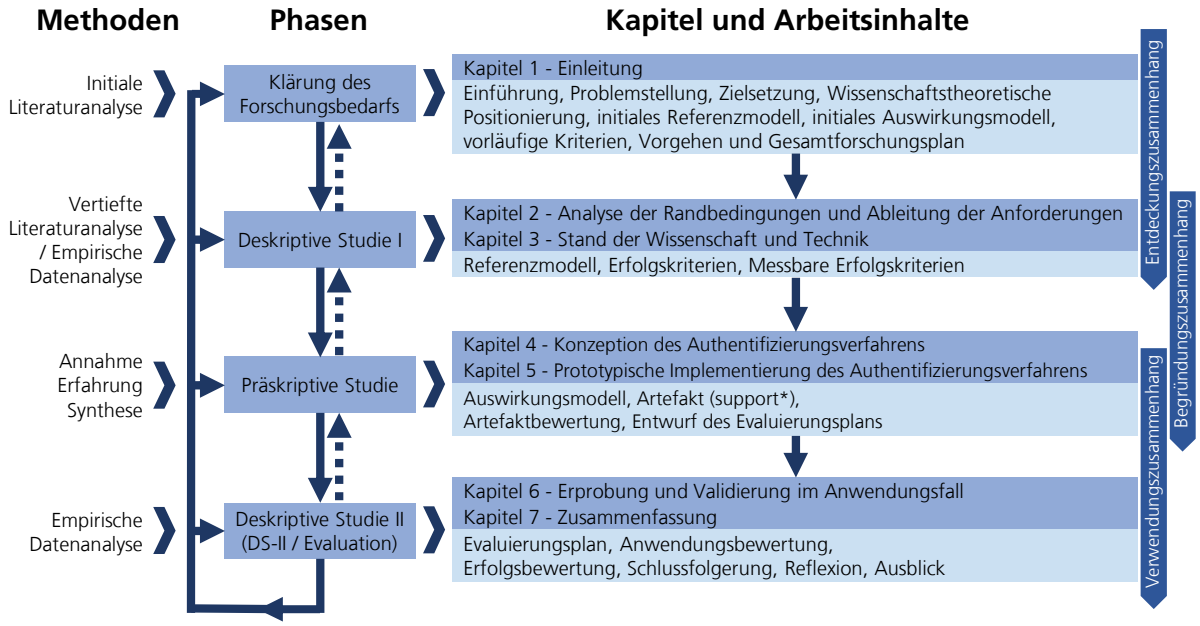


Abbildung 1.6 Gliederung der Arbeit

- Kapitel 1 gibt einen kurzen Abriss zum Hintergrund, zur Motivation und zur Problemstellung der vorliegenden Ausarbeitung. Zudem wird die gewählte Wissenschaftsmethodik erläutert, in deren Rahmen der Autor das Vorgehen zur Beantwortung der Forschungsfrage ausgestaltet.
- Kapitel 2 beschreibt den Rahmen und Kontext einer vernetzten und durch digitale Transformation geprägten Produktion und die damit verbundenen Herausforderungen, insbesondere in Hinblick auf die vorliegende Arbeit.
- Kapitel 3 diskutiert den Stand der Technik zu den für die Arbeit relevanten Schwerpunktthemen zur IT-Sicherheit, Authentifizierung und Verfahren zur Merkmalserfassung und -prüfung.

- Kapitel 4 dokumentiert die Konzeption und Herleitung des für die Beantwortung der Forschungsfrage entwickelten Verfahrens. Hierzu wird in einem ersten Schritt das Vorgehen zur Bestimmung von geeigneten Selbstbeschreibungsmerkmalen aus Datenquellen in der Produktion erläutert. Aus diesen werden geeignete Authentifizierungsfaktoren hergeleitet, die für das im Folgenden skizzierte Authentifizierungsverfahren eingesetzt werden können.
- Kapitel 5 stellt dar, wie ein Authentifizierungsverfahren auf Grundlage von Selbstbeschreibungsmerkmalen konzipiert und prototypisch implementiert werden kann.
- Kapitel 6 beschreibt den Versuchsaufbau, der zur Erprobung des entwickelten Ansatzes mittels der prototypischen Implementierung dient. Zudem werden die Ergebnisse und ihr Beitrag zur Beantwortung der Forschungsfrage diskutiert.
- Kapitel 7 fasst die Ergebnisse und Erkenntnisse der Arbeit zusammen, reflektiert diese und gibt einen Ausblick auf zukünftige Anwendungspotenziale und ggf. neu erschlossene Forschungsfragen.

2 Analyse der Randbedingungen und Ableitung der Anforderungen

Dieses Kapitel behandelt die relevanten Konzepte inklusive Terminologie, um ein Begriffssystem zu schaffen, das das weitere Verständnis für den Kontext und das Einsatzfeld unterstützt. Hierzu werden aufgrund des interdisziplinären Ansatzes dieser Arbeit relevante Begriffe aus dem Umfeld der Produktion (Produktionstechnik) und IKT (Softwaretechnik, IT-Sicherheit und Kommunikationstechnik) zusammengetragen und auf Grundlage der existierenden Literatur in einem für diese Arbeit adäquaten Kontext definiert und in Beziehung gesetzt.

2.1 Produktion im Wandel

Gutenberg bezeichnet Produktion als Prozess betrieblicher Leistungserstellung. Dabei sieht er den Sinn aller betrieblichen Betätigung darin Güter materieller Art (Sachgüter) zu fertigen oder Güter immaterieller Art (Dienste und Dienstleistungen) bereitzustellen (Gutenberg 1951, S. 1). Aus betriebswirtschaftlicher Sicht wird versucht diese betrieblichen Betätigungen bei möglichst geringen Kosten und maximaler Arbeitsproduktivität durchzuführen. Zur Gewinnmaximierung werden hierzu Maßnahmen getroffen, die im ökonomischen Kontext als Rationalisierung bezeichnet werden. Taylor prägte hierzu ein Prinzip zur Erschließung von Rationalisierungspotenzialen und Steigerung der Produktionseffizienz durch Beobachtungsstudien der Arbeitsabläufe und Prozesse. Die davon abgeleiteten optimierten Handlungsanweisungen sind stark auf Arbeitsteilung ausgerichtet, sodass beispielsweise Planung, Bereitstellung von Werkzeugen und Ausführung durch dedizierte individuell befähigte Arbeiter ausgeführt werden (Taylor 1998). Aufgrund seines Ansatzes unter anderem von einzelnen Beobachtungen auf allgemeine Gebote zu schließen wurde

der sog. Taylorismus jedoch zunehmend kritisch betrachtet. Die Prinzipien der Arbeitsteilung haben jedoch heute noch Bestand. Westkämper und Zahn beschreiben in diesem Zusammenhang den "neuen Taylorismus", der in der Moderne Taylors grundlegende Ansätze mit einem systemtechnischen Modell kombiniert. Automatisierung, vernetzte Information auf detailliertester Ebene, integrierte Planungssysteme und ein vergleichbar hohes Qualifikationsniveau der Mitarbeiter bestimmen in einem vernetzten System von Maschinen die Leistung des Produktionssystems (Westkämper 2009, S. 29 ff). Nagel et al. haben schon zur Jahrtausendwende angedeutet, dass der Fortschritt in der IKT bzw. die dadurch befähigten Prozesse einen revolutionären Charakter haben und einen Paradigmenwechsel wie Kuhn ihn beschreibt auslösen werden (Nagel et al. 2013, S. 7). Sie postulierten, dass die klassische, massenhafte Produktion von Standardgütern mehr und mehr an Bedeutung verlieren wird und die Fabrik der Zukunft auf flexiblen, agilen und interagierenden Einheiten basieren wird, die unter Nutzung moderner IKT kundenindividuelle Produkte in hoher Qualität und zu niedrigen Kosten herstellen (Nagel et al. 2013, S. 4).

2.1.1 Produktionssystem und Teilsysteme

Produktionsprozesse, ihre Organisation und die dazu notwendigen Betriebsmittel unterliegen einem vorgegebenen Organisationsprinzip. Diese systematische Arbeitsordnung unter Einbeziehung der für die Produktion von Gütern notwendigen Hand- und Maschinenarbeit und der dafür eingesetzten Werkzeuge und Maschinen wird als (ganzheitliches) Produktionssystem bezeichnet (Spur 1997, S. 18; Norm VDI 2870 Blatt 1). Das komplexe und abgestimmte Zusammenspiel dieser Komponenten ist es, das einen systemischen Charakter erzeugt.

Der allgemeine Begriff des Systems wird in der Norm ISO/IEC 10746-2:2009 definiert als etwas, das als Ganzes oder in Teilen von Interesse ist. Daher kann ein System als Einheit oder Entität (vgl. Abschnitt 2.3) bezeichnet werden. Eine Komponente eines Systems kann selbst ein System sein. In diesem Fall kann sie als Subsystem bzw. Teilsystem bezeichnet werden (Norm ISO/IEC 10746-2).

Technische Systeme bezeichnen Produktionssysteme, mit denen der Mensch interagiert, jedoch selbst nicht Bestandteil des Systems ist. Maschinen, Anlagen, Soft- und Hardware sind Teil technischer Systeme und diese lassen sich nach allgemeiner Definition beliebig in Sub- oder Teilsysteme unterteilen. Diese Elemente stehen in Wechselwirkung zueinander. Die Umwandlung des Input in den Output erfolgt über die Funktion des Systems (Winzer 2013, S. 65).

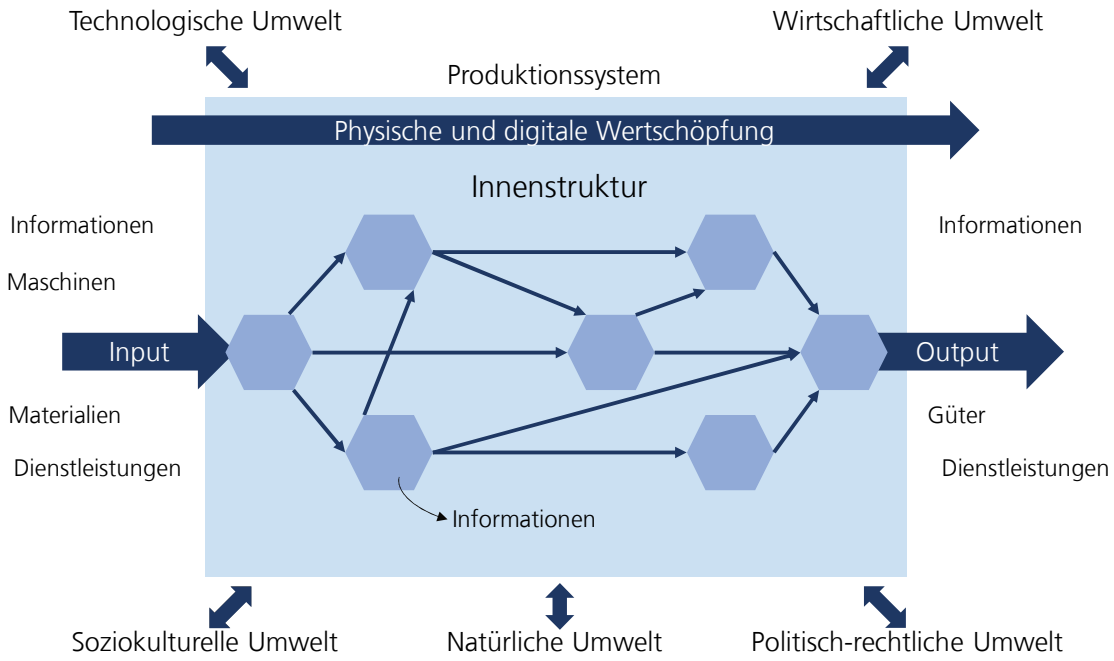


Abbildung 2.1 Das Produktionssystem in Anlehnung an (Günther et al. 2011, S. 2)

Ein Arbeitssystem wiederum umfasst das Zusammenwirken einer einzelnen oder mehrerer Bedienpersonen mit den Arbeitsmitteln, um die Funktion des Systems innerhalb des Arbeitsbereiches und der Arbeitsumgebung unter den durch die Arbeitsaufgaben vorgegebenen Bedingungen zu erfüllen (Norm DIN EN ISO 6385). Bezieht man diese Wechselbeziehungen zwischen Menschen und Maschinen oder Anlagen in ein technisches System ein, spricht man von einem soziotechnischen System (Winzer 2013, S. 66).

Die Vorliegende Arbeit widmet sich in diesem Kontext vornehmlich technischen Produktionssystemen, wie z. B. einer Fabrik, Produktionslinie oder Anlage, die als Sub- bzw. Teilsysteme in der Innenstruktur eines Produktionssystems eingegliedert sind (Dyckhoff 2003, S. 4). Diese Teilsysteme – und ihre Teilsysteme – sind durch Informations- und Materialflüsse miteinander verknüpft, die je nach Art der Beziehung zueinander die Funktion des Teilsystems und seiner Prozesse prägen (Westkämper 2013, S. 134). Hier stellt sich die Frage, welche Informationsflüsse bzw. die daraus extrahierbaren Informationen zur Beantwortung der Forschungsfrage dieser Arbeit verwendet werden können, insbesondere in Bezug auf Produktionsprozesse.

Nach Grote stellt ein Produktionsprozess einen Verbund aus Materialverarbeitungs-prozess, Datenverarbeitungsprozess und Wertschöpfungsprozess dar (vgl. Abbildung 2.2). Diese sind jeweils durch die Teilsysteme der Produktionstechnik, Produktionsinformatik und Produktionsorganisation ausgeprägt (Grote et al. 2014).

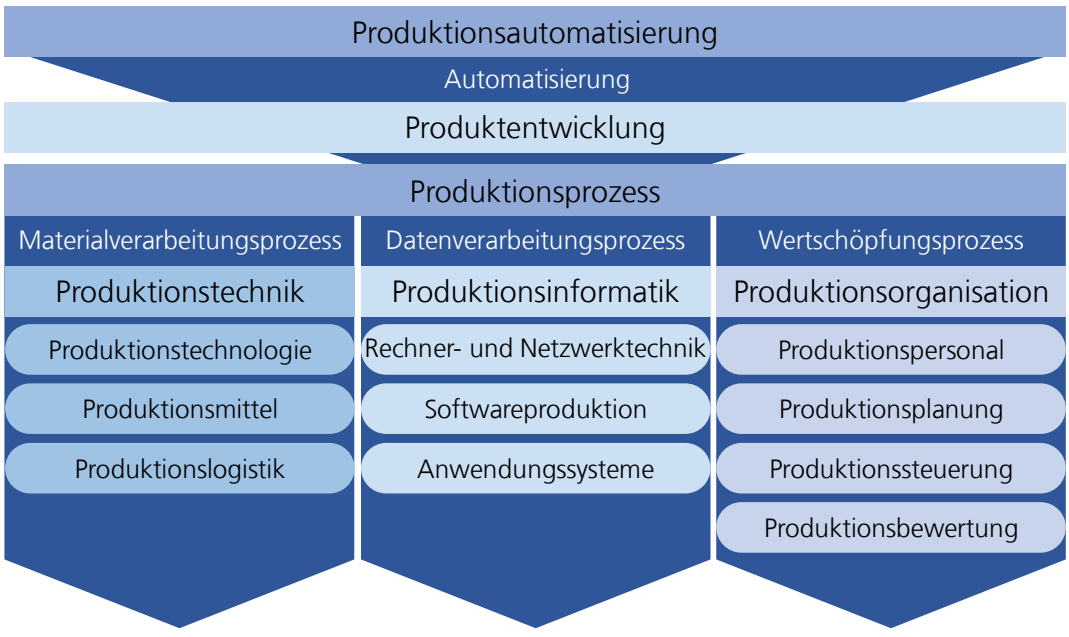


Abbildung 2.2 Produktionsprozess und Produktionsautomatisierung in Anlehnung an (Grote et al. 2014, S. 102)

Der Fokus liegt im Rahmen dieser Arbeit insbesondere auf den Produktionsmitteln, die zur Produktionstechnik gehören, der Rechner- und Netzwerktechnik und den Anwendungssystemen der Produktionsinformatik, die im Zuge der Produktionsautomatisierung eingesetzt werden. Zudem wird untersucht, welche Teilsysteme der Produktionsorganisation zur zusätzlichen Datenakquise und Informationsgewinn, beispielsweise für Meta- oder Kontextinformationen, zur Ableitung zusätzlicher Merkmale herangezogen werden können.

2.1.2 IT-Systeme in der Produktion

Die der Produktionsinformatik zugehörigen Anwendungssysteme und weitere Komponenten üben Funktionen aus, die ihren Prozessen im Produktionssystem zugehören und entsprechen (vgl. Abschnitt 2.1.1). Da diese Prozesse auf unterschiedlichen Ebenen des Unternehmens innerhalb des Produktionssystems stattfinden, können sie hierarchisch abgebildet werden (Westkämper 2013, S. 135). In Hinblick auf die Fertigungsprozesse in der Produktion werden die Techniken und Systeme der Leittechnik der Automatisierung nach dem im ISA-88 bzw. ANSI/ISA-95 Standard definierten physikalischen Modell in der Automatisierungspyramide dargestellt (Heinrich et al. 2015, S. 4).

Diese hat seit der Einführung der rechnergestützten Produktion (auch rechnerintegrierte Fertigung, von engl. computer-integrated manufacturing (CIM)) in den 80er-Jahren immer noch Bestand (Gevatter et al. 2006, S. 475), unterliegt aber auch einem Wandel, der in Anhang 1 diskutiert wird. Eine Darstellung der verschiedenen Ebenen der Automatisierungspyramide mit ihren Komponenten und Systemen ist in Abbildung 2.3 dargestellt.

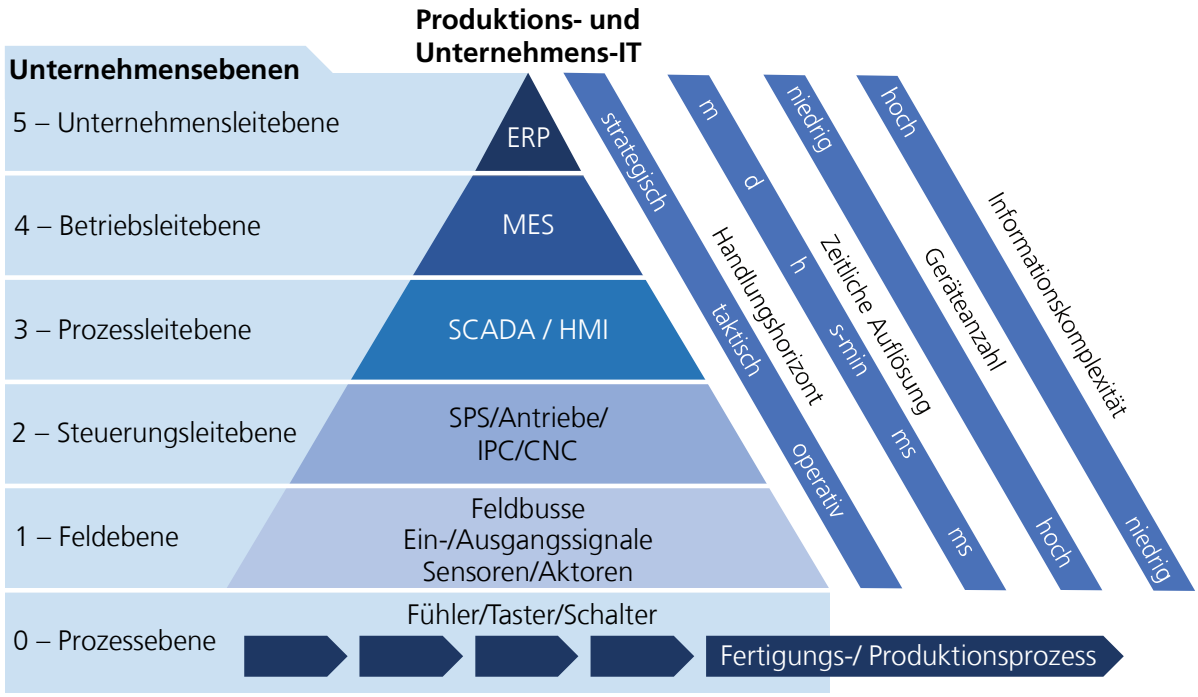


Abbildung 2.3 Die Automatisierungspyramide in Anlehnung an (Siepmann et al. 2016, S. 49)

Die Bezeichnung der Ebenen kann nach Branchenfokus variieren (Gebhardt 2019, S. 18). Die Bedeutung und Aufgabe der einzelnen Ebenen sind im Folgenden von der untersten bis zur obersten gemäß der Darstellung in Abbildung 2.3 erläutert:

- **0 – Prozessebene:** In der untersten Ebene findet der Fertigungs- und Produktionsprozess statt.
- **1 – Feldebene:** Die Feldebene umfasst den Hallenboden (engl. Shopfloor). Hier befinden sich Sensoren, Aktoren, Schalter und Regler, die als Feldgeräte im Produktionsbereich bzw. Produktionsstätte unmittelbar in Kontakt zum Produktionsprozess stehen. Die Ein- und Ausgangssignale der Feldgeräte dienen als Quelle für sämtliche relevanten Daten und Informationen aus den Produktionsprozessen.
- **2 – Steuerungsebene:** Die (Sensor-) Daten aus der Feldebene dienen den speicherprogrammierbaren Steuerungen (SPS) der Steuerungsebene als Eingangssignale. Diese verarbeiten diese und geben sie als Ergebnisdaten in Form von elektrischen Ausgangssignalen an die Feldebene zurück. Aktoren führen gemäß diesen

Signalen mechanische Bewegungen aus, die aufgrund der geforderten Präzision in deterministischer Echtzeit angewiesen und ausgeführt werden müssen. Hierdurch wird eine dezentral gesteuerte Maschinen- und Anlagensteuerung ermöglicht.

- **3 – (Prozess-) Leitebene:** Diese Ebene stellt in Summe eine Mensch-Maschinen-Schnittstellen bereit, die der Beobachtung und Bedienung der unterliegenden Prozesse dient. Die von der Feld- und Steuerungsebene erfassten und verarbeiteten Prozess- und Zustandsdaten werden an die Prozessleitsysteme, Human Machine Interfaces (HMI, Mensch-Maschine-Schnittstellen) und Supervisory Control and Data Acquisition (SCADA-Systeme, Überwachung, Steuerung und Datenerfassung) durchgereicht. Die Steuerungsdaten und Warnmeldungen werden von diesen zum Hauptzweck der Visualisierung aufbereitet und für Anwender nachvollziehbar dargestellt.
- **4 – Betriebsebene:** Die Steuerung der Produktion ist der zentrale Aufgabenbereich der Betriebsebene. Hierfür werden mittels eines Manufacturing Execution Systems (MES) Daten aus den darunter und darüber liegenden Ebenen in Form von Betriebs-, Maschinen- und Personaldaten erfasst und verarbeitet. Das MES wird hierbei zur Produktionsfeinplanung und -datenerfassung eingesetzt und gibt Daten zum Zweck der taktisch-strategischen Planung an die darüber liegende Ebene weiter.
- **5 – Unternehmensebene:** Die Unternehmensebene widmet sich der Produktionsgrobplanung und Bestellabwicklung der Aufträge in der industriellen Fertigung. Hierfür wird meist ein Enterprise Resource Planning System (ERP) eingesetzt, welches die unternehmerische Planung von Ressourcen wie Kapital, Personal, Betriebsmittel, Material und IT-Infrastruktur unterstützt.

Die Automatisierungspyramide stellt seit den 90er-Jahren den etablierten Standard in der vertikal vernetzten Produktion dar, jedoch wird durch den technologischen Fortschritt ein Paradigmenwechsel vorangetrieben, der diese hierarchische Struktur in eine flache Struktur wandelt. So wird die Automationstechnik in ihrer bisherigen Form vermehrt durch cyber-physische Systeme (vgl. Abschnitt 2.2) ersetzt. Der Kontext der vorliegenden Arbeit liegt auf dieser flachen Struktur, die in nachfolgenden Abschnitten im Detail erläutert

wird. Eine der Kernfragen, der im Zuge dieser Ausarbeitung nachgegangen wird, ist welche Daten bzw. Informationen in Form von Selbstbeschreibungsmerkmalen für eine Identifikation und Authentifizierung geeignet sind. Hierfür ist ein grundsätzliches Verständnis der Zusammenhänge und Informationsflüsse von der Prozessebene bis in die Unternehmensleitebene wie in der Automatisierungspyramide beschrieben und ggf. sogar darüber hinaus notwendig.

2.1.3 Produktionstechnik, Betriebstechnik und Informations- und Kommunikationstechnik

Die Gesamtheit der Maßnahmen und Einrichtungen zur industriellen Herstellung von Gütern und Bereitstellung von Dienstleistungen wird unter dem Oberbegriff Produktionstechnik zusammengefasst und erstreckt sich wie in Abbildung 2.4 dargestellt über die gesamte Automatisierungspyramide. Sie gliedert sich in die Energie-, Verfahrens- und Fertigungstechnik. Die Energietechnik befasst sich mit der Gewinnung, Umwandlung, Transport, Speicherung und Nutzung von Energie in allen Formen. In der Verfahrenstechnik widmet man sich der Anwendung chemisch-physikalischer oder biologischer Prozesse zur Herstellung von Produkten.

Die Fertigungstechnik ist die Lehre von der industriellen Herstellung geformter Werkstücke (Skolaut 2014, S. 968). Der Schwerpunkt der Betrachtung liegt in dieser Ausarbeitung auf der Fertigungstechnik, da sich der Arbeits- und Erfahrungsschwerpunkt des Autors in diesem Bereich befindet. Ziel des untersuchten Lösungsansatzes ist allerdings, dass eine Anwendung in allen Bereichen möglich ist.

Eine weitere Eingrenzung dieser Arbeit wird durch einen Schwerpunkt auf die Betrachtung der Einrichtungen der Produktionstechnik vorgenommen. Hier werden neben den gängigen IT-Systemen für die Produktion, die in Abschnitt 2.1.2 erläutert wurden, insbesondere die Betriebstechnik (OT, engl. Operational Technology) genannt (vgl. Abbildung 2.4), einbezogen.

Die OT umfasst die Hard- und Software, die durch die direkte Überwachung und/oder Steuerung von industriellen Geräten, Anlagen, Prozessen und Ereignissen eine Veränderung definierter Zustände erkennt oder verursacht (Norm ISO/IEC TR 23188).

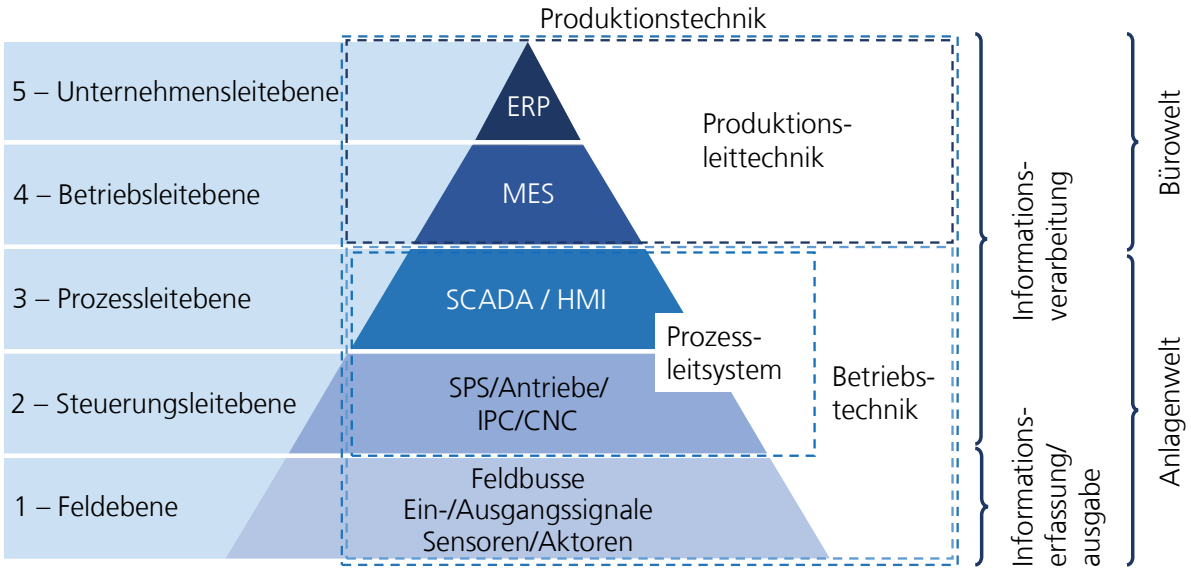


Abbildung 2.4 Übersicht Produktionstechnik und Bezug zur Betriebstechnik (OT) in Anlehnung an (Bindel et al. 2013)

Die Flexibilität automatisierter Fertigungssysteme in Bezug auf vielfältige Variationsmöglichkeiten, Arbeitsablauf und Produktseriengröße wurde durch die Einführung mikroelektronischer Systeme in die Produktionstechnik maßgeblich beeinflusst. So wurden moderne Rechnersteuerungen ermöglicht, die durch Programmierbarkeit der Arbeitsmittel den Übergang zur flexiblen Automatisierung der Produktion markieren (Spur 1997, S. 25). In den 90er-Jahren lag der Anteil dieser speicherprogrammierbaren Steuerungen am Automatisierungsmarkt bei fast 100 %. Zur Jahrtausendwende hatten PC-Systeme im Steuerungsmarkt einen Marktanteil von ca. 10 %, der weiter anwuchs und 2010 zu einer prognostizierten anteiligen Verbreitung von ca. 30 % intelligenter Feldgeräte führte (Gevatter et al. 2006, S. 477).

Diese graduelle Einführung der IKT in der OT-Welt wurde hauptsächlich durch den Bedarf getrieben, umfangreiche vernetzte Systeme zu schaffen, um so komplexe Hierarchien von Maschinen zu kontrollieren. Zudem sollen die Vorteile der flexiblen und modernen IKT in die OT-Welt eingebracht werden. Ein verfolgter Ansatz ist beispielsweise der Trend zu Steuerungen, die die physikalische Welt digital simulieren und ihre Steuerungsentscheidungen auf das Simulationsmodell und nicht auf die Vorgaben eines Steuerungsingenieurs stützen. Weitere Ansätze, die mittlerweile erfolgreich in der IKT genutzt werden, wie bspw. maschinelles Lernen, sollen so auch in der OT eingesetzt werden (Lin et al. 2019, S. 24).

Dieses Verschmelzen von IKT und OT ist jedoch ein komplexes Unterfangen, da diese beiden Welten durch starke Unterschiede geprägt sind, die in Tabelle 1 gegenübergestellt sind. Die fortschreitende Einführung der IKT in der Produktion und das daraus folgende Verschmelzen dieser Technologien treibt sowohl auf der technischen als auch auf der organisatorischen Seite flächendeckend eine digitale Transformation voran, die im folgenden Abschnitt diskutiert wird. Für diese Ausarbeitung ist insbesondere von Interesse, wie die neuen Möglichkeiten, die die IKT in der OT mit sich bringt, genutzt werden können, um die inhärenten Risiken auszugleichen, die in Anhang 3 diskutiert werden.

Tabelle 1 Gegenüberstellung von Betriebstechnik (OT) und Informationstechnik (IT) in Anlehnung an (U.S. Department of Homeland Security 2016, S. 4; Hahn 2016)

	Betriebstechnik	Informationstechnik
Zweck	Steuerung von Prozessen oder deren Veränderung durch die Überwachung und Steuerung von Geräten	Informationsübermittlung und Schutz Speicherung, Wiederherstellung, Übertragung, und Manipulation von Daten
Einsatzbereich	Industrieumfeld	Unternehmensumfeld
Zugriff	Lokal vernetzt, sehr eingeschränkter Zugang mit starken Zugriffskontrollen für wenige Personen	Lokal und global vernetzt; meist gruppenbasierter Zugriff
Verhältnis Anzahl Assets zu Bedienern	Unabhängiger und stärker automatisiert; mehr Geräte als Nutzer	Anzahl der Geräte ist in der Regel gleich (oder nahe) der Anzahl der Nutzer
Wandelbarkeit	Weniger wechselnde Umgebung; teilweise über Monate bis Jahre keine Veränderungen	Ständiger Wandel; Geräte werden mit neuen Mitarbeitern angeschlossen und bei Weggang suspendiert/stillgelegt
Umgebung	Ggf. widrige Bedingungen (extreme Temperaturen oder Luftfeuchtigkeit)	Kontrolliert, stabil und konstant
Bedienung	Kontrollschleifen mittels Sensoren, Steuerprogramme oder Touch-Screens	Tastatur/Maus, mobile Geräte, PCs, Webbrowser
Hauptpriorität	Verfügbarkeit und Integrität des Equipments und der Prozessdaten	Datensicherheit (in der Regel werden vertrauliche Daten verarbeitet)
Systemaktualisierung	Strategisch geplant; nicht-trivialer Prozess aufgrund der Auswirkungen auf die Produktion (Wartungsfenster)	Regelmäßig und planmäßig; abgestimmt auf Zeiträume mit geringer Nutzung
Lebenszyklus der Komponenten	10-20 Jahre; in der Regel derselbe Anbieter; End of Life (EOL) führt zu Sicherheits-Lücken	2-3 Jahre; mehrere Anbieter; Upgrades von Systemen und Komponenten oft problemlos möglich
Echtzeitanforderung	Sekunden bis Millisekunden	(Sekunden) Minuten bis Tage
Hauptschutzziele	Schutz der Umwelt, der Menschen und der Infrastrukturen	Logische Sicherheit (keine Gefahr für Menschenleben). Schutz vertraulicher Informationen vor Risiken (Naturkatastrophen, menschliches Versagen, Cyberattacken, etc.)
Komponenten und Betriebssystem	Spezielles Equipment mit proprietären Betriebssystemen.	Kommerzielle Produkte aus dem Regal (COTS); Standard-Betriebssysteme

2.2 Cyber-physische Systeme – Bausteine der digitalen Transformation

Cyber-physische Systeme (CPS) wurden schon im Hightech-Strategie-Aktionsplan der Bundesregierung als technologische Grundlage für die digitale Transformation der Produktion hervorgehoben und werden als kritischer Erfolgsfaktor für die Zukunftsfähigkeit des Produktionsstandortes Deutschland gesehen (BMBF 2012, S. 53). Eine eindeutige Begriffsdefinition ist aufgrund umfangreicher unterschiedlicher Definitionen in der Fachliteratur nicht zu finden. Jedoch ist zu erkennen, dass ein CPS in seiner Definition aber auch in seiner realen Implementierung einer kontinuierlichen Evolution unterliegt, die durch den ebenfalls fortlaufenden technischen und technologischen Fortschritt begründet ist. Für die vorliegende Ausarbeitung wird daher eine Definition aus der Primärliteratur abgeleitet und im folgenden Abschnitt erläutert.

2.2.1 CPS – Begriffsdefinition und Eigenschaften

Der Begriff cyber-physisches System (engl. „Cyber Physical System“) wurde erstmals von Lee definiert, jedoch wurde der Begriff selbst nach Aussage von Lee von Helen Gill geprägt (Lee et al. 2017, S. 4). Cyber-Physische Systeme (CPS) sind nach Lee „die Vereinigung von Berechnung und physikalischen Prozessen. Eingebettete Computer und Netzwerke überwachen und steuern die physikalischen Prozesse, meist mit Rückkopplungsschleifen, bei denen physikalische Prozesse die Berechnungen beeinflussen und umgekehrt“ (Lee 2006, S. 1). Diese Definition umreißt zwar die fundamentale Funktionsweise und den Zweck eines CPS, jedoch beinhaltet sie nicht alle Eigenschaften, die aktuellere Quellen in ihrer Definition und Diskussion von CPS-Fähigkeiten beinhalten.

Abbildung 2.5 stellt die grundsätzliche Struktur und die funktionalen Komponenten eines CPS dar. CPS sind prinzipiell als Weiterentwicklung klassischer eingebetteter Systeme zu verstehen sind. Sie verfügen jedoch zusätzlich immer über eine Kommunikationsschnittstelle, die eine Vernetzung ermöglicht. Diese Vernetzung kann lokal zwischen CPS statt-

finden. So ist ein CPS nicht als in sich geschlossene und an einem Ort befindliche Komponente zu verstehen, sondern kann örtlich verteilte Komponenten besitzen, die miteinander kommunizieren. Diese Komponenten können für sich betrachtet selbst als CPS bezeichnet werden, was eine weitere Eigenschaft von CPS, „Systems of Systems"-Verbünde zu bilden, kennzeichnet.

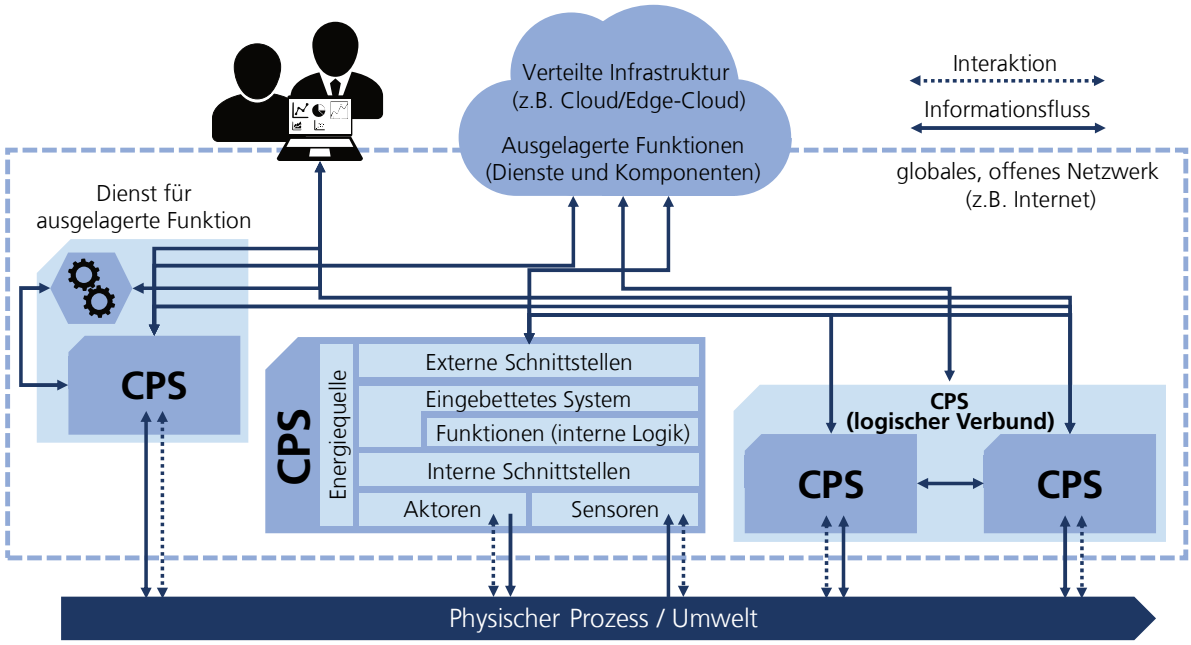


Abbildung 2.5 Struktur und Bestandteile cyber-physischer Systeme

Diese Schachtelbarkeit ist es, die CPS auch eine besondere Flexibilität verleiht. Noch prägnanter jedoch ist der Umstand, dass diese Eigenschaft den Begriff „cyber-physisch" im Besonderen kennzeichnet. So verfügt ein CPS neben seinem physischen Anteil auch über einen virtuellen Bestandteil in einer virtuellen Welt. Diese wird mit dem englischen Begriff Cyberspace bezeichnet, für den sich das Präfix „cyber" etabliert hat. Dieser virtuelle Bestandteil existiert in Form von softwaretechnischen Anwendungen und Diensten, die mit den physischen Komponenten und den anderen virtuellen Komponenten verbunden sind und nach dem SOA-Prinzip miteinander interagieren. Somit bilden diese Komponenten der physischen und virtuellen Welt ein komplexes System, das im Inneren bzw. innerhalb

seiner Systemgrenzen und mit seiner Umwelt über offene, globale Netzwerke wie dem Internet über seine Systemgrenzen hinweg interagiert. Hier ist die Verwandtschaft zum IoT zu erkennen, allerdings zeichnen sich CPS durch eben diese Interaktionsmöglichkeit aus, während IoT-Anwendungen primär darauf ausgelegt sind gesamtheitlich zum Zweck der Sammlung von Daten und Informationen vernetzt zu werden. Durch Sensoren nehmen CPS ihre Umgebung wahr und können optional durch Aktuatoren auf diese einwirken. Hierzu gehört auch die Notwendigkeit einer Benutzerinteraktion, insbesondere im Kontext der Produktion. Die Mensch-Maschine-Interaktion ist eine Voraussetzung für eine sichere und zuverlässige Produktion, da der Mensch zum aktuellen Zeitpunkt immer noch die Deutungshoheit hat und im Notfall eingreifen können muss. Sicherheitsaspekte (Safety und Security) sind einer der Hauptgründe, weshalb auf absehbare Zeit eine weitere Fähigkeit von CPS nicht vollständig umsetzbar sein wird: die Autonomie (Spath et al. 2013, S. 135). Verschiedene Untersuchungen deuten jedoch darauf hin, dass die geschickte Kombination von Mensch und Maschine einem auf sich gestellten Fachexperten statistisch immer überlegen ist (Weber 2015, S. 15). Allerdings werden insbesondere durch die Entwicklungen im Bereich der künstlichen Intelligenz die Eigenfähigkeiten technischer Systeme kontinuierlich erweitert. Nach aktuellem Stand der Technik sind CPS in ihrer momentanen Ausprägung jedoch nur bedingt zu Autonomie fähig. Im Arbeitspapier Technologieszenario „Künstliche Intelligenz in der Industrie 4.0“ sind hierzu verschiedene Stufen der Autonomie definiert (Ahlborn et al. 2019, S. 13).

Die Umsetzungsstrategie Industrie 4.0 sieht hier ab dem Jahr 2020 den Startpunkt zur Entwicklung für Methoden und Beschreibungsmittel für das Engineering und Testen von autonomen Systemen vor. Dynamische Regelung komplexer Fertigungsprozesse ist demnach frühestens ab dem Jahr 2025 realistisch realisierbar (Dorst et al. 2015, S. 29).

2.2.2 Cyber-physische Produktionssysteme

Produktionssysteme und ihre Teilsysteme werden durch die digitale Transformation beeinflusst. CPS sind selbst Teil eines solchen Produktionssystems und stellen wie bereits

erwähnt eine der wichtigsten Grundlagen der digitalen Transformation der Produktion dar. Die Adaption von CPS in die Produktion führt somit implizit zu einer Wandlung dieser Produktionssysteme zu cyber-physischen Produktionssystemen (CPPS).

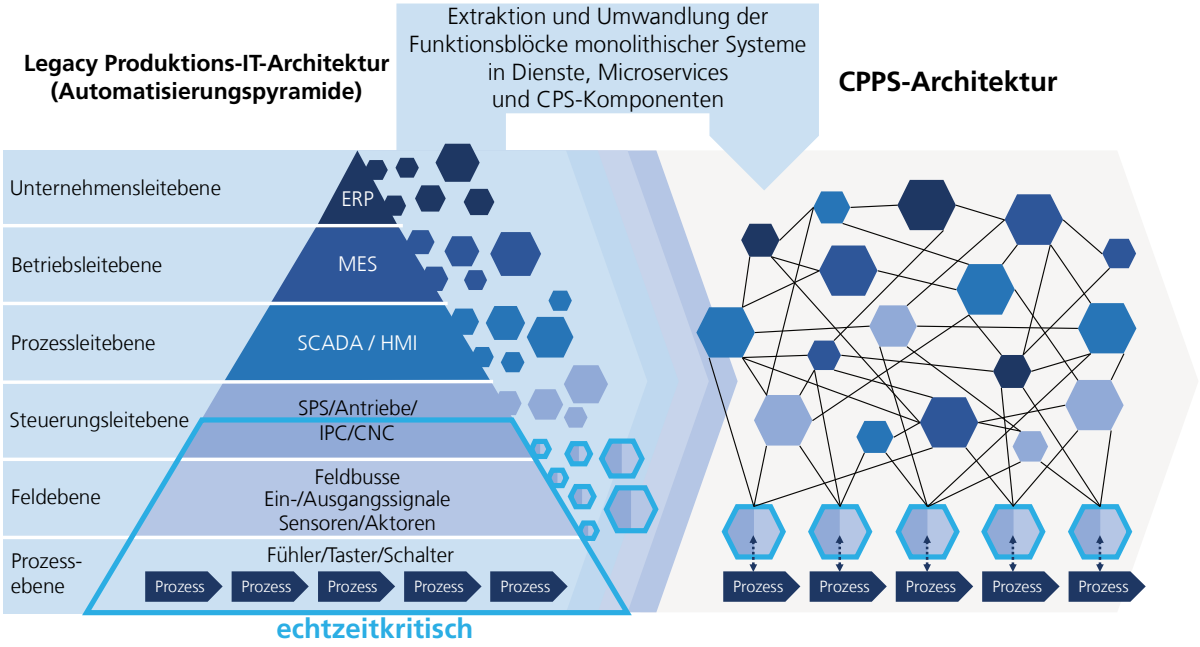


Abbildung 2.6 Architektur cyber-physischer Produktionssysteme nach (Bettenhausen et al. 2013)

Diese besitzen dieselben Fähigkeiten wie CPS und befähigen somit Produktionsressourcen zu Flexibilität und Wandlungsfähigkeit, die durch die bereits diskutierten Autonomie-Fähigkeiten gestützt werden. Sie kommunizieren untereinander und mit Produkten und sind in der Lage abhängig vom Kontext eigenständig Entscheidungen zu treffen (Bauernhansl et al. 2016, S. 11). Dieser Wandlungsprozess kann durch eine Ist-Analyse des Produktionssystems, Gap-Analysen und Identifikation geeigneter Technologien und Ermittlung von Prozessen und Abhängigkeiten methodisch unterstützt werden. Dies ist notwendig um im komplexen Umfeld der Produktion unternehmensindividuelle und modulare Konzepte zur digitalen Transformation eines Produktionssystems in ein cyber-physisches Produktionssystem zu ermöglichen und um die Komplexität beherrschbar zu machen (Siedler

et al. 2018). CPS sind neben zahlreichen weiteren Technologien einer der wichtigsten Bausteine und diese Ausarbeitung hat zum Ziel nach diesem Vorbild einen zusätzlichen Beitrag für die Wandlung von Produktionssystemen in CPPS zu leisten.

Produktionstechnisch sind CPPS ganzheitlich zu betrachten, somit auch im Fokus dieser Arbeit in Form von technischen Systemen. Abbildung 2.6 stellt hierzu dar, wie sich die Architektur der Unternehmens-IT im Kontext eines CPPS verändert.

Die klassische Automatisierungspyramide, die sich durch eine klare Hierarchie der IT-Systeme und ihrer Aufgaben auszeichnet, wird in einem CPPS aufgelöst. Die Funktionen und Aufgaben der monolithischen IT-Systeme werden in eine netzartige Struktur aus verbundenen Diensten und Komponenten überführt. Dies hat zur Folge, dass Daten und Informationen nicht mehr unbedingt zentral in Silos bzw. in einer der Ebenen der Automatisierungspyramide abgelegt oder verarbeitet werden. In einem CPPS können diese Daten flexibel und bedarfsgerecht in einem der Teilsysteme in Form von CPS bzw. der Teilsysteme der CPS persistiert und bereitgestellt werden. Ein Konzept zu einer solchen CPS-gestützten Informationsarchitektur wurde in (Stock et al. 2019b) vorgestellt und beschrieben. Diese stützt sich auf die Eigenfähigkeiten von CPS, die für die vorliegende Ausarbeitung von zentraler Bedeutung sind und in den folgenden Abschnitten erläutert werden.

2.2.3 Self-X-Fähigkeiten – Eigenfähigkeiten von CPS

Das Konzept der Eigenfähigkeiten, englisch Self-X genannt, ist eine Voraussetzung für die Autonomie eines Systems. Ein Positionspapier von IBM zur zukünftigen Governance von Rechenzentren und Netzwerken ging kurz nach der Jahrtausendwende in diesem Kontext auf das „Autonomic Computing“ (AC) ein, abgeleitet vom „Autonomic Nervous System“ (dt. vegetatives Nervensystem). Das vegetative Nervensystem steuert die unwillkürlichen Körperfunktionen, wie beispielsweise die Atmung oder den Herzschlag. Dieses Prinzip kann sich auf technische Komponenten von IKT-Systemen übertragen lassen, indem man die eigenständige Kontrolle und Steuerung bestimmter Teilkomponenten im Rahmen ihrer vorgegebenen Fähigkeiten und Aufgaben dem System selbst überlässt. Hierzu gehören

beispielsweise Selbst-Steuerung, Selbst-Optimierung oder Selbst-Schutz eines Systems (IBM 2001). Einen ähnlichen Ansatz, der jedoch über die

Selbstorganisation von Rechenzentren und Netzen hinaus geht, verfolgt das Organic Computing. Dieses ist ebenfalls von der Natur inspiriert und an den Eigenschaften eines biologischen Systems orientiert. Müller-Schloer et al. definieren hierzu einen „organischer Computer" (OC) als ein selbst-organisierendes System, das sich den jeweiligen Umgebungsbedürfnissen dynamisch anpasst und auch in der Lage ist zu lernen. Der Betrachtungshorizont umfasst hier das Gesamtsystem und nicht nur Teilsysteme (Müller-Schloer et al. 2004).

Als weiterer Ansatz widmet sich das Pervasive (dt. „durchdringend") bzw. „Ubiquitous (dt. „allgegenwärtig") Computing" (UC) wiederum dem Einsatz eingebetteter Prozessoren, die die Alltagsumgebung und Gegenstände „intelligent" machen sollen (Mattern 2004). Der Begriff des UC für allgegenwärtige und unsichtbare Computersysteme wurde jedoch bereits Anfang der 90er Jahre von Weiser geprägt (Weiser 2002).

Die drei Ansätze des AC, OC und UC unterscheiden sich in ihrem Geltungsbereich, jedoch setzen sie im Kern auf das Prinzip des „Self-X", um das System in gewissen Grenzen eigenständig agieren zu lassen. Dies kann bedeuten, es robuster gegen Veränderungen und Angriffe zu machen oder bestimmte Optimierungen oder Konfigurationen selbstständig durchzuführen. Eine Entscheidungsfreiheit im Sinne eines wahrhaftig autonomen Systems ist jedoch noch nicht gegeben, allerdings sind Self-X-Fähigkeiten eine notwendige Voraussetzung für Autonomie. Tabelle 2 listet eine Übersicht der fundamentalen Self-X-Eigenschaften auf und erläutert diese im Zusammenhang. Tabelle 2 erhebt keinen Anspruch auf Vollständigkeit. Zudem sind die Ordnung bzw. Entwicklung der Self-X-Fähigkeiten und ihre Abhängigkeiten voneinander nicht strikt linear. Jedoch wird nach einer Analyse der umfangreichen Literatur klar, dass Self-X-Fähigkeiten zwar zahlreich sind, sich aber in bestimmte Klassen einteilen lassen. Die jeweiligen Fähigkeiten innerhalb dieser Klassen weisen oft Ähnlichkeiten auf, bauen jedoch meist aufeinander auf.

Tabelle 2 Übersicht über CPS Self-X-Eigenschaften in Anlehnung an (Würtz 2008; Jeschke et al. 2017; Burmeister et al. 2018; Gurgen et al. 2013; Bakakeu et al. 2017; Monostori et al. 2016)

Abhängigkeit ↓	Self-X	Bedeutung
	replication, reproduction	Selbstreplikation oder Selbstreproduktion ist die Fähigkeit sich selbst oder einzelne Systemkomponenten zu vervielfältigen.
	organization, modifying, modeling, design, structuring, patterning, assembly	Die Selbstorganisation eines Systems ist die Fähigkeit seine innere Struktur zu modifizieren, ohne dabei durch externe Kontrollelemente beeinflusst zu werden. Dies dient hauptsächlich dazu Emergenzeffekten entgegenzuwirken, also dem Auftreten unvorhergesehener Wechselwirkungen komplexer Systeme. Äußere Einflüsse sind möglich, werden aber auf einer höheren Ebene betrachtet, wodurch die innere Komplexität des Systems nach außen reduziert wird und nur lenkende Einflüsse zugelassen werden.
	protection, healing, repair, servicing	Der Selbstschutz (self-protection) eines Systems ist die Fähigkeit sich gegen Bedrohungen oder negative Effekte zu wappnen, die in der Designphase nicht existent oder unbekannt waren. Hierzu nutzt das System Selbstheilung oder Selbstreparatur, um bestimmte Systemkomponenten oder ihre Verbindung untereinander bei unerwarteter Störung oder Ausfall wiederherzustellen oder vorzubeugen.
	adaptiveness, generating, optimizing, improvement, learning, evolution	Die Fähigkeit der Selbstanpassung dient der Erreichung eines optimalen Betriebszustands (Selbstoptimierung) bei sich ständig ändernden Bedingungen und Anforderungen durch selbstgenerierte Handlungsanweisungen. Der optimale Zustand kann dabei auch systemweit oder lokal verbessert werden. Durch das Erlenen neuer Informationen oder Fähigkeiten kann das System kontinuierlich einen evolutionären Prozess durchlaufen, durch den es sich selbst mit neuen Fähigkeiten versieht.
	control, regulation, configuration, stabilizing	Die Selbststeuerung und -regulierung als Folge einer erkannten notwendigen Handlung ist in erster Linie dafür zuständig, dass das System einen stabilen Zustand beibehalten kann. Die Fähigkeit zur Selbstkonfiguration gibt dabei den Handlungsspielraum vor, in welchem eine Selbstregulierung möglich ist.
	monitoring, perception, reflection, diagnosis, assessment, consciousness	Seinen eigenen Zustand mittels Monitoring zu erfassen und zu kennen ist die Grundlage für eine tiefergehende Wahrnehmung (perception), die den Zustand der eigenen Systemressourcen (reflection) in Bezug zur Umgebung bzw. anderen Systemen setzt. Hierzu ist die Fähigkeit der Diagnose und Abschätzung von Folgen durch eine Handlung Teil der Selbstreflexion. Die Fähigkeit ein Bewusstsein zu entwickeln, wird in diesem Kontext auch als Selbstreflexion von Selbstreflexionen in Verbindung einer Systemeigenen Erinnerungsfähigkeit genannt.
	description	Die Fähigkeit sich mittels einer definierten Sprache L (formell) selbst zu beschreiben.

Viele der Self-X-Fähigkeiten zeichnen sich durch inhärente Klassenübergreifende Abhängigkeiten aus. Beispielsweise benötigt eine „self-reflection"-Fähigkeit zur Beschreibung der Systemeigenen Ressourcen eine Sprache, die durch eine „self-description"-Fähigkeit befähigt wird. Eine Selbst-Regulierung ist abhängig von der Kenntnis des Systemzustands mittels Self-Monitoring und Selbst-Wahrnehmung. Für CPPS werden dieselben Self-X- oder darauf aufbauende Fähigkeiten abgeleitet. So listet Monostori beispielsweise Robustheit, Autonomie, Selbstorganisation, Selbstwartung, Selbstreparatur, Transparenz, Vorhersagbarkeit, Effizienz, Interoperabilität und globales Tracking und Tracing als einige der wichtigsten Fähigkeiten von CPPS (Monostori et al. 2016).

CPS sollten somit über die in Tabelle 2 genannten Self-X-Fähigkeiten in mindestens rudimentärer Ausprägung verfügen. Im Rahmen dieser Arbeit liegt der Fokus jedoch auf der Fähigkeit sich selbst zu beschreiben, also auf der Selbstbeschreibung und der Formalisierung dieser Selbstbeschreibung.

2.2.4 Selbstbeschreibung von CPS

Das Konzept der Selbstbeschreibung wurde ursprünglich hauptsächlich im Umfeld des Semantic Web eingesetzt (Fulcher et al. 2008, S. 383). Hierbei wird versucht die Schnittstellen eines Dienstes über offene und einheitliche Beschreibungsformate bereitzustellen (Page et al. 2011; Panziera et al. 2013). Dies soll eine semantische Interoperabilität herstellen, da die bei der Komposition von Diensten in einem nach SOA zusammengesetzten System keine syntaktisch und semantisch einheitliche Beschreibung der Datenaustauschformate und Schnittstellen garantiert und sogar unwahrscheinlich ist. Im Bereich des Plug & Produce ist eine Selbstbeschreibung von Komponenten ein Ansatz, um eine automatisierte Interoperabilität herzustellen. Hierzu wird meist eine eigene formalisierte Sprache entwickelt, die in Form einer Ontologie abgebildet wird (Jirkovský et al. 2018). Diese Selbstbeschreibung kann einer Komponente manuell zugewiesen werden oder aber durch die Fähigkeit der Selbstreflexion generiert werden. Dies ermöglicht die Generierung einer

dynamischen Selbstbeschreibung, die nicht nur die statischen Fähigkeiten eines CPS wiedergibt, sondern auch den aktuellen Zustand, Handlungsanweisungen, Ziele und Interaktionen (Burmeister et al. 2017). Die Formalisierung dieser Beschreibungssprachen ist nicht nur notwendig, um die Maschinenlesbarkeit sicherzustellen, sondern auch um die Interoperabilität zwischen verschiedenen Ontologien herzustellen, um beispielsweise ein automatisches Mapping zwischen Daten- und Informationsfeldern durchzuführen (Burmeister et al. 2018). Zudem sind sie die Grundlage für eine Klassifizierung von CPS im IoT (Fortino et al. 2014), die für den in dieser Ausarbeitung verfolgten Ansatz eine notwendige Voraussetzung ist. Weitere Anwendungsfelder für Selbstbeschreibungen werden in Abschnitt 3.2.2 vorgestellt. Ein Beispiel für eine mögliche Selbstbeschreibung ist im Anhang in Abbildung A 16 und Abbildung A 17 zu finden.

2.2.5 CPS und IoT – Smarte Objekte und Smarte Dienste

In der vorherigen Definition eines CPS wurde die Möglichkeit der Schachtelung von CPS zur Bildung eines System of Systems beschrieben. An dieser Stelle soll allerdings noch eine weitere Unterscheidung eingeführt werden, die jedoch nur semantischer Natur ist. Als Basisbausteine eines CPS sollen nicht nur CPS dienen, sondern auch Smarte Objekte und Smarte Dienste (Fortino et al. 2014; Kortuem et al. 2009). Ein smartes Objekt besitzt Charakteristika eines CPS, stellt aber nur eine Art Proto-CPS, also die Vorstufe eines CPS mit begrenzten Self-X-Fähigkeiten in einer rudimentären Form dar (Stock et al. 2020b). Es stellt eine physische Komponente dar, muss aber nicht zwingend mit einem Dienst im Cyberspace verknüpft sein. Ein smarter Dienst wiederum stellt eine Cyber-Komponente dar, ist aber nicht zwingend mit einem physischen Teil verknüpft (Stock et al. 2019b). Allerdings markiert das Präfix „Smart“, dass das Objekt bzw. der Dienst jeweils eine gewisse Eigenintelligenz besitzt und zumindest in der Lage ist eine Selbstbeschreibung von sich selbst bereitzustellen (Schel et al. 2018). Smart ist als Begriff von der IEC definiert und bedeutet in diesem Fall jedoch nur, dass ein smarter Ansatz eine neuartige technologische

Lösung ist, die mittels der im smarten Ansatz genutzten Technologie eine bessere Lösung bietet als die nicht-smarte Lösung.

CPS- und IoT-Konzepte entstammen historisch gewachsen verschiedenen Umfeldern, konvergieren aber zunehmend. CPS-Konzepte entspringen hauptsächlich dem Systems Engineering und der Steuerung industrieller Anlagen. IoT-Ansätze kommen ursprünglich aus dem Wunsch die Cyberwelt der Vernetzung und IT-Systeme mit der physischen Welt zu verbinden (Greer et al. 2019, S. 10). Hierzu werden wie in Abbildung 2.7 dargestellt vom National Institute of Standards and Technology (NIST) vier Modelle gelistet, die die unterschiedlichen Interpretationen der Beziehung von CPS und IoT widerspiegeln, die in der Fachliteratur zu finden sind. Modell 1 geht dabei von einer teilweisen Überschneidung aus und sieht die Gemeinsamkeit in der Erfassung von Informationen aus der Umgebung und der Vernetzung. Dabei liegt der Fokus des IoT auf der Verbindung von Dingen und wird eher als offene Plattform betrachtet. CPS hingegen legen in diesem Modell den Schwerpunkt auf den Informationsaustausch und Feedback, wobei das System neben der Erfassung der physikalischen Welt auch Rückmeldung geben und die physikalische Welt kontrollieren soll, wodurch ein geschlossener Regelkreis entsteht. Modell 2 differenziert nicht weiter zwischen IoT und CPS und sieht sie funktional als gleichwertig an. Modell 3 und 4 sehen jeweils das eine als Subset des anderen an. Während Modell 3 CPS als Bausteine einer vernetzten IoT-Welt sieht, steht bei Modell 4 das CPS als Engineering-Konstrukt mit spezifischen Aufgaben und Interaktion mit dem Menschen im Mittelpunkt, die im Kontrast zu den allgemein nur vernetzten Objekten Dingen des IoT stehen.

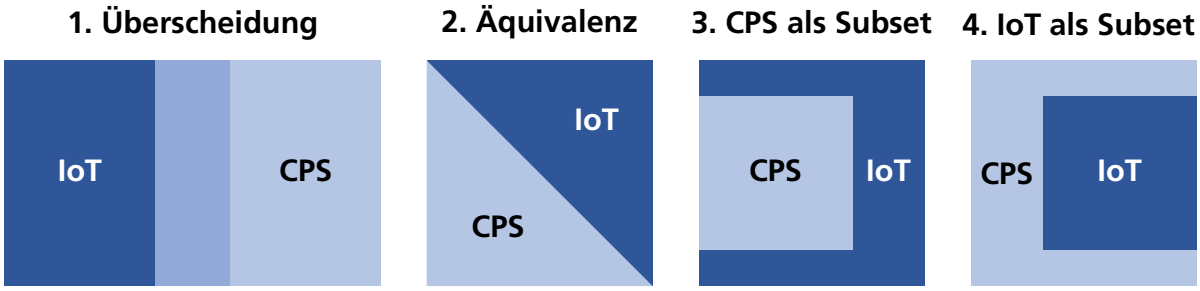


Abbildung 2.7 Überlappungsmodelle von CPS und IoT nach (Greer et al. 2019, S. 11)

Die vorliegende Ausarbeitung folgt hier dem Modell 2. Die Definitionen von CPS und (I)IoT werden sich auch in Zukunft immer weiter annähern und umfassen einen gemeinsamen Schwerpunkt auf hybriden Systemen zur Interaktion digitaler, analoger, physikalischer und menschlicher Komponenten in Systemen, deren Funktion durch die interne Physik und Logik geprägt ist (Greer et al. 2019, S. 28).

2.2.6 CPS-Engineering und Modellierung

Ein Aspekt von CPS, der an dieser Stelle nochmals hervorgehoben werden soll, ist der Umstand, dass CPS aus miteinander interagierenden Komponenten bestehen. Ein CPS formiert sich zum heutigen Stand jedoch (noch) nicht selbst, sondern wird zu einem Zweck erschaffen, es wird „engineered", um eine bestimmte Aufgabe zu erfüllen (Stock et al. 2020b). Dies gilt sowohl für die einzelnen Bausteine des CPS als auch für das CPS als Ganzes. Das Engineering eines komplexen CPS ist ein gleichermaßen komplexes Unterfangen, da sich ein CPS aus heterogenen Bestandteilen zusammensetzt, die die komplette Beherrschbarkeit des Systemverhaltens erschweren. Für die nachträgliche Adaption eines CPPS wird von (Hoang et al. 2016) als Lösungsansatz ein in systematisches Vorgehen vorgeschlagen, das auf der Erfassung von Merkmalen der Fertigungsfähigkeit von Maschinen basiert.

Hier ist zu beachten, dass in einem System, dessen Komponenten in einer permanenten Wechselwirkung miteinander stehen, unvorhergesehene und insbesondere unerwünschte Effekte auftreten können. Dies ist insbesondere in Bezug auf sicherheitsrelevante Aspekte in allen Ausprägungen zu beachten, auf die in Anhang 3 eingegangen wird. Dieses Verhalten wird als Emergenz bezeichnet und stellt ein eigenes Forschungsgebiet komplexer Systeme aller Art dar (Kopetz et al. 2016). Im Rahmen dieser Ausarbeitung soll der Einfluss der Emergenz ausgeklammert oder zumindest stark vereinfach betrachtet werden. Die Komponenten eines CPS, insbesondere eines höherwertigen komplexen CPS, können selbst CPS darstellen. Das Verhalten dieser einzelnen CPS kann durch eine Simulation abgebildet werden, indem die einzelnen Bestandteile zur Laufzeit durch eine Co-Simulation

ersetzt werden, um so die systemischen Auswirkungen abschätzen zu können. Durch die Service-orientierte Architektur eines IoT-Systems lassen sich so flexibel verschiedenste Simulationswerkzeuge als CPS-Komponenten kapseln und flexibel über einen Multi-Agenten-Ansatz mit dem übergeordneten CPS koppeln (Jung et al. 2019).

Einzelne CPS-Komponenten werden in ihrem grundsätzlichen systemischen Verhalten als deterministisch und wie im Zuge des Engineerings vorgesehen und ausgelegt betrachtet (Popper et al. 2018). Es wird von einem idealen und stabilen Zustand des Gesamtsystems ausgegangen. Diese Abstraktion ist notwendig, um eine Handhabbarkeit und Nachvollziehbarkeit des untersuchten Ansatzes zu gewährleisten.

Ein Aspekt des CPS-Engineerings, die strukturelle Modellierung, wird jedoch explizit betrachtet. Die strukturelle Modellierung kann zusätzliche Informationen in Hinblick auf die Selbstbeschreibung eines CPS liefern, da sie die quasistatische Beziehung und Interaktion von CPS-Komponenten zueinander festlegt und beschreibt (Stock et al. 2020b). Nach Ansicht des Autors gehört dies neben den Daten in Form von Merkmalen der Selbstbeschreibung und weiteren Kontextinformationen zu den Eigenschaften und Merkmalen der Selbstbeschreibung, wie sie im folgenden Abschnitt vorgestellt werden.

2.3 Beschreibung und Differenzierung von Entitäten

Möchte man etwas beschreiben, nutzt man intuitiv meist Eigenschaften, die man diesem Etwas zuschreibt. Auf abstrakter Ebene kann das Beschriebene als Entität bezeichnet werden. Eine Entität im ursprünglichen und philosophischen Sinn ist das Dasein im Unterschied zum Wesen eines Dinges. Dabei können Entitäten eine Person, ein Ort, ein physisches oder rechnerisches Objekt sein (Abowd et al. 1999). Für die vorliegende Arbeit sind insbesondere Entitäten in Form von physischen oder rechnerischen Objekten relevant. Ein rechnerisches Objekt ist eine virtuelle Entität, also ist eine gedachte, „abstrakte“ Konstruktion, die zwar nicht physisch vorliegt (man sie also nicht anfassen kann), aber doch in ihrer Funktionalität oder Wirkung vorhanden ist (Jeschke et al. 2014, S. 9). Dies bedeutet, dass die physischen und virtuellen „cyber“ Komponenten eines CPS oder das CPS

selbst als gesamtheitliches System als Entitäten betrachtet werden können. Im Kontext der Industrie 4.0 wird hier auch von der Informationswelt und der physischen Welt gesprochen, der diese Komponenten jeweils angehören (Epple et al. 2014, S. 4).

Innerhalb eines informationstechnischen Systems, beispielsweise einer Datenbank, ist eine Entität eine eigenständige Einheit, die im Rahmen des betrachteten Modells eindeutig identifiziert werden kann (Unterstein et al. 2012, S. 213). Eindeutige Identifizierbarkeit, also die Differenzierung von Entitäten mit ähnlichen oder gleichen Eigenschaften, ist im Kontext der digitalisierten smarten Produktion (Industrie 4.0) ebenfalls eine notwendige Eigenschaft für eine Entität. Sie ist definiert als eindeutig identifizierbarer Gegenstand, der aufgrund seiner Bedeutung in der Informationswelt verwaltet wird (Schleipen et al. 2019, S. 12). Die Identifizierbarkeit der Entität wird durch einige oder alle dieser Eigenschaften der Entität erreicht. Hierfür besitzen Eigenschaften einen Bezeichner und einen Wert. Im Kontext eines Datenbanksystems, also in der Informationswelt, kann eine Entität einfach erzeugt oder gelöscht und ihre Eigenschaften (bzw. Attribute, siehe Abschnitt 2.3.1) geändert werden (Unterstein et al. 2012, S. 213).

Wie Eigenschaften in Form von Merkmalen genutzt werden können, um eine Identifizierung auch in der physischen Welt durchführen zu können, ist eine der Fragen, der im Rahmen dieser Arbeit nachgegangen werden soll. Hiermit sind die Verknüpfung und der eindeutige Bezug zwischen der virtuellen Repräsentation und der Entität bzw. ihrer Identität gemeint.

2.3.1 Eigenschaften, Merkmale und Attribute

Um eine Entität, sei es ein Lebewesen oder ein Gegenstand, aufgrund ihrer intrinsischen Bestandteile (Norm DIN SPEC 92000) zu charakterisieren, können wie im vorherigen Abschnitt diskutiert Eigenschaften genutzt werden. Allerdings stehen hierzu nicht nur Eigenschaften zur Verfügung, sondern es kann hier weiter differenziert werden. So findet man neben Eigenschaften oft auch den Begriff „Merkmal“ oder „Attribut“. Insbesondere die

Begriffe „Eigenschaft“ und „Merkmal“ stehen in enger Beziehung zueinander und werden im allgemeinen Sprachgebrauch oft gleichbeutend eingesetzt. Eigenschaften werden wesentlich einer Person oder einer Sache zugeschrieben und weisen entweder keine Ausprägung auf oder ihre Ausprägung ändert in einem Betrachtungszeitraum nicht. Dies bedeutet, dass sie beispielsweise keinen Wert besitzen oder ihr Ursprungswert gleich bleibt (Bedenbender et al. 2019, S. 13). Im Gegensatz dazu sind Merkmale kennzeichnende und unterscheidende Eigenschaften, die eine Merkmalsausprägung besitzen. Dies sind die tatsächlichen Erscheinungsformen in denen das Merkmal jeweils auftritt, also ihre quantitativen und qualitativen Differenzierungen (Knoblich 1969, S. 48). Somit dienen Sie der Differenzierung von Betrachtungsgegenständen, da sie klassifizierte Eigenschaften eines Systems darstellen (Epple 2011). Implizit sind Eigenschaften charakteristische Merkmale allgemeiner Natur, die nicht unbedingt einer eindeutigen Entität zugewiesen werden.

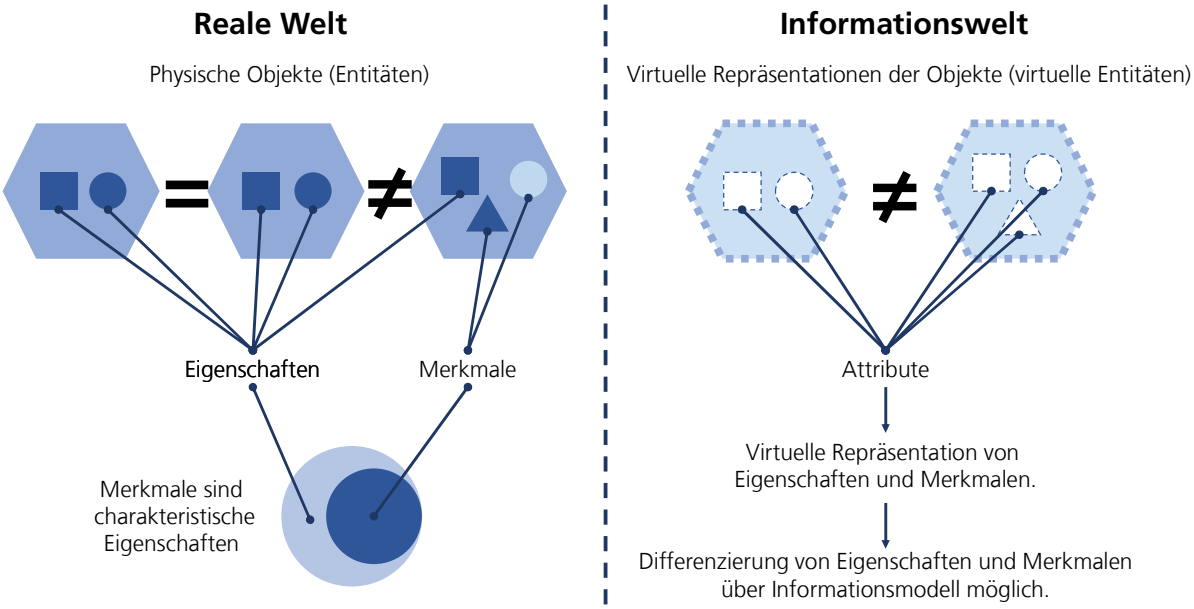


Abbildung 2.8 Entität, Eigenschaften, Merkmale und Attribute

Attribute sind prinzipiell gleichbedeutend mit Eigenschaften, werden aber im aktuellen Kontext als informationstechnische Repräsentation einer Eigenschaft in Form eines Datenelements zur computerlesbaren Beschreibung einer Eigenschaft, einer Beziehung oder einer Klasse definiert (Norm ISO/IEC GUIDE 77-2). Abbildung 2.8 illustriert das Verhältnis zwischen Eigenschaften, Merkmalen und Attributen.

Merkmale können auch als individuelle Eigenschaften aufgefasst werden, die ihren Träger durch ihre Existenz und ihren Eigenschaftswert beschreiben. Nach Art der Ausprägung können sie unterschiedlichen eingeordnet werden. Die DIN SPEC 92000 zum „Datenaustausch auf der Grundlage von Eigenschafts-ausprägungsaussagen" definiert hierzu eine mögliche Klassifizierung von Eigenschaften (Norm DIN SPEC 92000):

- **Besitz-Eigenschaften**, sind Eigenschaften, die nur durch ihr Vorhandensein oder Nicht-Vorhandensein den Gegenstand charakterisieren. Besitz-Eigenschaften haben üblicherweise keine Ausprägung. In Informationsmodellen kann man die Eigenschaft jedoch immer mitmodellieren und durch eine boolesche Ausprägung des „Existenzwerts" vorhanden/nicht vorhanden kennzeichnen, ob sie im Einzelfall vorhanden ist oder nicht.
- **Struktur-Eigenschaften** sind Eigenschaften, die Zusammenhänge beschreiben. Dazu gehören z. B. Systemmodelle, Relationsmodelle usw. In diesem Fall bilden die formal möglichen Strukturvarianten die Ausprägung. Eine zulässige Strukturvariante entspricht einem Wert der Struktur-Eigenschaft.
- **Wert-Eigenschaften** sind Eigenschaften, deren Ausprägung durch einfache Werte beschrieben werden können (z. B. Merkmale, Parameter, Zustände). Die Werte können nicht-metrisch (nominal, ordinal) oder metrisch (Intervall, Verhältnis) skaliert werden.
- **Seins-Eigenschaften** sind Eigenschaften, die einen Zustand des Gegenstands beschreiben.
- **Funktions-Eigenschaften** sind Eigenschaften, die die funktionalen Fähigkeiten eines Gegenstandes beschreiben.

- **Verhaltens-Eigenschaften** sind Eigenschaften, die das dynamische bzw. zeitlich abhängige Verhalten eines Gegenstandes beschreiben, z.B. seine Eigendynamik oder die Reaktion auf äußere Anregungen.
- **Zustände** sind Eigenschaften, deren Wert sich aufgrund der internen Systemdynamik im Betrachtungszeitraum ändern können.
- **Merkmale** sind Eigenschaften ohne Wert (Besitz-Eigenschaften) und Eigenschaften, deren Ausprägung sich im Betrachtungszeitraum typischerweise nicht ändern. (Anmerkung: Die DIN SPEC 92000 fasst den Begriff Merkmal sehr eng auf, während diese Arbeit sich mit Selbstbeschreibungsmerkmalen auf individuellen Eigenschaften im Allgemeinen bezieht und diese sogar weiter auffasst. Der Verständlichkeit wegen werden Selbstbeschreibungsmerkmale im weiteren Verlauf jedoch nur als Merkmale bezeichnet).
- **Parameter** sind Eigenschaften, deren Wert sich typischerweise nur durch Einstellung von außen, also nicht durch die interne Systemdynamik ändern.

Im I4.0-Kontext werden Merkmale zudem eingesetzt, um die Charakteristiken von Assets in der in der Informationswelt datentechnisch darzustellen. Die Methodik der Charakterisierung eines Gegenstands mittels Merkmalen wird im Industrie 4.0-Kontext als Merkmalsprinzip bezeichnet (Bedenbender et al. 2017a, S. 7f) (siehe auch Abschnitt 3.2.3 zur Verwaltungsschale).

Eigenschaften und Merkmale sind die Bausteine, aus denen sich eine Selbstbeschreibung (vgl. Abschnitt 2.2.4) zusammensetzt und sollen in dieser Ausarbeitung dazu eingesetzt werden eine Differenzierung bzw. eine eindeutige Differenzierung in Form einer Identifikation zu ermöglichen. Hierzu soll in den folgenden Abschnitten das prinzipielle Vorgehen diskutiert werden.

2.3.2 Typisierung und Klassifizierung

Schon vor dem Einzug des IIoT und CPS in der Produktion bestand eine unübersehbare Vielzahl verschiedener Erscheinungsformen von technischen Systemen. In einem ersten Schritt muss daher eine sinnvolle systematische Ordnung der unterschiedlichen Erscheinungsformen erstellt werden, um eine zielgerichtete Untersuchung durchführen zu können. Hierfür können die Verfahren der Typologie und Klassifikation eingesetzt werden (Kautz 1996, S. 22).

Die Typologie stellt eine wissenschaftliche Methode dar, die durch die Auswertung charakteristischer Merkmale von Erscheinungen eine zweckorientierte Ordnung derselben ermöglicht. Dies führt zur Entstehung von Typen, deren Differenzierung auf einem Merkmal basieren kann, meist jedoch durch den zielgerichteten Verbund mehrerer Merkmale erzeugt wird. Ein Typ ist somit der Repräsentant einer Reihe von Erscheinungen (Objekten bzw. Entitäten), die eine Anzahl gemeinsamer Merkmale (Eigenschaften) aufweisen (Tietz 1960, S. 29).

Klassifizierung ist die systematische Einteilung einer Menge von Dingen in Teilmengen entsprechend ihren Unterschieden in vorbestimmten Merkmalen, die eine Klassifikation zum Ergebnis haben (Norm DIN EN 61360-1). Eine (vollständige) Klassifikation basiert auf einer Menge von Kriterien, die auf jedes der Elemente der klassifizierten Menge entweder zutreffen oder nicht zutreffen. Sie erfasst daher alle Elemente einer Menge und ordnet jedes genau einer Klasse zu. Hierbei hat kein Element einen besonderen Status (Lehmann 2011). Der Unterschied zwischen Typologie und Klassifikation ist zum eindeutigen Verständnis in Abbildung 2.9 dargestellt.

Bei einer Klassifikation ist eine scharfe Trennung der Elemente bzw. Individuen in Klassen über eine eindeutige Zuweisung der Merkmale möglich. Im Gegensatz dazu weisen Typen in einer Typologie bestimmte Merkmalsausprägungen auf, die zu Überschneidungen und Unschärfen bei den definierten Typen führen können. Die den Typen zugehörigen Individuen können unterschiedlich stark einem oder mehreren Typen zugehören oder keinem Typen zuordenbar sein.

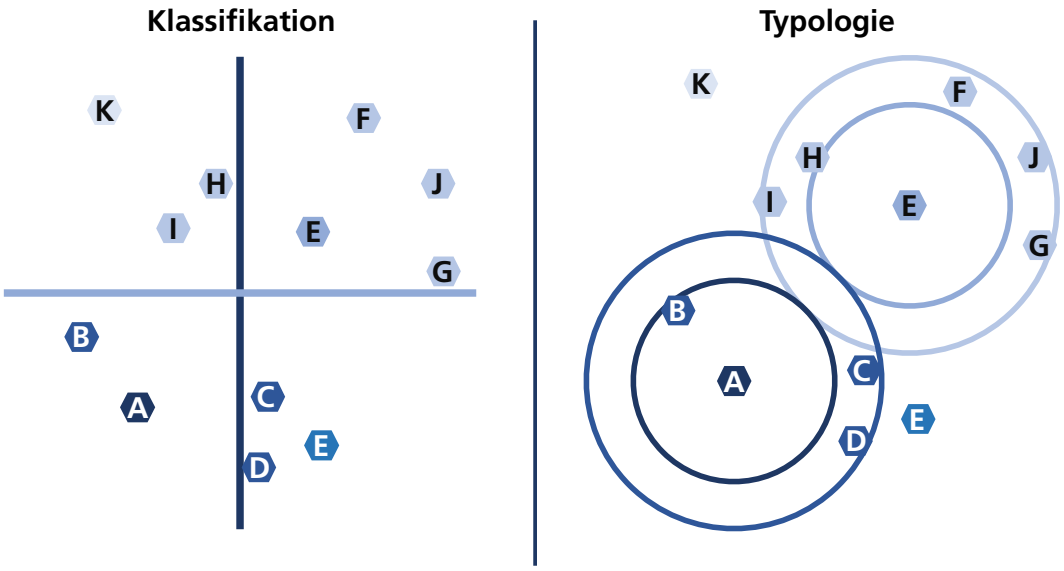
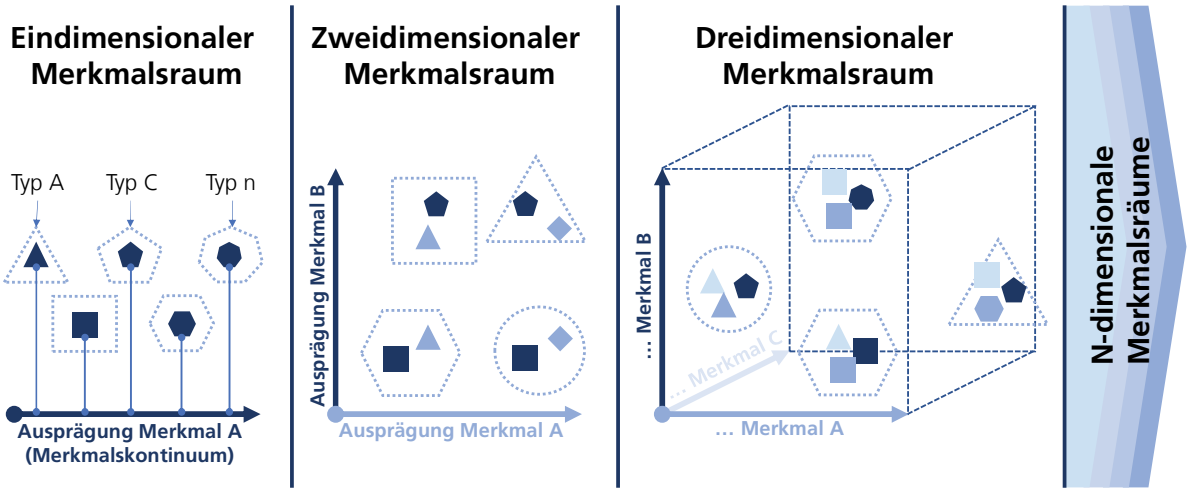


Abbildung 2.9 Unterschied zwischen Klassifikation und Typologie in Anlehnung an (Lehmann 2011)

Weitergehend können Typen auch als ein- oder mehrdimensionale Typen auftreten. Dies hängt davon ab, ob zur Typisierung ein oder mehrere Merkmale eingesetzt werden, wobei für die Differenzierung einer großen Anzahl von Entitäten sinnvollerweise auch eine n-dimensionale Anzahl von Merkmalen genutzt werden sollte. Diese Merkmale bilden den Merkmalsraum einer Typologie der entsprechend n-dimensional sein kann und aus den Merkmalen und ihren Merkmalsausprägungen besteht (Lazarsfeld 1937, S. 13). Merkmale können in Form von Merkmalsvektoren abgebildet werden, die numerisch parametrisierbaren Eigenschaften darstellen und ihrer jeweiligen Summe einen Merkmalsraum bilden.

Während die Kriterien einer Klassifikation eine eindeutige Abgrenzung ermöglichen, bestehen zwischen Typen fließende Übergänge da Typen unterschiedliche stark ausgeprägte Merkmalskombinationen besitzen können und Entitäten mehreren oder auch keinem Typ zugeordnet werden können. Das Prinzip der n-dimensionalen Merkmalsäume und Typologien ist in Abbildung 2.10 dargestellt.



- nominalskalierte Merkmale → Anordnung vertauschbar
- ordinalskalierte Merkmale → Anordnung nicht vertauschbar
- metrisch skalierte Merkmale → Werte können als „Koordinaten" rechnerisch in Beziehung gesetzt werden

Abbildung 2.10 Mehrdimensionale Merkmalsräume in Anlehnung an (Patzelt 2008)

Als Teil der Beantwortung der untergeordneten Forschungsfrage, welche Merkmale geeignet sind um eine eindeutige Differenzierung (vgl. Identifikation) von Entitäten durchzuführen, muss zunächst untersucht werden, wie Eigenschaften bzw. Merkmale selbst typisiert und klassifiziert werden können.

2.3.3 Klassifizierung und Typisierung von Merkmalen und Entitäten

In der Statistik werden Merkmale eingesetzt, um Klassen zu bilden. Hierfür können Merkmale selbst unterschiedlicher Natur sein. Daher ist es üblich vor dem Einsatz statistischer Methoden die unterschiedlichen Merkmalstypen zu klassifizieren, da diese einen Einfluss auf die Methodik und die Genauigkeit der Aussage haben. Es werden stetige und diskrete Größen, sowie ordinale und gruppierende Größen unterschieden um Merkmale zu charakterisieren (Teschl et al. 2014, S. 209).

Die Entitäten bzw. Merkmale werden zunächst untersucht und aufgrund differenzierender Merkmale in Klassen getrennt. Dieser Prozess wird auch als Generalisierung bezeichnet (Dengel 2011, S. 44).

Mittels dieses Merkmalsystems lassen sich formalisierte Klassifikationen von Merkmalen und Entitäten durchführen. Reicht ein Merkmal nicht aus oder ist das Merkmal selbst unscharf, können die im vorherigen Kapitel erwähnten Merkmalsvektoren eingesetzt werden. Ein Merkmalsvektor ermöglicht es die parametrisierbaren Eigenschaften eines Merkmals-Musters in vektorieller Weise zusammenzufassen. Die charakteristischen Merkmale für das Muster bilden die verschiedenen Dimensionen dieses Vektors (Recknagel 2005)

Dabei können die Merkmale explizit zur Typisierung von Entitäten eingesetzt werden, da sie charakteristische Eigenschaften darstellen, die sich bei Ontologien zur Bildung von Kategorien bewährt haben, die wiederum den Klassen in der Informatik entsprechen. Dabei ist die Bedeutung der Merkmale relevant, weshalb dieses Konzept auch seinen Ursprung im Semantic Web und der Ressourcenbeschreibung hat (Stuckenschmidt 2009, S. 24). Dies bietet die Möglichkeit Smarte Objekte auf Grundlage ihrer Fähigkeiten bzw. Fähigkeitsbeschreibung zu klassifizieren (Pérez Hernández et al. 2014). Auch komplexere Zusammenhänge lassen sich modellieren, die beispielsweise eine kontextabhängige Klassifizierung von IoT-Komponenten erlauben (Otebolaku et al. 2017).

An diesen Prinzipien der Klassifizierung und Typisierung orientiert sich die vorliegende Arbeit, um einerseits Merkmalsklassen zu definieren. Andererseits sind eine Klassifizierung und Typisierung notwendig für eine Implementierung, die eine Eingrenzung zum Zweck einer effizienten Suche und Identifikation umsetzt, insbesondere wenn die Anzahl der Entitäten Millionen oder Milliarden erreicht. Auf die spezifischen Such- und Identifikationsstrategien wird im Rahmen dieser Arbeit nicht näher eingegangen, da sie Außerhalb des Betrachtungsrahmens liegen.

2.4 Authentifizierung von Entitäten

In den vorherigen Abschnitten wurden die für diese Ausarbeitung namensgebenden Themengebiete diskutiert. In Anhang 3 ist dargestellt, welchen Gefahren ein CPS im Cyberspace ausgesetzt ist bzw. welche Gefahren es als Teil eines CPPS für einen CPPS-Verbund darstellen kann. Nun soll der Begriff des Authentifizierungsverfahrens im Kontext erläutert werden. Hierzu müssen die Begriffe „Authentifizierung" und „Authentifikation" semantisch voneinander abgegrenzt werden, da sie meist gleichgesetzt werden. Dies liegt daran, dass im Englischen nur der Begriff „authentication" existiert. Authentifizierung bezeichnet den prinzipiellen Vorgang der Beglaubigung der Echtzeit von irgendetwas (Dudenredaktion 2019b).

Die Authentifikation ist der Vorgang bei dem die Prüfung der Authentizität einer Identitätsbekundung von einem informationstechnischen System durchgeführt wird (Dudenredaktion 2019a). Der Vorgang der Bekundung der Identität wird dabei als Authentisierung bezeichnet, die nach erfolgreicher Authentifikation authentifiziert wird. Die hier erläuterten Zusammenhänge sind in Abbildung 2.11 illustriert.

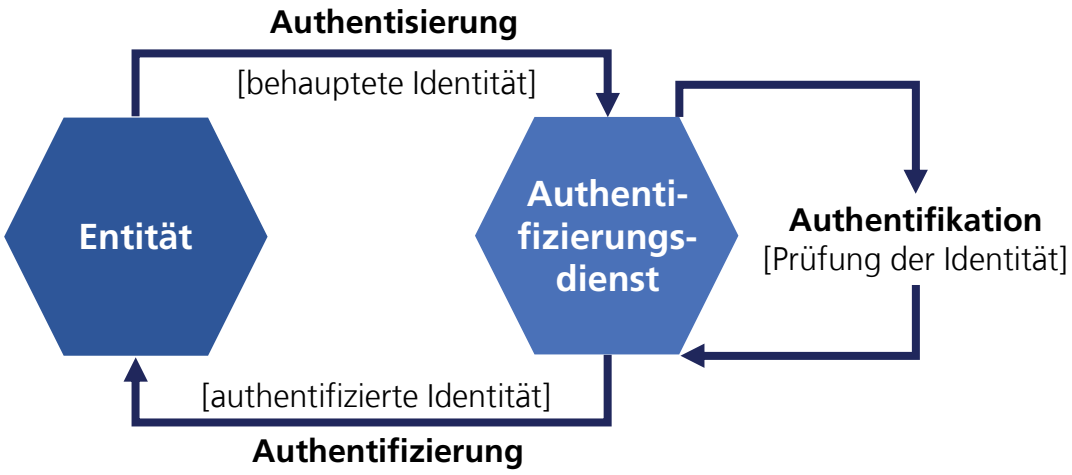


Abbildung 2.11 Authentisierung, Authentifizierung und Authentifikation

Der Verständlichkeit wegen soll im weiteren Verlauf nicht weiter zwischen dem Begriff Authentifizierung und Authentifikation unterschieden werden und der geläufigere Begriff der Authentifizierung für beide gleichbedeutend genutzt werden.

In den folgenden Unterabschnitten werden zudem die Begriffe der Identität, Identifikation und Authentifizierung etwas näher betrachtet und der Bezug zu den vorhergehenden Kapiteln hergestellt.

2.4.1 Digitale und sichere Identität

Der Begriff der Identität stammt ursprünglich aus dem Forschungsfeld der Soziologie und bezeichnet eine Gesamtheit eines Individuums, die eines Menschen oder Objekts, welches sich durch Eigentümlichkeiten und Fähigkeiten in Form von qualitativen Merkmalen von anderen unterscheidet (Straub 2011, S. 278). Diese personelle Identität ist allerdings in Kontext dieser Ausarbeitung nur im übertragenen Sinne relevant und soll auf die allgemeine Identität einer Entität bezogen werden, also auf Objekte und keine Personen. Die Identität bzw. physische Identität einer Entität ist ein der Entität eigener Merkmalssatz, der es erlaubt, diese Entität eineindeutig zu erkennen und von anderen, ähnlichen (gleichartigen) zu unterscheiden (Hippenmeyer et al. 2017, S. 11; Tsolkas et al. 2017, S. 25). Ausgehend davon soll an dieser Stelle der Begriff der **logischen** bzw. **virtuellen** oder **technischen Identität** eingeführt werden, da dieser die Abbildung einer physischen Identität in eine nicht-reale Umgebung, den Cyberspace, darstellt (Tsolkas et al. 2017, S. 26). Zudem kann von einer Entität noch eine **kontextuelle Identität** angenommen werden, die eine bestimmte Rolle in einem Kontext darstellt. Diese hängt von der gelebten Identität ab, die von der jeweils ausgeführten Rolle abhängig ist (Tsolkas et al. 2017, S. 26). Die logische Identität ist somit eine digitale Identität einer Entität, die für diese rollen- und kontextabhängig erschaffen wird. Zu diesem Zweck werden initial die relevanten Merkmale der Entität extrahiert und als Attribute einem digitalen Datensatz als Referenzmerkmale abgebildet. Die relevanten Merkmale sind die charakteristischen Merkmale der Entität mit denen die digitale Identität (dem Datensatz mit der Sammlung von Attributen)

im Zuge der Einrichtung gekoppelt wird. Eine Identität ist also die Eigenschaft einer Entität als Identitätsträger, gekennzeichnet durch eine Menge von Attributen. Eine Entität kann mehrere Identitäten haben, ebenso können mehrere Entitäten die gleiche Identität haben. Um eine eindeutige Identität (UID) zu erlangen, muss diese durch eine spezifizierte Menge an Attributen, die innerhalb eines bestimmten Anwendungskontextes die zugehörige Entität eindeutig repräsentieren, abgebildet werden (Jänicke et al. 2016, S. 8).

So wird eine Verknüpfung zwischen Entität und eindeutiger Identität z.B. durch mindestens ein eineindeutiges Merkmal erzeugt, welches die Entität besitzt oder welches auf sie aufgebracht oder integriert wird. „Eineindeutig" bedeutet dabei, dass ein Attributsatz nur für diese eine Entität existiert - also einmalig ist (Stephan et al. 2018, S. 87). Abbildung 2.12 stellt den Bezug der Identitätsbegriffe zueinander dar.

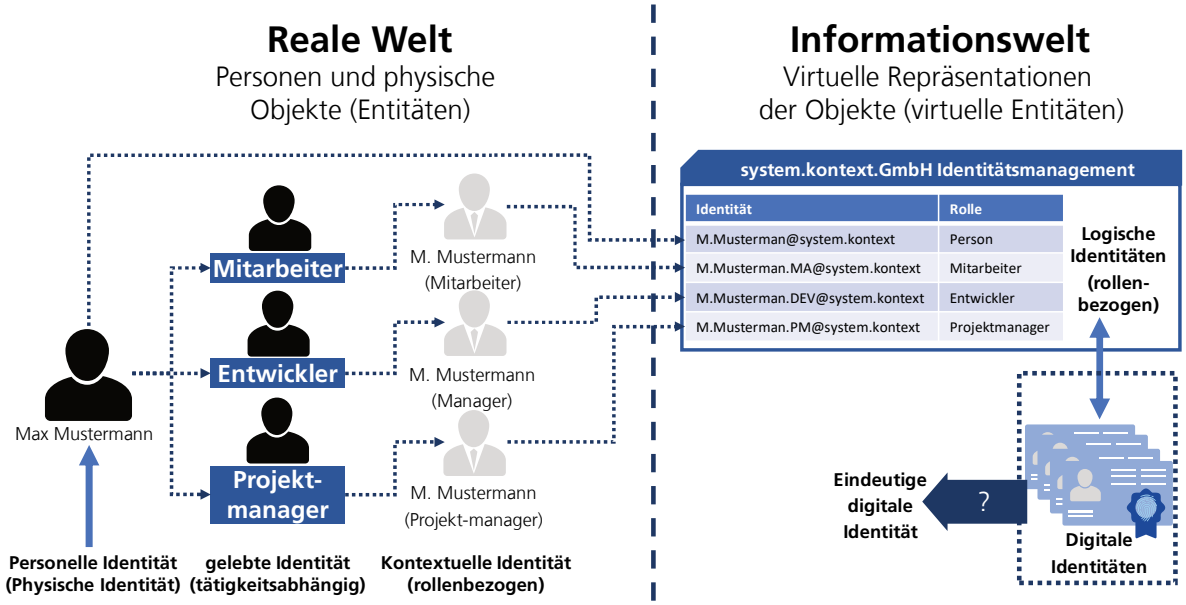


Abbildung 2.12 Physische, kontextuelle und digitale Identität in Anlehnung an (Tsolkas et al. 2017, S. 27; Vacca 2013, S. 77)

Weitergehend ist eine **sichere Identität (SID)** eine eindeutige Identität mit zusätzlichen Sicherheitseigenschaften für eine belastbar vertrauenswürdige Authentifizierung der En-

tität (d.h. mit angemessenen Maßnahmen zur Verhinderung der Vortäuschung einer falschen Identität) (Jänicke et al. 2016, S. 9). Wird die Entität in einem Prozess in irgendeiner Weise genutzt, kann durch das eineindeutige Merkmal die digitale Identität aufgerufen und bspw. zur Verifikation genutzt werden (Stephan et al. 2018, S. 87).

Im Kontext dieser Ausarbeitung sollen die Begriffe digitale Identität (bzw. logische, virtuelle oder technische Identität) und Identität gleichbedeutend behandelt werden.

Die Untersuchung der Möglichkeit eine eindeutige Identität rein durch Selbstbeschreibungsmerkmale und darauf aufbauend eine sichere Identität mittels eines Authentifizierungsverfahrens auf Basis von Selbstbeschreibungsmerkmalen zu erzeugen ist die primäre Forschungsfrage.

2.4.2 Identifikation und Authentifizierung von Entitäten

Identifikation, auch Identifizierung, ist der Vorgang der Feststellung der Identität einer Entität auf Grundlage eines Merkmalssatzes, der es erlaubt, diese

Entität eineindeutig zu erkennen und von anderen, ähnlichen (gleichartigen) zu unterscheiden (Norm DIN 6763). Im Kontext informationstechnischer Systeme wird dabei von der Entität ein Merkmalssatz erfasst, der ihre physische Identität repräsentiert. Dieser wird mit allen vorhandenen digitalen Identitäten abgeglichen. Bei der Identifikation wird also der Merkmalssatz mit allen im System gespeicherten Referenzmerkmalen verglichen (1:n-Vergleich) (BSI 2008, S. 1). Existiert also nur eine einzige digitale Identität, die zum bereitgestellten Merkmalssatz gehört, so wurde die Entität identifiziert und ihre Identität festgestellt.

Die Erfassung und Extraktion der Merkmale wird mittels verschiedener Identifikationsverfahren durchgeführt, die in Abschnitt 4.2.1 und 4.2.2 diskutiert werden.

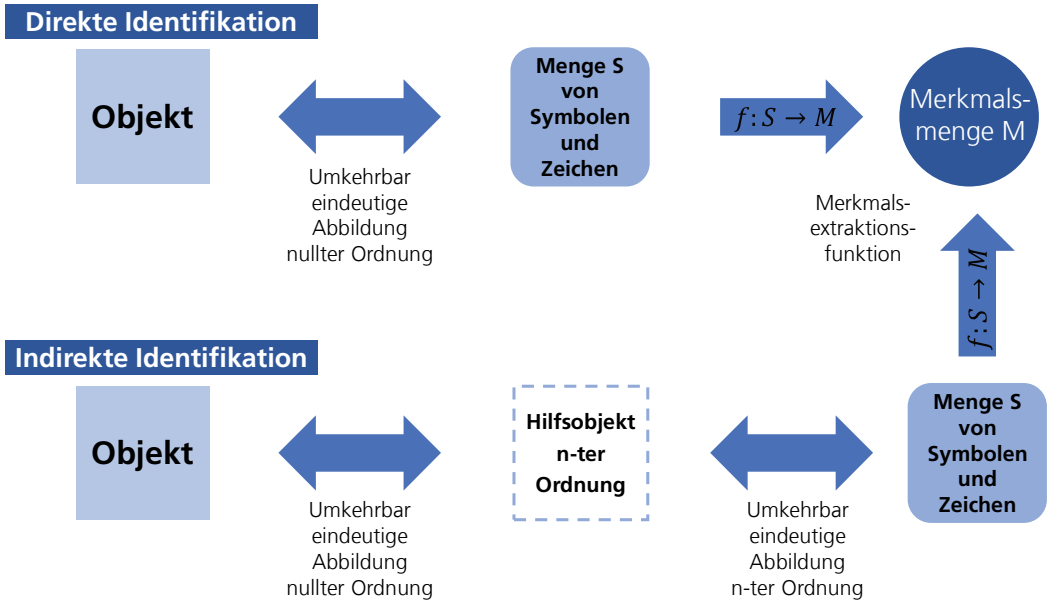


Abbildung 2.13 Direkte und indirekte Identifikation und Merkmalsextraktion in Anlehnung an (Sauter 1990, S. 55)

Grundsätzlich wird wie in Abbildung 2.13 dargestellt zwischen direkten Verfahren und indirekten Verfahren unterschieden (Krämer 2002, S. 85). Direkte Verfahren zielen auf die Erkennung von natürlichen bzw. intrinsischen Merkmalen einer Entität (Form, Größe, Gewicht, Farbe, usw.) ab. Indirekte Verfahren lesen ein der Entität zugewiesenes künstliches Merkmal aus, z.B. einen Barcode oder einen beigefügten Datenträger (z.B. RFID) dessen Informationen das Merkmal repräsentieren (Kiefer et al. 2019, S. 205).

Gibt die Entität im Vorfeld ihre Identität eineindeutig vorab bekannt, beispielsweise durch ein eineindeutiges Merkmal, muss diese bestätigt werden. In diesem Fall spricht man von Verifikation. Da sichere Identitäten mit hoher Wahrscheinlichkeit aus einem mehrdimensionalen Merkmalssatz bestehen, werden sämtliche Merkmale der physischen mit den Referenzmerkmalen der digitalen Identität in einem 1:1-Vergleich verifiziert (BSI 2008, S. 1).

Identifikationsverfahren greifen auf technische Hilfsmittel zurück, um die Merkmale einer Entität zu erfassen. Diese technischen Hilfsmittel wurden bisher in der Produktion als nicht kompromittiert angenommen, da sie ebenfalls durch die Abkapselung („Air Gap“) vom

Cyberspace als sicher angenommen werden konnten. Die Echtheit der erfassten Merkmale konnte also mit an Sicherheit grenzender Wahrscheinlichkeit angenommen werden. Die Identifikation und Verifikation eines CPS gestaltet sich jedoch etwas komplexer. Stammen die Merkmale zur Identifikation und Verifikation eines CPS aus seiner Selbstbeschreibung, kann man nicht grundsätzlich darauf vertrauen, dass diese authentisch sind und eine Identität nur vorgetäuscht wird. Daher soll im Rahmen dieser Arbeit aufgezeigt werden, mit welchen Methoden im Zuge einer Authentifizierung einer Entität die Authentifizierung der Merkmale sichergestellt werden kann.

Die Feststellung, Überprüfung und Verifikation der Identität einer Entität mit größtmöglicher Sicherheit wird als Authentifizierung bezeichnet. Die Authentisierung (vgl. Abbildung 2.11) findet vor der Authentifizierung statt und stellt die Behauptung einer Identität durch eine Entität mittels bestimmter Eigenschaften dar (Meinel et al. 2014, S. 19). Diese Eigenschaften, auch Authentifizierungsfaktoren genannt, stellen die im Abschnitt 2.3.1 diskutierten Merkmale dar. Sie existieren geläufig in drei grundsätzlichen Ausprägungen (Kappes 2013, S. 42):

- Wissen, über das die Entität verfügt
- Gegenstände, die sich im Besitz der Entität befinden
- Die Entität selbst bzw. ihre Merkmale

Handelt es sich bei der Entität um eine Person, so kann das Wissen ein Passwort oder eine PIN sein, der Gegenstand im Besitz der Person eine Smart Card und das Merkmal ein biometrisches Erkennungsmerkmal wie ein Fingerabdruck oder Verhaltensmuster (siehe Abschnitt 4.2.1.1). Im Detail werden Authentifizierungsfaktoren in Abschnitt 3.1.4 diskutiert. Die größtmögliche Sicherheit wird mittels verschiedener Authentifizierungsmechanismen in Form von Verfahren und Protokollen erreicht, die in Abschnitt 3.1 diskutiert werden.

Der Vollständigkeit wegen sei an dieser Stelle noch die Autorisierung erwähnt, die die Einräumung von speziellen Rechten darstellt. War die Authentifizierung erfolgreich und die Identität der Entität wurde authentifiziert, sind in informationstechnischen Systemen beispielsweise Zugriffsrechte an diese Identität gekoppelt.

Gängige Authentifizierungsverfahren sind für Menschen ausgelegt und sind daher auch an deren Fähigkeiten und Eigenschaften ausgerichtet. Dies stellt einerseits für CPS eine Herausforderung und zugleich auch einen Vorteil dar. Im Rahmen dieser Ausarbeitung soll untersucht werden, welche Ansätze für die Authentifizierung von Menschen auf CPS sinngemäß im Produktionsumfeld übertragbar sind und wie CPPS diese ggf. sogar mittels Self-X-Eigenschaften besser ausführen können. So sollte die Automatisierung der potenziell zahlreichen Verfahrensschritte und verschiedenartigen Verfahren eine Kombination dieser und somit eine Steigerung der statistischen Sicherheit ermöglichen.

2.5 Zusammenfassung der Anforderungen

Produzierende Umgebungen bieten eine Vielzahl von Datenquellen. Diese wurden mit der fortscheitenden Vernetzung und dem zunehmenden Einsatz von „intelligenten" bzw. „smarten" IKT- und OT-Komponenten im Zuge der digitalen Transformation der Produktion über alle Ebenen hinweg erschlossen. Die IT-Systeme der ursprünglichen Produktions-IT wandeln sich zunehmend von monolithischen Systemen mit Daten-Silos in Service-basierte verteilte Systeme, die auf flexiblen und skalierbaren Service-orientierten Architekturen basieren. Sie bilden so Verbünde aus ihren zugehörigen Diensten und physischen Komponenten in Form von Aktoren und Sensoren bzw. in aggregierter Form als Baugruppen und Maschinen. Diese Verbünde aus über (offene globale) Netzwerke kommunizierenden Komponenten werden als cyber-physische Systeme bezeichnet. Nun stellt sich die Frage wie diese in der Produktion eingesetzten cyber-physischen Produktionssysteme auf Basis ihrer Daten differenziert

Im Folgenden wird im Stand der Technik und den weiteren Abschnitten betrachtet, welche Authentifizierungsverfahren und Ansätze geeignet sind, um aus den verschiedenartigen Daten eines CPPS eine digitale Identität zu konstruieren, die sich aus dessen Selbstbeschreibung ableitet und sich mittels weiterer Self-X-Fähigkeiten des CPPS verifizieren lässt.

3 Stand der Wissenschaft und Technik

Dieses Kapitel befasst sich mit ausgewählten Themengebieten zum Stand der Technik. Es werden einige Schlüsselkonzepte zur Authentifizierung und der IT-Sicherheit, Web-Technologien und der digitalen Transformation der Produktion diskutiert, die der Autor als relevant erachtet und welche in die Entwicklung des Konzepts für den Lösungsansatz im folgenden Kapitel einbezogen werden sollen.

3.1 Authentifizierungsverfahren

Das in Abschnitt 2.4.2 vorgestellte Prinzip der Authentifizierung wird mittels verschiedener Authentifizierungssysteme bzw. -dienste technisch umgesetzt. Diese wiederum können wie in den vorherigen Kapiteln vorgestellt auf einer Vielzahl von Identifikationsverfahren und verschiedener Ansätze zur Merkmalsextration basieren.

Authentifizierungsverfahren, die mit direkter Merkmalserfassung arbeiten, werden überwiegend für Personen eingesetzt, weshalb die meisten Verfahren sich damit befassen Merkmale von eben diesen zu erfassen und zu authentifizieren. Allerdings sind die meisten Verfahren in ihrer prinzipiellen Funktionsweise auf CPS übertragbar. Im Folgenden werden daher die grundsätzliche Funktionsweise von Identitätsmanagementsystemen, relevante Standards und Authentifizierungssysteme diskutiert. Eine Authentifizierung kann verfahrensseitig unterschiedlich implementiert sein, daher werden die bekannten Verfahrensarten von der einfachen, über die Zwei- bzw. Multifaktorauthentifizierung und die zertifikatbasierte Authentifizierung bis hin zur kontinuierlichen Authentifizierung und ihre Authentifizierungsfaktoren vorgestellt.

3.1.1 Identitätsmanagement

Die Authentifizierung ist Teil eines Authentifizierungssystems bzw. -dienstes (vgl. Abschnitt 3.1.3), welcher Teil eines Identitätsmanagementsystems (IDMS) ist. Dieses unterstützt das Identitätsmanagement (IDM), welches sich auf den „Prozess der Anwendung aufkommender Technologien zur Verwaltung von Informationen über die Identität von Entitäten und zur Kontrolle des Zugriffs auf (Unternehmens-) Ressourcen" bezieht (Lee 2003). Ziel des IDM ist es, die Produktivität und Sicherheit zu verbessern und gleichzeitig die Kosten für die Verwaltung der Entitäten und ihrer Identitäten, Attribute und Anmeldedaten möglichst niedrig zu halten.

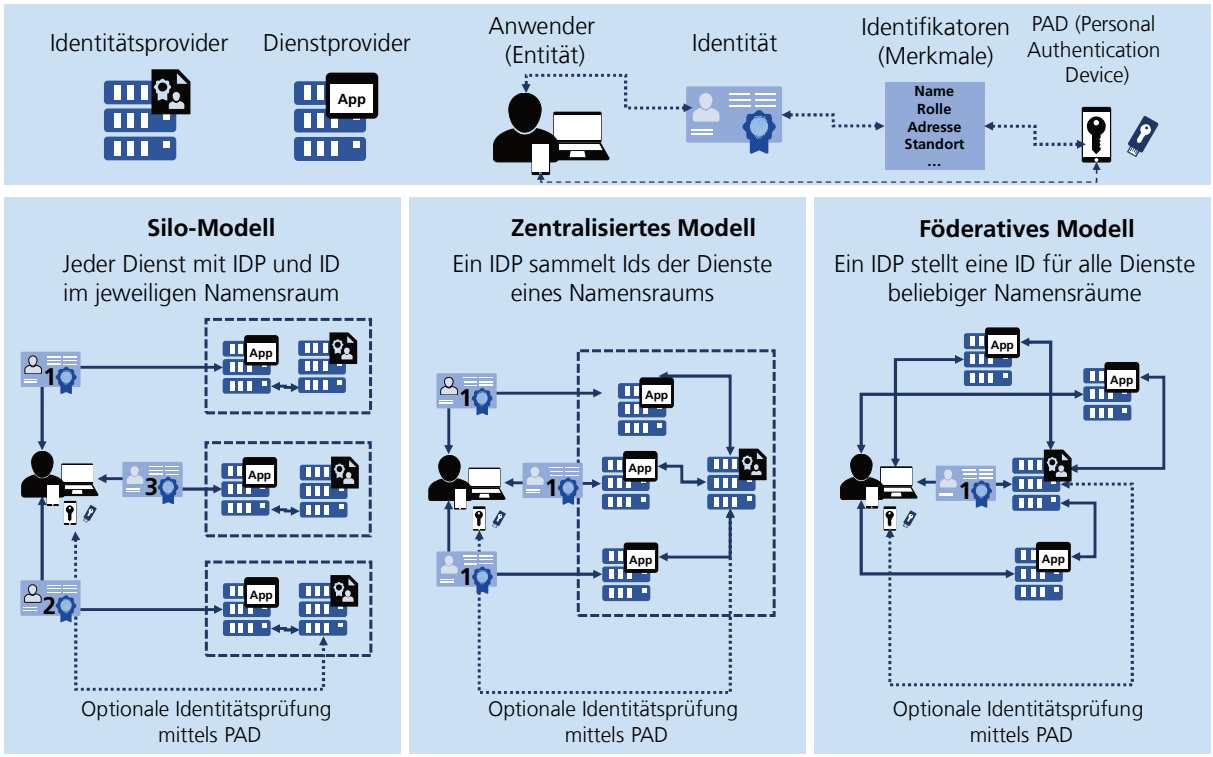


Abbildung 3.1 Identitätsmanagement-Komponenten und Varianten in Anlehnung an (Vacca 2013, S. 81f)

Ein IDM setzt sich aus den folgenden Komponenten zusammen:

- Eine Entität, die sich authentifizieren lassen möchte
- Identity Provider (IDP): Aussteller der Benutzeridentität
- Service Provider (SP): Vermittelnde Partei, die eine Identitätsprüfung anfordert
- Identität (ID): Satz von Attributen bzw. Merkmalen und Identifikatoren der Entität
- Persönliches Authentifizierungsgerät (Personal Authentication Device - PAD): Gerät mit verschiedenen Identifikatoren (z.B. Token/PIN) und Anmeldeinformationen (falls die Entität eine Person ist)

Die Architektur eines IDMS, die diese Komponenten miteinander in Beziehung setzt, kann wie es in Abbildung 3.1 dargestellt ist unterschiedlich ausgeprägt sein. Die üblichen Varianten eines IDMS sind demnach nach folgenden Grundmustern aufgebaut (Vacca 2013, S. 81f):

- Silo Modell: jeder SP verfügt über einen eigenen IDP. Ein Nutzer muss für jeden Namensraum über eine eigene digitale Identität verfügen.
- Zentralisiertes Modell: mehrere SP teilen sich einen IDP. Dies erlaubt es einem Nutzer eine digitale Identität für alle Dienste zu nutzen, da diese in einem Namensraum operieren, jedoch von einem IDP abhängig sind.
- Föderatives Modell: Jeder SP verwaltet die ID der Entitäten in seinem eigenen Namensraum mit einem eigenen IDP, erweckt jedoch den Eindruck eines einzigen IDP. Mittels über APIs integrierbarer Softwarekomponenten und Protokolle werden die Identitätsdomänen miteinander gekoppelt. So kann eine Entität die Authentifizierung mit den Anmeldeinformationen einer ID für alle verknüpften Domänen durchführen. Hierbei

Das föderative Model findet seit einigen Jahren meist als Single-Sign-On (SSO) Verbreitung. Hierfür existieren verschiedene Implementierungen, wie beispielsweise die offenen Keycloak und Shibboleth oder proprietäre Lösungen wie Facebook connect und Microsoft account. Die Authentifizierung der Identität durch das IDMS findet mittels verschiedener Verfahren statt, die in den folgenden Abschnitten eingeführt werden.

3.1.2 Standards und Spezifikationen für die Authentifizierung

Die Komplexität des Verfahrens, das zur Erstellung, Feststellung und Authentifizierung der Identität eingesetzt wird, hängt von der Kombination der eingesetzten Methoden ab. Allerdings sollten hier aufgrund der integralen Wichtigkeit der Absicherung der Identität Standards und Best-Practices eingehalten werden. Standarddokumente der ISO/IEC und des NIST, liefern hierzu normative Vorgaben.

So bietet das „Entity authentication assurance framework" der ISO/IEC 29115 Norm ein Rahmenwerk zur Authentifizierung beliebiger Entitäten. Dieses definiert die notwendigen Bausteine für eine sichere Authentifizierung. Hierzu gehören die Akteure, Lebenszyklusphasen der Authentifizierung und Assurance Levels (LoA) zur Formalisierung der Bewertung des Vertrauen in die behauptete oder bestätigte Identität einer Entität (Norm ISO/IEC 29115).

Das NIST bietet die „Digital Identity Guidelines" (Grassi et al. 2017c) mit drei begleitenden Dokumenten zu den Themen Enrollment (erstmalige Anmeldung und Erstellung einer digitalen Identität) und Identitätsprüfung (Grassi et al. 2017a), Authentifizierung und Lebenszyklusmanagement von Identitäten (Grassi et al. 2017b) und Föderation und Zusicherung (Grassi et al. 2017d). Die dreiteilige Normreihe ISO/IEC 24760 „A framework for identity management" definiert die wesentlichen Begriffe für das Identitätsmanagement, spezifiziert die Kernkonzepte von Identität und Identitätsmanagement sowie Beziehungen zueinander und definiert praxisorientierte Handlungsempfehlungen zum Umgang mit Identitätsmanagementsystemen (Norm ISO/IEC 24760-1; Norm ISO/IEC 24760-2; Norm ISO/IEC 24760-3). Sie definiert zudem die Anforderungen an die Zuverlässigkeit für die Erstanmeldung der erforderlichen Identitätsinformationen zur Schaffung einer digitalen Identität.

Zudem werden Bedingungen und Abläufe zur Aktivierung einer Identität, zur Pflege einer Identität (z.B. Überprüfung der Genauigkeit und Richtigkeit von Identitätsinformationen), und für die Anpassung der Identitätsinformationen einer Entität definiert. Die Aussetzung (Suspendieren) einer Identität, die Identifizierung zur Reaktivierung einer Identität, das

Löschen oder Archivieren einer Identität gehören ebenfalls dazu. Zuletzt werden auch die Verwaltung der Informationen zur Wiederherstellung einer Identität, zu archivierende Informationen, sowie Archivierungszeitraum und Aufbewahrungsbedingungen für eine archivierte Identität und Aufhebung oder Löschung einer Identität beschrieben.

Die technische Spezifikation ISO/IEC 29003:2018 „Information technology - Security techniques - Identity proofing" gibt Richtlinien für den Identitätsnachweis einer Person vor und legt die Stufen der Identitätsprüfung und die Anforderungen zur Erreichung dieser Stufen fest.

An den in diesen teils normativen und teils informationellen Dokumenten dargestellten Prinzipien orientiert sich der Autor bei der Entwicklung des Authentifizierungsverfahrens, das in Kapitel 3.3 behandelt wird.

3.1.3 Authentifizierungsdienste

Aus technischer Sicht lässt sich die Implementierung eines innerhalb eines Authentifizierungssystems genutzten Authentifizierungsdienstes nach dem in Abbildung 3.2 dargestellten internen Modell darstellen. Das Authentifizierungssystem stellt dabei einen Dienst dar, der selbst aus mehreren Diensten bestehen kann und mit mehreren Diensten nach SoA-Prinzip (vgl. Anhang 2.3) kommuniziert.

Der Ablauf einer einfachen Authentifizierung am Beispiel einer Passworteingabe als Authentifizierungsfaktor lässt sich in folgende Schritte einteilen, die auch in Abbildung 3.2 dargestellt sind:

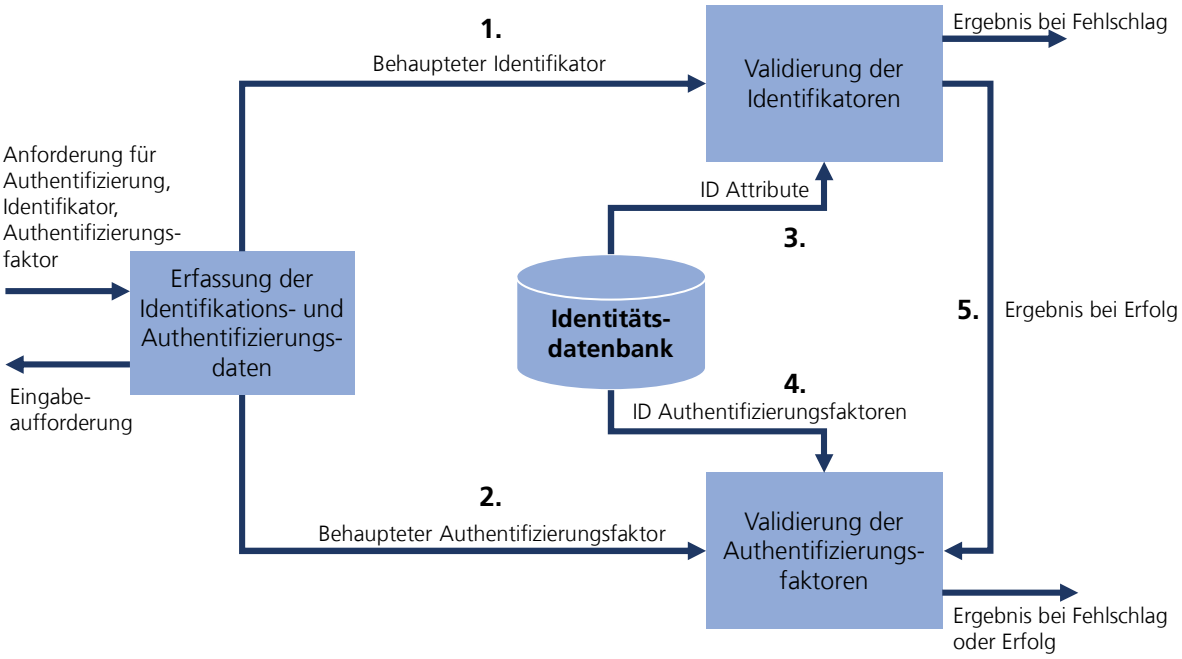


Abbildung 3.2 Aufbau eines Identifikations- und Authentifizierungsdienstes nach (Schumacher 2006, S. 191)

1. Übergabe eines Identifikators, beispielsweise ein Benutzername oder eine eindeutige Identifikationsnummer, die den Bezug der Entität zu einer digitalen Identität herstellt.
2. Übergabe des Passworts, das einen Authentifizierungsfaktor in Form von geheimem Wissen der Entität darstellt.
3. Mittels des behaupteten Identifikators wird versucht die Identität zu ermitteln. Falls dies erfolgreich ist, ist die Authentisierung erfolgt und die Authentifizierung wird eingeleitet.
4. Mittels des behaupteten Authentifizierungsfaktors wird die behauptete Identität mit der ermittelten Identität abgeglichen.
5. Ist der Abgleich des behaupteten Authentifizierungsfaktors erfolgreich, ist auch die Authentifizierung der Entität abgeschlossen.

3.1.4 Authentifizierungsfaktoren

Authentifizierungsverfahren können unterschiedlichen Anforderungen genügen, die davon abhängen, wie diese implementiert sind. Die Assurance Levels (LoA) für Authentifizierung und die Kriterien und Richtlinien zur Erreichung jedes der vier Niveaus definiert die ISO/IEC 29115 (Norm ISO/IEC 29115):

Tabelle 3 LoA (Level of Assurance) Ausprägungen und Bedeutung nach (Norm ISO/IEC 29115)

LoA	Vertrauen in die behauptete Identität	Kontrollmittel
1: low	Geringes oder keines	Selbstbehauptung
2: medium	Etwas	Identitätsnachweis durch Verwendung von Identitätsinformationen aus einer zuverlässigen Quelle
3: high	Hoch	Identitätsnachweis durch Verwendung von Identitätsinformationen aus einer maßgeblichen Quelle und Verifikation der Identitätsinformationen durch Zugehörigkeit zur Entität
4: very high	Sehr hoch	Identitätsnachweis durch Verwendung von Identitätsinformationen aus mehreren zuverlässigen Quellen und Überprüfung der Identitätsinformationen durch Zugehörigkeit zur Entität (und persönlich bezeugte Entität im Fall einer Person)

Als zuverlässige Quelle gilt eine Repository, die als genaue und aktuelle Informationsquelle anerkannt ist (Norm ISO/IEC 29115). Die Identitätsinformationen setzen sich aus Authentifizierungsfaktoren zusammen. Wie in Abschnitt 2.4.2 bereits dargestellt sind die grundsätzlichen Arten von Authentifizierungsfaktoren Wissen der Entität, ein Gegenstand, den die Entität besitzt, oder die Entität und ihre Merkmale selbst. Insbesondere seit der Verbreitung mobiler Endgeräte wird auch vermehrt als vierter Faktor der Standort einer Entität übermittelt. Das Endgerät kann hierbei als PAD (Abbildung 3.1) fungieren. Im Fall eines CPS kann dieses auch mit dem PAD vereint sein. Die Stärke der Authentifizierung hängt sowohl von der Anzahlt als auch von der Art der Authentifizierungsfaktoren ab (Norm ISO/IEC 29115). Tabelle 4 gibt eine Übersicht der aktuell geläufigen biometrischen Authentifizierungsfaktoren.

Tabelle 4 Biometrische Authentifizierungsfaktoren (Abschnitt 4.2.1.1) nach (Ometov et al. 2018)

Faktor	Universalität	Einzigartigkeit	Erfassbarkeit	Robustheit	Akzeptanz	Fälschungssicherheit
Passwort	--	Niedrig	Hoch	Hoch	Hoch	Hoch
Token	--	Mittel	Hoch	Hoch	Hoch	Hoch
Stimme	Mittel	Niedrig	Mittel	Niedrig	Hoch	Hoch
Gesicht	Hoch	Niedrig	Mittel	Niedrig	Hoch	Mittel
Augen	Hoch	Hoch	Mittel	Mittel	Niedrig	Hoch
Fingerabdruck	Mittel	Hoch	Mittel	Hoch	Mittel	Hoch
Handgeometrie	Mittel	Mittel	Mittel	Mittel	Mittel	Mittel
Standort	--	Niedrig	Mittel	Hoch	Mittel	Hoch
Venen	Mittel	Mittel	Mittel	Mittel	Mittel	Mittel
Wärmebild	Hoch	Hoch	Niedrig	Mittel	Hoch	Hoch
Verhalten	Hoch	Hoch	Niedrig	Niedrig	Niedrig	Niedrig
Beam-Forming	--	Mittel	Niedrig	Niedrig	Niedrig	Hoch
Insassenklassifizierungssystem	--	Niedrig	Niedrig	Niedrig	Niedrig	Mittel
Elektrokardiografie (EKG)	Niedrig	Hoch	Niedrig	Mittel	Mittel	Niedrig
Elektroenzephalografie (EEG)	Niedrig	Hoch	Niedrig	Mittel	Niedrig	Niedrig
Desoxyribonukleinsäure (DNS)	Hoch	Hoch	Niedrig	Hoch	Niedrig	Niedrig

Diese Faktoren sind direkt auf CPS übertragbar, teilweise jedoch nur im übertragenen Sinne. Da ein CPS nach aktuellem Stand der Technik nicht über organische Komponenten verfügt, können statt der biometrischen Faktoren entweder automatische Identifikationsverfahren eingesetzt werden oder Fingerprinting. Dies sind beispielsweise die Physische nicht klonbare Funktionen (PUF), die mittels Hardware-Fingerprinting erfasst werden (Abschnitt 4.2.2.4). Diese eigenen sich bei passiven Verfahren auch insbesondere für Komponenten, die über sehr knappe Ressourcen verfügen und somit keine komplexen Self-X-Fähigkeiten aufweisen oder kryptographische Verfahren nutzen können (Kirkpatrick et al. 2009).

3.1.5 Einfache und starke Authentifizierung

Die einfachste Form der Authentifizierung ist die Ein-Faktor-Authentifizierung (Single-Factor Authentication SFA), die in Abschnitt 3.1.3 am Beispiel einer Passwortabfrage dargestellt wurde. Eine weitere Form der Authentifizierung, die Zwei-Faktor-Authentifizierung (Two-Factor Authentication - 2FA), setzt zwei unabhängige Faktoren zur Authentifizierung ein. 2FA gilt somit auch als starke Authentifizierung, da sie einen verlässlicheren Identitätsnachweis darstellt (vgl. Tabelle 3). Bekannte Anwendungsbeispiele aus dem Alltag hierfür sind Bankkarten, die zusammen mit einem PIN genutzt werden, die Identitätsbestätigung beim Login mit einmalig nutzbaren Codes, die dem Nutzer per SMS zugesandt werden (auch Zwei-Schritt Verifikation genannt) oder das TAN-Verfahren bei Online-Überweisungen. Ein weiteres Beispiel für eine 2FA ist die Zertifikat-basierte Authentifizierung, die im folgenden Abschnitt 3.1.6 eingeführt wird.

Komplexere Authentifizierungsmethoden für Personen sind im Alltag selten und ungewöhnlich, da mit steigender Anzahl der Authentifizierungsfaktoren die Komplexität steigt und somit die Handhabbarkeit für menschliche Anwender sinkt (vgl. Infosec-Triaden Abbildung 1.3). Die Prämisse für den in dieser Ausarbeitung verfolgten Ansatz ist jedoch, dass eine beliebig große – oder zumindest mittels Self-X und Nutzung verfügbarer Daten wirtschaftlich darstellbare – Anzahl von Authentifizierungsfaktoren für ein CPS mit ausreichenden Ressourcen und Self-X-Fähigkeiten keine Einschränkung darstellt.

3.1.6 Zertifikatbasierte Authentifizierung und PKI

Die Zertifikat-basierte Authentifizierung stellt eine starke Authentifizierung dar, da sie zwei Authentifizierungsfaktoren (Wissen und Besitz) verwendet und zudem mit kryptographischen Methoden und asymmetrischer Verschlüsselung arbeitet (Meinel et al. 2014, S. 43). Die meistverbreitete Variante basiert auf dem X.509 Public Key Infrastructure (PKI) Standard (Norm ITU-TX.509; Norm ISO/IEC 9594-8).

Das Zertifikat stellt einen Besitz-Faktor dar und ist an einen öffentlichen Schlüssel und zu diesem passenden privaten Schlüssel gebunden, der einen Wissens-Faktor darstellt. Nachrichten werden mittels des öffentlichen Schlüssels verschlüsselt und können nur mit dem zugehörigen privaten Schlüssel entschlüsselt werden, was die Vertraulichkeit der übermittelten Nachrichten sicherstellt. Die Authentizität und Integrität einer Nachricht kann durch eine Signatur garantiert werden, indem die Nachricht mit dem privaten Schlüssel verschlüsselt und mit dem öffentlichen Schlüssel verifiziert wird.

Die Verteilung der Schlüssel und Zertifikate muss in einer vertrauenswürdigen Infrastruktur stattfinden, daher ist das PKI-Verfahren auch mit hohem Aufwand verbunden. Eine vertrauenswürdige dritte Instanz, die Certification Authority (CA), überprüft Identitäten und bindet sie an erzeugte öffentliche kryptographische Schlüssel. Das Zertifikat stellt dann diese Verbindung aus Identität und öffentlichem Schlüssel dar. Diese Abläufe sind in Abbildung 3.3 zusammengefasst.

Die Sicherstellung der Vertrauenswürdigkeit aller Zertifikate ist die Hauptaufgabe der CA. Eine ernannte Registration Authority (RA) stellt dabei durch Policies (Richtlinien) sicher, dass der Antrag für ein Zertifikat tatsächlich von der Person bzw. Entität gestellt wird, die sie vorgibt zu sein. Es wird überprüft ob ihre Merkmale, mit denen der im Zertifikat abgebildeten digitalen Identität übereinstimmen. Im Fall einer Person, kann diese beispielsweise persönlich mittels eines amtlichen Ausweisdokuments ihre Identität bei der RA nachweisen (vgl. LoA4, Tabelle 3).

Zudem muss die CA den Schutz ihres eigenen privaten Schlüssels gewährleisten, da dieser genutzt wird, um die von ihr ausgestellten Zertifikate zu signieren. Ein Angreifer, der in Besitz dieses CA-Schlüssels gelangt, kann mit diesem unautorisierte Zertifikate ausstellen, die von autorisierten nicht zu unterscheiden sind. Entitäten können sich somit missbräuchlich durch eine mittels der CA vermeintlich verifizierten Identität authentifizieren.

Um bei einem Sicherheitsbruch sicherzustellen, dass kompromittierte Zertifikate weiterhin eingesetzt werden oder um die Verwendung abgelaufener Zertifikate zu verhindern, werden Zertifikatsperrlisten (Certificate Revocation List - CRL) verwendet. Zudem können für Echtzeitabfragen Validierungsdienste (Validation Authority, VA) wie das Online Certificate

Status Protocol (OCSP) oder das Server-based Certificate Validation Protocol (SCVP) eingesetzt werden.

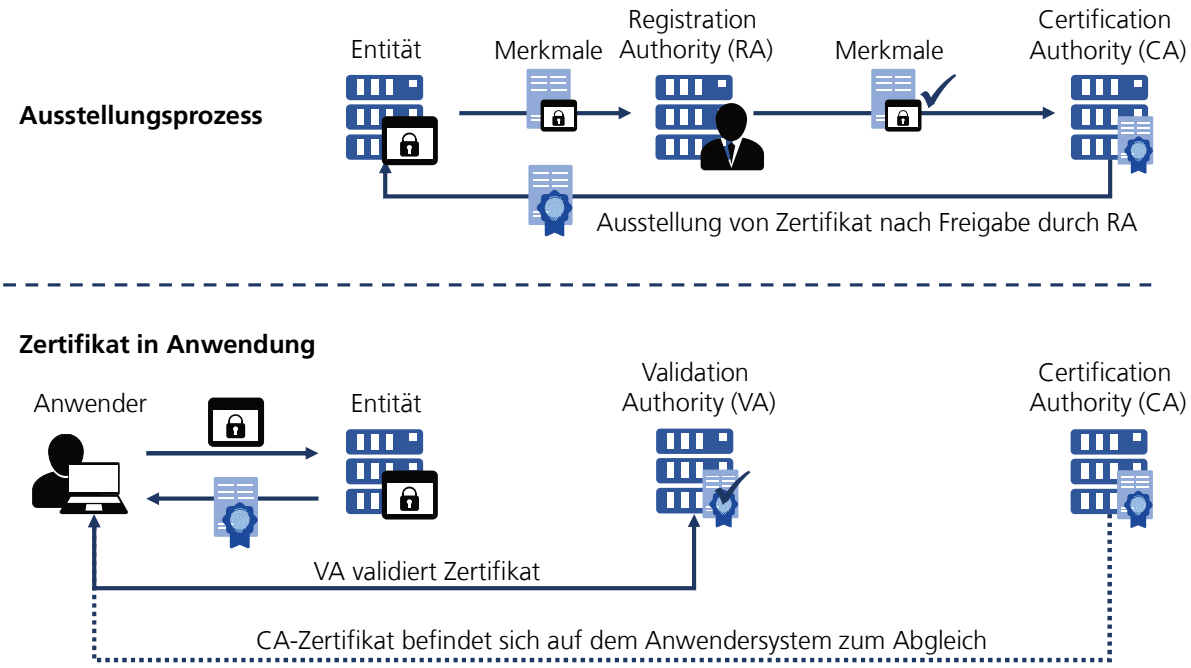


Abbildung 3.3 Prinzip der Zertifikat-basierten Authentifizierung

Eine Entität, die sich authentifizieren möchte, erhält von der angefragten Gegenseite, beispielsweise einem Dienst, einen zufällig generierten Wert übermittelt. Die Entität verschlüsselt diesen Wert mit ihrem geheimen privaten Schlüssel und überträgt die Verschlüsselte Nachricht, das sog. Kryptogramm, zurück an die Gegenseite. Ist diese in der Lage die Nachricht mittels des öffentlichen Schlüssels zu entschlüsseln, ist die Identität der Entität bestätigt und die Identität authentifiziert. Die Authentifizierung geschieht somit durch den Nachweis des Besitzes des zu dem Zertifikat der Entität zugehörigen privaten kryptographischen Schlüssels.

3.1.7 Zwei-Wege- und Multifaktor-Authentifizierung

Im vorherigen Abschnitt wurde Anhand der Authentifizierung in einer PKI dargestellt, die wie Identität einer Entität mittels ihres Zertifikats überprüft werden kann. Möchte man sicherstellen, dass die Gegenseite, z.B. ein angefragter Dienst, auch vertrauenswürdig ist, kann nach dem gleichen Prinzip die Entität die Identität der Gegenseite überprüfen. Diese Variante der Authentifizierung wird als gegenseitige oder Zwei-Wege-Authentifizierung (engl. mutual authentication) bezeichnet. Multifaktor-Authentifizierung (MFA), auch Mehrfaktor-Authentifizierung, folgt demselben Prinzip, wie die 2FA. Genauer gesagt, handelt es sich bei der 2FA um ein Subset der MFA und umgekehrt ist die MFA eine Verallgemeinerung der 2FA, bei der allerdings mehr als zwei Authentifizierungsfaktoren zum Einsatz kommen.

Der Prozess der der MFA ist vergleichbar mit Fingerprinting bzw. Device Fingerprinting im Speziellen (Abschnitt 4.2.2.3). Der Unterschied ist jedoch, dass bei der MFA mehrere temporär getrennte Authentifizierungsfaktoren eingesetzt werden, während beim Fingerprinting (mehrere) distinkte Merkmale eingesetzt werden, um mittels eines oder mehrere Fingerprinting-Algorithmen einen Fingerprint zu erzeugen (Bezawada et al. 2019).

Der Vorteil der MFA liegt hierbei in der höheren Flexibilität und dass die Authentifizierung mit einer höheren Vertrauenswürdigkeit durchgeführt werden kann, da mehrere Faktoren herangezogen werden (Pohlmann 2019, S. 187f; Ross et al. 2003). So können für eine Personen-Authentifizierung z.B. die in Tabelle 8 genannten Verfahren mit den Wissens- und Besitzfaktoren kombiniert werden. Hinzu kommen zusätzliche Faktor-Klassen wie Ort und Zeit (Dasgupta et al. 2017, S. 191) oder weitere in Tabelle 4 gelistete Faktoren.

Die Wirkungsbreite und Flexibilität der MFA bring allerdings auch eine Reihe von Herausforderungen mit sich, die unter anderem in Abbildung 3.4 dargestellt sind.

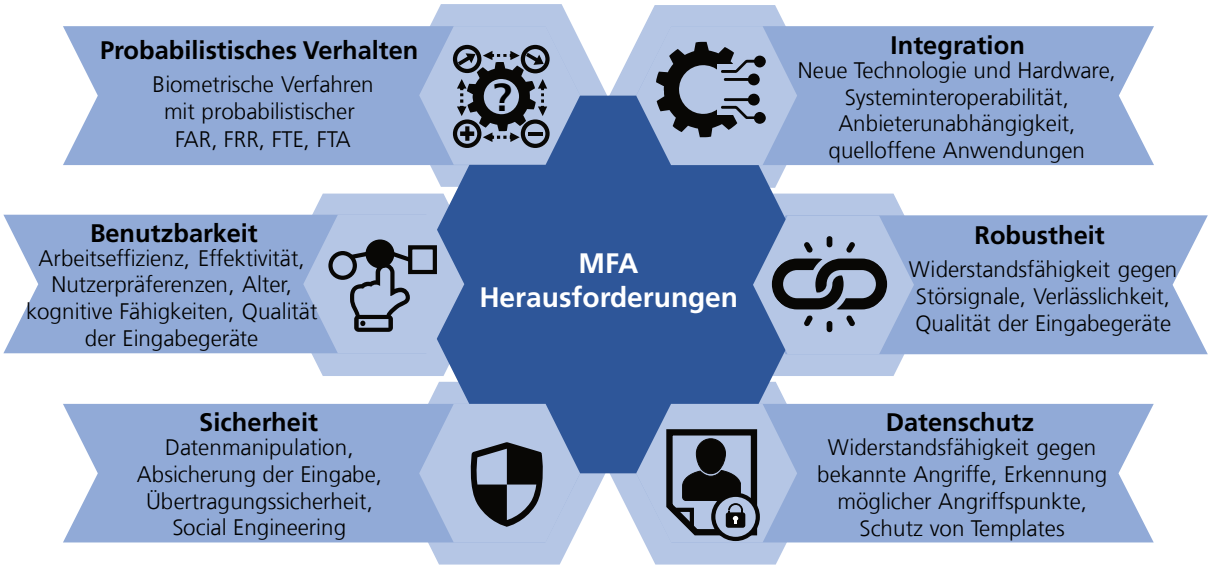


Abbildung 3.4 Herausforderungen der Multifaktor Authentifizierung in Anlehnung an (Ometov et al. 2018)

So ist ein signifikanter Teil der MFA stark von der Biometrie (bzw. Fingerprinting) abhängig und kann aufgrund dieser Eigenschaft als inhärent probabilistisch eingestuft werden (Golfarelli et al. 1997). Hier ist das Problem, dass die Nutzung biometrischer oder Fingerprinting-basierter Verfahren auf einem binären Entscheidungsmechanismus beruht (Jin et al. 2004). Um dieses Problem zu adressieren wurden die Verfahren der statistischen Entscheidungstheorie aus der Authentifizierungsperspektive bereits ausführlich untersucht (Jain et al. 2004; Ratha et al. 2001). Zudem können mittlerweile bewährte Verfahren zur Datenfusion (Castanedo 2013; Ross et al. 2003) und Ansätze des maschinellen Lernern eingesetzt werden, um die jeweiligen Merkmale besser zu erfassen und auszuwerten (Ometov et al. 2018).

Es gibt verschiedene Ansätze, um die Diskrepanz zwischen den aktuell gemessenen Merkmalen und den in den Templates zuvor erfassten und gespeicherten Daten zu kontrollieren. Dies ist einerseits die false accept rate (FAR), also das Verhältnis der Anzahl der falschen Annahmen zu der Anzahl der Identifikationsversuche. Sie ist also das Maß für die Wahrscheinlichkeit, dass das biometrische Sicherheitssystem einen Zugriffsversuch eines

unberechtigten Benutzers fälschlicherweise akzeptiert. (Schroff et al. 2015). Die false reject rate (FRR) wiederum ist das Maß für die Wahrscheinlichkeit, dass das biometrische Sicherheitssystem einen Zugriffsversuch eines berechtigten Benutzers fälschlicherweise zurückweist (Feng et al. 2012). Diese Verfahren lassen innerhalb eines Authentifizierungs-Frameworks eine Parametrisierung der Entscheidungskriterien wie Kosten, Risiken und Nutzen zu. Da es kaum möglich ist wegen der probabilistischen Natur der Verfahren eine FAR oder FRR von Null zu erreichen ist für eine verlässliche MFA hier besondere Umsicht geboten (Ometov et al. 2018). Bei Verfahren, die eine Maschine-Mensch-Interaktion voraussetzen, werden häufig auch noch die Raten-Metriken Failure to Enroll (FTE) sowie Failure to Acquire (FTA) herangezogen, die anzeigen, wie geeignet bestimmte Merkmale für eine Extraktion sind (vgl. Erfassbarkeit und Robustheit; Abschnitt 4.2.1.1) (Raja et al. 2015).

Neben den grundsätzlichen Herausforderungen der IT-, Informationssicherheits- und Datenschutzaspekte ist die Herausforderung biometrischer und vergleichbarer Verfahren wie dem Fingerprinting also die Robustheit einzelner Merkmale zu beachten (Ratha et al. 2004). Werden beispielsweise Versuche in einer Laborumgebung statt im Feld durchgeführt, ist man oft mit anderen Rahmen- und Umgebungsbedingungen konfrontiert. Während eine Spracherkennung beispielsweise in einem stillen Raum sehr zuverlässig funktioniert, so versagt sie oft in einem öffentlichen Umfeld oder ein Produktionshalle und kann einen Benutzer nicht verifizieren. Die Gesichtserkennung benötigt meist ausreichend gute Lichtverhältnisse oder eine überdurchschnittlich Leistungsfähige Kamera (Sariyanidi et al. 2015).

Um diese Inkonsistenz bei der momentanen Erfassung und Extraktion von Merkmalen zu adressieren, kann als Lösungsansatz eine kontinuierliche Überwachung einer Person bzw. Entität verwendet werden, um so Merkmale und ihre Prüfung zeitlich zu entzerren. Dieses Prinzip ist der Ansatz der kontinuierlichen Authentifizierung.

3.1.8 Kontinuierliche Authentifizierung

Die kontinuierliche Authentifizierung, auch aktive Authentifizierung, vereint die Multifaktor-Authentifizierung mit den Ansätzen der biometrischen Verhaltenserfassung bzw. des Device Fingerprintings, mit einem Fokus auf passive Methoden, die die zu authentifizierende Person nicht beeinträchtigen (Dasgupta et al. 2017, S. 238) und Verhaltensmuster erfassen (Guidorizzi 2013). Der Hauptunterschied ist jedoch, dass die Authentifizierung nicht initial abgeschlossen ist, sondern nur ein gewisses Vertrauenslevel und Authentifikationstreue erreicht werden, die mit der Zeit steigen, wenn weitere Prüfschritte erfolgreich sind und Verhaltensmuster umfassender geprüft werden (Guidorizzi 2012). Wird eine Abweichung der erwarteten Verhaltensmuster erkannt, so wird das Vertrauenslevel herabgesetzt und erneut eine neue Reihe verschiedener Authentifizierungsmethoden ausgeführt.

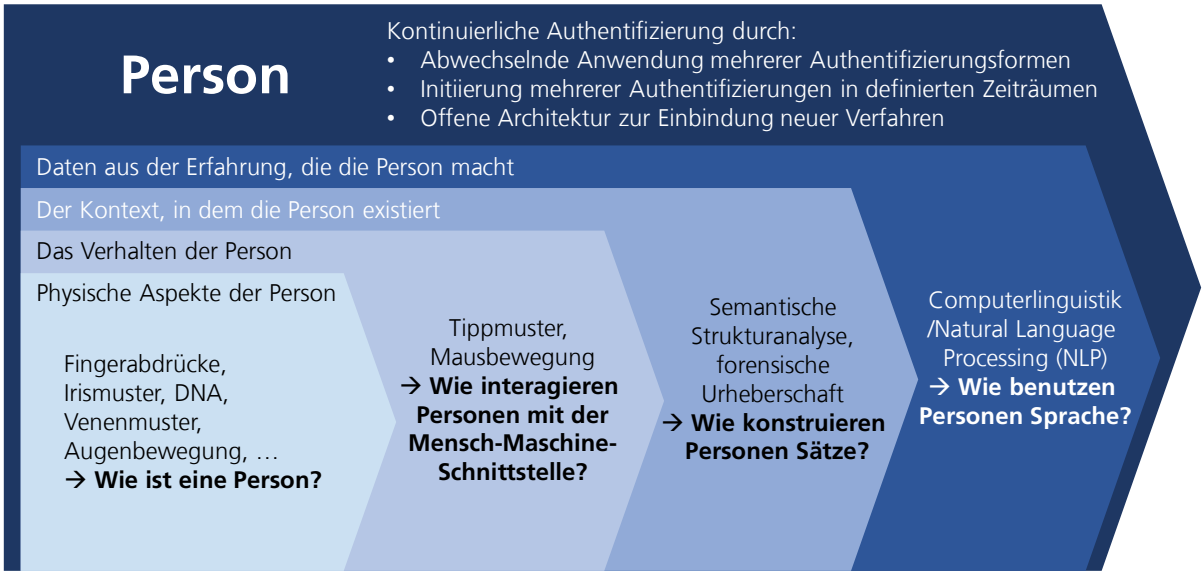


Abbildung 3.5 Prinzipien der aktiven Authentifizierung für Personen in Anlehnung an (Guidorizzi 2012)

Der von der Defense Advanced Research Projects Agency (DARPA) in Abbildung 3.5 verfolgte Ansatz der aktiven Authentifizierung involviert eine Reihe mehrschichtig eingesetzter Technologien, deren Eignung zur Personenidentifikation bereits in zivilen Bereichen erfolgreich eingesetzt werden und in Kombination die Anforderungen militärischer Anwendungen erfüllen. Dedizierte Hardwaresensoren messen ein bestimmtes Merkmal, während Software-Sensoren eine bestimmte Sensorart, beispielsweise eine Infrarot-Kamera, nutzen, um verschiedene biometrische Merkmale zu prüfen und kontinuierlich zu überwachen. Neben dem üblichen Gesichts-, Retina- und Iris Scan, ist dies beispielsweise Augen-Tracking, um charakteristische Augenbewegungen zu erfassen oder Wärmebild-Aufnahmen des Gesichts. Kombination kontinuierlich erfasster Merkmale, beispielsweise Augen-Tracking und Bewegungen des Maus-Cursors sind ebenfalls möglich (Chen et al. 2001). Komplexe Verhaltensmuster wie z.B. der Gebrauch bestimmter Sprachmuster lässt sich mittels der forensischer Urheberschaft von Texten erkennen (Grant 2007). Dieser Ansatz ist vergleichbar mit der Identifikation von Programmierern mittels Code-Beispielen (Abschnitt 4.2.2.2) (Caliskan-Islam et al. 2015; Caliskan et al. 2015).

Tastenanschläge und Gangart bzw. Gangdynamik sind weitere mögliche Faktoren für eine kontinuierliche Authentifizierung (Ayeswarya et al. 2019). Das Berliner Start-Up Nexenio beispielsweise Verknüpft die Daten von Smartphone-Sensoren, die Personen bei sich tragen, um Arbeitnehmer bzw. Mitarbeiter anhand ihres Laufstils zu identifizieren (Bath 2018).

3.1.9 Anwendung der Authentifizierungsverfahren im Kontext von CPPS

Eine Reihe weiterer Arbeiten befasst sich mit der Benutzererkennung mittels mobiler Endgeräte durch Erfassung von Sensordaten und Interaktionsmuster (Alzubaidi et al. 2016; Centeno et al. 2018; Lalithamani et al. 2017; Sbeyti 2016b; 2016a). Eine umfassende Literaturstudie zur Authentifizierung und Autorisierung im IoT-Umfeld wurde von (Trnka

et al. 2018) durchgeführt. Diese zeigt, dass neben den üblichen klassischen Authentifizierungsfaktoren mit Bezug zu Wissen und Besitz vor allem die durch Sensorik befähigte Kontext-Awareness von IoT-Komponenten in verschiedensten Ausprägungen als zusätzlicher Authentifizierungsfaktor genutzt werden kann.

Gerätebezogene Sensorik, beispielsweise die eines CPS, kann äquivalent unmittelbar genutzt werden, um nicht nur die Charakteristik der Hardware und das Verhalten innerhalb des Systems zu erkennen, sondern auch im Kontext und mit Korrelation seiner Umgebung. Hierzu gehören auch Interaktionen in Form von Prozessen und damit verbundene Daten, Informationen und Wissen (Stock et al. 2019a).

Die Anwendung dieser durch Wearables und Smart Devices gestützten MFA-Verfahren werden von (Ometov et al. 2019) als erweiterte IoT-Anwendungen (Advanced IoT – A-IoT) bezeichnet. Die Einsatzfälle beziehen sich jedoch auf die Extraktion biometrischer Merkmale und das Verhalten der Anwender, das in Korrelation mit den Gerätedaten und den gesammelten Umgebungsdaten ausgewertet wird. Eine Anwendung des konzeptuellen Ansatzes im Produktionsumfeld findet bisher nicht statt. Eine ganzheitliche Lösung im Kontext von CPS unter Einsatz der Self-X-Fähigkeiten wurde bisher nicht umfassend untersucht, sondern nur die punktuellen Einsatzmöglichkeiten der unterschiedlichen Fingerprinting Verfahren und ihre jeweilige Methodik, die in Abschnitt 4.2.2 vorgestellt wurden. In Kombination mit den bestehenden Daten- und Informationsquellen in einer vernetzten Produktion, die in den folgenden Abschnitten im Detail diskutiert werden, und dem vermehrten Einsatz datengetriebener Technologien im Zuge der digitalen Transformation der Produktion zu CPPS mit zukünftig autonomen Fähigkeiten (Stock et al. 2020a) eröffnen sich hier Möglichkeiten, die die Nutzung der diskutierten Ansätze technisch und wirtschaftlich befähigen.

Dies stellt nach Ansicht des Autors der vorliegenden Arbeit die primäre Lücke im Stand der Technik und Wissenschaft dar, die durch das in dieser Arbeit vorgestellte Konzept geschlossen werden soll. Im Kern ist dies der in dieser Ausarbeitung dargelegte Ansatz zur Authentifizierung auf Basis von Selbstbeschreibungsmerkmalen von CPPS.

3.2 Informationsverwaltung in IIoT und CPPS

Wie im Einleitungskapitel dargestellt ist die Verwaltung von Daten ein zentraler Bestandteil zur Beherrschung der Komplexität in einer vernetzten Produktion. Daten entfalten ihren Nutzen und Wert erst, wenn sie mit Bedeutung und Kontext zu Informationen und in Folge zu Wissen werden. Dieses Prinzip wurde als Daten-Informations-Wissens-Modell formuliert (Aamodt et al. 1995, S. 198), das in Form einer Wissenspyramide wie in Abbildung 3.6 abgebildet werden kann (Fuchs-Kittowski 2002) (vgl. Abbildung 1.1). Sowohl Daten, die in wertschöpfenden Prozessen in der Produktion entstehen, als auch Daten, die mittels datengetriebener Technologien verarbeitet werden, befähigen die Self-X-Fähigkeiten von I4.0- Komponenten bzw. CPS und erweitern diese zusätzlich mittels zusätzlicher Fähigkeiten (Heidel et al. 2017, S. 67).

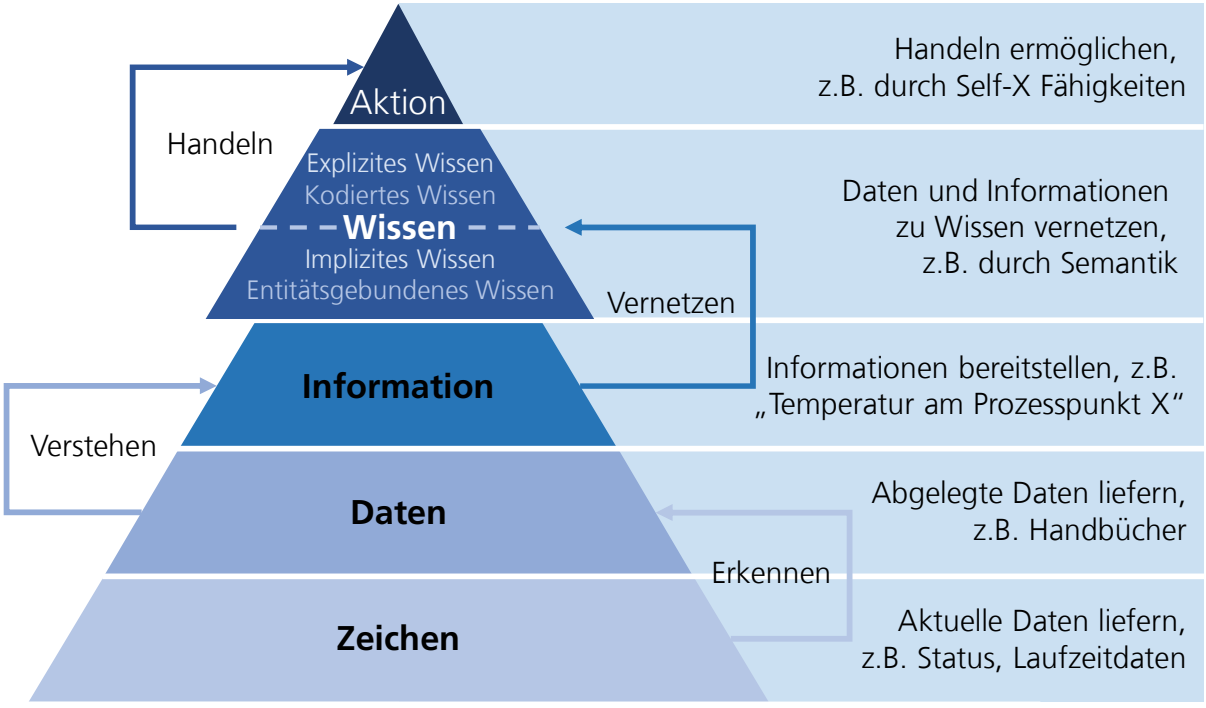


Abbildung 3.6 Die Wissenspyramide in einer vernetzten Produktion in Anlehnung an (Aamodt et al. 1995, S. 198; Fuchs-Kittowski 2002, S. 21; Heidel et al. 2017, S. 67)

Einige der Technologien, die für die Informationsverwaltung in einer vernetzten und datengetriebenen Produktion eingesetzt werden, können ebenfalls für die Extraktion und Verwaltung von Informationen und Wissen (explizit und implizit) aus Merkmalsdaten eingesetzt werden und werden in den folgenden Abschnitten diskutiert. Dabei ist das implizite Wissen das Wissen, das im Gedächtnis eines Individuums gespeichert und daher nicht direkt zugänglich ist. Explizites Wissen ist wiederum kommunizierbar und dokumentierbar, sodass es formalisiert und interpretiert werden kann. Auf ein CPS übertragen handelt es sich hierbei um Daten und Informationen, die einerseits über das CPS bekannt sind oder von diesem kommuniziert werden können. Hierzu gehören auch Daten und Informationen, die ein CPS als Entität in sich trägt und deren Umfang und Bedeutung jedoch erst erschlossen werden müssen.

3.2.1 Wissensrepräsentation - Ontologien für das IIoT

Daten mit Bedeutung zu versehen und so Informationen aus diesen zu gewinnen ist das Forschungsfeld mit dem sich die Semantik (Bedeutungslehre) als Teilgebiet der Linguistik befasst. Semantik versucht Konzepten Bedeutung zu verleihen, was meist mittels Informationsmodellen geschieht, die sich aus Klassen und Klassenattributen zusammensetzen. Die Grundlage hierfür ist das in Abbildung 3.7 abgebildete semiotische Dreieck. Es stellt die Beziehung zwischen einem Ding, einem Symbol, welches das Ding in der Informationswelt repräsentiert und der Bedeutung des Begriffs, der das Ding bezeichnet, dar. Implizit sind Informationsmodelle als Menge von Datenobjekttypen und deren Abhängigkeitsbeziehungen, die gemeinsam ihre Bedeutung definieren, auch als semantische Datenmodelle zu verstehen (Diedrich et al. 2019, S. 15). Ein solches Datenmodell, das die Spezifizierung konkreter oder abstrakter Dinge und der Beziehungen zwischen ihnen in einem vorgegebenen Wissensgebiet beinhaltet, wird als Ontologie bezeichnet (Norm ISO/IEC 19763-3). Während das semiotische Dreieck die Bedeutung von Begriffen oder bspw. in komplexeren Zusammenhängen auch von Satzkonstrukten beschreibt und so eine formale Logik zur Formalisierung diese Beschreibung bereitstellt, konzentriert sich

eine Ontologie auf die inhaltlichen Aspekte. Stuckenschmidt sieht die formale Logik als eine der wesentlichsten Methoden zur Repräsentation von Ontologien. Hier werden primär die Formalismen aus dem Bereich der diskreten Mathematik eingesetzt, um Wissen in seiner expliziten und impliziten Form formal abzubilden. Maschinen bzw. CPS und ihren in Diensten implementierten Algorithmen fehlt aktuell noch das Abstrakte Verständnis über den Zustand und die Geschehnisse in ihrer Umgebung, um befähigt zu werden Schlussfolgerungen zu ziehen und so die menschliche Problemlösungs-kompetenz nachzubilden. Daher ist die formale Darstellung des Wissens die Voraussetzung für eine Automatisierung der semantischen Analyse, die für den Einsatz Künstlicher Intelligenz notwendig ist und im Zuge der Wissensrepräsentation als Teilgebiet der KI entwickelt wird (Stuckenschmidt 2009, S. 27). Die Möglichkeit Schlussfolgerungsregeln aufzustellen erlaubt es so aus Ontologien implizites Wissen über die Welt abzuleiten, sowie automatisch zu überprüfen, ob ein bestimmter Zustand der Welt dem in der Ontologie beschriebenen expliziten Wissen entspricht (Stuckenschmidt 2009, S. 38).

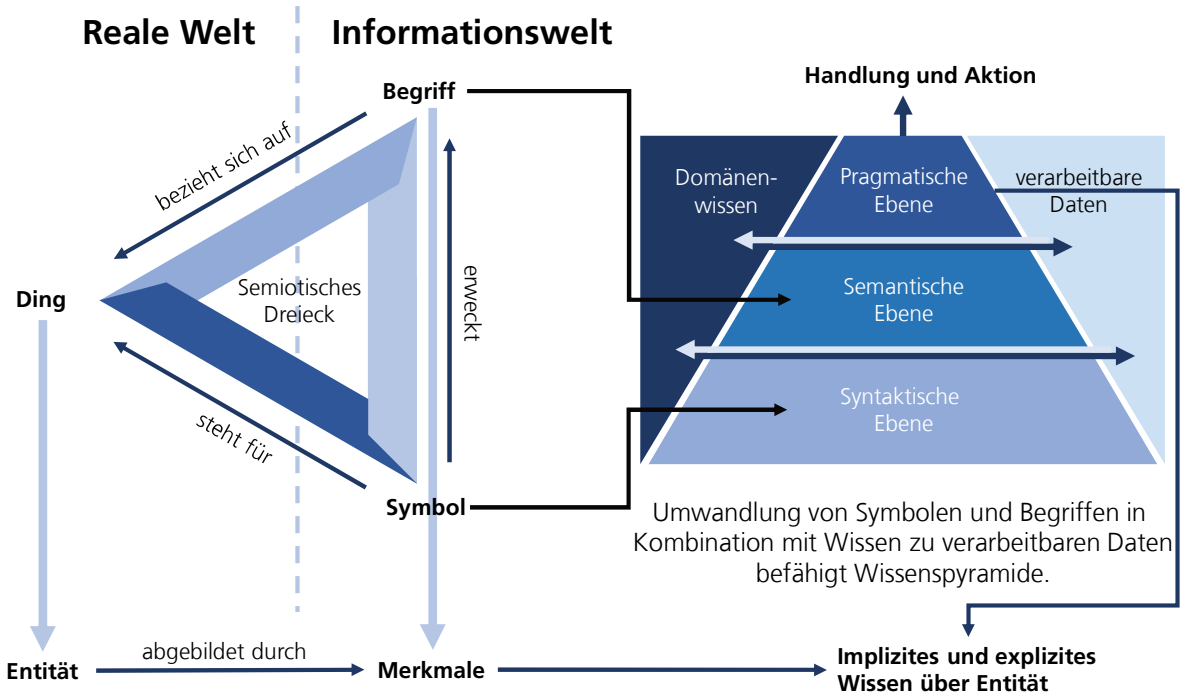


Abbildung 3.7 Semantik und Merkmale in Anlehnung an (Diedrich et al. 2016)

Ein Ansatz Semantik in einer vernetzten Produktion, wie sie beispielsweise Industrie 4.0 und die Informationsebene des RAMI 4.0 vorsieht, ist die Erstellung von Merkmalssystemen (Epple 2011). Dabei werden Merkmale zur Beschreibung der Eigenschaften von Komponenten verwendet. Diese Merkmale können mit einem Informationsmodell unterlegt werden, welches maschinell auswertbar ist (Diedrich et al. 2016). Für Industrie 4.0-Komponenten existiert das Konzept der Verwaltungsschale (siehe Abschnitt 3.2.3) und ein Meta-Informationsmodell, welches beliebige Assets und ihre Eigenschaften mittels definierter Begriffe und Merkmale beschreibt. Über Teilmodelle (siehe Abschnitt 3.2.4) ermöglicht dieser Ansatz beliebige Erweiterungen der Self-X-Fähigkeiten und Detailgrade der Selbstbeschreibung (Barnstedt et al. 2020).

Aufgrund der steigenden Anzahl von Ontologien innerhalb verschiedener Domänen und ihrer Bedeutung für die Interoperabilität von Systemen und Schnittstellen ist es auch eine Bestrebung von Normierungsorganisationen wie der ISO und IEC Standards für die Handhabung von Ontologien im IoT-Umfeld zu schaffen. Ein Beispiel hierfür ist die Norm ISO/IEC 21823-3:2018 - Internet of Things (IoT) - Interoperability for IoT Systems - Part 3: Semantic interoperability (Norm ISO/IEC CD 21823-3).

Ontologien können zur Beschreibung von Sensoren (Xue et al. 2015) oder für die Plug & Play-Fähigkeit von CPS mittels semantischer Komponentenbeschreibungen (Jirkovský et al. 2018) eingesetzt werden. Oft nutzen sie in der Implementierung das Resource Description Framework (RDF), eine Spezifikation der W3C zur konzeptionellen Beschreibung oder Modellierung von Informationen. Nach dem Subjekt-Prädikat-Objekt-Prinzip kann RDF so zur Abbildung von Metadaten verwendet werden und unter anderem in XML- oder JSON-Formate serialisiert werden. Diese Beziehung wird als Tripel bezeichnet und setzt Subjekt und Objekt in Beziehung zueinander. Da diese Beziehungen gerichtet sind, können sie formell nach der Graphentheorie als gerichtete Graphen dargestellt werden. Bei komplexeren Beziehungen, bei denen Objekte und Subjekte mehrere Beziehungen untereinander aufweisen, spricht man von einem semantischen Netz bzw. einem Wissensnetz.

An dieser Stelle ist für den diskutierten Ansatz primär die triviale Beziehung und semantische Anreicherung von Merkmalen relevant, um einem informations-technischen System

die Bedeutung eines Merkmals als Attribut bzw. Datum zu vermitteln. Komplexere Verhalte liegen außerhalb des Umfangs dieser Arbeit.

Eine Ontologie, die zum Ziel hat als Grundlage für IIoT-Systeme zu dienen, ist die oneM2M Base Ontology. Diese wird vom oneM2M-Konsortium entwickelt und zielt darauf ab die Beschreibung vom Sensor, über die Kommunikations-Infrastruktur bis hin zum komplexen Verbund verschiedenster Komponenten zu modellieren (oneM2M 2019). Es existieren auch spezielle Konzepte, wie z.B. eine Ontologie, die explizit für die kontinuierliche Authentifizierung entwickelt wurde (Nespoli et al. 2018).

Ein Informationsmodell zur Selbstbeschreibung von Smarten Objekten und Applikationen in der Produktion wird in (Schel et al. 2018) vorgestellt und in (Stock et al. 2020b) bzw. in der vorliegenden Arbeit um Metadaten erweitert, um z.B. die Modellierung von CPPS abzubilden, die nicht nur die Selbstbeschreibung einzelner Komponenten, sondern auch die Beziehung der Komponenten zueinander voraussetzt.

3.2.2 Selbstbeschreibung von Maschinen und Diensten

Die Selbstbeschreibung von Maschinen und Diensten wird aus Gründen der automatisierten Integration und Interoperabilität benötigt (vgl. Abschnitt 3.2.1), was nur gelingen kann, wenn diese Selbstbeschreibung auch standardisiert, maschinell lesbar, semantisch eindeutig ist und die benötigten Informationen enthält (Bedenbender et al. 2017b, S. 8). Diese Informationen können Gerätehersteller vorab ermitteln und sie auf den Komponenten hinterlegen, die von der Maschinensteuerung oder einem übergelagerten System, wie einem MES, ausgelesen und korrekt interpretiert werden können (Heinze et al. 2015, S. 71). In einer CPS-gestützten Produktionsumgebung ist die Selbstbeschreibungsfähigkeit eine Grundvoraussetzung dafür, dass sich ein CPPS bilden kann (Monostori et al. 2016). AutomationML ist ein Standard, der für eine solche Selbstbeschreibungen eingesetzt werden kann (Norm IEC 62714-1). Eine AutomationML-basierte Selbstbeschreibung für mittels OPC UA vernetzte CPS-Komponenten wird in (Barton et al. 2018) vorgestellt. Ein wei-

terer Ansatz ist die Semantic Sensor Network Ontology (SSN) der W3C, die in RDF abgebildet so auf ein OPC UA Datenmodell gemappt werden kann (Jirkovský et al. 2018). Zudem müssen die Begriffe, die eingesetzt werden, um Merkmale für eine Selbstbeschreibung abzubilden, standardisiert werden. Hierfür wurde vom VDI mit der Richtlinie 5600, Blatt 3, „Fertigungsmanagementsysteme (MES): Logische Schnittstelle zur Maschinen und Anlagensteuerung“ ein Vorschlag erarbeitet (Norm VDI 5600 Blatt 3).

Das Projekt GAIA-X, das die Schaffung einer deutschen bzw. europäische Cloud-Infrastruktur anstrebt, setzt eine Selbstbeschreibung der Infrastruktur-Knoten in Bezug auf deren Spezifika und Fähigkeiten voraus (Ahrens et al. 2019, S. 14). Hierbei setzt es auf den Vorarbeiten des International Data Space Projekts der Fraunhofer Gesellschaft auf, das initial einen Fokus auf der Beschreibung von Datenquellen und Daten zur Schaffung eines geschützten Datenraums zur Erhaltung der Datensouveränität hatte (Otto et al. 2017, S. 27). Ein weiterer Ansatz ist das im Projekt BaSys 4.0 entwickelte BaSyx-Framework, welches auf eine am Verwaltungsschalenkonzept orientierte Selbstbeschreibung von Komponenten setzt (Kuhn et al. 2019b). Ein IIoT-orientierter Ansatz in Kopplung mit einer Middleware wird in (Schel et al. 2018) vorgestellt. Dieser basiert auf der Selbstbeschreibungsfähigkeit von Objekten und Diensten und bildet einen Teil der Grundlage des vorgestellten Konzepts und der prototypischen Implementierung (vgl. Abschnitt 3.2.5, 4.4.1 und 5.1).

3.2.3 Verwaltungsschale als digitale Repräsentation

Das ursprüngliche Konzept einer digitalen Repräsentation wird oft als digitaler Zwilling bezeichnet. Allerding existiert keine eindeutige Definition dazu, wie ein Digitaler Zwilling genau aussieht, welche Rolle er erfüllt und wie genau er implementiert werden soll. Es gibt allerdings eine Reihe von Konzepten, die prinzipiell dem entsprechen, was unterschiedliche Interpretationen eines Digitalen Zwillings sein können (Wagner et al. 2017).

Ein alternatives, jedoch eng verwandtes Konzept, ist die Verwaltungsschale, die im RAMI 4.0 definiert wurde (Anhang 2.5). Diese umgibt jedes relevante Asset in einem Industrie 4.0-System und bildet so mit diesem eine I4.0-Komponente (siehe Abbildung 3.8).

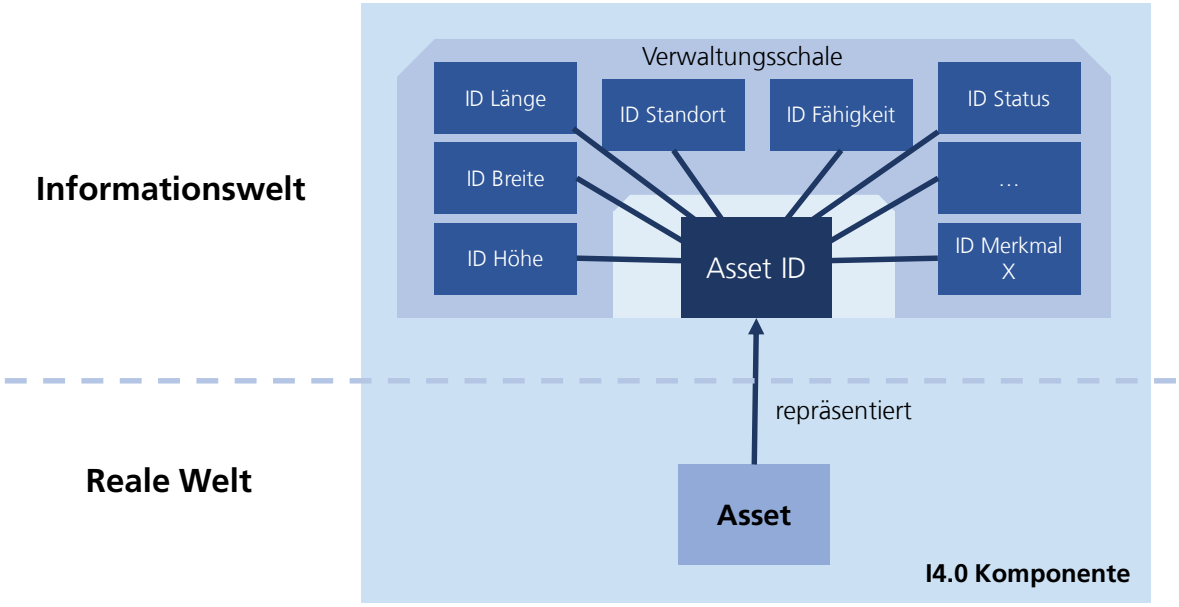


Abbildung 3.8 I4.0 Komponente mit Verwaltungsschale und Merkmalen in Anlehnung an (Bedenbender et al. 2017a)

Während das Asset als physische Komponente in der realen Welt existiert, repräsentiert die Verwaltungsschale dieses in der Informationswelt auf den oberen fünf RAMI-Schichten (Integration, Kommunikation, Information, Funktionen, Geschäftsprozesse) durch definierte Begriffe und Merkmale (Heidel et al. 2017, S. 68).

Die Verwaltungsschale besitzt eine definierte Struktur, die in (Adolphs et al. 2016) vorgestellt wird und in (Barnstedt et al. 2020) um ein Meta-Informationsmodell für diese ergänzt wird. Da die Verwaltungsschale einen essenziellen Teil von I4.0-Komponenten darstellt, müssen sie selbst und die mit ihr verbundenen Konzepte aus Gründen der Interoperabilität auch standardisiert werden. Für die I4.0-konforme Kommunikation (I4.0-Sprache)

zwischen Verwaltungsschalen definieren VDI-Blätter die Nachrichtenstruktur und das Interaktionsprotokoll für die Kommunikation zwischen I4.0-Komponenten bzw. Verwaltungsschalen (Norm VDI/VDE 2193 Blatt 1; Norm VDI/VDE 2193 Blatt 2).

Ein Informationsaustausch in einem I4.0-System setzt voraus, dass Komponenten auch in der Lage sind diesen auszuführen. Jedoch sind nicht unbedingt alle Assets in der Lage dies auch selbst technisch umzusetzen, weshalb eine Verwaltungsschale in drei Ausprägungen bereitgestellt werden kann (Belyaev et al. 2019) (Abbildung 3.9):

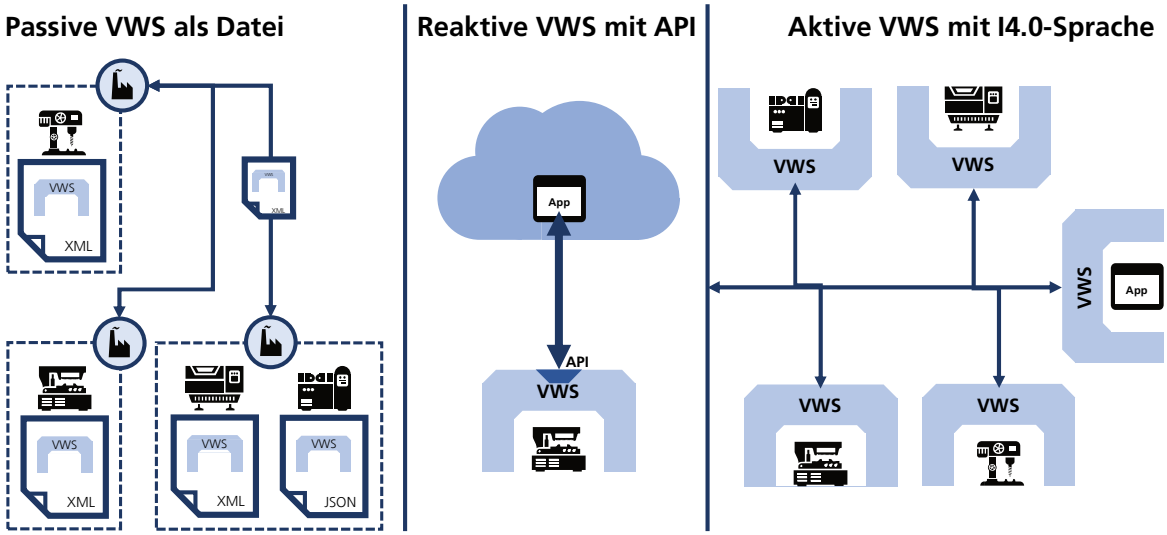


Abbildung 3.9 Verwaltungsschalen-Typen in Anlehnung an (Belyaev et al. 2019)

- Verwaltungsschale als Datei, z.B. im XML- oder JSON-Format nach Informationsmodell-Spezifikation in (Barnstedt et al. 2020).
- Reaktive Verwaltungsschalen stellen ihre Informationen und Funktionen über Dienste mittels API bereit und reagieren auf Aufrufe (zukünftig standardisierte CRUD-orientierte Spezifikation).
- Aktive Verwaltungsschalen verfügen zusätzlich über Entscheidungs- und Optimierungsalgorithmen, die die Grundlage für Self-X-Fähigkeiten und das autonome Verhalten von I4.0-Komponenten bilden.

3.2.4 Verwaltungsschalen-Teilmodelle

Neben den wichtigsten grundsätzlichen Informationen zum Asset beinhaltet eine Verwaltungsschale die Teilmodelle (Bedenbender et al. 2019). Diese ermöglichen es eine Beschreibung mittels Merkmalen, Parametern und Variablen die Eigenschaften und Fähigkeiten eines Assets abzubilden. Dabei kann eine Verwaltungsschale mehrere Teilmodelle beinhalten, die verschiedene fachliche Funktionalität erfüllen können (Abbildung 3.10).

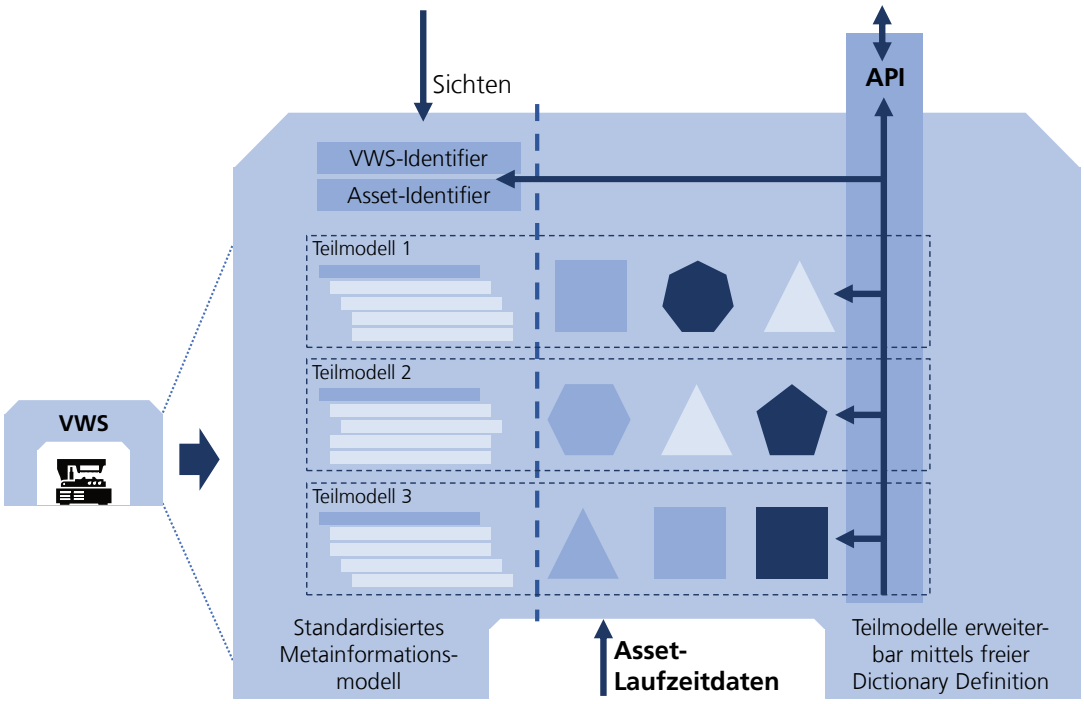


Abbildung 3.10 Verwaltungsschale und Teilmodelle
in Anlehnung an (Bedenbender et al. 2016, S. 5)

Verpflichtende oder optionale Basis-Teilmodelle werden durch Asset-Klassen-spezifische - verpflichtende und optionale Teilmodelle ergänzt. Zuletzt besteht die Möglichkeit freie Teilmodelle zu definieren. Die Teilmodelle selbst können nach bestehenden Standards ausgestaltet werden. So bieten die 61360 CDD- und eCl@ss-Spezifikationen Parameter

von Feldbusprofilen sowie Variablen von OPC UA Companion Specifications an, um Merkmale für Teilmodelle semantisch eindeutig und interoperabel zu definieren und zu instanziieren. Als eine der ersten Implementierungen integriert das BaSyx-Software Development Kit (SDK) das Meta-Informationsmodell und bietet so die Möglichkeit Teilmodelle zu definieren und ausführbar zu machen (Kuhn et al. 2019a).

3.2.5 Daten- und Informationsintegration in einer vernetzten Produktion

Das Verwaltungsschalen-Konzept hat unter anderem das Ziel den Informationsaustausch in Industrie 4.0 Wertschöpfungsnetzwerken zu vereinfachen. Letztendlich ist die technische Umsetzung jedoch offen. Es gibt bewährte Muster, Architekturen und Technologien zur Integration von IoT-Komponenten bzw. Maschinen und Diensten.

Ein verbreiteter Ansatz zur Integration sind Middlewares. Hierzu zählen beispielsweise Enterprise Service Bus Software-Systeme, die dazu eingesetzt werden, um die wachsende Anzahl von IT-Systemen in Unternehmen zentral miteinander zu integrieren, anstatt die Systeme direkt miteinander zu verbinden. Hierzu können auch Konnektoren zählen, die ein flexibles Mapping zwischen den Kommunikations-protokollen in einem IIoT-System erlauben (Faul et al. 2016). Eine auf die Selbstbeschreibungsfähigkeiten von CPS ausgerichtete Middleware-Lösung ist der am Fraunhofer IPA entwickelte Manufacturing Service Bus (MSB) (Schel et al. 2018). Smarte Objekte und Dienste, die sich am MSB registrieren, teilen diesem ihre Selbstbeschreibung mit. Diese kann daraufhin genutzt werden, um Integration Flows zu modellieren und über einen verschlüsselten Kommunikationskanal auszuführen, wie es in Abbildung 3.11 dargestellt ist. Integration Flows verknüpfen kontrolliert die Datenquellen (Events) mit den Datensenken (Operations) der Smarten Objekte und Dienste. Dabei kann mittels der Selbstbeschreibung, die auf der OpenAPI-Spezifikation basiert, das Datenformat der Datenobjekte auf den jeweiligen Endpunkten gemappt und transformiert werden. Durch dieser Modellierung von Daten- und Informationsflüssen

zwischen einfachen CPS in Form von „smarten“ Objekten und Diensten sind Anwender in der Lage höherwertigere CPPS zu modellieren (Stock et al. 2020b).

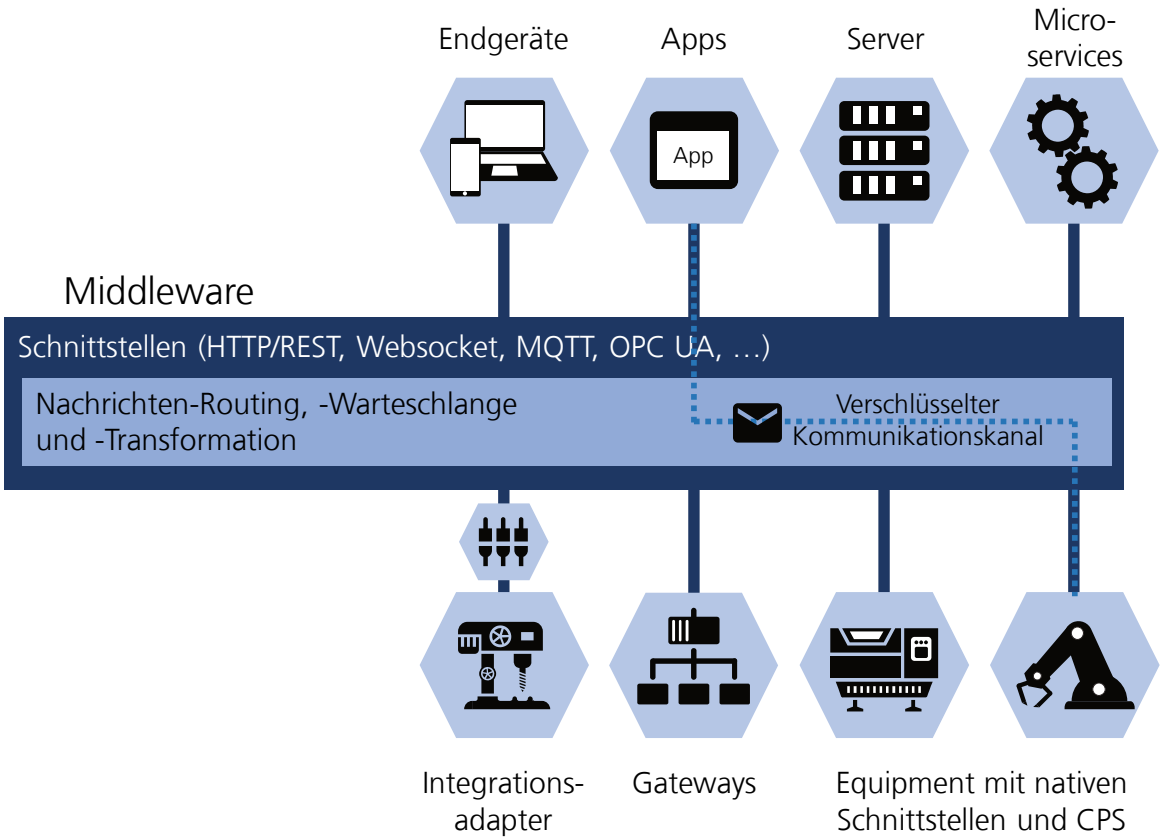


Abbildung 3.11 Middleware-basierte Integration von Maschinen und Diensten in Anlehnung an (Schel et al. 2018)

Ein ganzheitliches Konzept zur Daten- und Informationsintegration und -verarbeitung in der Produktion ist der Digitale Schatten (Bauernhansl et al. 2018). Eine Vorstufe zur Realisierung des Digitalen Schattens stellt der Cyber-Physical Data Access Layer (CPDAL) (Stock et al. 2019b) dar, der auf dem MSB aufsetzt. Dieses Konzept nutzt die Selbstbeschreibungsfähigkeiten der Dienste und smarten Objekte bzw. CPS, die selbst als Datenquellen fungieren sollen, anstatt eines Data Warehouses (DW) oder Data Lakes (DL). Der Hauptunterschied hier liegt hier in der Art und Weise wie mit Rohdaten umgegangen

wird, um effizient Zugriff auf diese in der benötigten Form zu erhalten und ist schematisch in Abbildung 3.12 dargestellt. Für DW wird im Vorfeld in Abstimmung mit den Business-Anforderungen ein zentrales Schema für Daten festgelegt, um diese bei Bedarf in der exakt benötigten Form zu erhalten. Hierzu werden die Daten aus den Datenquellen periodisch abgefragt und in dieses zentrale Schema übertragen.

Im Gegensatz dazu speichern DL unstrukturierte oder nur teilweise strukturierte Daten nach dem am Schema-on-Read-Prinzip, d.h. die Rohdaten werden extrahiert, geladen und in ein Schema bzw. eine Struktur transformiert (ELT), die für die Abfrage benötigt wird. DWs hingegen verwenden das Schema-auf-Schreib- bzw. Extraktions-, Transformations- und Ladeprinzip (ETL), bei dem die Daten strukturiert werden müssen, bevor sie in einer Datenbank gespeichert werden können. ELT ist essenziell für Data Scientists, die Daten meist in Rohform benötigen, da die Daten im ETL nur noch in ihrer vorverarbeiteten Form vorhanden sind und sich an Endanwender richten.

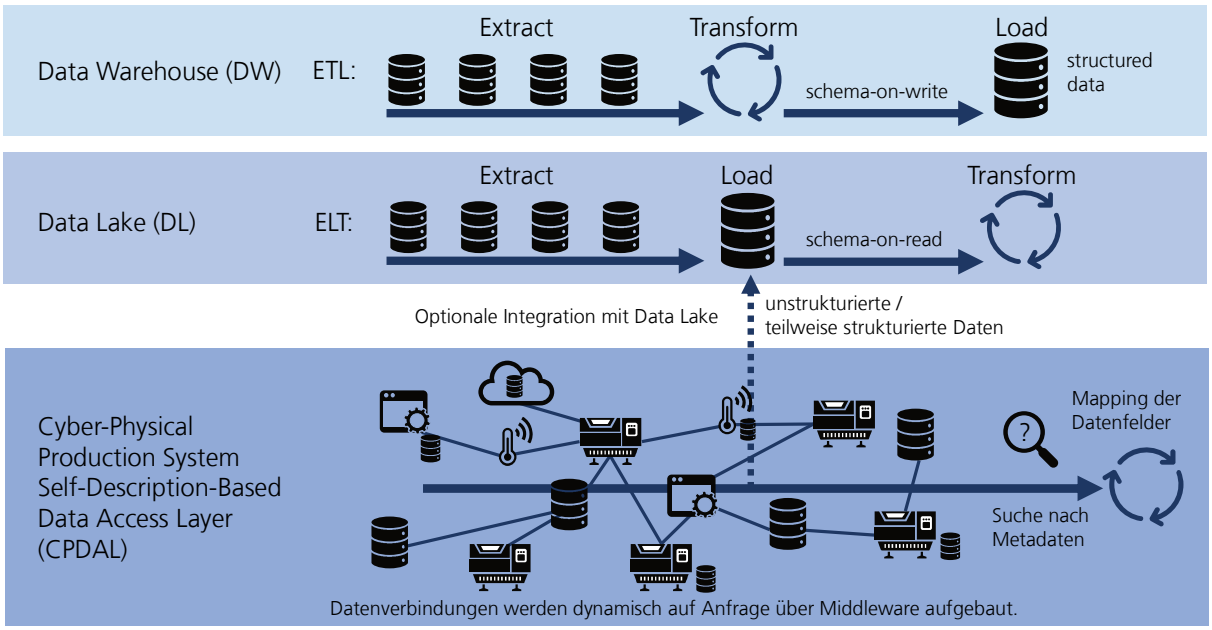


Abbildung 3.12 Konzept einer Selbstbeschreibungs-basierten Datenzugriffsschicht für CPPS nach (Stock et al. 2019b)

Der CPDAL wählt einen Weg, bei dem im Prinzip jede Datenquelle direkt erreichbar ist, jedoch Daten durch die Selbstbeschreibung immer mit Meta-Informationen versehen sind. Die Meta-Informationen zu den Datenquellen sind durchsuchbar zentral abgelegt, vergleichbar mit einer Registry, wie sie auch für Verwaltungsschalen eingesetzt wird. Bei Bedarf wird eine Zugriffsanfrage auf bestimmte Daten gestellt und über den MSB oder einen Daten-Proxy eine Datenverbindung vermittelt. Die Struktur und das Format der Daten kann durch die Selbstbeschreibung der Datenquelle und -senke über den MSB gemappt oder durch die bekannte Selbstbeschreibung der Datenstruktur in der Endanwendung verarbeitet werden. Sicherzustellen, dass die anfragenden Entitäten und die Datenquellen-Entitäten auch diejenigen sind, die sie vorgeben zu sein, ist die primäre Motivation und der Hauptbeitrag dieser Arbeit. Hierzu sollen unter anderem die in diesem Kapitel beschriebenen Ansätze und Konzepte adaptiert und genutzt werden.

3.3 Zusammenfassung und Analyse des Stands der Technik

Die in diesem Kapitel vorgestellten existierenden Ansätze und Technologien aus dem Bereich der Identifikation, Fingerprinting, Authentifizierung und Informationsverwaltung bilden in Teilen die Grundlage des hier zu entwickelnden Ansatzes. Jedoch erfüllen sie für sich alleinstehend nicht die Anforderungen, die eine Authentifizierung auf Basis von Selbstbeschreibungsmerkmalen von CPPS voraussetzt.

Bestehende Identifikationsverfahren verwenden keine Self-X-Fähigkeiten von CPPS, die über den Einsatz fester künstlicher Identifikatoren hinaus gehen. Die Möglichkeit Merkmale zur Identifikation heranzuziehen, wird bei Objekten mittels statischer Merkmale umgesetzt. Dynamische Merkmale werden vereinzelt nur bei menschlichen Anwendern verwendet, da sie aufwendiger handzuhaben oder nicht zumutbar sind für Menschen.

Authentifizierung wird im Kontext menschlicher Nutzer in den meisten Anwendungen daher auf zwei Faktoren begrenzt. Bei Maschinen kommt entweder eine einfache Authentifizierung mit starken Passwörtern zum Einsatz oder aber es werden Zertifikate bzw. Hardware-Token als zweiter Faktor verwendet. Eine Multi-Faktor Authentifizierung in

Kombination mit menschlichen Nutzern und mobilen Geräten existiert bereits, jedoch nicht im Kontext von CPPS.

Die breite Anzahl der verschiedenen Ansätze des Fingerprintings impliziert eine große Anzahl möglicher Merkmale, die zur Identifikation und Authentifizierung herangezogen werden können. Allerdings werden die jeweiligen Ansätze für sich alleinstehend betrachtet. Eine ganzheitliche Lösung die verschiedenartigen Verfahren zusammen-zuführen und strukturiert für eine Authentifizierung einzusetzen existiert bisher nicht. Ansätze zur Selbstbeschreibung von Objekten und Diensten bzw. CPPS werden bereits verwendet, werden jedoch nicht zur Bestimmung eindeutiger Merkmale bzw. zur Erstellung sicherer Identitäten und Authentifizierung eingesetzt. Diese Arbeit hat zum Ziel hier einen ganzheitlichen Ansatz zu entwickeln und diese Lücken zu schließen.

Tabelle 5 listet eine Übersicht der konventionellen Ansätze zur Authentifizierung im Vergleich zum vorgeschlagenen selbstbeschreibungsmerkmalbasierten Ansatz für CPPS. Die dargestellten Kriterien sind im Folgenden definiert:

- Sicherheit
- Anzahl Faktoren
- Faktorarten
- Infrastruktur
- Merkmalsprüfung
- Merkmalsdynamik
- Komplexität
- Komplexitätskapselung
- Funktionale Skalierbarkeit
- Self-X

Tabelle 5 Übersicht konventioneller Authentifizierungsverfahren und des vorgeschlagenen Ansatzes

	Konventionelle Ansätze						Vorgeschlagener Ansatz
	1-Faktor	2-Faktor		Multi-Faktor			
	Benutzername und Passwort	2-Faktor Authentifizierung	HW-Token / Dongle	SW-Token / Zertifikat	Biometrische Authentifizierung	Hylemetrische Authentifizierung	Device Fingerprinting	Selbstbeschreibungsbasierte Authentifizierung (Self-X)
Sicherheit	Niedrig	Mittel	Hoch	Mittel	Niedrig-Hoch	Niedrig-Hoch	Niedrig-Hoch	Mittel-Hoch
Anzahl Faktoren	1	2	2	2	n (1, wenige)	n (1, wenige)	n (1, wenige)	n (2, viele)
Faktorarten	Wissen	Wissen, Besitz	Wissen, Besitz	Wissen, Besitz	Sein, Verhalten	Sein, Verhalten	Sein, Verhalten	Wissen, Besitz, Sein, Verhalten
Infrastruktur	Benutzer-Datenbank	Benutzer-Datenbank	PKI	PKI	Template-Datenbank	Template-Datenbank	Template-Datenbank	Selbstbeschreibungs-Datenbank und Template-Datenbank
Merkmalsprüfung	zentral	zentral	zentral	zentral	zentral	zentral	zentral	dezentral
Merkmalsdynamik	statisch	statisch	statisch	statisch	statisch / dynamisch	statisch / dynamisch	statisch / dynamisch	statisch / dynamisch
Komplexität	Niedrig	Mittel	Mittel	Mittel	Hoch	Hoch	Hoch	Hoch
Komplexitätskapselung	Niedrig	Niedrig	Niedrig	Niedrig	Mittel	Niedrig	Niedrig	Hoch
Funktionale Skalierbarkeit	-	-	-	-	Niedrig	Niedrig	Mittel	Hoch
Self-X	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Ja

4 Konzeption eines Authentifizierungsverfahrens

Das Umfeld der vernetzten Produktion, seine Herausforderungen und Risiken, die Konzepte von CPS und ihren Self-X-Fähigkeiten, sichere Identitäten, Merkmalsdifferenzierung von Entitäten und die Prinzipien der Authentifizierung wurden in Kapitel 2 eingeführt und sind im Detail in Anhang 2 und Anhang 3 weiter ausgeführt. Die in diesem Zusammenhang relevanten Methoden und Technologien nach Stand der Wissenschaft und Technik wurden daraufhin in Kapitel 3 vorgestellt. In diesem Kapitel soll nun das Konzept der Authentifizierung mittels der Selbstbeschreibungsmerkmale von CPPS eingeführt und erläutert werden, um so die im Stand der Technik identifizierten Lücken zu schließen (vgl. Abschnitt 3.3).

4.1 Vorgehen zur Entwicklung des Ansatzes

Die aktuell existierenden Ansätze zur Identifikation und Authentifizierung mittels sicherer Identitäten haben einen Fokus auf menschliche Entitäten, also Personen. Das Prinzip des in diesem Kapitel vorgestellten Authentifizierungskonzepts und dargestellten Verfahrens basiert jedoch darauf, die CPS-Eigenfähigkeiten zur Identifikation und Authentifizierung von CPPS zu nutzen. Hierfür werden die vorgestellten existierenden Ansätze aus den Themengebieten der Identifikation, der Authentifizierung und des Fingerprinting aufgegriffen, integriert und adaptiert.

4.1.1 Zieldefinition

Primäres Ziel dieser Arbeit ist es darzustellen, wie Selbstbeschreibungsmerkmale genutzt werden können, um CPS in ihrer Ausprägung als CPPS zu authentifizieren (F1.1). Hierbei

wird grundsätzlich angenommen, dass sämtliche Merkmale eines CPPS über seine Selbstbeschreibungsmerkmale explizit und implizit abgeleitet werden können, da sie die Basis eines Authentifizierungsverfahrens bilden.

Hierzu muss zu Beginn geklärt werden, was genau (Selbstbeschreibungs-)Merkmale sind, wie diese beschaffen sind und welche Merkmalsquellen existieren. Die in Abschnitt 4.2.2 dargestellte Übersicht der Ansätze zur Erfassung von Merkmalen und Identifikation mittels dieser zeigt die hohe Komplexität, Vielfalt und stetige Wandlung der hierfür einsetzbaren Technologien. Daher wird in den folgenden Abschnitten ein Verfahren aufgezeigt und keine spezifische und definitive Authentifizierungslösung, die eine Abhängigkeit von einer bestimmten Technologie aufweist. Der Autor ordnet die Arbeit als im Entstehen begriffene Designtheorie ein und will Wissen über Funktionsprinzipien bzw. eine Architektur vermitteln. Hierzu gehören Konstrukte, Methoden, Konstruktionsprinzipien und technologische Regeln (vgl. Tabelle 6).

Tabelle 6 Design Science Forschungsbeitragsarten nach (Gregor et al. 2013, S. 342)

	Beitragsart	Beispielartefakt
Abstrakteres, vollständigeres und ausgereifteres Wissen	Stufe 3. Gut entwickelte Designtheorie über eingebettete Phänomene.	Designtheorien (mittlere und große Theorien)
↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑ ↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓	Stufe 2. Entstehendes Designtheorie-Wissen als Funktionsprinzipien /Architekturen.	Konstruktionen, Methoden, Modelle, Konstruktionsprinzipien, technologische Regeln.
Spezifischeres, begrenztes und weniger ausgereiftes Wissen	Stufe 1. Situierte Implementierung eines Artefakts.	Instanziierungen (Softwareprodukte oder implementierte Prozesse).

Hierzu werden methodische Ansätze zur Bestimmung, Klassifizierung bzw. Typisierung von Selbstbeschreibungsmerkmalen eingeführt. Zudem wird beschrieben, wie basierend auf diesen Merkmalen ein Authentifizierungsverfahren für CPPS durchgeführt werden kann. Die allgemeine Beschreibung eines technologischen Artefakts zur Umsetzung des Ansatzes wird ebenfalls entwickelt. Abgeleitet aus dieser wird die spezifische Umsetzung

dieses Artefakts und der Teilartefakte in Form ausgewählter Merkmale und Merkmalsprüfungsverfahren zum Zweck der Validierung.

Gesamtheitlich wird somit ein Framework dargestellt, das eine Anleitung gibt, wie (Selbstbeschreibungs-) Merkmale in einem CPPS zur Authentifizierung eingesetzt werden können und welche Komponenten hierzu benötigt werden.

Die technische Ausprägung dieser verschiedenen Komponenten ist hierbei nachrangig, da diese austauschbar und erweiterbar sein sollen. Insbesondere die Methoden, die zur Prüfung von Merkmalen eingesetzt werden können, beginnen bei einfachen Verfahren, wie beispielsweise einem Abgleich von Werten in Form von alphanumerischen String-Werten oder reinen numerischen Werten. Allerdings können auch aufwendige Verfahren eingesetzt werden, insbesondere in Hinblick auf komplexe Merkmale. Hier sind Verfahren des maschinellen Lernens oder sogar schwache KI-Systeme vorstellbar, die für die Erkennung komplexer Muster eingesetzt werden können. Die spezifischen Prüfverfahren werden daher nur oberflächlich behandelt, da sie nicht zentraler Betrachtungsgegenstand der vorliegenden Ausarbeitung sind und auch den Umfang dieser überschreiten würden.

Als Instanz zur Demonstration und Validierung des Ansatzes dient in Folge eine beispielhafte Technologie-abhängige Implementierung. Mit dieser wird ein Authentifizierungsverfahren für CPPS und seinen Komponenten mit ausgewählten Technologien dargestellt, getestet und validiert. Dieser Ansatz wurde gewählt, da das Artefakt, das entwickelt wird, rein technisch ist und nur teilweise von Menschen benutzt wird bzw. Menschen nicht direkt betrifft. Der Bedarf oder das Problem, das mit dem Entwurf angesprochen wird, besteht zwar heute schon, kann jedoch nicht unter Nutzung seines vollen Potenzials eingesetzt werden, da CPPS in ihrer reinen Definition noch nicht existieren und viele Befähiger-Technologien aktuell im Entstehen sind. Das Artefakt ist daher rein technisch und es wird auch diese rein technische Strategie für eine Evaluierung gewählt. Dies ist notwendig, da keine Notwendigkeit für eine Nutzung durch Menschen besteht und da reale Nutzer und räumliche Gegebenheiten nicht zugänglich sind (oder nicht existieren), sodass eine naturalistische Bewertung unmöglich ist (Venable et al. 2016).

4.1.2 Grundprinzip des Ansatzes und Struktur

In den weiteren Abschnitten dieses Kapitels soll der methodische Weg zum Aufbau des Authentifizierungsframeworks dargestellt werden. Zudem wird der Bezug zu den fachlichen Inhalten der Kapitel 2 und 3 und den Forschungsfragen in Kapitel 1 hergestellt. Abbildung 4.1 zeigt eine Übersicht, die das Vorgehen zur Entwicklung des Ansatzes gesamtheitlich skizziert und die Bausteine in Bezug zu den inhaltlichen Abschnitten dieser Arbeit setzt.

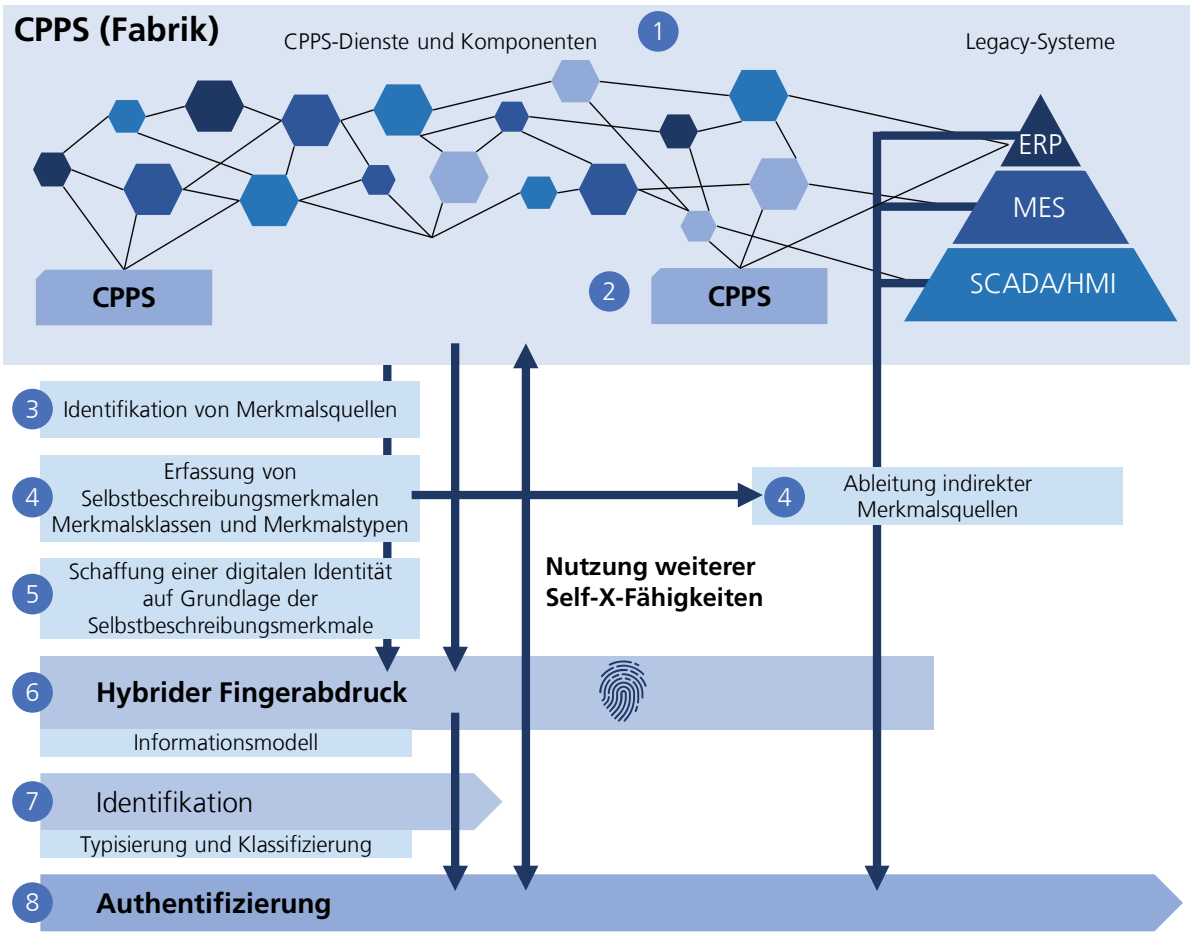


Abbildung 4.1 Grundkonzept des Ansatzes und Vorgehen

Dabei lassen sich die Bausteine des Konzepts gemäß ihrer Nummerierung inhaltlich primär bestimmten Abschnitten der vorliegenden Arbeit zuweisen:

1. Der Kontext einer vernetzten Produktion ist in Abschnitt 2.1 beschrieben.
2. CPS und ihre Self-X-Fähigkeiten werden im Detail in Abschnitt 2.2 diskutiert.
3. Die technologischen Grundlagen und Verfahren, die bei einer Authentifizierung auf Basis von Selbstbeschreibungsmerkmalen Verwendung finden, werden in Abschnitt 4.2 vorgestellt.
4. Die Daten- und Merkmalsquellen in einer vernetzten Produktion werden in Abschnitt 4.3.1 behandelt.
5. Die Differenzierung von Merkmalen und die Möglichkeit der Nutzung zum Zweck der Authentifizierung ist in den Abschnitten 4.3.2 bis 4.3.5 erläutert.
6. Die digitale Identität und ihr Lebenszyklus werden in den Abschnitten 4.4.1 und 4.4.2 dargelegt.
7. Das grundlegende Konzept eines hybriden Fingerabdrucks für CPPS wird in Abschnitt 4.4.3 eingeführt.
8. Die Identifikation von Entitäten mittels ihrer Merkmale wird in Abschnitt 4.4.4 skizziert.
9. Das auf den Selbstbeschreibungsmerkmalen basierte Authentifizierungsverfahren wird in Abschnitt 5.1 im Detail beschrieben.
10. Zur einfacheren Nachvollziehbarkeit des Ansatzes sind in Abschnitt 6.1 vier anschauliche Fallstudien dokumentiert.

4.2 Verwendete technologische Grundladen

Das in dieser Arbeit vorgestellte Konzept setzt auf existierenden technologischen Ansätzen auf. Hierzu gehören die systemischen Prinzipien der automatischen Identifikationsverfahren. Als Inspiration dient hier insbesondere die biometrische und die hylemetrische Identifikation, die ebenfalls charakteristische Merkmale nutzen, um Entitäten zu identifizieren. Zudem ist die Verwendung von Verfahren zur Erfassung charakteristischer Merkmale von Maschinen, das sogenannte Fingerprinting, Teil des Ansatzes. Diese Ansätze werden in den folgenden Unterabschnitten diskutiert.

4.2.1 Automatische Identifikationsverfahren

Identifikationsverfahren werden verwendet, um die erforderlichen Informationselemente für die Erzeugung einer digitalen Identität bzw. für die Authentifizierung einer digitalen Identität zu sammeln bzw. zu extrahieren. In Abschnitt 2.4.2 wurde bereits kurz auf die grundsätzliche Unterscheidung zwischen direkten und indirekten Verfahren eingegangen. Direkte Identifikation ist die direkte Extraktion von Merkmalen in Form von Entitätseigenschaften hinsichtlich ihrer physischen Beschaffenheit. Indirekte Identifikation ist die Bereitstellung von Informationen über eine Entität mithilfe eines oder mehrerer Hilfsobjekte, die der Entität eindeutig zugewiesen sind oder Teil von ihr sind (Sauter 1990, S. 54). Im Kontext informationstechnischer Systeme werden diese Verfahren als automatische Identifikationsverfahren (Auto-ID) bezeichnet, da die Datenerfassung zur Merkmalsextraktion und Identifikation automatisiert ausgeführt werden (Wölker 2004, S. 8). Das oder die eindeutigen Merkmale, die erfasst werden und zur eindeutigen Identifikation einer Entität innerhalb eines Aktionsraums genutzt werden können, werden als Identifikatoren bezeichnet, da sie mit der Identität verknüpft sind. Hierbei handelt es sich im Fall von Auto-ID-Verfahren meist um alphanumerische Zeichenketten. Deskriptoren, natürlichsprachliche Identifikatoren, beispielsweise beschreibende Merkmale wie Namen, Geburtsdatum, Auftragsnummern oder Adressdaten können zu einem Identifikator kombiniert werden (ten Hompel et al. 2007, S. 12f). Abbildung 4.2 stellt den Identifikationsprozess mittels

Auto-ID am Beispiel von RFID schematisch dar. Eine eindeutige Identifikation einer Entität ist nicht möglich, wenn Aufgrund der erfassten Merkmale mehrere übereinstimmende Entitäten gefunden werden. Im Fall einer Identifikation führt dies zu einem Fehler bzw. einer fehlgeschlagenen Identifikation. Auf diese Weise können jedoch eine Gruppierung bzw. Filterung nach Entitäten die Typen oder Klassen angehören durchgeführt werden. Durch ein mehrstufiges Verfahren mit gradueller Erweiterung der Menge M extrahierter Merkmale oder Ausweitung der Merkmalsräume kann ggf. eine Erfolgreiche Identifikation durchgeführt werden.

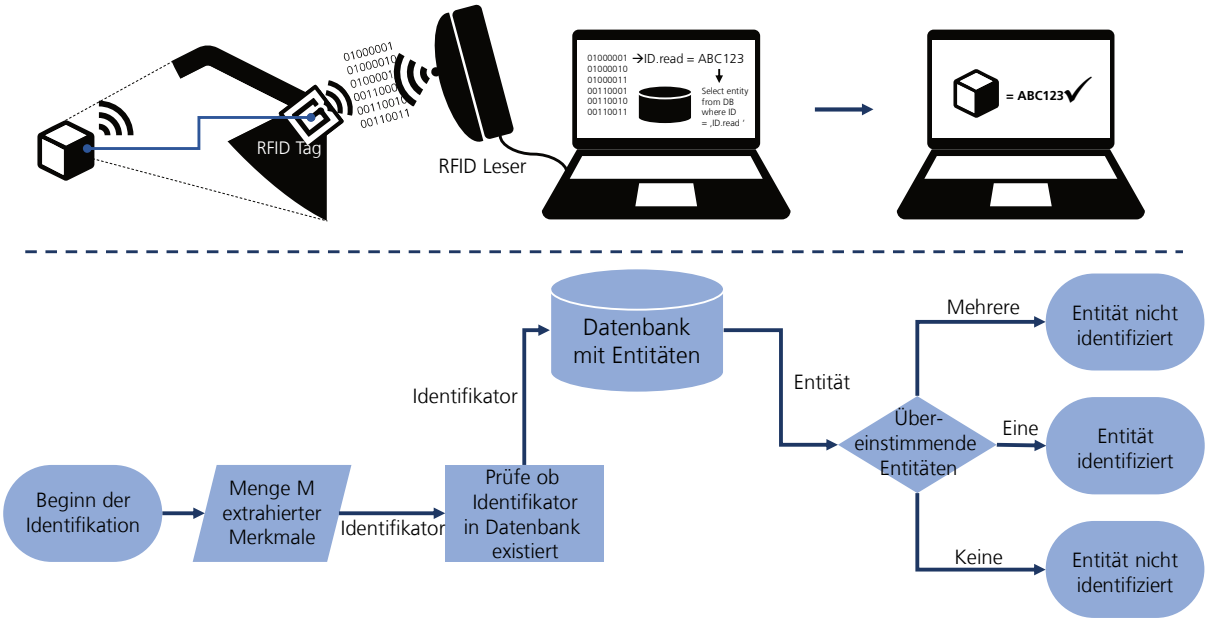


Abbildung 4.2 Ablaufschema eines Identifikationsprozesses am Beispiel von RFID

Die zur automatischen Identifikation eingesetzten Technologien und Systeme unterscheiden sich grundsätzlich darin, dass die eingesetzten Verfahren entweder berührend (taktil) oder berührungslos ihre Funktion ausführen. Weiterhin lässt sich wie in Tabelle 7 aufgelistet die Art der Datenerfassung zur Merkmalsextraktion unterscheiden. Neben elektronischen Verfahren sind dies Schrift- und Symbolbasierte Verfahren. Es ist zu erkennen, dass indirekte Technologien meist mit künstlichen Merkmalen und Identifikatoren arbeiten. Direkte Verfahren jedoch scheinen fast ausschließlich natürliche Merkmale zu erfassen, die

bei Menschen zu finden sind. Diese Verfahren werden daher den biometrischen Systemen zugeordnet.

Tabelle 7 Übersicht automatischer Identifikationsverfahren nach Funktionsprinzip in Anlehnung an (Krämer 2002; Wölker 2004; ten Hompel et al. 2007)

			Art der Erfassung	Technologiebeispiel
Identifikationsverfahren	indirekt	berührend	elektrisch	Speicherkarte, Chipkarte
			mechanisch	Nockenkodierung, Lochkarte
		berührungslos	optisch	Barcode, QR-Code, OCR
			magnetisch	Magnetstreifen/-karten
			induktiv	RFID (passiv)
			Funk	RFID (aktiv), GSM/GPS
	direkt	berührend	mechanisch	Fingerabdruck, Handabdruck
			optisch	Fingerabdruck, Handvenenscan/ Handgeometrie (IR)
			kapazitiv	Fingerabdruck
		berührungslos	optisch	Gesichtserkennung, Irisscan, Netzhaut
			akustisch	Stimmerkennung
			Funk	Herzschlagerkennung (Radar)

Im Folgenden soll die biometrische Identifikation im Detail diskutiert werden, da sie als Auto-ID-Technologie Ansätze bietet, die für das in dieser Arbeit vorgestellte Konzept anwendbar sind. Zudem wird das zur biometrischen Identifikation äquivalente Verfahren der hylemetrischen Identifikation vorgestellt.

4.2.1.1Biometrische Identifikation

Biometrie ist aus dem Griechischen abgeleitet und steht für biologische Statistik bzw. die Zählung und Messung von Lebewesen. Biometrik ist in Folge das automatisierte Messen eines oder mehrerer spezifischer Merkmale eines Lebewesens. Die biometrische Identifikation ist ein Identifikationsverfahren, das für Menschen verwendet wird, um sie durch eindeutige natürliche Merkmale zu identifizieren, da sie im Gegensatz zu personenbezogenen Wissens- oder Besitzelementen unmittelbar personengebunden sind (Michael et al. 2013, S. 10ff). Um diese Merkmale zu erfassen, werden Hilfsmittel verwendet, die diese physikalisch einzigartigen und unveränderlichen Merkmale aus einer bestimmten Quelle durch eine Messung extrahieren können, die Menschen gemeinsam haben. Beispiele hierfür sind die direkten Identifikationsverfahren in Tabelle 7. Merkmale, die zur biometrischen Identifikation eingesetzt werden sollen, müssen grundsätzlich folgende vier Eignungskriterien erfüllen (Jain et al. 2005, S. 4; Cozzella et al. 2012):

- **Universalität**: ein Merkmal ist bei jeder Person vorhanden
- **Einzigartigkeit**: keine zwei Personen sollten über dasselbe Merkmal verfügen
- **Permanenz**: ein Merkmal ist zeitlich invariant
- **Erfassbarkeit**: ein Merkmal lässt sich quantitativ erheben

Zudem sind folgende Kriterien in der praktischen Anwendung dieser Merkmale notwendig:

- **Robustheit**: Ein Merkmal lässt sich mit hoher Zuverlässigkeit und Genauigkeit unter verschiedenen Umgebungsbedingungen erfassen.
- **Akzeptanz**: Anwender akzeptieren die Nutzung eines Merkmals und des technischen Systems, welches zur Erfassung genutzt wird.
- **Umgehungssicherheit**: Der Aufwand ein Merkmal und das System zur Erfassung zu umgehen oder zu täuschen sollte möglichst hoch sein.

Menschliche Fingerabdrücke sind eines der am weitesten verbreiteten Merkmale, das zur biometrischen Identifikation eingesetzt wird. Weitere Beispiele für biometrische Verfahren zur Merkmalsextraktion inklusive zueinander relativer Bewertung nach Zuverlässigkeit,

Permanenz und weiteren Faktoren sind in Tabelle 8 gelistet. Es zeigt sich, dass andere Verfahren bzw. die damit verknüpften Merkmale zwar eine höhere Zuverlässigkeit bieten, jedoch offenbar andere Faktoren dazu führen, dass ein bestimmtes Merkmal einem anderen vorgezogen wird. Bei biometrischen Verfahren sind dies vor allem die Akzeptanz und die Kosten der Umsetzung. Bei der Auswahl von Selbstbeschreibungsmerkmalen sind dies Faktoren, die ebenfalls zum Tragen kommen.

Tabelle 8 Relative Bewertung biometrischer Verfahren in Anlehnung an (Pettersson et al. 2001; Thakkar 2017)

Biometrisches Verfahren	Zuverlässigkeit	Permanenz	Akzeptanz	Kosten	Template
Gesichtserkennung	Niedrig	Niedrig	Niedrig	Hoch	Groß
Iris-Scan	Hoch	Mittel	Mittel	Hoch	Klein
Fingerabdruckerkennung	Mittel	Niedrig	Hoch	Niedrig	Klein
Fingervenen-Scan	Hoch	Hoch	Niedrig	Mittel	Mittel
Stimmerkennung	Niedrig	Niedrig	Niedrig	Mittel	Klein
Retina-Scan	Hoch	Hoch	Mittel	Hoch	Mittel
Unterschriftenabgleich	Niedrig	Niedrig	Hoch	Niedrig	Klein
DNS-Abgleich	Hoch	Hoch	Niedrig	Hoch	Groß

Fingerabdruckleser werden verwendet, um bestimmte Merkmale eines Fingerabdrucks zu extrahieren, die sich im Muster der Hautleisten auf der Fingerkuppe eines jeden Fingers befinden. Abbildung 4.3 bildet diesen Ablauf in einem biometrischen Identifikationssystem beispielhaft ab. Zunächst wird ein Bild der Fingerlinien genommen, eine Klassenbildung durchgeführt und charakteristische Merkmale, die Minutien, erfasst (Michael et al. 2013, S. 13).

Die aus den Minutien erfassten Merkmale werden ausgewertet und zur Erzeugung einer Signatur genutzt, die ein Referenzmuster darstellen und als Template bezeichnet wird.

Zur Identifizierung (oder Authentifizierung) wird dieses Template beim Matching durch einen Abgleichsprozess geprüft (Weaver 2006).

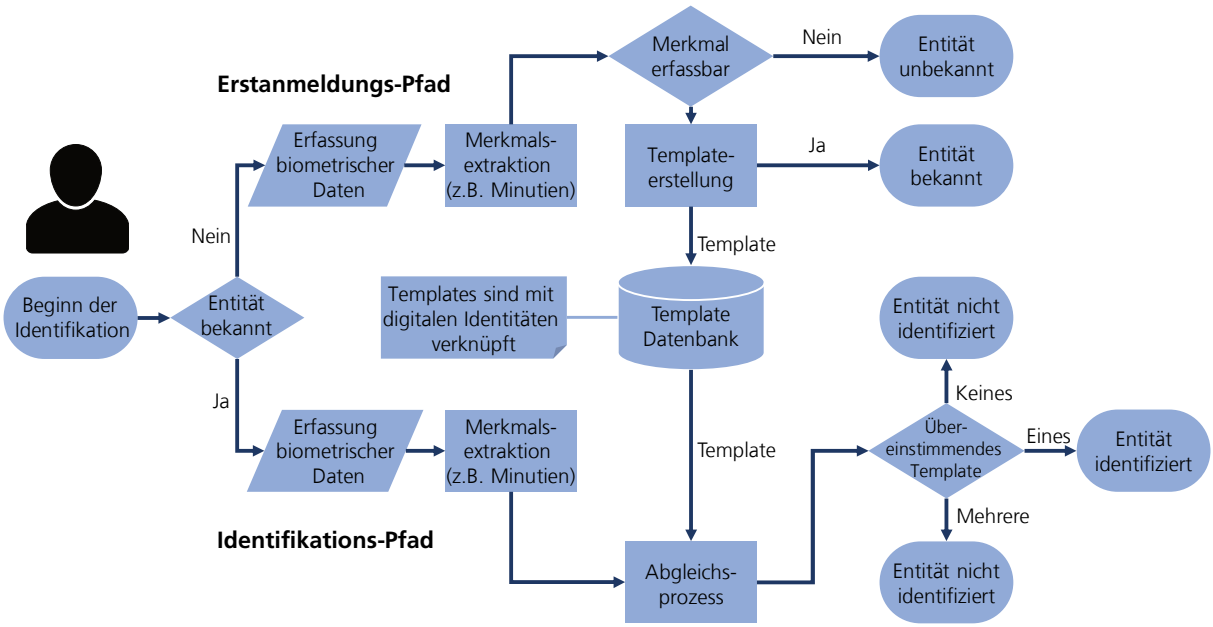


Abbildung 4.3 Biometrisches Identifikationssystem und -prozess in Anlehnung an (Jain et al. 2005, S. 22)

Auch die anderen Verfahren wie Gesichts-, Iris- oder Retinaerkennung oder bestimmte Merkmale menschliche Verhaltens werden genutzt, um Muster zu erzeugen, die zur biometrischen Identifizierung verwendet werden können (Padma et al. 2016). Eine Besonderheit der biometrischen Identifikation ist, dass die Verifizierung der Merkmale nicht strikt stattfindet. Dies ist begründet durch die Varianz in den Technologien zur Erfassung der Merkmale und den Umstand, dass natürliche Merkmale statistisch nicht zu hundert Prozent identisch reproduzierbar sind. Sie unterliegen unvermeidlichen, langfristigen Veränderungen und werden daher mit einer gewissen Toleranz ausgewertet. Biometrische Systeme können daher lediglich mit einer im Vorfeld definierten, System-typischen Wahrscheinlichkeit eine Entität identifizieren. Aus diesem Grund werden für das Matching Toleranzen festgelegt und nicht die Gleichheit der erfassten Merkmale, sondern die hinreichende Ähnlichkeit beurteilt (Helmus et al. 2009, S. 200).

4.2.1.2Hylemetrische Identifikation

Angelehnt an die biometrische Identifikation kann das Konzept biometrischer Merkmale von Lebewesen auf nicht lebende Objekte übertragen werden. Dieser Ansatz wird sinngemäß als Hylemetrie bezeichnet, abgeleitet vom griechischen Wort „hyle“, das „nicht lebende Materie“ bedeutet. Der primäre Anwendungsfall für hierfür ist die Authentifizierung von Banknoten, die mittels der Erfassung der eindeutigen zufälligen Verteilung von Metallfasern in jeder Banknote durchgeführt wird (Spagnolo et al. 2010). Das Konzept kann auch auf Kunstgegenstände und Arzneimittelverpackungen angewandt werden (Cozzella 2013). Grundsätzlich nutzt die hylemetrische Identifikation die gleichen Mechanismen wie die biometrische Identifikation (vgl. Abbildung 4.3) und stellt dieselben Anforderungen an die Eignungskriterien (Cozzella et al. 2012) (siehe Abschnitt 4.2.1.1). Die vorliegende Arbeit ist von der Übertragung des Konzepts der biometrischen Identifikation bzw. im Fall von nicht-lebendigen CPPS von der hylemetrischen inspiriert. Jedoch werden bei diesen zusätzlichen Technologien genutzt, beispielsweise hochauflösende Bilderkennung in Kombination mit UV-Licht (Spagnolo et al. 2010), um Merkmale zu erfassen. Im Gegensatz dazu widmet sich der hier verfolgte Ansatz der Nutzung der durch die Komponenten eines CPPS bereitgestellten Self-X-Fähigkeiten zur Erfassung dieser Merkmale.

4.2.2 Fingerprinting – Schaffung eines digitalen Fingerabdrucks

Die in Abschnitt 4.2.1 beschriebenen Identifikationsverfahren können ähnlich zur biometrischen Identifikation dann eingesetzt werden, wenn sie die in Abschnitt 4.2.1.1 gelisteten Eignungskriterien zumindest teilweise erfüllen. So müsse Merkmale eine ausreichende Universalität, Einzigartigkeit, Permanenz und Erfassbarkeit aufweisen. Dies ist bei CPS, die physische Komponenten besitzen, auf die man nicht immer Zugriff hat, nicht möglich. Zudem stellt es sich schwierig dar, die virtuellen Cyber-Komponenten von CPS entsprechend zu identifizieren, da diese über keine unmittelbar greifbaren Merkmale verfügen, die man identifizieren könnte. Es stellt sich nun die Frage, ob man ein Äquivalent zu einem bzw. mehreren Merkmalen wie einem menschlichen Fingerabdruck oder anderen biometrischen Merkmalen in Form von hylemetrischen Merkmalen bei einem CPS einsetzen kann.

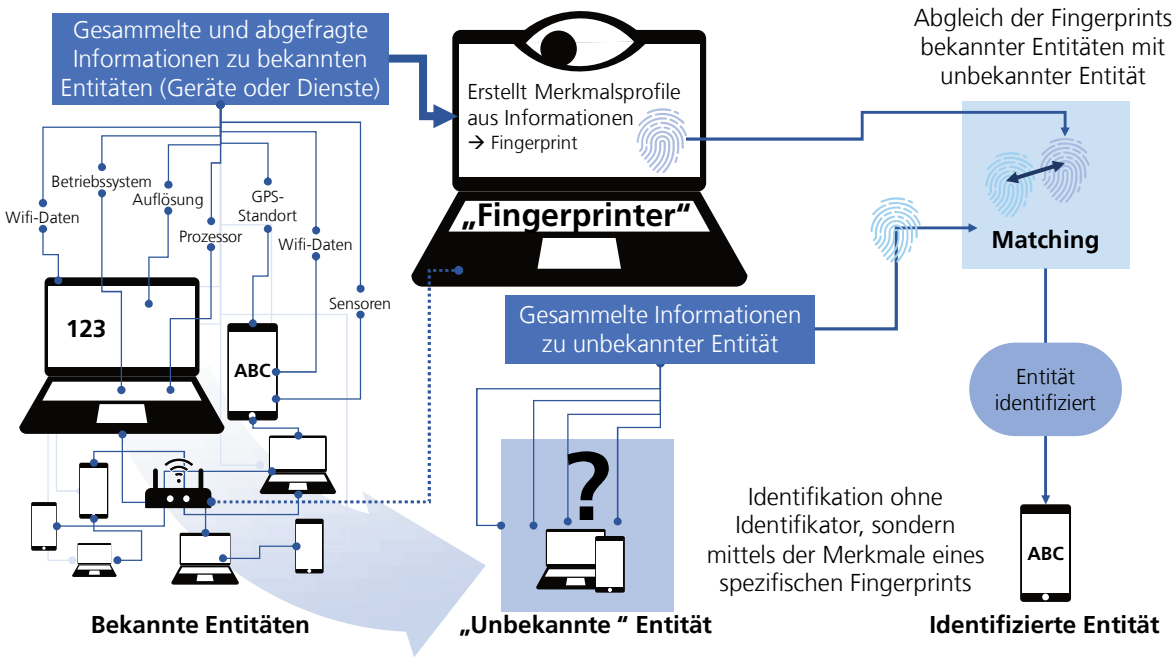


Abbildung 4.4 Grundsätzliches Prinzip des Fingerprintings

Zur Erstellung eines solchen künstlichen Fingerabdrucks können verschiedene Ansätze genutzt werden, die alternative Methoden nutzen, die die Schaffung einer Identität und

Identifikation von Entitäten ermöglichen, ohne künstliche angebrachte Merkmale zu nutzen. Dies ist jedoch ein ungewollter Effekt, da dieses Fingerprinting (engl. Fingerabdruckerzeugung) in Hinblick auf personenbezogene Informationen zu verhindern ist (Markou 2016, S. 219). Fingerprinting ist definiert als ein Prozess bei dem ein Beobachter oder Angreifer ein Gerät oder eine Applikationsinstanz bzw. Dienst auf Grundlage mehrerer Informationselemente, die an diesen Beobachter oder Angreifer kommuniziert werden, eineindeutig (bzw. mit ausreichend hoher Wahrscheinlichkeit) wie in Abbildung 4.4 bildlich dargestellt identifiziert (Cooper et al. 2013, S. 8).

Es werden also Informationen über Entitäten gesammelt, aus denen eine digitale Identität generiert werden kann, die direkt oder indirekt mit der Entität verknüpft wird. Die Internet Engineering Task Force (IETF) definiert den so geschaffenen digitalen Fingerabdruck bzw. Fingerprint (vgl. Template) als einen Satz von Informationselementen, die zur Identifikation eines Geräts oder einer Anwendungsinstanz dienen (Cooper et al. 2013, S. 8).

4.2.2.1Fingerprinting Varianten

Fingerprinting-Verfahren existieren in verschiedenen Ausprägungen, die sich aufgrund der verwendeten Verfahren stark unterscheiden können. Allerdings sind sie in ihrer Art der Anwendung und Methode nicht immer scharf voneinander abzugrenzen. Einige Varianten basieren auch auf einer Kombination der jeweiligen anderen Ansätze. Abbildung 3.4 bringt die wichtigsten Verfahren zur besseren Übersicht in Bezug zueinander. Fingerprinting-Verfahren können je nach Art des Ziels sowohl aktiv, passiv als auch semipassiv durchgeführt werden (Kohno et al. 2005; Spitzner 2000). Bei passiven Verfahren werden Informationen nicht-invasiv durch Beobachtung des Ziels gesammelt, während aktive Methoden das Ziel aktiv ansprechen, um Informationen zu gewinnen. Semipassive Verfahren nutzen eine Interaktion, die vom Ziel ausgelöst wird, beispielsweise eine Verbindung vom Ziel zu einer Webseite, die den Beobachter bzw. Angreifer darstellen kann. Dieser kann dann diese Verbindung nutzen oder missbrauchen, um diverse Fingerprinting-Verfahren anzuwenden, ohne dass das Ziel sich dessen bewusst ist.

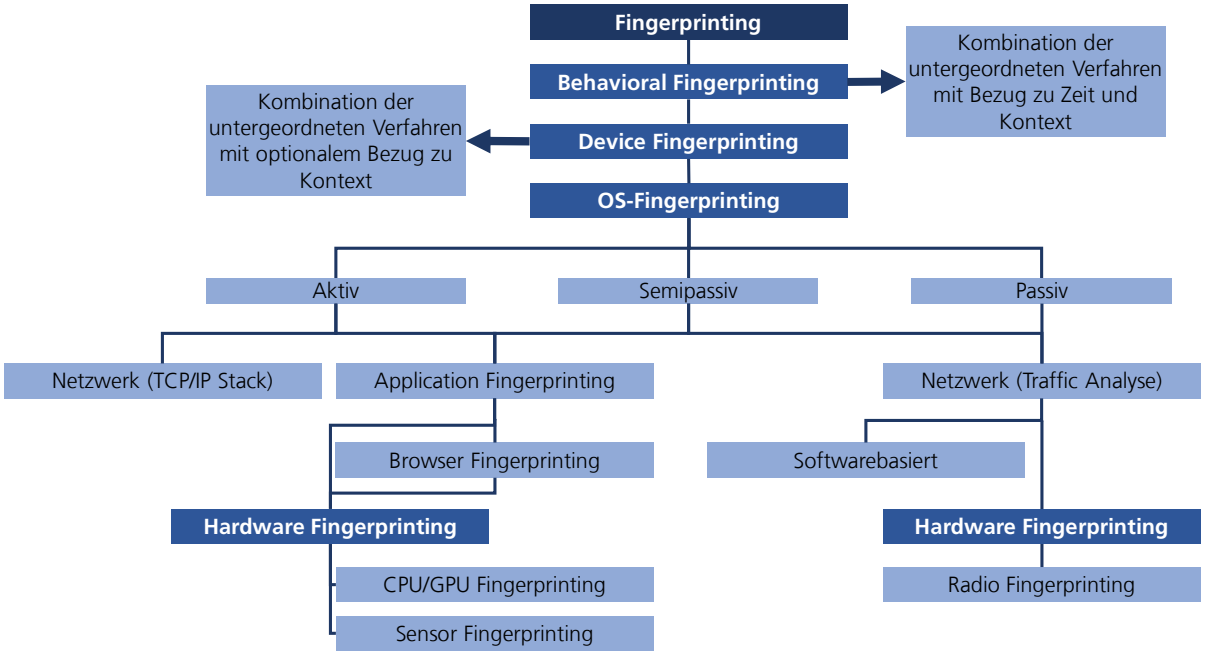


Abbildung 4.5 Fingerprinting-Varianten in Bezug zueinander

Gegen bestimmte Fingerprinting-Verfahren kann mit der Zeit auch eine „Immunität" entwickelt werden, wenn sich beispielsweise die technischen Voraussetzungen ändern (Polčák et al. 2014).

Das Prinzip des Fingerprintings eignet sich somit auch - oder besser gesagt sogar insbesondere - für cyber-physische Produktionssysteme. So lassen sich verschiedene Verfahren kombinieren, um für einzelne Komponenten oder für das CPPS als Verbund einen digitalen Fingerabdruck zu erzeugen (Stock et al. 2019a). In den folgenden Abschnitten werden die hier angesprochenen verschiedenen Verfahrensvarianten im Detail vorgestellt.

4.2.2.2Behavioral Fingerprinting

Das behavioral Fingerprinting nutzt charakteristische Verhaltensweisen, um Entitäten zu identifizieren. Dabei können beispielsweise Personen oder Geräte auf verschiedene Arten identifiziert werden (vgl. biometrische Identifikation in Abschnitt 4.2.1.1). Ein Ansatz für das Fingerprinting von Personen ist beispielsweise die Erfassung der Geschwindigkeit der

Tippeingabe auf einer Tastatur (Hupperich et al. 2015, S. 194). Denkt man diesen Ansatz weiter, kann man das komplette komplexe Interaktionsmuster einer Person mit einem Computer erfassen, bspw. neben der Geschwindigkeit auch einen spezifischen Rhythmus oder fehlerhafte Eingaben auswerten (Ometov et al. 2018, S. 19). Weitere Verhaltensweisen, wie z.B. der Laufstil einer Person, der mittels der Daten der Sensoren einer Smartwatch oder eines Smartphones analysiert werden kann, lässt sich ebenfalls nutzen (Bath 2018). Ein abstrakterer Ansatz ist die Analyse von Texten oder Programmcode, um den jeweiligen Autor zu identifizieren (Caliskan-Islam et al. 2015; Caliskan et al. 2015). Der Standort bzw. der Standortverlauf eines Nutzers kann ebenfalls herangezogen werden und kann als zusätzlicher vierter Identifikationsfaktor (vgl. Abschnitt 2.4.2) genutzt werden (Choi et al. 2012). Verhaltensmuster von Nutzern können somit zur Identifikation der zugehörigen Geräte, die diese zum jeweiligen Zeitpunkt einsetzen, genutzt werden (Manning 2018, S. 20).

Netzwerk-Identifikatoren wie IP-Adressen, MAC-Adressen, Portnummern usw. werden zur Identifizierung von Geräten verwendet, allerdings handelt es sich hierbei um "weiche" Identifikatoren bzw. Merkmale, die leicht gefälscht werden können, da sie eher statisch sind. Daher werden auch hier charakteristische dynamische Verhaltensweisen von Geräten und Maschinen eingesetzt, um Verhaltensprofile von Geräten zu erstellen (Bezawada et al. 2018). Dies ist beispielsweise der Zeitversatz von Antwortzeiten in der Netzwerkkommunikation, Standortverlauf, oder physikalisch bedingte Merkmale wie z.B. Signalstärke von Funksignalen, (Bezawada et al. 2019) und weitere in Abschnitt 4.2.2.3 und 4.2.2.4 behandelte Ansätze. Diese erfassten Verhaltensweisen lassen sich schwer fälschen und können somit auch zur Authentifizierung eingesetzt werden (François et al. 2011). Zusammenfassend können Merkmale also in statische und dynamische Merkmale aufgeteilt werden (Gray et al. 2017; Dolev et al. 2014) . Zusätzlich zur Kombination dieser Faktoren ist es auch möglich spezifische Interaktions- und Verhaltensmuster eines CPPS zu erfassen um einen Fingerprint zu erzeugen, beispielsweise aus den Daten zu Prozesszeiten, Transportzeiten oder Taktzeiten (Stock et al. 2019a).

4.2.2.3Device Fingerprinting

Das Device Fingerprinting zielt darauf ab ein Gerät aufgrund spezifischer intrinsischer Merkmale und Verhaltensweisen zu identifizieren. Es besteht eine Ähnlichkeit zum behavioral Fingerprinting, da beim Device Fingerprinting auch Verhaltensweisen erfasst werden, jedoch sind diese allein durch die technischen und physikalischen Eigenarten des Geräts bedingt und nicht zusätzlich durch die Interaktion mit Nutzern oder anderen Geräten. Zusätzlich können Informationen von auf dem Gerät installierten Programmen, beispielsweise Browsern oder Browser-Plugins (siehe Abschnitt 4.2.2.4) gewonnen werden. In Kombination mit Informationen, die aufgrund von Netzwerk- und Kommunikationsprotokollen extrahiert werden (Alaca et al. 2016) können auch multiple Ansätze in Kombination genutzt werden (Jose et al. 2016). Device Fingerprinting ist somit auch meist eine Kombination von Merkmalen, die mittels unterschiedlicher Fingerprinting-Verfahren extrahiert werden, die durch die Soft- und Hardware des Geräts bedingt sind (siehe Abschnitt 4.2.2.4).

Eine Variante des Device Fingerprintings ist das Operating System (OS) Fingerprinting, welches aufgrund der Eigenarten der Implementierungen bestimmter Softwarekomponenten eindeutige Rückschlüsse auf das eingesetzte Betriebssystem eines eingebetteten Systems und im Umkehrschluss auf das Gerät selbst erlaubt (Spitzner 2000). Dies ist beispielsweise der durch die OS-spezifische Implementierung eines Kommunikationsprotokolls verursachte Zeitversatz beim Austausch von Nachrichten-Paketen (Kohno et al. 2005). Hierbei können nach einem Blackbox-Verfahren durch das Versenden einer Reihe von Paketen die Veränderungen nachdem diese Pakete die Blackbox verlassen haben beobachtet werden (Gao et al. 2010). Neuere Ansätze nutzen hierfür zusätzlich Methoden des maschinellen Lernens, um noch besser Muster bzw. Anomalien in Mustern zu erkennen. So können nicht nur Betriebssysteme sondern auch spezifische Gerätearten typisiert werden (Radhakrishnan et al. 2015). Die Analyse von Nachrichtenpaketen kann somit zur Bestimmung von Geräte-Typen eingesetzt werden (Miettinen et al. 2017).

Da die Betrachtung des reinen Zeitversatzes ihre Grenzen hat wird sie oft auch in Kombination mit anderen Methoden genutzt (Lanze et al. 2012). Auch die eigentlichen Nachrichten können in Bezug auf die Zusammensetzung des Pakets untersucht werden, da diese sich je nach Implementierung unterscheiden kann (Greenwald et al. 2007). Die Antwortzeiten von Applikationen erlauben durch die Hardware bedingte Rückschlüsse auf das Gerät. Wenn das Verhaltensmuster bekannt ist, lassen sich diese ebenfalls nutzen.

Da sich IoT-Geräte auch oft verteilt und nicht im selben Netz befinden, existieren auch Ansätze für verteilte Fingerprinting Systeme (Thangavelu et al. 2019). Zudem ist die Anzahl der möglichen Protokolle für die Kommunikation der IoT Geräte in der Vergangenheit gewachsen. François et al. haben beispielsweise aus diesem Grund eine Methode zur automatischen Erfassung neuer Verhaltensmuster entwickelt (François et al. 2009).

Neben durch die Implementierung bestimmter Softwarekomponenten verursachten Charakteristika in der Netzwerkkommunikation können auch die durch den physikalischen Layer (PHY) der Kommunikationsschnittstelle verursachte Effekte genutzt werden (Sieka 2006). Im IoT-Umfeld sind dies meist drahtlose Schnittstellen, die mittels passivem Fingerprinting die Messung der Signalstärke der Funksignale (RSSI - Received Signal Strength Indication) durchführen (Ramsey et al. 2015).

Unterscheidungen können je nach gewähltem Merkmal auf Gerätetypen, individuelle Geräte, Typen von Netzwerkkarten oder Access-Point Typen getroffen werden (Xu et al. 2015). Ein aktiver Ansatz hierfür ist beispielsweise verschieden geartete Nachrichten und Aufrufe an Endgeräte und sogar Access Points zu senden, um ihre charakteristische Reaktion zu erfassen (Bratus et al. 2008). Ein alternativer Ansatz ist zudem anstatt der Datenpakete, die beispielsweise über veränderbare Header verfügen, die Datenframes des 802.11 Protokolls (WLAN) auf der Vermittlungsschicht zu prüfen (Neumann et al. 2014).

Besteht die Möglichkeit mehrere Merkmale über verschiedene Fingerprinting-Methoden abzufragen, kann je nach Risikolevel bzw. benötigtem Vertrauenslevel (vgl. Abschnitt 3.1.4) die Anzahl der abzufragenden Merkmale variiert werden (Spooren et al. 2015). Hierfür eignet sich vor allem das Fingerprinting von mobilen Geräten, da diese sowohl Browser Fingerprinting (Abschnitt 4.2.2.4) als auch verschiedene Varianten des Hardware-

Fingerprintings (Abschnitt 4.2.2.4) ermöglichen (Hupperich et al. 2015). Dies ist dadurch bedingt, dass mobile Endgeräte über ein Vielzahl von Sensoren verfügen, die genutzt werden können um ein Device Fingerprinting mittels der Sensoreigenschaften durchzuführen (Bojinov et al. 2014; Amerini et al. 2017). Der Ansatz die integrierte Sensorik zu nutzen ist unmittelbar auf CPS übertragbar (Ahmed et al. 2017). Indirekt können auch mittels der Sensorik erfasste Informationen über die Umgebung genutzt werden, auch in Kombination von Standortdaten (GPS, Funkzelle, Wifi-Netzwerke), um ein Fingerprinting-Profil abzuleiten (Azizyan et al. 2009), beispielsweise aus Umgebungsgeräuschen (Zhou et al. 2014).

4.2.2.4Hardware Fingerprinting

Das Hardware Fingerprinting ist eine Grundlage für die Device Fingerprinting-Ansätze, die im vorherigen Abschnitt vorgestellt wurden. Es erfasst Muster, die auf physikalische Eigenschaften bestimmter Komponenten und Bauteile eines Geräts zurückzuführen sind. Meist wird es im Kontext des Sensor Fingerprintings eingesetzt, allerdings können auch wie im vorherigen Abschnitt erwähnt z.B. die Charakteristika einer physikalischen Netzwerkschnittstelle in Form differenzierbarer Rauschsignale genutzt werden (Rasmussen et al. 2007). Es wird aber auch das Verhalten mechanischer Bauteile genutzt. So lassen sich die Schaltzeiten eines magnetischen Relais Hersteller- und Modellspezifisch unterscheiden (Formby et al. 2016).

Sensoren, die aus Silizium gefertigt werden, verfügen aufgrund von Imperfektionen auf molekularer Ebene über spezifische Rauschmuster, die eindeutig zugeordnet werden können. Diese Micro-Electro-Mechanical Systems (MEMS) finden sich in Form von Beschleunigungssensoren, Gyroskopen (Dey et al. 2014) oder Mikrofonen und Lautsprechern (Das et al. 2014) in fast jedem mobilen Gerät und weisen das beschrieben Verhalten auf. Das fundamentale Konzept, auf dem das Hardware Fingerprinting basiert, wird allgemein als Physical(ly) Unclonable Function (PUF) bezeichnet, also physikalisch bedingte Funktionen, die sicher gegenüber Nachahmung sind (Maes et al. 2010). PUFs können optischer Natur

sein und können somit auch für CCD-Kamerasensoren (charge-coupled device) eingesetzt werden um einzigartige Rauschmuster in den Rohdaten der einzelnen Pixel eines Kamerasensors zu erfassen (Amerini et al. 2017). Wechselwirkungen von SMD-Bauteilen die abhängig von ihrer Position und den Leiterbahnen auf einem PCB sind können ebenfalls eine Auswirkung auf die Signalcharakteristik haben. Dies kann einerseits zur Typisierung baugleicher CPS und zur Identifikation spezifischer CPS bei der Erfassung charakteristischer Muster einzelner extrahierter Merkmale genutzt werden (Desmond et al. 2008).

4.2.2.5Browser Fingerprinting

Ähnlich wie beim Device Fingerprinting wird das Browser Fingerprinting eingesetzt, um ein Gerät zu identifizieren. Allerdings handelt es sich hierbei um einen PC oder ein vergleichbares (mobiles) Endgerät, das über eine Benutzeroberfläche von einem Nutzer bedient wird. Dabei werden bestimmte Merkmale des Gesamtsystems mittels des Internetbrowsers erfasst (Eckersley 2010). Hier gibt es mehrere Ansätze, die kombiniert werden, um Informationen zu sammeln, aus denen ein Fingerprint erzeugt wird (Nikiforakis et al. 2013; 2014). Diese lassen sich in drei Klassen einteilen:

- Klasse A: Es werden über die Webseiten vom Server auf dem Zielgerät im Browser gezielt Cookies mit spezifischen eindeutigen Informationen gesetzt, die es erlauben mittels Tracking den Nutzer und sein Verhalten nachzuverfolgen, was oft im Konflikt mit dem Datenschutz steht (Buchmann et al. 2013, S. 297f).
- Klasse B: Internetbrowser über APIs, die es erlauben grundsätzliche Informationen über das Hostsystem (vgl. OS Fingerprinting) wie die Betriebssystemversion, Informationen über Systemressourcen wie CPU, GPU und Speicher, die Bildschirmauflösung und weitere betriebssystemspezifische Information abzufragen. Informationen über den Browser, wie z.B. Version, Größe des sichtbaren Bereichs im Browserfenster, installierte Schriftarten, installierte Erweiterungen können ebenfalls erfragt werden (Rausch et al. 2014).

- Klasse C: Browser erlauben auf der Clientseite meist die Ausführung von JavaScript-Code, der entweder weitere Schnittstellen anspricht. Dieser kann Informationen abfragen oder dazu genutzt werden bestimme Metriken zu berechnen, beispielsweise die Zeit für die Ausführung eines Algorithmus in Form einer bestimmten Funktion. Somit kann unabhängig von den Informationen, die der Browser über die Systemressourcen übermittelt, eine direkte Messung der Systemleistung durchgeführt werden. Alternativ zu JavaScript lassen sich auch Messungen mittels HTML 5 durchführen (Nakibly et al. 2015).

Die Kombination dieser Faktoren erlaubt auch eine Browser-unabhängige Identifikation, was zeigt, dass die Kombination der Merkmale ausschlaggebend ist (Cao et al. 2017). Das Prinzip kann auf Webseiten wie Panopticlick der Electronic Frontier Foundation (Electronic Frontier Foundation 2019) oder amiunique.org (AmIUnique 2019) nachvollzogen werden und zeigt, wie der PC eines Nutzers eindeutig aufgrund seiner Merkmale mittels Browser Fingerprinting identifiziert werden kann.

Eine Variante des Browser Fingerprintings ist das Website Fingerprinting, bei dem umgekehrt agiert wird, indem vom Browser aufgerufene Seiten mittels der übertragenen Pakete identifiziert (vgl. Device Fingerprinting) und so implizit ermittelt werden kann, welche Seite ein Nutzer aufruft, ohne die Adresse zu kennen (Panchenko et al. 2016).

Browser Fingerprinting kann ein Ansatz für CPPS sein, zu deren Systemkomponenten PCs und eingebettete Systeme gehören, deren Einsatz im industriellen Umfeld geläufig ist. Zudem können einige der Ansätze des Browser Fingerprintings, beispielweise die aktive Ausführung von Rechenoperationen oder Abfrage von Systeminformationen, für das Fingerprinting von CPPS genutzt werden (Stock et al. 2019a). Aktuelle Verfahren nutzen meist passive Ansätze. CPPS verfügen jedoch über zunehmend komplexere Self-X-Fähigkeiten, die es erlauben die teilweise aufgrund des Schutzes der Privatheit ungewollten Browser Fingerprinting Methoden für aktives Fingerprinting zu nutzen und mit den passiven Methoden zu kombinieren.

4.2.3 Zwischenfazit

Automatische Identifikationsverfahren finden bereits breite Anwendung in der Produktion. Allerdings sind diese primär an künstliche, festgelegte und eindeutig kennzeichnende Merkmale gebunden und dienen ausschließlich der Identifikation. Komplexere Methoden, die ähnlich wie die biometrischen Identifikationsverfahren anwendbar sind, finden in einigen Bereichen der IT-Sicherheit bereits Anwendung. Dieser als Fingerprinting bezeichnete und hier in seinen Ausprägungen vorgestellte Ansatz soll als technologische Grundlage für den entwickelten Ansatz dienen. Fingerprinting basiert auf der Bestimmung geeigneter Merkmale einer Entität und der Erstellung eines Profils aus den beobachteten spezifischen Merkmalsausprägungen. Dieses Profil kann als digitaler Fingerabdruck bezeichnet werden. Dieser ist angelehnt an einen natürlichen Fingerabdruck eines Menschen, der mittels der biometrischen Prüfverfahren eine Identifikation und Authentifizierung der Identität einer Person erlaubt. Aus Gründen der Praktikabilität werden Menschen jedoch nicht mit mehr als einem zusätzlichen Faktor, z.B. dem Fingerabdruck, geprüft, da ein übermäßiger Mehraufwand im Authentifizierungsprozess keine Akzeptanz findet. Bei CPPS ist es jedoch möglich mit Self-X-Fähigkeiten ausgestattet zu werden, die eine Erfassung, Ableitung und Prüfung zahlreicher Merkmale zum Zweck der Authentifizierung aus ihnen selbst, ihrer Umgebung und mit Ihnen vernetzten Systemen erlaubt.

4.3 Bestimmung geeigneter Selbstbeschreibungsmerkmale

In einer vernetzten Produktion entstehen große Mengen erschließbarer Daten. Diese Daten stammen aus zahlreichen Maschinen und IT-Systemen, die in der Produktion im Einsatz sind, und den damit verbundenen Prozessen. CPS verfügen über die Fähigkeit diese Daten mittels ihrer Fähigkeit zur Selbstbeschreibung mit Kontext zu versehen und sie so zu Informationen anzureichern. Im Umkehrschluss können diese Informationen als Selbstbeschreibungsmerkmale von CPPS dazu dienen zu ermitteln, welche dieser Daten in welcher Form dazu geeignet sind, um eine sichere Identität zu bilden. Im Folgenden werden

diese möglichen Merkmalsquellen betrachtet, beschrieben und die Merkmale aufgrund ihrer Eigenschaften auf die Eignung zur Identitätsbildung untersucht.

4.3.1 Daten- und Merkmalsquellen

4.3.1.1Betriebliche Daten und Datenquellen

Die in einem Produktionsumfeld erhobenen Daten dienen wesentlich der Steuerung und Optimierung von Abläufen und Prozessen auf verschiedenen Ebenen (vgl. Abbildung 2.3) und zu ihrer Qualitätskontrolle. Dieser Zweckbezug der Daten lässt sich nutzen, um aus diesen Primärdaten Sekundärdaten zu gewinnen, die als Merkmalsdaten eingesetzt werden können. Daten können neben ihrem Zweck auch nach ihrer Herkunft, Funktion, Verarbeitung und Zeitdauer in Form von Zuständen oder Ereignissen in Beziehung zueinander gesetzt und klassifiziert werden. Abbildung 4.6 stellt neben diesen unterschiedlichen Arten des Datenbezugs auch die zugehörigen Datentypen dar. Im betrieblichen Kontext lassen sich diese Datentypen alle in einem ganzheitlichen CPPS wiederfinden, also einem CPPS, das die CPPS bzw. CPS unterschiedlicher Komplexitätsgrade einer gesamten Produktion nach dem „System of Systems"-Grundsatz umfasst.

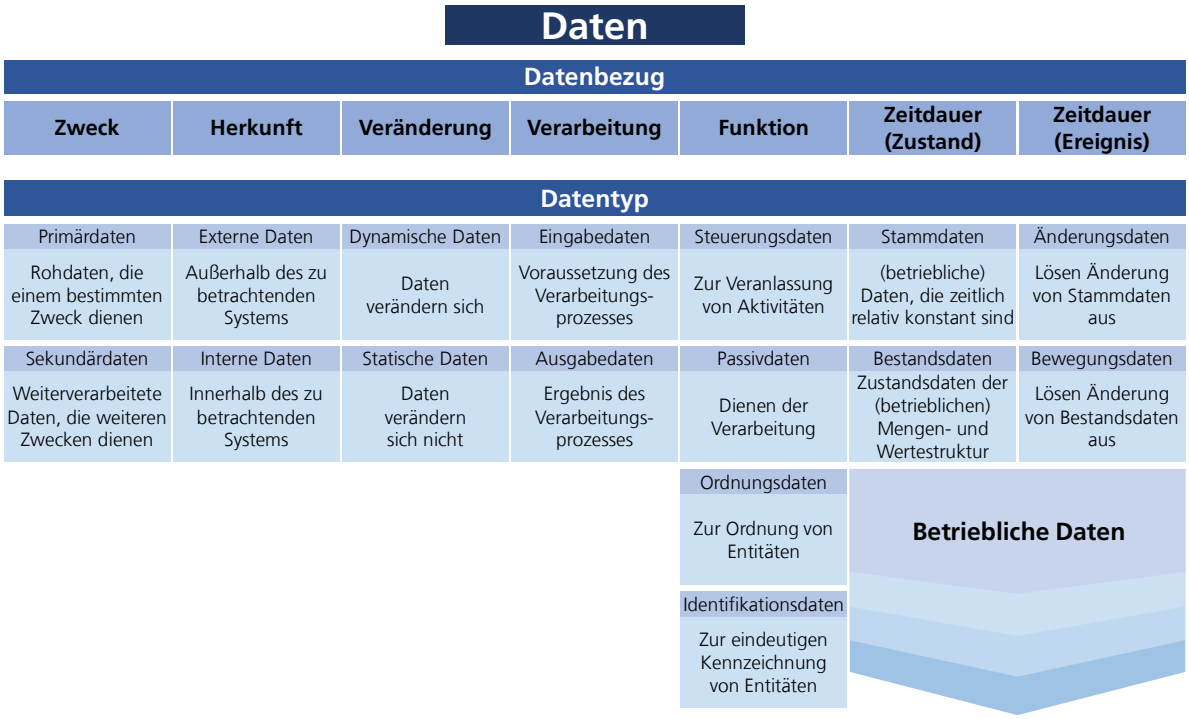


Abbildung 4.6 Klassifikationsmerkmale von Daten in Anlehnung an (Lassmann 2006, S. 218)

Diese Fähigkeit zur Schachtelung von CPS führt dazu, dass die Herkunft von Daten als externe oder interne Daten relativ betrachtet werden kann (vgl. Abbildung 4.6). Betrachtet man den physischen Verbund eines CPS, dann sind die Daten, die ein CPS mit anderen CPS austauscht, externe Daten. Werden diese CPS jedoch als logische Einheit definiert, dann können diese Daten in Bezug auf eine logische Einheit als interne Daten ausgelegt werden. Für die Herkunft der Daten hat dieser Umstand dann eine Relevanz, wenn die Vertrauensbeziehung zwischen Komponenten beachtet werden muss, um die Integrität der Daten sicherzustellen. Daten, deren Ursprung nicht eindeutig zugeordnet werden kann, sind daher grundsätzlich als nicht vertrauenswürdig einzustufen. Dies ist vor allem bei externen Daten der Fall, falls diese nicht mittels einer vertrauenswürdigen Komponente „internalisiert" werden können. Das bedeutet, dass externe Daten durch zusätzlichen vertrauenswürdigen Kontext auf diese Weise in interne Daten gewandelt werden können. Die Veränderung von Daten ist ein wichtiger Aspekt ihrer Eignung als Merkmal.

Fixe, nicht variable bzw. statische Daten sind zeitlich konstant. Sie können daher unmittelbar als Ankerpunkt dienen. Im Gegensatz dazu stehen die variablen Daten, die sich dynamisch verändern. Als Primärdaten sind Daten ohne weiteren Kontext kaum sinnvoll für die Merkmalsgewinnung zu verwenden, außer der Sie können durch den Kontext unmittelbar mit einer Quelle verknüpft werden. Werden sie zusätzlich in Form von Sekundärdaten im Zuge einer Verarbeitung als Eingabedaten verwendet, so können die vorliegenden Ausgabedaten ebenfalls als Merkmale dienen.

Spezifischer kann der Kontext ausgelegt werden, wenn Daten einen Bezug zu einer Funktion haben. Dienen sie beispielsweise der Steuerung, indem ein bestimmtes Datum eine Aktivität auslöst, muss aus dem Kontext bekannt oder zumindest ermittelbar sein, welche Eigenschaft dieses Datum hat, um eine bestimmte Aktivität auszulösen oder welche Auswirkung diese Aktivität hat. Im Vergleich zu Steuerungsdaten lösen Passivdaten nicht unmittelbar eine Aktivität aus, sondern dienen primär der Verarbeitung. Ihr eigentlicher Zweck wird nach der Verarbeitung erreicht.

Ordnungs- und Identifikationsdaten sind Datentypen, deren Funktion eine der Grundlagen des hier diskutierten Ansatzes bilden. Ordnungsdaten dienen der Ordnung von Entitäten. Dies kann beispielsweise die Eingruppierung von Entitäten in Klassen sein, also die Klassifikation mittels bestimmter Merkmale einer Klasse. Identifikationsdaten dienen der eindeutigen Kennzeichnung von Entitäten, beispielsweise durch die Seriennummer einer Maschine.

Besteht ein zeitlicher Bezug, so können Zustände und Ereignisse von Entitäten mittels Daten abgebildet werden. Zustandsbezogene Daten sind Stammdaten, die über einen Betrachtungszeitraum unverändert bleiben. Bestandsdaten beschreiben den Zustand einer Mengen- und Wertestruktur, also beispielsweise die in einem ERP abgebildeten Materialkonten oder Kapazitäten von Lagerplätzen. Sind nur momentane Ereignisse von Relevanz, spricht man von Änderungsdaten, die Änderungen an den Stammdaten verursachen. Dies können beispielsweise die Standortinformationen, Benennung oder technische Informationen zu einer Maschine sein. Bestandsdaten wiederum werden von Bewegungsdaten beeinflusst, also die Zu- oder Abgänge in den Konten bzw. Materiallagern.

In einem vernetzten und durch datengetriebene Technologien gestützten System im betrieblichen Kontext, wie es ein CPPS ist, finden sich alle diese Datentypen in unterschiedlicher Ausprägung. Die für die Merkmalsgewinnung geeigneten Datentypen sind vor allem in diesen betrieblichen Daten zu finden. Diese lassen sich differenzierter und qualifizierter, wie in Abbildung 4.7 dargestellt, unterscheiden. Die Zweckorientierung der Daten gibt Aufschluss darüber, welchen Zweck ein Datentyp im betrieblichen Kontext erfüllt.

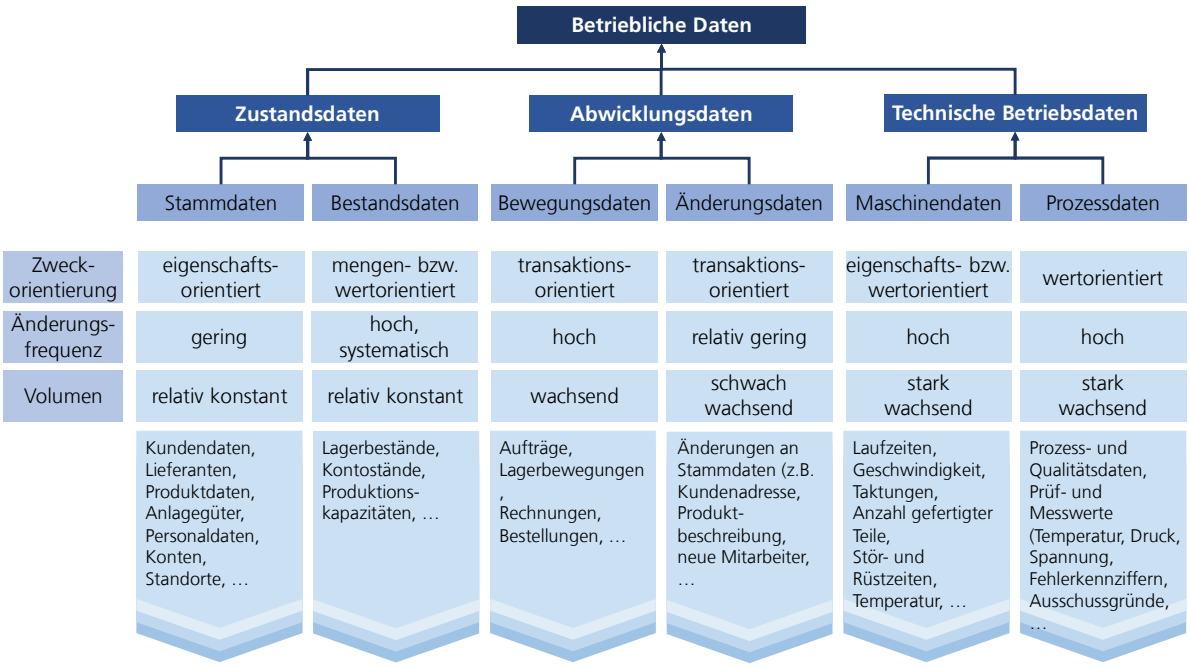


Abbildung 4.7 Unterscheidung von betrieblichen Daten im CPPS-Kontext in Anlehnung an (Schuh et al. 2012, S. 265; Schemm 2008, S. 20)

So beschreiben die Stammdaten die Eigenschaften einer betrachteten Entität, während Bestandsdaten mengen- und wertorientierte Auskünfte über das betrachtete Objekt liefern. Bewegungs- und Änderungsdaten werden im betrieblichen Kontext als Abwicklungsdaten zusammengefasst und beziehen sich in ihrer Funktion auf die Abbildung von Transaktionen. Die technischen Betriebsdaten umfassen neben den Maschinendaten, die Eigenschaften und Werte abbilden, auch die Prozessdaten, die über die Erfassung von Werten zur Gewinnung von Informationen zu Prozessen eingesetzt werden können. Ein

großer Unterschied besteht auch zwischen den Änderungsfrequenzen und dem Volumen der unterschiedlichen Datentypen. Stammdaten sind beispielsweise durch eine geringe Änderungsfrequenz gekennzeichnet und gehen bei gleichbleibender Anzahl betrachteter Entitäten mit einem konstanten Volumen einher. Maschinendaten wiederum weisen in vielen Fällen eine hohe Änderungsfrequenz und stark wachsendes Volumen auf.

4.3.1.2CPS als Datenquelle

Neben den betrieblichen Daten, die ein CPPS liefern kann, kann die domänenagnostische CPS-Komponente eines CPPS selbst als Datenquelle dienen. Dies ist der Teil eines CPS, der die IKT- und OT-Komponenten und Dienste eines CPS ohne Bezug zu einer spezifischen Anwendung umfasst. Dieser Teil muss als atomare Komponente in der Lage sein die Fähigkeiten eines CPS abzubilden.

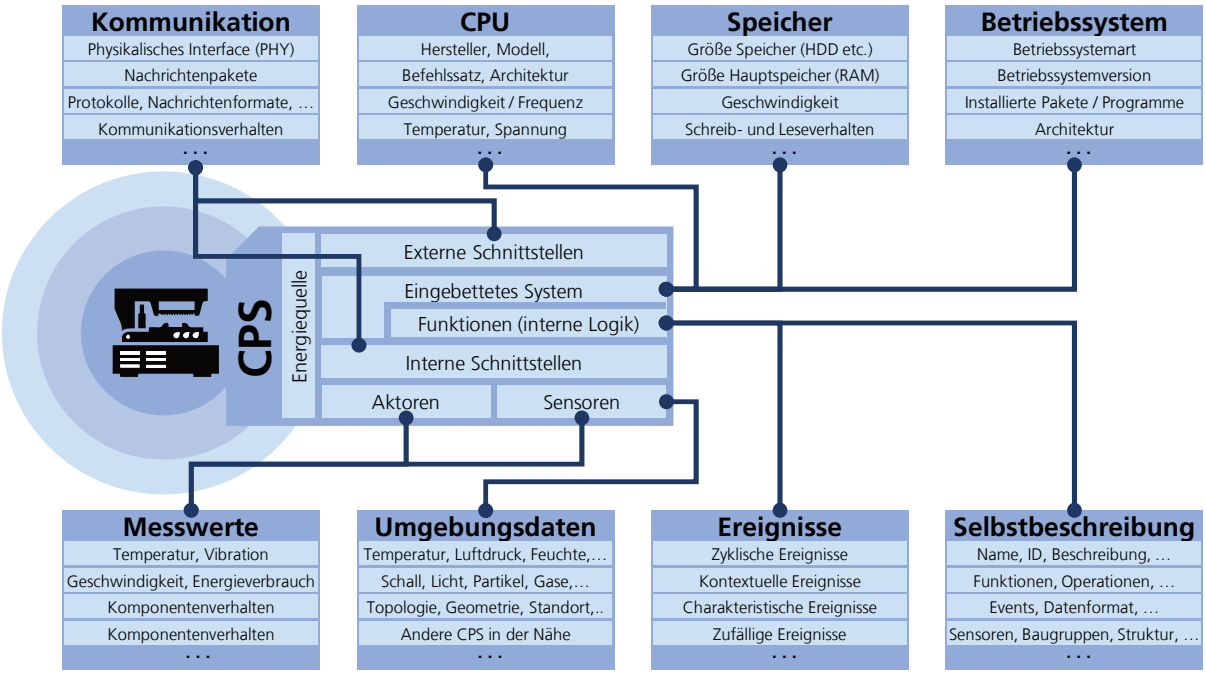


Abbildung 4.8 Beispiele eines CPS als Datenquelle

Abbildung 2.5 stellt die Struktur und Bestandteile eines CPS schematisch dar. Diese Bestandteile werden im Folgenden in Bezug zu einer aktuell möglichen Implementierung diskutiert und auf mögliche Datenquellen untersucht.

Hierbei liegt der Schwerpunkt der Betrachtung auf den offensichtlicheren und vergleichsweise einfach zu integrierenden Datenquellen. Grundsätzlich besteht jedoch die Möglichkeit mittels aufwendigerer Verfahren (vgl. Abschnitt 4.2.2) weitere Datenquellen zu erschließen, jedoch ist hier zusätzlich eine Abwägung zwischen technischer Umsetzbarkeit und wirtschaftlicher Tragfähigkeit durchzuführen. Abbildung 4.8 zeigt die schematische Struktur eines CPS (vgl. Abschnitt 2.2.1) und leitet mögliche Datenquellen ab. Die Sensorik eines CPS ist eine offensichtliche Quelle für Daten. Jedoch sind sämtliche Komponenten eines CPS mögliche Datenquellen und somit auch potenzielle Merkmalsquellen.

4.3.1.3Identifikation von Merkmalsquellen

Merkmale können direkt aus den in den vorherigen Abschnitten dargestellten Datentypen abgeleitet werden. So gibt die CPS-Selbstbeschreibung prinzipiell die Stammdaten zu einem CPPS wieder. Diese Stammdaten liefern im Normalfall Informationen zum CPPS, die als Ordnungs- und Identifikationsdaten genutzt werden können.

Die möglichen Merkmalsquellen sind neben einem CPS selbst auch andere CPS in der Umgebung und die sich daraus ergebenden Kontextinformationen (vgl. Anhang 2.1 bzw. Abschnitt 3.2.5). Durch die inhärente Fähigkeit eines CPS mittels Sensoren seine Umgebung wahrzunehmen kann ein CPS seine Selbstbeschreibung nicht nur mit Daten über sich selbst, sondern auch über seine Umgebung anreichern (vgl. Abschnitt 2.2.2 und 2.2.3). Zusätzlich lassen sich einem CPPS in sämtlichen IKT- und OT-Systemen entlang seines Lebenszyklus in der Produktion Daten bzw. Informationen zuordnen (vgl. Abschnitt 2.2.2 und 2.2.5). Abbildung 4.9 skizziert diesen Zusammenhang.

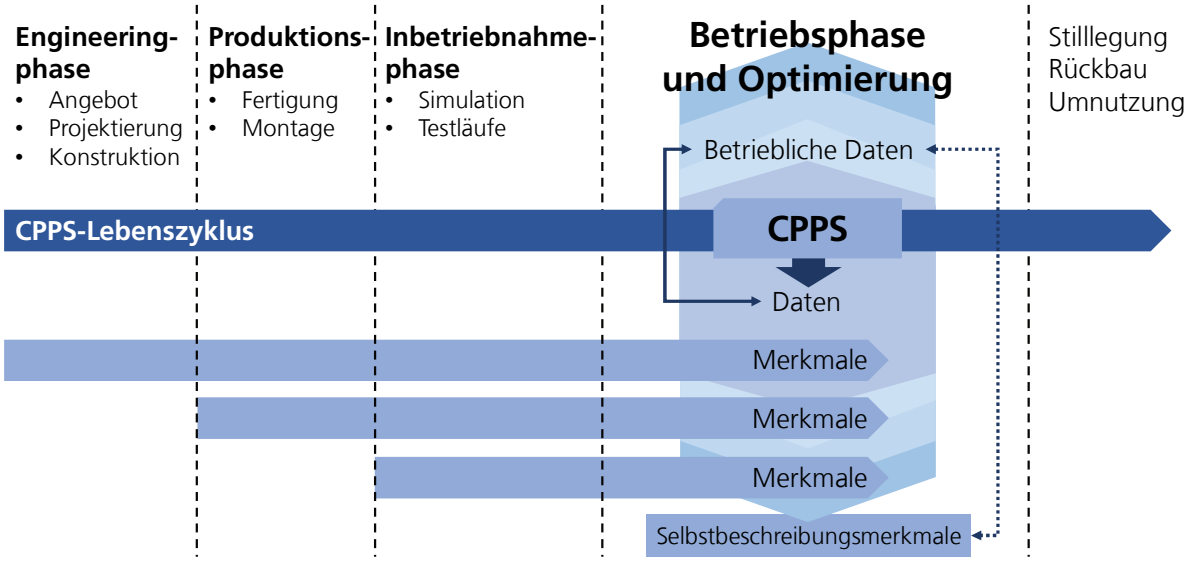


Abbildung 4.9 Merkmalsquellen entlang des CPPS-Lebenszyklus

Ein Ansatz Maschinen mit einer sicheren Identität zu versehen, ist es entsprechende Security Hardware wie Trusted Platform Module (TPM), HW-Token oder Crypto-Chips schon während der Engineering-Phase und Produktion des CPS herstellerseitig zu integrieren. Allerdings werden diese meist nur nachträglich angebracht (Jänicke et al. 2016, S. 5). Für das hier vorgeschlagene Konzept ist das Vorhandensein einer solchen Security-Komponente und der darin befindlichen geschützten Informationen im Prinzip nur ein weiteres Merkmal. Zudem können während des Designs und Engineerings Profile für die statische Selbstbeschreibung eines CPS erstellt werden, auf die ein Anwender in der Betriebsphase nur noch zurückgreifen muss.

Während der Inbetriebnahme-Phase eines CPS können Daten generiert und erfasst werden, die ggf. charakteristisch für bestimmte Betriebszustände, Prozesse oder Verhaltensweisen eines CPS oder seiner Komponenten sind. Diese können das Profil des CPPS um weitere statische (bspw. Standort) und dynamische Daten erweitern. Dieser Ansatz entspricht dem Konzept des Fingerprintings, das in Abschnitt 4.2.2 diskutiert wird.

Das Hauptaugenmerk liegt jedoch auf der Betriebsphase, da hier noch zusätzliche weitere Merkmalsquellen angesiedelt sind. In dieser finden Prozesse und Interaktionen statt, die Daten erzeugen, die zu den dynamischen betrieblichen Daten gehören. Auf diese Weise

lassen sich Merkmale auch aus den unterschiedlichen Ebenen der Automatisierungspyramide bzw. den in diesen Ebenen beheimateten Systemen während dieser gesamten Lebenszyklusphase des CPPS gewinnen. In einer Produktionsumgebung, die als CPPS ausgelegt ist, sind diese Ebenen nur noch logisch vorhanden. Die Merkmalsquellen sind in diesem Fall jedoch in einem Netzwerk aus Diensten und Maschinen verteilt.

Die primäre Merkmalsquelle ist somit die Selbstbeschreibung des CPS selbst. Hier finden sich grundsätzliche Informationen über ein CPS, wie man sie von einer gängigen Maschine kennt, die mit ihren Basisdaten in den Stammdaten eines MES oder ERP hinterlegt ist. Dies sind beispielsweise ein menschenlesbarer Name, ID, Seriennummer, Standort, Besitzer, Herstellername, Typ oder Geräteklasse. Zudem beinhaltet die Selbstbeschreibung eines CPS Informationen zu den Fähigkeiten eines CPS. Diese lassen sich zwar aus dem Typ oder der Geräteklasse ableiten, jedoch ist eine implizite Angabe der von einem CPS angebotenen Fähigkeiten Teil seines autonomen Charakters. In der Umsetzung können hier Events als Datenquellen und Operationen als Fähigkeiten gelistet sein. Diese können die Parameter für die Nutzung der Operation und der dahinter liegenden Funktionen liefern oder die vom CPS angebotenen Daten, die über Events (Ereignisse) transportiert werden. Die Fähigkeit Informationen über Events, also ereignissteuert Informationen auszutauschen ist ein Kennzeichen von CPS (vgl. Anhang 2.3 und Abschnitt 3.2.5).

Beziehungs- und Strukturdaten sind auch Informationen, die aus der Beziehung einzelner CPS-Komponenten zueinander gewonnen werden können (vgl. Abschnitt 2.2.6). Die erläuterten Zusammenhänge stellt Abbildung 4.10 schematisch dar.

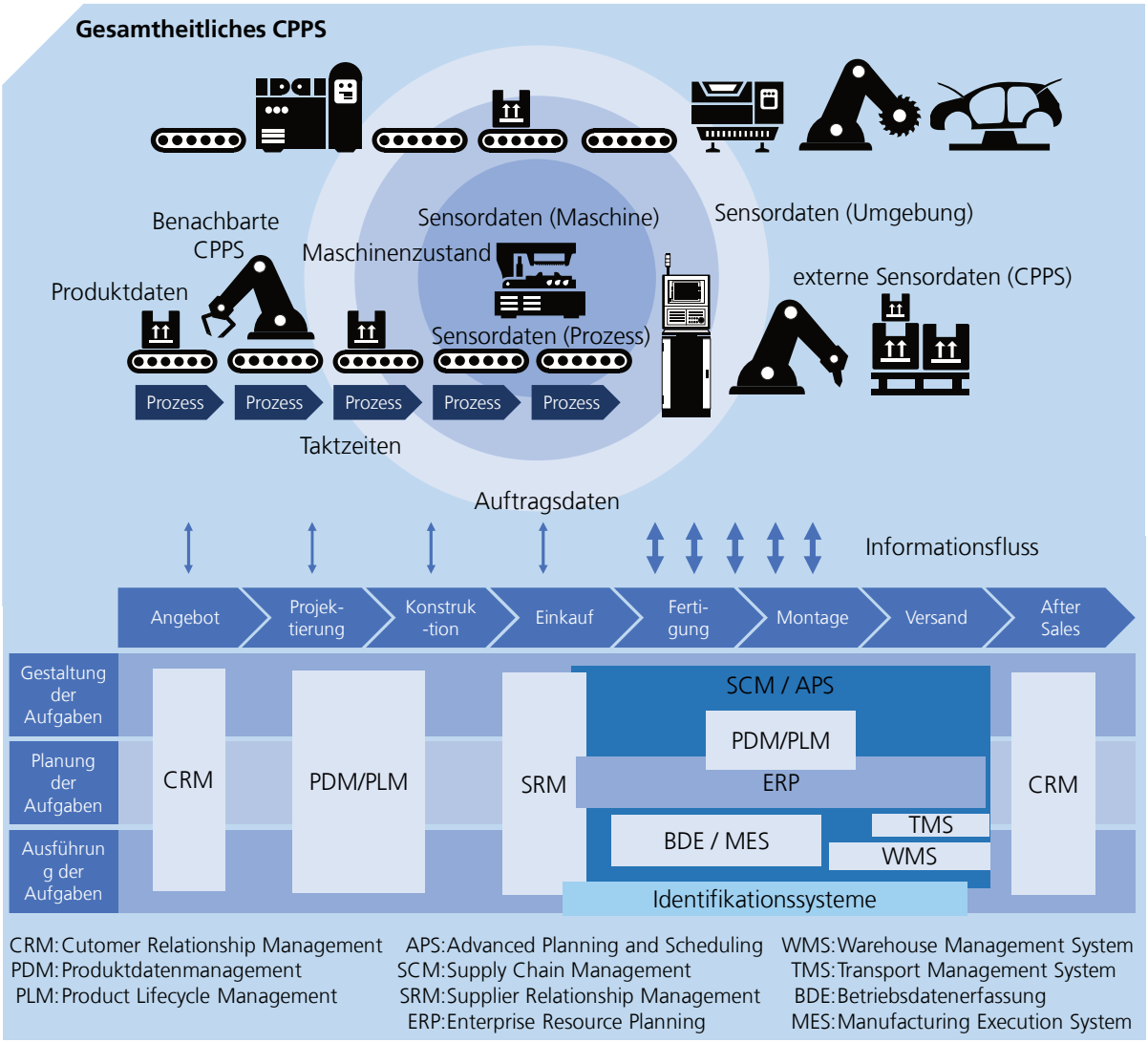


Abbildung 4.10 Merkmalsquellen in einer CPPS-basierten Produktion (Produktions-IT Systeme in Anlehnung an (Schuh et al. 2012, S. 259))

4.3.2 Merkmalsklassen und -typen

Merkmale lassen sich zwar aus den Datentypen und den damit verbundenen Quellen herleiten und so diesen zuweisen, jedoch besitzen Sie eigene Klassen und Typen.

Sie lassen sich in Anlehnung an die Eigenschaftsklassen der DIN SPEC 92000 (Datenaustausch auf der Grundlage von Eigenschaftsausprägungsaussagen, Abschnitt 2.3.1) klassifizieren. Allerdings ist im Kontext von Selbstbeschreibungsmerkmalen dieser Arbeit ihre Definition etwas abweichend und für den Ansatz adaptiert:

- **Seins-Merkmale** sind Merkmale, die die spezifische Ausprägung einer Entität mittels ihrer charakteristisch ausgeprägten Eigenschaften beschreiben.
- **Besitz-Merkmale** sind Merkmale, die nur durch ihr Vorhandensein oder Nicht-Vorhandensein eine Entität charakterisieren.
- **Wert-Merkmale** sind Merkmale, deren Ausprägung durch einfache Werte beschrieben werden können (z. B. Merkmale, Parameter, Zustände). Die Werte können nicht-metrisch (nominal (beliebige Ordnung), ordinal (feste Ordnung)) oder metrisch (Intervall, Verhältnis) skaliert werden.
- **Struktur- oder Beziehungs-Merkmale** sind Merkmale, die charakteristische Zusammenhänge beschreiben. Dazu gehören z. B. Systemmodelle oder Relationsmodelle. In diesem Fall bilden die formal möglichen Strukturvarianten die Ausprägung.
- **Fähigkeits-Merkmale** sind Merkmale, die die funktionalen Fähigkeiten einer Entität beschreiben.
- **Verhaltens-Merkmale** sind Merkmale, die das dynamische Verhalten einer Entität beschreiben. Dies ist beispielsweise ihre charakteristische Eigendynamik oder die Reaktion auf äußere Anregungen.
- **Zustands-Merkmale** sind Merkmale, deren Ausprägung sich aufgrund der internen Systemdynamik einer Entität im Betrachtungszeitraum ändern können.
- **Kontext-Merkmale** sind Merkmale, die einem zeitlichen-, örtlichen-, ereignis-, präsenz- oder interaktionsgetriebenen Kontext besitzen.

Innerhalb der Merkmalsklassen muss jedoch noch eine weitere Unterteilung vorgenommen werden. Diese ist notwendig, da nicht alle Merkmale innerhalb einer Merkmalsklasse gleichartig sind. Teilweise sind diese Untergruppen überschneidend und unscharf, weshalb eine abschließend eindeutige Klassifizierung nicht möglich ist. Allerdings können

Merkmalstypen erzeugt werden (vgl. Abschnitt 2.3.2), um eine unscharfe Einteilung durchzuführen und die Merkmale weiter zu charakterisieren. Grundsätzliche lassen sich Merkmalen gemäß ihrer Beschaffenheit wie folgt qualifizieren:

- **Statische Merkmale** sind Merkmale, die sich nicht oder über einen betrachteten Zeitraum nicht ändern.
- **Dynamische Merkmale** sind Merkmale, die keinen festen Wert oder Zustand haben und sich über einen betrachteten Zeitraum kontinuierlich ändern, wobei die Frequenz der Änderung beliebig sein kann.
- **Natürliche Merkmale** sind Merkmale, die intrinsischer Bestandteil einer Entität sind.
- **Künstliche Merkmale** sind Merkmale, die künstliche geschaffen und einer Entität zugewiesen wurden.
- **Schwache Merkmale** sind Merkmale, die im Kontext der Authentifizierung einfach zu umgehen sind.
- **Starke Merkmale** sind Merkmale, die im Kontext der Authentifizierung schwer zu umgehen sind.
- **Offene (öffentliche) Merkmale** sind Merkmale, die eine Entität öffentlich publiziert. Dies kann beispielsweise der Name einer Maschine sein. Offene Merkmale eigenen sich sehr gut zur Identifikation.
- **Geschlossene (private) Merkmale** sind Merkmale, die nicht grundsätzlich öffentlich verfügbar sind, bzw. nur für autorisierte Entitäten einsehbar sind.
- **Geschützte Merkmale** sind Merkmale, die privat sind und zugleich mit zusätzlichen Zugriffsschutzmechanismen versehen sind. So sind geschützte Merkmale beispielsweise verschlüsselt oder sie befinden sich in einem geschützten Speicherbereich.
- **Einfache Merkmale** sind Merkmale, die für sich selbst stehen und unabhängig von anderen Merkmalen betrachtet werden.

- **Aggregierte Merkmale** oder **komplexe Merkmale** sind Merkmale, die aus einer Kombination mehrerer Merkmale bestehen. Dies trifft beispielsweise auf Verhaltensmerkmale zu, die von einem bestimmten Kontext abhängig sind.
- **Kontextgebundene Merkmale** mit
    - *örtlichem* Kontext sind Merkmale, die eine Abhängigkeit zu einem bestimmten Ort oder einem Standortverlauf aufweisen, also die Position der Entität in ihrer Umwelt kennzeichnen.
    - *zeitlichem* Kontext sind Merkmale, die einen direkten Bezug zu einem bestimmten Zeitpunkt oder betrachteten Zeitraum haben, wenn sie von der Entität kommuniziert werden.
    - *präsenzbezogenem* Kontext sind abhängig von der Präsenz anderer Entitäten und geben so Auskunft über die Umgebung und indirekt über den Standort der Entität.
    - *interaktionsbezogenem* Kontext bilden bekannte und charakteristische Interaktionsmuster zwischen der betrachteten Entität und anderen Entitäten ab.
    - *ereignisbezogenem* Kontext zeigen einen direkten Bezug zu einem spezifischen Ergebnis auf, das durch eine Entität selbst oder Entitäten in seiner Umgebung ausgelöst werden können.

Unterschiedliche Merkmalsklassen können somit mit unterschiedlichen Charakteristika behaftet sein. Ein bestimmtes Merkmal kann hier auch mehrere dieser Eigenschaften in sich vereinen und so auch eine etwas unterschiedliche Typenausprägung erzeugen. Zudem ist zu beachten, dass die Daten, aus denen ein Merkmal gewonnen wird, auch Merkmale bilden können, die je nach Anwendungsfall mehreren Merkmalsklassen zugewiesen werden können bzw. eine eindeutige Zuordnung nicht möglich oder zumindest von weiteren Informationen abhängig ist.

Dies ist beispielsweise dann der Fall, wenn Daten bzw. Merkmale komplexere Beziehungen aufweisen. So kann ein Zustandsmerkmal unter Einbeziehung von Kontextdaten, wie einem bestimmten Ereignis oder Orts- und Zeitbezug, als Kontextmerkmal ausgewiesen

werden. Dieser Bezug ist bei einer ersten Betrachtung nicht unbedingt implizit und setzt tiefergehendes Wissen zum Anwendungsfall voraus. Kontextmerkmale können wiederum im Fall einer zeitlich dauerhaften und auf ihre Veränderung bezogenen Betrachtung zu Verhaltensmerkmalen werden. Auch dies setzt eine Kenntnis des Anwendungsfall-Kontextes voraus. Abbildung 4.11 stellt eine Übersicht der Merkmalsklassen, den Zusammenhang zwischen den Merkmalsklassen und ihren Eigenschaften dar.

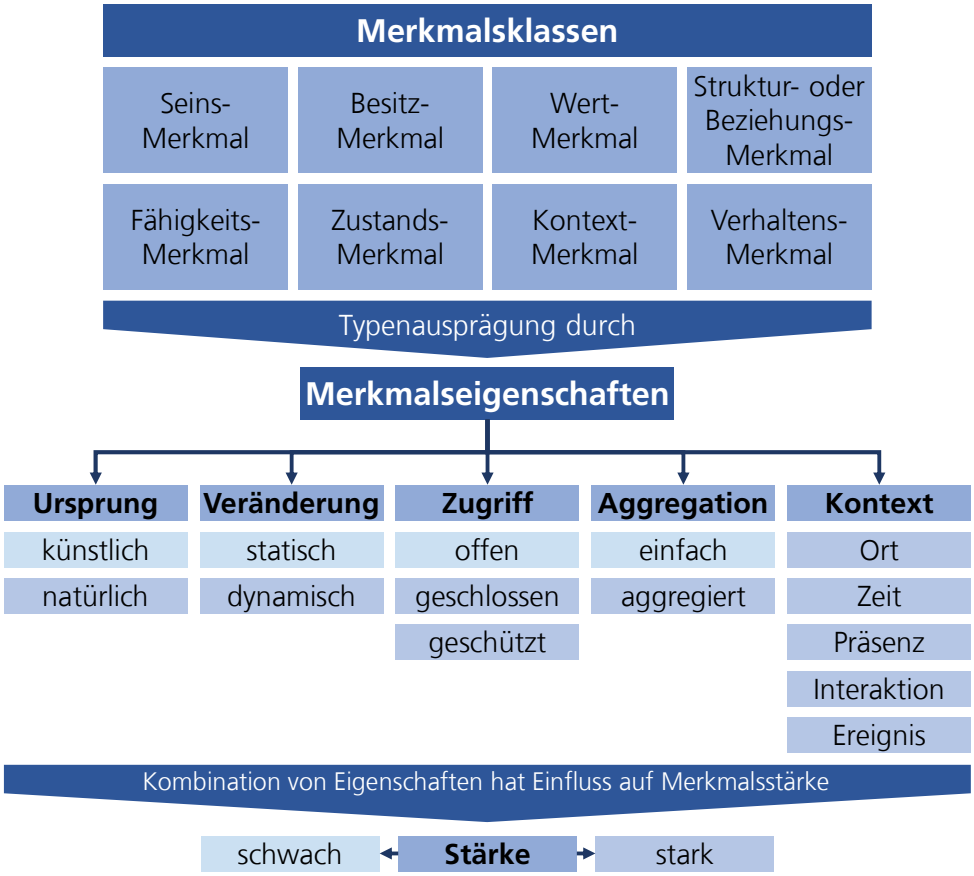


Abbildung 4.11 Merkmalsklassen und Merkmalseigenschaften

Merkmalsklassen lassen sich nicht immer definitiv mit spezifischen Eigenschaften versehen. In einigen Fällen können, wie für eine Typisierung üblich, gewisse Überschneidungen in den Eigenschaften bzw. Ausprägungen von Merkmalen auftreten. In diesem Fall kann die Entscheidung der Zuweisung einer Eigenschaft dem Anwender überlassen werden.

Im Folgenden soll allerdings als Orientierungshilfe eine generische Übersicht der Typenausprägungen eingeführt werden. Hier ist zu beachten, dass auch diese in einigen Punkten von einer ideal-objektiven Zuteilung abweichen kann und der einer nach bestem Wissen und Gewissen objektiven Darstellung des Autors entspricht. Hierzu bildet Tabelle 9 ab, welche Merkmalsklasse jeweils einen ausgeprägten Bezug zu einer oder mehreren jeweiligen Merkmalseigenschaften hat, die diese beeinflussen und so eine jeweilige Typenausprägung erzeugen.

Tabelle 9 Typenausprägung von Merkmalen durch Merkmalseigenschaften

Merkmalsklasse / Eigenschaft	Seins-Merkmal	Besitz-Merkmal	Wert-Merkmal	Struktur- / Beziehungs-Merkmal	Fähigkeits-Merkmal	Zustands-Merkmal	Präsenz-Merkmal	Verhaltens-Merkmal
natürlich	•	•	•			•	•	•
künstlich	•	•	•		•			
dynamisch			•	•		•	•	•
statisch	•	•					•	
Orts-Kontext			•				•	•
Zeit-Kontext			•			•	•	•
Präsenz-Kontext		•	•	•			•	•
Interaktions-Kontext			•	•				•
Ereignis-Kontext			•			•		•
offen	•	•	•		•	•		
geschlossen	•	•	•	•	•	•	•	•
geschützt	•	•	•	•	•	•	•	•
aggregiert				•	•		•	•
einfach	•	•	•			•		
stark	•	•	•	•	•		•	•
schwach	•		•		•	•		

Merkmalstypen, die in ihrer Ausprägung mehrere Merkmalseigenschaften in sich vereinen, weisen eine höhere Abhängigkeit von verschiedenen Kontextfaktoren auf, was die Komplexität des betrachteten Merkmals erhöht. Komplexität ist eine Eigenschaft, die prinzipiell zugunsten der Handhabbarkeit zu vermeiden ist, allerdings die Merkmalsstärke erhöht (vgl. Abschnitt 4.3.5).

4.3.3 Ableitung von Merkmalen aus Datenquellen

Die Ableitung von Merkmalen aus Datenquellen ist ein weiterer nicht-trivialer Schritt und setzt tiefergehendes Wissen über die jeweilige Anwendung voraus. Die Erkenntnis darüber, welche Daten und Informationen in welcher Form als Merkmal in einer bestimmten Ausprägung dienen können ist stark vom Wissen und der Erfahrung eines Anwenders abhängig. So stellt bereits die Wissenstreppe den Zusammenhang zwischen Zeichen, Daten, Informationen und Wissen dar. Hierbei kann die Bestimmung eines Merkmals und seiner Eigenschaften als der Handlungsschritt eine Ebene über dem Wissen zu einem Merkmal interpretiert werden. Dieses Wissen muss entsprechend formalisiert dargestellt werden, um möglichst einfach maschinell verarbeitbar zu werden (vgl. Abschnitt 1.1 und 3.2.1). Abbildung 4.12 stellt den schematischen Ablauf der Bestimmung vom Datum zum Merkmal dar.

Die formale Logik zur Bestimmung der Bedeutung bestimmter Daten lässt sich hier durch den Einsatz von Informations-Ontologien abbilden. Diese ermöglicht es Daten mittels zusätzlicher Semantik und einem Kontext in Informationen umzuwandeln. Der nächste Schritt ist allerdings für die Ableitung von Merkmalen kritisch, da durch die Verknüpfung bzw. Vernetzung zwischen weiteren Daten und Informationen Wissen über diese Daten geschaffen wird, welches es erlaubt ihre Eignung als Merkmal zu bewerten.

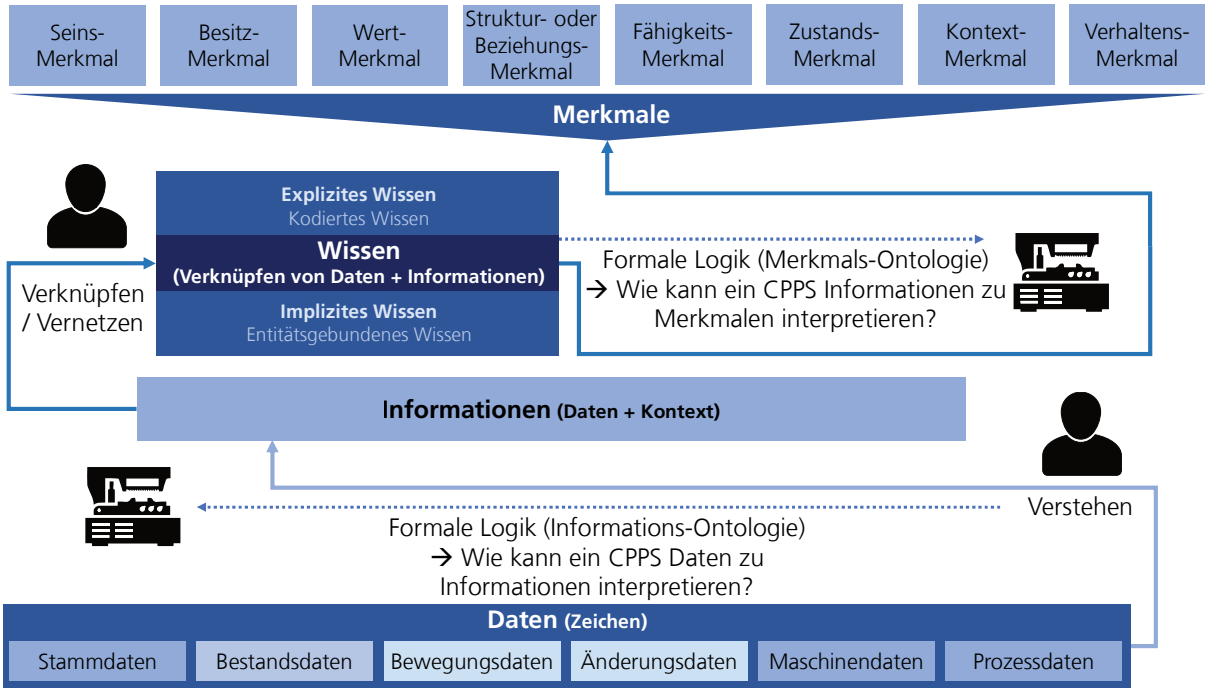


Abbildung 4.12 Ableitung von Merkmalen aus betrieblichen Datentypen in einem ganzheitlichen CPPS

Explizites Wissen, also das eindeutig kodierte und mittels Zeichen eindeutig kommunizierbare Wissen, lässt sich hier ebenfalls in einer Merkmals-Ontologie abbilden. Allerdings existiert noch das implizite Wissen, über das Anwender oft verfügen, welches sich jedoch nur schwer eindeutig formulieren lässt.

Hier versucht die vorliegende Arbeit durch die Definition von festen Merkmalsklassen und zugehörigen Eigenschaftsausprägungen einem Anwender, der über implizites Wissen verfügt, ein Hilfsmittel an die Hand zu geben, mittels dessen dieses Wissen in eine Formale Logik überführt werden kann. Welche Art von (Betriebs-) Daten zudem meist mit einer jeweiligen Merkmalsklasse korreliert ist in Tabelle 10 dargestellt.

Tabelle 10 Ableitungsmöglichkeiten von Merkmalen aus Datentypen

	Seins-Merkmal	Besitz-Merkmal	Wert-Merkmal	Struktur- / Beziehungs-Merkmal	Fähigkeits-Merkmal	Zustands-merkmal	Präsenz-Merkmal	Verhaltens-Merkmal
Stammdaten	●	●	●		●	●	●	
Bestandsdaten	●	●	●					
Bewegungsdaten			●	●			●	●
Änderungsdaten		●					●	●
Maschinendaten	●	●	●		●	●	●	●
Prozessdaten			●			●	●	●

4.3.4 Merkmalsbasierte Authentifizierungsfaktoren und Eignungskriterien

Die in Abschnitt 4.3.2 dargestellten Merkmalsklassen lassen sich Authentifizierungsfaktoren (Abschnitt 3.1.4) zuteilen und stellen somit die Grundlage einer selbstbeschreibungsbasierten Identifikation und Authentifizierung dar. Die merkmalsbasierten Authentifizierungsfaktoren müssen, wie die Bezeichnung andeutet, aus den entsprechenden Merkmalen hergeleitet werden. In Anlehnung an die Prinzipien der aktiven Authentifizierung für Personen (siehe Abbildung 3.5) lässt sich wie in Abbildung 4.13 dargestellt für CPPS eine Hierarchie von Merkmalen und daraus abzuleitenden Authentifizierungsfaktoren aufbauen.

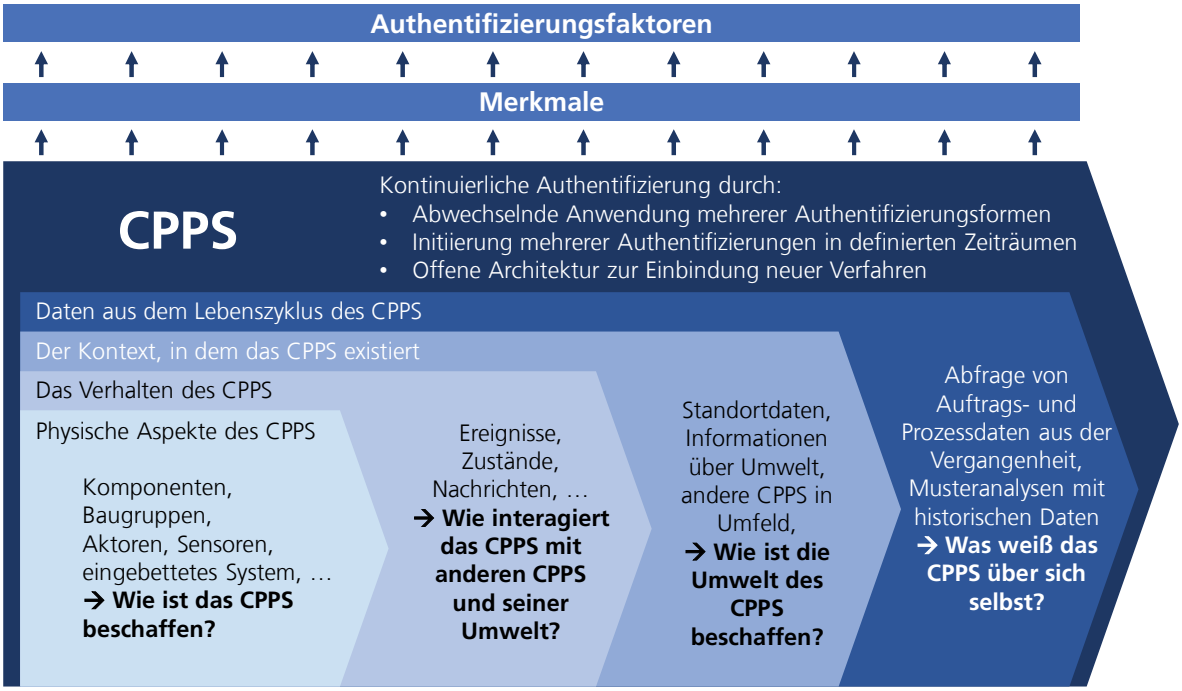


Abbildung 4.13 Bestimmung von Authentifizierungsfaktoren aus Merkmalen

Diese Hierarchie bezieht sich auf die in den vorherigen Abschnitten diskutierten Merkmale und ihre Merkmalsquellen eines CPPS, die zugehörigen verteilten Dienste im gesamtheitlichen CPPS und die darin enthaltenen betrieblichen Daten. Die Abbildung von Merkmalen

auf Authentifizierungsfaktoren lässt wie bei den klassischen Authentifizierungsfaktoren für die Multifaktor-Authentifizierung (Abschnitt 3.1.7) durchführen und um zusätzliche Faktoren erweitern. Dies ist möglich, da ein CPPS und eine zugehörige Authentifizierung mit einem größeren Merkmalsraum arbeiten kann, als es einem Menschen zumutbar wäre. Diese zusätzlichen Selbstbeschreibungsfaktoren und der Bezug der Authentifizierungsfaktoren zu diesen sind in Abbildung 4.14 abgebildet. Da Selbstbeschreibungsmerkmale als Authentifizierungsfaktoren fungieren, müssen sie auf ihre Eignung geprüft werden. Es muss auch unterschieden werden, ob ein Merkmal nur für eine Identifikation eingesetzt wird oder ob es für eine Authentifizierung eingesetzt werden kann. Hierbei können prinzipiell die gleichen Eignungskriterien angesetzt werden wie für biometrische Merkmale (Abschnitt 4.2.1.1).

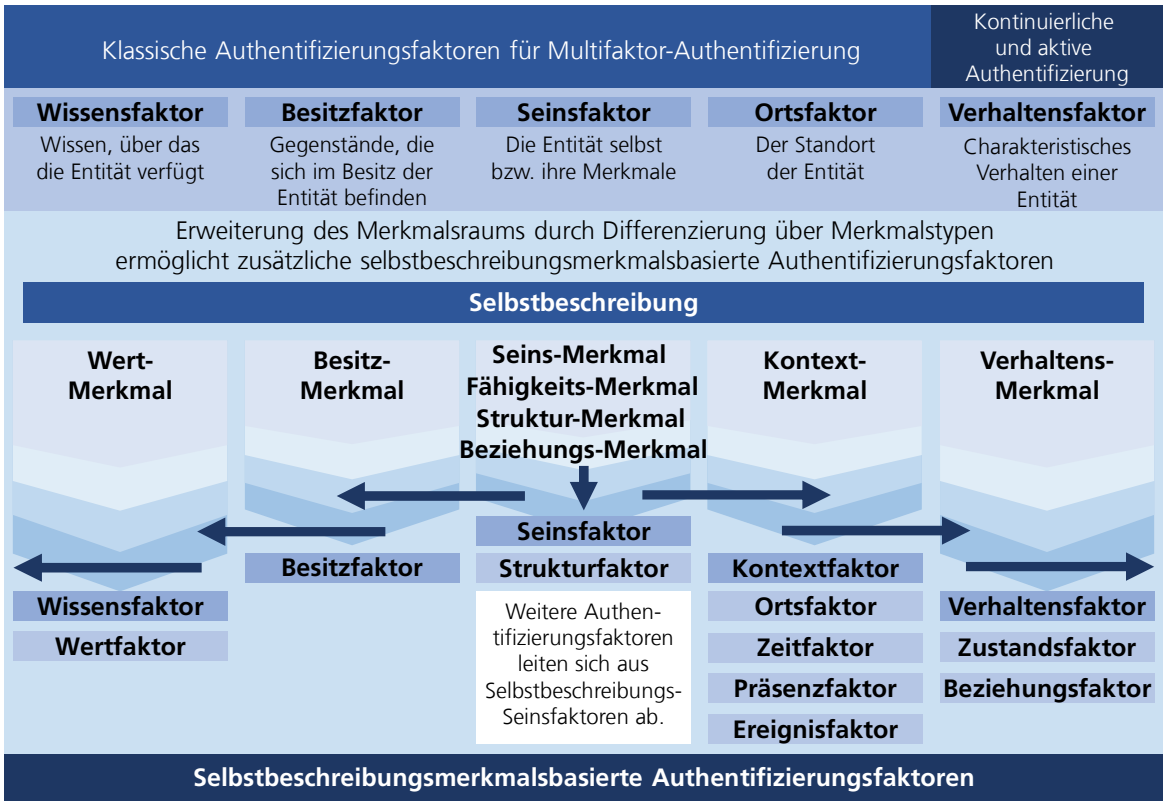


Abbildung 4.14 Authentifizierungsfaktoren auf Basis von Selbstbeschreibungsmerkmalen

Allerdings müssen diese in ihrer Definition teilweise etwas angepasst werden, da ein CPPS kein lebendiger Organismus ist und die ihm zugehörigen Merkmale sich ebenso in ihrem Verhalten unterscheiden. Die Eignungskriterien für Authentifizierungsfaktoren auf Basis von Selbstbeschreibungsverfahren lauten somit:

- **Universalität**: ein Merkmal ist bei jeder Entität vorhanden.

Menschen sind in ihrer grundsätzlichen Beschaffenheit gleich und verfügen somit über die gleichen Merkmale, was die Grundlage der Funktionsweise der biometrischen Identifikation ist. Maschinen und Dienste sind in ihrer Ausprägung jedoch so unterschiedlich, dass man sie zunächst Klassifizieren bzw. Typisieren muss, da prinzipiell gleiche Maschinen oder Dienste, die dieselben Fähigkeiten und Aufgaben besitzen, andere Komponenten mit verschiedenen Eigenschaften beinhalten können, die Einfluss auf das Merkmal haben. Dies muss bei der Identifikation und bei der darauffolgenden Authentifizierung berücksichtigt werden.

- **Einzigartigkeit**: keine zwei Entitäten sollten über dasselbe Merkmal verfügen.

Dadurch, dass Maschinenkomponenten künstlich hergestellt und Dienste programmiert und nur virtuell existent sind, kann nicht ausgeschlossen werden, dass zwei unterschiedliche Entitäten identische Merkmale aufweisen. Deswegen muss eine Merkmalsart gewählt werden, die dieses Eignungskriterien erfüllt. Grundsätzlich ist jedoch ein ausreichend großer Merkmalsraum und eine Kombination von mehreren Merkmalen oder die Generierung von Merkmalsvektoren notwendig, um eine eindeutige bzw. sichere Identifikation und Authentifizierung zu ermöglichen.

- **Permanenz**: ein Merkmal ist zeitlich invariant.

Während die künstliche Natur von Maschinen und Diensten einen Nachteil für die Einzigartigkeit darstellen kann, stellt sie für die Permanenz einen Vorteil dar. Die Stabilität vieler dynamischen Merkmale kann eine hohe Permanenz aufweisen. Merkmale, die über einen zeitlichen Verlauf Veränderungen aufweisen, können jedoch auftreten. Folgt die Veränderung einem bestimmbaren Muster, so kann dieses Verhalten selbst als Merkmal ver-

wendet werden und die Permanenz des Merkmals zeichnet sich durch den deterministischen Charakter dieser Veränderung aus. Unbekannte, beispielsweise zufällige oder unvorhergesehene Veränderungen außerhalb bestimmter Toleranzen, können wiederum ein Anzeichen dafür sein, dass ein Merkmal nicht authentisch ist.

- **Erfassbarkeit**: ein Merkmal lässt sich quantitativ erheben.

Auch hier profitieren Maschinen und Dienste, insbesondere CPS mit ihren Selbstfähigkeiten, davon, dass sie die Technologie zur quantitativen Erhebung von Merkmalen entweder bereits in sich tragen oder diese vergleichsweise einfach zu integrieren ist.

- **Robustheit**: ein Merkmal lässt sich mit hoher Zuverlässigkeit und Genauigkeit unter verschiedenen Umgebungsbedingungen erfassen.

Die Robustheit hängt wiederum von der Art des Merkmals ab. Insbesondere dynamische Merkmale, die aus Sensoren der Verhaltensmuster entstammen, können stark von den Umgebungsbedingungen abhängen. Daher können für dynamische Merkmale probabilistische Bewertungsmethoden eingesetzt werden.

- **Akzeptanz**: Anwender akzeptieren die Nutzung eines Merkmals und des technischen Systems, welches zur Erfassung genutzt wird.

Akzeptanz ist ein Kriterium, das bei Menschen einerseits in der Privatheit und dem Datenschutz fußt, andererseits aber auch darin, dass die Erfassung des Merkmals für den Menschen ggf. nicht zumutbar ist. Diese Faktoren sind für CPS nicht relevant, allerdings kann ein Merkmal, welches IP-relevante Informationen enthält, beispielsweise bestimmte Prozessdaten, dieses Kriterium eines Faktors tangieren.

- **Umgehungssicherheit**: Der Aufwand ein Merkmal bzw. das System zur Erfassung zu umgehen oder zu täuschen sollte möglichst hoch sein.

Auch hier hängt es von der Merkmalsklasse oder dem Merkmalstyp ab, ob das Merkmal einfach zu umgehen ist. Das System zur Erfassung sollte außer in Ausnahmefällen das CPPS selbst sein. Ziel der selbstbeschreibungs-merkmalsbasierten Authentifizierung soll sein, diese Umgehung zu erschweren bzw. die Umgehungssicherheit in der Gesamtheit zu erhöhen, selbst wenn einzelne Merkmale umgangen werden können. Grundsätzlich

ist bei einer Bestimmung von Selbstbeschreibungsmerkmalen, die als Authentifizierungsfaktoren dienen sollen, zu beachten, dass diese die Eignungskriterien weitestgehend erfüllen. Die Einflussfaktoren, die die Eignung eines Merkmals bzw. seine Eignungskriterien für ein Authentifizierungsverfahren festlegen, sind in Abbildung 4.15 geordnet dargestellt. Sie zeigen, dass neben Einflussfaktoren auf Daten und den Umgang mit diesen die jeweiligen Erfassungsverfahren und im einigen Fällen unvorhergesehenes Verhalten eines CPPS die Eignungskriterien negativ beeinflussen können.

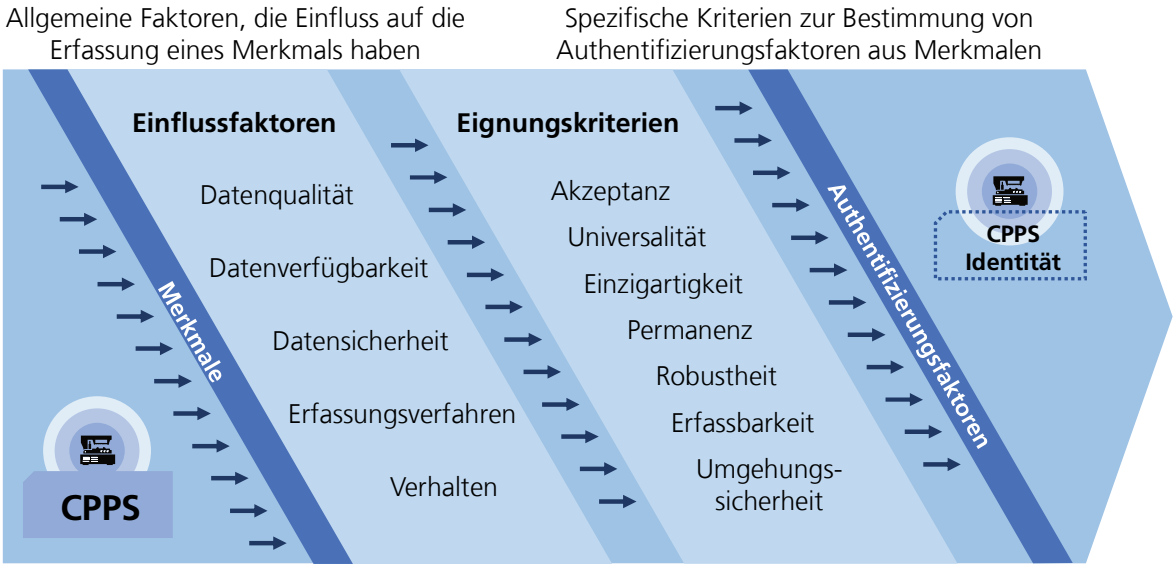


Abbildung 4.15 Einflussfaktoren auf Merkmalsstärke und Eignung als Authentifizierungsfaktoren

Da der hier verfolgte Ansatz den Einsatz von möglichst vielen dieser Merkmale zur Authentifizierung vorsieht, können Faktoren, die ein oder mehrere schwach ausgeprägte Eignungskriterien besitzen durch die anderen Faktoren ausgeglichen werden. Ein formelles Verfahren zur empirisch-qualitativen Bewertung einzelner Faktoren liegt außerhalb des Umfangs dieser Arbeit, jedoch lässt sich der hier verfolge Ansatz durch den Framework-Charakter durch einen solchen Verfahrensschritt erweitern.

4.3.5 Merkmalsgewichtung

Ausgehend von den Eignungskriterien für die Authentifizierungsfaktoren auf Basis von Selbstbeschreibungsmerkmalen ist zu erkennen, dass Merkmale sich nicht nur in ihrer grundsätzlichen Art und Ausprägung unterscheiden. Ein Merkmalstyp bzw. ein spezifisches Merkmal, das bei einer Entität vorkommt und bestimmte Eignungskriterien erfüllt, kann bei einer anderen Entität und in einem anderen Kontext ggf. eine abweichende Bewertung der Eignungskriterien besitzen. Zudem ist zu beachten, dass die Merkmale einer Entität, die zur Identifizierung bzw. Authentifizierung ausgewählt werden durch diesen Umstand auch in Bezug zueinander gesetzt unterschiedliche Aussagekraft besitzen können. Das bedeutet, dass ein offenes, statisches und künstliches Merkmal sich zwar gut für eine schnelle und präzise Identifizierung eignen kann, jedoch einfach zu umgehen ist und somit alleinstehend nicht für eine verlässliche Authentifizierung geeignet ist. Ein natürliches, dynamisches und geschütztes Merkmal ist jedoch nur mit erheblichem Aufwand zu umgehen. Es ist jedoch aufgrund seiner ggf. probabilistischen Natur weniger robust. Daher empfiehlt es sich die jeweiligen Merkmale einer Entität bzw. eines Entitätstyps zu gewichten.

Tabelle 11 Gewichtungsfaktoren der Merkmalseigenschaften

Ursprung me(U)	Veränderung me(V)	Zugriff me(Z)	Aggregation me(A)	Kontext me(K)
$me(U)_{natürlich}$	$me(V)_{dynamisch}$	$me(Z)_{offen}$	$me(A)_{einfach}$	$me(K)_{Ort}$
0,8	0,8	0,1	0,4	0,2
$me(U)_{künstlich}$	$me(V)_{statisch}$	$me(Z)_{geschlossen}$	$me(A)_{aggregiert}$	$me(K)_{Zeit}$
0,2	0,2	0,3	0,6	0,2
		$me(Z)_{geschützt}$		$me(K)_{Präsenz}$
		0,6		0,2
				$me(K)_{Interaktion}$
				0,2
				$me(K)_{Ereignis}$
				0,2

Tabelle 11 listet die in Abschnitt 4.3.2 bzw. Abbildung 4.11 dargestellten Merkmalseigenschaften auf. Der jeweiligen Ausprägung wird ein Gewichtungsfaktor zugewiesen. Die Werte der Faktoren sind so festgelegt, dass die jeweiligen Ausprägungen einer Merkmalseigenschaft in Summe 1 ergeben.

Innerhalb eines Geltungsbereichs, beispielsweise einem übergeordneten ganzheitlichen CPPS-Verbund oder einer Domäne, müssen diese Faktoren den gleichen Wert besitzen, um eine Basis-Referenz zu bieten und eine grundsätzliche Vergleichbarkeit zu ermöglichen.

Dabei sind Ursprung, Veränderung, Zugriff und Komplexität Merkmalseigenschaften, deren Ausprägung exklusiv zugewiesen wird. Die Kontext-Eigenschaft ist jedoch kumulativ, da ein Merkmal mehrere Kontext-Ausprägungen zugleich aufweisen kann. Diese Merkmalseigenschaften bilden die individuelle Merkmalsstärke ms_i eines Merkmals, die somit als die Summe der Ausprägungsfaktoren definiert wird:

$$\mathrm{ms}_i = \sum \mathrm{me(X)}_x = c_u * me(U)_u + c_u * me(V)_v + c_u * me(Z)_z$$
$$+c_u * me(A)_a + c_u * me(K)_{\sum k}$$

$c_x > 1$

Für jede Merkmalseigenschaft kann wahlweise ein Koeffizient als Verstärkungsfaktor festgelegt werden, um die individuelle Merkmalstärke zu erhöhen. Dies ist dann sinnvoll, wenn ein Merkmal sich zwar aus identischen Merkmalseigenschaften zusammensetzt wie ein anderes Merkmal desselben oder eines anderen CPPS, jedoch bedingt durch das implizite Wissen über dieses Merkmal bzw. seine Typenausprägung eine höhere Bewertung der Merkmalsstärke angesetzt werden soll. Verfügt man über eine ausreichend große Datenbasis von Selbstbeschreibungsmerkmalen und Informationen zu ihrer Typisierung kann hierfür sogar explizites Wissen herangezogen werden und der Prozess zur Bewertung der Merkmalsstärken automatisiert werden. Auch hier muss darauf geachtet werden, dass

innerhalb eines Geltungsbereichs eine objektive Bewertung gleichartiger Merkmale durchgeführt wird, wenn ein Merkmal durch den Einsatz von Koeffizienten modifiziert wird.

Die individuellen Merkmalsstärke-Werte eines CPPS sind die Grundlage für weitere Metriken, die einer differenziertere Betrachtung der Merkmalseigenschaften eines CPPS dienen. Die Summe der Merkmalsstärke-Werte eines CPPS ergibt die Gesamtmerkmalsstärke. Der Merkmalsindex ist das Verhältnis der tatsächlichen Gesamtmerkmalsstärke und der maximal möglichen individuellen Merkmalsstärke, die das Produkt der Anzahl der Merkmale und der maximalen die individuellen Merkmalsstärke ist.

Zudem kann ein Grenzwert bestimmt werden, der eine objektive Unterscheidung zwischen einem schwachen und einem starken Merkmal erlaubt. Dies kann beispielsweise der Mittelwert der minimalen und maximalen individuellen Merkmalsstärke sein.

Aus der Anzahl der schwachen und starken Merkmale kann ebenfalls ein Verhältnis ermittelt werden, das Aufschluss darüber erlaubt, ob bei einem CPPS die Anzahl der starken Merkmale überwiegt. Ein CPPS mit 100 schwachen und 10 starken Merkmalen hat zwar in Summe gleich viele Merkmale vorzuweisen wie eines mit 10 schwachen und 100 starken Merkmalen, allerdings erzeugen diese Merkmale ein höheres Vertrauenslevel (vgl. Abschnitt 3.1.8).

4.3.6 Zwischenfazit

Zur Erstellung eines digitalen Fingerabdrucks steht in der vernetzten Produktion eine Vielzahl von Datenquellen zur Verfügung, die in diesem Kapitel umfassend diskutiert wurden. Hier können sowohl das CPPS selbst als auch die mit dem CPPS vernetzten IT-Systeme und weitere CPPS herangezogen werden. Diese Datenquellen stellen meist auch Merkmalsquellen dar, aus denen sich Merkmale direkt gewinnen oder ableiten lassen. Merkmale unterscheiden sich in ihrer Beschaffenheit und in ihrem Kontext, was wiederum Auswirkung auf ihre Eignung als Merkmale zur Identifikation und Authentifizierung hat. Daher wurden an dieser Stelle zur systematischen Charakterisierung der Merkmale Merkmalsklassen und -typen eingeführt, die eine Einordnung, Unterscheidung und Bewertung

von Merkmalen zum Zweck des Einsatzes als Authentifizierungsfaktoren und eine Gewichtung einzelner Merkmale erlauben. Durch die systematische Ordnung von Merkmalen lässt sich die durch ihre Anzahl und Verschiedenartigkeit begründete Komplexität reduzieren, so dass sie effizient für einen strukturierten digitalen Fingerabdruck verwendet werden können.

4.4 Schaffung einer Identität aus Selbstbeschreibungsmerkmalen

Nachdem mit den Selbstbeschreibungsmerkmalen die Bausteine, aus denen sich die Identität einer Entität zusammensetzt, erläutert und definiert wurden, wird im Folgenden dargestellt, die wie eine Identität aus diesen konstruiert werden kann. Zudem wird der Lebenszyklus dieser Identität skizziert und wie die Identifikation einer Entität mittels der Selbstbeschreibungsmerkmale der digitalen Identität durchgeführt werden kann.

4.4.1 Grundbausteine eines CPS und CPPS

Das idealtypische CPS ist in Abschnitt 2.2 beschrieben. Aktuell finden sich jedoch kaum Maschinen, die die Fähigkeiten eines solchen CPS allumfassend besitzen. Insbesondere die Fähigkeit zur Autonomie ist bisher nur rudimentär ausgeprägt und im Fokus aktueller Forschungsbestrebungen im Themengebiet der Künstlichen Intelligenz. Zudem verfügen die meisten „smarten" Maschinen über unterschiedlich stark ausgeprägte Self-X Fähigkeiten. Im Rahmen dieser Arbeit soll daher eine zusätzliche Differenzierung verwendet werden, um diese „Proto-CPS" von den idealtypischen CPS zu unterscheiden.

So werden hier die atomaren und eigenständigen Bestandteile eines CPS als Smarte Objekte und Smarte Applikationen bezeichnet. Smarte Objekte sind der physische Teil eines CPS, verfügen jedoch noch um keine ausgelagerten Fähigkeiten in Form bestimmter Dienste. Smarte Applikationen sind ausschließlich in der Cyber-Welt beheimatet, sind aber auf keine physischen Komponenten angewiesen. Aus der abstrakten Sicht eines informationstechnischen Systems stellen sowohl Smarte Objekte als auch Smarte Applikationen

bestimmte Fähigkeiten in Form von Events und Operationen in Form von Diensten bereit, die neben zusätzlichen Metadaten in ihrer Selbstbeschreibung dargestellt sind. Daher erben beide von der abstrakten Klasse eines Smarten Dienstes, der eine fachliche Funktionalität und damit eine Fähigkeit in sich kapselt. Erst die Kombination mindestens eines Smarten Objekts mit einem anderen oder einer Smarten Applikation bildet ein Proto-CPS, da durch diese Verknüpfung die Verbindung einer höherwertigen physischen und cyber-Komponente stattfindet. Abbildung 4.16 illustriert dieses Prinzip.

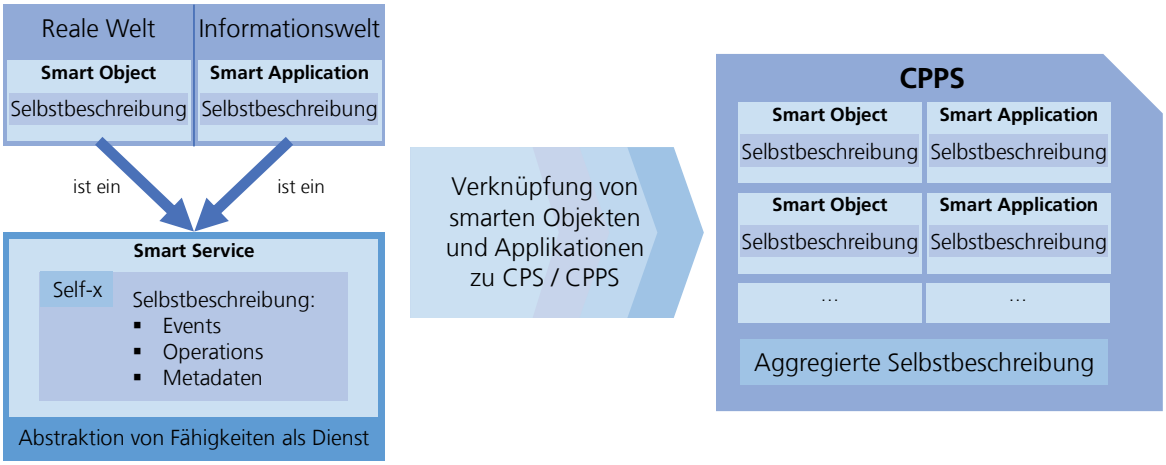


Abbildung 4.16 Smarte Objekte und Dienste als kleinste atomare CPPS Bausteine in Anlehnung an (Stock et al. 2020b)

Der beschriebene Ansatz findet bereits Anwendung in einer Implementierung des in Abschnitt 3.2.5 beschriebenen Manufacturing Service Bus. Das formale Datenmodell hierzu ist in Abbildung 4.17 dargestellt, eine beispielhafte Instanziierung kann Anhang 4 entnommen werden. Dieses einfache Datenmodell verfügt über eine Beschreibung der Datenfelder der jeweiligen Operationen und Events, die zum Zweck der syntaktischen Kompatibilität der Komponenten in einem einheitlichen Datenformat nach dem OpenAPI Specification 2.0 beschrieben sind. Dies erlaubt einen programmiersprachenagnostischen Austausch von Nachrichten zwischen Diensten und Objekten bzw. CPS über den MSB, der ein durch einen Nutzer frei definierbares Mapping der jeweiligen Datenformate erlaubt.

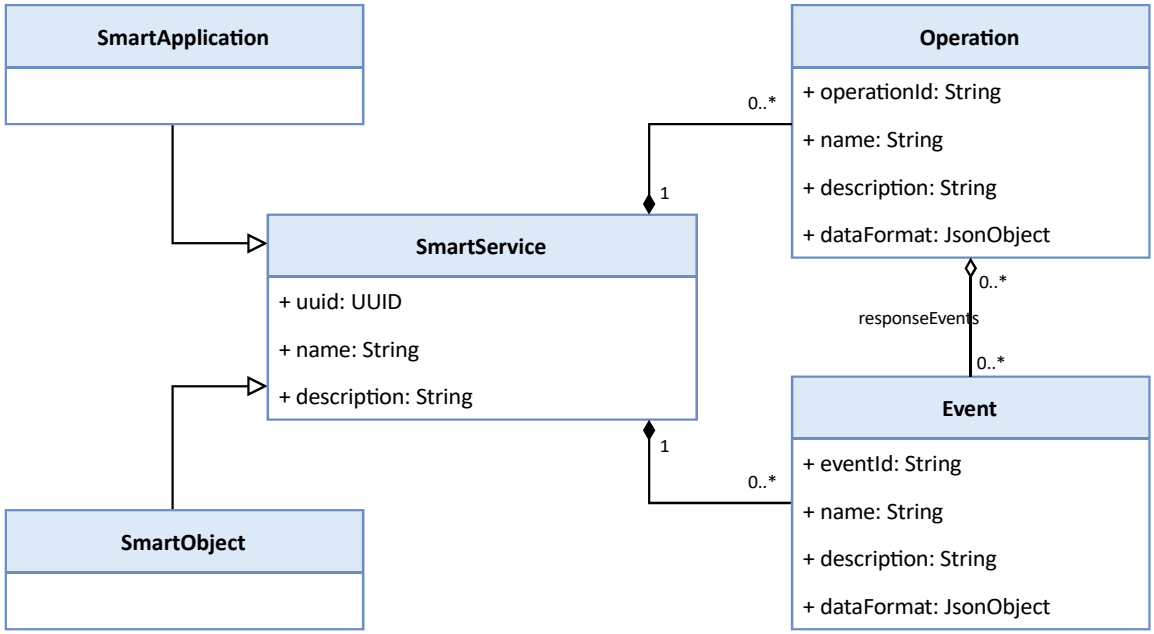


Abbildung 4.17 Smart Object und Smart Service Datenmodell nach (Schel et al. 2018)

4.4.2 Die digitale Identität eines CPPS und ihr Lebenszyklus

Eine digitale Identität (vgl. Abschnitt 2.4.1) durchläuft von ihrer Erschaffung bis zu ihrer Löschung mehrere Zustände. Eine Identität eines CPPS besitzt demnach einen Lebenszyklus, der in Abbildung 4.18 dargestellt ist. Die Lebenszyklusphasen ermöglichen es eine diesem Kontext entsprechende Zuweisung von Rechten mit Hilfe eines Identitätsmanagements (IdM, vgl. Abschnitt 3.1.1) durchzuführen und ihre Autorisierung für Zugriffe auf Informationen und Ressourcen zu kontrollieren. Die grundsätzlichen funktionalen Anforderungen an ein IdM und die Verwaltung von Identitätsinformationen lassen sich der ISO/IEC Norm 24760-2 „Information technology - Security techniques - A framework for identity management - Part 2: Reference architecture and requirements“ entnehmen (Abschnitt 3.1.2).

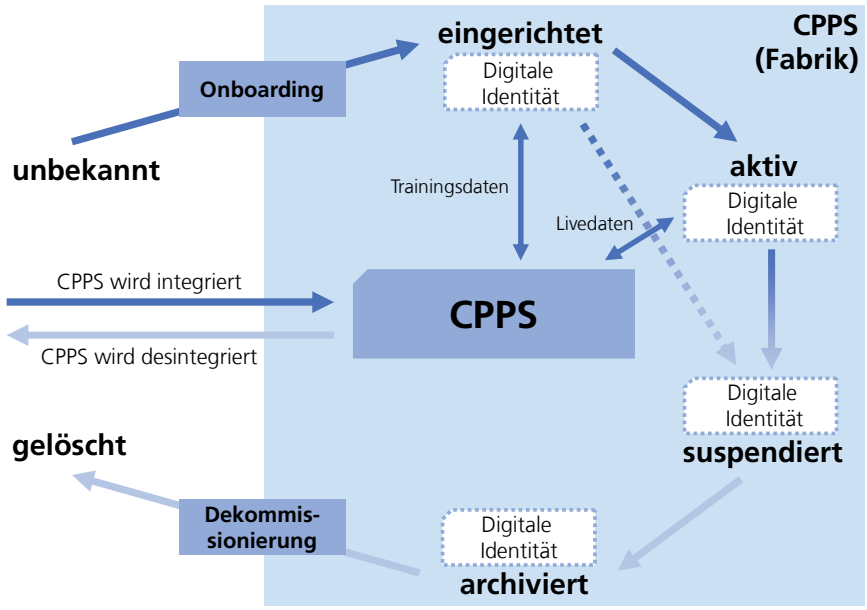


Abbildung 4.18 Lebenszyklus einer digitalen Identität

Die Zustände, die ein Identität in ihrem Lebenszyklus durchläuft, haben im Kontext des hier diskutierten Ansatzes folgende Bedeutung:

- **unbekannt** – eine Entität besitzt keine digitale Identität, kann daher nicht zu einer Authentifizierung herangezogen werden und wird daher vom System abgewiesen.
- **eingerichtet** – eine digitale Identität wurde für eine Entität eingerichtet und diese kann im System integriert werden. Mittels zusätzlicher Trainingsdaten der Entität kann diese weiter abgesichert werden. Die digitale Identität der Entität kann nun mit den vorgesehenen Rollen und Rechten versehen werden, allerdings sind diese noch nicht aktiv benutzbar. Die digitale Entität ist unter Umständen nach ihrer Einrichtung in einem suspendierten Zustand, bis eine explizite Freigabe in einen eingerichteten oder aktiven Zustand stattfindet.
- **aktiv** – im aktiven Zustand werden die zugewiesenen Rollen und Rechte der Entität aktiv und die Entität kann ihre fachlichen Aufgaben vollständig ausführen.
- **suspendiert** – die Rollen und Rechte der Entität werden vorübergehend eingezogen. In diesem Zustand kann die Entität keine fachlichen Aufgaben ausführen, allerdings kann ggf. eine eingeschränkte Authentifizierung durchgeführt werden.

- **archiviert** – die digitale Identität einer Entität wird stillgelegt, mit der Option diese bei Bedarf zu reaktivieren. Die Entität wird in diesem Fall innerhalb des Systems als unbekannt behandelt und es kann keine Authentifizierung durchgeführt werden.
- **gelöscht** – die digitale Identität einer Entität wird gelöscht, ohne die Option diese wiederherzustellen. Die Entität ist im System nicht mehr bekannt und bei Bedarf muss eine neue digitale Identität geschaffen werden.

Eine Entität, insbesondere im Fall eines CPPS, kann mehrere digitale Identitäten besitzen. Dies ist ausdrücklich dann möglich, wenn beispielsweise kontextuelle Identitäten eingesetzt werden (vgl. Abschnitt 2.4.1). Während sich kontextuelle Identitäten bei Personen als kontextabhängige Rollen darstellen, sind sie bei CPS komplexer gelagert.

Insbesondere der „System of Systems"-Aspekt als intrinsisches Merkmal eines CPS (Abschnitt 2.2.1) wirft die Frage auf, wie sich nun eine digitale Identität darstellt, die sich aus mehreren physischen Identitäten einzelner Entitäten zusammensetzt. In Abschnitt 2.2.6 wird das kontextuelle Zusammensetzen von CPPS zu einem bestimmen Einsatzzweck diskutiert, das für die Middleware-basierte strukturelle Modellierung von CPPS eingesetzt werden kann (Stock et al. 2020b). Das Prinzip hierzu ist in Abbildung 4.19 skizziert. Diese Fähigkeit trägt auch das Wertversprechen von CPPS mit, welches die Flexibilisierung der Produktion ermöglicht, indem eine CPPS basierte Anlage bedarfsgerecht und schnell neu strukturiert und (re-)konfiguriert werden kann. So können sich Komponenten eines CPS, die in ihrer kleinsten Einheit selbst über gewisse CPS-Fähigkeiten verfügen müssen und die einfachste Ausprägung eines CPS darstellen, zu einem „höherwertigen" CPS oder CPPS formieren, wie im vorherigen Abschnitt diskutiert. Dieser neue Verbund stellt allerdings eine neue Entität dar, die eine eigene digitale (kontextuelle) Identität benötigt.

Zudem setzt sie sich aus mehreren Entitäten zusammen, die eigene digitale Identitäten benötigen können oder bereits besitzen. Die digitale Identität lässt sich im Fall des CPPS aus der Selbstbeschreibung bzw. aus der Aggregation der Selbstbeschreibung der einzelnen Bausteine des CPPS ableiten (vgl. Abbildung 4.16). Im Umkehrschluss lassen sich die Identitäten der einzelnen Bestandteile eines CPPS als Teilidentitäten bzw. partielle Identitäten bezeichnen.

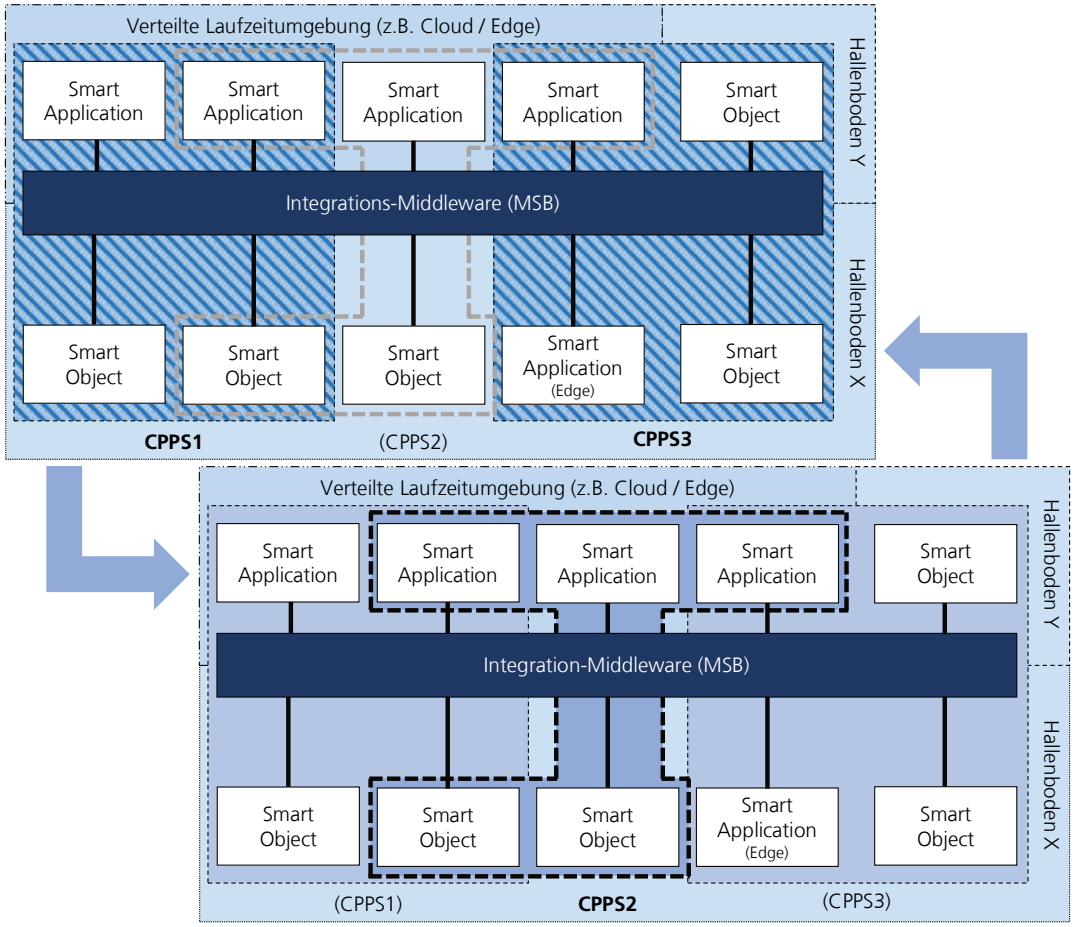


Abbildung 4.19 CPPS-Komponenten-Deployment, -Kommunikation, -Austausch und -Neukonfiguration nach (Stock et al. 2020b)

Das Konzept einer „partiellen Identität" wird in der Norm ISO/IEC 24760-1 „IT Security and Privacy – A framework for identity management – Part 1: Terminology and concepts" definiert, bezieht sich jedoch nur auf ein Subset eines Merkmalsatzes, der eine Identität ausmacht (Norm ISO/IEC 24760-1). Dieser Ansatz ist insofern übertragbar, da eine Selbstbeschreibung eines CPPS im Prinzip eine strukturierte Darstellung von Merkmalen ist. Somit ist die Selbstbeschreibung einer Komponente eines CPPS teil der aggregierten Selbstbeschreibung und stellt ein Subset ihres Merkmalssatzes dar. Allerdings sind diese Merkmale erst einmal statisch, was bedeutet, dass sie sich nicht ändern. Folgt man dieser Definition, dann können mehrere Entitäten dieselbe Identität besitzen, falls nicht spezielle

künstliche Merkmale in Form von Identifikatoren eingesetzt werden, die eine Eindeutigkeit des Merkmals innerhalb der betrachteten Systemgrenzen oder einer Domäne garantieren. Würde man beispielsweise eine Produktionslinie aus mehreren CPPS-basierten Maschinen betrachten, die aus den gleichen und identisch konfigurierten CPS-Komponenten bzw. smarten Objekten und Applikationen bestehen, dann könnte man ohne den Einsatz von Identifikatoren keine Unterscheidung und somit eindeutige Identifikation der jeweiligen Entitäten durchführen. Da die Merkmale zusätzlich zur Authentifizierung genutzt werden sollen sind sie als rein statische Merkmale nur bedingt nutzbar, da eine unbefugte Entität diese statischen Merkmale einfach kopieren bzw. imitieren kann. Dies ist dann der Fall, wenn es sich nicht um durch spezielle kryptographische Verfahren geschützte Schlüssel oder digitale Zertifikate wie z.B. Hardwaretoken oder eingebettete hardwarebasierte Sicherheitsmodule handelt (Wiedermann 2015). Hardwarebasierte Ansätze dieser Art bieten eine hohe Sicherheit, sind allerdings komplex zu handhaben, vergleichsweise teuer, benötigen zusätzlichen Platz im eingebetteten System und sind an einen spezifischen kryptographischen Algorithmus gebunden.

Der hier verfolge Ansatz möchte daher die statischen Selbstbeschreibungsmerkale nur als Ausgangspunkt nutzen, um zusätzlich die dynamischen Merkmale eines CPPS heranzuziehen, die in Kombination miteinander eindeutiger einer Entität zugewiesen werden können und nur mit unverhältnismäßigem Mehraufwand zu umgehen sind.

4.4.3 Eindeutige und sichere CPS-Identitäten – Konzept eines hybriden Fingerabdrucks für CPPS

Die erste sekundäre Forschungsfrage (F1.1) der vorliegenden Arbeit befasst dich damit, ob sich das Prinzip biometrischer Verfahren, die eindeutige Muster in physischen Merkmalen einer Person wie beispielsweise einen Fingerabdruck nutzen, um eine eindeutige Identifikation dieser Person durchzuführen, auf Maschinen in Form von CPPS übertragen lässt. Maschinen besitzen per se keinen Fingerabdruck in diesem Sinne, jedoch soll hier der Frage nachgegangen werden, ob und wie sich ein "künstlicher Fingerabdruck" mit

Hilfe von Selbstbeschreibungsmerkmalen konstruieren lässt. Die Abschnitte 4.2.1 und 4.2.2 befassen sich hierzu mit den Verfahren und Technologien, die bereits eingesetzt werden, um eine Identifikation eines Objekts oder einer Person durchzuführen. Die Veröffentlichung „Cyber-Physical Production System Fingerprinting“ (Stock et al. 2019a) geht dieser Frage im Ansatz nach und untersucht die verschiedenen Variationen und Ansätze des Fingerprintings, zu denen Abbildung 4.5 einen Überblick gibt.

Die Betrachtung der verschiedenen untersuchten Verfahren zeigt, dass diese grundsätzlich einen Fokus auf ein bestimmtes Merkmal aufweisen. Zudem wird meist eine spezifische Methode genutzt dieses Merkmal zu prüfen oder im Fall dynamischer Merkmale charakteristische Muster zu erkennen. Eine ganzheitliche Betrachtung eines CPPS und seiner Merkmale und ihrer Prüfung findet bisher nicht statt. So lassen sich die Self-X Fähigkeiten der Komponenten eines CPS, die wenn sie in einem smarten Produktionssystem eingesetzt werden, ein CPPS bilden, dazu nutzen mittels verschiedener Fingerprinting Verfahren Informationen zu sammeln und zu strukturiert zu speichern. Dieses Schema ist in Abbildung 4.20 dargestellt und kapselt die Grundlage für den in dieser Arbeit diskutierten Ansatz.

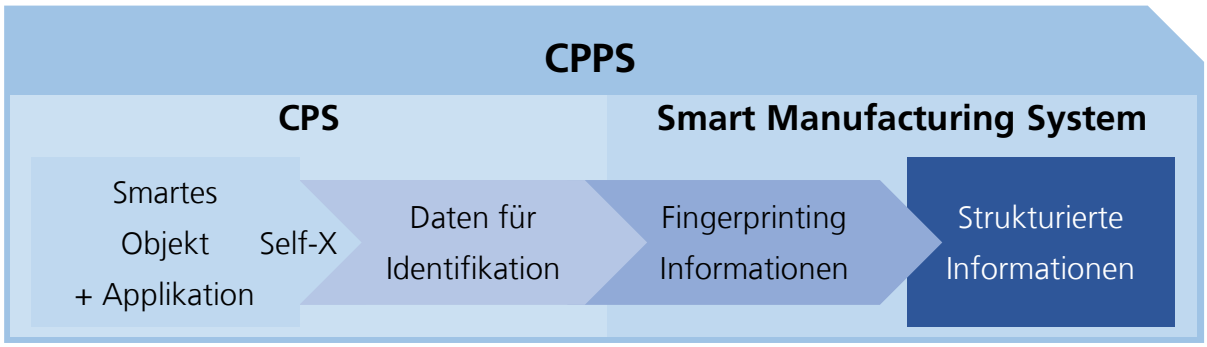


Abbildung 4.20 Prinzip des CPPS Fingerprintings nach (Stock et al. 2019a)

Diese strukturierten Informationen bilden einen digitalen Fingerabdruck. Allerdings bestehen diese Informationen aus verschiedenen Datensätzen aus statischen und dynamischen Daten bzw. Merkmalen, wie sie in Abschnitt 4.3.2 umfassend diskutiert werden. Dies

führt daher zur zweiten sekundären Forschungsfrage (F1.2), die sich damit befasst, welche Selbstbeschreibungsmerkmale sich für die Konstruktion eines "künstlichen Fingerabdrucks" und somit einer sicheren Identität eignen. Dieser künstliche digitale Fingerabdruck kann sich aus genau diesen Merkmalsklassen zusammensetzen, die in Abschnitt 4.3.2 formell vorgestellt und Anhand der Fallstudien in Abschnitt 6.1 dargelegt werden.

Daher schlägt die vorliegende Ausarbeitung, aufbauend auf dem Ansatz der Veröffentlichung „Cyber-Physical Production System Fingerprinting" das Konzept eines hybriden Fingerabdrucks für CPPS vor. Der hybride Fingerabdruck besteht aus statischen und dynamischen Informationen, die sich aus den statischen und dynamischen Merkmalen einer Entität bzw. eines CPPS zusammensetzen.

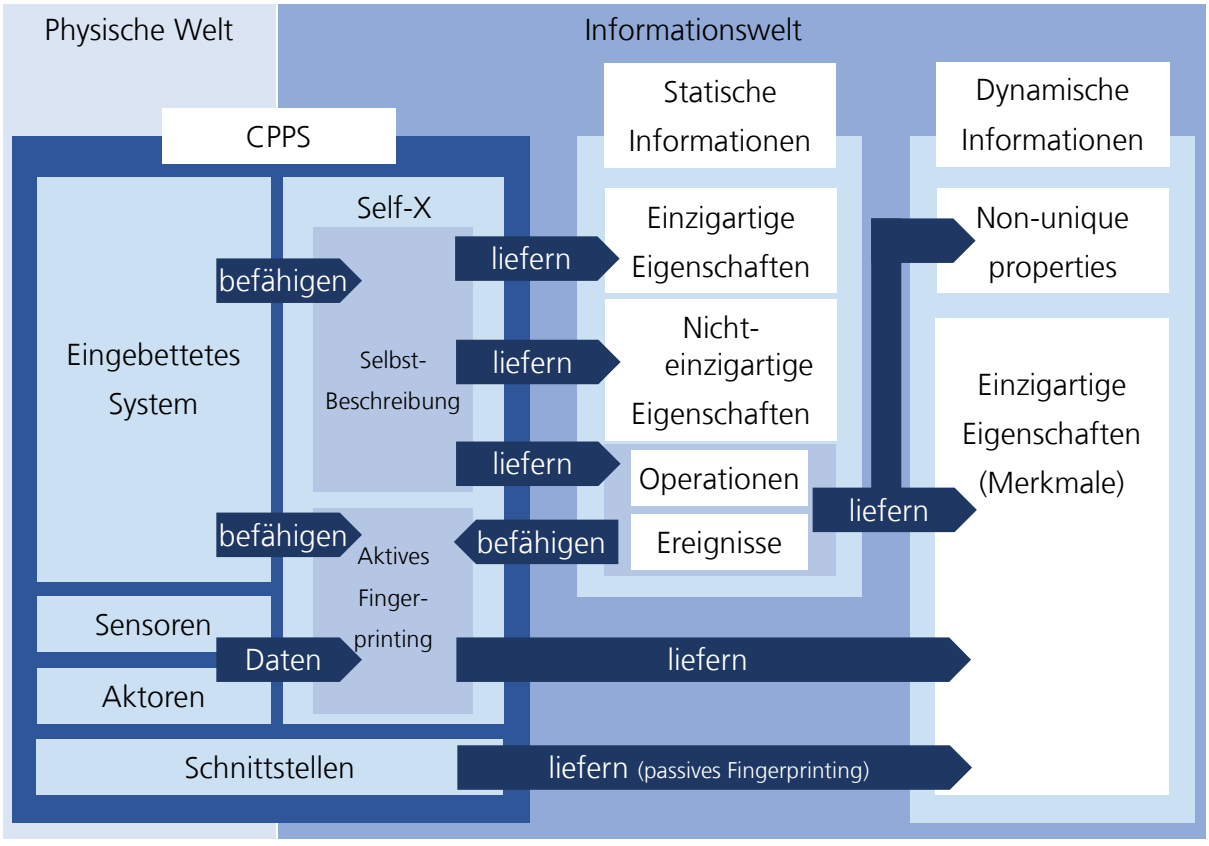


Abbildung 4.21 Fingerprint-Informationsbeziehungen für die Merkmalsextraktion nach (Stock et al. 2019a)

Abbildung 4.21 gibt hierzu einen Überblick der Beziehungen zwischen verschiedenen CPPS Komponenten und den Informationsbeziehungen, die zur Merkmalsextraktion eingesetzt werden können. Diese Darstellung stellt die in Abschnitt 4.3.1.2 diskutierten CPS-Datenquellen in Beziehung zueinander und wird durch die weiteren Datenquellen eines CPPS bzw. eines CPPS, das in einer CPPS-basierten Produktion eingebettet ist erweitert (vgl. Abschnitt 4.3.1). Hier wird bereits ein Teil der dritten sekundären Forschungsfrage (F1.3) angesprochen, die klären soll, ob ein Authentifizierungsverfahren auf Grundlage der Selbstbeschreibungsmerkmale unter Nutzung der Self-X-Eigenschaften eines CPS geschaffen werden kann, ohne dass die Anwendbarkeit und Funktionalität der Anwendung beeinträchtigt wird. Abbildung 4.21 stellt hierzu bereits dar, dass die meisten Informationen, die aus den Merkmalen eines CPPS extrahiert werden, durch die Self-X-Fähigkeiten eines CPPS gewonnen werden können. Die Extraktion der Daten zur Authentifizierung sollte daher keinen Einfluss auf die Anwendbarkeit und Funktionalität haben, insbesondere dann, wenn ohnehin entstehende oder vorhandene Daten zum Zweck des passiven Fingerprintings einfach nur abgegriffen werden. Aktives Fingerprinting muss als Self-X-Fähigkeit bereits im CPPS integriert sein und sollte so implementiert sein, dass es auch keinen Einfluss auf die Anwendbarkeit und Funktionalität des CPPS hat.

4.4.4 Identifikation mittels eines hybriden Fingerabdrucks

Abbildung 4.2 zeigt das Ablaufschema eines Identifikationsprozesses am Beispiel von RFID. Das RFID-Tag ist an einem Objekt angebracht und trägt einen Identifikator in sich, der eine Verbindung zwischen dem Objekt und der digitalen Identität des Objekts, in der dieser Identifikator hinterlegt ist, mittels eines Identifikationssystems herstellt. Ein Identifikator ist ein Merkmal, welches eine Entität eindeutig charakterisiert und zu ihrer Identifikation eingesetzt wird. Diese Eindeutigkeit gilt grundsätzlich für einen bestimmten Geltungsbereich, also beispielsweise innerhalb einer Fabrik als CPPS oder innerhalb eines Unternehmens. Um eine globale Eindeutigkeit herzustellen, die unabhängig vom Geltungs-

bereich ist, werden spezielle global eindeutige Identifikatoren eingesetzt. Diese Identifikatoren sind künstliche Merkmale, beispielswiese eine eindeutige UUID. Im Fall der Industrie 4.0 Verwaltungsschale wird eine IRDI (International Registration Data Identifier) nach ISO TS 29002 (Norm ISO TS 29002-10) oder URI (Uniform Resource Identifier) (Norm RFC 3986) bzw. IRI (Internationalized Resource Identifier) (Norm RFC 3987) eingesetzt (Barnstedt et al. 2020, S. 33). Diese Identifikatoren müssen zentral verwaltet werden, um einerseits ihre Validität und andererseits ihre Eindeutigkeit sicherzustellen.

Daher ist in Bezug auf die primäre Forschungsfrage ((F1) – Wie können die Selbstbeschreibungsmerkmale eines CPS genutzt werden, um eine sichere Identität zur Identifikation und Authentifizierung eines CPPS zu schaffen?) zu prüfen, ob neben Identifikatoren auch Merkmale bzw. die Kombination von mehreren Merkmalen in Form eines hybriden Fingerabdrucks als eindeutiger und gleichzeitig sicherer Identifikator bzw. als sichere Identität dienen kann.

Dieser Ansatz ist inspiriert von der Arbeit von Arvind Narayanan, einem Professor der Princeton University, dessen Schwerpunkt die Forschungen zur De-Anonymisierung von Daten ist. Eine seiner Thesen ist, dass es möglich ist unter 6,6 Milliarden Menschen einen Menschen mit einer Datenmenge von nur 33 Bits zu identifizieren, indem verschiedene persönliche Informationen einer Person kombiniert werden, um ein eindeutiges Identitätsprofil zu erstellen (Narayanan 2008).

Während es zum Schutz der Privatheit einer Person sinnvoll ist kritische Daten zu identifizieren, zu anonymisieren und zu schützen, kann im Fall eines CPPS dieser Ansatz umgedreht werden. Die meisten von einem CPPS erstellten Daten sind zwar schützenswert, betreffen jedoch keine personenbezogenen Daten. Daher besteht hier die Möglichkeit neben den statischen Daten eines CPPS, die einen oder mehrere Identifikatoren beinhalten können, auch die dynamischen Daten zur Merkmalsextraktion und zur Erstellung eines hybriden Fingerabdrucks zu nutzen. Die theoretischen Grundlagen zur Beschreibung und Differenzierung von Entitäten werden in Abschnitt 2.3 diskutiert und sollen im Folgenden zum Einsatz kommen. Abbildung 4.22 stellt den hier verfolgten Ansatz dar, die zu einem

CPPS zugehörigen Merkmale zur Erstellung einer digitalen Identität mittels eines hybriden Fingerabdrucks zu nutzen.

Identifikatoren sind künstliche, offene und schwache Merkmale. Das bedeutet, dass sie sehr gut zur Identifikation geeignet sind, was ihre implizite Aufgabe ist, jedoch ungeeignet zur Authentifizierung. Die Identifikation und insbesondere die darauffolgende Authentifizierung sollte daher nicht primär abhängig von solchen schwachen Identifikatoren sein, sondern aus der Summe der Selbstbeschreibungsmerkmale, die aus möglichst vielen starken Merkmalen besteht. Daher ist ein Identifikator, beispielsweise eine ID in Form einer alphanumerischen Zeichenkette, nur ein weiteres Merkmal unter vielen, welches zwar eine Entität mit ihrer digitalen Identität eindeutig verknüpft, allerdings darüber hinaus keine weiteren Informationen über die Entität beinhaltet. Eine Ausnahme kann beispielsweise eine URI sein, die sich aus mehreren eindeutigen und uneindeutigen Identifikatoren zusammensetzt. Aus Sicherheitsgründen empfiehlt es sich die statischen Merkmale des hybriden Fingerabdrucks, die zur Identifikation eingesetzt werden sollen, als Referenzmuster in Anlehnung an die biometrische Identifikation in Form eines Templates separat zu speichern (vgl. Abschnitt 3.1.7).

Der in Abbildung 4.22 skizzierte Identifikationsprozess führt einen Abgleich zwischen den Markmalen einer CPPS-Entität und den Merkmalen ihrer digitalen Identität durch. Der Ansatz soll jedoch nicht über einen eindeutigen Identifier die digitale Identität ermitteln, sondern durch bestimmte Schlüsselmerkmale, die bestimmten CPPS-Klassen und -Typen zugewiesen werden können. Dies ermöglicht es einerseits eine Klassifizierung und Typisierung von Entitäten durchzuführen. Andererseits kann so ein Clustering von Entitäten durchgeführt werden, das die Suchräume in denen ein Abgleich durchgeführt werden muss mittels Vektorraum-Retrieval verkleinert (Salton et al. 1975). Der spezifische Mechanismus der Identifikation mittels eines Merkmalsabgleichs wird nicht näher betrachtet, da hier bereits verschiedene Vorarbeiten existieren. Beispielsweise stellen (Pêgo et al. 2017) eine Methode vor IoT-Devices mittels der von diesen kommunizierten Daten zu klassifizieren und zu identifizieren, was im Ansatz teilweise dem hier diskutierten Vorgehen entspricht. Hierzu können demnach verschiedene Strategien, wie beispielsweise ein direkter

Abgleich von Merkmalen und Synonymen, die Levenshtein-Distanz mittels Levenshtein-Algorithmus zur Bestimmung der Ähnlichkeit von Zeichenketten und das Tf-idf-Maß (term frequency - „Vorkommenshäufigkeit“ und inverse document frequency - „inverse Dokumenthäufigkeit“) zur Gewichtung eines Wortes bezüglich eines Dokuments, eingesetzt werden. Ein komplexerer Ansatz zum wissensbasierten Entitäts-Matching, der semantische Technologien nutzt, wird in (Bortoli 2013) diskutiert und könnte zukünftig adaptiert werden.

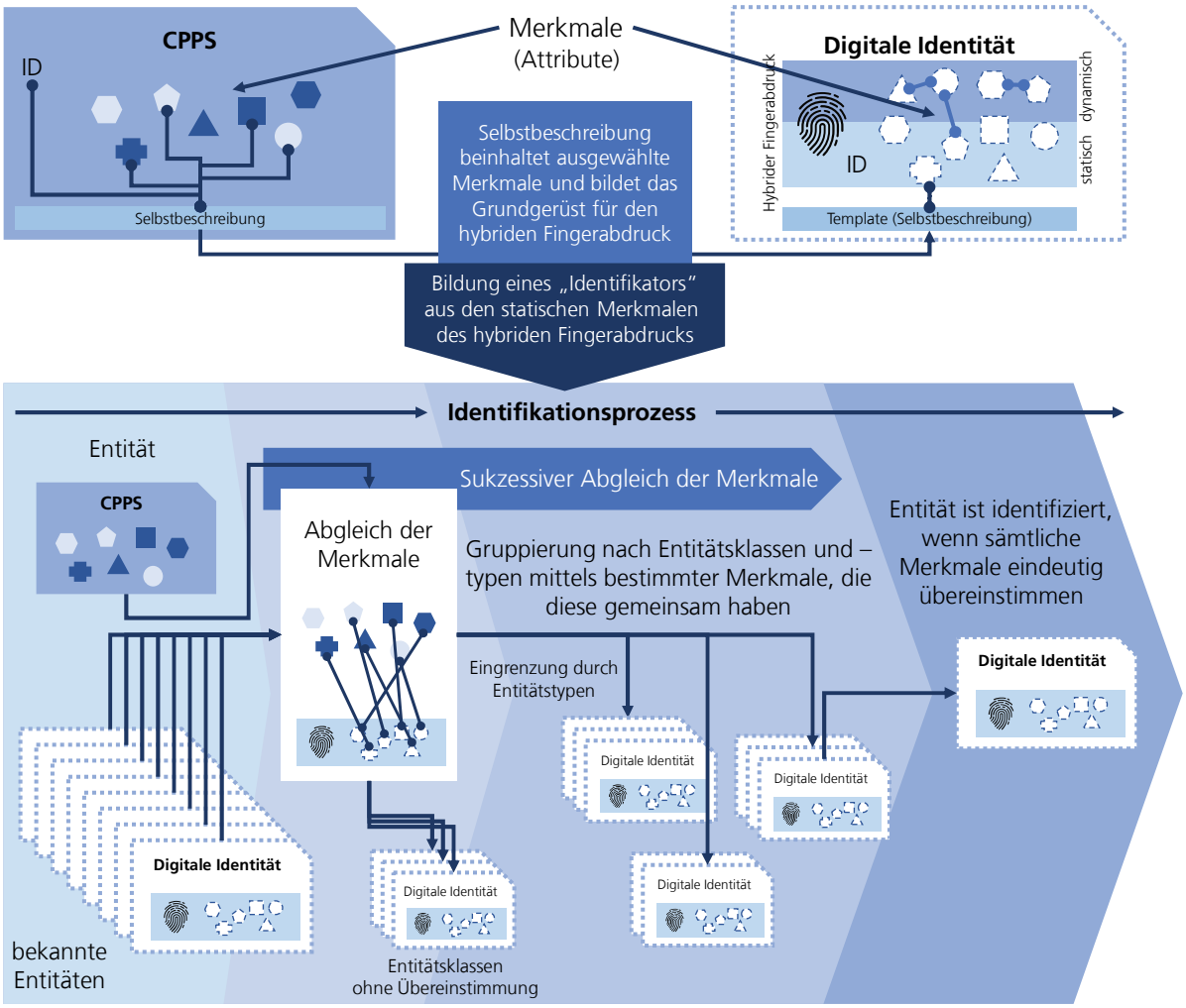


Abbildung 4.22 Identifikation mittels eines hybriden Fingerabdrucks

Eine Besonderheit, die hier zu beachten ist, ist die Schachtelung und der verteilte Charakter von CPPS-Komponenten. So können sich Merkmale eines CPPS sich auch außerhalb der „intuitiven“ physischen Kernkomponenten des CPPS befinden, sondern wie in Abschnitt 4.3.1.1 beschrieben auch als Betriebliche Daten in verschiedenen Produktions-IT Systemen vorhanden sein und zusätzlich herangezogen werden.

4.4.5 Zwischenfazit

Das Grundprinzip des digitalen Fingerabdrucks, das durch den natürlichen Fingerabdruck eines Menschen inspiriert ist, lässt sich wie in diesem Kapitel diskutiert als hybrider Fingerabdruck erweitern. Stammdaten in Form von Selbstbeschreibungsdaten sind wiederum statischer Natur. Die vorgestellten Fingerprinting-Verfahren basieren auf der Erfassung dynamischer Merkmale unterschiedlichster Ausprägung. Laufzeitdaten, Zustandsdaten, Bewegungsdaten und Prozessdaten sind ebenfalls stark dynamisch und kontextabhängig. Der in dieser Arbeit verfolgte Ansatz führt diese verschiedenartigen Daten und Verfahren zusammen. Die Merkmale bzw. die aus den Selbstbeschreibungsmerkmalen von CPPS und ihren Self-X-Fähigkeiten direkt ableitbaren Merkmale sollen hierzu in der Engineering-Phase identifiziert werden, um aus ihnen einen hybriden Fingerabdruck zu erstellen. Eine Forschungsfrage der vorliegenden Arbeit befasst sich mit dem hybriden Fingerabdruck. Hier soll festgestellt werden, ob es möglich ist mit dem hybriden Fingerabdruck eine digitale Identität abzubilden und mittels geeigneter Merkmalsprüfung diese digitale Identität als sichere Identität zu nutzen und diese für eine Authentifizierung zu nutzen.

5 Prototypische Implementierung des Authentifizierungsverfahrens

Dieses Kapitel befasst sich mit einer prototypischen Implementierung des im vorherigen Kapitel behandelten Konzepts in Form eines CPPS-Authentifizierungssystems. Die in den folgenden Abschnitten beschriebene Implementierung basiert auf der im Abschnitt 5.1.3 vorgestellten Referenzarchitektur.

5.1 Entwurf des Authentifizierungsverfahrens auf Grundlage von Selbstbeschreibungsmerkmalen

Ein Identitätsnachweis ist nach ISO/IEC 24760-1 die präsentierte und gesammelte Information bezüglich einer Entität, die für eine erfolgreiche Authentifizierung auf einer bestimmten (hohen) Sicherheitsstufe erforderlich ist (Norm ISO/IEC 24760-1). Die grundsätzliche Struktur des in den folgenden Abschnitten beschriebenen Frameworks und Verfahrens orientiert sich an den Grundsätzen der ISO/IEC 24760 und folgt somit anerkannten Normen für Identitätsmanagementsysteme.

5.1.1 Erstanmeldung von Entitäten

Die Erstanmeldung (engl. Enrollment) ist in Identitätsmanagementsystemen der Prozess der Erstellung einer digitalen Identität einer Entität. Hierzu wird ein Satz von Attributen gesammelt, die zur Identifikation eingesetzt werden, jedoch auch zu anderen Zwecken genutzt werden können. Diese Informationen müssen jedoch verifiziert werden. In zertifikatsbasierten Systemen beispielsweise ist eine RA (siehe Abschnitt 3.1.6) für die initiale Feststellung der Identität der anfragenden Entität zuständig.

Dieser Satz von Attributen ist für diese eine bestimmte Domäne bzw. den gewünschten Einsatzbereich gültig. Grundsätzlich werden während der Erstanmeldung Identitätsinformationen zur Speicherung in einem Identitätsregister gesammelt und erstellt, die bei der späteren Identifizierung der Einheit in der Domäne verwendet werden. Es ist der Beginn des Lebenszyklus einer Identität in der Domäne für eine Entität.

Der Identitätsnachweis bzw. die initiale Entitäts-Authentifizierung ist eine besondere Form der Authentifizierung auf der Grundlage von Identitätsnachweisen, die als Voraussetzung für die Erstanmeldung durchgeführt wird.

Typischerweise beinhaltet der Identitätsnachweis eine umfassende Überprüfung der bereitgestellten Identitätsinformationen und kann eine Kontrolle, Untersuchung und Eindeutigkeitsprüfung umfassen, möglicherweise nach dem Vorbild biometrischer Verfahren. Die Authentifizierung, das Kernelement des Identitätsnachweises, basiert in der Regel auf einer Anmelderichtlinie, die eine Spezifizierung der Verifizierungskriterien der von der Entität vorgelegten Identitätsnachweise beinhaltet.

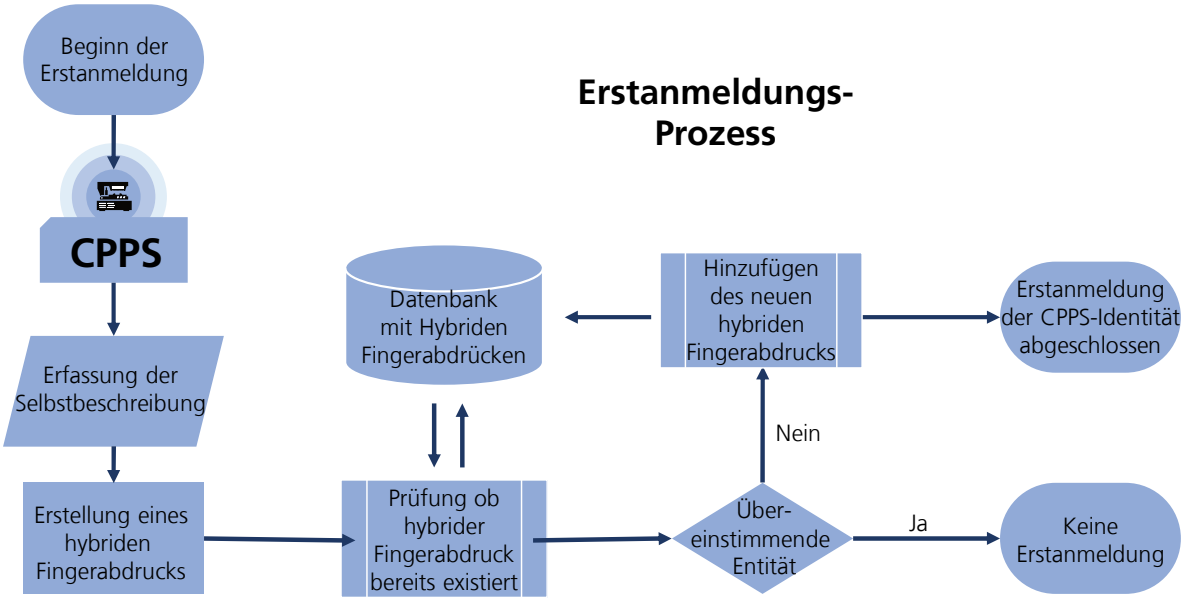


Abbildung 5.1 Erstanmeldungs-Prozess

Die Erstanmeldung, wie in Abbildung 5.1 dargestellt, kann zur Schaffung einer oder mehrerer Identitäten für die eingeschriebene Entität führen. Insbesondere kann ein Referenz-Identifikator erstellt werden. Erstellte Identitätsinformationen werden als Identität der angemeldeten Entität in einer Domäne registriert. Identitätsinformationen, die aus dem Identitätsnachweis ausgewählt werden, können zum Zeitpunkt der Anmeldung ebenfalls mit dieser Identität registriert werden. Der Wert der eindeutigen Attribute in einer erstellten Identität kann von der Entität gewählt oder vom Identitätsmanagementsystem zugewiesen werden, z.B. auf der Grundlage des Referenz-Identifikators, der bei der Registrierung der Identität für die angemeldete Entität erstellt wird. Die Registrierung kann die Erfassung passender Daten als Identitätsinformationen für die registrierte Entität beinhalten.

Zur Erstellung der digitalen Identität müssen die Selbstbeschreibungsmerkmale auf die Attribute eines entsprechenden Informationsmodells gemappt werden. Möchte man allerdings eine sichere digitale Identität schaffen, so müssen neben einfachen Merkmalen auch komplexe Merkmale gewählt oder konstruiert werden. Falls die Selbstbeschreibung bereits über eine formale Beschreibung dieser Merkmale verfügt, können auch diese einfach in Attribute überführt werden. Allerdings müssen bestimmte komplexe Merkmale modelliert werden, da diese zusätzliches Domänenwissen voraussetzen, welches ggf. nur implizit vorhanden ist.

Der Erstanmeldungs-Prozess muss daher von einer autorisierten Entität durchgeführt bzw. überwacht werden. Eine autorisierte Entität ist in diesem Fall eine Person, die die entsprechenden Rechte besitzt, um die Erstanmeldung einer Entität zu verifizieren. Prinzipiell ist auch ein automatisierter Prozess möglich, der von einem Erstanmeldungs-Dienst ohne menschliche Überwachung durchgeführt wird, vorstellbar sind auch mehrstufige Verfahren. So kann eine initiale Erstellung einer digitalen Identität aus einer Selbstbeschreibung stattfinden, die darauffolgend durch einen menschlichen Bediener verifiziert und freigegeben wird, so dass die digitale Identität nach der Einrichtung in einen suspendierten Zustand wechselt.

5.1.2 Skizzierung der Authentifizierungsphasen

Der grundlegende Ansatz mehrere verschiedenartige Merkmale in einem hybriden Fingerabdruck zu kombinieren ist angelehnt an eine Authentifizierung mit mehreren Authentifizierungsfaktoren (vgl. Multifaktor-Authentifizierung, Abschnitt 3.1.7). Da unterschiedliche Merkmale verschiedenartig beschaffen sind (vgl. Abschnitt 4.3.2), müssen auch spezifische Prüfstrategien für diese angewandt werden, allerdings muss hier gleichzeitig sichergestellt werden, dass ein Merkmal auch als Authentifizierungsfaktor geeignet ist (vgl. Abschnitt 4.3.4).

Eine Authentifizierung auf Basis von Selbstbeschreibungsmerkmalen setzt sich daher aus mehreren Phasen zusammen, die sequenziell durchlaufen werden und aus mehreren Authentifizierungsschritten bestehen. Jeder Authentifizierungsschritt erhöht das Vertrauenslevel, bis ein ausreichend hoher Wert erreicht wird. Hier muss ein Gleichgewicht zwischen den Fähigkeiten des CPPS ein Merkmal bereitzustellen und der Möglichkeit des Authentifizierungssystems dieses zu prüfen gefunden werden. Im Folgenden sind die jeweiligen Phasen knapp skizziert, um einen Überblick zu verschaffen. Weitere Details zu den jeweiligen Phasen werden in den später folgenden Abschnitten 5.1.5, 5.1.6 und 5.1.7 behandelt:

- **Identifikationsphase:** Die Identifikationsphase dient primär der Identifikation des CPPS und somit der Zuordnung zu seiner digitalen Identität und seinem hybriden Fingerabdruck. Hierzu wird ein Abgleich mittels der in der Selbstbeschreibung hinterlegten statischen Merkmale und der digitalen Identität bzw. dem zugehörigen hybriden Fingerabdruck durchgeführt.
    - Die Erstanmeldung ist ein optionaler Zweig der Identifikationsphase, falls das CPPS noch keine digitale Identität besitzt.
- **Initiale Authentifizierungsphase:** Die initiale Authentifizierungsphase dient der Abfrage von Merkmalen, die explizit als Authentifizierungsfaktoren dienen. Dies können beispielsweise starke Merkmale wie hardwaregestützte kryptographische Schlüssel, Zertifikate und zustands- oder wissensbezogene Merkmale des eingebetteten Systems des CPPS sein.

- **Aktive Authentifizierungsphase:** In der aktiven Authentifizierungsphase werden dynamische Merkmale eines CPPS überprüft. Dies sind beispielsweise natürliche Merkmale, die durch aktive Fingerprinting-Verfahren gewonnen werden. Bei der aktiven Prüfung eines Merkmals ist zu beachten, dass diese erstens während des Prüfprozesses Rechenressourcen des CPPS nutzt und zweitens dieser Prüfprozesses abhängig von der Art der Durchführung auch einige Zeit benötigt. Die Prüfung eines Merkmals kann Bruchteile von Sekunden bis zu Minuten dauern.
- **Kontinuierliche Authentifizierungsphase:** Falls ein ausreichend hohes Vertrauenslevel in der aktiven Authentifizierungsphase erreicht wurde, kann das CPPS in einen regulären Betriebszustand wechseln. Die kontinuierliche Authentifizierung ist während der gesamten Betriebsphase des CPPS aktiv. Während dieser Phase werden bevorzugt kontinuierlich passive Fingerprinting-Verfahren durchgeführt, die keinen direkten Einfluss auf das CPPS nehmen, sondern sein Verhalten überwachen.

Abbildung 5.2 stellt den gesamtheitlichen Authentifizierungsprozess und die für die jeweiligen Phasen typischen Merkmalstypen in Bezug auf ihre Eigenschaften dar.

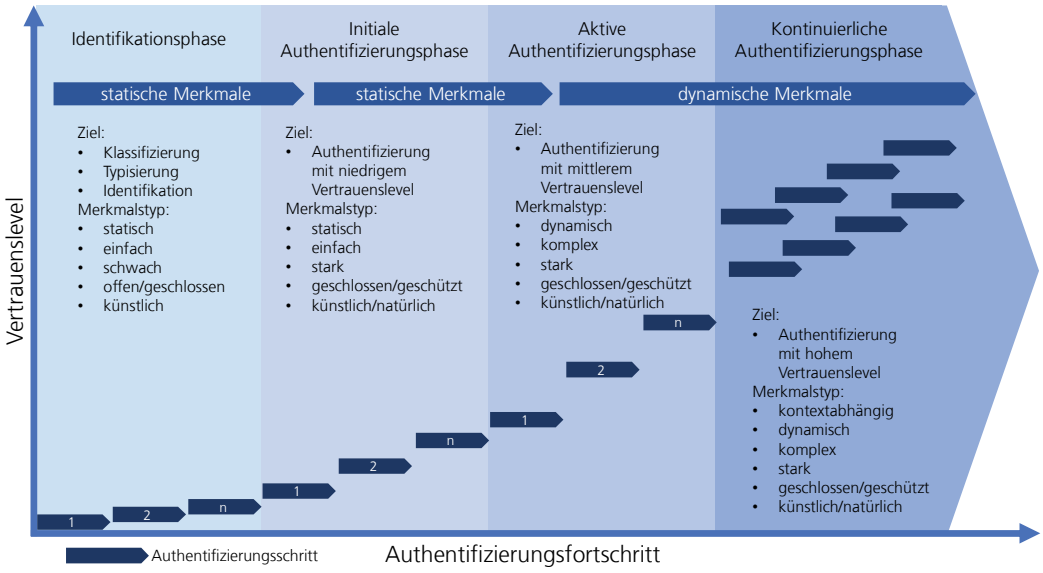


Abbildung 5.2 Phasen der merkmalsbasierten Authentifizierung

Einfache Merkmale lassen sich mit einfachen Methoden prüfen. Mittels der Self-X-Fähigkeiten eines CPPS lassen sich viele der Prüfschritte automatisieren. Während der kontinuierlichen Authentifizierungsphase werden zunehmend neue Daten und Informationen über das Verhalten des CPPS gewonnen. Daher kann hier der hybride Fingerabdruck oder ein spezifisches dynamisches Merkmal in diesem mittels dieser zusätzlichen Daten gestärkt und weiterentwickelt werden.

5.1.3 Referenzarchitektur eines Authentifizierungssystems auf Basis von Selbstbeschreibungsmerkmalen

Die Selbstbeschreibungsmerkmale eines CPPS und die Verfahren diese als Authentifizierungsfaktoren zu nutzen und zu prüfen können eine hohe Varianz und Komplexität aufweisen. Daher muss ein Authentifizierungssystem, das Selbstbeschreibungsmerkmale nutzt, einige grundsätzliche Anforderungen erfüllen, die die sich aus den Best Practices des Software-Engineerings ableiten, die den Vorgaben des in ISO/IEC 9126 definierten Modells zur Sicherstellung von Softwarequalität entsprechen:

- **Erweiterbarkeit** – das Gesamtsystem und die einzelnen funktionalen Blöcke des Authentifizierungssystems müssen durch neue Unterkomponenten erweiterbar sein, um ihre Funktionalität bei Bedarf zu erweitern.
- **Flexibilität** – das System muss die Möglichkeit bieten die Funktionalität bedarfsgerecht zu nutzen, was insbesondere aufgrund der Verschiedenartigkeit von CPPS eine Voraussetzung für die effiziente Anwendung der Lösung ist.
- **Skalierbarkeit** – das System muss so ausgelegt und implementiert werden können, dass einerseits eine Skalierung des Systems als Ganzes, aber auch der Funktionalität, z.B. die Anzahl der zu prüfenden Merkmale, möglich ist.
- **Redundanz** – das System muss in der Lage seine Komponenten redundant abzubilden und so eine hohe Ausfallsicherheit zu garantieren, da insbesondere die kontinuierliche Authentifizierung auf eine stetige Funktion angewiesen sind.

- **Wartbarkeit** – einzelne Komponenten müssen einfach und schnell austauschbar, erweiterbar und anpassbar sein, ohne die Systemstabilität zu gefährden.
- **Portabilität** – das System muss offen und Technologie-ungebunden implementierbar sein, um eine Integrierbarkeit in beliebige übergeordnete Systeme zu ermöglichen, die gängige offene Technologie-Standards bieten.

Diese Anforderungen können sehr gut von einer Service-orientierten Architektur (SOA) erfüllt werden. Alternativ kann auch eine rein Microservice-Architektur gewählt werden, die dieselben Vorteile bietet. Allerdings nutzt der hier verfolge Ansatz eine zentrale Integrationskomponente als Infrastruktur-Dienst, während eine Microservice-Architektur eigenständige feingranularere Dienste abbildet. Jede zusätzliche Komponente kann jedoch als ein oder mehrere Microservices technologieunabhängig implementiert werden. Insbesondere die Dienste, die zur Prüfung von Merkmalen eingesetzt werden, können auf diese Weise modular ausgelegt werden und frei erweiterbar oder austauschbar sein. So lässt sich das Authentifizierungssystem über offene Schnittstellen in bestehende Plattformen oder Systeme integrieren.

Dies setzt allerdings voraus, dass diese auch offene Schnittstellen und Datenformate mit möglichst einheitlichen Informationsmodellen in Form von modernen Interoperabilitätsstandards aufweisen, wie z.B. die Industrie 4.0 Verwaltungsschale. Die Bestandteile der Referenzarchitektur setzen sich aus den in Abbildung 5.3 dargestellten Komponenten zusammen.

Es wird vorausgesetzt, dass sämtliche Produktions-IT-Systeme, die für die Authentifizierung relevante betriebliche Daten enthalten, entsprechende Schnittstellen bereitstellen, über die die benötigten Daten abgefragt werden können. In einer CPPS-basierten Produktion ist zu erwarten, dass diese Systeme ihre Funktionalität in einer SOA als Microservices bereitstellen und diese Daten auch entsprechend auffindbar sind. Dies ist in einer zukünftigen Produktion als der Status quo zur Befähigung vernetzter digitale Ökosysteme notwendig (DIN/DKE 2020, S. 12).

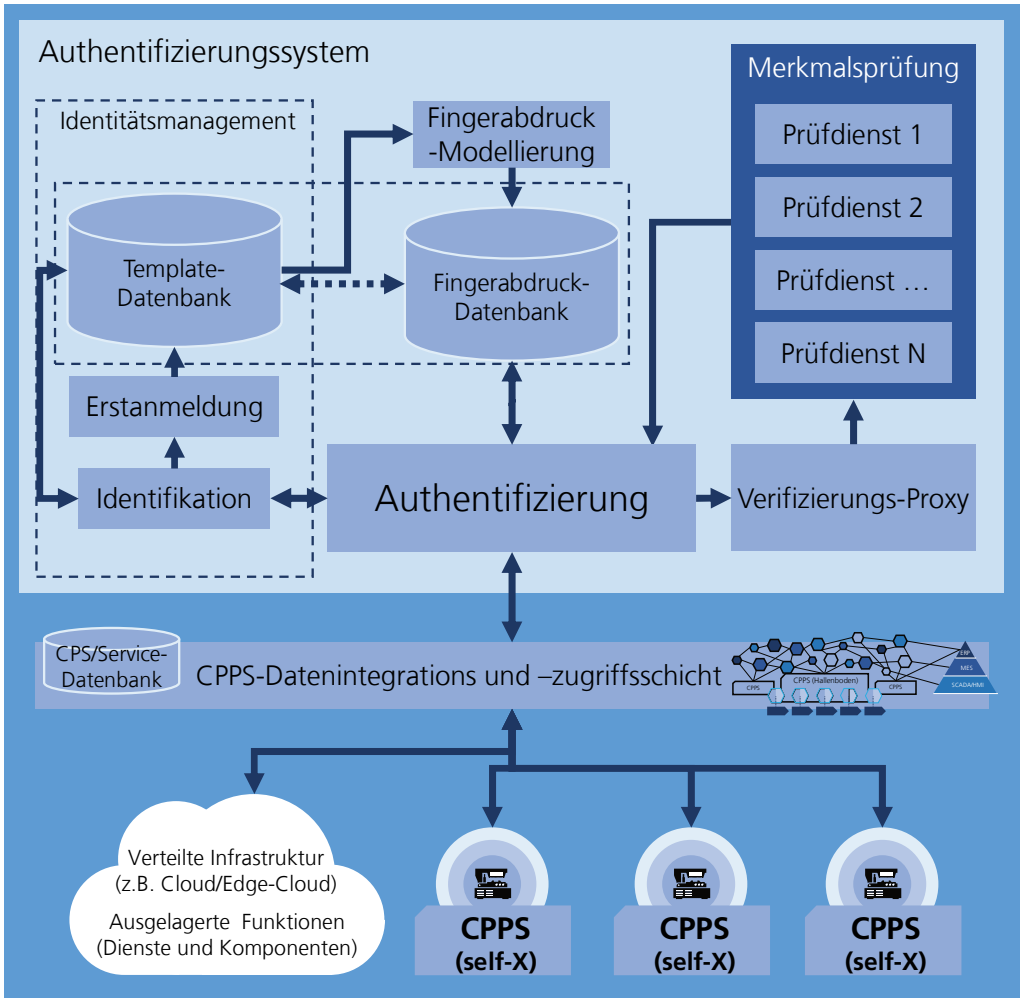


Abbildung 5.3 Referenzarchitektur eines Authentifizierungssystems auf Basis von Selbstbeschreibungsmerkmalen

In einem aktuellen Szenario mit Legacy-Systemen ist eine Anbindung über entsprechende Schnittstellen, wie Integrations-Dienste oder Adapter und Middleware-Lösungen möglich, die eine Integration ermöglichen. Ein Konzept, das eine einfache Middleware-Lösung um Selbstbeschreibungsfähigkeiten und dynamische Datenzugriffe erweitert, ist der in Abschnitt 3.2.5 vorgestellte Cyber-Physical Data Access Layer (CPDAL) (Stock et al. 2019b).

Im einzelnen Stellen die Kernelemente des Authentifizierungssystem folgende Bausteine dar:

- Die **Authentifizierung** ist die zentrale Komponente des Authentifizierungssystems. Initiale Anfragen von einem CPPS zur Authentifizierung kommen hier an und werden verarbeitet. Der Workflow des gesamten Authentifizierungsprozesses wird ausgeführt und die spezifischen Prozessschritte werden von hier an weitere Komponenten delegiert. Basierend auf den Ergebnissen der Merkmalsprüfung der Merkmale des CPPS wird das Vertrauenslevel für dieses CPPS von der Authentifizierung festgelegt und kann an einen festgelegten Grenzwert gekoppelt werden, ab welchem das CPPS nicht mehr als vertrauenswürdig gilt. Alternativ kann angelehnt an die risikobasierte Authentifizierung in Verbindung mit einem Zugriffsrechtemanagement dynamisch der Zugriff und die Interaktion auf bestimmte Ressourcen reguliert werden.
- Die **Identifikation** hat die Aufgabe auf Grundlage der statischen Merkmale der Selbstbeschreibung die behauptete Identität des CPPS zu verifizieren. Hierzu werden diese mit dem hinterlegten Referenzmusters (Template) aus statischen Merkmalen des hybriden Fingerabdrucks abgeglichen. Dynamische Merkmale lassen sich prinzipiell auch für eine Identifikation nutzen, allerdings ist hier der Aufwand eines Merkmalsabgleichs höher. Eine Authentifizierung findet erst statt, wenn auch die Authentizität der geschützten statischen bzw. dynamischen Merkmale durch die Merkmalsprüfung bestätigt wurde.
- Die **Erstanmeldung** ist dafür zuständig den Onboarding-Prozess eines noch unbekannten CPPS durchzuführen und dessen digitale Identität zu festzulegen. Hierzu wird in einem ersten Schritt ein Template erstellt, das aus den direkt aus der Selbstbeschreibung ableitbaren statischen Merkmalen besteht, die als Identifikatoren dienen. Zusätzlich werden hier die Erstellung und Verknüpfung des hybriden Fingerabdrucks mit dem Template in der Fingerabdruck-Modellierung angestoßen. Das Template bildet gemeinsam mit dem hybriden Fingerabdruck die digitale Identität des CPPS ab, welche wiederum mittels der Merkmalsprüfung zu einer sicheren Identität wird.
- Die **Template- und Fingerabdruck-Datenbank** speichert die Templates, die als Referenzmuster zur Identifikation dienen. Sie enthält die hybriden Fingerabdrücke,

die neben den statischen zusätzlich die dynamischen und abgeleiteten Merkmale enthält, beispielsweise zusätzliche Informationen zu Beziehungen von zwischen einzelnen Merkmalen. Die Datenbank kann entweder integriert für die Templates und Fingerabdrücke und als zentraler Speicher oder dezentral in Form einer verteilten Datenbank umgesetzt werden.

- Die **Fingerabdruck-Modellierung** besteht aus verschiedenen Diensten, die entweder automatisch einen hybriden Fingerabdruck generieren oder Anwendern Tools oder Apps hierfür bieten. Mit Hilfe dieser Anwendungen können Nutzer bei Bedarf aus den aus der Selbstbeschreibung direkt extrahierbaren Merkmalen weitere Merkmale ableiten, die zusätzliches Wissen voraussetzen, beispielsweise die Abhängigkeit bestimmter Werte von einem bestimmten Kontext. Für diese abgeleiteten Merkmale wird zusätzlich hinterlegt, welche Prüfdienst diese prüfen kann. Auch diese manuelle Erweiterung und Schaffung komplexerer Merkmale lässt sich automatisieren, jedoch liegt dieser Matching-Prozess außerhalb des Rahmens dieser Arbeit.
- Der **Verifizierungs-Proxy** verfügt über eine Liste der verfügbaren Prüfdienste. Soll ein Merkmal geprüft werden, wird die Anfrage erst an den Verifizierungs-Proxy geleitet, welcher mittels der im hybriden Fingerabdruck hinterlegen Information zum passenden Prüfdienst einen adäquaten Prüfdienst in einer Liste registrierter Dienste sucht. Wird kein Prüfdienst aufgefunden, kann das Merkmal nicht geprüft werden und die Prüfung gilt als fehlgeschlagen. In diesem Fall muss ggf. die Fingerabdruck-Modellierung angepasst werden oder eine manuelle Freigabe für dieses Merkmal eingerichtet werden.
- Die Merkmalsprüfung ist die Summe der Prüfdienste, die zur Prüfung von Merkmalen eingesetzt werden können. Das System sollte eine Grundauswahl von Standard-Prüfdiensten besitzen, mit welchen gängige Merkmalsarten geprüft werden, beispielsweise durch einen trivialen Wertevergleich oder einen Ähnlichkeitsvergleich von Messreihen. Abgeleitete und komplexe Merkmale benötigen meist spezielle Prüfverfahren, beispielsweise Mustererkennungen und -abgleiche, die auch

auf maschinellen Lernverfahren basieren können. In diesem funktionalen Block findet sich das Erweiterungspotenzial und die Möglichkeit der funktionalen Skalierung. Das Authentifizierungssystem kann weiter ausgebaut und um neue Dienste erweitert werden, die es ermöglichen Merkmale zu prüfen, die zwar schon erkannt wurden, aber aufgrund des Fehlens eines passenden Prüfdienstes, noch nicht zu Authentifizierung eingesetzt werden konnten.

5.1.4 Authentifizierungsprotokoll

Die Authentifizierung auf Basis von Selbstbeschreibungsmerkmalen ist durch die folgenden Phasen und ihre spezifischen Schritte definiert.

I-a Identifikation (die Entität bzw. das CPPS ist bereits bekannt):

1. Das CPPS sendet seine Selbstbeschreibung an das Authentifizierungssystem
2. Der zuständige Dienst im Authentifizierungssystem extrahiert die Merkmale, die als Authentifizierungsmerkmale gekennzeichnet sind.
3. Die statischen und einfachen Merkmale, die unmittelbar als Identifikatoren geeignet sein, werden an den Identifikationsdienst gesendet.
4. Der Identifikationsdienst sendet basierend auf den Merkmalen eine Abfrage an die Template-Datenbank.

Wie bei einem Identifikationssystem üblich (vgl. Abschnitt 4.2.1), können folgende Fälle auftreten:

5. a: Die Abfrage liefert ein übereinstimmendes Template zurück.
6. a: Das CPPS wurde identifiziert und die behauptete die Identität wurde somit verifiziert (jedoch noch nicht authentifiziert).
5. b: Die Abfrage liefert mehr als ein übereinstimmendes Template zurück.
6. b: Das CPPS könnte nicht eindeutig identifiziert werden, die Verifikation der behaupteten Identität ist fehlgeschlagen.
5. c: Die Abfrage liefert kein übereinstimmendes Template zurück.

6. c: Das CPPS könnte nicht identifiziert werden, die Verifikation der behaupteten Identität ist fehlgeschlagen.

I-b Erstanmeldung (die Entität bzw. das CPPS ist noch nicht bekannt):

Die Schritte 1-5a sind identisch zur Identifikationsphase

6. Die Abfrage liefert kein übereinstimmendes Template zurück.
7. Der zuständige Dienst im Authentifizierungssystem erstellt eine digitale Identität aus der Selbstbeschreibung und sendet diese an die Erstanmeldung.
8. Die digitale Identität wird als Template in der Template-Datenbank gespeichert.
9. Die Erstanmeldung startet den Prozess der Fingerabdruck-Modellierung.
10. Der hybride Fingerabdruck wird aus den extrahierten Merkmalen der Selbstbeschreibungsdaten des Templates modelliert.
11. Der hybride Fingerabdruck wird in der Fingerabdruck-Datenbank gesichert.
12. Die Erstanmeldung wird über die Erstellung des Fingerabdrucks benachrichtigt.
13. Die digitale Identität wird dem Authentifizierungssystem als erstellt zurückgemeldet.

Von diesem Punkt an können die Authentifizierungsphasen durchlaufen werden:

Phase I-a wurde erfolgreich abgeschlossen.

II. Authentifizierung

1. Der hybride Fingerabdruck des identifizierten CPPS wird aus der Fingerabdruck-Datenbank gelesen.
2. Das Vertrauenslevel für das CPPS wird zurückgesetzt.

Initiale Authentifizierung

1. Die statischen Merkmale, die direkt aus der Selbstbeschreibung entnommen werden können, werden mit den Merkmalen im hybriden Fingerabdruck als Referenz geprüft.
2. Für jedes Merkmal wird ein passender Prüfdienst identifiziert.

3. Jedes Merkmal wird geprüft.
4. Ist die Merkmalsprüfung positiv, wird das Vertrauenslevel erhöht, ansonsten zurückgesetzt.

Aktive Authentifizierung

1. Die statischen und dynamischen Merkmale, die aus der Selbstbeschreibung abgeleitet werden können, werden mit den Merkmalen im hybriden Fingerabdruck als Referenz geprüft.
2. Für jedes Merkmal wird ein passender Prüfdienst identifiziert.
3. Jedes Merkmal wird geprüft, entweder durch eine Abfrage von Produktions-IT Systemen des gesamtheitlichen CPPS oder durch direkte Abfrage des CPPS.
4. Ist die Merkmalsprüfung positiv, wird das Vertrauenslevel erhöht, ansonsten zurückgesetzt.

Kontinuierliche Authentifizierung

1. Die dynamischen Merkmale, die aus der Selbstbeschreibung abgeleitet werden können, werden kontinuierlich mit den Merkmalen im hybriden Fingerabdruck als Referenz geprüft.
2. Für jedes Merkmal wird ein passender Prüfdienst identifiziert.
3. Jedes dynamische Merkmal wird durch eine periodische oder ereignisgetriebene Abfrage von Produktions-IT Systemen des gesamtheitlichen CPPS geprüft, die kontinuierlich vom CPPS betriebliche Daten speichern.
4. Ist die Merkmalsprüfung positiv, wird das Vertrauenslevel erhöht, ansonsten zurückgesetzt.

Abbildung 5.4 stellt die beschriebenen Schritte ganzheitlich ein einem Sequenzdiagramm dar.

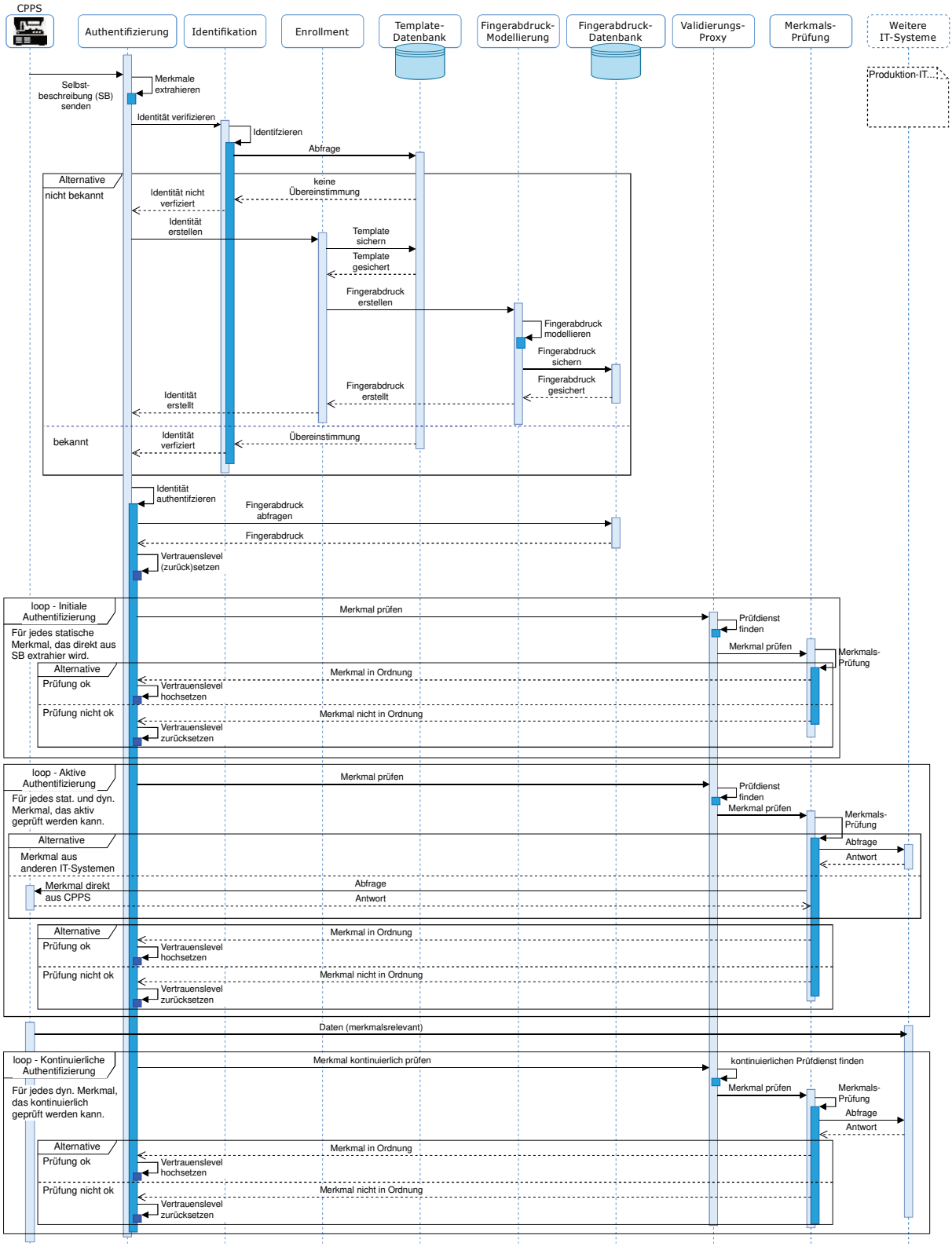


Abbildung 5.4 Sequenzdiagramm der Authentifizierungsschritte

5.1.5 Identifikation und initiale Authentifizierung

Die Identifikation und die initiale Authentifizierung sind sich im Hinblick auf die für sie verwendeten Merkmale sehr ähnlich und werden hier daher zusammengefasst behandelt. Das Prinzip der Identifikation mittels eines hybriden Fingerabdrucks wird bereits in Abschnitt 4.4.4 beschrieben. In der Umsetzung wird für die Identifikation eine Teilmenge der Merkmale des hybriden Fingerabdrucks verwendet, die in Anlehnung an die biometrische Authentifizierung als Template bezeichnet wird und ein Referenzmuster für einen Abgleich darstellt. Die Merkmale, die hierfür überwiegend verwendet werden, sind primär Seins-Merkmale und Besitz-Merkmale, die statisch, einfach, künstlich und offen sind und sich somit gut als Identifikatoren eignen, aus denen relativ schnell und einfach eine „öffentliche" Identität konstruiert werden kann. Merkmale dieser Art eigenen sich für einen schnellen und einfachen Abgleich.

Das hier vorgestellte Konzept will sich hier jedoch nicht von globalen Identifikatoren abhängig machen, die zentral verwaltet werden. Ein eindeutiger globaler Identifikator eignet sich sehr gut als zusätzliches Merkmal für die Identifikation, aber es soll die Frage geklärt werden, wie eine Identität aus Selbstbeschreibungsmerkmalen konstruiert werden kann, die zum Einsatz in beliebigen Systemen geeignet ist, selbst wenn diese nicht einen domänenspezifischen eindeutigen globalen Identifikator nutzen. Diese Identität soll intrinsisch entstehen und nicht von außen bestimmt werden. Nachdem ein passender Abgleich der behaupteten Identität durchgeführt wurde, muss diese initial authentifiziert werden. Hierfür wird der hybride Fingerabdruck herangezogen und die dort hinterlegten verschlüsselten Merkmale mit den in der Selbstbeschreibung übermittelten abgeglichen. Die initiale Authentifizierung setzt auf statische Merkmale, die geschlossen oder geschützt sind und als Authentifizierungsfaktoren fungieren und daher auch deren Eignungskriterien erfüllen müssen. Als geschützte Merkmale stellen sie überwiegend Wissensfaktoren dar, jedoch basieren sie grundsätzlich auf den aus Seins-, Besitz-, Wert-, Struktur- bzw. Beziehungs- und Fähigkeits-Merkmalen abgeleiteten Faktoren (Seins-, Struktur-, Besitz-, Wissens- und

Wertfaktor; vgl. Abbildung 4.14). Sie sind wie die für die Identifikation genutzten Merkmale einfach durch einen Abgleich unter Einsatz verschiedener Methoden zu prüfen, wie sie in Abschnitt 4.4.4 diskutiert werden.

5.1.6 Aktive Authentifizierung

Die aktive Authentifizierung setzt primär auf dynamische Merkmale, die aktiv vom CPPS abgefragt werden. Hierzu werden neben der Selbstbeschreibungsfähigkeit weitere Self-X-Fähigkeiten zur aktiven Authentifizierung des CPPS benötigt. Das Vorhandensein dieser Fähigkeiten wird in der Selbstbeschreibung selbst in Form von Merkmalen übermittelt, so dass die Merkmalsprüfung diese Abfragen kann. Das Prinzip dieser aktiven Merkmalsprüfungen orientiert sich am aktiven Fingerprinting (vgl. Abschnitt 4.2.2). Die Bandbreite der Authentifizierungsfaktoren bzw. Merkmalklassen, die hierfür eingesetzt werden, ist etwas größer, da hier hauptsächlich dynamische Merkmale abgefragt werden, jedoch auch statische Merkmale abgefragt werden können. Beispielsweise können bestimmte Informationen (Wissens-Merkmale oder Besitz-Merkmale) mittels eines Challenge-Response-Verfahrens wie einem Zero-Knowledge-Proof (Giani 2001) geprüft werden. Der Fokus liegt hier jedoch darauf, Seins-Merkmale dynamischer Natur abzufragen, beispielsweise bestimmte Leistungsdaten oder durch die Hardware-, Software- oder spezifische Konfiguration des CPPS-Verbunds bestimmte Merkmale aktiv zu prüfen. Hierzu werden vom CPPS Operationen offengelegt, die es erlauben die spezifischen Merkmale abzugleichen, die während der Erstanmeldung als Referenzwerte hinterlegt wurden.

Zusätzlich kommen hier neben den Informationen über das CPPS selbst auch die betrieblichen Daten zum Tragen, die von dem CPPS erzeugt wurden. Diese umfassen statische Merkmale in Form von Informationen über Aufträge aus der Betriebsphase des Lebenszyklus des CPPS, aber auch dynamische Merkmale in Form von Sensor-, Mess- und Prozessdaten mit Bezug zu diesen Aufträgen und den mit ihnen verknüpften Prozessen. Zudem können auch Kontext-Merkmale zum Einsatz kommen, wie z.B. die Abfrage der Präsenz anderer CPPS. Dies setzt voraus, dass das CPPS bereits im Einsatz war und nicht direkt

nach der Erstanmeldung geprüft wird. Um hier ein grundsätzliches Vertrauenslevel zu erreichen, kann wie in Abbildung 4.18 dargestellt eine Trainingsphase durchlaufen werden, in der bereits eine Grundmenge an Daten erzeugt wird, die als geschlossene bzw. geschützte Merkmale im CPPS als Referenzen gespeichert werden, um als Wissensfaktoren zu dienen. Diese Referenzen können periodisch erneuert werden, um eine Nachahmung bei Kompromittierung des CPPS zu erschweren. Merkmale mit Bezug zu echten Aufträgen bzw. Auftragsdaten können aus den jeweiligen Produktions-IT-Systemen abgefragt und mit den vom CPPS gespeicherten Informationen abgeglichen werden. Der hybride Fingerabdruck kann hierfür eine Referenz beinhalten, die zum Abgleich verwendet wird.

5.1.7 Kontinuierliche Authentifizierung

Die kontinuierliche Authentifizierung bedient sich vornehmlich der Methoden des passiven Fingerprintings. Der Hauptunterschied zur aktiven Authentifizierung ist hier, dass das CPPS selbst nicht tangiert wird, sondern das Authentifizierungssystem und seine Prüfdienste kontinuierlich während des Betriebs das Verhalten des CPPS beobachten und die während des Fingerprint-Modellings in der Erstanmeldungs-Phase festgelegten Merkmale prüfen. Zudem wird durch die Kontinuität die zeitliche Dimension berücksichtigt. Während die aktive Authentifizierung sich auf Momentaufnahmen und hauptsächlich das CPPS selbst bezieht, werden während der kontinuierlichen Authentifizierung längere Zeitabschnitte betrachtet. Die hier zur Anwendung kommenden Merkmale sind daher stark an kontextuellen Daten orientiert. Diese Merkmale umspannen einfache beobachtbare Verhaltensmuster, beispielsweise das protokollspezifische Verhalten der Kommunikation in einem Netzwerk, können aber auch komplexe Zusammenhänge und Interkationen mehrerer CPPS miteinander abbilden. Zudem können die entstehenden betrieblichen Daten, wie beispielswiese Prozessdaten, die eine bestimmte charakteristische Abhängigkeit aufweisen, mit zusätzlichen Kontextdaten wie Zeitstempeln, Ereignissen, Ortsangaben, Präsenzdaten in Relation gebracht werden.

5.2 Implementierungsarchitektur

Die große Anzahl und Verschiedenartigkeit der Merkmale und der Möglichkeit diese mittels verschiedener Verfahren wie in Abschnitt 4.2.2 diskutiert zu prüfen, führt zu einem Komplexitätsproblem. Der hier verfolgte Lösungsansatz basiert daher auf einer flexiblen Service-orientierten Architektur in Kombination mit Microservices (vgl. Anhang 2.3), die eine bedarfsgerechte funktionale Erweiterung erlauben. Abbildung 5.5 zeigt die aus der in Abschnitt 5.1.3 diskutierten Referenzarchitektur abgeleitete Implementierungsarchitektur.

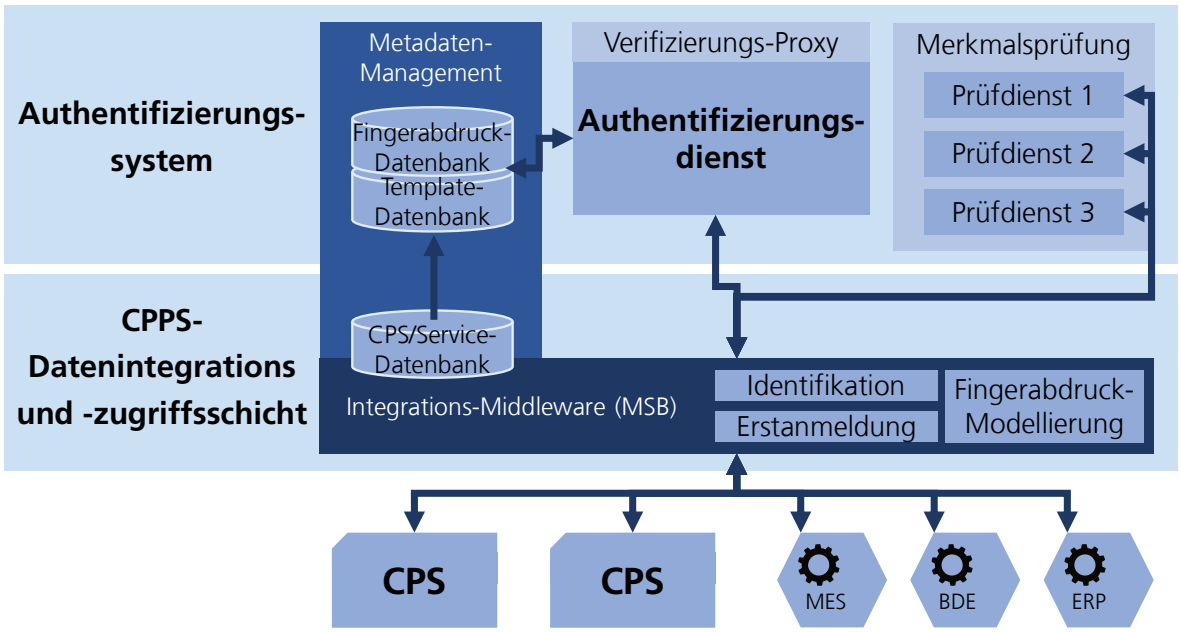


Abbildung 5.5 Implementierungsarchitektur des Authentifizierungssystems

Die Implementierungsarchitektur weist einige Anpassungen auf, da einige der Komponenten neu entwickelt und andere bereits bestehende Komponenten adaptiert und integriert wurden. Die Integration der Komponenten wird mittels einer für diesen Anwendungsfall modifizierten Instanz der Manufacturing Service Bus Middleware (MSB) realisiert (Schel et al. 2018). Abbildung 5.6 gibt eine Übersicht zur Architektur des MSB.

Der MSB wurde entwickelt, um eine einfache Integration smarter Objekte und Applikationen im Produktionsumfeld zu ermöglichen. Die auf der Shopfloor-Ebene befindlichen smarten Objekte bzw. Applikationen, die an einem beliebigen Ort bereitgestellt werden können, sind als Smart Services abstrahiert. Sie stellen ihre Fähigkeiten als Dienste in einer SOA bereit und können daher zum Zweck der Orchestrierung Fähigkeiten mittels des MSB als solche betrachtet werden. Ein ähnlicher Ansatz wird im Virtual Automation Bus des Projekts BaSys 4.0 bzw. der BaSyx 4.0 Middleware verfolgt (vgl. Abschnitt 3.2.2). Die mit dem MSB verbundenen Objekte und Dienste sind in der Lage über verschiedene Schnittstellen zu kommunizieren, die gängige industrielle und Webprotokolle unterstützen. Nachrichten werden in einer Nachrichtenwarteschlange in einem Broker gepuffert, da die Sende- und Empfangsfrequenzen zwischen den Kommunikationsteilnehmern abweichen können.

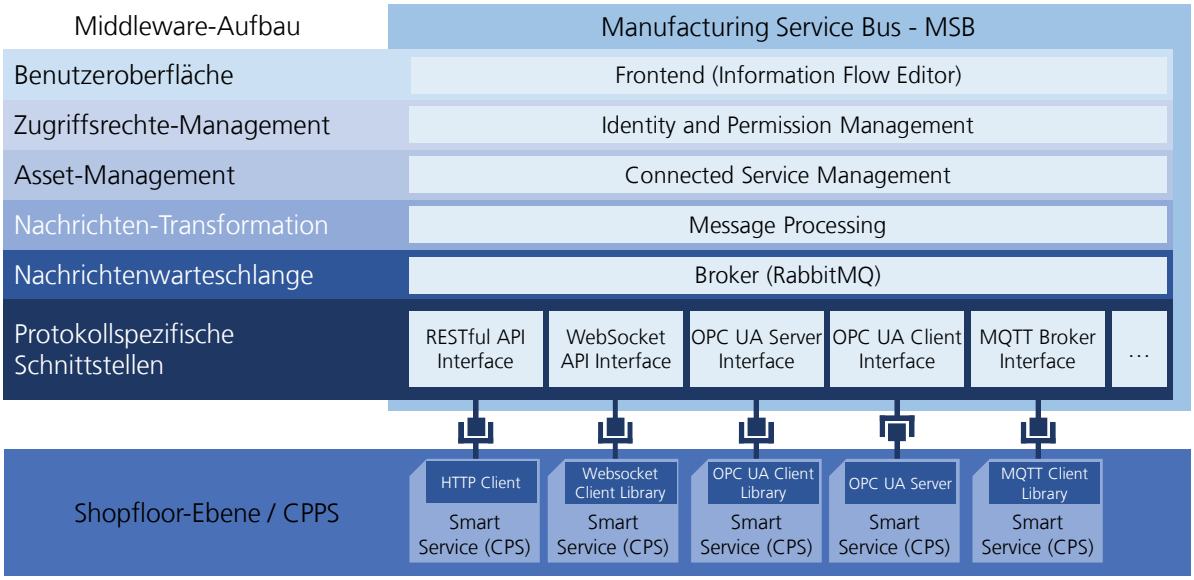


Abbildung 5.6 Manufacturing Service Bus Architektur

Zudem verfügt der MSB bereits über ein Asset-Management und eine Benutzerverwaltung. Benutzer sind damit in der Lage ihre smarten Objekte und Applikationen im Frontend grafisch miteinander verknüpfen. Die so modellierten Integration Flows mappen und

transformieren die ausgetauschten Datenobjekte gemäß der Selbstbeschreibung ihrer Datenformate.

Der MSB ist eine Eigenentwicklung, daher besteht voller Zugriff auf die Quellcode-Dateien, sodass sämtliche notwendigen Modifikationen durchgeführt werden können. Die mit dem MSB verbundenen Dienste stellen eine Selbstbeschreibung bereit, die mittels der als Open Source verfügbaren Client-Bibliotheken eine Implementierung verschiedener Kommunikationsprotokolle (http/REST, Websocket, MQTT, OPC UA) in den gängigsten Hochsprachen (C, C++, C#, Java, Python, Node.js/JavaScript) erlaubt.

Die mittels des MSB so miteinander verbundenen smarten Objekte bzw. CPS und Applikationen bzw. beliebige weitere Produktions-IT-Dienste bilden so ein CPPS, welches durch eine Integration mehrerer CP(P)S ein gesamtheitliches CPPS bilden können (Stock et al. 2020b). Der MSB bildet somit die CPPS-Datenintegrations- und Zugriffsschicht, die für das Konzept benötigt ist, um die für die Authentifizierung notwendigen Merkmale aus den CPS und Diensten in Form von betrieblichen Daten zu extrahieren.

Das Authentifizierungssystem setzt auf dieser Schicht auf und ist mit den MSB-Komponenten integriert. Da der MSB nach dem SOA-Prinzip modular aufgebaut ist, ist eine einfache funktionale Erweiterung der Schnittstellen und Kernkomponenten möglich und vorgesehen. So ist das Metadaten-Management eine Komponente, die eine solche Erweiterung darstellt und das einfache syntaktische Informationsmodell des MSB mit semantischen Technologien erweitert. Es dient so dazu neben der Template-Datenbank zur Identifikation auch die Fingerabdruck-Datenbank zu verwalten.

Die Authentifizierungskomponente, die das Authentifizierungsprotokoll ausführt, ist eine separate Komponente, als MSB-Applikation umgesetzt und über diesen integriert. Der Verifizierungs-Proxy wurde der Einfachheit wegen mit dieser Komponente kombiniert. Die notwendigen Prüfdienste der Merkmalsprüfung sind ebenfalls als Microservices mittels des MSB integriert. So ist es möglich die Integration Flow-Modellierung des MSB auch zur Fingerprint-Modellierung zu nutzen und so die Merkmale des hybriden Fingerabdrucks

mit den Prüfdiensten zu verbinden. Die CPS Komponenten sind zudem mit einer entsprechend angepassten Client-Bibliothek ausgestattet, die die Möglichkeit zur semantisch erweiterten Selbstbeschreibung bietet.

5.3 Informationsmodell für einen hybriden Fingerabdruck

Das Standard-Informationsmodell des MSB, der das Rückgrat der Implementierung bildet, ist bereits in Abbildung 4.17 eingeführt worden. Wie beschrieben bietet dieses einfache Informationsmodell nur eine Beschreibung der Datenfelder der jeweiligen Operationen und Events eines CPS.

Für eine Authentifizierung auf Basis von Selbstbeschreibungsmerkmalen musste dieses Informationsmodell daher erweitert werden. Abbildung 5.7 ist eine Darstellung dieses erweiterten Informationsmodells in Form eines UML-Modells, welches für den hybriden Fingerabdruck genutzt wird.

Die Erweiterung des Informationsmodells um Metadaten-Felder in Kombination mit dem Einsatz semantischer Technologien erlaubt es, Anwendungen zusätzliche Informationen zu übermitteln, um die Daten interpretieren zu können und mehr Informationen über das CPPS zu gewinnen. Dies sind beispielsweise der Einsatz von Fingerprinting für CPPS (Stock et al. 2019a), eine Typisierung von CPS zur automatisierten Integration mit Diensten zum Zweck eines dynamischen Datenzugriffs (Stock et al. 2019b) oder die strukturellen Modellierung von CPPS (Stock et al. 2020b).

Das Metadatenmanagement selbst nutzt das Metainformationsmodell der Industrie 4.0 Verwaltungsschale (vgl. Abschnitt 3.2.3). Der hybride Fingerabdruck stellt in diesem Kontext also ein Teilmodell der Verwaltungsschale dar und ist somit eine anwendungsspezifische Erweiterung des Konzepts (vgl. Abschnitt 3.2.4). Das Mapping-Konzept zur Abbildung des internen Fingerabdruck-Modells auf ein das Verwaltungsschalen-Teilmodell-Format hierzu ist in Anhang 5 dargestellt.

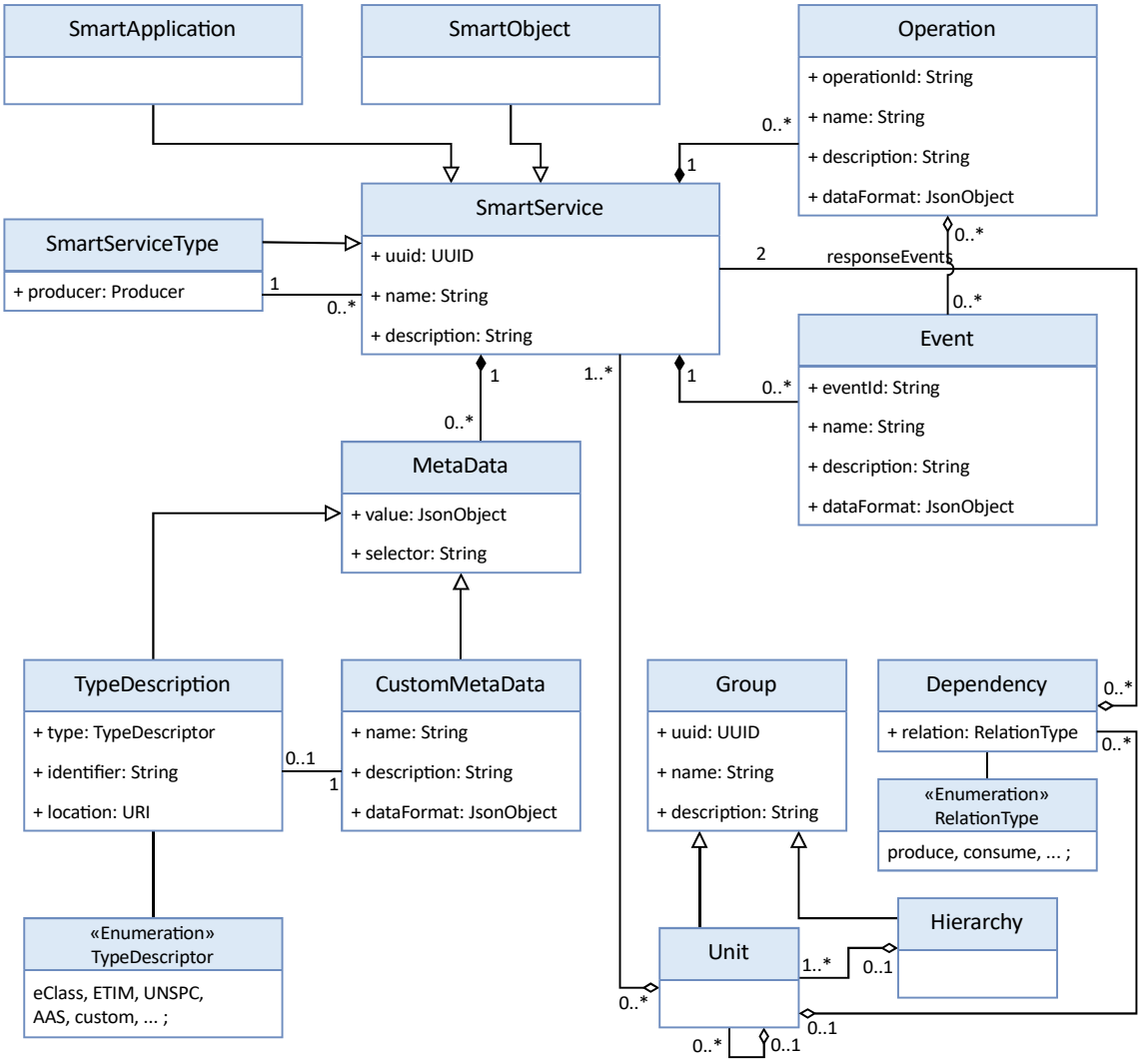


Abbildung 5.7 Erweitertes MSB Informationsmodell

5.4 Technologieauswahl, Implementierung und Deployment

Da die Implementierungsarchitektur auf dem SOA-Prinzip basiert ist die Implementierung der einzelnen Komponenten komplett Technologie-unabhängig.

Das bedeutet, dass jede Komponente im Prinzip mit jeder beliebigen Technologie umgesetzt werden kann, die ihre grundsätzlichen Anforderungen erfüllt. Im Folgenden soll daher noch eine Übersicht der verwendeten Technologien inklusive einer kurzen Begründung für die Auswahl der jeweiligen Technologie gegeben werden.

Abbildung 5.8 zeigt hierzu eine Übersicht der Komponenten und ihrer jeweiligen Implementierungstechnologie bzw. Sprache.

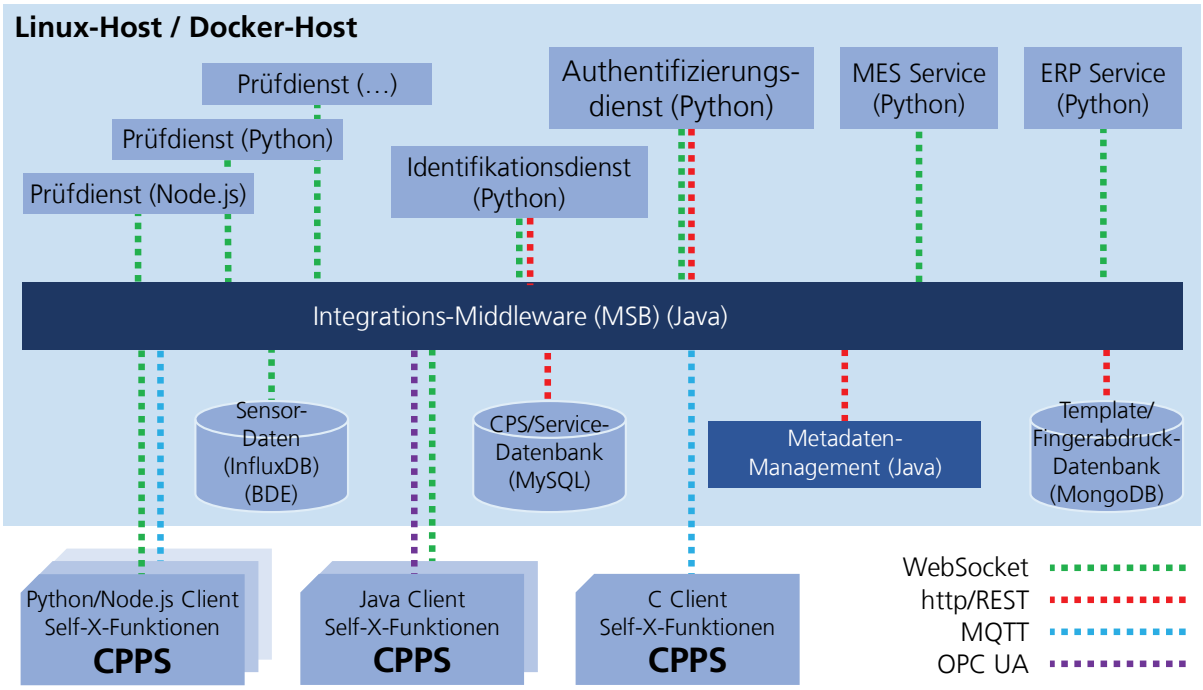


Abbildung 5.8 Komponenten-Implementierung und -Deployment

Der MSB bzw. seine Komponenten sind in Java implementiert. Daher ist das Metadatenmanagement auch mit Java umgesetzt, da der MSB ein internes Framework beinhaltet, das die Entwicklung zusätzlicher Module erleichtert. Jede MSB-Komponente ist zudem mittels des Spring-Frameworks umgesetzt, welches mit Spring Boot die Möglichkeit bietet, sie als eigenständigen Microservice selbst ausführbar zu machen. Die MSB-Komponenten kommunizieren untereinander über http/REST-Schnittstellen.

Der Authentifizierungsdienst ist als Python-Applikation umgesetzt und nutzt den MSB Python-Client. Die Prüfdienste sind ebenfalls als leichtgewichtige Microservices in Node.js oder Python implementiert und nutzen die jeweiligen Client-Implementierungen. Der Vorteil von Node.js ist eine sehr einfache und direkte Modifikation des Quellcodes und die hohe Flexibilität und umfassende Verfügbarkeit von Bibliotheken für Webanwendungen.

Python wiederum bietet aufgrund der Verwendung in vielen Data Science-Anwendungen eine große Anzahl von Bibliotheken, die auf die Verarbeitung von Daten ausgelegt sind. Je nach Art eines Merkmals und der gewählten Prüfstrategie kann also eine Implementierung in der jeweiligen Sprache vorteilhaft sein.

Die CPS/Service-Datenbank nutzt die bereits vorhandene relationale MySQL-Datenbank des MSB und implementiert das angepasste Datenmodell zur Abbildung der Smarten Objekte (CPS) und Applikationen (Dienste). Die Template- und Fingerabdruck-Datenbank ist mit MongoDB umgesetzt. Alternativ kann OrientDB genutzt werden, eine Multi-Model NoSQL Datenbank, die es ermöglicht gleichzeitig eine Dokumentendatenbank und eine Graphdatenbank zu nutzen. Die Legacy-MES-, -ERP-Systeme werden durch Microservices emuliert. Sensordaten werden in einer Zeitreihendatenbank (InfluxDB) gespeichert, die ebenfalls als Microservice über einen Node.js-Client-Adapter an den MSB angebunden ist.

Die angebundenen eingebetteten Systeme der CPS-Komponenten nutzen überwiegend erweiterte MSB-Python-Clients, die über das WebSocket-Protokoll kommunizieren. Die ausgewählten Komponenten verfügen über Linux-basierte Betriebssysteme. Diese wurden ausgewählt, da sie die notwendige Leitungsfähigkeit und Flexibilität bieten, um die Self-X-Fähigkeit zur Selbstbeschreibung und zur Umsetzung diverser Fingerprinting-Fähigkeiten zu implementieren. Python ist im Umfeld der Linux-basierten eingebetteten Systeme und Mikrocomputer weitverbreitet. Daher ist eine Vielzahl von Bibliotheken verfügbar die zum Device-Fingerprinting eingesetzt werden können. Clients können jedoch auch in Node.js, Java oder C implementiert sein und auch das MQTT- oder OPC UA-Protokoll nutzen, je nachdem was die Anwendung oder das eingebettete System erfordert. Diese Ausprägung kann auch als charakteristisches Merkmal verwendet werden.

Sämtliche Dienste werden auf Linux-Hostsystemen ausgeführt, sind aber prinzipiell auch unter Windows bzw. jedem Betriebssystem lauffähig, welches eine Laufzeitumgebung für Java (JVM), Node.js und Python bietet. Zudem lassen sich die Dienste des Authentifizierungssystems als Docker-Dienste in Container kapseln, was ihre Portabilität und Möglichkeit zur Skalierung ermöglicht.

6 Erprobung und Validierung

Dieses Kapitel beschreibt die Szenarien, die zur Dokumentation und Validierung des entwickelten Konzepts dienen. Im Rahmen von vier Fallstudien wird zunächst dargelegt, welche Merkmale verschiedene CPPS aufweisen können und wie diese gemäß dem entwickelten Konzept klassifiziert werden können. Zudem werden die im Rahmen der Erprobung verwendeten Versuchsaufbauten zur experimentellen Validierung dargestellt. Darauffolgend sind die Ergebnisse dargestellt, die im Anschluss diskutiert werden.

6.1 Fallstudien

CPPS können in zahlreichen verschiedenen Ausprägungen mit unterschiedlicher Komplexität auftreten. Dadurch können sie über eine Vielzahl von Merkmalsquellen verfügen. Im Folgenden soll daher an ausgewählten Beispielen in Form von Fallstudien dargestellt werden, wie die charakteristischen Merkmale eines solchen jeweiligen CPPS-Typs aussehen können. Die Fallstudien entstammen realen Anwendungsfällen bzw. Produkten von Unternehmen und wurden teilweise abstrahiert. Zudem wurden sensitive Daten entfernt, um Interna und IP-relevante Informationen zu schützen. Die Fallstudien wurden mit dem Ziel ausgewählt, möglichst unterschiedliche Charakteristika abzubilden und um die Breite der Variation darzustellen, in der sich CPPS und das Potenzial für Merkmalsquellen zum Zweck der merkmalsbasierten Authentifizierung vorfinden. Sie stellen vier Archetypen dar (vgl. Tabelle 12), die exemplarisch für die in der Produktion überwiegend eingesetzten Gruppen von intelligenten Maschinen stehen sollen: Werkzeugmaschinen, smartifiziertes Legacy-Equipment, mobile Roboter und eine modulare Produktionsanlage:

- Eine moderne „smarte“ Werkzeugmaschine, die bereits viele der CPS-Charakteristika in sich trägt.
    - Vernetzte Laserschneidanlage

- Eine „smartifizierte“ Anlage, die mittels intelligenter Vorschaltgeräte mit den notwendigen CPS-Fähigkeiten ausgestattet wird.
    - Scitis.io - SOTEC CloudPlug Edge und Kompressoren
- Ein mobiler Roboter in Form eines FTF, der durch die Nutzung offener und moderner Komponenten großes Potenzial bietet neben bereits bestehenden CPS-Fähigkeiten mit zusätzlichen Fähigkeiten ausgestattet zu werden.
    - BÄR Automation FTF mit Leichtbauroboterarm
- Eine Anlage, die sich aus mehreren CPS-Komponenten zusammensetzt, die eine CPPS-Einheit bilden und einen verketteten Prozess abbilden.
    - Festo Didactic CP LAB

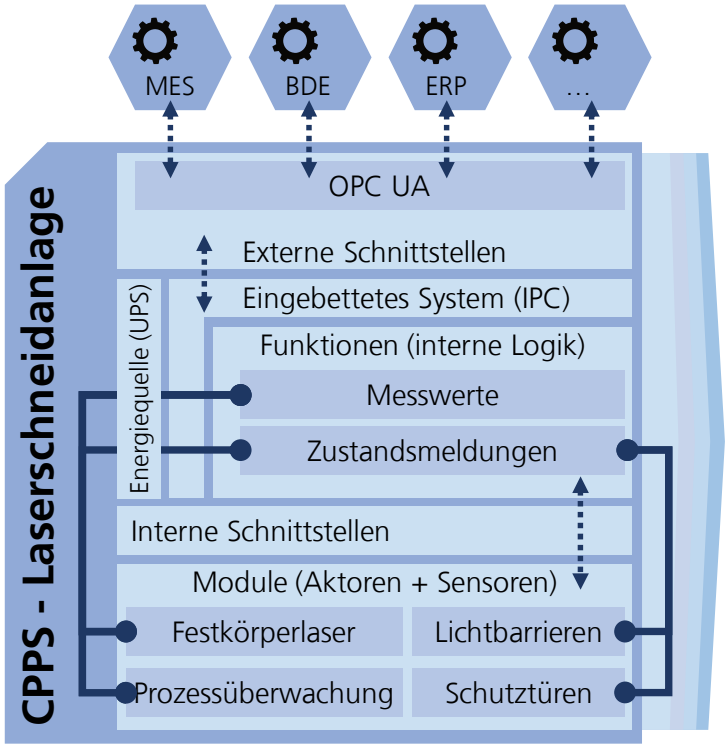
Die ausgewählten CPPS-Archetypen lassen sich wie in Tabelle 12 dargestellt unterscheiden.

Tabelle 12 Betrachtete CPPS-Archetypen

Archetyp	Intelligente Werkzeug-maschine	Smartifizierte Legacy-Maschine	Mobiles Roboter-System	Vernetzte, modulare Anlage
Merkmal	**Ausprägung**			
Einsatzzweck	Bearbeitungs-prozess	Flexible Logistik	Prozess-Überwachung	Prozess-verkettung
Module	Autark	Nicht-autark	Hybrid	
Rechenkapazität	Niedrig	Mittel	Hoch	
Kern-Dienste	Lokal	Ausgelagert	Hybrid	
Intelligenz	Integriert	Vorschaltgerät	Ausgelagert	Hybrid
CPPS-Struktur	Atomar	Geschachtelt	Modular	
Steuerung	Proprietär	Offen	Hybrid	
Steuerungsarchi-tektur	Zentral	Dezentral	Hybrid	
Mobilität	Mobil	Stationär	Mobile Komponenten	
Energiequelle	Intern-zentral	Intern verteilt	Extern	Hybrid
Kommunikation	Kabel	Kabellos	Hybrid	
Kommunikati-ons-Protokolle	OPC UA	MQTT	ROS	Hybrid (inkl. Websocket)
Echtzeit	Hart/Weich	Keine	Hybrid	

6.1.1 Fallstudie 1 – Vernetzte Laserschneidanlage

In dieser Fallstudie wurde eine Laserschneidanlage eines deutschen Herstellers untersucht, die einen hohen Automatisierungsgrad in Bezug auf die Bestückung, Verarbeitung und Entnahme von Metallteilen besitzt und bei zahlreichen metallverarbeitenden Unternehmen zum Einsatz kommt. Die Anlage ist von Grund auf als IoT-fähige Maschine konzipiert und verfügt über viele Eigenschaften eines CPPS. Abbildung 6.1 zeigt eine Abbildung der Anlage und eine schematische Darstellung der CPPS-Struktur. Zudem ist ein beispielhafter Auszug der Signale inklusive Benennung gelistet.



Beispiele für Signale:
ID x: LaserTechnology
ID x: SlugDetected
ID x: PartsSuspect
ID x: LaserBeamOnTime
ID x: ClampPositions
ID x: EnergyMetering
ID x: VoltagePhase2
ID x: Workpiece
ID x: StationNumber
ID x: Name
ID x: Status.Running
ID x: Methods
ID x: BatchNumber
ID x: OperatingMode
ID x: BeamQualityFactorCondition
ID x: …

Abbildung 6.1 Vernetzte Laserschneidanlage - CPPS Schema und Signale

Zur schematischen Darstellung ist anzumerken, dass diese nur die ideale Struktur, Funktion und Beziehungen von Komponenten zueinander darstellt, um das CPPS-Prinzip auf

die Anlage abzubilden. Dies ist notwendig, um die Komplexität der Maschine zu reduzieren und das Beispiel greifbarer zu gestalten. Dieser Ansatz kann jedoch auch in der realen Anwendung eingesetzt werden und entspricht dem Gedanken bestimmte komplexe Komponenten und ihre Fähigkeiten als Dienste zu abstrahieren. So ist das eingebettete System der Anlage ein Industrie PC (IPC) und wird in diesem Beispiel als die zentrale Recheneinheit des CPPS gewertet. Die Sensoren und Aktoren sind als nicht-eigenständige Module gruppiert, die bestimmte Aufgaben erfüllen. Tatsächlich verfügen sie selbst über eigene eingebettete Rechner-Einheiten, die je nach Fähigkeit auch als vollwertige CPS gewertet werden könnten. An dieser Stelle sollen sie jedoch der Einfachheit wegen nur als nicht-eigenständige funktionale Baugruppen des gesamten CPPS zusammengefasst werden sollen.

Die Dokumentation der Anlage listet weit über 400 spezifische Signale, die als unterschiedliche Merkmalsquellen dienen können. Zudem verfügt beispielsweise jedes Laser-Modul über eine zusätzliche große Anzahl von Signalen, die umfassend die Zustands- und Prozesswerte während des Laserschneidens erfassen. Aus Gründen der Vertraulichkeit wurde nur ein kleiner Auszug dieser Signale in Abbildung 6.1 mit Klarnamen gelistet, wobei die interne ID-Nummer zusätzlich entfernt wurde. In Tabelle 13 sind weitere Signale des Laservollautomaten aus der Dokumentation sinngemäß übertragen und als Merkmale inklusive einer möglichen Klassifizierung und Zuteilung von Merkmalseigenschaften gelistet. Hierbei ist zu beachten, dass einzelne Merkmale unterschiedlich oder mehrfach ausgelegt werden können, weshalb ggf. mehrere Merkmalsklassen mit unterschiedlichen Merkmalseigenschaften gelistet sind.

Offene, geschlossene oder geschützte Eigenschaften von Merkmalen werden nicht betrachtet, da diese frei definierbar sind und neben der natürlichen bzw. künstlichen Charakteristik eines Merkmals Auswirkungen auf die Merkmalsstärke haben, die hier deshalb auch nicht explizit betrachtet wird.

Die Anlage bietet eine Vielzahl von möglichen Merkmalsquellen und bringt grundsätzlich die Voraussetzungen mit als vollwertiges CPPS den in dieser Arbeit diskutierten Authentifizierungsansatz auf Basis von Selbstbeschreibungsmerkmalen zu adaptieren. Eine Auswahl der möglichen Merkmale ist in Tabelle 13 gelistet.

Tabelle 13 Merkmale Laserschneidanlage (Auswahl)

Merkmal	Ausprägung/ Anmerkung	Merkmalsklasse	Merkmalseigenschaften
Produktname	Formeller Name	Seins-Merkmal	statisch, einfach, künstlich
Gerätenummer	Eindeutige Nummer	Seins-Merkmal	statisch, einfach, künstlich
Produktionsplan	Produktionsplan Steuerung Status	Besitzmerkmal Fähigkeits-Merkmal Zustands-Merkmal	statisch, komplex, künstlich statisch, komplex, künstlich dynamisch, einfach, künstlich
Technologieliste	Einzelne Einträge Spezifische Technologie Komponenten-Struktur	Besitz-Merkmal Seins-Merkmal Struktur-Merkmal	statisch, einfach, künstlich statisch, komplex, künstlich statisch, komplex, natürlich
Laserschneiden (Modul)	Laser-Modul Modulbeschreibung	Besitz-Merkmal Fähigkeits-Merkmal	statisch, einfach, künstlich statisch, komplex, künstlich
Laser (Komponente)	Laser-Komponente Anzahl Gas-Art Laserstrahl-Betriebszeit	Besitz-Merkmal Seins-Merkmal Zustands-Merkmal Seins-Merkmal	statisch, einfach, künstlich statisch, einfach, künstlich dynamisch, einfach, künstlich dynamisch, einfach, natürlich
Energie-Metering (Laser)	Live (echtzeitnah) Historisch (aus DB)	Wert-Merkmal	dynamisch, einfach, natürlich dynamisch, einfach, natürlich
Funktionale Sicherheitsgeräte	Zustände Zustände mit Kontext	Zustands-Merkmal Kontext-Merkmal	Statisch Ereignis-bezogen, Zeit-bezogen
Palettenwechsel (Modul)	Palettenwechsel-Modul Palettenposition	Besitz-Merkmal Wert-Merkmal	statisch, einfach, künstlich dynamisch, einfach, natürlich
Energie-Metering	Energie-Metering Echtzeit-Werte	Fähigkeits-Merkmal Wert-Merkmal	statisch, einfach, künstlich dynamisch, einfach, natürlich
Stanzbutzen	Detektion- Ereignis Anzahl - Wert	Kontext-Merkmal Wert-Merkmal	Ereignis-bezogen, Zeit-bezogen dynamisch, einfach, natürlich
Teile-Zähler	Anzahl produzierter Teile	Wert-Merkmal	dynamisch, einfach, natürlich
Werkstück	Bezug zu ERP/MES Daten	Beziehungsmerkmal	statisch, komplex, natürlich
IPC (Industrie-PC)	IPC Freier Speicher Ladezustand UPS	Besitz-Merkmal Wert-Merkmal Wert-Merkmal	statisch, einfach, künstlich dynamisch, einfach, natürlich dynamisch, einfach, natürlich
Diagnostik	Abfrage der Diagnostik z.B. Konnektivität	Fähigkeitsmerkmal Zustandsmerkmal	statisch, einfach, künstlich dynamisch, einfach, künstlich
Uhrzeit (lokal)	Referenz und zeitlicher Bezug von Ereignissen	Kontext-Merkmal	dynamisch, komplex, natürlich, Zeit-bezogen (alle Ereignisse)

Der IPC bietet die Möglichkeit die notwendige zusätzliche interne Logik zur Umsetzung weiterer Self-X-Fähigkeiten umzusetzen, um weitere Fingerprinting-Verfahren zu integrieren. Über die OPC UA-Schnittstelle, können beliebige dieser Signale an Dienste, wie beispielsweise ein BDE, MES, ERP oder weitere (siehe Abbildung 6.1) verteilt werden.

Abbildung 6.2 zeigt eine schematische Selbstbeschreibung, die an ausgewählten Beispielen darlegt, wie diese Merkmale in einer Selbstbeschreibung zur Ableitung von möglichen Authentifizierungsmaßnahmen abgebildet werden können.

Es ist möglich mit wenig zusätzlichem Aufwand eine komplexe Selbstbeschreibung mittels der bestehenden Fähigkeiten der Anlage zu erstellen. Diese beinhaltet neben allgemeinen statischen Merkmalen auch Identifikatoren. Zusätzlich zu den bestehenden Signalen, die Komponenten- und Fähigkeitsbezogen sind und Zugriff auf dynamische Merkmale ermöglichen können noch die externen Dienste referenziert werden, um beispielsweise eine Abfrage historischer Daten zu ermöglichen. Diese erlauben eine Ableitung weiterer komplexer Beziehungs-/Struktur-, Kontext- und Verhaltensmerkmale.

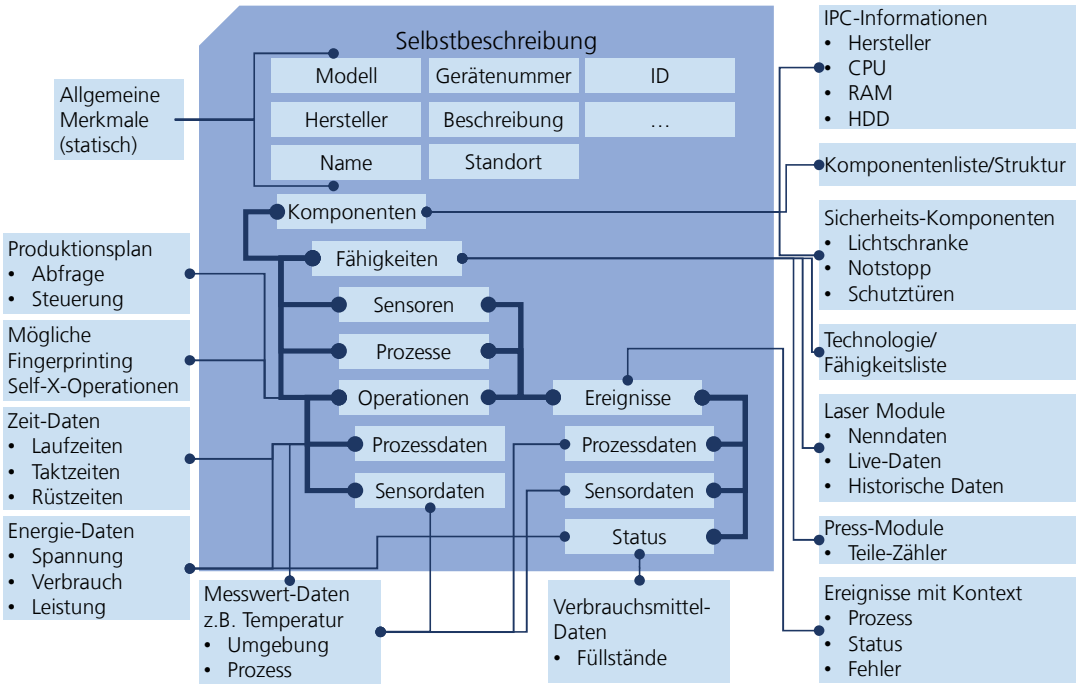


Abbildung 6.2 Vereinfachte CPPS-Selbstbeschreibung einer Laserschneidanlage

6.1.2 Fallstudie 2 – Cloud-Integration mit einem Intelligenten Vorschaltgerät

Die Firma scitis.io nutzt einen SOTEC CloudPlug Edge um Kompressoren der Firma CompAir über Modbus anzubinden und mit einer Cloud-Infrastruktur zu verbinden, in welcher die gesammelten Daten zu Optimierungszwecken gesammelt und ausgewertet werden. Die Struktur dieses CPPS ist in Abbildung 6.3 dargestellt. Der CloudPlug Edge ist ein Vorschaltgerät und dient zur Integration von Maschinen und Sensorik in Cloud-Infrastrukturen und mit Diensten. Dies ist vor allem dann notwendig, wenn diese beispielsweise Legacy-Equipment nicht IP-fähig ist und keine eigene Compute-Hardware besitzen, die das „Gehirn" eines CPS bilden könnte. Hierfür verfügt der CloudPlug Edge über einen leistungsfähigen Chipsatz, der es ihm ermöglich gemeinsam im Verbund mit anderen Peripheriegeräten ein CPPS zu bilden.

Im Vorliegenden Beispiel sind vier Kompressoren und ein Volumenstromsensor über Modbus angebunden. Zudem sind mehrere Sensoren, die analoge Signale ausgeben, die mit einem Signalwandler in digitale Signale umgewandelt werden, mit dem CloudPlug verbunden. Tabelle 14 listet einige der möglichen Merkmale, die sich aus dieser Konfiguration ergeben.

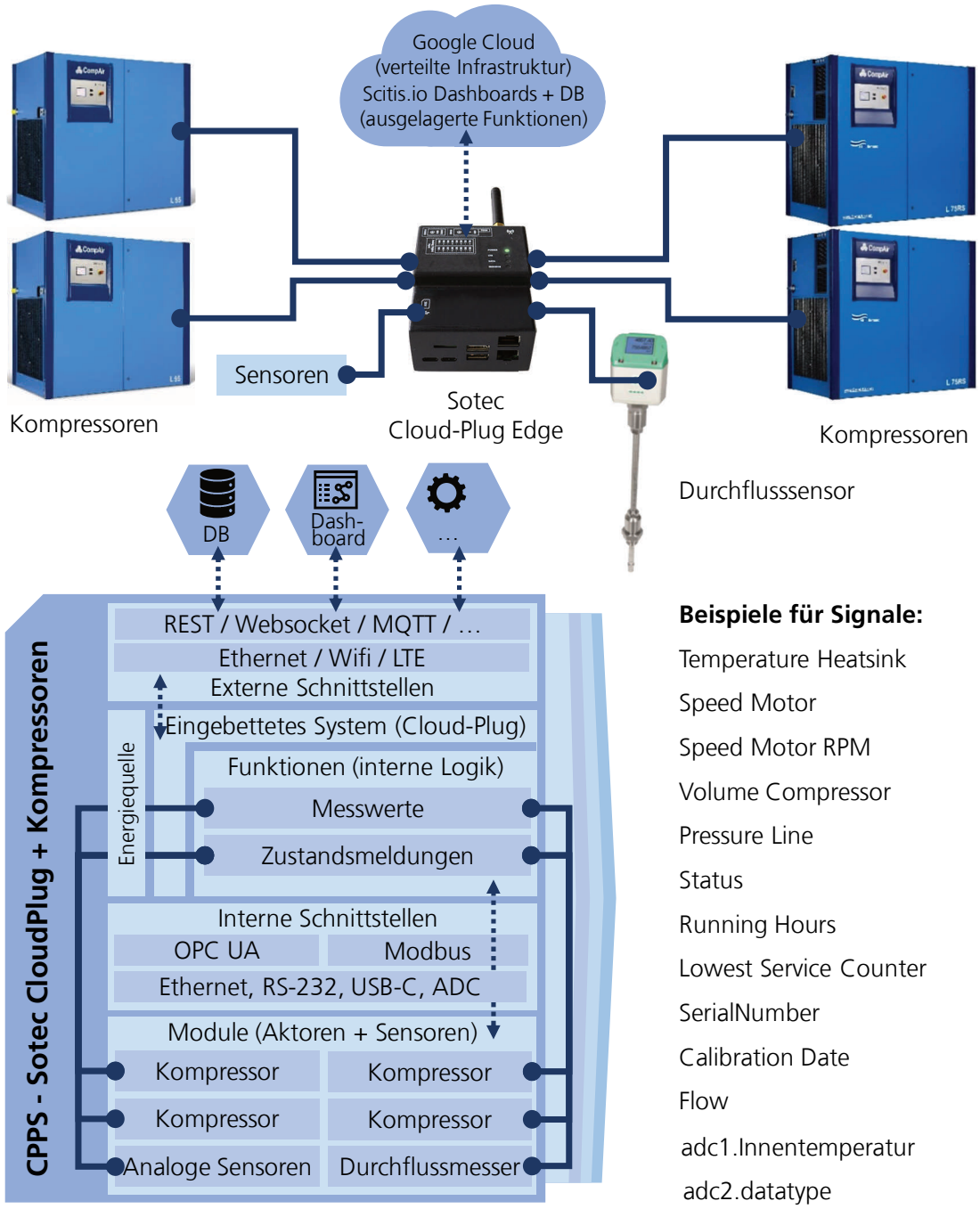


Abbildung 6.3 Darstellung CompAir Kompressoren und SOTEC CloudPlug Edge (Bildquellen: SOTEC, CS-INSTRUMENTS, CompAir)

Tabelle 14 Merkmale Kompressoren und SOTEC CloudPlug

Merkmal	Ausprägung/Anmerkung	Merkmalsklasse	Merkmalseigenschaften
Embedded System	Cloud Plug, Betriebssystem (Freier) Speicher CPU-Geschwindigkeit CPU-Architektur Installierte Pakete	Besitz-Merkmal Seins-Merkmal Wert-Merkmal Wert-Merkmal Seins-Merkmal Seins-Merkmal	statisch, einfach, künstlich dynamisch, einfach, natürlich dynamisch, einfach, natürlich dynamisch, einfach, natürlich statisch, einfach, natürlich dynamisch, einfach, künstlich
Kompressoren	2x L55, 2x L75RS	Besitz-Merkmal Fähigkeits-Merkmal Struktur-Merkmal	statisch, einfach, künstlich statisch, einfach, natürlich statisch, komplex, künstlich
Volumenstrom-Sensor	-	Besitz-Merkmal Fähigkeits-Merkmal	statisch, einfach, künstlich statisch, einfach, künstlich
Analoge Sensoren	Drucksensor, Temperatursensoren, Taupunktsensor	Besitz-Merkmal Fähigkeits-Merkmal	statisch, einfach, künstlich statisch, einfach, natürlich
Analoge Sensordaten	Umgebungsdaten (Druck, Temperatur (innen/außen), Taupunkt)	Wert-Merkmal	dynamisch, einfach, natürlich
Kühlkörper-Temperatur	-	Wert-Merkmal	dynamisch, einfach, natürlich
Nachlauf-Timer	-	Fähigkeits-Merkmal Wert-Merkmal	statisch, einfach, künstlich dynamisch, einfach, künstlich
Motor Drehzahl	-	Wert-Merkmal	dynamisch, einfach, natürlich
Motor (Verbrauch)	Aktueller Verbrauch Verbrauch im Lastkontext	Wert-Merkmal Verhaltens-Merkmal	dynamisch, einfach, natürlich dynamisch, komplex, natürlich
Betriebs-stunden	-	Seins-Merkmal	dynamisch, einfach, natürlich
Laststunden	-	Seins-Merkmal	dynamisch, einfach, natürlich
Fehlerliste	Liste der möglichen Fehlermeldungen	Fähigkeits-Merkmal Wert-Merkmal	statisch, einfach, künstlich statisch, einfach. künstlich
Uhrzeit (lokal)	Referenz und zeitlicher Bezug von Ereignissen	Kontext-Merkmal	dynamisch, komplex, natürlich, Zeit-bezogen (alle Ereignisse)

Da die Kompressor-Komponenten dieses CPPS „unintelligent“ sind, ergeben sich nicht viele Eigenfähigkeiten aus diesen Modulen, die als komplexe Merkmale dienen könnten, sondern überwiegend einfache Sensordaten-basierte Wert-Merkmale. Allerdings besteht die Möglichkeit durch eine vierfache Verfügbarkeit vieler Merkmale aus einfachen Merkmalen in Kombination mit z.B. Zeitstempeln oder einem bestimmten Betriebszustand komplexe Verhaltensmerkmale zu konstruieren. Der offene Charakter des CloudPlugs als eingebettetes Kernsystem des CPPS ermöglicht es zudem spezifische Systemdaten aus diesem abzufragen und aktive Fingerprinting-Funktionalität zu implementieren. Abbildung 6.4 zeigt wie sich diese Merkmale in eine Selbstbeschreibung fügen können.

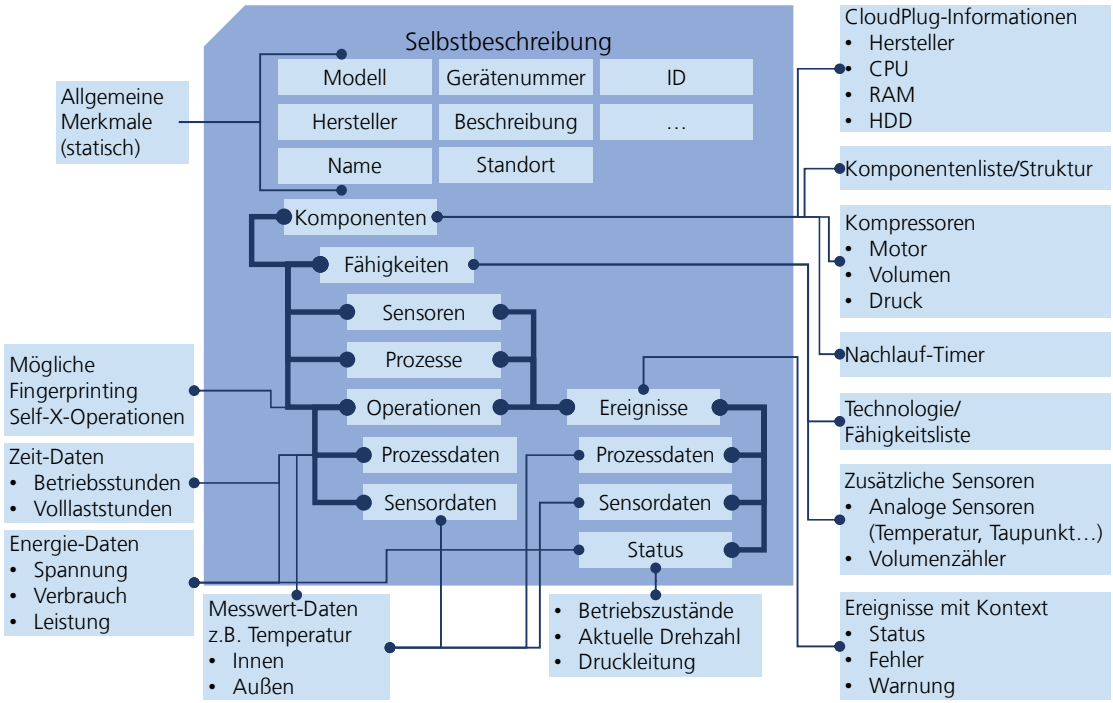


Abbildung 6.4 Vereinfachte CPPS-Selbstbeschreibung für CloudPlug-Kompressor-CPPS-Verbund

Die Möglichkeit über zusätzliche Sensorik Umgebungsdaten zu erfassen erlaubt es zudem beispielsweise diese entweder für den Abgleich von Wertmerkmalen aus der externen Datenbank zu nutzen, indem das CPPS einige Werte per Zeitstempel kontextualisiert lokal verschlüsselt vorhält.

6.1.3 Fallstudie 3 – Mobile Roboterplattform

BÄR Automation ist ein Systemintegrator, der auf Sondermaschinenbau und fahrerlose Transportfahrzeuge (FTF) spezialisiert ist. Das von BÄR Automation vorliegende FTF ist eine Sonderanfertigung, die im Future Work Lab des Fraunhofer IPA zum Einsatz kommt und zusätzlich mit einem Leichtbauroboterarm ausgestattet ist. Eine Übersicht des Systems kann Abbildung 6.5 entnommen werden. Ein FTF stellt einen mobilen Roboter dar und verfügt zum Zweck der autonomen Navigation und Bahn- und Trajektorieplanung über

eine Vielzahl von Sensoren zur Wahrnehmung der Umgebung und einen integrierten Rechner mit hoher Rechenkraft, der dazu dient die Sensordaten zu verarbeiten und eine Laufzeitumgebung für lokale Dienste zu bieten.

Beispiele für Signale:

Temperatur Antrieb innen	Kamerabild
Temperatur Antrieb außen	Stellwinkel
Drehmoment	Spannung, Stromaufnahme
Transpondersignal (Id)	Status Überstromschutz
	Positionierung und Koordinaten

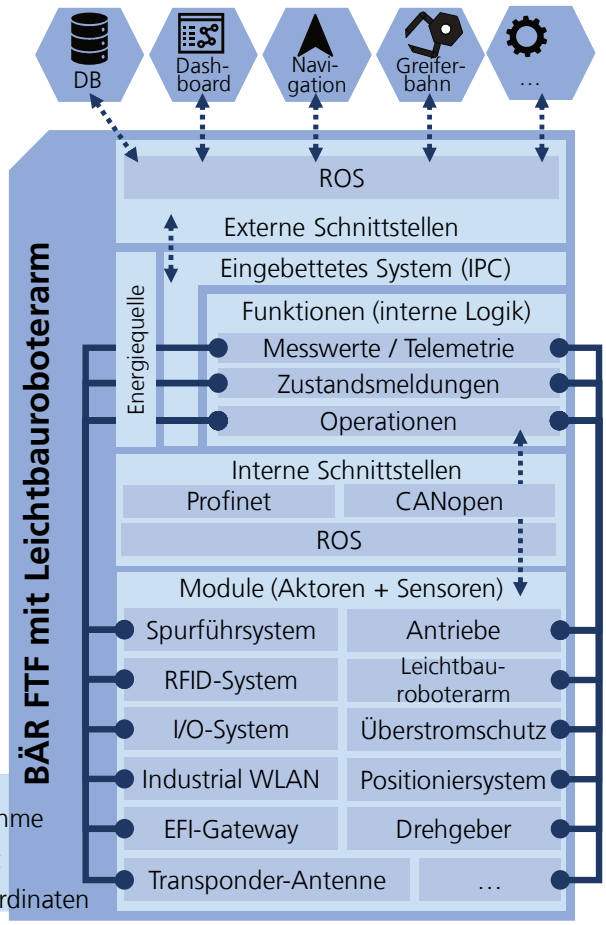


Abbildung 6.5 Darstellung BÄR Automation FTF

Es sollte erkennbar sein, dass ist ein FTF aufgrund des Einsatzes moderner und offener Soft- und Hardwarekomponenten ein CPS bzw. durch seinen Einsatz auf dem Hallenboden ein Beispiel für ein fortgeschritteneres CPPS darstellt. Insbesondere die dargestellten Dienste sind vollkommen optional und durch offene Middleware-Software wie ROS (Robot Operating System) einfach zu integrieren, um die Fähigkeiten des CPPS zu erweitern. Beispielsweise lässt sich die Fähigkeit der Berechnung von Greiferbahnen des Greifarms

aus dem integrierten IPC in einen Dienst auf eine Edge-Cloud verlagern. Ebenso lässt sich eine Cloud-basierte Navigation anbinden, die die lokalen Sensordaten des FTF um Sensor- und Navigationsdaten anderer FTF und Daten externer Sensor anreichern kann. So können beispielsweise andere (bereits authentifizierte) FTF bzw. CPPS in der unmittelbaren Umgebung des FTF dessen Lage und Positionsdaten oder andere von diesem zur Authentifizierung bereitgestellte Merkmalsdaten mit Umgebungs- oder Präsenz-Bezug bestätigen.

Die Hardware des vorliegenden BÄR AGV besteht aus Komponenten verschiedener Hersteller, die über das Profinet-Prokoll untereinander kommunizieren können. Einige Komponenten, die nicht über Ethernet-Schnittstellen verfügen, sind über das CANopen-Prokotoll oder entsprechende Gateways über andere Schnittstellen (z.B. Seriell, EFI-Bus oder EnDat2.2) angebunden. CANopen stellt eine EDS-Datei (Electronic Data Sheet) bereit, die die durch den Bus verfügbaren Datenpunkte beschreibt und somit als Quelle für Merkmale dienen kann. Der IPC wird in diesem Beispiel als das führendes eingebettete System betrachtet, da andere Komponenten zwar über eigene eingebettete Systeme verfügen, diese aber nicht offen oder explizit für einen Einsatzzweck zur Ansteuerung und Daten(vor)verarbeitung von Sensoren und Aktoren verwendet werden und Teilsysteme des Gesamtsystems darstellen. Da Linux als Betriebssystem für den IPC eingesetzt wird besteht die Möglichkeit beliebige Dienste auf dem IPC bereitzustellen oder IPC-bezogene Fingerprinting-Fähigkeiten zu implementieren, die eine Bereitstellung der Daten und bestimmter Merkmale erlauben. Die Kommunikation über externe Schnittstellen findet hier auf der physikalischen Schnittstelle über Wireless LAN (IEEE 802.11n) statt. Es können zudem sämtliche TCP/IP-basierte Kommunikationsprotokolle integriert werden, für die eine Implementierung für Linux verfügbar ist, wobei der Einsatz von ROS beispielsweise sehr charakteristisch für Robotik-Systeme ist. Mit dem steigenden Freiheitsgrad, der sich durch die Offenheit und die Fähigkeiten der einzelnen Komponenten des CPPS ergibt, zeigt sich, dass auch die Anzahl der Möglichen Merkmale erhöht. Dies führt allerdings auch einer Zunahme der Komplexität, insbesondere wenn der Detaillierungsgrad hoch gewählt wird. Die Handhabbarkeit und der Aufwand hängen vom Implementierungsgrad der Self-X-Fähigkeiten im CPPS ab. Auf viele der in Tabelle 15 gelisteten ausgewählten Datenquellen bzw. Merkmale des BÄR AGV und seiner Komponenten kann direkt zugegriffen werden.

Tabelle 15 Merkmale BÄR Automation FTS mit Leichtbauroboterarm

Merkmal	Ausprägung/Anmerkung	Merkmalsklasse	Merkmalseigenschaften
Gerätename	Formeller Name	Seins-Merkmal	statisch, einfach, künstlich
Gerätenummer	Eindeutige Nummer	Seins-Merkmal	statisch, einfach, künstlich
Herstellername	-	Seins-Merkmal	statisch, einfach, künstlich
Standort	Mobil	Kontext-Merkmal	dynamisch, komplex, natürlich
Navigations-dienst	Navigieren Navigationsziele (Jobs) Navigationsrouten	Fähigkeitsmerkmal Wert-Merkmal Verhaltens-Merkmal	statisch, einfach, natürlich dynamisch, einfach, künstlich dynamisch, komplex, künstlich
IPC (Industrie-PC)	IPC-Hardware Abfrage Systemdaten Hardware-Architektur Betriebssystem Speicher CPU CPU-Leistung	Besitz-Merkmal Fähigkeits-Merkmal Seins-Merkmal Seins-Merkmal Seins-Merkmal Seins-Merkmal Seins-Merkmal	statisch, komplex, natürlich statisch, einfach, natürlich statisch, einfach, natürlich statisch, einfach, natürlich statisch, einfach, natürlich statisch, einfach, natürlich dynamisch, einfach, natürlich
Induktiver Näherungs-sensor	Hardware Näherungserkennung Status Status/Präsenz	Besitz-Merkmal Fähigkeits-Merkmal Zustands-Merkmal Kontext-Merkmal	statisch, komplex, natürlich statisch, einfach, natürlich dynamisch, einfach, natürlich dynamisch, komplex, natürlich
Spurführungs-system	Kamera Optical-Line Tacker Linien-Tracking Barcode-Lesen	Besitz-Merkmal Besitz-Merkmal Fähigkeits-Merkmal Fähigkeits-Merkmal	statisch, komplex, natürlich statisch, komplex, natürlich statisch, einfach, natürlich statisch, einfach, natürlich
Transponder-/ und Ident-Antenne	Hardware Transponder-Navigation Temperatur Spannung Stromaufnahme Transpondercode (Id) X/Y Position, Frequenzen Systemzustand Generierte Spannung auf Positionierspule	Besitz-Merkmal Fähigkeits-Merkmal Wert-Merkmal Wert-Merkmal Wert-Merkmal Kontext-Merkmal Kontext-Merkmal Zustands-Merkmal Wert-Merkmal	statisch, komplex, natürlich statisch, einfach, natürlich dynamisch, einfach, natürlich dynamisch, einfach, natürlich dynamisch, einfach, natürlich statisch, einfach, künstlich dynamisch, einfach, natürlich dynamisch, einfach, künstlich dynamisch, einfach, natürlich
Auflicht-Positio-niersystem	Hardware Farbband-Lesen Codeband-Lesen Tag-Lesen (Data-Matrix) Tag-Daten Tag-Daten	Besitz-Merkmal Fähigkeits-Merkmal Fähigkeits-Merkmal Fähigkeits-Merkmal Wert-Merkmal Kontext-Merkmal	statisch, komplex, natürlich statisch, einfach, natürlich statisch, einfach, natürlich statisch, einfach, natürlich dynamisch, einfach, natürlich dynamisch, komplex, natürlich
Sicherheits-Laserscanner	Hardware Umgebungs-Scan Hinderniserkennung Winkel (max.) Reichweite (max.) Umgebungsgeometrie	Besitz-Merkmal Fähigkeits-Merkmal Fähigkeits-Merkmal Seins-Merkmal Seins-Merkmal Wert-Merkmal	statisch, komplex, natürlich statisch, einfach, natürlich statisch, einfach, natürlich statisch, einfach, natürlich statisch, einfach, natürlich dynamisch, komplex, natürlich
RFID-System	Hardware RFID-Erkennung RFID-Daten	Besitz-Merkmal Fähigkeits-Merkmal Wert-Merkmal	statisch, komplex, natürlich statisch, einfach, natürlich statisch, einfach, künstlich

	RFID-Daten	Kontext-Merkmal	dynamisch, einfach, natürlich
Industrial-Wireless LAN	Hardware Modell Hersteller WLAN-Technik Max. Bandbreite HW-Adresse	Besitz -Merkmal Seins-Merkmal Seins-Merkmal Seins-Merkmal Fähigkeits-Merkmal Seins-Merkmal	statisch, komplex, natürlich statisch, einfach, künstlich statisch, einfach, künstlich statisch, einfach, natürlich statisch, einfach, natürlich statisch, einfach, natürlich
Komponenten (individuell)	Komponentenliste Fähigkeitsliste Schnittstellen Topologie	Seins-Merkmal Seins-Merkmal Seins-Merkmal Seins-Merkmal	statisch, einfach, künstlich statisch, einfach, künstlich statisch, einfach, künstlich statisch, einfach, künstlich
I/O-System	Hardware Integrierte Komponenten Integrierte interne Komponenten	Besitz-Merkmal Fähigkeits-Merkmal Beziehungs-/ Struktur-Merkmal	statisch, komplex, natürlich statisch, einfach, natürlich statisch, komplex, natürlich
Antriebe	Hardware Telemetrie-Auslesen Temperatur Leistungsaufnahme Beschleunigung	Besitz-Merkmal Fähigkeits-Merkmal Wert-Merkmal Wert-Merkmal Verhaltens-Merkmal	statisch, komplex, natürlich statisch, einfach, natürlich dynamisch, einfach, natürlich dynamisch, einfach, natürlich dynamisch, komplex, natürlich
Antriebs-verstärker	Hardware Temperatur Motor Temperatur Extern Status	Besitz-Merkmal Wert-Merkmal Wert-Merkmal Zustands-Merkmal	statisch, komplex, natürlich dynamisch, einfach, natürlich dynamisch, einfach, natürlich dynamisch, komplex, natürlich
Drehgeber	Hardware Drehwinkel HW-Adresse	Besitz-Merkmal Wert-Merkmal Seins-Merkmal	statisch, komplex, natürlich dynamisch, einfach, natürlich statisch, einfach, natürlich
Uhrzeit (lokal)	Referenz und zeitlicher Bezug von Ereignissen	Kontext-Merkmal	dynamisch, komplex, natürlich, Zeit-bezogen (alle Ereignisse)
Ort	Koordinaten Präsenz	Kontext-Merkmal Kontext-Merkmal	Orts-bezogen (alle Ereignisse)

Die vereinfachte Selbstbeschreibung in Abbildung 6.6 zeigt aus Darstellungsgründen eine vereinfachte Struktur der möglichen Selbstbeschreibung. Die Fähigkeiten des CPPS sind hauptsächlich auf eine Auswahl der fachlichen Funktionen bezogen.

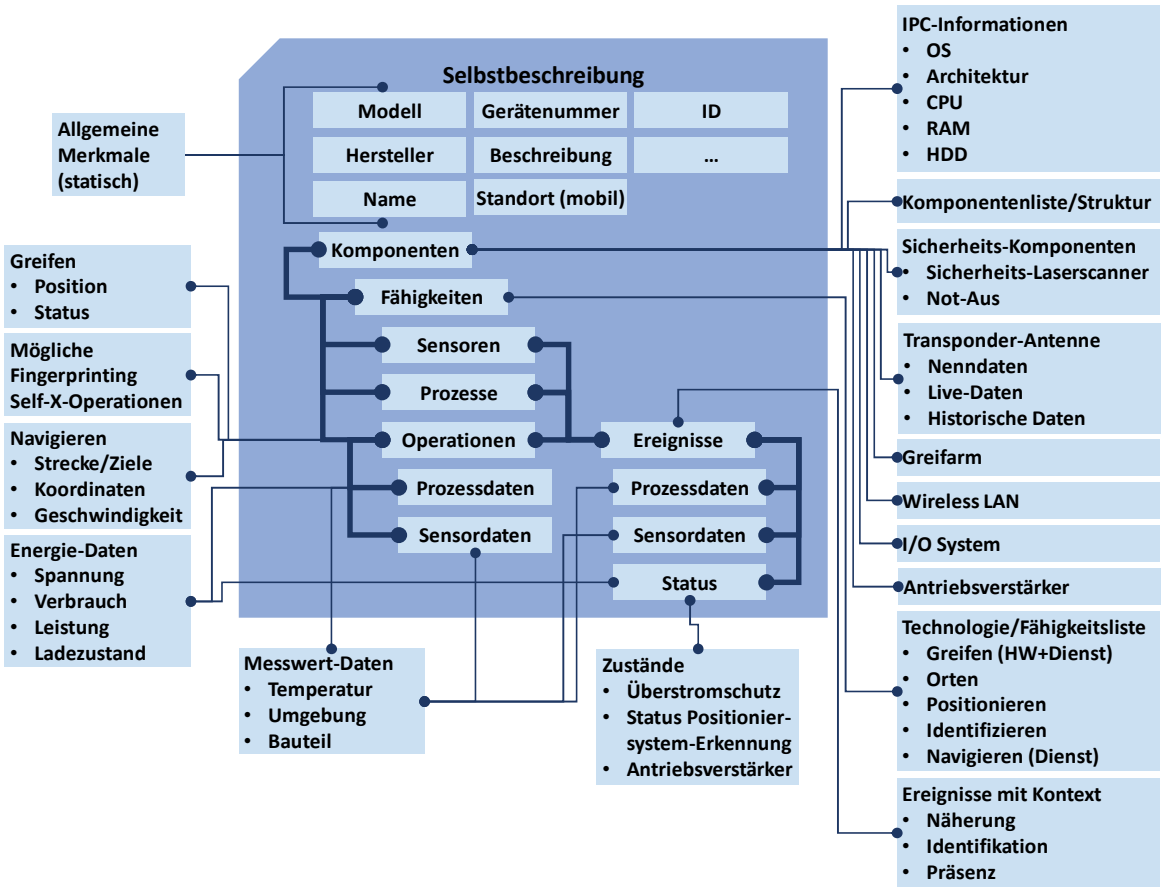


Abbildung 6.6 Vereinfachte CPPS-Selbstbeschreibung BÄR FTF

Allerdings kann jede Möglichkeit ein bestimmtes Datum aus dem System als Wert-Merkmal zu extrahieren selbst als Fähigkeits-Merkmal ausgelegt werden. Der Bezug dieser Daten zu Zeitdaten und insbesondere aufgrund der Mobilität des CPPS zu Ortsdaten erlaubt eine Schaffung von komplexen Kontext-Daten. Weitere Komponenten erlauben Erfassung von Umwelt- und Umgebungsdaten und Präsenzdaten. Diese können wiederum mit einem zeitlichen Verlauf versehen als Verhaltens-Merkmale ausgelegt werden. Durch die Verfügbarkeit einer großen Komponentenliste, deren einzelne Komponenten charakteristisch miteinander verknüpft sind, lassen sich auch Struktur- und Beziehungsmerkale ableiten.

6.1.4 Fallstudie 4 – Modulare Umlaufband-Anlage

Das FESTO Cyber-Physical (CP) Lab ist ein kompaktes Industrie 4.0-Lernsystem von Festo Didactic. Es wird zu Lehrzwecken angeboten und enthält die relevanten Technologien und Komponenten, beispielsweise einen integrierten OPC UA Server oder alternative Steuerungskomponenten, um Kenntnisse über die Vernetzung von Komponenten zu vermitteln.

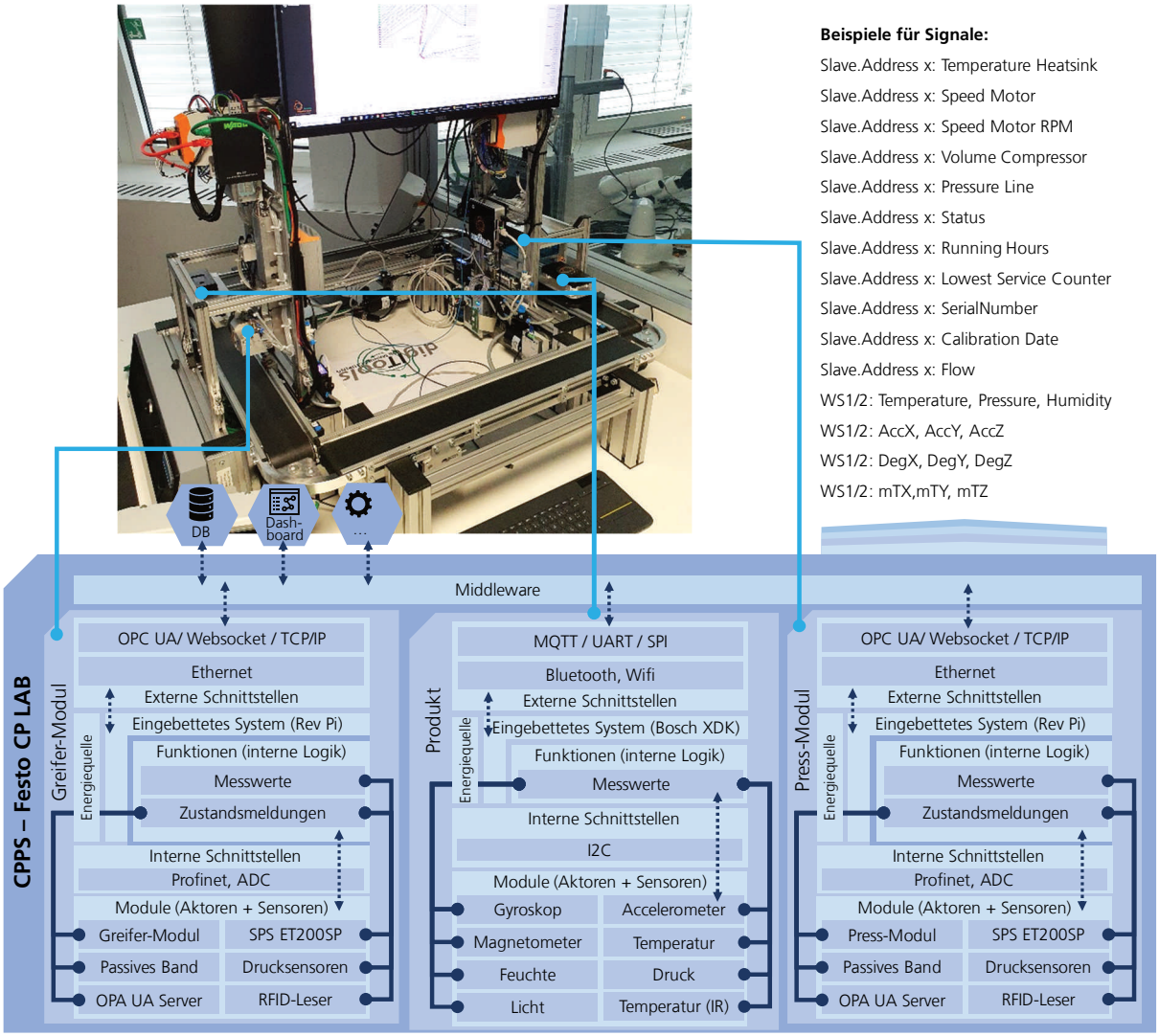


Abbildung 6.7 Darstellung Festo Didactic CP Lab Demonstrator

Der modulare und flexible Aufbau ermöglicht es verschiedene Szenarien abzubilden, vom einzelnen Palettentransfersystem mit integrierter Steuerung bis hin zur vernetzten Produktionsanlage mit Cloud-Diensten.

Der hier betrachtete Aufbau ist in Abbildung 6.7 als 3D-Rendering dargestellt und besteht aus zwei Hauptmodulen (Presse und Wende-Greifer), die zwei Werkstückträger in einer Umlaufband-Konfiguration bewegen. Das auf dem Werkstückträger gelagerte Produkt wird so zu den Bearbeitungsstationen transportiert. Die Produkte wurden im Rahmen dieser Arbeit zusätzlich mit einem eingebetteten System und Sensorik versehen und so zu intelligenten Produkten erweitert, um die hier diskutierten Ansätze zu erproben.

Die Anlage wird als Entwicklungsumgebung im CPS-Labor des Zentrums für Cyberphysische Systeme (ZCPS) am Fraunhofer IPA, zu Lehrzwecken und als Messe-Demonstrator eingesetzt. Hierzu werden multi-Protokoll-basierte (http/REST, Websocket, OPC UA, MQTT) Cloud-Integrationsszenarien mit der Virtual Fort Knox Research Plattform (siehe Anhang 2.4) dargestellt.

Die erfassten Daten werden unter anderem echtzeitnah in einer 3D-Visualisierung, in einem konfigurierbaren Dashboard und für die Entwicklung von Diensten genutzt, beispielsweise durch maschinelles Lernen unterstützte vorausschauende Wartung.

Tabelle 16 listet die aus den Anlagenkomponenten ableitbaren Merkmale.

Tabelle 16 Merkmale Festo CP Lab (in der vorliegenden Konfiguration)

Merkmal	Ausprägung/Anmerkung	Merkmalsklasse	Merkmalseigenschaften
Produktname	Formeller Name	Seins-Merkmal	statisch, einfach, künstlich
Geräte-nummer	Eindeutige Nummer	Seins-Merkmal	statisch, einfach, künstlich
Greifer-Modul	Greifer-Modul, Greifprozess, Prozesssteuerung	Besitzmerkmal Fähigkeits-Merkmal Zustands-Merkmal	statisch, komplex, natürlich statisch, einfach, natürlich dynamisch, einfach, natürlich
Press-Modul	Press-Modul, Press-Prozess, Prozesssteuerung	Besitz-Merkmal Seins-Merkmal Fähigkeits-Merkmal	statisch, komplex, natürlich statisch, einfach, natürlich dynamisch, einfach, natürlich
RFID-System	RFID-Sensorik RFID-Datenerfassung	Besitz-Merkmal Fähigkeits-Merkmal	statisch, komplex, natürlich statisch, einfach, natürlich
Revolution Pi Steuerung	RevPI-Hardware, Abfrage Systemdaten,	Besitz-Merkmal Fähigkeits-Merkmal	statisch, komplex, natürlich statisch, einfach, natürlich

	Hardware-Architektur, Betriebssystem, Speicher, CPU, CPU-Leistung, Systemtemperatur, Speicherleistung	Seins-Merkmal Seins-Merkmal Seins-Merkmal Seins-Merkmal Seins-Merkmal Seins-Merkmal Seins-Merkmal	statisch, einfach, natürlich statisch, einfach, natürlich statisch, einfach, natürlich statisch, einfach, natürlich dynamisch, einfach, natürlich dynamisch, einfach, natürlich dynamisch, einfach, natürlich
Revolution Pi I/O Modul	I/O-Modul, I/O-Modul, zusätzliche Werte, zusätzliche Werte	Besitz-Merkmal Struktur-Merkmal Fähigkeits-Merkmal Wert-Merkmal	statisch, komplex, natürlich statisch, komplex, natürlich statisch, einfach, natürlich dynamisch, einfach, natürlich
Drucksensor	Zusatz-Sensorhardware, Sensorhardware, Druckmessung, Durchfluss, Luftdruck	Besitz-Merkmal Seins-Merkmal Fähigkeits-Merkmal Wert-Merkmal Wert-Merkmal	statisch, komplex, natürlich statisch, einfach, natürlich statisch, einfach, künstlich dynamisch, komplex, künstlich dynamisch, einfach, natürlich
Werkstück-träger RFID	Prozessschritt Standort	Zustands-Merkmal Kontext-Merkmal	Ereignis-bezogen, Zeit-bezogen Ereignis-bezogen, Zeit-bezogen
Produkt-Sensorik	Temperatur Luftdruck Relative Feuchte Lichtintensität, Lichtintensität, 3-Achs-Beschleunigung, 3-Achs-Beschleunigung, 3-Achs-Magnetfeld, 3-Achs-Magnetfeld, 3-Achs-Orientierung, 3-Achs-Orientierung	Wert-Merkmal Wert-Merkmal Wert-Merkmal Wert-Merkmal Kontext-Merkmal Wert-Merkmal Kontext-Merkmal Wert-Merkmal Kontext-Merkmal Wert-Merkmal Kontext-Merkmal	dynamisch, einfach, natürlich dynamisch, einfach, natürlich dynamisch, einfach, natürlich dynamisch, einfach, natürlich dynamisch, komplex, natürlich dynamisch, einfach, natürlich dynamisch, komplex, natürlich dynamisch, einfach, natürlich dynamisch, komplex, natürlich dynamisch, einfach, natürlich dynamisch, komplex, natürlich
Taktzeiten	Zeitstempel zwischen Prozessschritten	Fähigkeits-Merkmal Wert-Merkmal	statisch, einfach, künstlich dynamisch, einfach, natürlich
Förderband-geschwindig-keit	Zeitdifferenz zwischen Erkennungspunkten	Kontext-Merkmal Wert-Merkmal	Ereignis-bezogen, Zeit-bezogen dynamisch, einfach, natürlich
Notaus-Schalter	Notaus-Signal	Wert-Merkmal	dynamisch, einfach, natürlich
Stückzähler	Seit Einschaltung / gesamt produzierte Teile, gesamt produzierte Teile	Wert-Merkmal, Wert-Merkmal, Seins-Merkmal,	dynamisch, einfach, natürlich dynamisch, einfach, natürlich dynamisch, einfach, natürlich
Zustände / Fehlermel-dungen	RFID Prozessschritt Prozessschritt Ort Fehler-Ereignis Fehler-Ereignis Ursprung	Ereignis-Merkmal Kontext-Merkmal Ereignis-Merkmal Kontext-Merkmal	statisch, einfach, künstlich dynamisch, einfach, natürlich dynamisch, einfach, natürlich dynamisch, einfach, natürlich
OPC UA Server	OPC UA Server OPC UA Datenmodell	Besitzmerkmal Fähigkeitsmerkmal	statisch, komplex, natürlich statisch, einfach, natürlich
Uhrzeit (lokal)	Referenz und zeitlicher Bezug von Ereignissen	Kontext-Merkmal	dynamisch, komplex, natürlich, Zeit-bezogen (alle Ereignisse)

Jedes Modul dieses Aufbaus verfügt über eine eigene „CPS-Steuereinheit“ in Form einer Revolution Pi Steuerung, die unabhängig ihre Komponenten ansteuert. Daher kann jedes

Modul auch als eigenständiges CPS betrachtet werden, das seinen funktionalen Zweck als CPPS jedoch nur im Verbund erfüllen kann. Zudem sind die Produkte intelligent und verfügen über ein Eingebettetes System, welches mit mehreren Sensoren versetzt ist. Der Werkstückträger verfügt über einen RFID-Chip und kann als passives CPS betrachtet werden. Grundsätzlich muss also jedes CPS-Modul für sich selbst authentifiziert werden, da aus der Ferne initial nicht erkennbar ist ob eine Komponente, die sich am übergeordneten System anmelden will, auch tatsächlich die ist, die sie vorgibt zu sein.

Die vereinfachte Selbstbeschreibung in Abbildung 6.8 fasst die beiden Hauptmodule des Aufbaus zusammen.

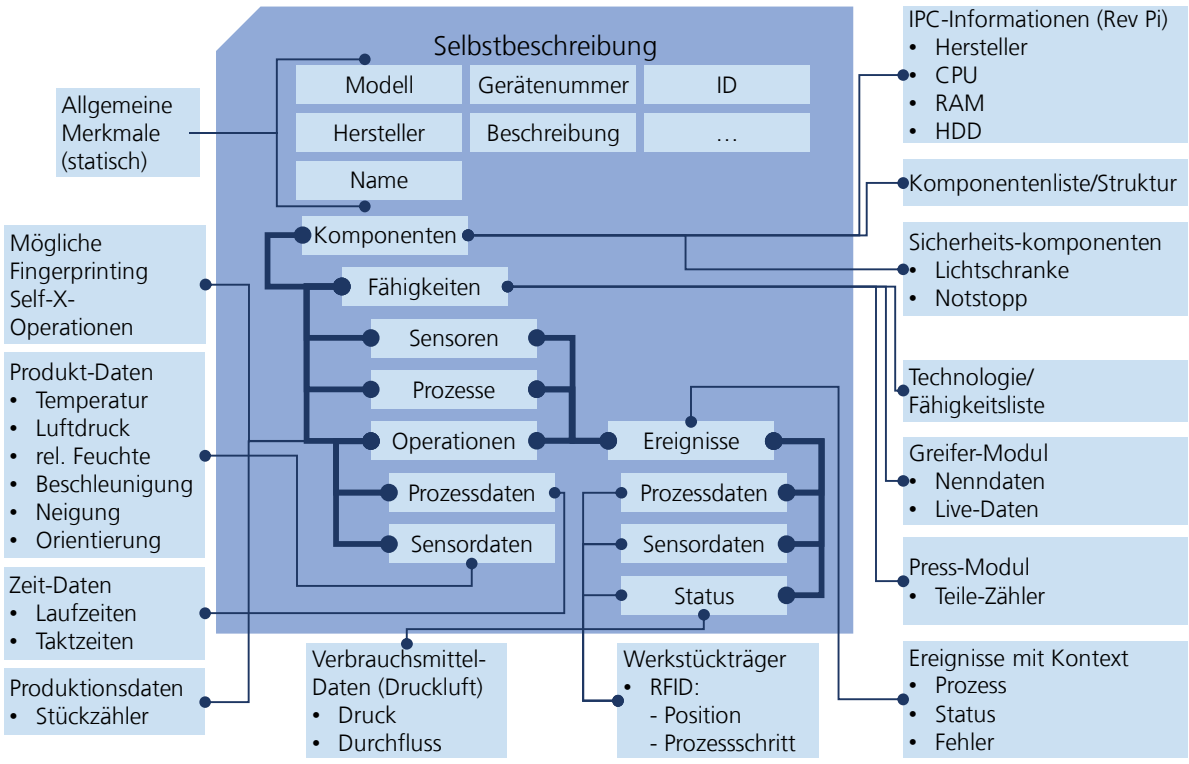


Abbildung 6.8 Vereinfachte CPPS-Selbstbeschreibung für Festo Didactic CP Lab

Der in diesem Fallbeispiel abgebildete Prozess findet zyklisch und nur in Wechselwirkung mit den Anlagen-Modulen statt. Daher bietet dieser CPPS-Verbund die Möglichkeit Merkmale zu nutzen, die einen kontextuellen Verhaltenszusammenhang besitzen, also z.B.

Prozessdaten verschiedener Komponenten nach einem bestimmten Verhaltensmuster und weitere betriebliche Daten miteinander zu korrelieren und so aggregierte Kontext-Merkmale zu bilden. Da die CP Lab Anlage über moderne offene IoT-fähige Komponenten verfügt und die Hauptsteuereinheiten des CPPS so eine einfache Umsetzung des beschriebenen Konzepts ermöglichen, dient sie als Versuchsaufbau für diese Arbeit. Das Demonstrations- und Testszenario hierzu wird in Kapitel 6 weiter im Detail beschrieben.

6.2 Versuchsaufbau

Die Validierung des Konzepts mittels der prototypischen Implementierung wird anhand verschiedener Szenarien, die sich auf unterschiedliche Aspekte eines CPPS fokussieren, durchgeführt. Hierfür wird in einem ersten Versuchsaufbau dargestellt, wie verschiedene eingebettete Systeme anhand ihrer statischen Selbstbeschreibungsmerkmale und der daraus abgeleiteten dynamischen Merkmale unterschieden, identifiziert und authentifiziert werden können. Ein zweiter Versuchsaufbau besteht aus dem im Abschnitt 6.1.4 vorgestellten Fallbeispiel eines Festo Didactic CP Lab. An diesem komplexen Szenario wird dargestellt, wie mittels einer Korrelation verschiedener Verhaltensmerkmale eines CPPS eine kontinuierliche Authentifizierung mittels konstruierter aggregierter Merkmale durchgeführt werden kann.

6.2.1 Identifikation und Authentifizierung von eingebetteten Systemen

Eingebettete Systeme bilden das Herz und Gehirn von CPPS. Daher soll zunächst gezeigt werden, wie diese elementare Gemeinsamkeit genutzt werden kann, um CPPS allein aufgrund ihrer intrinsischen Merkmale dieser Komponenten zu identifizieren und zu authentifizieren.

Die prinzipielle Funktionsweise der Identifikation mittels statischer Merkmale ist in Abschnitt 4.4.4 beschrieben. Die Identifikation wird durch einen Abgleich der von einem CPS

gesendeten Selbstbeschreibung mit den hinterlegten Templates durchgeführt, die im hybriden Fingerabdruck hinterlegt wurden. Der Versuchsaufbau hierzu besteht aus einer Reihe verschiedener eingebetteter Systeme in Form von Embedded-Boards verschiedener Hersteller. Zudem werden einige Systeme verschiedener Hersteller eingesetzt, die gleiche oder vergleichbare Hardware-Komponenten verwenden. So verbaut die Firma Kunbus in Revolution Pi-Steuerungen die gleichen Chipsätze in Form von Raspberry Pi Compute Modulen, wie sie in einem herkömmlichen Raspberry Pi Board zu finden sind. Sämtliche Systeme nutzen Linux als Betriebssystem, da dieses in verschiedenen Ausprägungen schon seit Jahren immer breitere Verwendung in industriellen Anwendungen und IoT-Komponenten findet. Der Versuchsaufbau hierfür ist als Prüfstand realisiert, der neben der Erprobung des hier vorgestellten Verfahrens auch dazu dient, verschiedene Cyber-Sicherheit-Anwendungen wie beispielsweise die Überwachung von Datenverkehrs-Mustern im Netzwerk und weitere Fingerprinting-Methoden wie sie in Abschnitt 4.2.2.1 beschrieben sind zu erforschen.

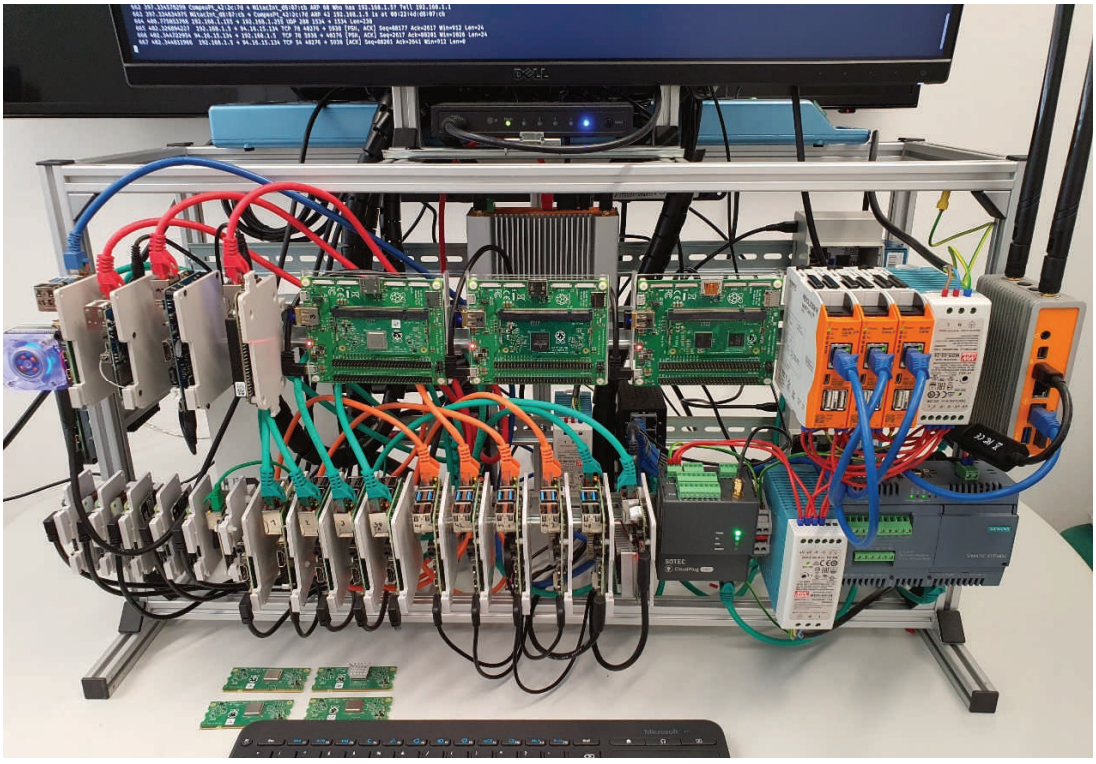


Abbildung 6.9 Versuchsaufbau für CPS-Prüfstand

Abbildung 6.9 zeigt ein Foto des Prüfstands, um einen Eindruck zu vermitteln, wie eine Auswahl verschiedener Geräte aussieht, die heute schon als CPS zum Einsatz kommen und die sich einerseits funktional ähnlich sind, sich aber andererseits in zahlreichen Merkmalen stark unterscheiden. Eine detaillierte Übersicht der für den Prüfstand verbauten Komponenten inklusive ihrer technischen Kenndaten kann Anhang 6 entnommen werden.

Einige der eingebetteten Systeme sind beispielsweise nur mit speziell angepassten Varianten eines jeweiligen Betriebssystems funktionsfähig, was die spezifische Betriebssystemversion beispielsweise zu einem statischen Merkmal des CPS macht. Die interne Logik für die Versuchsdurchführung ist in Python implementiert, da Python weite Verbreitung findet, einfach auf eingebetteten Linux-Systemen auszuführen ist und sehr viele Möglichkeiten bietet Merkmale des Host-Geräts und des Betriebssystems auszulesen. Prinzipiell könnte auch jede beliebige andere moderne Programmier-Hochsprache, wie z. B. Node.js oder C++ genutzt werden, allerdings hat sich Python während der Implementierung als einfach und effizient handhabbar erwiesen. Auch die Programmiersprache, die zur Implementierung gewählt wurde, kann als Merkmal abgefragt werden. Im Fall von Python kann auch die genaue Version, die zum Einsatz kommt, abgefragt werden, da hier oft noch Python 2 neben Python 3 und den jeweiligen Unterversionen eingesetzt werden können.

Abbildung 6.10 zeigt das Modell eines Raspberry Pi 4 (Pi4), eine Modellreihe des Raspberry Pi, und soll an diesem Beispiel eine Auswahl spezifischer Kenndaten des Geräts darstellen, die als Merkmale herangezogen werden können. Der Pi4 ist beispielsweise in vier Varianten verfügbar, die sich nur durch die Größe des verbauten Arbeitsspeichers unterscheiden. Sämtliche weiteren Komponenten sind identisch. Eine Unterscheidung ist nur noch über die in der Hardware eingebetteten MAC-Adressen der Ethernet- und Wifi-Schnittstellen möglich. Raspberry Pi Entwicklungsboards verfügen über keine eigenen Festplattenspeicher bzw. Speicher.

Der Speicher wird über microSD-Karten bereitgestellt, die in einen Speicherkarten-Slot eingeführt werden und das Betriebssystem beinhalten. Speicherkarten sind von zahlreichen Herstellern in verschiedenen Größen und Leistungsklassen verfügbar.

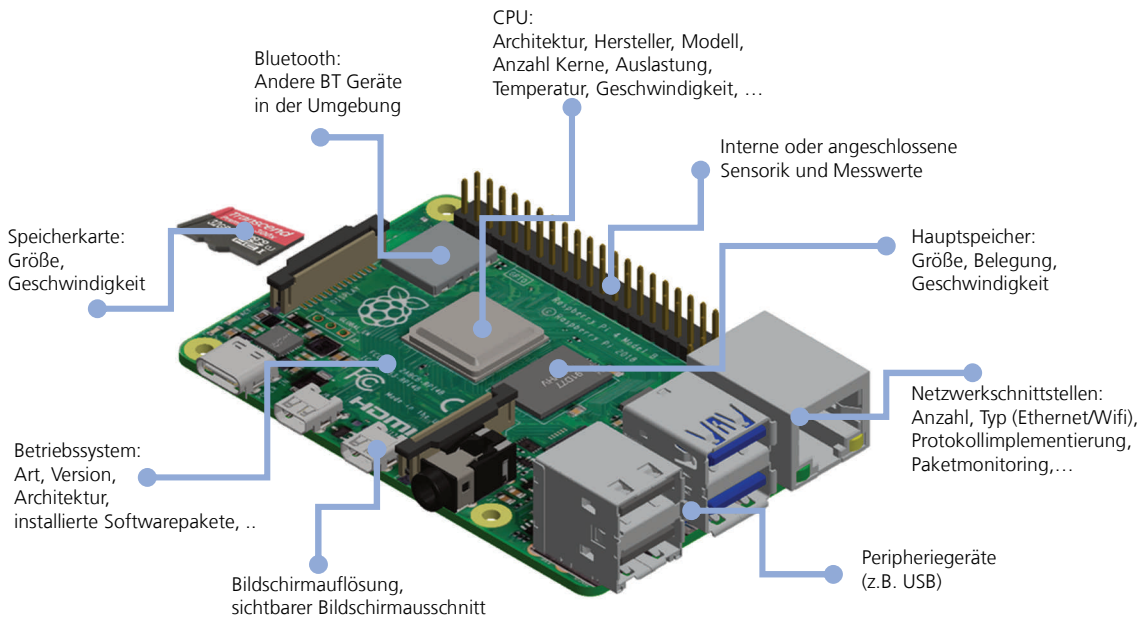


Abbildung 6.10 Merkmale eines eingebetteten Systems bzw. CPS am Beispiel des Raspberry Pi 4

Zwar findet man auf der Modell-Bezeichnung des jeweiligen Herstellers die standardisierten Größenangaben, bei aktuellen Speicherkarten beispielsweise 4, 8, 16, 32, 64, 128, 256, 400, 512 GB und 1 TB, allerdings unterscheiden sich die jeweiligen Speicherchips des jeweiligen Herstellers darin, welche Speichergröße in Bytes tatsächlich verfügbar und dem Betriebssystem zurückgemeldet wird. Hierdurch wird die aktuell im Gerät befindliche Speicherkarte zu einem natürlichen Merkmal des CPS, da die Größe durch den Herstellungsprozess des Herstellers bestimmt und nicht willkürlich festgelegt wird. Die aus diesen System-Informationen erfassbaren statischen Merkmale sind in einem Beispiel in Anhang 7.1 dargestellt.

Die für industrielle Anwendungen verwendete Variante des Raspberry als Compute-Modul, kann ebenfalls mit SD-Karte betrieben werden, wird allerdings für produktive Anwendungen mit einem fest verbauten NAND-Flashspeicher verwendet, der im Gegensatz zu SD-Karten weitaus bessere Leistungsdaten in Bezug auf Schreib- und Leseraten aufweist. Dieser Umstand lässt sich für eine Erfassung dynamischer Merkmale nutzen und erlaubt auch eine Unterscheidung der Modellvarianten der Raspberry Pi Compute-Module des Typs 1, 3 und 3+ (siehe Anhang 7.2).

Der Einfluss der Art und Weise, in der die jeweiligen Module und Boards verbaut sind, lässt sich vermutlich ebenfalls über bestimmte Merkmale, insbesondere die Temperatur des Prozessors ermitteln. Daher wurden die Boards willkürlich mit unterschiedlich leistungsfähigen Kühllösungen versehen, die jeweils die Temperatur eines baugleichen Boards charakteristisch beeinflusst (siehe Anhang 7.4). Die weiteren verwendeten bauähnlichen Entwicklungsboards verschiedener Hersteller, die zwar funktional identisch sind, sich jedoch in ihren verwendeten Bauteilen, wie z. B. dem Prozessor und somit auch ihrer Leistung (siehe Anhang 7.3), unterscheiden, zeigen den Einfluss des Einsatzes dieser verschiedenartigen Bauelemente und die daraus erkennbare Charakteristik. Zusätzlich sind beliebige Sensoren als Bestandteile von CPPS verwendbar (siehe Anhang 7.1). Hier können entweder direkte sensorbezogene Merkmale oder Sensorwerte mit Kontext aus der Umwelt gekoppelt werden.

6.2.2 Identifikation und Authentifizierung von CPPS im komplexen Szenario

Nachdem im vorherigen Abschnitt beschrieben wurde, wie beliebige CPS nur aufgrund ihrer intrinsischen Merkmale identifiziert und authentifiziert werden können, soll dieses Konzept nun auf CPPS ausgeweitet werden. Für die in CPPS verbauten Komponenten sind dieselben Prüfverfahren geeignet, zusätzlich können aber die betrieblichen Daten und weitere Kontext-Daten für die Merkmalsgewinnung eingesetzt werden, um den Merkmalsraum zu erweitern und eine kontinuierliche Authentifizierung zu realisieren, die auf der Erfassung der betrieblichen Daten basiert. Hierzu wird ein etwas komplexeres Szenario in einem Versuchsaufbau realisiert. Das in Abschnitt 6.1.4 vorgestellte Fallbeispiel 4 wird hierfür in einem Aufbau eines Festo CP Lab umgesetzt.

Das Festo CP Lab besteht aus zwei aktiven Modulen, die über passive Förderbänder miteinander verbunden sind und bildet so ein zirkuläres Förderband, auf welchem sich zwei Werkstückträger bewegen (Abbildung 6.11, links). Die Aktoren und Sensoren der Module werden von einer Siemens S7-1200 SPS angesteuert, die über einen integrierten OPC UA

Server verfügt. Dieser OPC UA Server erlaubt Zugriff auf die SPS Daten. Das zentrale eingebettete System des Festo CP Labs bildet pro Modul jeweils ein Revolution Pi der Firma Kunbus. Für diese lassen sich dieselben Prüfverfahren zur Identifikation und Authentifizierung verwenden, wie sie im vorherigen Abschnitt 6.2.1 vorgestellt wurden. Prinzipiell lässt sich sagen, dass es sich um zwei CPPS handelt, die im Verbund eine CPPS-Einheit bilden.

Die zwei Werkstückträger transportierten zwei Produkte, die im jeweiligen aktiven Modul in Form einer Presse und einem Greifer gepresst bzw. gewendet werden (Abbildung 6.11, rechts unten).

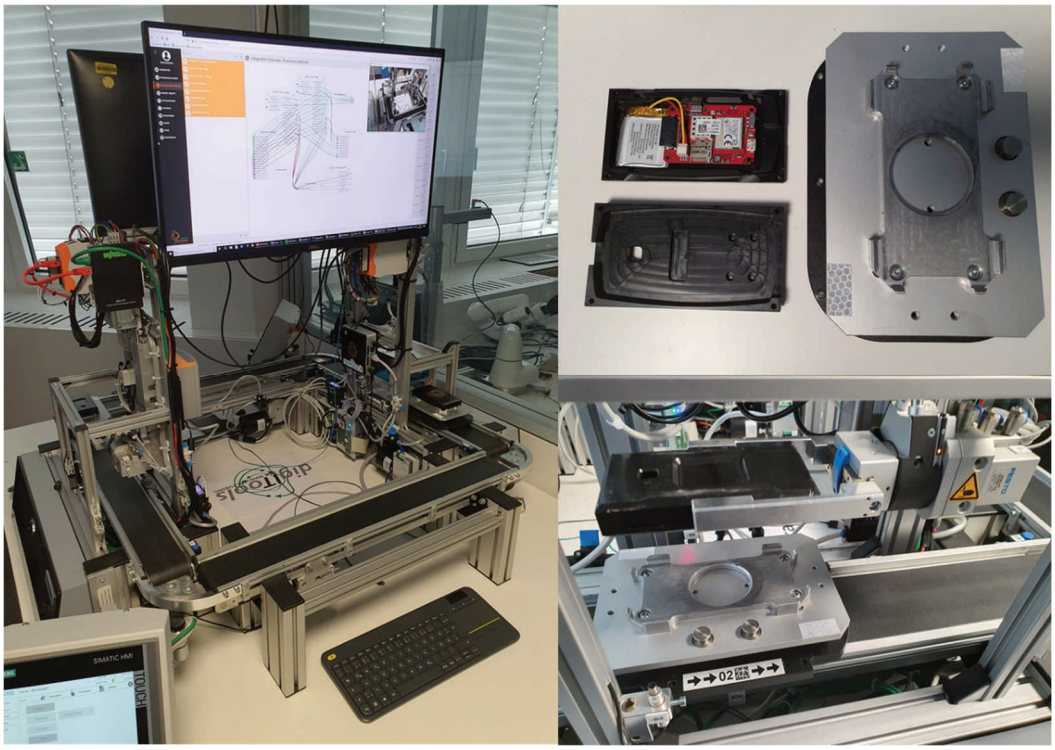


Abbildung 6.11 Aufbau Festo CP Lab CPPS

Der Prozessablauf wird durch einen im Werkstückträger befindlichen RFID-Chip gesteuert und kontrolliert, der den jeweiligen aktuellen und nächsten Bearbeitungsschritt und Zustand persistiert bzw. über RFID-Leser an der Anlage an diese weitergibt. Die Produkte

wurden mit zusätzlicher Sensorik ausgestattet (Abbildung 6.11, rechts oben), die zusätzliche betriebliche Daten in Form von Prozess- bzw. Zustandsdaten und weiteren Messwerten erzeugen, die währen dem Prozess entstehen. Dies wurde durch die Integration von Sensorboards in die Produkte bewerkstelligt. Diese Daten werden an eine Datenbank weitervermittelt, die stellvertretend für die Datenbank eines BDE-Dienstes bzw. eines BDE Moduls eines MES fungiert und sämtliche betrieblichen Daten des Festo CP Lab persistiert, sodass diese für eine Authentifizierung verwendet werden können.

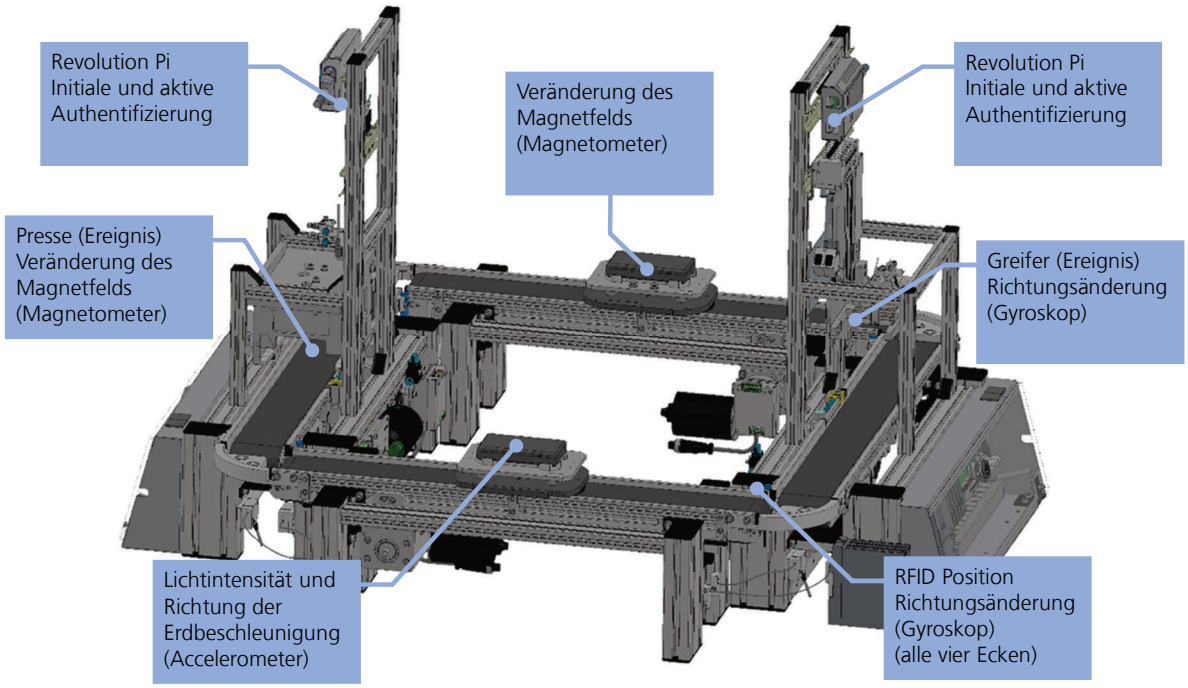


Abbildung 6.12 Konzeptbild für komplexes Testszenario mit Festo CP Lab

Die zwei Werkstückträger transportieren in diesem Beispiel die Produkte in einer Endlosschleife zwischen zwei Bearbeitungsstationen. Hier wird also ein einfacher Prozess abgebildet, der es erlaubt die Daten der Anlagenmodule und die Daten der Werkstückträger bzw. Produkte miteinander zu korrelieren. So können eindeutige Verhaltensmerkmale mit kontextuellem Schwerpunkt bestimmt werden.

6.3 Versuchsdurchführung

Da es sich bei der Implementierung um einen prototypischen Aufbau handelt, sind einige der Prozessschritte nicht vollständig automatisiert und erfordern manuelle Eingriffe. Die Erstanmeldung und die Erstellung des hybriden Fingerabdrucks ist hier besonders auf die Eingabe von Informationen angewiesen, die das explizite und implizite Wissen über das CPPS bzw. die Prozesse beinhalten. Sind diese Informationen erstmals formalisiert und strukturiert erfasst, können die weiteren Schritte weitestgehend automatisiert werden.

6.3.1 Erstanmeldung

Die Erstanmeldung folgt bei allen CPPS und den zugehörigen Diensten demselben Ablaufschema und ist in Abbildung 6.13 dargestellt:

- Das CPPS verbindet sich mit der Integrations-Middleware (MSB) und sendet eine Registrierungsnachricht, die die Selbstbeschreibung des CPPS beinhaltet.
- Die Selbstbeschreibung beinhaltet Metadaten, die zusätzliche Informationen zu den Eigenschaften und Fähigkeiten des CPPS beinhalten
- Aus dem Metadaten-Management wird ein Gerüst für den hybriden Fingerabdruck extrahiert, der aus den Grundinformationen der Selbstbeschreibung besteht und durch zusätzliche Template-Daten zu den zu prüfenden Merkmalen ergänzt wird.

Die Metadaten der Selbstbeschreibung werden verwendet, um die Selbstbeschreibungsmerkmale zu markieren, die zur Authentifizierung als Authentifizierungsfaktoren verwendet werden sollen und welchen Merkmalstyp sie darstellen. Die statischen Selbstbeschreibungsmerkmale entsprechen überwiegend Seins- und Wissensmerkmalen. Zusätzlich werden die Merkmale markiert, die für die aktive und kontinuierliche Authentifizierung verwendet werden. Dies sind dynamische Merkmale, die eine direkte Verbindung zu den Fähigkeitsmerkmalen und kontextbasierten Merkmalen haben. Hierfür verfügt jedes CPPS über Operationen, die als Callback-Funktionen über den MSB aufgerufen werden können und Response-Events mit den Antwortdaten liefern.

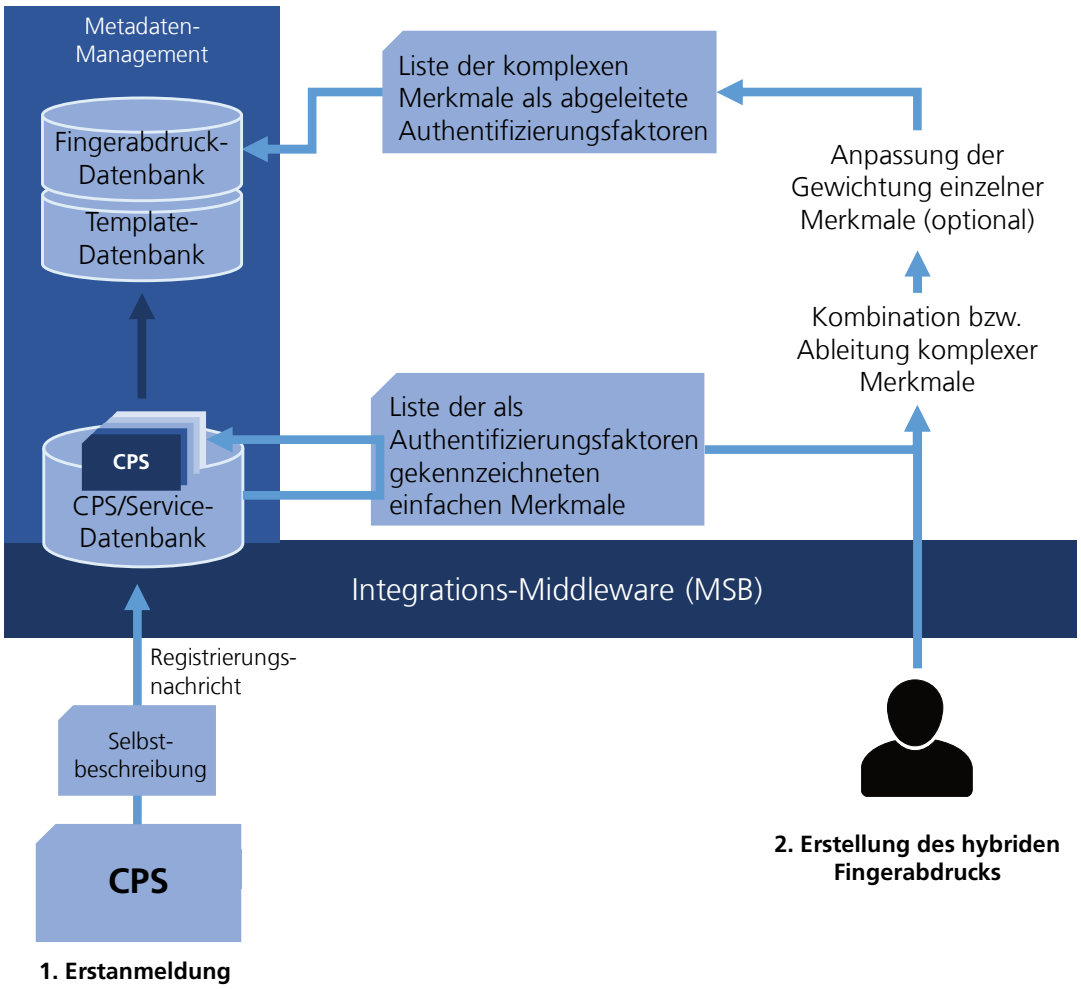


Abbildung 6.13 Übersicht der Anmeldeprozedur

Gewöhnliche Events haben eine Beziehung zu kontextbezogenen Prozessen und Interaktionen von CPPS bzw. ihren Komponenten und werden im Rahmen der kontinuierlichen Authentifizierung überwacht, jedoch nicht aktiv angesprochen. Abbildung 6.14 zeigt die Benutzeroberfläche des MSB, die erweitert wurde, um die Metadaten der Selbstbeschreibung darzustellen. Ein Anwender kann hier einzelne Merkmale gezielt aktivieren, die Merkmalseigenschaften und ihre Gewichtung anpassen (Abbildung 6.15). Zudem kann festgelegt werden, in welcher Phase der Merkmalsprüfung das jeweilige Merkmale geprüft wird (vgl. Abschnitt 5.1.2).

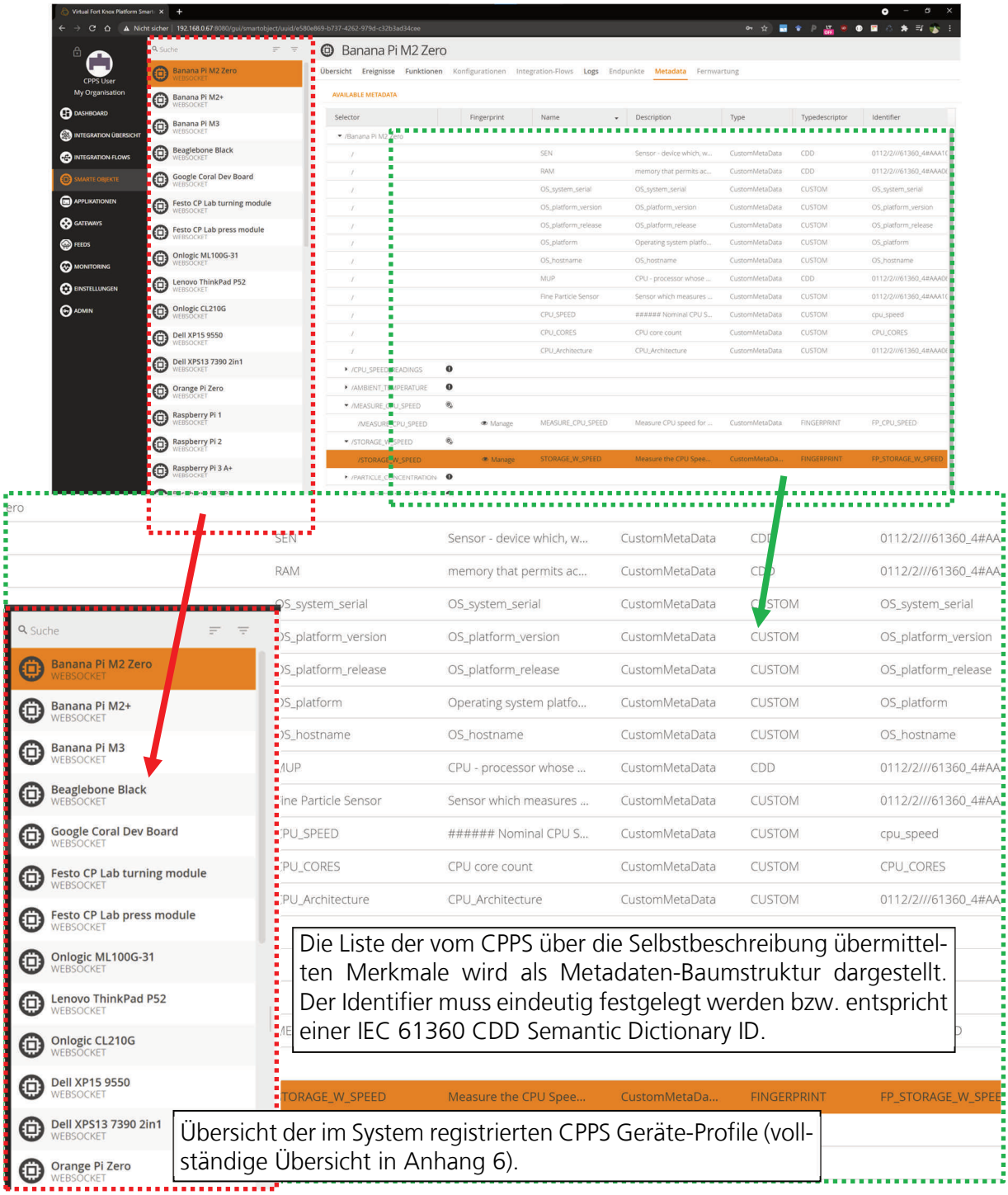
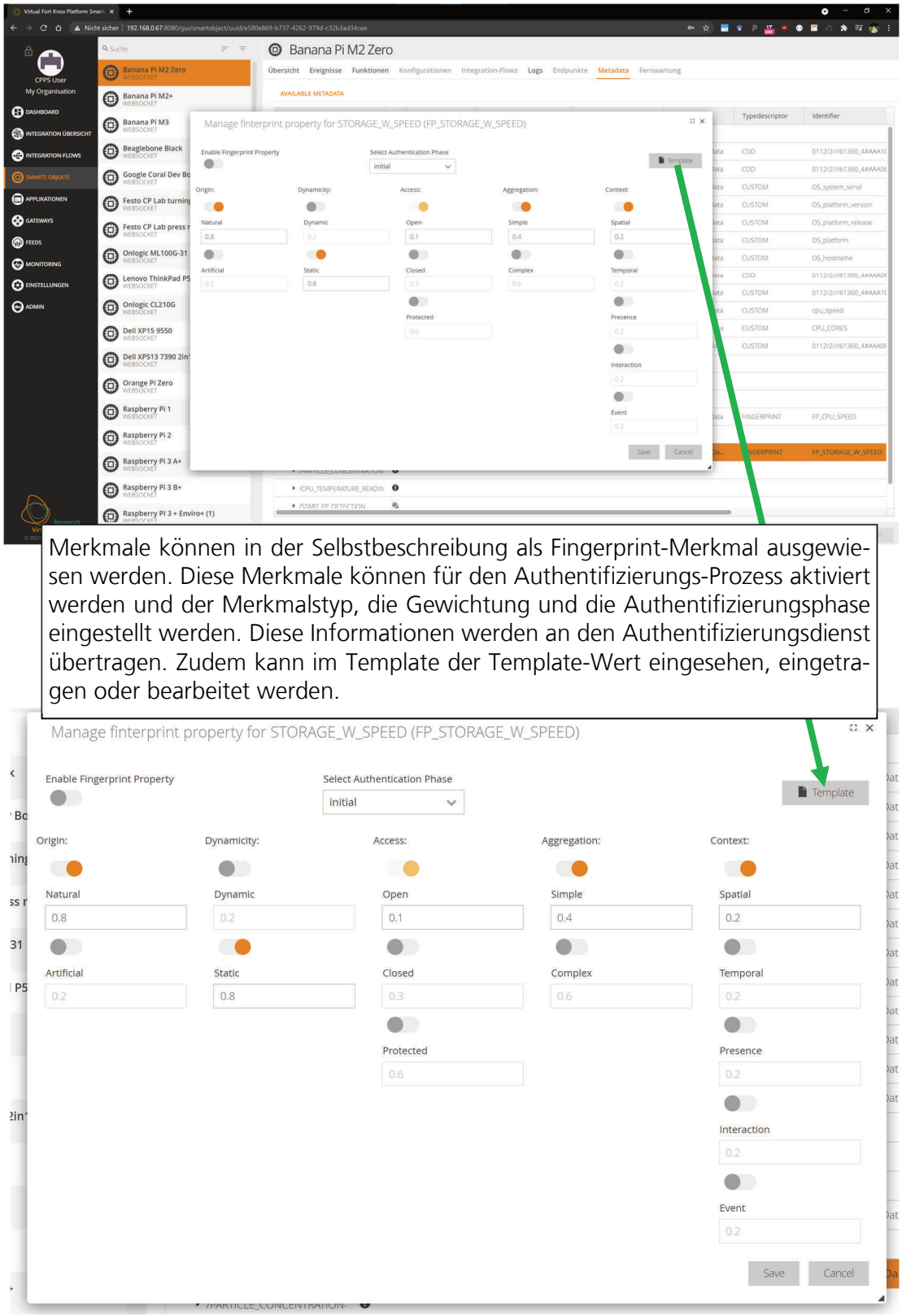


Abbildung 6.14 MSB-Visualisierung von Selbstbeschreibung und Metadaten von CPPS-Komponenten



Merkmale können in der Selbstbeschreibung als Fingerprint-Merkmal ausgewiesen werden. Diese Merkmale können für den Authentifizierungs-Prozess aktiviert werden und der Merkmalstyp, die Gewichtung und die Authentifizierungsphase eingestellt werden. Diese Informationen werden an den Authentifizierungsdienst übertragen. Zudem kann im Template der Template-Wert eingesehen, eingetragen oder bearbeitet werden.

Abbildung 6.15 Verwaltungsfunktion für ein Selbstbeschreibungsmerkmal

Die Template-Daten für ein Merkmal können wie in Abbildung 6-16 eingesehen und bearbeitet werden. Template Daten können auch gezielt vom CPPS abgefragt werden, wenn dieses über eine Funktion zur Abfrage des aktiven Merkmals verfügt.

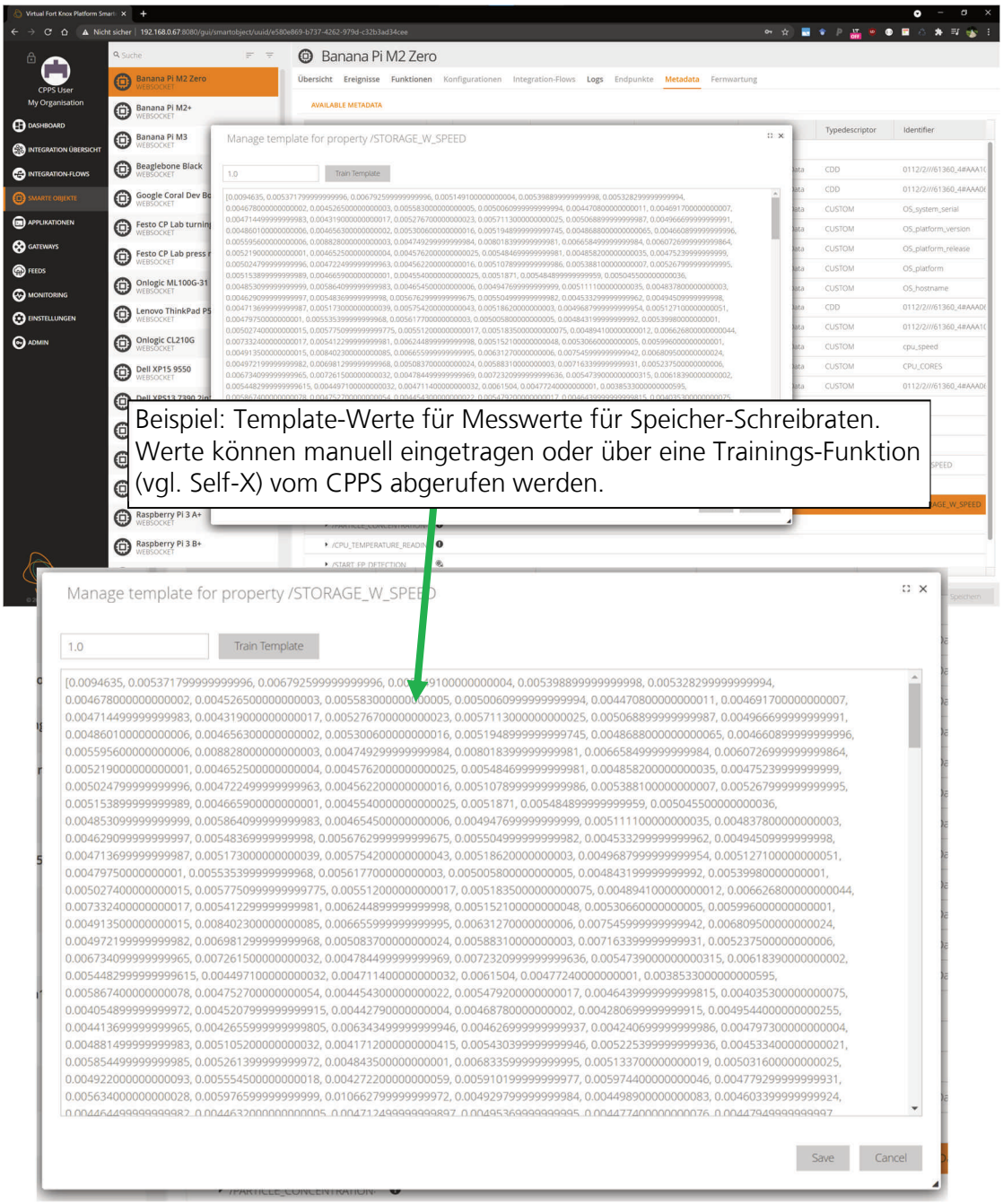


Abbildung 6.16 Einstellen eines Template-Werts für ein Merkmal

Grundsätzlich wird dieser Prozess automatisiert für jedes Merkmal durchgeführt, da der manuelle Aufwand mit steigender Zahl von Merkmalen entsprechend ansteigt. Jedoch besteht die Möglichkeit Template-Daten gezielt zu bearbeiten.

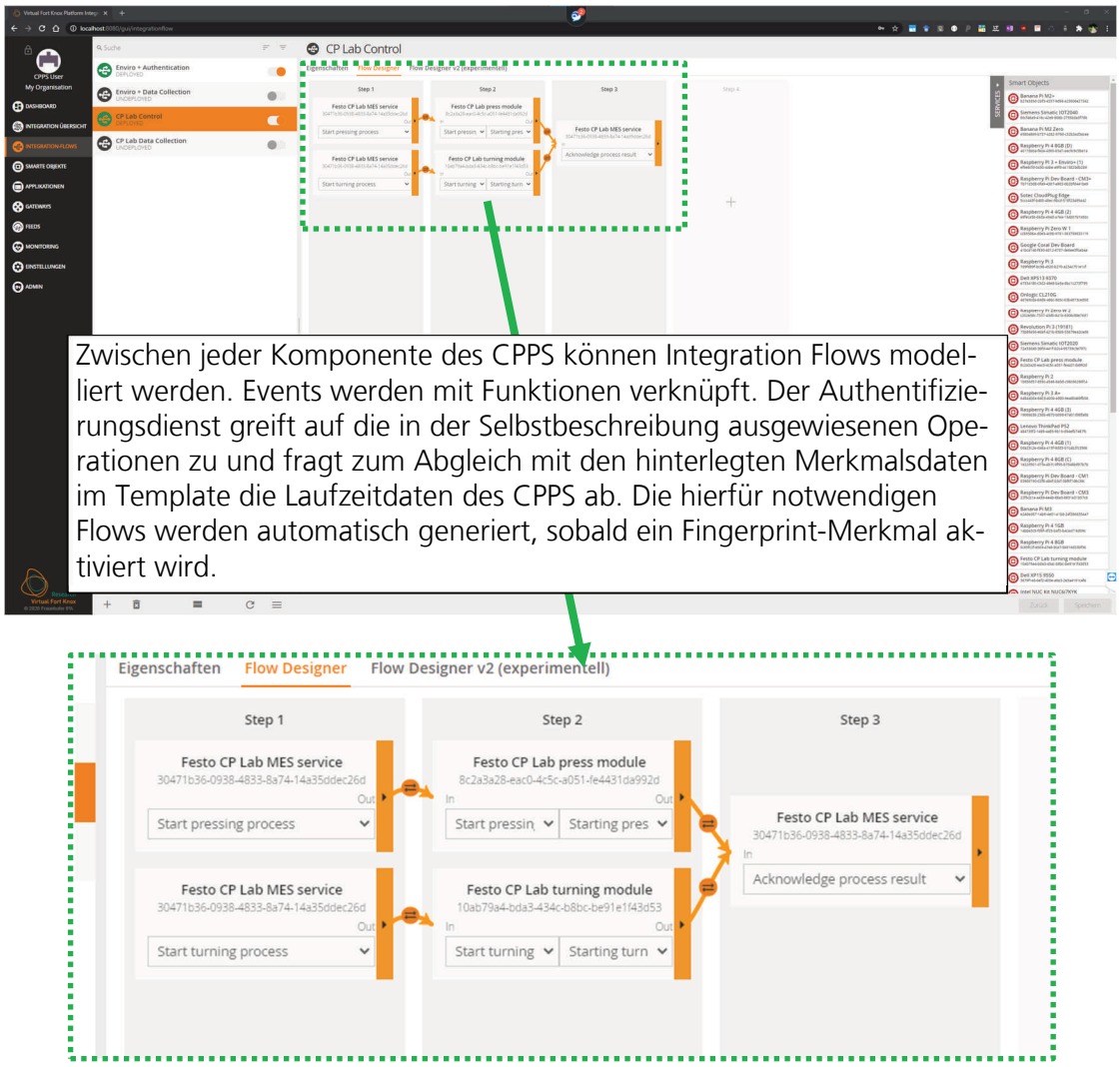


Abbildung 6.17 MSB-Benutzeroberfläche zur Modellierung von Integration Flows und Beziehungen zwischen CPPS-Komponenten

Zudem können wie in Abbildung 6.17 dargestellt die Integration Flows (kontrollierte Informationsflüsse mit Mapping zur Datenintegration) zwischen CPPS-Komponenten und Diensten modelliert bzw. eingesehen werden. In diesem Beispiel werden unter anderem

die Steuerungs-Ereignisse für das Festo CP Lab als Ereignisse im MSB erfasst und können so als Kontext-Merkmale genutzt werden. Diese Information Flows werden ebenfalls automatisch generiert und können bei Bedarf manuell angepasst werden.

Da die Anzahl der realen CPPS, die im Versuchsaufbau eingesetzt werden, aus praktischen Gründen begrenzt ist, können zusätzliche CPPS mittels Python-Skripten simuliert werden. Hierfür werden „generische" CPPS-Selbstbeschreibungen generiert und der Template-Datenbank hinzugefügt. Zusätzlich können aktive CPPS emuliert werden, die ein aktives CPPS-Verhalten nachbilden und Software-generierte Werte für dynamische Merkmale liefern.

6.3.2 Identifikation und initiale Authentifizierung

Die Identifikation findet über einen Abgleich der spezifischen Selbstbeschreibungs-merkmale eines jeden CPPS statt und ist in Abbildung 6.18 dargestellt. Hierfür übermittelt das CPPS seine Selbstbeschreibung an den MSB. Dabei werden die offenen Merkmale für eine Identifikation mittels der vorhandenen Templates herangezogen. Die geschlossenen bzw. geschützten Merkmale werden zusätzlich mit den im hybriden Fingerabdruck hinterlegten Merkmalen abgeglichen.

Die Implementierte Lösung nutzt grundsätzlich Selbstbeschreibungsdaten für Smarte Objekte und Applikationen (Dienste) (vgl. Abschnitt 4.4.1).

Der Authentifizierungsdienst und die Prüfdienste für Merkmale übermitteln ebenfalls eine Selbstbeschreibung. Prüfdienste beispielsweise übermitteln ein Metadatum mit dem Wert „verification_service", das diesen Dienst so im System als Prüfdienst kennzeichnet. Zudem weisen Prüfdienste über ihre Metadaten bzw. Merkmals-Identifier aus, welche Merkmale sie prüfen können.

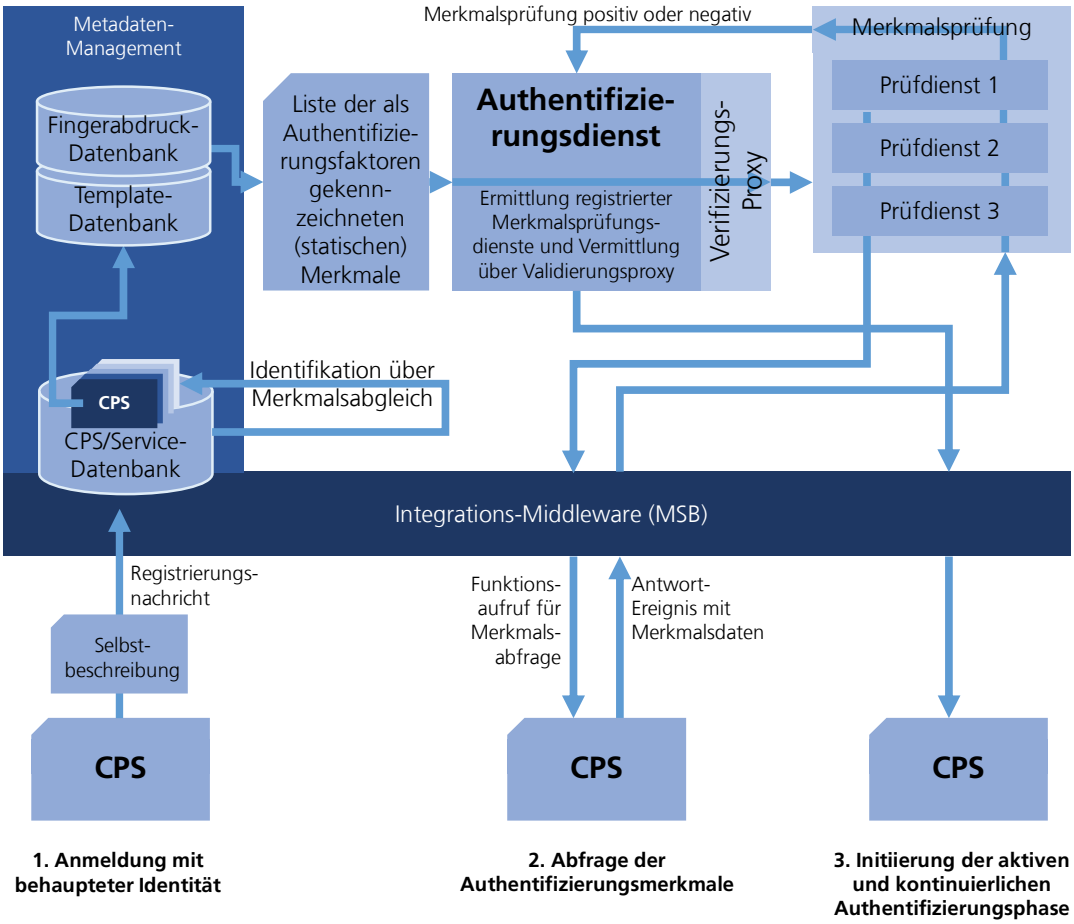


Abbildung 6.18 Prüfablauf für CPPS Identifikation und initiale Authentifizierung

Der Abgleich der einzelnen Merkmale findet durch einen Vergleich der Strukturen und Schlüsselwerte der Selbstbeschreibungsdaten statt, die als JSON-Struktur hinterlegt wurden. Abbildung 6.19 zeigt die Schritte der Identifikationsphase.

1. Das CPS schickt eine Selbstbeschreibung.
2. Die Selbstbeschreibung wird mit den Selbstbeschreibungen der registrierten bzw. bekannten Entitäten verglichen.
3. Wenn eine Übereinstimmung festgestellt wird, gilt die Identifikation als erfolgreich und die Identifikationsphase ist abgeschlossen.

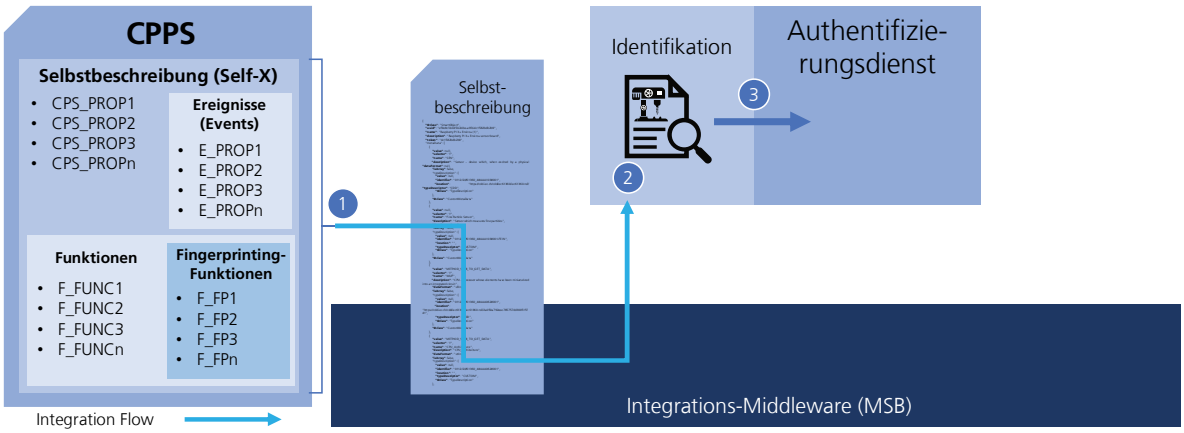


Abbildung 6.19 Schritte der CPPS-Identifikation

Die Identifikation wurde als Teilfunktion des Authentifizierungsdienstes implementiert und wird über einen einfachen Abgleich der Merkmalsfelder des Selbstbeschreibungsobjekts durchgeführt. Merkmalsbasierte Suchstrategien können jedoch beliebig komplex implementiert werden. Im Fall dieser Implementierung wird eine sukzessive Abfrage der Felder nach einem festgelegten Muster durchgeführt. Dies ist keine effektive Methode einer Identifikation auf Basis der Merkmale, jedoch ist die optimale Strategie zur Suche und Eingrenzung über eine Typisierung nicht Betrachtungsgegenstand dieser Arbeit.

Abbildung 6.20 zeigt den Ablauf der initialen Authentifizierungsphase für ein Merkmal. Dieser Ablauf wiederholt sich für jedes Merkmal, für das ein Prüfdienst vorhanden ist und kann parallelisiert werden.

Bevor eine Prüfung eines Merkmals initialisiert wird, prüft der Authentifizierungsdienst ob passende Prüfdienste registriert und aktiv sind. Wie zu Beginn dieses Abschnitts beschrieben, übermittelt jeder Prüfdienst eine Selbstbeschreibung und gibt Auskunft über die prüfbaren Merkmale. Werden hier Übereinstimmungen gefunden, so generiert der Authentifizierungsdienst alle notwendigen Information Flows am MSB, die ein jeweiliges Event mit Merkmalsdaten mit der Prüffunktion eines Prüfdienstes verknüpfen. Merkmale bestehen im Fall der initialen Authentifizierung aus überwiegend einfachen und statischen Merkmalen. Dies sind beispielsweise Datentypen vom Typ String oder JSON-Strukturen. Prüfdienste, deren Prüfstrategie also beispielsweise daraus besteht, die Gleichheit oder

Ähnlichkeit von String-Werten zu vergleichen, können für mehrere Merkmale verwendet werden, deren Datentyp bzw. Werte einem jeweiligen Datentyp entsprechen. Die Prüfung findet zwischen dem zur Prüfung vorgelegten Wert und dem Template-Wert statt. Diese müssen typengleich sein, sonst ist eine positive Prüfung vornherein ausgeschlossen bzw. ist implizit nicht erfolgreich. Die Prüfschritte laufen wie folgt ab:

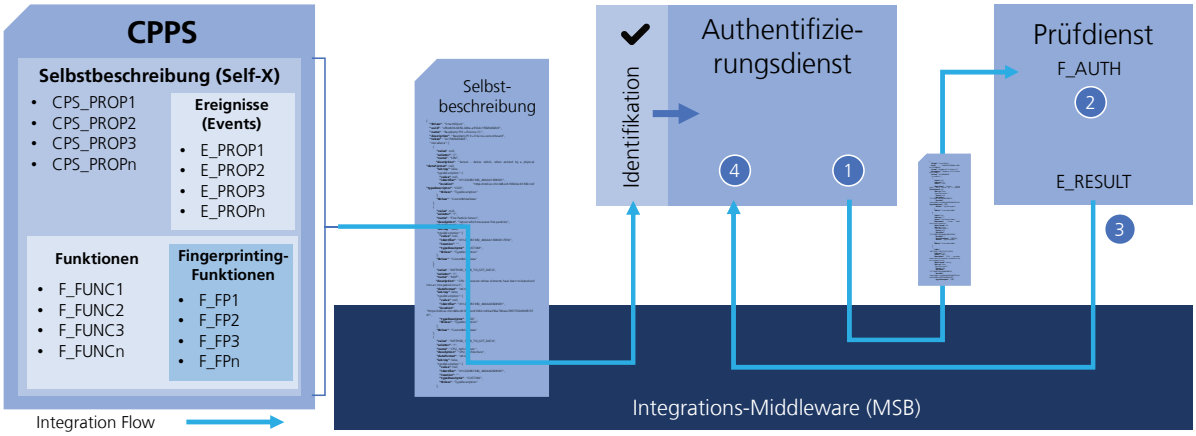


Abbildung 6.20 Schritte der initialen CPPS-Authentifizierung

1. Der Authentifizierungsdienst fragt über den Identifier des Merkmals den Verifizierungs-Proxy ab, ob ein passender Prüfdienst für ein Merkmal verfügbar ist. Falls dies der Fall ist, wird ein Event mit den empfangenen Merkmalsdaten und den hinterlegten Template-Daten über den vorab generierten Integration Flow zu diesem Prüfdienst gesendet.
2. Der Prüfdienst führt eine Prüfung des Merkmals durch und das Ergebnis der Prüfung wird als erfolgreich oder nicht erfolgreich gekennzeichnet.
3. Das Ergebnis der Prüfung wird an den Authentifizierungsdienst gesendet.
4. Der Prüfdienst setzt abhängig vom Prüfergebnis das Vertrauenslevel des CPPS entsprechend der Merkmalsgewichtung höher oder setzt dieses herab.

Die Folgen einer erfolgreichen oder nicht erfolgreichen Prüfung können individuell bestimmt werden. Eine stringente Konfiguration kann dazu führen, dass die Prüfung eines

Merkmals das Zurücksetzen des Vertrauenslevels zur Folge hat und der komplette Prüfprozess aller Merkmale zurückgesetzt wird. Alternativ kann das CPPS für eine Anmeldung bzw. Autorisierung gesperrt werden oder ein Alarmzustand im System aktiviert und die Benachrichtigung eines Anwenders durchgeführt werden.

6.3.3 Aktive und kontinuierliche Authentifizierung

Nachdem die Identität des CPPS, welches sich am System anmelden möchte, verifiziert und initial authentifiziert wurde, werden die Phasen der aktiven und kontinuierlichen Authentifizierung ausgeführt. Die aktive Authentifizierungsphase wird nach Ablauf der für die im hybriden Fingerabdruck festgelegten Prüfprozeduren beendet. Das CPPS wird in seiner Vertrauensstufe weiter heraufgesetzt. Die kontinuierliche Authentifizierungsphase beginnt im Anschluss und führt eine kontinuierliche Prüfung anhand der im hybriden Fingerabdruck hinterlegten Merkmale durch. Für die Anzahl der Fehlschläge bei der Prüfung eines bestimmten Merkmals kann ein Toleranzbereich festgelegt werden (vgl. false reject rate (FRR) bzw. false acceptance rate (FAR) Abschnitt 3.1.7). Insbesondere bei kontextuellen Merkmalen, die bestimmte Abhängigkeiten aufweisen, kann es zu Unschärfen kommen.

Die aktive Authentifizierung wird primär am in Abschnitt 6.2.1 beschriebenen CPS-Prüfstand erprobt. Hierfür wurden die vorhandenen eingebetteten Systeme mit Self-X-Funktionen für aktive Fingerprinting-Verfahren ausgestattet. Um die Vergleichbarkeit zu gewährleisten ist in allen Fällen die Implementierung in Python mit demselben Quellcode zur Durchführung der Versuche verwendet worden. Geprüft werden die CPU-Leistung, Speicher-Leistung (Schreibzugriff) und CPU-Temperatur der eingebetteten Systeme. Insbesondere die Schreibzugriffe des verwendeten bzw. verbauen Speichers variieren stark. Im Fall der Entwicklungsboards werden SD-Karten verwendet, die abhängig vom Hersteller und Modell starke Unterschiede in ihrem Schreibverhalten aufweisen. Die für den produktiven Einsatz verwendeten Compute Module der Kunbus Revolution Pi Steuerungen verwenden eMMC-Speicher, der eine bessere Leistung bei Schreibzugriffen aufweist, jedoch in Bezug

auf die jeweilige Generation des verbauten Compute Moduls charakteristische Leistungsmerkmale aufweist. Die CPU-Leistung der geprüften eingebetteten Systeme ist ebenfalls stark abweichend. Selbst wenn teilweise die gleichen SoCs (System on a Chip) mit gleicher CPU verbaut sind, wie es bei einem Raspberry Pi und einem RPi Compute Modul der ersten Generation der Fall ist, so ist die baugleiche CPU eines Raspberry Pi Zero mit 1,0 GHz gegenüber 0,7 GHz bei anderen Systemen höher getaktet. Ebenso ist die CPU eines Raspberry Pi Compute Modules 3+ mit 1,2 GHz niedriger getaktet als die baugleiche CPU eines Raspberry Pi 3B+ mit 1,4 GHz.

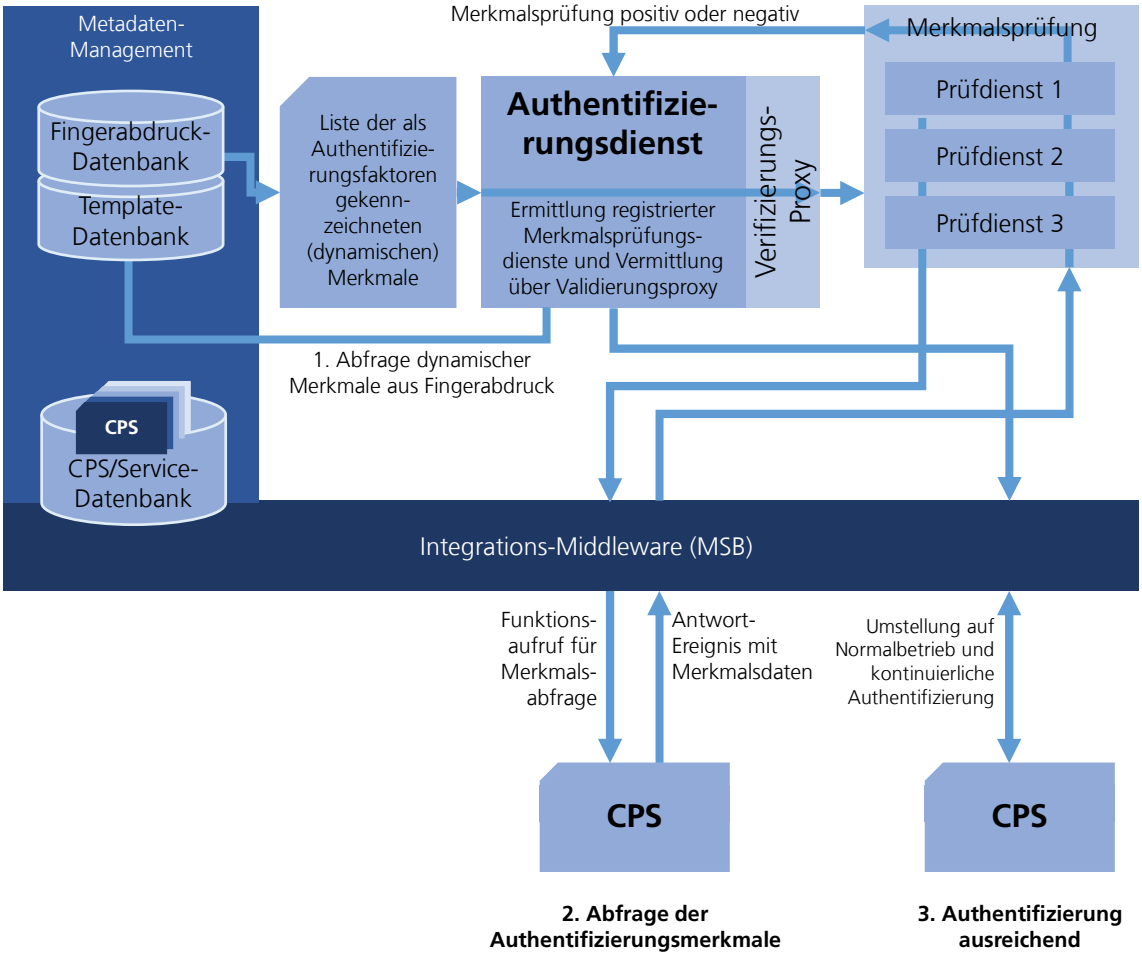


Abbildung 6.21 Prüfablauf für aktive und kontinuierliche CPPS Authentifizierung

Der Ablauf der aktiven und kontinuierlichen CPPS-Authentifizierung ist in Abbildung 6.21 gesamtheitlich dargestellt. Im Folgenden werden die Schritte jeweiligen einzelnen Prozeduren im Kontext der Implementierung erläutert. Zudem wird an dieser Stelle die kontinuierliche Authentifizierung aufgrund der funktionalen Prinzipien und die daraus folgend zu differenzierende Handhabung bei der Implementierung unterschieden in Bezug auf die direkte und indirekte Beobachtung von Merkmalen.

Abbildung 6.22 zeigt die Schritte der aktiven CPPS-Authentifizierung. Wie bereits beschrieben werden die für jeden Schritt notwendigen Integration Flows im Vorfeld automatisch generiert. Der Ablauf lautet wie folgt:

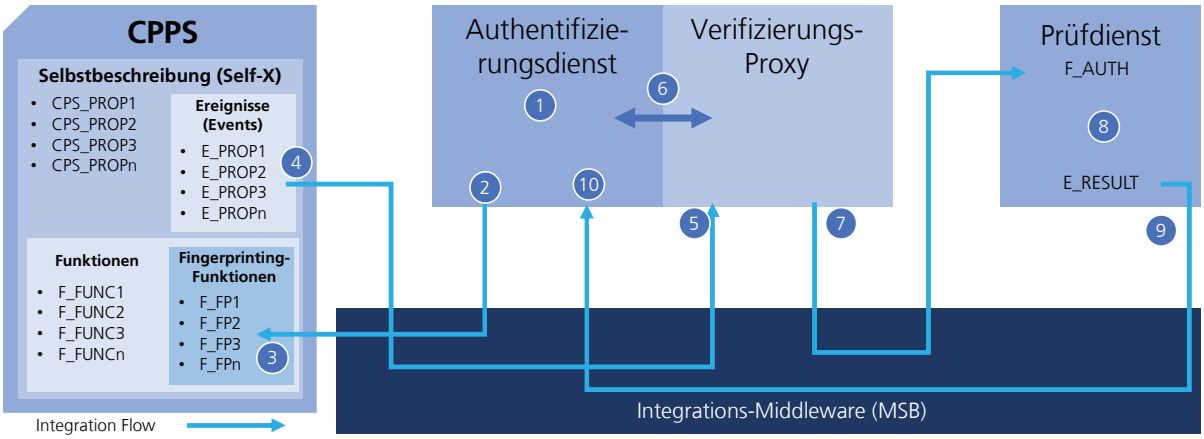


Abbildung 6.22 Schritte der aktiven CPPS-Authentifizierung

1. Der Authentifizierungsdienst wählt ein Merkmal zur aktiven Prüfung aus.
2. Der Authentifizierungsdienst sendet initial ein Event an das CPPS.
3. Das Event löst eine zugehörige Funktion im CPPS aus, die im CPPS eine aktive Merkmalsabfrage durchführt.
4. Das Ergebnis der Merkmalsabfrage wird als Event vom CPPS an den Authentifizierungsdienst gesendet.
5. Der Authentifizierungsdienst empfängt das Event und die Merkmalsdaten.

6. Der Verifizierungsproxy des Authentifizierungsdienstes ermittelt die zugehörigen Template-Daten und den passenden Prüfdienst.
7. Der Verifizierungsproxy des Authentifizierungsdienstes sendet ein Event mit den Merkmalsdaten und den Template-Daten an den zugehörigen Prüfdienst.
8. Der Prüfdienst führt eine Prüfung des Merkmals durch und das Ergebnis der Prüfung wird als erfolgreich oder nicht erfolgreich gekennzeichnet.
9. Das Ergebnis der Prüfung wird an den Authentifizierungsdienst gesendet.
10. Der Prüfdienst setzt abhängig vom Prüfergebnis das Vertrauenslevel des CPPS entsprechend der Merkmalsgewichtung höher oder setzt dieses herab.

Die aktive Merkmalsprüfung greift wie schon in Abschnitt 4.2.2f beschrieben aktiv in das CPPS ein. Hier muss berücksichtigt werden, dass dies die Funktion des CPPS beeinträchtigen kann. Daher werden aktive Prüfschritte bevorzugt direkt nach der initialen Authentifizierungsphase durchgeführt und das CPPS geht nach Abschluss der aktiven Authentifizierungsphase in seine reguläre Betriebsphase über, wenn ein ausreichendes Vertrauenslevel erreicht wurde.

Wie zu Beginn des Abschnitts beschrieben können Leistungsdaten des Prozessors oder der Schreibleistung des Speichers genutzt werden, um eine Prüfung durchzuführen. Da es sich hier im Gegensatz zur initialen Prüfung überwiegend um dynamische Daten handelt, müssen komplexere Prüfstrategien verwendet werden. Die Leistungsdaten des Prozessors lassen sich beispielsweise als Ergebnisarray von Messwerten darstellen. Hier kann das Messwerte-Array der aktiven Merkmalsabfrage mit dem Messwerte-Array des Templates mittels eines Korrelationskoeffizienten vergleichen werden. Liegt dieser innerhalb eines festgelegten Bereichs, gilt ein Merkmal als positiv geprüft.

Die kontinuierliche Authentifizierung ist während der Betriebsphase (bzw. während einer Trainingsphase zur Ermittlung der Merkmalstemplates) des CPPS aktiv und „beobachtet" die Merkmale des CPPS. Dabei wird wie in Abbildung 6.23 dargestellt im Kontext der Implementierung in direkt beobachtbare Merkmale und wie Abbildung 6.24 dargestellt in indirekt beobachtbare Merkmale unterschieden.

Direkt beobachtbar bedeutet, dass sich das Merkmal direkt aus der Selbstbeschreibung ableitet und Merkmalsdaten direkt mit den Event-Daten des CPPS verknüpft sind. Diese Unterscheidung ist relevant im Kontext der im Rahmen dieser Arbeit durchgeführten Implementierung, da der MSB ereignisgetrieben Daten über Information Flows austauscht. Merkmalsdaten, die nicht unmittelbar über ein Event übermittelt werden, können nicht über das Event abgefangen und geprüft werden, sondern müssen separat über einen Prüfdienst erfasst und geprüft werden.

Im Folgenden werden die Abläufe der kontinuierlichen Authentifizierung beschrieben.

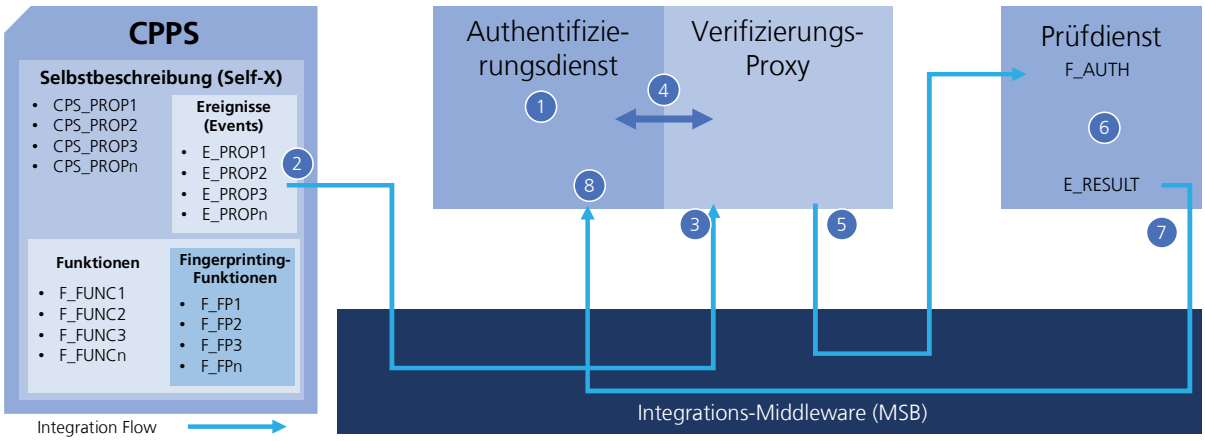


Abbildung 6.23 Schritte der kontinuierlichen CPPS-Authentifizierung mit direkt beobachtbaren Merkmalen

1. Der Authentifizierungsdienst wählt ein Merkmal zur kontinuierlichen Prüfung aus, das eine entsprechende Beziehung zu einem Event hat.
2. Das CPPS sendet ein Event mit Merkmalsdaten.
3. Der Authentifizierungsdienst empfängt das Event und die Merkmalsdaten.
4. Der Verifizierungsproxy des Authentifizierungsdienstes ermittelt die zugehörigen Template-Daten und den passenden Prüfdienst.
5. Der Verifizierungsproxy des Authentifizierungsdienstes sendet ein Event mit den Merkmalsdaten und den Template-Daten an den zugehörigen Prüfdienst.

6. Der Prüfdienst führt eine Prüfung des Merkmals durch und das Ergebnis der Prüfung wird als erfolgreich oder nicht erfolgreich gekennzeichnet.
7. Das Ergebnis der Prüfung wird an den Authentifizierungsdienst gesendet.
8. Der Prüfdienst setzt abhängig vom Prüfergebnis das Vertrauenslevel des CPPS entsprechend der Merkmalsgewichtung höher oder setzt dieses herab.

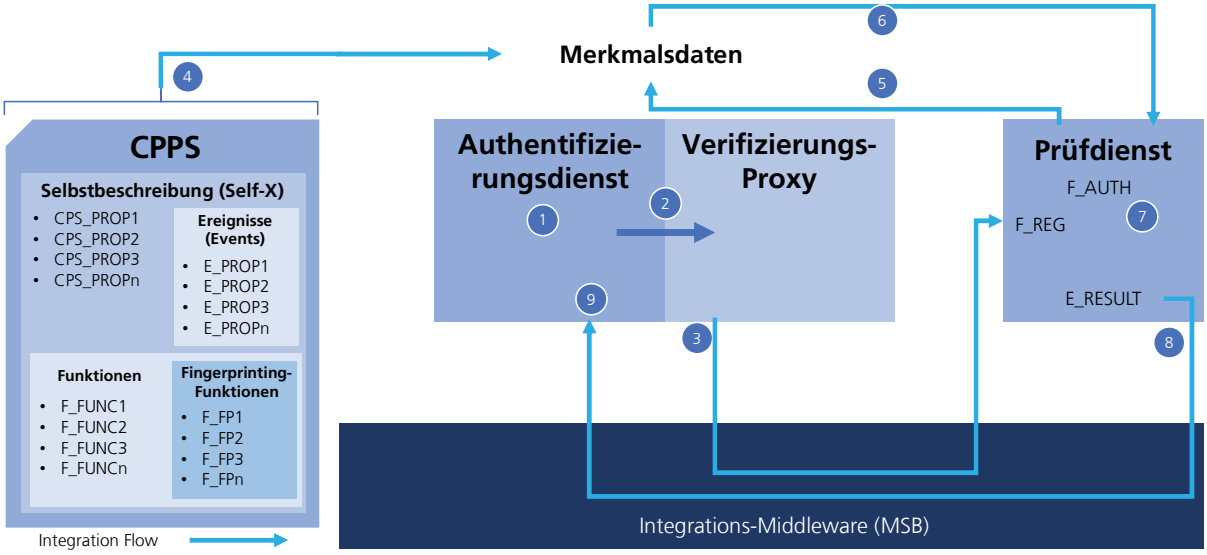


Abbildung 6.24 Schritte der kontinuierlichen CPPS-Authentifizierung mit indirekt beobachtbaren Merkmalen

1. Der Authentifizierungsdienst wählt ein Merkmal zur kontinuierlichen Prüfung aus.
2. Im Verifizierungsproxy wird ermittelt, ob ein Prüfdienst und Template-Daten verfügbar sind.
3. Das Verifizierungsproxy des Authentifizierungsdienstes sendet ein Event mit Template-Daten an den zugehörigen Prüfdienst und registriert diese zur Prüfung.
4. Das CPPS sendet bzw. erzeugt kontinuierlich Merkmalsdaten.
5. Der Prüfdienst beobachtet die Merkmalsdaten.
6. Der Prüfdienst sammelt und verarbeitet die Merkmalsdaten.
7. Der Prüfdienst führt eine Prüfung des Merkmals durch und das Ergebnis der Prüfung wird als erfolgreich oder nicht erfolgreich gekennzeichnet.

8. Das Ergebnis der Prüfung wird an den Authentifizierungsdienst gesendet.
9. Der Prüfdienst setzt abhängig vom Prüfergebnis das Vertrauenslevel des CPPS entsprechend der Merkmalsgewichtung höher oder setzt dieses herab.

Für die kontinuierliche Authentifizierung können Kontextmerkmale herangezogen werden. Dies ist beispielsweise die Präsenz von anderen CPPS, die im Versuch als iBeacon simuliert werden und mittels des Bluetooth-Moduls eines CPPS detektiert werden können (vgl. Anhang 7.5). Zudem kann das Verhalten des CPPS in Bezug auf seine Netzwerkkommunikation überwacht werden. Der Prüfdienst beobachtet hierbei den Paketdatenverkehr im Netzwerk und analysiert die Datenpakete. Diese sind charakteristisch für ein CPPS. Solange das Muster Protokollnachrichten und Datenpakete mit dem im Template übereinstimmen, wird das Vertrauenslevel gehalten. Wird eine Abweichung festgestellt, kann das Vertrauenslevel herabgesetzt werden oder eine bestimmte Aktion ausgelöst werden.

Im komplexen Szenario werden die Ereignis-Daten des Werkstückträgers mit den Sensordaten des Produkts abgeglichen. Hierzu ist bei der Modellierung des hybriden Fingerabdrucks Wissen über den Prozessablauf notwendig. So wird das Ereignis zum Beginn des Wendevorgangs des Greifers genutzt, um eine zeitgleiche Veränderung der Sensordaten im Produkt, welches gewendet wird, zu erkennen. Tritt diese Korrelation nicht oder abweichend ein, kann dieses Merkmal als Authentifizierungsfaktor nicht positiv geprüft werden. Somit ist die kontinuierliche Authentifizierung an dieser Stelle fehlgeschlagen. Diese Art der Korrelation von Ereignissen und Sensorwerten basierend auf Interaktionen kann durch eine länger andauernde Sammlung und Analyse von Daten auch mittels verschiedener Verfahren zur Musteranalyse automatisiert werden, um komplexe Merkmalsmuster zu identifizieren.

Abbildung 6.25 zeigt die Visualisierung der von den Produktsensoren erfassten Daten, die die Datensätze zweiter Sensoren nebeneinander gegenüberstellen.

Aus der Darstellung ergeben sich drei wichtige Punkte, die ebenfalls in Abbildung 6.25 markiert sind:

1. Es sind „mit bloßem Auge“ eindeutige Muster erkennbar, die als Charakteristik herangezogen und von Merkmalsprüfungsdiensten kontinuierlich überwacht werden können (rot markiert).
2. Die Korrelation von Ereignissen und Veränderungen bestimmter Sensoren ist erkennbar. So verändern sich die Daten bestimmter Sensoren stark und eindeutig charakteristisch und bestätigen den Kontext des Ereignisses, beispielsweise den Wendevorgang durch den Greifer (Nummer 1 und 2).
3. Es kann zwischen beiden Sensoren unterschieden werden. So sind die Muster beider Sensoren ähnlich, allerdings zeigt sich insbesondere beim Magnetfeldsensor, dass beide Sensoren unterschiedlich ausgeprägt auf Einflüsse auf das Magnetfeld durch ihre relative Position im Raum und andere Gegenstände reagieren. Ihre Muster ähneln sich, sind jedoch unterschiedlich ausgeprägt (Nummer 3).

Eine detailliertere Darstellung und Erläuterung der Beziehungen zwischen Ereignissen und Sensordaten ist in Anhang 8 bzw. Abbildung A 32 zu finden.

Abbildung 6.25 Visualisierung der CP Lab Sensor- und Ereignisdaten

6.4 Diskussion der Ergebnisse in Bezug auf die Forschungsfragen

Die Ergebnisse der durchgeführten Versuche lassen sich abschließend wie folgt zur Beantwortung der initial in Abschnitt 1.3 definierten Forschungsfragen verwenden:

(F1) Wie können die Selbstbeschreibungsmerkmale eines CPS genutzt werden, um eine sichere Identität zur Identifikation und Authentifizierung eines CPPS zu schaffen?

Im Rahmen dieser Arbeit wurde ein Klassifizierungs- und Typisierungsansatz für Selbstbeschreibungsmerkmale entwickelt. Dieser dient zur Beschreibung von Selbstbeschreibungsmerkmalen zum Zweck der Ableitung von Authentifizierungsfaktoren. An vier Fallstudien wurde gezeigt, welche Merkmale von Maschinen zu diesem Zweck bestimmt werden können. Die Authentifizierungsfaktoren wiederum werden für ein Multifaktor-Authentifizierungsverfahren verwendet. Für dieses wurde ein Ablaufprotokoll entwickelt und prototypisch in einem serviceorientierten Authentifizierungssystem implementiert, welches mit den Self-X-Fähigkeiten der CPPS arbeitet. Zudem wurde gezeigt, wie spezifisch sich bestimmte Merkmale eines eingebetteten Systems eines CPPS äußern und somit für eine Identifikation und Authentifizierung verwendet werden können.

(F1.1) Biometrische Verfahren nutzen eindeutige Muster in physischen Merkmalen einer Person wie beispielsweise einen Fingerabdruck, um eine eindeutige Identifikation dieser Person durchzuführen. Maschinen besitzen per se keinen Fingerabdruck in diesem Sinne, jedoch soll in dieser Arbeit der Frage nachgegangen werden, ob und wie sich ein "künstlicher Fingerabdruck" mit Hilfe von Selbstbeschreibungsmerkmalen konstruieren lässt.

Das zentrale Informationsmodell zur Abbildung der sicheren digitalen Identität wurde als hybrider Fingerabdruck definiert. Dieser ist prinzipiell mit einem Template, wie es für biometrische Identifikationsverfahren verwendet wird, vergleichbar. Allerdings ist die Hybridität des Fingerabdrucks dadurch bedingt, dass sowohl statische, also auch dynamische

Merkmale und zusätzliches explizites und implizites Wissen in der Struktur abgebildet werden. Es ist somit möglich diesen künstlichen Fingerabdruck mit Hilfe von Selbstbeschreibungsmerkmalen zu erschaffen, der für eine Identifikation und Authentifizierung verwendet werden kann und eine sichere digitale Identität bildet.

(F1.2) Welche Selbstbeschreibungsmerkmale eignen sich für die Konstruktion eines "künstlichen Fingerabdrucks" und somit einer sicheren Identität?

Die in Abschnitt 4.3.2 eingeführten Merkmalsklassen und -typen wurden definiert, um eine systematische Einordnung geeigneter Merkmale zu ermöglichen. Diese wurden zusätzlich mit Eignungs- und Bewertungskriterien zur Bestimmung von Authentifizierungsfaktoren ergänzt, um eine Merkmalsgewichtung durchführen zu können. Dies ist notwendig, da die Frage F1.2 sich nicht direkt und allgemeingültig mit einem bestimmten Merkmalstyp beantworten lässt, sondern die Eignung eines Merkmals individuell und im Kontext zu betrachten ist. Grundsätzlich ist Kontextmerkmalen und Verhaltensmerkmalen, die auch als komplexe Merkmale kombiniert werden können, eine besondere Eignung zur Erstellung einer sicheren Identität zuzuschreiben.

(F1.3) Können Authentifizierungsverfahren auf Grundlage der Selbstbeschreibungsmerkmale unter Nutzung der Self-X-Eigenschaften eines CPS geschaffen werden, ohne dass die Anwendbarkeit und Funktionalität der Anwendung beeinträchtigt wird?

Der Grad der Beeinträchtigung der Anwendbarkeit hängt direkt mit dem Grad der Self-X-Fähigkeit des CPPS zusammen. Der größte Aufwand ist aktuell noch die Modellierung des hybriden Fingerabdrucks in der Onboarding- bzw. Enrollment-Phase, die im Rahmen der prototypischen Implementierung manuell durchgeführt wird, und hängt von der Komplexität des Fingerabdrucks ab. Diese kann insbesondere beim Einsatz starker und komplexer Merkmale initial sehr aufwendig sein. Die in dieser Arbeit umgesetzte prototypische Implementierung nutzt IEC 61360 CDD (Common Data Dictionary) Semantic Dictionary IDs für die eindeutige Kennzeichnung von Merkmalen. Dieser Ansatz orientiert sich an der

I4.0 Verwaltungsschale. Prinzipiell können daher auch eCl@ss Identifier für die semantische Annotation von Merkmalen genutzt werden. Es muss jedoch entweder ein einheitlicher Ansatz gewählt werden oder das System muss auf die Verwendung mehrerer Dictionaries umgesetzt werden. Durch die semantisch eindeutige Kennzeichnung von Merkmalen ist die maschinelle Interpretierbarkeit der Merkmale gewährleistet. So können aus der Selbstbeschreibung automatisch Merkmale entsprechenden Prüfdiensten zugewiesen werden. Der Aufwand liegt hier also zum größten Teil in der Umsetzung des Authentifizierungssystems und der Implementierung der Self-X-Fähigkeiten von CPPS. Der Anwender bzw. der Domänenexperte in der Produktion hat einen anfänglichen Aufwand bei der optionalen Festlegung komplexer Merkmale. Da die einzelnen Merkmale eines komplexen Merkmals jedoch wie bereits beschrieben eindeutig interpretierbar sind, können komplexe Merkmale bzw. das komplette Template als Vorlage für CPPS gleichen Typs verwendet werden. Die Merkmalsausprägungen der jeweiligen Merkmale werden jedoch CPPS-individuell über dessen Self-X-Fähigkeiten in Form von zugehörigen aufrufbaren Operationen ausgelesen. Die eigentliche Authentifizierung im Nachgang ist ebenfalls vollständig automatisierbar und hat somit keine Auswirkung auf die Verwendung und Funktionalität während der Betriebsphase durch den Anwender. Hier muss allerdings beachtet werden, dass aktive Fingerprinting-Methoden nicht prozess- oder systemkritische Ressourcen durch Interrupts im eingebetteten System des CPPS stören. Daher werden diese fast ausschließlich zu Beginn des Authentifizierungsprozesses verwendet, während in der Betriebsphase passive Verfahren genutzt werden.

7 Zusammenfassung

Abschließend soll in diesem Kapitel rückblickend der Gesamtansatz und das Ergebnis dieser Arbeit diskutiert und ein Ausblick gegeben werden, wie die Erkenntnisse in die Praxis transportiert werden können und welche weiteren Schritte in Zukunft angesetzt werden können, um an das Konzept anzuknüpfen und es weiterzuentwickeln.

7.1 Reflexion

Das vorgestellte Konzept zeigt, wie schon heute mit den immer leistungsfähigeren eingebetteten Systemen, die in industriellen Anwendungen zum Tragen kommen und die Grundlagen von CPPS bilden, eine Authentifizierung auf der Grundlage von Selbstbeschreibungsmerkmalen durchgeführt werden kann, die keinen Einfluss auf die Handhabbarkeit des Systems durch die Anwender in der Betriebsphase hat. Dieser Umstand wird im Kontext der Forschungsfrage F1.3 diskutiert (vgl. Abschnitt 6.4). Der Ansatz macht sich die zunehmenden Self-X-Fähigkeiten zunutze, die aktuell erst noch sehr rudimentär vorhanden sind. Daher ist auch mit zunehmendem Fortschritt in diesen Bereichen damit zu rechnen, dass die aktuellen Schwächen des Ansatzes noch beseitigt werden können, die sich hauptsächlich auf die maschinelle Interpretierbarkeit und komplexere Algorithmen zur automatisierten Generierung und Auswertung von Fingerprint-Templates beziehen.

Im Hinblick auf die Merkmalsarten zeigt sich, dass diese unterschiedlich gut geeignet sind und die Eignung auch stark abhängig vom Kontext und dem individuellen CPPS ist.

Dies ist vor allem der Umstand geschuldet, dass die statischen und dynamischen Merkmale im Fall einer Kompromittierung vergleichsweise einfach nachzuahmen sind. Zwar ist der Ansatz des Verfahrens als Zusatzmaßnahme in einem Defense-in-Depth-Konzept zusätzliche Hürden für Angreifer zu bieten, allerdings ist es darauf angewiesen, dass insbesondere die geschützten und geschlossenen Merkmale einem Angreifen nicht bekannt sind.

Auch ist eine direkte Modifikation eines Geräts, auf das ein Angreifer direkten Zugriff hat, nur bedingt detektierbar. Insbesondere wenn gezielte Angriffe ausgeführt werden, beispielsweise auf Prozessparameter oder passives Mitschneiden bestimmter Daten. Für die Erstellung einer eindeutigen und sicheren Identität aus Selbstbeschreibungsmerkmalen wird auch vorausgesetzt, dass Hersteller ihre Produkte mit entsprechenden Fähigkeiten ausstatten. Vorausgesetzt wird vor allem auch eine ausreichende Leitungsfähigkeit eines CPPS in Hinblick auf die internen Compute-Ressourcen, funktionale Komponenten, die es ermöglichen eine Vielzahl von Komponenten zu erfassen und eine Offenheit des Systems. Das Konzept ist grundsätzlich auch auf leistungsschwachen eingebetteten Systemen verwendbar, allerdings ist hier der Aufwand viel höher entsprechende aktive Prüfverfahren zu implementieren und diese sind infolgedessen funktional eingeschränkt.

Die Handhabbarkeit ist aktuell noch stark von einer manuellen Onboarding- bzw. Enrollment-Phase abhängig, die nicht ohne zusätzlichen Aufwand für den Anwender einhergeht. Insbesondere komplexe und kontextuelle Merkmale sind fast immer mit implizitem und explizitem Wissen behaftet, welches vom Anwender während der Modellierung eines hybriden Fingerabdrucks abgebildet werden muss. Die Ersteinrichtung der Authentifizierung setzt Expertenwissen in Verbindung mit dem domänenspezifischen Prozesswissen der jeweiligen Anwendung voraus. Hier sind insbesondere zusätzliche Werkzeuge notwendig, die die Handhabbarkeit, beispielsweise die Modellierung eines hybriden Fingerabdrucks durch den Anwender, besser unterstützen.

Dieser Umstand kann allerdings im Laufe der Zeit und unter Anwendung fortschrittlicherer Methoden behoben werden. So ist vorstellbar, dass nach einer ausreichend großen Datenbasis durch die wiederholte Ableitung von Authentifizierungsfaktoren aus Selbstbeschreibungsmerkmalen graduell in einem ersten Schritt ein Regelsystem zur automatisierten Ableitung von einfachen Faktoren und in der weiteren Entwicklung zunehmend komplexere Ansätze zur Bestimmung der Authentifizierungsfaktoren eingesetzt werden können.

Die Entwicklung von Prüfdiensten, die bestimmte Merkmale adäquat und effektiv prüfen, ist eine Herausforderung für sich. Im Rahmen dieser Arbeit wurde nur eine Auswahl von

Beispielen mit einfachen Prüfmethoden implementiert und dargestellt. Das Konzept ist jedoch explizit so ausgelegt, dass die Merkmalsprüfung beliebig ausgebaut und mit dem technologischen Fortschritt mitwachsen kann. Insbesondere Methoden des maschinellen Lernens und der künstlichen Intelligenz wurden in der Implementierung nicht betrachtet, sind aber voraussichtlich insbesondere für Merkmale, die komplexe kontextuelle Zusammenhänge oder Muster aufweisen, ausgezeichnet geeignet, um für eine Merkmalsprüfung eingesetzt zu werden.

7.2 Ausblick

Das Konzept beschreibt die grundlegenden Ansätze, wie die Merkmale eines CPPS, die sich aus der Selbstbeschreibung ableiten lassen, genutzt werden können, um eine Authentifizierung von CPPS durchzuführen, die dessen Self-X-Fähigkeiten verwendet. Das tatsächliche Potenzial des Ansatzes ist nicht nur abhängig vom technischen Fortschritt der CPPS, sondern auch von der Adaption der Verfahren und Normen. Hierzu gehören vor allem einheitliche Informationsmodelle und semantische Standards, die die Ableitung von Merkmalen aus der Selbstbeschreibung weiter vereinfachen. Hier zeichnet sich am Beispiel der Industrie 4.0 Verwaltungsschale ab, dass diese mittels ihrer standardisierten Teilmodelle diese Hürde in Zukunft senken und sogar beseitigen könnte. Hier sind dedizierte Teilmodelle vorstellbar, die den hybriden Fingerabdruck und bestimmte Merkmalsprüfverfahren vereinheitlichen. In einer Industrie 4.0 Systemumgebung kann dann ein CPPS als Industrie 4.0-konformes System betrachtet werden. Hierfür definiert der „Functional View" der Verwaltungsschale eine Compute-Infrastruktur, die neben Rechenkapazitäten auch Softwaredienste vorsieht. Diese Softwaredienste lassen sich in Applikationskomponenten und systemisch relevante Infrastrukturdienste einteilen. Das in dieser Arbeit entwickelte Konzept ist aufgrund seiner Service-orientierten Architektur so ausgelegt, dass es in eine solche Infrastruktur integriert werden kann und die Dienste des merkmalsbasierten Authentifizierungssystems entweder Teil der Infrastrukturdienste oder einer speziellen Anwendung werden können. Nach dem Defense-in-Depth-Prinzip können so die

durch die Industrie 4.0 Systemumgebung definierten und bereitgestellten Sicherheitsmechanismen dynamisch ergänzt und funktional skaliert werden. Die durch Verwaltungsschalen-Teilmodelle strukturierten und semantisch eindeutig annotierten Daten und Informationen können so unmittelbar als Selbstbeschreibungsdaten herangezogen werden. CPPS, die reaktive Typ2-Verwaltungsschalen besitzen können mit diesen mittels aktiver Teilmodelle Self-X-Fähigkeiten realisieren. Zukünftig könnten Typ3-Verwaltungsschalen durch den Einsatz einer einheitlichen „Industrie 4.0-Sprache“ die merkmalsbasierte Prüfung inklusive der Erstanmeldung vollkommen autonom für alle Komponenten in einer Industrie 4.0-Systemumgebung durchführen und so sogar den Engineering-Aufwand zur erstmaligen Einrichtung der sicheren Identität reduzieren oder sogar beseitigen.

Zudem werden weitere Bestrebungen vorangetrieben, um das Verständnis und die Umsetzung eines Digitalen Zwillings in seinen Ausprägungen zu normieren. Dies ist auch durch den Bedarf nach einer besseren Data Governance für Anwendungen der Künstlichen Intelligenz in im industriellen Umfeld begründet. Daten und Informationen in ausreichender Verfügbarkeit, Qualität und Menge sind hierfür eine Voraussetzung. Jedoch sind die aktuellen IT-Architekturen im Produktionsumfeld hierfür nicht adäquat definiert und implementiert. Die Hoffnung liegt auf der kontinuierlichen Wandlung dieser in CPPS-Architekturen, die die notwendige Leistungsfähigkeit und insbesondere die Self-X-Fähigkeiten mit sich bringen. Unternehmen bieten und nutzen immer mehr Produkte, die auf Open Source-basierten offenen Architekturen und Schnittstellen aufbauen und so eine schnelle Adaption und Nutzung neuartiger Ansätze ermöglichen. Der Ansatz zur Merkmalsbewertung ist im aktuellen Ansatz noch relativ einfach gelöst und kann in Zukunft noch weiter ausgebaut werden. Insbesondere die Adaption von komplexeren Verfahren, die es durch zusätzliches formalisiertes und geteiltes implizites Wissen ermöglichen Merkmale und Merkmalszusammenhänge maschinell zu interpretieren und Zusammenhänge zu abstrahieren. Dies bietet zusätzliches Potenzial die Authentifizierung auf Basis von Selbstbeschreibungsmerkmalen weiter zu verbessern und zu stärken. Offene Ansätze, wie die Entwicklung von Merkmalsprüfungsdiensten im Open Source-Umfeld, kann ein An-

satz sein, um diese komplexen Verfahren in einem Community-Ansatz gemeinsam zu voranzutreiben und so eine umfangreiche Landschaft leistungsfähiger Merkmalsprüfungsverfahren und -dienste zu abzubilden.

8 Literaturverzeichnis

Aamodt et al. 1995 Aamodt, Agnar; Nygård, Mads, 1995. Different roles and mutual dependencies of data, information, and knowledge — An AI perspective on their integration. *Data & knowledge engineering* **16** (3), S. 191–222

Abowd et al. 1999 Abowd, Gregory D.; Dey, Anind K.; Brown, Peter J.; Davies, Nigel; Smith, Mark; Steggles, Pete, 1999. Towards a Better Understanding of Context and Context-Awareness. In: *Handheld and Ubiquitous Computing*. Berlin: Springer, S. 304–307

acatech 2013 acatech, 2013. Technikwissenschaften: Erkennen - Gestalten - Verantworten (acatech IMPULS). Berlin: Springer Vieweg. ISBN 9783642346040

acatech et al. 2015 acatech; Arbeitskreis Smart Service Welt (Hrsg.), 2015. *SMART SERVICE WELT - Umsetzungsempfehlungen für das Zukunftsprojekt Internetbasierte Dienste für die Wirtschaft - Kurzversion*. Berlin: acatech - Deutsche Akademie der Technikwissenschaften e.V. Verfügbar unter: https://www.acatech.de/publikation/abschlussbericht-smart-service-welt-umsetzungsempfehlungen-fuer-das-zukunftsprojekt-internetbasierte-dienste-fuer-die-wirtschaft/download-pdf?lang=de_excerpt Zugriff am: 21.01.2021

Ackerman 2017 Ackerman, Pascal, 2017. *Industrial Cybersecurity*. Birmingham: Packt Publishing. ISBN 9781788395151

Adolphs et al. 2016 Adolphs, Peter; Auer, Sören; Bedenbender, Heinz; Billmann, Meik; Hankel, Martin; Heidel, Roland; Hoffmeister, Michael; Huhle, Haimo; Jochem, Michael; Kiele-Dunsche, Markus; Koschnick, Gunther; Koziolek, Heiko; Linke, Lukas; Pichler, Reinhold; Schewe, Frank; Schneider, Karsten; Waser, Bernd; Plattform Industrie 4.0, 2016. *Struktur der Verwaltungsschale - Fortentwicklung des Referenzmodells für die Industrie 4.0-Komponente*.
Berlin: Bundesministerium für Wirtschaft und Energie (BMWi).
Verfügbar unter: https://www.plattform-i40.de/PI40/Redaktion/DE/Downloads/Publikation/struktur-der-verwaltungsschale.pdf?__blob=publicationFile&v=5
Zugriff am: 21.01.2021

Ahlborn et al. 2019 Ahlborn, Klaus; Bachmann, Gerd; Biegel, Fabian; Bienert, Jörg; Falk, Svenja; Fay, Alexander; Gamer, Thomas; Garrels, Kai; Grotepass, Jürgen; Heindl, Andreas; Heizmann, Jörg; Hilger, Claus; Hoffmann, Martin; Hoffmeister, Michael; Jochem, Michael; Kalhoff, Johannes; Kamp, Martin; Kramer, Stefan; Kosch, Bernd; Legat, Christoph; Michels, Jan Stefan; Mildner, Alexander; Nettsträter, Andreas; Pant, Rohitashwa; Pittschellis, Reinhard; Schauf, Thomas; Schlinkert, Hans-Jürgen; Ulrich, Marco; Zinke, Guido, 2019. *Technologieszenario „Künstliche Intelligenz in der Industrie 4.0“*.
Berlin: Plattform Industrie 4.0.
Verfügbar unter: https://www.plattform-i40.de/PI40/Redaktion/DE/Downloads/Publikation/KI-industrie-40.pdf?__blob=publicationFile&v=10
Zugriff am: 21.01.2021

Ahmed et al. 2017 Ahmed, Chuadhry Mujeeb; Mathur, Aditya P., 2017. Hardware Identification via Sensor Fingerprinting in a Cyber Physical System.
In: *2017 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)*.
New York: IEEE, S. 517–524

Ahrens et al. 2019 Ahrens, Maximilian; Biegel, Fabian; Breit, Marco-Alexander; Fier, Andreas; Jochem, Michael; Kaesberg, Mirco; Kohler, Fabian; Lange, Thomas; Otto, Boris; Polenz, Carsten; Post, Peter; Ritz, Sebastian; Stöckl-Pukall, Ernst; Summa, Harald A.; Zeisel, Herbert, 2019. *Das Projekt GAIA-X - Eine vernetzte Dateninfrastruktur als Wiege eines vitalen, europäischen Ökosystems*.
Berlin: Bundesministerium für Wirtschaft und Energie (BMWi).
Verfügbar unter: https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/das-projekt-gaia-x.pdf?__blob=publicationFile&v=24
Zugriff am: 21.01.2021

Alaca et al. 2016 Alaca, Furkan; van Oorschot, P. C., 2016. Device fingerprinting for augmenting web authentication: classification and analysis of methods.
In: *Proceedings of the 32nd Annual Conference on Computer Security Applications*.
New York: ACM, S. 289–301
ISBN 9781450347716

Alzubaidi et al. 2016 Alzubaidi, Abdulaziz; Kalita, Jugal, 2016. Authentication of Smartphone Users Using Behavioral Biometrics.
IEEE Communications Surveys Tutorials **18** (3), S. 1998–2026

Amerini et al. 2017 Amerini, Irene; Becarelli, Rudy; Caldelli, Roberto; Melani, Alessio; Niccolai, Moreno, 2017. Smartphone Fingerprinting Combining Features of On-Board Sensors.
IEEE Transactions on Information Forensics and Security **12** (10), S. 2457–2466

AmIUnique 2019 AmIUnique, 2019. Learn how identifiable you are on the Internet
Verfügbar unter: https://amiunique.org/tools
Zugriff am: 21.01.2021

Andress 2011 Andress, Jason, 2011. The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice.
1. Aufl.
Waltham: Syngress Publishing.
ISBN 9781597496537

Andress et al. 2013 Andress, Jason; Winterfeld, Steve, 2013. *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. 2. Aufl.
Waltham: Syngress Publishing.
ISBN 9780124166721

Ashton 2009 Ashton, Kevin, 2009. That „Internet of Things" Thing. *RFID journal* **22** (7), S. 97–114

Ayeswarya et al. 2019 Ayeswarya, S.; Norman, Jasmine, 2019. A survey on different continuous authentication systems.
International Journal of Biometrics **11** (1), S. 67

Azizyan et al. 2009 Azizyan, Martin; Constandache, Ionut; Roy Choudhury, Romit, 2009. SurroundSense: Mobile Phone Localization via Ambience Fingerprinting.
In: *Proceedings of the 15th Annual International Conference on Mobile Computing and Networking*.
New York: ACM, S. 261–272
ISBN 9781605587028

Bachlechner et al. 2016 Bachlechner, Daniel; Behling, Thorsten; Bollhöfer, Esther; Dexheimer, Thomas; Borges, Georg; et al., 2016. *IT-Sicherheit für die Industrie 4.0*.
Berlin: Bundesministerium für Wirtschaft und Energie (BMWi).
Verfügbar unter: https://www.bmwi.de/Redaktion/DE/Publikationen/Studien/it-sicherheit-fuer-industrie-4-0.pdf?__blob=publicationFile&v=4
Zugriff am: 21.01.2021

Bakakeu et al. 2017 Bakakeu, Jupiter; Schäfer, Franziska; Bauer, Jochen; Michl, Markus; Franke, Jörg, 2017. Building Cyber-Physical Systems - A Smart Building Use Case.
In: Song, Houbing, Srinivasan, Ravi, Sookoor, Tamim, Jeschke, Sabina (Hrsg.), *Smart Cities*.
Hoboken: John Wiley & Sons, Inc.
Lecture Notes in Computer Science., S. 605–639
ISBN 9781119226444

Barnstedt et al. 2020 Barnstedt, Erich; Bedenbender, Heinz; Billman, Meik; Boss, Birgit; Clauer, Erich; Fritsche, Michael; Garrels, Kai; Hankel, Martin; Hillermeier, Oliver; Hoffmeister, Michael; Jochem, Michael; Koziolek, Heiko; Legat, Christoph; Mendes, Marco; Neidig, Jörg; Sauer, Manuel; Schier, Marc; Schmitt, Michael; Schröder, Tizian; Uhl, André; Usländer, Thomas; Walloschke, Thomas; Waser, Bernd; Wende, Jörg; Ziesche, Constantin; Plattform Industrie 4.0; ZVEI, 2020. *Details of the Asset Administration Shell - Part 1 - The exchange of information between partners in the value chain of Industrie 4.0 (Version 3.0RC01)*.
Berlin: Federal Ministry for Economic Affairs and Energy (BMWi).
Verfügbar unter: https://www.plattform-i40.de/PI40/Redaktion/DE/Downloads/Publikation/Details_of_the_Asset_Administration_Shell_Part1_V3.pdf?__blob=publicationFile&v=5
Zugriff am: 21.01.2021

Barton et al. 2018 Barton, David; Gönnheimer, Philipp; Qu, Chuanqi; Fleischer, Jürgen, 2018. Self-describing connected components for live information access within production systems.
In: *4th International Conference on System-Integrated Intelligence: Intelligent, Flexible and Connected Systems in Products and Production*.
Hannover: Elsevier B.V., S. 250–257

Bath 2018 Bath, Dominik, 2018. Berliner Firma entwickelt neue Zugangskontrollen für Büros
Verfügbar unter: https://www.morgenpost.de/wirtschaft/article215018459/Berliner-Firma-entwickelt-neue-Zugangskontrollen-fuer-Bueros.html
Zugriff am: 21.01.2021

Bauer et al. 2017 Bauer, Dennis; Stock, Daniel; Bauernhansl, Thomas, 2017. Movement Towards Service-orientation and App-orientation in Manufacturing IT.
Procedia CIRP **62**, S. 199–204

Bauernhansl 2014 Bauernhansl, Thomas, 2014. Komplexe Märkte erfordern komplexe Fabrik- und Managementstrukturen - Vielfalt ist Trumpf, aber nur wenn man mit ihr umgehen kann.
Interaktiv **2014** (1), S. 36–39

Bauernhansl et al. 2018 Bauernhansl, Thomas; Hartleif, Silke; Felix, Thomas, 2018. The Digital Shadow of production – A concept for the effective and efficient information supply in dynamic industrial environments.
Procedia CIRP **72**, S. 69–74

Bauernhansl et al. 2016 Bauernhansl, Thomas; Krüger, Jörg; Reinhart, Gunther; Schuh, Günther, 2016. *WGP-Standpunkt Industrie 4.0*.
Darmstadt: Wissenschaftliche Gesellschaft für Produktionstechnik WGP e. V.
Verfügbar unter: https://www.ipa.fraunhofer.de/content/dam/ipa/de/documents/Presse/Presseinformationen/2016/Juni/WGP_Standpunkt_Industrie_40.pdf
Zugriff am: 21.01.2021

Bawa et al. 2015 Bawa, Ranjit; Clark, Rick, 2015. Software-defined everything - Breaking virtualization's final frontier.
Tech Trends 2015 **The fusion of business and IT**, S. 66–79

Becker 2011 Becker, Alexander, 2011. *Nutzenpotenziale und Herausforderungen Service-orientierter Architekturen*.
1. Aufl.
Wiesbaden: Gabler Verlag.
ISBN 9783834929464

Bedenbender et al. 2017a Bedenbender, Heinz; Bentkus, Alexander; Epple, Ulrich; Hadlich, Thomas; Hankel, Martin; Heidel, Roland; Hillermeier, Oliver; Hoffmeister, Michael; Huhle, Haimo; Kiele-Dunsche, Markus; Koziolek, Heiko; Lohmann, Steffen; Mendes, Marco; Neidig, Jörg; Palm, Florian; Pollmeier, Stefan; Rauscher, Benedikt; Schewe, Frank; Waser, Bernd; Weber, Ingo; Wollschlaeger, Martin; Plattform Industrie 4.0; ZVEI, 2017a. *Beziehungen zwischen I4.0-Komponenten - Verbundkomponenten und intelligente Produktion Fortentwicklung des Referenzmodells für die Industrie 4.0-Komponente SG Modelle und Standards*.
Berlin: Bundesministerium für Wirtschaft und Technologie (BMWi).
Verfügbar unter: https://www.plattform-i40.de/PI40/Redaktion/DE/Downloads/Publikation/beziehungen-i40-komponenten.pdf?__blob=publicationFile&v=7
Zugriff am: 21.01.2021

Bedenbender et al. 2017b Bedenbender, Heinz; Bentkus, Alexander; Epple, Ulrich; Hadlich, Thomas; Heidel, Roland; Hillermeier, Oliver; Hoffmeister, Michael; Huhle, Haimo; Kiele-Dunsche, Markus; Koziolek, Heiko; Lohmann, Steffen; Mendes, Marco; Neidig, Jörg; Palm, Florian; Pollmeier, Stefan; Rauscher, Benedikt; Schewe, Frank; Waser, Bernd; Weber, Ingo; Wollschlaeger, Martin; Plattform Industrie 4.0; ZVEI, 2017b. *Industrie 4.0 Plug-and-Produce for Adaptable Factories: Example Use Case Definition, Models, and Implementation*. Berlin: Bundesministerium für Wirtschaft und Technologie (BMWi).
Verfügbar unter: https://www.zvei.org/fileadmin/user_upload/Presse_und_Medien/Publikationen/2017/Juni/Industrie_4.0_Plug_and_produce/Industrie-4.0-_Plug-and-Produce-zvei.pdf
Zugriff am: 21.01.2021

Bedenbender et al. 2016 Bedenbender, Heinz; Billmann, Meik; Epple, Ulrich; Hadlich, Thomas; Hankel, Martin; Heidel, Roland; Hillermeier, Oliver; Hoffmeister, Michael; Huhle, Haimo; Jochem, Michael; Kiele-Dunsche, Markus; Koschnick, Gunther; Koziolek, Heiko; Linke, Lukas; Lohmann, Steffen; Palm, Florian; Pichler, Reinhold; Pollmeier, Stefan; Rauscher, Benedikt; Schewe, Frank; Schneider, Karsten; Waser, Bernd; Weber, Ingo; Wollschlaeger, Martin; Zinn, Marcus, 2016. *Beispiele zur Verwaltungsschale der Industrie 4.0-Komponente - Basisteil*.
Frankfurt am Main: Zentralverband Elektrotechnik- und Elektronikindustrie e. V.
Verfügbar unter: https://www.zvei.org/fileadmin/user_upload/Presse_und_Medien/Publikationen/2016/November/Beispiele_zur_Verwaltungsschale_der_Industrie_4.0-Komponente_-_Basisteil/Beispiele-Verwaltungsschale-Industrie-40-Komponente-White-Paper-Final.pdf
Zugriff am: 21.01.2021

Bedenbender et al. 2019 Bedenbender, Heinz; Bock, Jürgen; Boss, Birgit; Diedrich, Christian; Garrels, Kai; Gatterburg, Andreas Graf; Heidrich, Konrad; Hillermeier, Oliver; Rauscher, Benedikt; Sauer, Manuel; Schmidt, Jan; Werner, Thomas; Zimmermann, Patrick; Plattform Industrie 4.0; VDI/VDE-GMA, 2019. *Verwaltungsschale in der Praxis - Wie definiere ich Teilmodelle, beispielhafte Teilmodelle und Interaktion zwischen Verwaltungsschalen (Version 1.0)*.
Berlin: Bundesministerium für Wirtschaft und Energie (BMWi).
Verfügbar unter: https://www.bmwi.de/Redaktion/DE/Publikationen/Industrie/industrie-4-0-verwaltungsschale-in-der-praxis.pdf?__blob=publicationFile&v=6
Zugriff am: 21.01.2021

Bedner et al. 2010 Bedner, Mark; Ackermann, Tobias, 2010. Schutzziele der IT-Sicherheit.
DuD - Datenschutz und Datensicherheit (10), S. 323–328

Belyaev et al. 2019 Belyaev, Alexander; Diedrich, Christian, 2019. Aktive Verwaltungsschale von I4.0-Komponenten.
In: VDI Wissensforum GmbH (Hrsg.), *AUTOMATION 2019*.
Baden-Baden: VDI Verlag GmbH, S. 517–530

Bettenhausen et al. 2013 Bettenhausen, Kurt D.; Kowalewski, Stefan, 2013. *Cyber-Physical Systems - Chancen und Nutzen aus Sicht der Automation*.
Düsseldorf: Verein Deutscher Ingenieure e.V.
Verfügbar unter: https://www.vdi.de/ueber-uns/presse/publikationen/details/cyber-physical-systems-chancen-und-nutzen-aus-sicht-der-automation
Zugriff am: 21.01.2021

Bezawada et al. 2018 Bezawada, Bruhadeshwar; Bachani, Maalvika; Peterson, Jordan; Shirazi, Hossein; Ray, Indrakshi; Ray, Indrajit, 2018. Behavioral Fingerprinting of IoT Devices.
In: *Proceedings of the 2018 Workshop on Attacks and Solutions in Hardware Security*.
New York: ACM, S. 41–50
ISBN 9781450359962

Bezawada et al. 2019 Bezawada, Bruhadeshwar; Ray, Indrakshi; Ray, Indrajit, 2019. Behavioral fingerprinting of Internet-of-Things devices.
Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery **24**, S. 2

Bindel et al. 2013 Bindel, Thomas; Hofmann, Dieter, 2013. *Projektierung von Automatisierungsanlagen: Eine effektive und anschauliche Einführung*.
2. Aufl.
Wiesbaden: Springer Vieweg.
ISBN 9783834813329

Bitkom 2018 Bitkom, 2018. *Spionage, Sabotage und Datendiebstahl - Wirtschaftsschutz in der Industrie*.
Berlin: Bitkom Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.
Verfügbar unter: https://www.bitkom.org/sites/default/files/file/import/181008-Bitkom-Studie-Wirtschaftsschutz-2018-NEU.pdf
Zugriff am: 21.01.2021

Bitkom et al. 2018 Bitkom; Berg, Achim, 2018. *Industrie 4.0 - Wo steht Deutschland*.
Berlin: Bitkom Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.
Verfügbar unter: https://www.bitkom.org/sites/default/files/file/import/180423-Bitkom-Pressekonferenz-Industrie-40-Praesentation-neu.pdf
Zugriff am: 21.01.2021

Bitkom et al. 2017 Bitkom; F-Secure, 2017. *Status Quo IT-Sicherheit in deutschen Unternehmen*.
Berlin: Bitkom Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.
Verfügbar unter: https://shop.strato.de/WebRoot/Store19/Shops/63742557/59DC/D547/0580/0EF0/5A67/0A0C/6D0A/E059/F-Secure_StatusQuoITSicherheit.pdf
Zugriff am: 21.01.2021

Blake 1978 Blake, Stewart P., 1978. *Managing for Responsive Research and Development*.
1. Aufl.
New York: W.H.Freeman & Co Ltd.
ISBN 9780716700364

Blessing et al. 2009 Blessing, Lucienne T. M.; Chakrabarti, Amaresh, 2009. *DRM, a Design Research Methodology*.
London: Springer.
ISBN 9781848825864

Blowers et al. 2016 Blowers, Misty; Iribarne, Jose; Colbert, Edward J. M.; Kott, Alexander, 2016. In Conclusion: The Future Internet of Things and Security of Its Control Systems.
In: Colbert, Edward J. M., Kott, Alexander (Hrsg.), *Cybersecurity of SCADA and Other Industrial Control Systems*.
1. Aufl.
Cham: Springer, S. 323–355
ISBN 9783319321257

BMBF 2012 BMBF, 2012. *Zukunftsprojekte der Hightech-Strategie (HTS-Aktionsplan)*.
Berlin: Bundesministerium für Bildung und Forschung (BMBF).
Verfügbar unter: https://www.iwbio.de/fileadmin/Publikationen/IWBio-Publikationen/HTS-Aktionsplan.pdf
Zugriff am: 21.01.2021

Bojinov et al. 2014 Bojinov, Hristo; Michalevsky, Yan; Nakibly, Gabi; Boneh, Dan, 2014. *Mobile Device Identification via Sensor Fingerprinting*.
Verfügbar unter: http://arxiv.org/abs/1408.1416
Zugriff am: 21.01.2021

Bortoli 2013 Bortoli, Stefano, 2013. *Knowledge Based Open Entity Matching*.
Trento, University of Trento, Diss., 2013.
DOI: 10.13140/RG.2.2.18554.70088

Bratus et al. 2008 Bratus, Sergey; Cornelius, Cory; Kotz, David; Peebles, Daniel, 2008. Active behavioral fingerprinting of wireless devices.
In: *Proceedings of the first ACM conference on Wireless network security*.
New York: ACM, S. 56–61
ISBN 9781595938145

Bruns et al. 2010 Bruns, Ralf; Dunkel, Jürgen, 2010. Event-Driven Architecture: Softwarearchitektur für ereignisgesteuerte Geschäftsprozesse.
Berlin: Springer.
ISBN 9783642024382

BSI 2006 BSI, 2006. *Pervasive Computing: Entwicklungen und Auswirkungen*.
Bonn: Bundesamt für Sicherheit in der Informationstechnik - BSI.
Verfügbar unter: https://www.internet-sicherheit.de/fileadmin/docs/downloads/andere_studien_dokumente/BSI/2006_Pervasive-Computing.pdf
Zugriff am: 21.01.2021

BSI 2008 BSI, 2008. *Einführung in die technischen Grundlagen der biometrischen Authentisierung*.
Bonn: Bundesamt für Sicherheit in der Informationstechnik - BSI.
Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Biometrie/Technische_Grundlagen_pdf.pdf?__blob=publicationFile&v=1
Zugriff am: 21.01.2021

BSI 2011 BSI, 2011. *Internet-Sicherheit: Einführung, Grundlagen, Vorgehensweise*.
Bonn: Bundesamt für Sicherheit in der Informationstechnik - BSI.
Verfügbar unter: https://www.bsi.bund.de/DE/Themen/StandardsKriterien/ISi-Reihe/ISi-Reihe_node.html
Zugriff am: 21.01.2021

BSI 2012a BSI, 2012. *Industrial Control System Security - Top 10 Bedrohungen*.
Bonn: Bundesamt für Sicherheit in der Informationstechnik - BSI.
Verfügbar unter: https://www.internet-sicherheit.de/fileadmin/docs/downloads/andere_studien_dokumente/BSI/2012-04_Industrial_Control_System_Security.pdf
Zugriff am: 21.01.2021

BSI 2012b BSI, 2012. *Register aktueller Cyber-Gefährdungen und -Angriffsformen*.
Bonn: Bundesamt für Sicherheit in der Informationstechnik - BSI.
Verfügbar unter: https://www.internet-sicherheit.de/fileadmin/docs/downloads/andere_studien_dokumente/BSI/2012-01_Register_aktueller_Cyber-Gefaehrdungen_und_-Angriffsformen.pdf
Zugriff am: 21.01.2021

BSI 2013 BSI, 2013. *Schutz Kritischer Infrastrukturen: Risikoanalyse Krankenhaus-IT*.
Bonn: Bundesamt für Sicherheit in der Informationstechnik - BSI.
Verfügbar unter: https://www.internet-sicherheit.de/fileadmin/docs/downloads/andere_studien_dokumente/BSI/2013-06_Risikoanalyse_Krankenhaus-IT_Langfassung.pdf
Zugriff am: 21.01.2021

BSI 2014 BSI, 2014. *Leitfaden Cyber-Sicherheits-Check - Ein Leitfaden zur Durchführung von Cyber-Sicherheits-Checks in Unternehmen und Behörden*.
Bonn: Bundesamt für Sicherheit in der Informationstechnik - BSI.
Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/ACS/leitfaden_CSC_v2.pdf?__blob=publicationFile&v=3
Zugriff am: 21.01.2021

BSI 2017a BSI, 2017. *Die Lage der IT-Sicherheit in Deutschland 2017*. Bonn: Bundesamt für Sicherheit in der Informationstechnik - BSI. Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2017.pdf?__blob=publicationFile&v=4 Zugriff am: 21.01.2021

BSI 2017b BSI, 2017. *Leitfaden zur Basis-Absicherung nach IT-Grundschutz - In drei Schritten zur Informationssicherheit*. Bonn: Bundesamt für Sicherheit in der Informationstechnik - BSI. Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Leitfaden_zur_Basis-Absicherung.pdf?__blob=publicationFile&v=3 Zugriff am: 21.01.2021

BSI 2018 BSI, 2018. *Industrial Control System Security - Innentäter*. Bonn: Bundesamt für Sicherheit in der Informationstechnik - BSI. Verfügbar unter: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_061.pdf?__blob=publicationFile&v=5

BSI 2019 BSI, 2019. *Industrial Control System Security - Top 10 Bedrohungen und Gegenmaßnahmen 2019*. Bonn: Bundesamt für Sicherheit in der Informationstechnik - BSI. Verfügbar unter: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS/BSI-CS_005.pdf?__blob=publicationFile&v=12 Zugriff am: 21.01.2021

Buchmann et al. 2013 Buchmann, Johannes; Capurro, Rafael; Löw, Martina; Müller, Günter; Pretschner, Alexander; Roßnagel, Alexander; Waidner, Michael; Eldred, Michael; Flender, Christian; Kelbert, Florian; Nagel, Daniel; Nebel, Maxi; Ochs, Carsten; Peters, Martin; Richter, Philipp; Shirazi, Fatemeh; Simo, Hervais; Wüchner, Tobias, 2013. *Internet Privacy: Eine multidisziplinäre Bestandsaufnahme/ A multidisciplinary analysis*.
2012.
Berlin: Springer.
acatech STUDIE.
ISBN 9783642319433

Bullinger et al. 2007 Bullinger, Hans-Jörg; ten Hompel, Michael, 2007. *Internet der Dinge: www.internet-der-dinge.de*.
Berlin: Springer.
ISBN 9783540367291

Bundeskriminalamt 2021 Bundeskriminalamt, 2021. *Cybercrime - Bundeslagebild 2020*.
Wiesbaden: Bundeskriminalamt.
Verfügbar unter: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2020.pdf;jsessionid=0871ACC5CA2C81B7D3A7705AEEF1C000.live2302?__blob=publicationFile&v=4
Zugriff am: 21.05.2021

Bunge 1966 Bunge, Mario, 1966. Technology as Applied Science. *Technology and culture* **7** (3), S. 329–347

Burmeister et al. 2017 Burmeister, Daniel; Burmann, Florian; Schrader, Andreas, 2017. The smart object description language: Modeling interaction capabilities for self-reflection.
In: *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*.
New York: IEEE, S. 503–508

Burmeister et al. 2018 Burmeister, Daniel; Gerlach, Bennet; Schrader, Andreas, 2018. Formal Definition of the Smart Object Matching Problem.
Procedia Computer Science **130**, S. 302–309

Byres 2013 Byres, Eric, 2013. The air gap: SCADA's enduring security myth.
Communications of the ACM **56** (8), S. 29–31

Caliskan et al. 2015 Caliskan, Aylin; Yamaguchi, Fabian; Dauber, Edwin; Harang, Richard; Rieck, Konrad; Greenstadt, Rachel; Narayanan, Arvind, 2015. *When Coding Style Survives Compilation: De-anonymizing Programmers from Executable Binaries*.
Verfügbar unter: http://arxiv.org/abs/1512.08546
Zugriff am: 21.01.2021

Caliskan-Islam et al. 2015 Caliskan-Islam, Aylin; Harang, Richard; Liu, Andrew; Narayanan, Arvind; Voss, Clare; Yamaguchi, Fabian; Greenstadt, Rachel, 2015. De-anonymizing programmers via code stylometry.
In: *24th USENIX Security Symposium (USENIX Security 15)*.
Austin: USENIX Association, S. 255–270

Cao et al. 2017 Cao, Yinzhi; Li, Song; Wijmans, Erik, 2017. (Cross-)Browser Fingerprinting via OS and Hardware Level Features.
In: *Proceedings 2017 Network and Distributed System Security Symposium*.
Reston: Internet Society.
ISBN 9781891562464
DOI: 10.14722/ndss.2017.23152

Cardenas et al. 2009 Cardenas, Alvaro A.; Amin, Saurabh; Sinopoli, Bruno; Giani, Annarita; Perrig, Adrian; Sastry, Shankar, 2009. Challenges for Securing Cyber Physical Systems.
In: *Workshop on Future Directions in Cyber-physical Systems Security*.
Newark: Department of Homeland Security.
Verfügbar unter: https://ptolemy.berkeley.edu/projects/chess/pubs/601/cps-security-challenges.pdf
Zugriff am: 21.01.2021

Castanedo 2013 Castanedo, Federico, 2013. A review of data fusion techniques.
The Scientific World Journal **2013**.
DOI: 10.1155/2013/704504

Centeno et al. 2018 Centeno, Mario Parreño; Guan, Yu; van Moorsel, Aad, 2018. Mobile Based Continuous Authentication Using Deep Features.
In: *Proceedings of the 2nd International Workshop on Embedded and Mobile Deep Learning*.
New York: ACM, S. 19–24
ISBN 9781450358446

Chen et al. 2001 Chen, Mon Chu; Anderson, John R.; Sohn, Myeong Ho, 2001. What can a mouse cursor tell us more? correlation of eye/mouse movements on web browsing.
In: *CHI '01 Extended Abstracts on Human Factors in Computing Systems*.
New York: Association for Computing Machinery, S. 281–282
ISBN 9781581133400

Cho et al. 2014 Cho, Hsin-Hung; Lai, Chin-Feng; Shih, Timothy K.; Chao, Han-Chieh, 2014. Integration of SDR and SDN for 5G.
IEEE Access **2**, S. 1196–1204

Choi et al. 2012 Choi, Sung; Zage, David, 2012. Addressing insider threat using "where you are" as fourth factor authentication.
In: *2012 IEEE International Carnahan Conference on Security Technology (ICCST)*.
New York: IEEE, S. 147–153

Christiaans 2004 Christiaans, Thomas, 2004. Volkswirtschaftslehre als Wissenschaft.
Das Wirtschaftsstudium : wisu ; Zeitschrift für Ausbildung, Prüfung, Berufseinstieg und Fortbildung **33**, S. 1087–1094

Cisco 2019 Cisco, 2019. *Cisco Annual Internet Report (2018–2023)*.
San Jose: Cisco.
Verfügbar unter: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.pdf
Zugriff am: 21.01.2021

Computerwoche 1996 Computerwoche, 1996. Neue Produkte: GSM-Modul M1
Verfügbar unter: https://www.computerwoche.de/a/gsm-modul-m1,1105147
Zugriff am: 21.01.2021

Cooper et al. 2013 Cooper, Alissa; Tschofenig, Hannes; Aboba, Bernard; Peterson, Jon; Morris, J.; Hansen, Marit; Smith, Rhys, 2013. Privacy considerations for internet protocols
Verfügbar unter: https://tools.ietf.org/html/rfc6973
Zugriff am: 21.01.2021

Cozzella 2013 Cozzella, Lorenzo, 2013. *Hylemetric Techniques for Data and Information Security*.
Roma, Università degli studi Roma Tre, Diss., 2013.
Verfügbar unter: http://hdl.handle.net/2307/4523

Cozzella et al. 2012 Cozzella, Lorenzo; Simonetti, Carla; Spagnolo, Giuseppe Schirripa, 2012. Is it possible to use biometric techniques as authentication solution for objects? Biometry vs. hylemetry.
In: *2012 5th International Symposium on Communications, Control and Signal Processing*.
New York: IEEE, S. 1–6

Das et al. 2014 Das, Anupam; Borisov, Nikita; Caesar, Matthew, 2014. Do You Hear What I Hear?: Fingerprinting Smart Devices Through Embedded Acoustic Components.
In: *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*.
New York: ACM, S. 441–452
ISBN 9781450329576

Dasgupta et al. 2017 Dasgupta, Dipankar; Roy, Arunava; Nag, Abhijit, 2017. *Advances in User Authentication*.
Cham: Springer.
ISBN 9783319588063

Dengel 2011 Dengel, Andreas, 2011. *Semantische Technologien: Grundlagen. Konzepte. Anwendungen*.
Wiesbaden: Spektrum Akademischer Verlag.
ISBN 9783827426635

Desmond et al. 2008 Desmond, Loh Chin Choong; Yuan, Cho Chia; Pheng, Tan Chung; Lee, Ri Seng, 2008. Identifying Unique Devices Through Wireless Fingerprinting.
In: *Proceedings of the First ACM Conference on Wireless Network Security*.
New York: ACM, S. 46–55
ISBN 9781595938145

Dey et al. 2014 Dey, Sanorita; Roy, Nirupam; Xu, Wenyuan; Choudhury, Romit Roy; Nelakuditi, Srihari, 2014. AccelPrint: Imperfections of Accelerometers Make Smartphones Trackable.
In: *Proceedings 2014 Network and Distributed System Security Symposium*.
Reston: Internet Society.
DOI: 10.14722/ndss.2014.23059

Dhillon 1997 Dhillon, Gurpreet, 1997. *Managing Information System Security*.
London: MacMillan Press Ltd.
ISBN 9781349144549

Diedrich et al. 2016 Diedrich, Christian; Hadlich, Thomas; Thron, Mario, 2016. Semantik durch Merkmale für Industrie 4.0.
In: Vogel-Heuser, Birgit, Bauernhansl, Thomas, ten Hompel, Michael (Hrsg.), *Handbuch Industrie 4.0: Produktion, Automatisierung und Logistik*.
Berlin: Springer, S. 1–16
ISBN 9783662455371

Diedrich et al. 2019 Diedrich, Christian; Schneider, Karsten; Hodges, Jack; Anicic, Darko; Jankowiak, Frank; Jeong, Eui Suk; Rossi, Gernot; Hu, Yun Chao; Wang, Di; Michahelles, Florian; Jedich, Wolfgang; Lee, Jaeho; Kalhoff, Johannes; Li, Shitao; Kleber, Ulrich; Diller, Juergen; Gao, Kunlun; Chai, Bo; Liu, Weilin; Verheyen, Mark; Knechtel, Martin; Zhuang, Qikai; Yamashita, Lan; Sakuma, Masatake; Lanctot, Peter, 2019. *Semantic interoperability: challenges in the digital transformation age*.
Geneva: IEC.
Verfügbar unter: https://basecamp.iec.ch/download/iec-white-paper-semantic-interoperability-challenges-in-the-digital-transformation-age-en/?wpdmdl=2021&ind=1572438296844
Zugriff am: 21.01.2021

DIN/DKE 2020 DIN/DKE, 2020. 4: DEUTSCHE NORMUNGSROADMAP - Industrie 4.0 - Version 4.
S.l.: DIN e. V.

Dolev et al. 2014 Dolev, Shlomi; Krzywiecki, Łukasz; Panwar, Nisha; Segal, Michael, 2014. Dynamic Attribute Based Vehicle Authentication.
In: *2014 IEEE 13th International Symposium on Network Computing and Applications*.
New York: IEEE, S. 1–8

Dönicke et al. 2018 Dönicke, Nicole; Fritsche, Wolfgang; Gamer, Thomas; Heer, Tobias; Jänicke, Lutz; Jochem, Michael; Klasen, Wolfgang; Lantermann, Thomas; Linke, Lukas; Mehrfeld, Jens; Pfeiffer, Tobias; Teuscher, Andreas; Plattform Industrie 4.0; ZVEI, 2018. *Integrität von Daten, Systemen und Prozessen als Kernelement der Digitalisierung - Teil 1*.
Berlin: Bundesministerium für Wirtschaft und Energie (BMWi).
Verfügbar unter: https://www.plattform-i40.de/PI40/Redaktion/DE/Downloads/Publikation/hm-2018-integritaet-daten.pdf?__blob=publicationFile&v=5
Zugriff am: 21.01.2021

Dorst et al. 2019 Dorst, Wolfgang; Falk, Svenja; Hoffmann, Martin W.; Lehmann-Brauns, Sicco; Löwen, Ulrich; Plass, Christoph; Polenz, Carsten; Possel, Thorsten; Ripperda, Christian; Schmidt, Fabian; Unkelhäußer, Lisa; Plattform Industrie 4.0, 2019. *Digitale Geschäftsmodelle für die Industrie 4.0*.
Berlin: Bundesministerium für Wirtschaft und Energie (BMWi).
Verfügbar unter: https://www.plattform-i40.de/PI40/Redaktion/DE/Downloads/Publikation/digitale-geschaeftsmodelle-fuer-industrie-40.pdf?__blob=publicationFile&v=8
Zugriff am: 21.01.2021

Dorst et al. 2015 Dorst, Wolfgang; Glohr, Carsten; Hahn, Thomas; Knafla, Frank; Loewen, Ulrich; Rosen, Roland; Schiemann, Thomas; Vollmar, Friedrich; Winterhalter, Christoph; Diegner, Bernhard; Diemer, Johannes; Dümmler, Mathias; Erker, Stefan; Herfs, Werner; Hilger, Claus; Jänicke, Lutz; Jasperneite, Jürgen; Kalhoff, Johannes; Kubach, Uwe; Mattis, Georg; Menges, Georg; Mildner, Frank; Quetschlich, Mathias; Steffens, Ernst-Joachim; Stiedl, Thomas; Adolphs, Peter; Bedenbender, Heinz; Ehlich, Martin; Epple, Ulrich; Hankel, Martin; Heidel, Roland; Hoffmeister, Michael; Huhle, Haimo; Kärcher, Bernd; Koziolek, Heiko; Pichler, Reinhold; Pollmeier, Stefan; Schewe, Frank; Schulz, Thomas; Schweichhart, Karsten; Walter, Armin; Waser, Bernd; Wollschlaeger, Martin; Jänicke, Lutz; Jochem, Michael; Kaiser, Hartmut; Kisch, Marcel; Klasen, Wolfgang; Lehmann, Jörn; Linke, Lukas; Mehrfeld, Jens; Sandner, Michael, 2015. *Umsetzungsstrategie Industrie 4.0 - Ergebnisbericht der Plattform Industrie 4.0*.
Berlin: Plattform Industrie 4.0.
Verfügbar unter: https://www.its-owl.de/fileadmin/PDF/Industrie_4.0/2015-04-10_Umsetzungsstrategie_Industrie_4.0_Plattform_Industrie_4.0.pdf
Zugriff am: 21.01.2021

Dresch et al. 2015 Dresch, Aline; Lacerda, Daniel Pacheco; Antunes, José Antônio Valle, Jr, 2015. *Design Science Research: A Method for Science and Technology Advancement*.
Cham: Springer.
ISBN 9783319073736

Dudenredaktion 2019a Dudenredaktion, 2019. Duden | Authentifikation | Rechtschreibung, Bedeutung, Definition, Herkunft
Verfügbar unter: https://www.duden.de/rechtschreibung/Authentifikation
Zugriff am: 21.01.2021

Dudenredaktion 2019b Dudenredaktion, 2019. Duden | Authentifizierung | Rechtschreibung, Bedeutung, Definition, Herkunft
Verfügbar unter: https://www.duden.de/rechtschreibung/Authentifizierung
Zugriff am: 21.01.2021

Dudenredaktion 2019c Dudenredaktion, 2019. Duden | Sicherheit | Rechtschreibung, Bedeutung, Definition, Herkunft
Verfügbar unter: https://www.duden.de/rechtschreibung/Sicherheit
Zugriff am: 21.01.2021

Durand et al. 2019 Durand, Jacques; Hirsch, Frederick; Morrish, Jim; Zarkout, Bassam; Buchheit, Marcellus, 2019. 1: *The Industrial Internet of Things: Managing and Assessing Trustworthiness for IIoT in Practice*.
Needham: Industrial Internet Consortium IIC.
Verfügbar unter: https://www.iiconsortium.org/pdf/Managing_and_Assessing_Trustworthiness_for_IIoT_in_Practice_Whitepaper_2019_07_29.pdf
Zugriff am: 21.01.2021

Dyckhoff 2003 Dyckhoff, Harald, 2003. Grundzüge der Produktionswirtschaft: Einführung in die Theorie betrieblicher Wertschöpfung : mit 98 Abbildungen und 20 Tabellen.
4., verb. Aufl.
Berlin: Springer.
ISBN 9783540440482

Eckersley 2010 Eckersley, Peter, 2010. How Unique Is Your Web Browser?
In: *Privacy Enhancing Technologies*.
Berlin Heidelberg: Springer, S. 1–18

Electronic Frontier Foundation 2019 Electronic Frontier Foundation, 2019. Panopticlick
Verfügbar unter: https://panopticlick.eff.org/
Zugriff am: 21.01.2021

Epple 2011 Epple, Ulrich, 2011. Merkmale als Grundlage der Interoperabilität technischer Systeme.
at - Automatisierungstechnik **59** (7), S. 440–450

Epple et al. 2014 Epple, Ulrich; Bangemann, Thomas; Barbian, Matthias; Bauer, Christian; Braune, Annerose; Diesner, Markus; Friedrich, Jens; Göbe, Florian; Greiner, Thomas; Grüner, Sten; Heidel, Roland; Herfs, Werner; Hesselmann, Klaus; Janßen, Markus; Jasperneite, Jürgen; Kehl, Heinrich; Koziolek, Heiko; Lederer, Albrecht; Lohde, Sven; Loskyll, Matthias; Löwen, Ulrich; Lubnau, Frank; Pfrommer, Julius; Schleipen, Miriam; Schnurrer, Matthias; Traschewski, Holk; Usländer, Thomas; Westerkamp, Clemens; Winter, Albrecht; Wollschlaeger, Martin, 2014. *Industrie 4.0 Gegenstände, Entitäten, Komponenten*.
Düsseldorf: Verein Deutscher Ingenieure e.V.
Verfügbar unter: https://www.vdi.de/ueber-uns/presse/publikationen/details/industrie-40-gegenstaende-entitaeten-komponenten
Zugriff am: 21.01.2021

Evans 2011 Evans, Dave, 2011. *The Internet of Things - How the Next Evolution of the Internet Is Changing Everything*.
San Jose: Cisco.
Verfügbar unter: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf
Zugriff am: 21.01.2021

Faul et al. 2016 Faul, A.; Jazdi, N.; Weyrich, M., 2016. Approach to interconnect existing industrial automation systems with the Industrial Internet.
In: *2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA)*.
New York: s.n., S. 1–4

Feng et al. 2012 Feng, Tao; Liu, Ziyi; Kwon, Kyeong-An; Shi, Weidong; Carbunar, Bogdan; Jiang, Yifei; Nguyen, Nhung, 2012. Continuous mobile authentication using touchscreen gestures.
In: *2012 IEEE Conference on Technologies for Homeland Security (HST)*.
New York: IEEE, S. 451–456

Formby et al. 2016 Formby, David; Srinivasan, Preethi; Leonard, Andrew; Rogers, Jonathan; Beyah, Raheem, 2016. Who's in Control of Your Control System? Device Fingerprinting for Cyber-Physical Systems.
In: *Proceedings 2016 Network and Distributed System Security Symposium*.
Reston: Internet Society.
DOI: 10.14722/ndss.2016.23142

Fortino et al. 2014 Fortino, Giancarlo; Rovella, Anna; Russo, Wilma; Savaglio, Claudio, 2014. On the Classification of Cyberphysical Smart Objects in the Internet of Things.
In: *CEUR Workshop Proceedings*.
Berlin: CEUR-WS.org.
DOI: 10.1.1.662.2882

François et al. 2009 François, Jérôme; Abdelnur, Humberto; State, Radu; Festor, Olivier, 2009. Automated Behavioral Fingerprinting.
In: *Recent Advances in Intrusion Detection*.
Berlin: Springer, S. 182–201

François et al. 2011 François, Jérôme; State, Radu; Engel, Thomas; Festor, Olivier, 2011. Enforcing security with behavioral fingerprinting.
In: *2011 7th International Conference on Network and Service Management*.
New York: IEEE, S. 1–9

Fraunholz et al. 2016 Fraunholz, Daniel; Schneider, Jorg; Anton, Simon Duque; Lipps, Christoph; Schotten, Hans D., 2016. Honeypots for Industrial IoT Applications.
In: *Kleinheubacher Tagung (KH-2016)*.
Miltenberg: U.R.S.I..
Verfügbar unter:
https://www.kh2016.de/KH2016_book_of_abstracts.pdf
Zugriff am: 21.01.2021

Fuchs-Kittowski 2002 Fuchs-Kittowski, Klaus, 2002. Wissens-Ko-Produktion. Verarbeitung, Verteilung und Entstehung von Informationen in kreativ-lernenden Organisationen.
Stufen zur Informationsgesellschaft..
Verfügbar unter: https://www.informatik.uni-leipzig.de/~graebe/Texte/Fuchs-02.pdf
Zugriff am: 21.01.2021

Fulcher et al. 2008 Fulcher, John; Jain, Lakhmi C., 2008. *Computational Intelligence: A Compendium*.
Berlin: Springer.
ISBN 9783540782926

Gao et al. 2010 Gao, Ke; Corbett, Cherita; Beyah, Raheem, 2010. A passive approach to wireless device fingerprinting.
In: *2010 IEEE/IFIP International Conference on Dependable Systems Networks (DSN)*.
New York: IEEE, S. 383–392

Gartner 2017 Gartner, 2017. Gartner Says 8.4 Billion Connected „Things" Will Be in Use in 2017, Up 31 Percent From 2016
Verfügbar unter: https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016
Zugriff am: 06.01.2020

Gebhardt 2019 Gebhardt, Karl Friedrich, 2019. *Prozessautomatisierung*.
Stuttgart: DHBW Stuttgart.
Verfügbar unter: http://wwwlehre.dhbw-stuttgart.de/~kfg/pdv/pdv.pdf
Zugriff am: 21.01.2021

Geisberger et al. 2012 Geisberger, Eva; Broy, Manfred, 2012. *agendaCPS - Integrierte Forschungsagenda Cyber-Physical Systems*.
Berlin: acatech - Deutsche Akademie der Technikwissenschaften e. V.
Verfügbar unter: https://www.acatech.de/publikation/agendacps-integrierte-forschungsagenda-cyber-physical-systems/download-pdf?lang=de
Zugriff am: 21.01.2021

Gevatter et al. 2006 Gevatter, Hans-Jürgen; Grünhaupt, Ulrich, 2006. *Handbuch der Mess- und Automatisierungstechnik in der Produktion*.
Berlin: Springer.
ISBN 9783540212072

Giani 2001 Giani, Annarita, 2001. *Identification with Zero Knowledge Protocols*.
Maryland: SANS Institute.
Verfügbar unter: https://www.sans.org/reading-room/whitepapers/vpns/identification-zero-knowledge-protocols-719
Zugriff am: 21.01.2021

Golfarelli et al. 1997 Golfarelli, Matteo; Maio, Dario; Maltoni, Davide, 1997. On the error-reject trade-off in biometric verification systems. *IEEE transactions on pattern analysis and machine intelligence* **19** (7), S. 786–796

Grant 2007 Grant, Tim, 2007. Quantifying evidence in forensic authorship analysis.
International Journal of Speech Language and the Law **14** (1), S. 1–25

Grassi et al. 2017a Grassi, Paul A.; Fenton, James L.; Lefkovitz, Naomi B.; Danker, Jamie M.; Choong, Yee-Yin; Greene, Kristen K.; Theofanos, Mary F., 2017. *Enrollment and Identity Proofing*.
Gaithersburg: National Institute of Standards and Technology.
DOI: 10.6028/NIST.SP.800-63a

Grassi et al. 2017b Grassi, Paul A.; Fenton, James L.; Newton, Elaine M.; Perlner, Ray A.; Regenscheid, Andrew R.; Burr, William E.; Richer, Justin P.; Lefkovitz, Naomi B.; Danker, Jamie M.; Choong, Yee-Yin; Greene, Kristen K.; Theofanos, Mary F., 2017. *Authentication and Lifecycle Management*.
Gaithersburg: National Institute of Standards and Technology.
DOI: 10.6028/NIST.SP.800-63b

Grassi et al. 2017c Grassi, Paul A.; Garcia, Michael E.; Fenton, James L., 2017. *Digital Identity Guidelines*.
Gaithersburg: National Institute of Standards and Technology.
DOI: 10.6028/NIST.SP.800-63-3

Grassi et al. 2017d Grassi, Paul A.; Richer, Justin P.; Squire, Sarah K.; Fenton, James L.; Nadeau, Ellen M.; Lefkovitz, Naomi B.; Danker, Jamie M.; Choong, Yee-Yin; Greene, Kristen K.; Theofanos, Mary F., 2017. *Federation and Assertions*. Gaithersburg: National Institute of Standards and Technology. DOI: 10.6028/NIST.SP.800-63c

Gray et al. 2017 Gray, Nicholas; Zinner, Thomas; Tran-Gia, Phuoc, 2017. Enhancing SDN security by device fingerprinting. In: *2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*. New York: IEEE, S. 879–880

Greenwald et al. 2007 Greenwald, Lloyd G.; Thomas, Tavaris J., 2007. Understanding and preventing network device fingerprinting. *Bell Labs technical journal* **12** (3), S. 149–166

Greer et al. 2019 Greer, Christopher; Burns, Martin; Wollman, David; Griffor, Edward, 2019. *Cyber-physical systems and internet of things*. Gaithersburg: National Institute of Standards and Technology (NIST). DOI: 10.6028/NIST.SP.1900-202

Gregor et al. 2012 Gregor, Shirley; Baskerville, Richard, 2012. The fusion of design science and social science research. In: *Information Systems Foundation Workshop*. Canberra: s.n.. Verfügbar unter: https://www.rsm.anu.edu.au/media/1029778/Gregor-Baskerville-ISF-2012-The-Fusion-of-Design-Science-and-Social-Science-Research.pdf Zugriff am: 21.01.2021

Gregor et al. 2013 Gregor, Shirley; Hevner, Alan R., 2013. Positioning and Presenting Design Science Research for Maximum Impact. *The Mississippi quarterly* **37** (2), S. 337–355

Grote et al. 2014 Grote, Karl-Heinrich; Engelmann, Frank; Beitz, Wolfgang; Syrbe, Max; Beyerer, Jürgen; Spur, Günter, 2014. *Das Ingenieurwissen: Entwicklung, Konstruktion und Produktion*.
Berlin: Springer Vieweg.
ISBN 9783662443927

Guidorizzi 2012 Guidorizzi, Richard, 2012. *Active Authentication: Moving Beyond Passwords - SECOND ROUND TABLE: From Biometric To Augmented Human Recognition*.
Arlington: DARPA.
Verfügbar unter: http://www.tabularasa-euproject.org/project/pdf/Richard%20Guidorizzi
Zugriff am: 21.01.2021

Guidorizzi 2013 Guidorizzi, Richard P., 2013. Security: Active Authentication.
IT professional **15** (4), S. 4–7

Günther et al. 2011 Günther, Hans-Otto; Tempelmeier, Horst, 2011. *Produktion und Logistik*.
9., akt.erw. Aufl.
Berlin: Springer.
ISBN 9783642251641

Gurgen et al. 2013 Gurgen, Levent; Gunalp, Ozan; Benazzouz, Yazid; Gallissot, Mathieu, 2013. Self-aware cyber-physical systems and applications in smart buildings and cities.
In: *2013 Design, Automation Test in Europe Conference Exhibition (DATE)*.
New York: IEEE, S. 1149–1154

Gutenberg 1951 Gutenberg, Erich, 1951. *Grundlagen der Betriebswirtschaftslehre*.
1. Aufl.
Berlin: Springer.
ISBN 9783662219669

Haas 2016 Haas, Andreas, 2016. Management von Cyber-Risiken und Möglichkeiten des Risikotransfers : eine ökonomische und versicherungstechnische Analyse.
Hohenheim, Universität Hohenheim, Diss., 2016.
URN: urn:nbn:de:bsz:100-opus-11925

Hahn 2016 Hahn, Adam, 2016. Operational Technology and Information Technology in Industrial Control Systems. In: Colbert, Edward J. M., Kott, Alexander (Hrsg.), *Cybersecurity of SCADA and Other Industrial Control Systems*. 1. Aufl. Cham: Springer, S. 51–68 ISBN 9783319321257

Heidel et al. 2017 Heidel, Roland; Hankel, Martin; Döbrich, Udo; Hoffmeister, Michael, 2017. *Basiswissen RAMI 4.0: Referenzarchitekturmodell und Industrie 4.0-Komponente Industrie 4.0*. 1. Aufl. Berlin: Beuth Verlag. ISBN 9783410264828

Heidrich et al. 2016 Heidrich, Mike; Luo, Jesse Jijun, 2016. *Industrial Internet of things: Referenzarchitektur für die Kommunikation*. München: Fraunhofer Gesellschaft. Verfügbar unter: https://www.iks.fraunhofer.de/content/dam/esk/dokumente/Whitepaper_IoT_dt_April16.pdf Zugriff am: 21.01.2021

Heinen 1985 Heinen, Edmund, 1985. *Einführung in die Betriebswirtschaftslehre*. 9., verb. Aufl. Wiesbaden: Gabler Verlag. ISBN 9783322829290

Heinrich et al. 2015 Heinrich, Berthold; Linke, Petra; Glöckler, Michael, 2015. *Grundlagen Automatisierung: Sensorik, Regelung, Steuerung*. Wiesbaden: Springer Vieweg. ISBN 9783658059606

Heinze et al. 2015 Heinze, Ronald; Manzei, Christian; Schleupner, Linus, 2015. *Industrie 4.0 im internationalen Kontext: Kernkonzepte, Ergebnisse, Trends*. 2., vollst. neu bearb. Aufl. Berlin: Beuth Verlag. ISBN 9783410260493

Helmus et al. 2009 Helmus, Manfred; Meins-Becker, Anica; Laußat, Lars; Kelm, Agnes, 2009. RFID in der Baulogistik: Forschungsbericht zum Projekt „Integriertes Wertschöpfungsmodell mit RFID in der Bau- und Immobilienwirtschaft".
1. Aufl.
Wiesbaden: Vieweg +Teubner.
ISBN 9783834807656

Hevner et al. 2004 Hevner, Alan R.; March, Salvatore T.; Park, Jinsoo; Ram, Sudha, 2004. Design Science in Information Systems Research.
The Mississippi quarterly **28** (1), S. 75–105

Hill et al. 2012 Hill, Richard; Hirsch, Laurie; Lake, Peter; Moshiri, Siavash, 2012. *Guide to Cloud Computing: Principles and Practice*.
London: Springer.
ISBN 9781447146025

Hilty et al. 2003 Hilty, Lorenz; Behrendt, Siegfried; Binswanger, Mathias; Bruinink, Arend; Erdmann, Lorenz; Fröhlich, Jürg; Köhler, Andreas; Kuster, Niels; Som, Claudia; Würtenberger, Felix, 2003. *Das Vorsorgeprinzip in der Informationsgesellschaft: Auswirkungen des Pervasive Computing auf Gesundheit und Umwelt*.
Bern: TA-Swiss, Zentrum für Technologiefolgen-Abschätzung.
ISBN 9783908174066

Hippenmeyer et al. 2017 Hippenmeyer, Heinrich; Moosmann, Thomas, 2017. *Automatische Identifikation für Industrie 4.0*.
Berlin: Springer.
ISBN 9783662527009

Hoang et al. 2016 Hoang, Xuan Luu; Fay, Alexander; Marks, Philipp; Weyrich, Michael, 2016. Systematization approach for the adaptation of manufacturing machines.
In: *2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA)*.
New York: s.n., S. 1–4

Höffe 2006 Höffe, Otfried, 2006. *Aristoteles*.
München: C.H.Beck.
ISBN 9783406541254

Holtewert et al. 2013 Holtewert, Philipp; Wutzke, Rolf; Seidelmann, Joachim; Bauernhansl, Thomas, 2013. Virtual Fort Knox Federative, Secure and Cloud-based Platform for Manufacturing. *Procedia CIRP* **7**, S. 527–532

Hölz 2018 Hölz, Maximilian, 2018. Gebrauchssicherheit, Funktionale Sicherheit, Angriffssicherheit - Anforderungen, Methoden und Synergien.
Stuttgart: Universität Stuttgart.
Masterarbeit, 2018.

Horvath et al. 2012 Horvath, Imre; Gerritsen, Bart H. M., 2012. Cyber-physical systems: Concepts, technologies and implementation principles.
In: *Proceedings of the ninth international symposium on tools and methods of competitive engineering - TCME-2012*.
Karlsruhe: Delft University of Technology, Netherlands and KIT, Germany, S. 19–36

Hunt et al. 2020 Hunt, Galen; Letey, George; Nightingale, Edmund B., 2020. *The Seven Properties of Highly Secured Devices (2nd Edition)*.
Redmond: Microsoft.
Verfügbar unter: https://www.microsoft.com/en-us/research/uploads/prod/2020/11/Seven-Properties-of-Highly-Secured-Devices-2nd-Edition-R1.pdf
Zugriff am: 21.01.2021

Hupperich et al. 2015 Hupperich, Thomas; Maiorca, Davide; Kührer, Marc; Holz, Thorsten; Giacinto, Giorgio, 2015. On the Robustness of Mobile Device Fingerprinting: Can Mobile Users Escape Modern Web-Tracking Mechanisms?
In: *Proceedings of the 31st Annual Computer Security Applications Conference*.
Los Angeles: ACM, S. 191–200
ISBN 9781450336826

IBM 2001 IBM, 2001. *Autonomic computing: IBM's Perspective on the State of Information Technology*.
Armonk: IBM.
Verfügbar unter: https://people.scs.carleton.ca/~soma/biosec/readings/autonomic_computing.pdf
Zugriff am: 21.01.2021

IBM 2003 IBM, 2003. *Introduction to Pervasive Computing for Business Partners - IBM's Pervasive Computing Strategy*.
Armonk: IBM.
Verfügbar unter: ftp://ftp.software.ibm.com/software/pervasive/info/BPIntro.pdf
Zugriff am: 21.01.2021

Jain et al. 2005 Jain, A. K.; Bolle, Ruud M.; Pankanti, Sharath, 2005. *Biometrics: Personal Identification in Networked Society*.
1. Aufl.
New York: Springer.
ISBN 9780387285399

Jain et al. 2004 Jain, Anil K.; Ross, Arun, 2004. Multibiometric systems. *Communications of the ACM* **47** (1), S. 34–40

Jajodia et al. 2014 Jajodia, Sushil; Kant, Krishna; Samarati, Pierangela; Singhal, Anoop; Swarup, Vipin; Wang, Cliff, 2014. *Secure Cloud Computing*.
New York: Springer.
ISBN 9781461492771

Jänicke et al. 2016 Jänicke, Lutz; Jochem, Michael; Kaiser, Hartmut; Klasen, Wolfgang; Klimke, Martin; Kosch, Bernd; Linke, Lukas; Mehrfeld, Jens; Nitschke, Torsten; Sandner, Michael; Stoltz, Mario; Walloschke, Thomas; Zimmermann, Steffen; Plattform Industrie 4.0, 2016. *Technischer Überblick: Sichere Identitäten*.
Berlin: Bundesministerium für Wirtschaft und Energie (BMWi).
Verfügbar unter: https://www.plattform-i40.de/PI40/Redaktion/DE/Downloads/Publikation/sichere-identitaeten.pdf?__blob=publicationFile&v=11
Zugriff am: 21.01.2021

Jasperneite 2011 Jasperneite, Juergen, 2011. *Safety und Security für sichere technische Systeme*.
Lemgo: Fraunhofer IOSB-INA.

Jeschke et al. 2017 Jeschke, Sabina; Brecher, Christian; Song, Houbing; Rawat, Danda B., 2017. *Industrial Internet of Things: Cybermanufacturing Systems*.
Cham: Springer.
ISBN 9783319425580

Jeschke et al. 2014 Jeschke, Sabina; Kobbelt, Leif; Dröge, Alicia, 2014. *Exploring Virtuality: Virtualität im interdisziplinären Diskurs*.
Wiesbaden: Springer Spektrum.
ISBN 9783658038847

Jin et al. 2004 Jin, Andrew Teoh Beng; Ling, David Ngo Chek; Goh, Alwyn, 2004. Biohashing: two factor authentication featuring fingerprint data and tokenised random number.
Pattern recognition **37** (11), S. 2245–2255

Jirkovský et al. 2018 Jirkovský, V.; Obitko, M.; Kadera, P.; Mařík, V., 2018. Toward Plug & Play Cyber-Physical System Components.
IEEE Transactions on Industrial Informatics **14** (6), S. 2803–2811

Jose et al. 2016 Jose, Arun Cyril; Malekian, Reza; Ye, Ning, 2016. Improving Home Automation Security; Integrating Device Fingerprinting Into Smart Home.
IEEE Access **4**, S. 5776–5787

Jung et al. 2019 Jung, Tobias; Weyrich, Michael, 2019. Synchronization of a "Plug-and-Simulate"-capable Co-Simulation of Internet-of-Things-Components.
Procedia CIRP **79**, S. 367–372

Kagermann et al. 2016 Kagermann, Henning; Anderl, Reiner; Gausemeier, Jürgen; Schuh, Günther; Wahlster, Wolfgang, 2016. *Industrie 4.0 im globalen Kontext - Strategien der Zusammenarbeit mit internationalen Partnern*.
Berlin: Acatech.
Verfügbar unter: https://www.acatech.de/publikation/industrie-4-0-im-globalen-kontext-strategien-der-zusammenarbeit-mit-internationalen-partnern/download-pdf?lang=de
Zugriff am: 21.01.2021

Kagermann et al. 2013 Kagermann, Henning; Wahlster, Wolfgang; Helbig, Johannes, 2013. *Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0 - Abschlussbericht*.
Berlin: acatech - Deutsche Akademie der Technikwissenschaften e.V.
Verfügbar unter: https://www.acatech.de/wp-content/uploads/2018/03/Abschlussbericht_Industrie4.0_barrierefrei.pdf
Zugriff am: 21.01.2021

Kaplan et al. 1981 Kaplan, Stanley; Garrick, B. John, 1981. On The Quantitative Definition of Risk.
Risk analysis: an official publication of the Society for Risk Analysis **1** (1), S. 11–27

Kappes 2013 Kappes, Martin, 2013. *Netzwerk- und Datensicherheit: Eine praktische Einführung*.
Wiesbaden: Springer Vieweg.
ISBN 9783834806369

Karnouskos 2011 Karnouskos, Stamatis, 2011. Stuxnet worm impact on industrial cyber-physical system security.
In: *IECON 2011 - 37th Annual Conference of the IEEE Industrial Electronics Society*.
New York: IEEE, S. 4490–4494

Kautz 1996 Kautz, Wolf-Eckhard, 1996. Produktionsplanungs- und -steuerungssysteme: Konzept zur technisch-ökonomisch begründeten Auswahl.
Wiesbaden: Gabler Verlag.
ISBN 9783409135221

Keller et al. 2019 Keller, Ivo; Holl, Friedrich-L, 2019. Kriterien: Wie Security auch für Safety verantwortlich wird - Safety-Inseln im Security-Komplex.
Datenschutz und Datensicherheit - DuD **43** (7), S. 426–433

Kephart et al. 2003 Kephart, Jeffrey O.; Chess, David M., 2003. The vision of autonomic computing.
Computer **36** (1), S. 41–50

Kiefer et al. 2019 Kiefer, Lucas; Voit, Patrick; Richter, Christoph; Reinhart, Gunther, 2019. Attribute-based identification processes for autonomous manufacturing systems – an approach for the integration in factory planning methods.
Procedia CIRP **79**, S. 204–209

Kieseberg et al. 2018 Kieseberg, Peter; Weippl, Edgar, 2018. Security Challenges in Cyber-Physical Production Systems.
In: *Software Quality: Methods and Tools for Better Software and Systems*.
Cham: Springer, S. 3–16

Kirkpatrick et al. 2009 Kirkpatrick, Michael S.; Bertino, Elisa; Sheldon, Frederick T., 2009. Restricted Authentication and Encryption for Cyber-physical Systems.
In: *DHS S&T: Workshop on Future Directions in Cyber-physical Systems Security*.
Newark: Department of Homeland Security.
Verfügbar unter: https://w3.cs.jmu.edu/kirkpams/papers/cps09-physrestcps.pdf
Zugriff am: 21.01.2021

Knoblich 1969 Knoblich, Hans, 1969. Allgemeines über die typologische Betrachtungsweise in der Betriebswirtschaftslehre.
In: Knoblich, Hans (Hrsg.), *Betriebswirtschaftliche Warentypologie: Grundlagen und Anwendungen*.
Wiesbaden: VS Verlag für Sozialwissenschaften, S. 24–41
ISBN 9783663023692

Kohno et al. 2005 Kohno, Tadayoshi; Broido, Andre; Claffy, Kimberly C., 2005. Remote physical device fingerprinting.
IEEE Transactions on Dependable and Secure Computing **2** (2), S. 93–108

Kopetz et al. 2016 Kopetz, Hermann; Bondavalli, Andrea; Brancati, Francesco; Frömel, Bernhard; Höftberger, Oliver; Iacob, Sorin, 2016. Emergence in Cyber-Physical Systems-of-Systems (CPSoSs).
In: Bondavalli, Andrea, Bouchenak, Sara, Kopetz, Hermann (Hrsg.), *Cyber-Physical Systems of Systems: Foundations – A Conceptual Model and Some Derivations: The AMADEOS Legacy*.
Cham: Springer, S. 73–96
ISBN 9783319475905

Kortuem et al. 2009 Kortuem, Gerd; Kawsar, Fahim; Fitton, Daniel; Sundramoorthy, Vasughi, 2009. Smart objects as building blocks for the internet of things.
IEEE Internet Computing **14** (1), S. 44–51

Krämer 2002 Krämer, Klaus, 2002. Automatisierung in Materialfluss und Logistik: Ebenen, Informationslogistik, Identifikationssysteme, intelligente Geräte.
1. Aufl.
Wiesbaden: Deutscher Universitätsverlag.
ISBN 9783824421527

Kruger et al. 2014 Kruger, Dan; Carbone, John N., 2014. Radically simplifying cyber security.
In: *Applied Cyber-Physical Systems*.
New York: Springer, S. 51–61
ISBN 9781461473350

Kuhn 2017 Kuhn, Thomas S., 2017. *Die Struktur wissenschaftlicher Revolutionen*.
Berlin: Suhrkamp Verlag.
ISBN 9783518276259

Kuhn et al. 2019a Kuhn, Thomas; Schnicke, Frank; Ziesche, Constantin, 2019. Gut verpackt - BaSys-Tutorial, Teil 2: Verwaltungsschalen und Teilmodelle mit der BaSyx-SDK definieren.
iX **2019** (12), S. 132–142

Kuhn et al. 2019b Kuhn, Thomas; Schnicke, Frank; Ziesche, Constantin, 2019. In Bewegung - Tutorial, Teil 1: BaSys und Eclipse BaSyx – Middleware für die wandelbare Produktion.
iX **2019** (11), S. 56–62

Lalithamani et al. 2017 Lalithamani, N.; Raam Balaji, D.; Dev, Svpkh Satya, 2017. Survey on nonobstructive and continuous user authentication on mobile devices.
In: *2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS)*.
New York: IEEE, S. 1–6

Lam et al. 2016 Lam, Kwok-Yan; Chi, Chi-Hung, 2016. Identity in the Internet-of-Things (IoT): New Challenges and Opportunities.
In: *Information and Communications Security*.
Cham: Springer, S. 18–26

Landoll 2011 Landoll, Douglas, 2011. Information Security Risk Assessment Basics.
In: Andress, Jason, Winterfeld, Steven (Hrsg.), *The Security Risk Assessment Handbook*.
2. Aufl.
Waltham: CRC Press, S. 23–37
ISBN 9781439821480

Lanze et al. 2012 Lanze, Fabian; Panchenko, Andriy; Braatz, Benjamin; Zinnen, Andreas, 2012. Clock skew based remote device fingerprinting demystified.
In: *2012 IEEE Global Communications Conference (GLOBECOM)*.
New York: IEEE, S. 813–819

Lassmann 2006 Lassmann, Wolfgang, 2006. *Wirtschaftsinformatik: Nachschlagewerk für Studium und Praxis*.
1. Aufl.
Wiesbaden: Gabler Verlag.
ISBN 9783409127257

Lazarsfeld 1937 Lazarsfeld, Paul F., 1937. Some Remarks on the Typological Procedures in Social Research.
Zeitschrift für Sozialforschung **6** (1), S. 119–139

Lee 2006 Lee, Edward A., 2006. Cyber-Physical Systems - Are Computing Foundations Adequate?
In: *NSF Workshop On Cyber-Physical Systems: Research Motivation, Techniques and Roadmap*.
Austin: UC Berkeley.
Verfügbar unter: https://ptolemy.berkeley.edu/publications/papers/06/CPSPositionPaper/Lee_CPS_PositionPaper.pdf
Zugriff am: 21.01.2021

Lee et al. 2017 Lee, Edward A.; Seshia, Sanjit A., 2017. *Introduction to Embedded Systems: A Cyber-Physical Systems Approach*. 1. Aufl.
Cambridge: MIT Press.
ISBN 9780262533812

Lee 2003 Lee, Spencer C., 2003. *An introduction to identity management*.
Bethesda: SANS Institute.
Verfügbar unter: https://www.sans.org/reading-room/whitepapers/authentication/introduction-identity-management-852
Zugriff am: 19.12.2019

Lehmann 2011 Lehmann, Christian, 2011. Typologie vs. Klassifikation
Verfügbar unter: https://www.christianlehmann.eu/ling/typ/typ_vs_klasse.php
Zugriff am: 21.01.2021

Lin et al. 2019 Lin, Shi-Wan; Miller, Bradford; Durand, Jacques; Bleakley, Graham; Chigani, Amine; Martin, Robert; Murphy, Brett; Crawford, Mark; IIC, 2019. *The Industrial Internet of Things Volume G1: Reference Architecture - IIRA*.
Needham: Industrial Internet Consortium.
Verfügbar unter: https://www.iiconsortium.org/pdf/IIRA-v1.9.pdf
Zugriff am: 21.01.2021

Lucke 2013 Lucke, Dominik, 2013. Smart Factory.
In: Westkämper, Engelbert, Spath, Dieter, Constantinescu, Carmen, Lentes, Joachim (Hrsg.), *Digitale Produktion*.
Berlin: Springer Vieweg, S. 251–269

Lucke et al. 2008 Lucke, Dominik; Constantinescu, Carmen; Westkämper, Engelbert, 2008. Smart Factory - A Step towards the Next Generation of Manufacturing.
In: Mitsuishi, Mamoru, Ueda, Kanji, Kimura, Fumihiko (Hrsg.), *Manufacturing Systems and Technologies for the New Frontier*.
London: Springer, S. 115–118

Maes et al. 2010 Maes, Roel; Verbauwhede, Ingrid, 2010. Physically Unclonable Functions: A Study on the State of the Art and Future Research Directions.
In: Sadeghi, Ahmad-Reza, Naccache, David (Hrsg.), *Towards Hardware-Intrinsic Security: Foundations and Practice*.
Berlin: Springer, S. 3–37
ISBN 9783642144523

Maheshwari et al. 2013 Maheshwari, Ketan; Lim, Marcus; Wang, Lydia; Birman, Ken; van Renesse, Robbert, 2013. Toward a reliable, secure and fault tolerant smart grid state estimation in the cloud.
In: *2013 IEEE PES Innovative Smart Grid Technologies Conference (ISGT)*.
New York: IEEE, S. 1–6

Mandl 2014 Mandl, Peter, 2014. Grundkurs Betriebssysteme: Architekturen, Betriebsmittelverwaltung, Synchronisation, Prozesskommunikation, Virtualisierung.
Wiesbaden: Springer Vieweg.
ISBN 9783658062170

Manning 2018 Manning, Paul Eugene, 2018. Device fingerprinting identification and authentication: A two-fold use in multi-factor access control schemes.
Ames: Iowa State University.
Masterarbeit, 2018.
DOI: 10.31274/etd-180810-5595

Markou 2016 Markou, Christina, 2016. Behavioural Advertising and the New 'EU Cookie Law' as a Victim of Business Resistance and a Lack of Official Determination.
In: Gutwirth, Serge, Leenes, Ronald, De Hert, Paul (Hrsg.), *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*.
Dordrecht: Springer, S. 213–247
ISBN 9789401773751

Mattern 2004 Mattern, Friedemann, 2004. Ubiquitous Computing: Schlaue Alltagsgegenstände - Die Vision von der Informatisierung des Alltags.
Bulletin SEV/VSE (Verband Schweizerischer Elektrizitätsunternehmen) **95** (19), S. 9–12

Mcafee Labs 2018 Mcafee Labs, 2018. Bedrohungsprognosen von McAfee Labs für 2019 | McAfee Blogs
Verfügbar unter: https://www.mcafee.com/blogs/languages/german/bedrohungsprognosen-von-mcafee-labs-fur-2019/
Zugriff am: 06.01.2020

McCarthy 1980 McCarthy, John, 1980. Circumscription - A form of non-monotonic reasoning.
Artificial intelligence **13** (1–2), S. 27–39

Meinel et al. 2014 Meinel, Christoph; Sack, Harald, 2014. *Sicherheit und Vertrauen im Internet: Eine technische Perspektive*.
Wiesbaden: Springer Vieweg.
ISBN 9783658048334

Menz et al. 2015 Menz, Nadja; Hoepner, Petra; Tiemann, Jens; Koußen, Frank, 2015. *S2: Safety und Security aus dem Blickwinkel der öffentlichen IT*.
Berlin: Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS.
Verfügbar unter: https://www.oeffentliche-it.de/documents/10181/14412/Safety+und+Security+aus+dem+Blickwinkel+der+%C3%B6ffentlichen+IT
Zugriff am: 21.01.2021

Meseke et al. 2019 Meseke, Bodo; Kuhlee, Lorenz; Greiner, Jens, 2019. *Datenklau: virtuelle Gefahr, reale Schäden - Ergebnisse einer Befragung von 453 deutschen Unternehmen*.
Eschborn: Ernst & Young.
Verfügbar unter: https://assets.ey.com/content/dam/ey-sites/ey-com/de_de/news/2019/12/ey-datenklau-studie-2019.pdf?download
Zugriff am: 21.01.2021

Mezgár et al. 2014 Mezgár, István; Rauschecker, Ursula, 2014. The challenge of networked enterprises for cloud computing interoperability.
Computers in Industry **65** (4), S. 657–674

Michael et al. 2013 Michael, Behrens; Roth, Richard, 2013. *Biometrische Identifikation: Grundlagen, Verfahren, Perspektiven*.
1. Aufl.
Wiesbaden: Vieweg+Teubner Verlag.
ISBN 9783322908445

Miettinen et al. 2017 Miettinen, Markus; Marchal, Samuel; Hafeez, Ibbad; Asokan, N.; Sadeghi, Ahmad-Reza; Tarkoma, Sasu, 2017. IoT SENTINEL: Automated device-type identification for security enforcement in IoT.
In: *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*.
New York: IEEE.
ISBN 9781538617922
DOI: 10.1109/icdcs.2017.283

Minerva et al. 2015 Minerva, Roberto; Biru, Abyi; Rotondi, Domenico, 2015. *Towards a definition of the Internet of Things (IoT)*.
New York: IEEE Internet Initiative.
Verfügbar unter: https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Issue1_14MAY15.pdf
Zugriff am: 21.01.2021

Monostori et al. 2016 Monostori, L.; Kádár, B.; Bauernhansl, T.; Kondoh, S.; Kumara, S.; Reinhart, G.; Sauer, O.; Schuh, G.; Sihn, W.; Ueda, K., 2016. Cyber-physical systems in manufacturing. *CIRP Annals - Manufacturing Technology* **65** (2), S. 621–641

Müller-Schloer et al. 2004 Müller-Schloer, Christian; von der Malsburg, Christoph; Würt, Rolf P., 2004. Organic Computing.
Informatik-Spektrum **27** (4), S. 332–336

Nagel et al. 2013 Nagel, Kurt; Piller, Frank; Erben, Roland, 2013. *Produktionswirtschaft 2000: Perspektiven für die Fabrik der Zukunft*.
1. Aufl.
Wiesbaden: Gabler Verlag.
ISBN 9783322894823

Nakibly et al. 2015 Nakibly, Gabi; Shelef, Gilad; Yudilevich, Shiran, 2015. *Hardware Fingerprinting Using HTML5*.
Verfügbar unter: http://arxiv.org/abs/1503.01408

Narayanan 2008 Narayanan, Arvind, 2008. About 33 Bits
Verfügbar unter: https://33bits.wordpress.com/about/
Zugriff am: 21.01.2021

Nespoli et al. 2018 Nespoli, Pantaleone; Zago, Mattia; Celdran, Alberto Huertas; Perez, Manuel Gil; Marmol, Felix Gomez; Garcia Clemente, Felix J., 2018. A Dynamic Continuous Authentication Framework in IoT-Enabled Environments.
In: *2018 Fifth International Conference on Internet of Things: Systems, Management and Security*.
New York: IEEE, S. 131–138

Neumann et al. 2014 Neumann, Christoph; Heen, Olivier; Onno, Stéphane, 2014. *An empirical study of passive 802.11 Device Fingerprinting*.
Verfügbar unter: http://arxiv.org/abs/1404.6457
Zugriff am: 21.01.2021

Nikiforakis et al. 2013 Nikiforakis, Nick; Kapravelos, Alexandros; Joosen, Wouter; Kruegel, Christopher; Piessens, Frank; Vigna, Giovanni, 2013. Cookieless Monster: Exploring the Ecosystem of Web-Based Device Fingerprinting.
In: *2013 IEEE Symposium on Security and Privacy*.
New York: IEEE, S. 541–555

Nikiforakis et al. 2014 Nikiforakis, Nick; Kapravelos, Alexandros; Joosen, Wouter; Kruegel, Christopher; Piessens, Frank; Vigna, Giovanni, 2014. On the Workings and Current Practices of Web-Based Device Fingerprinting.
IEEE Security Privacy **12** (3), S. 28–36

Norm DIN 6763 DIN 6763:1985-12.
Nummerung; Grundbegriffe.

Norm DIN EN 61360-1 DIN EN 61360-1.
Genormte Datenelementtypen mit Klassifikationsschema für elektrische Bauteile - Teil 1: Definitionen - Regeln und Methoden (IEC 61360-1:2002 + A1:2003); Deutsche Fassung EN 61360-1:2002 + A1:2004.

Norm DIN EN ISO 6385 DIN EN ISO 6385:2004-05.
Grundsätze der Ergonomie für die Gestaltung von Arbeitssystemen.

Norm DIN SPEC 91345 DIN SPEC 91345.
Reference Architecture Model Industrie 4.0 (RAMI4.0).

Norm DIN SPEC 92000 DIN SPEC 92000.
Datenaustausch auf der Grundlage von Eigenschaftsausprägungsaussagen - Data Exchange on the Base of Property Value Statements.

Norm IEC 62443-4-1 IEC 62443-4-1.
Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements.

Norm IEC 62714-1 IEC 62714-1:2018.
Engineering data exchange format for use in industrial automation systems engineering - Automation Markup Language - Part 1: Architecture and general requirements.

Norm IEC/TS 62443-1-1 IEC/TS 62443-1-1.
Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models.

Norm ISO TS 29002-10 ISO TS 29002-10:2009(R2015).
Industrial automation systems and integration - Exchange of characteristic data - Part 10: Characteristic data exchange format.

Norm ISO/IEC 9594-8 ISO/IEC 9594-8:2017.
Information technology - Open Systems Interconnection - The Directory - Part 8: Public-key and attribute certificate frameworks.

Norm ISO/IEC 10746-2 ISO/IEC 10746-2.
Information technology - Open distributed processing - Reference model: Foundations.

Norm ISO/IEC 13335-1 ISO/IEC 13335-1:2004.
Information technology - Security techniques - Management of information and communications technology security - Part 1: Concepts and models for information and communications technology security management.

Norm ISO/IEC 19763-3 ISO/IEC 19763-3:2010.
Information technology - Metamodel framework for interoperability (MFI) - Part 3: Metamodel for ontology registration.

Norm ISO/IEC 24760-1 ISO/IEC 24760-1.
Information technology - Security techniques - A framework for identity management - Part 1: Terminology and concepts.

Norm ISO/IEC 24760-2 ISO/IEC 24760-2.
Information technology - Security techniques - A framework for identity management - Part 2: Reference architecture and requirements.

Norm ISO/IEC 24760-3 ISO/IEC 24760-3.
Information technology - Security techniques - A framework for identity management - Part 3: Practice.

Norm ISO/IEC 27002 ISO/IEC 27002.
Information technology - Security techniques - Code of practice for information security management.

Norm ISO/IEC 29115 ISO/IEC 29115.
Information technology - Security techniques - Entity authentication assurance framework.

Norm ISO/IEC CD 21823-3 ISO/IEC CD 21823-3:2018(E).
Internet of Things (IoT) - Interoperability for IoT Systems - Part 3: Semantic interoperability.

Norm ISO/IEC GUIDE 77-2 ISO/IEC GUIDE 77-2:2008.
Guide for specification of product properties and classes - Part 2: Technical principles and guidance.

Norm ISO/IEC TR 23188 ISO/IEC TR 23188:2020.
Information technology - Cloud computing - Edge computing landscape.

Norm ITU-TX.509 ITU-TX.509.
Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks Recommendation.

Norm RFC 3986 RFC 3986.
Uniform Resource Identifier (URI).
Verfügbar unter: https://tools.ietf.org/html/rfc3986
Zugriff am: 01.12.2021

Norm RFC 3987 RFC 3987.
Internationalized resource identifiers (IRIs).
Verfügbar unter: https://tools.ietf.org/html/rfc3987
Zugriff am: 01.12.2021

Norm VDI 2870 Blatt 1 VDI 2870 - Blatt 1.
Ganzheitliche Produktionssysteme - Grundlagen, Einführung und Bewertung.

Norm VDI 5600 Blatt 3 VDI 5600 Blatt 3.
Fertigungsmanagementsysteme (Manufacturing Execution Systems - MES) - Logische Schnittstellen zur Maschinen- und Anlagensteuerung.

Norm VDI/VDE 2182 Blatt 1 VDI/VDE 2182 Blatt 1.
Informationssicherheit in der industriellen Automatisierung; Allgemeines Vorgehensmodell.

Norm VDI/VDE 2182 Blatt 2.3 VDI/VDE 2182 Blatt 2.3.
Informationssicherheit in der industriellen Automatisierung - Anwendungsbeispiel des Vorgehensmodells in der Fabrikautomation für Betreiber - Presswerk.

Norm VDI/VDE 2193 Blatt 1 VDI/VDE 2193 Blatt 1.
Sprache für I4.0-Komponenten - Struktur von Nachrichten.

Norm VDI/VDE 2193 Blatt 2 VDI/VDE 2193 Blatt 2.
Sprache für I4.0-Komponenten Interaktionsprotokoll für Ausschreibungsverfahren.

North 2011 North, Klaus, 2011. *Wissensorientierte Unternehmensführung: Wertschöpfung durch Wissen*.
5., akt.erw. Aufl.
Wiesbaden: Gabler Verlag.
ISBN 9783834925381

Nunamaker et al. 1990 Nunamaker, J. F.; Chen, M., 1990. Systems development in information systems research.
In: *Twenty-Third Annual Hawaii International Conference on System Sciences*.
New York: IEEE, S. 631–640 Bd.3

OECD 2007 OECD, 2007. *Revised Field of Science and Technology (FOS) classification in the Frascati Manual*.
Paris: OECD.
Verfügbar unter: http://www.oecd.org/science/inno/38235147.pdf
Zugriff am: 21.01.2021

Ometov et al. 2019 Ometov, A.; Petrov, V.; Bezzateev, S.; Andreev, S.; Koucheryavy, Y.; Gerla, M., 2019. Challenges of Multi-Factor Authentication for Securing Advanced IoT Applications.
IEEE network **33** (2), S. 82–88

Ometov et al. 2018 Ometov, Aleksandr; Bezzateev, Sergey; Mäkitalo, Niko; Andreev, Sergey; Mikkonen, Tommi; Koucheryavy, Yevgeni, 2018. Multi-Factor Authentication: A Survey.
Cryptography and Communications **2** (1), S. 1

oneM2M 2019 oneM2M, 2019. *Base Ontology (v3.7.3)*.
oneM2M.org:
Verfügbar unter: http://member.onem2m.org/Application/documentapp/downloadLatestRevision/default.aspx?docID=29554
Zugriff am: 21.01.2021

Otebolaku et al. 2017 Otebolaku, Abayomi Moradeyo; Lee, Gyu Myoung, 2017. Towards context classification and reasoning in IoT.
In: *2017 14th International Conference on Telecommunications (ConTEL)*.
New York: IEEE, S. 147–154

Otto et al. 2017 Otto, Boris; Lohmann, Steffen; Auer, Sören; Brost, Gerd; Cirullies, Jan; Eitel, Andreas; Ernst, Thilo, 2017. *Reference Architecture Model for the Industrial Data Space*.
München: Fraunhofer Gesellschaft.
Verfügbar unter: https://www.internationalda-taspaces.org/wp-content/uploads/2019/03/IDS-Reference-Architecture-Model-3.0.pdf
Zugriff am: 21.01.2021

Owen 1998 Owen, Charles L., 1998. Design research: building the knowledge base.
Design Studies **19** (1), S. 9–20

Padma et al. 2016 Padma, P.; Srinivasan, S., 2016. A survey on biometric based authentication in cloud computing.
In: *2016 International Conference on Inventive Computation Technologies (ICICT)*.
New York: IEEE, S. 1–5

Page et al. 2011 Page, Kevin R.; De Roure, David C.; Martinez, Kirk, 2011. REST and Linked Data: a match made for domain driven development?
In: *2nd International Workshop on RESTful Design*.
Hyderabad: ACM.
Verfügbar unter: http://www.ws-rest.org/2011/proc/a5-page.pdf
Zugriff am: 21.01.2021

Panchenko et al. 2016 Panchenko, Andriy; Lanze, Fabian; Zinnen, Andreas; Henze, Martin; Pennekamp, Jan; Wehrle, Klaus; Engel, Thomas, 2016. Website Fingerprinting at Internet Scale.
In: *Proceedings 2016 Network and Distributed System Security Symposium*.
Reston: Internet Society.
ISBN 9781891562419
DOI: 10.14722/ndss.2016.23477

Panziera et al. 2013 Panziera, Luca; De Paoli, Flavio, 2013. A framework for self-descriptive RESTful services.
In: *Proceedings of the 22nd International Conference on World Wide Web*.
Rio de Janeiro: ACM, S. 1407–1414
ISBN 9781450320382

Patzelt 2008 Patzelt, Werner J., 2008. *Forschungslogik V - Ringvorlesung Einführung in die Methoden der Empirischen Sozialforschung*.
Dresden: TU Dresden – Institut für Politikwissenschaft .
Verfügbar unter: https://tu-dresden.de/gsw/phil/iso/mes/ressourcen/dateien/prof/lehre/unterlagen_ringvorlesung/forschungslogik5.pdf?lang=de
Zugriff am: 21.01.2021

Peffers et al. 2007 Peffers, Ken; Tuunanen, Tuure; Rothenberger, Marcus A.; Chatterjee, Samir, 2007. A Design Science Research Methodology for Information Systems Research.
Journal of Management Information Systems **24** (3), S. 45–77

Pêgo et al. 2017 Pêgo, Pedro R. J.; Nunes, Luís, 2017. Automatic discovery and classifications of IoT devices.
In: *2017 12th Iberian Conference on Information Systems and Technologies (CISTI)*.
New York: IEEE, S. 1–10

Peirce 1998 Peirce, Charles Sanders, 1998. *Collected papers of Charles Sanders Peirce*.
London: Thoemmes Press.
ISBN 9781855065567

Pérez Hernández et al. 2014 Pérez Hernández, Marco E.; Reiff-Marganiec, Stephan, 2014. Classifying Smart Objects using capabilities.
In: *2014 International Conference on Smart Computing*.
New York: IEEE, S. 309–316

Pettersson et al. 2001 Pettersson, Magnus; Obrink, Marten, 2001. *Ensuring integrity with fingerprint verification*.
Lund: Precise Biometrics White Paper.
Verfügbar unter: https://pdfs.semanticscholar.org/2d84/e2c78662a93500e214a0020682499cf64120.pdf
Zugriff am: 21.01.2021

Pohlmann 2019 Pohlmann, Norbert, 2019. Cyber-Sicherheit: Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung.
Wiesbaden: Springer Vieweg.
ISBN 9783658253974

Polčák et al. 2014 Polčák, Libor; Jirásek, Jakub; Matoušek, Petr, 2014. Comment on "Remote Physical Device Fingerprinting".
IEEE Transactions on Dependable and Secure Computing **11** (5), S. 494–496

Pols et al. 2019 Pols, Axel; Vogel, Marko, 2019. *Cloud-Monitor 2019*.
Berlin: KPMG.
Verfügbar unter: https://www.bitkom.org/sites/default/files/2019-06/bitkom_kpmg_pk_charts_cloud_monitor_18_06_2019.pdf
Zugriff am: 21.01.2021

Popper et al. 2018 Popper, Jens; Blügel, Marius; Burchardt, Hagen; Horn, Steffen; Merx, Joachim; Richter, Detlev; Varro, Werner; Pfeifer, Michael; Staub-Lang, Pascal, 2018. 3.1: *Safety on modular machines*.
Kaiserslautern: SmartFactoryKL.
Verfügbar unter: https://smartfactory.de/wp-content/uploads/2018/04/SF_WhitePaper_Safety_3-1_EN_XS.pdf
Zugriff am: 21.01.2021

Popper 1935 Popper, Karl, 1935. *Logik der Forschung*.
Vienna: Springer Vienna.
ISBN 9783709120217

Poser 2016 Poser, Hans, 2016. *Homo Creator: Technik als philosophische Herausforderung*.
Wiesbaden: Springer VS.
ISBN 9783658081515

Preden et al. 2009 Preden, Jürgo; Helander, Johannes, 2009. Context Awareness in Distributed Computing Systems.
Annales Universitatis Scientiarum Budapestinensis de Rolando Eotvos Nominatae. Sectio Computatorica **31**, S. 57–73

Radhakrishnan et al. 2015 Radhakrishnan, Sakthi Vignesh; Uluagac, Arif Selcuk; Beyah, Raheem, 2015. GTID: A Technique for Physical Device and Device Type Fingerprinting.
IEEE Transactions on Dependable and Secure Computing **12** (5), S. 519–532

Raja et al. 2015 Raja, Kiran B.; Raghavendra, R.; Stokkenes, Martin; Busch, Christoph, 2015. Multi-modal authentication system for smartphones using face, iris and periocular.
In: *2015 International Conference on Biometrics (ICB)*.
New York: IEEE, S. 143–150

Ramsey et al. 2015 Ramsey, Benjamin W.; Mullins, Barry E.; Temple, Michael A.; Grimaila, Michael R., 2015. Wireless Intrusion Detection and Device Fingerprinting through Preamble Manipulation.
IEEE Transactions on Dependable and Secure Computing **12** (5), S. 585–596

Rasmussen et al. 2007 Rasmussen, Kasper Bonne; Capkun, Srdjan, 2007. Implications of radio fingerprinting on the security of sensor networks.
In: *2007 Third International Conference on Security and Privacy in Communications Networks and the Workshops - SecureComm 2007*.
New York: IEEE, S. 331–340

Ratha et al. 2004 Ratha, Nalini; Bolle, Ruud, 2004. *Automatic Fingerprint Recognition Systems*.
New York: Springer.
ISBN 9780387955933

Ratha et al. 2001 Ratha, Nalini K.; Connell, Jonathan H.; Bolle, Ruud M., 2001. Enhancing security and privacy in biometrics-based authentication systems.
IBM Systems Journal **40** (3), S. 614–634

Rausch et al. 2014 Rausch, Michael; Bakke, Andrew; Patt, Suzanne; Wegner, Beth; Scott, David, 2014. Demonstrating a Simple Device Fingerprinting System.
In: *MICS 2014 Proceedings*.
Verona: N. p..
Verfügbar unter: http://www.micsymposium.org/mics2014/Proceedings-MICS_2014/mics2014_submission_27.pdf
Zugriff am: 21.01.2021

Ray et al. 2017 Ray, Sandip; Jin, Yier, 2017. Guest Editorial: Security Challenges in the IoT Regime.
Journal of Hardware and Systems Security **1** (4), S. 297–297

Recknagel 2005 Recknagel, Matthias, 2005. *Integriertes Qualitätsinformations- und Recherchesystem für die dokumentierte Prüfung von Bauteilen*.
Heimsheim: Universität Stuttgart.
Stuttgart, Universität Stuttgart, Diss., 2005.
ISBN 9783936947779

Rogers 2006 Rogers, Marcus K., 2006. A two-dimensional circumplex approach to the development of a hacker taxonomy.
Digital Investigation **3** (2), S. 97–102

Ross et al. 2003 Ross, Arun; Jain, Anil, 2003. Information fusion in biometrics.
Pattern recognition letters **24** (13), S. 2115–2125

Sachs et al. 2019 Sachs, Joachim; Wallstedt, Kenneth; Alriksson, Fredrik; Eneroth, Göran, 2019. Boosting smart manufacturing with 5G wireless connectivity.
Ericsson Technology Review **2019** (02).
Verfügbar unter: https://www.ericsson.com/49232f/assets/local/reports-papers/ericsson-technology-review/docs/2019/5g-and-smart-manufacturing.pdf
Zugriff am: 21.01.2021

Salton et al. 1975 Salton, Gerard M.; Wong, Andrew; Yang, Chungshu, 1975. A vector space model for automatic indexing. *Communications of the ACM* **18** (11), S. 613–620

Sariyanidi et al. 2015 Sariyanidi, Evangelos; Gunes, Hatice; Cavallaro, Andrea, 2015. Automatic Analysis of Facial Affect: A Survey of Registration, Representation, and Recognition. *IEEE transactions on pattern analysis and machine intelligence* **37** (6), S. 1113–1133

Sauter 1990 Sauter, Klaus-Dieter, 1990. Werkstückbegleitender Informationsspeicher als Basis für ein informationstechnisches Konzept für Halbleiterfertigungen. Berlin: Springer. ISBN 9783540532361

Sbeyti 2016a Sbeyti, Hassan, 2016. Mobile user authentication based on user behavioral pattern (MOUBE). *International Journal of Computer Science and Security (IJCSS)* **10** (3), S. 1

Sbeyti 2016b Sbeyti, Hassan, 2016. Mobile user signature extraction based on user behavioural pattern (MUSEP). *International Journal of Pervasive Computing and Communications* **12** (4), S. 421–446

Schel et al. 2018 Schel, Daniel; Henkel, Christian; Stock, Daniel; Meyer, Olga; Rauhöft, Greg; Einberger, Peter; Stöhr, Matthias; Daxer, Marc Andre; Seidelmann, Joachim, 2018. Manufacturing Service Bus: An Implementation. *Procedia CIRP* **67**, S. 179–184

Schemm 2008 Schemm, Jan Werner, 2008. Zwischenbetriebliches Stammdatenmanagement: Lösungen für die Datensynchronisation zwischen Handel und Konsumgüterindustrie. Berlin: Springer. ISBN 9783540890294

Schleipen et al. 2019 Schleipen, Miriam; Boss, Birgit; Grothoff, Julian; Lieske, Matthias; Pfrommer, Julius; Rauschecker, Ursula; Schel, Daniel; Stock, Daniel; Westerkamp, Clemens; Zimmermann, Patrick; VDI/VDE-GMA, 2019. *Industrie 4.0 Begriffe/Terms*.
Düsseldorf: Verein Deutscher Ingenieure e.V.
Verfügbar unter: https://www.vdi.de/ueber-uns/presse/publikationen/details/industrie-40-begriffe-terms
Zugriff am: 21.01.2021

Schmeck 2005 Schmeck, Hartmut, 2005. Organic computing - a new vision for distributed embedded systems.
In: *ISORC '05: Proceedings of the Eighth IEEE International Symposium on Object-Oriented Real-Time Distributed Computing*.
New York: IEEE, S. 201–203

Schroff et al. 2015 Schroff, Florian; Kalenichenko, Dmitry; Philbin, James, 2015. Facenet: A unified embedding for face recognition and clustering.
In: *Proceedings of the IEEE conference on computer vision and pattern recognition*.
New York: IEEE, S. 815–823

Schuh et al. 2012 Schuh, Günther; Stich, Volker, 2012. *Logistikmanagement - Handbuch Produktion und Management 6*.
2., vollst. überarb. Aufl.
Berlin: Springer Vieweg.
ISBN 9783642289910

Schumacher 2006 Schumacher, Markus, 2006. *Security patterns: integrating security and systems engineering*.
Hoboken: John Wiley & Sons.
ISBN 9780470858844

Siedler et al. 2018 Siedler, Carina; Aurich, Jan C., 2018. Digitale Transformation eines Produktionssystems.
ZWF Zeitschrift für wirtschaftlichen Fabrikbetrieb **113** (7–8), S. 514–517

Sieka 2006 Sieka, Bartlomiej, 2006. Using radio device fingerprinting for the detection of impersonation and Sybil attacks in wireless networks.
In: *Lecture Notes in Computer Science*.
Berlin: Springer, S. 179–192
ISBN 9783540691723

Siepmann et al. 2016 Siepmann, David; Graef, Norbert, 2016. Industrie 4.0 – Grundlagen und Gesamtzusammenhang.
In: Roth, Armin (Hrsg.), *Einführung und Umsetzung von Industrie 4.0: Grundlagen, Vorgehensmodell und Use Cases aus der Praxis*.
Berlin: Springer, S. 17–82
ISBN 9783662485057

Simon 1996 Simon, Herbert A., 1996. *The Sciences of the Artificial*.
Cambridge: MIT Press.
ISBN 9780585360102

Skolaut 2014 2014. *Maschinenbau*.
Berlin: Springer Vieweg.
ISBN 9783827425539

Skopik 2017 Skopik, Florian, 2017. Collaborative Cyber Threat Intelligence: Detecting and Responding to Advanced Cyber Attacks on National Level.
Boca Raton: CRC Press.
ISBN 9781138031821

Spagnolo et al. 2010 Spagnolo, Giuseppe Schirripa; Cozzella, Lorenzo; Simonetti, Carla, 2010. Banknote security using a biometric-like technique: a hylemetric approach.
Measurement science & technology **21** (5), S. 055501

Spath et al. 2013 Spath, Dieter; Ganschar, Oliver; Gerlach, Stefan; Hämmerle, Moritz; Krause, Tobias; Schlund, Sebastian, 2013. *Produktionsarbeit der Zukunft - Industrie 4.0*.
Stuttgart: Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO.
Verfügbar unter: https://www2.iao.fraunhofer.de/images/iao-news/produktionsarbeit-der-zukunft.pdf
Zugriff am: 21.01.2021

Spitzner 2000 Spitzner, Lance, 2000. Passive Fingerprinting
Verfügbar unter: https://www.techsolvency.com/mirror/finger/
Zugriff am: 21.01.2021

Spooren et al. 2015 Spooren, Jan; Preuveneers, Davy; Joosen, Wouter, 2015. Mobile device fingerprinting considered harmful for risk-based authentication.
In: *Proceedings of the Eighth European Workshop on System Security*.
Bordeaux: ACM, S. 6
ISBN 9781450334792

Spur 1997 Spur, Günter, 1997. Evolution der industriellen Produktion.
In: Spur, Günter (Hrsg.), *Evolution der industriellen Produktion*.
Berlin: Akademie-Verlag, S. 15–50
ISBN 9783055018039

Stephan et al. 2018 Stephan, Michael; Weisgerber, Stefan; Jacumeit, Volker; Helfritz, Benjamin; Müller, Sven; Seipel, Christian; Kipker, Dennis Kenji, 2018. *Projektbericht Sichere Digitale Identitäten (SDI)*.
Berlin: Bundesministerium für Wirtschaft und Energie (BMWi).
Verfügbar unter: https://www.din.de/resource/blob/306552/1e281ee0a725f5569469af8285ff0183/din-dke-projektbericht-data.pdf
Zugriff am: 21.01.2021

Sterritt 2005 Sterritt, Roy, 2005. Autonomic computing.
Innovations in systems and software engineering **1** (1), S. 79–88

Stock et al. 2020a Stock, Daniel; Bauernhansl, Thomas; Weyrich, Michael; Feurer, Matthias; Wutzke, Rolf, 2020. System Architectures for Cyber-Physical Production Systems enabling Self-X and Autonomy.
In: *2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*.
New York: IEEE, S. 148–155

Stock et al. 2019a Stock, Daniel; Schel, Daniel, 2019. Cyber-Physical Production System Fingerprinting.
Procedia CIRP **81**, S. 393–398

Stock et al. 2019b Stock, Daniel; Schel, Daniel; Bauernhansl, Thomas, 2019. Cyber-Physical Production System Self-Description-Based Data Access Layer.
In: *2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*.
New York: IEEE, S. 168–175

Stock et al. 2020b Stock, Daniel; Schel, Daniel; Bauernhansl, Thomas, 2020. Middleware-based Cyber-Physical Production System Modeling for Operators.
Procedia Manufacturing **42**, S. 111–118

Stock et al. 2014 Stock, Daniel; Stöhr, Matthias; Rauschecker, Ursula; Bauernhansl, Thomas, 2014. Cloud-based Platform to Facilitate Access to Manufacturing IT.
Procedia CIRP **25**, S. 320–328

Straub 2011 Straub, Jürgen, 2011. Identität.
In: Jaeger, Friedrich, Liebsch, Burkhard (Hrsg.), *Handbuch der Kulturwissenschaften: Band 1: Grundlagen und Schlüsselbegriffe*.
Stuttgart: J.B. Metzler, S. 277–363
ISBN 9783476006318

Stuckenschmidt 2009 Stuckenschmidt, Heiner, 2009. *Ontologien: Konzepte, Technologien und Anwendungen*.
Berlin: Springer.
ISBN 9783540793335

Takeda et al. 1990 Takeda, Hideaki; Veerkamp, Paul; Tomiyama, Tetsuo; Yoshikawa, Hiroyuki, 1990. Modeling Design Processes.
AI Magazine **11** (4), S. 37–48

Taylor 1998 Taylor, Frederick Winslow, 1998. *The Principles of Scientific Management*.
New York: Courier Corporation.
ISBN 9780486299884

ten Hompel et al. 2007 ten Hompel, Michael; Büchter, Hubert; Franzke, Ulrich, 2007. *Identifikationssysteme und Automatisierung*.
Berlin: Springer.
ISBN 9783540758815

Teschl et al. 2014 Teschl, Gerald; Teschl, Susanne, 2014. *Mathematik für Informatiker: Band 2: Analysis und Statistik*.
3., überarb. Aufl.
Berlin: Springer.
ISBN 9783642542749

Thakkar 2017 Thakkar, Danny, 2017. Biometric Devices: Cost, Types and Comparative Analysis
Verfügbar unter: https://www.bayometric.com/biometric-devices-cost/
Zugriff am: 21.01.2021

Thangavelu et al. 2019 Thangavelu, Vijayanand; Divakaran, Dinil Mon; Sairam, Rishi; Bhunia, Suman Sankar; Gurusamy, Mohan, 2019. DEFT: A Distributed IoT Fingerprinting Technique.
IEEE Internet of Things Journal **6** (1), S. 940–952

Tietz 1960 Tietz, Bruno, 1960. Bildung und Verwendung von Typen in der Betriebswirtschaftslehre: dargelegt am Beispiel der Typologie der Messen und Ausstellungen.
Köln: Westdt. Verlag.
ISBN 9783509004120

Trnka et al. 2018 Trnka, Michal; Cerny, Tomas; Stickney, Nathaniel, 2018. Survey of Authentication and Authorization for the Internet of Things.
Security and Communication Networks **2018**.
DOI: 10.1155/2018/4351603

Tsolkas et al. 2017 Tsolkas, Alexander; Schmidt, Klaus, 2017. *Rollen und Berechtigungskonzepte: Identity- und Access-Management im Unternehmen*.
2. Aufl.
Berlin: Springer.
ISBN 9783658179878

Ulrich 1968 Ulrich, Hans, 1968. Die Unternehmung als produktives soziales System - Grundlagen der allgemeinen Unternehmungslehre.
Bern: Haupt.
Schriftenreihe Unternehmung und Unternehmungsführung 1.

Ulrich et al. 1976 Ulrich, Hans; Hill, Wilhelm, 1976. Wissenschaftstheoretische Grundlagen der Betriebswirtschaftslehre (Teil 1).
WiST Zeitung für Ausbildung und Hochschulkontakt **5** (7), S. 304–309

Unterstein et al. 2012 Unterstein, Michael; Matthiessen, Günter, 2012. *Relationale Datenbanken und SQL in Theorie und Praxis*.
5. Aufl.
Berlin: Springer.
ISBN 9783642289866

U.S. Department of Homeland Security 2016 U.S. Department of Homeland Security, 2016. *Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies*.
Washington: U.S. Department of Homeland Security.
Verfügbar unter: https://www.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf
Zugriff am: 21.01.2021

Vacca 2013 Vacca, John R., 2013. *Managing Information Security*.
2. Aufl.
Waltham: Elsevier.
ISBN 9780124166943

Vaishnavi et al. 2015 Vaishnavi, Vijay K.; Kuechler, William, 2015. Design Science Research Methods and Patterns: Innovating Information and Communication Technology, 2nd Edition.
2. Aufl.
London: CRC Press.
ISBN 9781498715263

VDE 2019 VDE, 2019. Funktionale Sicherheit: Der Schutz des Menschen vor der Maschine
Verfügbar unter: https://www.dke.de/de/arbeitsfelder/core-safety/funktionale-sicherheit
Zugriff am: 21.01.2021

VDMA et al. 2016 VDMA; Fraunhofer Institut für Angewandte und Integrierte Sicherheit (AISEC); accessec, 2016. *Leitfaden Industrie 4.0 Security - Handlungsempfehlungen für den Mittelstand*.
Frankfurt am Main: VDMA.
Verfügbar unter: http://industria-lsecurity.vdma.org/documents/16227999/16499033/1492086354471_Leitf_I40_Security_Dt_LR_neu.pdf/66f12fc7-2b8f-4795-9c48-20329ce35db5
Zugriff am: 21.01.2021

Venable et al. 2016 Venable, John; Pries-Heje, Jan; Baskerville, Richard, 2016. FEDS: a Framework for Evaluation in Design Science Research.
European Journal of Information Systems **25** (1), S. 77–89

Verl et al. 2014 Verl, Alexander; Lechler, Armin, 2014. Steuerung aus der Cloud.
In: Bauernhansl, Thomas, ten Hompel, Michael, Vogel-Heuser, Birgit (Hrsg.), *Industrie 4.0 in Produktion, Automatisierung und Logistik: Anwendung · Technologien · Migration*.
Wiesbaden: Springer Vieweg, S. 235–247
ISBN 9783658046828

Viswanathan 2012 Viswanathan, Harish, 2012. The Business of M2M.
In: Boswarthick, David, Elloumi, Omar, Hersent, Olivier (Hrsg.), *M2M Communications: A Systems Approach*.
Chichester, UK: John Wiley & Sons, Ltd, S. 23–36
ISBN 9781119974031

Wagner et al. 2017 Wagner, Constantin; Grothoff, Julian; Epple, Ulrich; Drath, Rainer; Malakuti, Somayeh; Grüner, Sten; Hoffmeister, Michael; Zimmermann, Patrick, 2017. The role of the Industry 4.0 asset administration shell and the digital twin during the life cycle of a plant.
In: *2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*.
New York: IEEE, S. 1–8

Waite 2010 Waite, Andrew, 2010. InfoSec Triads: Security/Functionality/Ease-of-use
Verfügbar unter: https://blog.infosanity.co.uk/?p=676
Zugriff am: 21.01.2021

Wankhade et al. 2013 Wankhade, Shama; Koshatwar, Payal; Thakare, Rupali, 2013. Autonomic Computing.
International Journal of Scientific and Research Publications **3** (7).
Verfügbar unter: http://www.ijsrp.org/research-paper-0713/ijsrp-p19100.pdf
Zugriff am: 21.01.2021

Weaver 2006 Weaver, Alfred C., 2006. Biometric authentication.
Computer **39** (2), S. 96–97

Weber 2015 Weber, Mathias, 2015. *Kognitive Maschinen - Meilenstein in der Wissensarbeit*.
Berlin: Bitkom Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.
Verfügbar unter: https://www.bitkom.org/sites/default/files/file/import/150213-Kognitive-Maschinen-11Febr2015.pdf
Zugriff am: 21.01.2021

Weiser 2002 Weiser, Mark, 2002. The computer for the 21st Century (reprint).
IEEE pervasive computing / IEEE Computer Society [and] IEEE Communications Society **1** (1), S. 19–25

Westkämper 2009 Westkämper, Engelbert, 2009. Wandlungsfähige Produktionsunternehmen: Das Stuttgarter Unternehmensmodell.
Berlin: Springer.
ISBN 9783540218890

Westkämper 2013 Westkämper, Engelbert, 2013. Integration in der digitalen Produktion.
In: Westkämper, Engelbert, Spath, Dieter, Constantinescu, Carmen, Lentes, Joachim (Hrsg.), *Digitale Produktion*.
Berlin: Springer, S. 133–143
ISBN 9783642202599

Westkämper et al. 2001 Westkämper, Engelbert; Braatz, Arnulf, 2001. Eine Methode zur objektorientierten Softwarespezifikation von dezentralen Automatisierungssystemen mit der Unified Modeling Language (UML).
at - Automatisierungstechnik **49** (5/2001).
DOI: 10.1524/auto.2001.49.5.225

Weyrich et al. 2017 Weyrich, Michael; Klein, Matthias; Schmidt, Jan-Philipp; Jazdi, Nasser; Bettenhausen, Kurt D.; Buschmann, Frank; Rubner, Carolin; Pirker, Michael; Wurm, Kai, 2017. Evaluation Model for Assessment of Cyber-Physical Production Systems.
In: Jeschke, Sabina, Brecher, Christian, Song, Houbing, Rawat, Danda B. (Hrsg.), *Industrial Internet of Things: Cybermanufacturing Systems*.
1. Aufl.
Cham: Springer, S. 169–199
ISBN 9783319425597

Weyrich et al. 2014 Weyrich, Michael; Schmidt, Jan-Philipp; Ebert, Christof, 2014. Machine-to-Machine Communication.
IEEE Software **31** (4), S. 19–23

Whitman et al. 2011 Whitman, Michael E.; Mattord, Herbert J., 2011. *Principles of Information Security*.
4. Aufl.
Boston: Cengage Learning.
ISBN 9781111138219

Wiedermann 2015 Wiedermann, Norbert, 2015. Absicherungskonzepte für Industrie 4.0.
Datenschutz und Datensicherheit - DuD **39** (10), S. 652–656

Wieringa 2014 Wieringa, Roel J., 2014. Design Science Methodology for Information Systems and Software Engineering.
Berlin: Springer.
ISBN 9783662438381

Winzer 2013 Winzer, Petra, 2013. Generic Systems Engineering: Ein methodischer Ansatz zur Komplexitätsbewältigung.
Berlin: Springer.
ISBN 9783642303654

Wölker 2004 Wölker, Martin, 2004. *Vorlesungsskript - Automatische Identifikation und Datenerfassung*.
Venlo: Fontys Hogeschool Bedrijfskunde en Logistiek.
Verfügbar unter: http://docplayer.org/78945805-Vorlesungsskript-automatische-identifikation-und-datenerfassung-von-dr-martin-woelker.html
Zugriff am: 21.01.2021

Würtz 2008 Würtz, Rolf P., 2008. *Organic Computing*.
Berlin: Springer.
ISBN 9783540776574

Xu et al. 2015 Xu, Qiang; Zheng, Rong; Saad, Walid; Han, Zhu, 2015. *Device Fingerprinting in Wireless Networks: Challenges and Opportunities*.
Verfügbar unter: http://arxiv.org/abs/1501.01367

Xue et al. 2015 Xue, Lingling; Liu, Yang; Zeng, Peng; Yu, Haibin; Shi, Zhao, 2015. An ontology based scheme for sensor description in context awareness system.
In: *2015 IEEE International Conference on Information and Automation*.
New York: IEEE, S. 817–820

Zelewski 1999 Zelewski, Stephan, 1999. Grundlagen.
In: Corsten, Hans, Reiß, Michael (Hrsg.), *Betriebswirtschaftslehre*.
München: Oldenbourg Wissenschaftsverlag, S. 5–9
ISBN 9783486250664

Zhou et al. 2014 Zhou, Zhe; Diao, Wenrui; Liu, Xiangyu; Zhang, Kehuan, 2014. Acoustic Fingerprinting Revisited: Generate Stable Device ID Stealthily with Inaudible Sound.
In: *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*.
New York: ACM, S. 429–440
ISBN 9781450329576

Anhang 1 – Ergänzungen zu Methodik und Aufbau der Arbeit

Anhang 1.1 – Wissenschaftstheoretische Positionierung

Mit der Frage, wie sich Wissenschaft in Bereiche, Klassen und Forschungsgebiete einteilen und einordnen lässt, befassten sich schon antike Philosophen wie Aristoteles. Diese Frage ist insofern wichtig, da Wissenschaften sich jeweils durch ihren Untersuchungsgegenstand und in der wissenschaftlichen Methode des Erkenntnisgewinns unterscheiden. So hat Aristoteles in theoretische, praktische und poietische (herstellende) Wissenschaften unterschieden (Höffe 2006), eine Einteilung, die in der Moderne überholt ist. Wissenschaft lässt sich nach Ulrich und Hill nicht abschließend analytisch definieren, sondern ist ein soziales Phänomen in einem bestimmten soziokulturellen Kontext (Ulrich et al. 1976, S. 305). Versucht man die Wissenschaften nach verschiedenen Kriterien zu systematisieren, finden sich in der Literatur unterschiedliche Darstellungen, beispielsweise von Ulrich und Hill, Zelewski und Christiaans (Ulrich et al. 1976; Zelewski 1999; Christiaans 2004), die jedoch grundsätzlich ähnlichen Ansätzen folgen. Dieser Umstand zeigt, dass Wissenschaft selbst das Objekt der wissenschaftlichen Betrachtung sein kann. In Zelewskis Darstellung eines Systems wissenschaftlicher Disziplinen spiegelt sich dies in einer zusätzlichen Betrachtungsebene wider, die zwischen Meta- und Objektwissenschaften unterscheidet (Zelewski 1999, S. 6). Erstere befassen sich mit der Wissenschaft selbst, während letztere sich konkreten Gegenständen widmen, die nicht Bestandteil der Wissenschaften selbst sind.

Ulrich und Hill und Christiaans unterteilen die Objektwissenschaften in Real- und Formalwissenschaften, Zelewski ergänzt diese noch zusätzlich um die Strukturwissenschaften, die sich mit allgemeinen funktionalen Mustern und Strukturen befassen (Zelewski 1999, S. 6). Die Formalwissenschaften, beispielsweise Mathematik, Logik und Linguistik, untersuchen die Art und der Anordnung von Zeichen (Wörter, Symbole) in einem Ausdruck,

nicht aber deren Bedeutung für die Realität und ohne Bezug auf Sinneseindrücke (Christiaans 2004, S. 1087).

Die Realwissenschaften können in "reine" Grundlagenwissenschaften (Ulrich et al. 1976, S. 305) bzw. Erkenntniswissenschaften (acatech 2013) und "angewandte" Handlungswissenschaften (Ulrich et al. 1976, S. 305; acatech 2013, S. 18) unterteilt werden. Die Naturwissenschaften werden somit den reinen Grundlagenwissenschaften zugeteilt, während die Kulturwissenschaften den Handlungswissenschaften zugehörig sind. Zelewski unterscheidet hier im normativen (präskriptiven) und nicht-normativen (deskriptiven) Charakter der Disziplinen, die den Kulturwissenschaften angehören (Zelewski 1999, S. 7).

Die OECD nimmt mit Fokus auf aufkommende Technologien eine etwas abweichende Einteilung in sechs Hauptfelder von Wissenschaft und Technik (Revised Field of Science and Technology (FOS) Classification) vor: Naturwissenschaften, Ingenieur- und Technikwissenschaften, Humanmedizin und Gesundheitswissenschaften, Agrarwissenschaften und Veterinärmedizin, Sozialwissenschaften und Geisteswissenschaften (OECD 2007, S. 12). Abbildung A 1 stellt hieraus abgeleitet eine Systematik der Wissenschaften dar.

Je weiter man in der Unterscheidung der wissenschaftlichen Disziplinen geht, desto mehr verschwimmen die Grenzen zwischen einzelnen Fachgebieten, insbesondere die Technik- und Ingenieurwissenschaften sind durch ihre starke Interdisziplinarität gekennzeichnet (acatech 2013, S. 18). Das Impulspapier der Acatech zu den Technikwissenschaften beschreibt die Technik als Gegenstand ebendieser. Diese stellt die Objekte und Prozesse dar, die künstliche, zweckgerichtete und materielle sowie immaterielle Elemente besitzen. Zudem wird die Technik hinsichtlich ihrer Struktur und Funktion, ihrer ökologischen Dimension sowie ihrer soziokulturellen Entstehungs- und Verwendungszusammenhänge betrachtet (acatech 2013, S. 18).

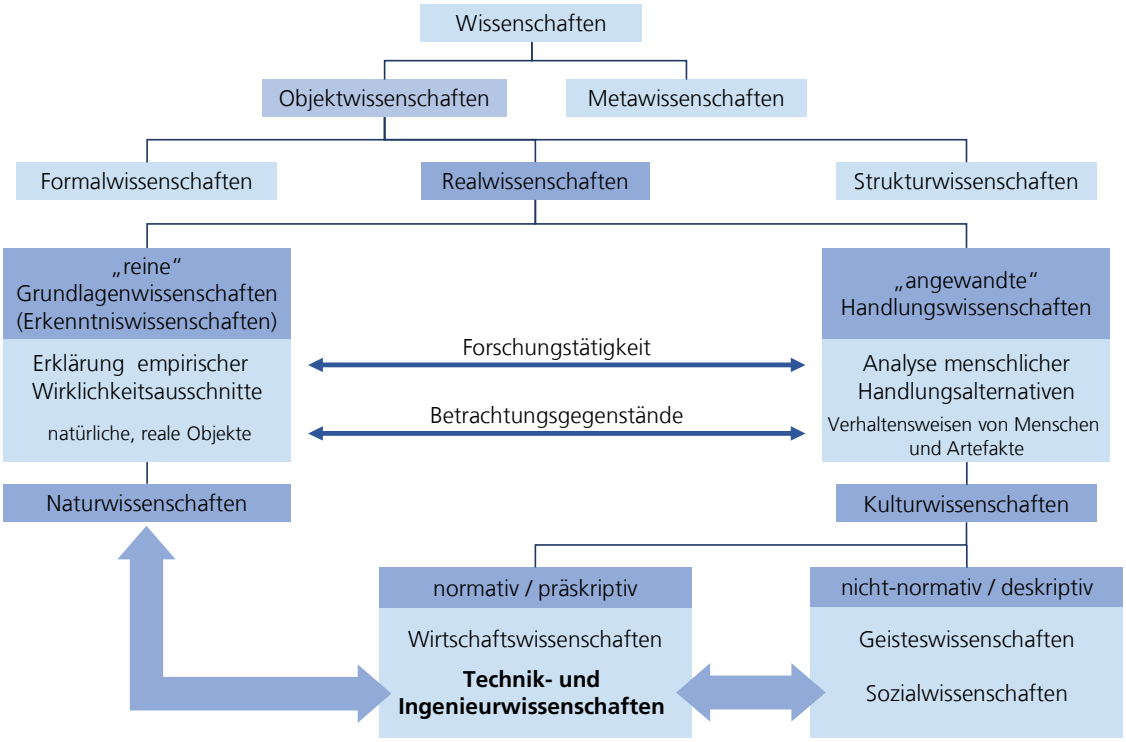


Abbildung A 1 Einordnung der Wissenschaften
in Anlehnung an (Christiaans 2004; Zelewski 1999; Ulrich et al. 1976)

Synthetische oder künstliche Objekte, also von Menschen geschaffene Artefakte, und insbesondere zukünftige künstliche Objekte mit gewünschten Eigenschaften, sind das zentrale Ziel der Ingenieurtätigkeit und Kompetenz. Nach Simon beschäftigt sich der technische Ingenieur somit damit, wie die Dinge sein sollten, und wie sie sein sollten, um Ziele zu erreichen und zu funktionieren (Simon 1996, S. 5). Der Ingenieur verfolgt in diesem Zusammenhang auch als Ziel maximale Effektivität, nicht Wahrheit (Bunge 1966, S. 335). Poser verweist darauf, dass technisches Handeln als zielgerichtetes, effektives (also wirksames) und effizientes (also leistungsfähiges) Handeln Kenntnisse des Verfahrens erfordert. Dieses besteht aus technischem und wissenschaftlichem Wissen, Fähigkeiten im Umgang mit technischen Geräten, sowie schließlich Fähigkeiten zur Zielbestimmung, im Hinblick darauf, wie eine Technik als Mittel eingesetzt werden soll (Poser 2016, S. 22). Bunge sieht eine Theorie in der angewandten Wissenschaft nicht nur als den Höhepunkt eines

Forschungszyklus und einen Leitfaden für die weitere Forschung, sondern auch als Grundlage für ein Regelwerk, das den Kurs eines optimalen praktischen Handelns vorschreibt (Bunge 1966, S. 330). Blake definiert Forschung, sowohl die der Grundlagen als auch die angewandte, als "systematisches, intensives Studium, das auf eine umfassendere wissenschaftliche Kenntnis des untersuchten Themas abzielt" (Blake 1978, S. 3). Für einen solchen Forschungsprozess werden von Ulrich und Hill in Bezug auf die Realwissenschaften der Entdeckungs-, Begründungs- und Verwendungszusammenhang als drei bestimmende Aspekte genannt (Ulrich et al. 1976, S. 306):

Der **Entdeckungszusammenhang** erfasst zu Beginn des Forschungsprozesses den gedanklichen Bezugsrahmen als methodische Grundlage für das Vorhaben. Aus wissenschaftspsychologischer Sicht ist zu beachten, dass die Definition der Zweckmäßigkeit eines Forschungsvorhabens dem Subjektivitätskriterium unterliegt. Ulrich und Hill weisen hierzu auch auf Einflüsse durch Wahrnehmungsfilter hin. Dies ist eine selektive Wahrnehmung aufgrund subjektiver Denkmuster, die durch die Erfahrungen des Betrachters geprägt sind. Zudem können Interessenbezüge durch eigene Normen und Interessen Einfluss haben (Ulrich et al. 1976, S. 306). Dieser Umstand wird durch das weiterhin von Ulrich und Hill angesprochene Heuristik-Problem verschärft, da begrenzte Ressourcen in Form von Zeit und Informationen den Suchprozess zur Lösung neuer Probleme zwingend abkürzen und so ggf. nicht die bestmögliche Lösungsalternative gewählt wird. Kuhn zufolge ist der Fortschritt in einer Disziplin unmittelbar durch das Vorhandensein allgemein anerkannter, zentraler Denkmuster positiv beeinflusst, die er als Paradigma bezeichnet (Kuhn 2017, S. 25). Diese sind ihm zufolge stärker in den Naturwissenschaften vertreten (Kuhn 2017, S. 30), jedoch eignen sich nach Ulrich und Hill beispielsweise in der BWL als Wirtschaftswissenschaft der faktortheoretische Ansatz von Gutenberg (Gutenberg 1951), der systemtheoretische Ansatz von Ulrich (Ulrich 1968) sowie der entscheidungstheoretische Ansatz von Heinen (Heinen 1985) als solche Grundmodelle. Für Technik- und Ingenieurwissenschaften haben sich jedoch vor allem Design Science Ansätze herausgebildet, die sich wie von Herbert A. Simon in "Wissenschaften vom Künstlichen" beschrieben mit wissenschaftlichen Entstehungsprozessen von Artefakten befassen. Die Entstehung eines Artefakts, seiner Komponenten und deren Organisation, das auf gewünschte Weise mit seiner

Umgebung in Wechselwirkung steht (Simon 1996, S. 6), ist durch die Design Science beschrieben, an der sich der Autor der vorliegenden Arbeit orientiert. Seit den 90er-Jahren werden hier die methodischen Ansätze kontinuierlich weiterentwickelt und sind meist etwas ambivalent mit den Begriffen Design Science Research (DSR), Design Research Methodology (DRM), Design Science Methodology (DSM) oder Design Science Research Methodology (DSRM) benannt. Nunamaker und Chen (Nunamaker et al. 1990), Hevner et al. (Hevner et al. 2004), Peffers et al. (Peffers et al. 2007), Blessing und Charkabarti (Blessing et al. 2009), Wieringa (Wieringa 2014), Vaishnavi und Kuechler (Vaishnavi et al. 2015) und Dresch et al. (Dresch et al. 2015) zeigen jeweils methodische Ansätze und Leitlinien auf, die sich mit der Forschung und Entwicklung von Artefakten befassen, die menschlichen Zwecken dienen. Gregor und Baskerville schreiben den Disziplinen, die sich der Design Science zuteilen lassen, jeweils einen präskriptiven und den sozialen Wissenschaften einen deskriptiven Charakter zu. Dies deckt sich mit der normativen und nicht-normativen Unterscheidung von Zelewski (Zelewski 1999, S. 7), jedoch schlagen sie hierzu ein Fusionsmodell vor. Aus der summativen Sicht der Realität ist demnach erkennbar, dass der Fortschritt der Wissenschaft durch das künstlich Geschaffene den Zustand der Realität weiterentwickelt und dadurch die nicht-normativen reinen Natur- und Sozialwissenschaften befähigt das Wissen über die Realität als Ergebnis dieser Entwicklung zu erweitern (Gregor et al. 2012). Ähnliches hat schon Kuhn beobachtet, der die technischen Disziplinen als Fertigkeiten bezeichnet, die Fakten leicht zugänglich gemacht haben. Diese konnten nicht zufällig entdeckt werden und Technologie spielte so oft eine entscheidende Rolle bei der Entstehung neuer Wissenschaften (Kuhn 2017, S. 30).

Der **Begründungszusammenhang** beschreibt die systematischen Verfahren, die eingesetzt werden, um den gedanklichen Bezugsrahmen einer empirischen Überprüfung zu unterziehen. Aus wissenschaftslogischer Sicht ist hierbei auf das Wahrheitskriterium zu achten, also den Anspruch zu überprüfen, dass die getroffenen Aussagen wahrheitsgemäß und konsistent mit der Wirklichkeit sind, wie Ulrich und Hill anmerken (Ulrich et al. 1976, S. 306). Hierbei verweisen sie auf ein Induktions-Problem, also den Umstand, ob von vereinzelten Beobachtungen auf allgemeine Zusammenhänge geschlossen werden kann. Der Umstand, dass unter diesem Umstand nicht auf eine vollständige Induktion

durch empirische Mittel geschlossen werden kann, wurde von Popper beschrieben und als kritischer Rationalismus geprägt (Popper 1935). Daher ergänzen Ulrich und Hill, dass auch deduktive Schlüsse verwendet werden können (Ulrich et al. 1976, S. 306). In den Ansätzen von Vaishnavi (Vaishnavi et al. 2015, S. 75) und Takeda (Takeda et al. 1990, S. 45) bedienen sich Design bzw. DSRM zusätzlich der Abduktion in ihren Denkmustern. Nach Peirce werden Vorschläge für eine Problemlösung abduktiv aus dem vorhandenen Wissen bzw. Theorieansatz für den Problembereich abgeleitet (Peirce 1998). Auch Peirce vertritt, wie Popper mit dem kritischen Rationalismus, eine fallibilistische Position, also die Überzeugung, dass absolute Gewissheit nicht erreichbar ist und sich Irrtümer niemals ausschließen lassen. Er sieht jedoch auf Basis der abduktiven Deutung der Wahrnehmung den Erkenntnisprozess als Wissen im Vordergrund und betrachtet Wissen nicht als statischen Zustand (Peirce 1998 (CP 1.234)).

Der **Verwendungszusammenhang** befasst sich mit der Frage nach dem Zweck bzw. dem Nutzen der Ergebnisse eines Forschungsvorhabens. Hierzu ist die wissenschaftspolitische Betrachtung heranzuziehen, die Ulrich und Hill im Kontext des Nutzenkriteriums um den Aspekt der gesellschaftlichen Relevanz ausweiten. Das Relevanzproblem bezieht sich hierbei auf die Spannung zwischen verfügbaren Ressourcen und Forschungsalternativen, die sowohl praktisch als auch ideologisch beeinflusst sind (Ulrich et al. 1976, S. 307).

Hevner et al. beispielsweise definieren als Ziel der Design Science-Forschung die Entwicklung technologiebasierter Lösungen für wichtige und relevante Geschäftsprobleme (Hevner et al. 2004, S. 83). Der Autor dieser Abhandlung betrachtet in diesem Kontext sowohl Probleme technischer Natur als auch soziotechnische Aspekte in Bezug auf die Anwendbarkeit einer technologiebasierten Lösung durch menschliche Anwender in einer Organisation.

Anhang 1.2 – Design Science

Design Science ist die Gestaltung (Design) und die Untersuchung von Artefakten in einem bestimmten Kontext. Die Artefakte, die untersucht werden, sind so konzipiert, dass sie mit einem Problemkontext interagieren, um etwas in diesem Kontext zu verbessern (Wieringa 2014, S. 3). Simon platziert Artefakte in einen Bezugsrahmen, der sich in eine innere Umgebung, eine äußere Umgebung und dem Artefakt als die Schnittstelle zwischen den beiden, die bestimmte gewünschte Ziele erreicht, aufteilen lässt (Simon 1996, S. 6). Die äußere Umgebung ist die Gesamtheit der äußeren Kräfte und Effekte, die auf das Artefakt wirken. Die innere Umgebung ist der Inhalt und Satz von Komponenten, aus denen das Artefakt und ihre Beziehungen zueinander bestehen. Das Verhalten des Artefakts wird sowohl durch seine Organisation als auch durch seine äußere Umgebung eingeschränkt (Simon 1996, S. 9). Abbildung A 2 stellt dieses Verhältnis angelehnt an Wieringa und Simon dar.

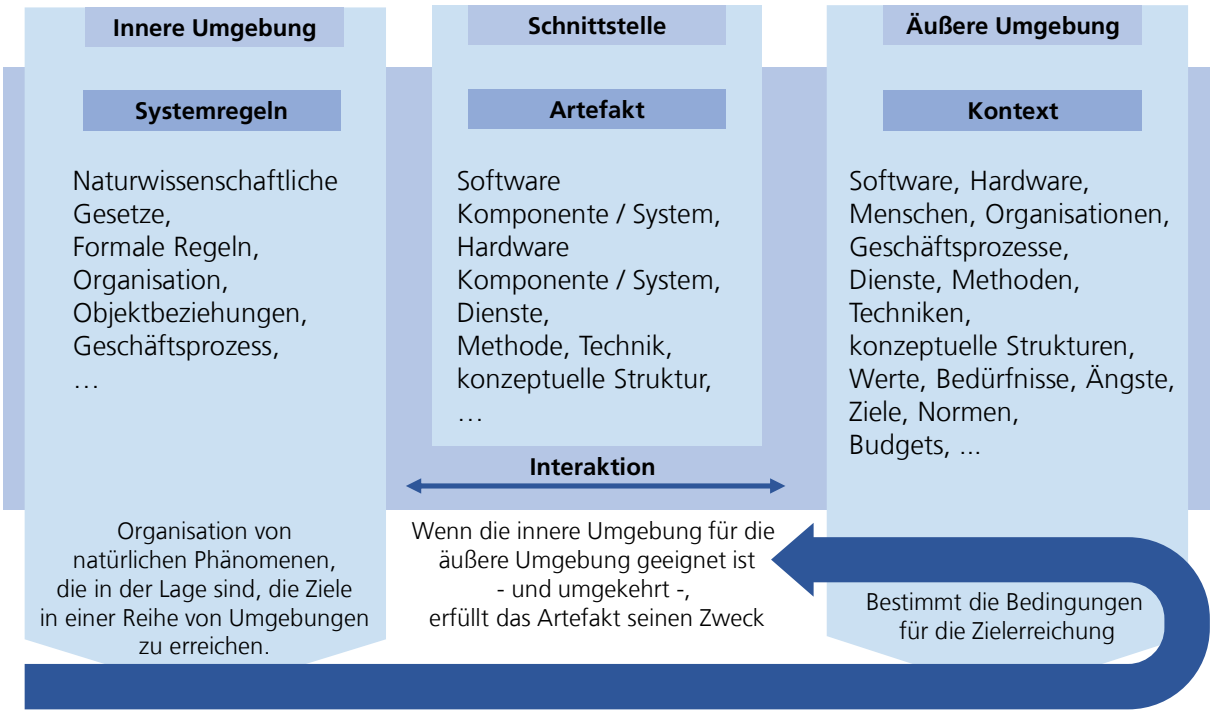


Abbildung A 2 Artefakt und Umwelt

Wissensnutzung und Wissensaufbau sind wie Owen beschreibt keine unstrukturierten Prozesse. Sie werden durch Kanäle gesteuert, die die Verfahren, die zur Durchführung des Forschungsprozesses verwendet werden, steuern und die das Geschaffene (Artefakte) beurteilen. Diese Kanäle sind die Systeme von Konventionen und Regeln, nach denen eine Disziplin arbeitet (vgl. Paradigma nach Kuhn, (Kuhn 2017)). Sie verkörpern die Maßnahmen und Werte, die empirisch als "Erkenntniswege" im Zuge der Reifung einer Disziplin entwickelt wurden (Owen 1998). Hevner et al. haben zum Zweck der Forschung und Entwicklung informationstechnischer Systeme einen konzeptionellen Rahmen für das Verständnis, die Durchführung und Bewertung dieser Systeme aufgestellt, der verhaltenswissenschaftliche Paradigmen der Design Science einbezieht (Hevner et al. 2004, S. 80). Der kognitive Prozess zur Lösung eines Problems, der innerhalb eines solchen Rahmens stattfindet, beinhaltet nach Takeda und Vaishnavi et al. Abduktion, Deduktion und Circumscription (Vaishnavi et al. 2015, S. 17). Circumscription ist eine von McCarthy begründete formale logische Methode (McCarthy 1980), die davon ausgeht, dass jedes Fragment des Wissens nur in bestimmten Situationen gültig ist. Dies ist insofern ein wichtiger Bestandteil des Design Science Prozesses, weil es Verständnis erzeugt, das nur durch den spezifischen Akt der Konstruktion eines Artefakts gewonnen werden konnte (vgl. Erkenntnisprozess nach Peirce (Peirce 1998)). Die Anwendbarkeit von Wissen kann nur durch die Erkennung und Analyse von Widersprüchen bestimmt werden, wenn Dinge nicht funktionieren, obwohl die aufgestellte Theorie sie postuliert. Dies geschieht oft nicht aufgrund eines Unverständnisses der Theorie, sondern aufgrund der notwendigerweise unvollständigen Natur einer jeden Wissensbasis.

Anhang 2 – Digitale Transformation der Produktion

Die in Abschnitt 2.1 diskutierten Bereiche der Produktion befinden in einer kontinuierlichen Evolution. Diese ist durch den stetigen gesellschaftlichen Wandel und den technischen Fortschritt getrieben (Spur 1997, S. 16). Dieser technische Fortschritt ist seit Mitte des 20. und insbesondere im 21. Jahrhundert stark durch den Einsatz von immer leistungsfähigeren Informations- und Kommunikationstechniken (IKT) stark beschleunigt. Diese haben das Internet und eine durchgängig vernetzte Welt ermöglicht und die Menschheit so in das Zeitalter der Information geführt (Nagel et al. 2013, S. 5). In der Produktion bzw. Industrie hat der Einsatz dieser Technologie im Hinblick auf die eigene Historie einen so starken Paradigmenwechsel ausgelöst, dass man von der vierten industriellen Revolution spricht (Kagermann et al. 2013, S. 17). Die Stufen der industriellen Revolutionen seit dem 18. Jahrhundert bis heute sind in Abbildung A 3 dargestellt. Es ist zu erkennen, dass jede Stufe durch die Einführung und den Einsatz einer bestimmten Technologie befähigt wurde, die zu einem Innovationssprung geführt und die jeweilige Periode geprägt hat.

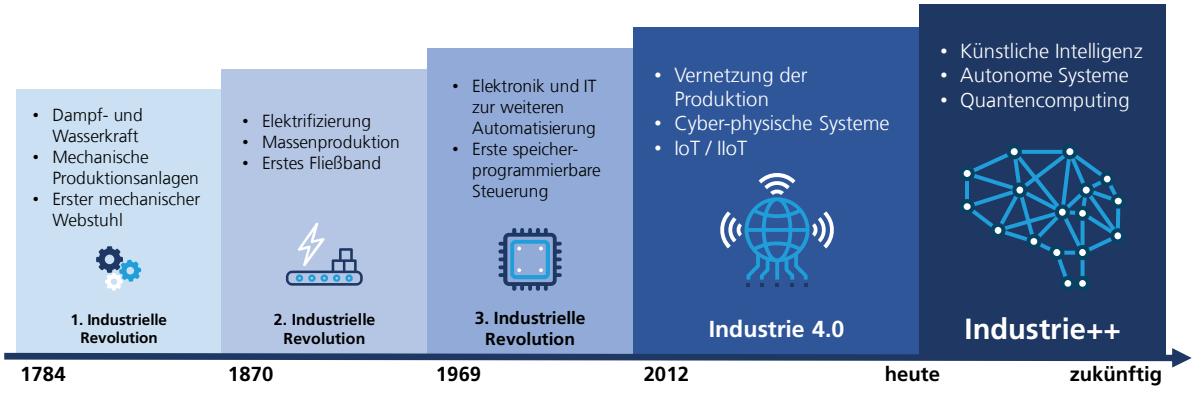


Abbildung A 3 Die Stufen der industriellen Revolutionen

Der Aktionsplan „Zukunftsprojekte der Hightech-Strategie 2020“ der Bundesregierung aus dem Jahr 2012 definierte „Industrie 4.0“ als eines der Zukunftsprojekte (BMBF 2012, S. 52), durch welches der Begriff Industrie 4.0 sinnbildlich für die vierte industrielle Revolution durch die digitale Transformation der Industrie geprägt und zu einer globalen Marke wurde (Kagermann et al. 2016, S. 19). Oftmals werden die Ansätze von Industrie 4.0 international im Kontext der Produktion auch als Industrial Internet bezeichnet. Industrie 4.0 setzt nicht nur auf eine vertikal durchgängig vernetzte Produktion mittels moderner Systemarchitekturen, sondern auch auf eine horizontale globale echtzeitnahe Vernetzung über Unternehmensgrenzen hinweg (Geisberger et al. 2012, S. 24). Die Wissenschaftliche Gesellschaft für Produktionstechnik (WGP) hebt die Bedeutung dieser echtzeitfähigen Vernetzung gegenüber der reinen Digitalisierung von Produkten und Produktion hervor. So ermöglicht Industrie 4.0 darüber hinaus die Entstehung disruptiver Geschäftsmodelle durch die Möglichkeit partnerschaftliche, firmenübergreifende Vernetzung von produzierenden Unternehmen mit Zulieferern, Kunden oder ggf. auch Wettbewerbern (Bauernhansl et al. 2016, S. 3). Allgemein lässt sich Digitalisierung als Ziel der digitalen Transformation, also als die Bereitstellung, Speicherung und Verarbeitung von Daten im Rahmen von Wertschöpfungsprozessen, bezeichnen (Dönicke et al. 2018, S. 5). Die vorliegende Arbeit gliedert sich hier primär in die von der WGP beschriebenen technologischen Aspekte dieser Revolution ein. Nicht nur die Produktions-IT-Systeme unterliegen einer Veränderung durch den technischen Fortschritt. So befähigt der Wandel der klassischen technischen Systeme auf allen Ebenen der Automatisierungspyramide in der Produktion hin zu cyber-physischen Systemen diesen echtzeitnahen Austausch von Daten und Informationen. Dies setzt wiederum einen Wandel in den Architekturen technischer Produktionssysteme und ein Auflösen der Automatisierungspyramide voraus (Bettenhausen et al. 2013, S. 4). Die technischen Aspekte, Voraussetzungen und Möglichkeiten hierzu werden in den folgenden Abschnitten dieses Anhangs diskutiert.

Anhang 2.1 – Vernetzung von Dingen in der smarten Produktion

Die Möglichkeit IT-Systeme zu vernetzten besteht grundsätzlich schon seit der Einführung der IT in der Produktion. Grundsätzlich kann Vernetzung als der Vorgang bezeichnet werden, bei dem Dinge miteinander verbunden werden (digital und analog), die vorher nicht miteinander verbunden waren (Dönicke et al. 2018, S. 5). Automatisierungssysteme wurden zunehmend zur Jahrtausendwende vornehmlich dezentral und verteilt ausgelegt (Westkämper et al. 2001, S. 255). Dieser Trend hat nicht nachgelassen und wird durch neue und leistungsfähigere Kommunikations-technik wie 5G auch in Zukunft nicht abreißen (Sachs et al. 2019).

Der Ansatz, dass jede Maschine bzw. jedes Objekt, inklusive Menschen und Tieren, mit eindeutiger Kennung in der Lage ist eigenständig über ein globales Netz wie dem Internet mit anderen physischen oder virtuellen Objekten zu kommunizieren, wird als Internet of Things (IoT) bezeichnet (Ashton 2009). Die ersten Anwendungen hierfür wurden mit RFID Tags umgesetzt. Die eigentliche Technik, mit der dies ermöglicht wird, ist jedoch nachrangig, da sie dem technischen Fortschritt und permanentem Wandel unterliegt. Miniaturisierung gemeinsam mit steigender Rechenleistung und verbesserte Funk-basierte Kommunikationstechnik haben auch hier dazu geführt, dass Anwendungsfälle möglich wurden, die technisch vorher nicht umsetzbar waren (Bullinger et al. 2007, S. 94). Diese Ansätze machen die Vision des Ubiquitous Computing (vgl. Abschnitt 1.1) in der Produktion möglich. So wird mittels dieser Befähiger-Technologien eine Smart Factory möglich, in der die Produktion und die darin tätigen Menschen und Maschinen bei der Ausführung ihrer Aufgaben kontextsensitiv unterstützt werden (Lucke et al. 2008). Diese Kontextsensitivität wird durch die Anreicherung von Daten mittels Kontextinformationen erreicht. Kontext kann hierbei einen Zustandsbezug, Ortsbezug oder Zeitbezug haben. Der Zeitbezug kann durch Zeitstempel und beispielsweise damit gekoppelte zeitbasierte Regeln abgebildet werden. Zustandsbezug kann neben Führungsgrößen wie z. B. Kapazitätsmodelle, Soll-Lagerbestände, Prüfpläne oder Maschinenzustände und durch Regelgrößen wie Ressourcenauslastungen, Ist-Lagerbestände oder Messergebnisse wie Temperatur, Kraft oder Drehmoment dargestellt werden. Ortsbezug kann statisch durch Ortsangaben wie

z. B. Adressen oder geografische Adressierung oder dynamisch und echtzeitnah durch Lokalisierungssysteme hergestellt werden (Lucke 2013).

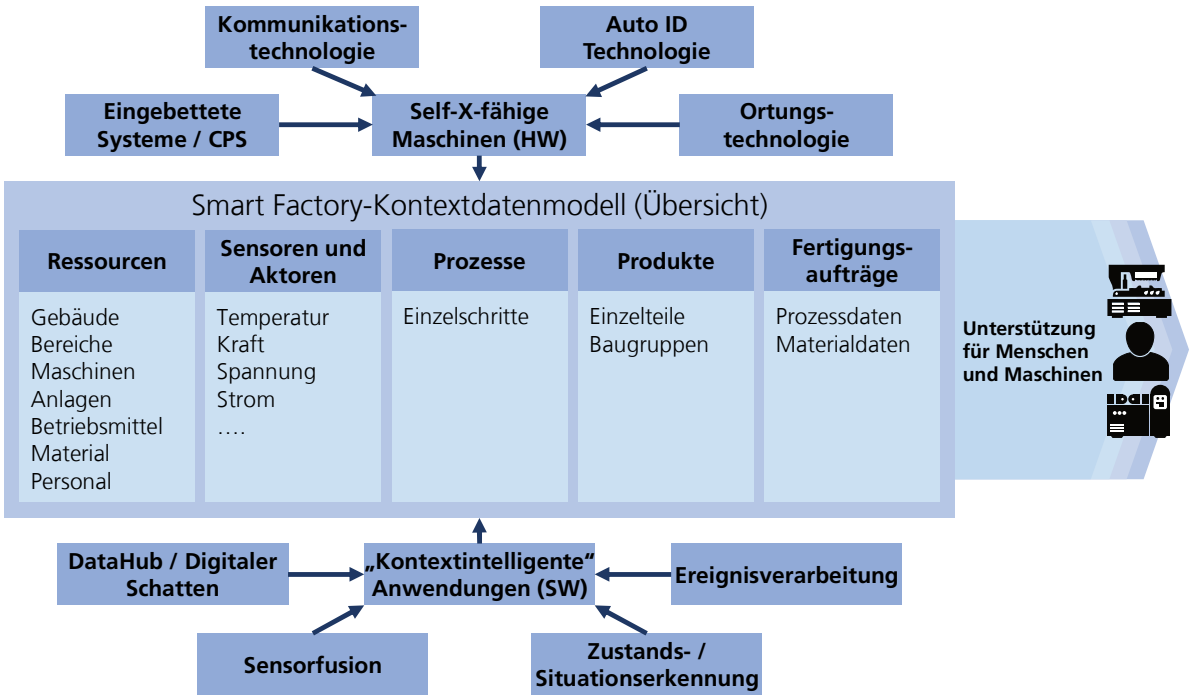


Abbildung A 4 Kontextbezug von Daten in der Smart Factory in Anlehnung an (Lucke et al. 2008; Lucke 2013)

Diese Kontextinformationen können in der Produktion wie in Abbildung A 4 dargestellt aus einer Reihe von Datenquellen gewonnen werden. Die Informationsverwaltung in einer heterogenen Systemlandschaft, wie sie eine vernetzte Produktion darstellt, ist eine Herausforderung für sich. Die Ansätze hierfür werden in Abschnitt 3.2 diskutiert.

Viele Anwendungen des IoT stammen aus dem Verbraucher- und Unternehmens-bereich. Um für den industriellen Einsatz nutzbar zu sein, müssen die für IoT eingesetzten Technologien jedoch Garantien in Bezug auf Sicherheit, Stabilität, Resilienz oder Faktoren wie Echtzeitfähigkeit ermöglichen. Einsatz von Technologien, die dies ermöglichen, werden äquivalent zu IoT als Industrial Internet of Things (IIoT) bezeichnet (Heidrich et al. 2016;

Lin et al. 2019). Die Risiken, die mit einer solchen Vernetzung auf Basis von IoT-Technologien einhergehen, werden in Anhang 3 diskutiert. Die Vorliegende Arbeit hat den Anspruch dazu beizutragen, die dort diskutierten Risiken zukünftig zu mindern bzw. die Wahrscheinlichkeit ihres Eintretens zu senken.

Anhang 2.2 – Wandel der IKT-Infrastruktur in der Produktion

Die Veränderungen der IT-Systemlandschaft und der Systemarchitekturen in der Produktion ist stark von der Veränderung der IKT-Infrastruktur geprägt. Neben den in den vorherigen Abschnitten erwähnten intelligenter werdenden Komponenten der OT auf dem Hallenboden kam es auch in den Rechenzentren der Unternehmen und außerhalb der Unternehmen zu Veränderungen. Der Einsatz von Cloud-Computing und das stetige Wachstum von Cloud-Infrastruktur ist einer der Hauptbefähiger der digitalen Transformation. Cloud-Infrastruktur zeichnet sich durch Flexibilität und Skalierbarkeit aus, die es ermöglichen Nutzern bedarfsgerecht Speicher- und Rechenressourcen bereitzustellen (Hill et al. 2012, S. 4). Grund hierfür ist die Miniaturisierung und immer effizientere Prozessoren und IKT-Komponenten mit steigender Rechenkapazität in Kombination mit Virtualisierung. Virtualisierung ist eine Technologie, die es ermöglicht Funktionen eines IKT-Systems oder einer Komponente, die über dedizierte, proprietäre und meist teure Hardware bereitgestellt werden muss, mittels Software abzubilden (Mandl 2014, S. 47). Größere Unternehmen nutzen hier meist eigene Infrastruktur in Form einer private Cloud (Hahn 2016, S. 65). Kleinere Unternehmen greifen vornehmlich auch auf eine hybride oder öffentliche Cloud-Infrastruktur zurück (Pols et al. 2019, S. 30). Zwar haben viele Unternehmen oft noch Sicherheitsbedenken, allerdings stehen diesen Vorteilen gegenüber, wie beispielsweise Kostenreduzierung, Steigerung der Verlässlichkeit, beschleunigter Datenaustausch und Konsistenz in verteilten Systemen und datengetriebene Cloud-Dienste (Maheshwari et al. 2013). Cloud-Plattform-Architekturen lassen sich auf einer konzeptuellen Ebene wie in Abbildung A 5 dargestellt abbilden. Sie werden grundsätzlich in drei Schichten aufgeteilt, die unterschiedliche Funktionen erfüllen. Möchte man Infrastruktur

in Form von Rechenressourcen, Speicher oder Servern als Laufzeitumgebung für eigene Anwendungen nutzen, kann man auf eine Plattform zurückgreifen, die „Infrastruktur als Dienst“ also „Infrastructure as a Service“ (IaaS) anbietet. Für Anwendungsentwickler, die sich auf die Entwicklung und Bereitstellung von Diensten und Anwendungen fokussieren, bietet eine „Platform as a Service“ (PaaS) ein Framework aus Basisdiensten, beispielsweise Nutzerverwaltung, Datenbanken oder Dienste für die Erfassung von Nutzungsdaten, um darauf basierend Abrechnungsmodelle zu gestalten.

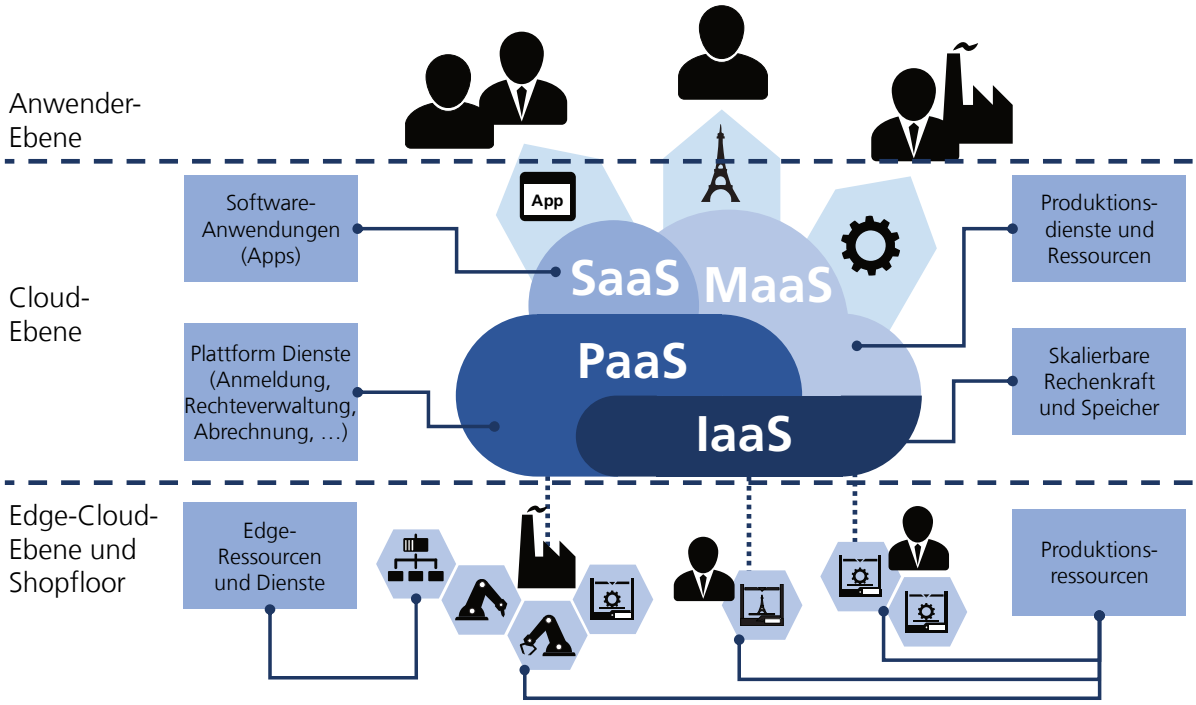


Abbildung A 5 Cloud-Architekturebenen und Everything as a Service (XaaS)

Für reine Endanwender, die nur Anwendungen nutzen möchten, werden nach dem „Software as a Service“-Prinzip (SaaS) diese Anwendungen direkt aus der Cloud-Plattform bereitgestellt. Allerdings ist es auch möglich weitere Ressourcen als Cloud-Services anzubieten, beispielsweise Produktionsressourcen. So kann Manufacturing as a Service (MaaS) zur Bildung virtueller Produktionsnetzwerke und Unternehmen genutzt werden (Mezgár et al. 2014).

Virtualisierung hat auch auf spezifische Anwendungen Einfluss. Der Einsatz von Virtualisierungstechnik in der Netzwerktechnik erlaubt es Netzwerksegmentierung flexibel per Software durchzuführen (Jajodia et al. 2014, S. 77). Dieser Ansatz wird als Software-defined networking (SDN) bezeichnet und lässt sich auf weitere Bereiche übertragen, die unter dem Sammelbegriff „Software-defined X" (SDx), auch „Software-defined Everything" (SDE), zusammengefasst werden können (Bawa et al. 2015). Der 5G-Mobilfunkstandard ist in seiner Form und technischen Umsetzung nur durch durchgängigen Einsatz von Virtualisierungstechnik möglich. Während bei 4G/LTE noch hoch spezialisierte und teure Komponenten zum Einsatz kamen, ermöglichen beispielsweise Software-defined Radio (SDR) Komponenten den Einsatz von COTS (commercial off-the-shelf), also seriengefertigten Produkte aus dem Elektronik- oder Softwaresektor. Die dynamische Netzwerksegmentierung, das Network Slicing, das es ermöglicht die Kommunikationsinfrastruktur bedarfsgerecht zu konfigurieren, wird durch SDN umgesetzt (Cho et al. 2014). Im Kontext der OT lässt sich Virtualisierung im Sinne von SDx ebenfalls anwenden. So existieren bereits Ansätze, mit denen die klassische SPS durch eine vollständig virtualisierte Komponente ersetzt werden kann. Der aktuelle Trend geht zudem in Richtung der Edge-Clouds, also die Verlagerung von Rechenressourcen und Laufzeitumgebungen für Dienste nah an den „Rand" der Cloud, also näher an den Prozess, was vor allem Vorteile in Bezug auf Latenzen und Datensouveränität mit sich bringt.

Es ist erkennbar, dass der Wandel zu einer immer leistungsfähigeren und flexibleren IKT zu immer komplexeren verteilten Systemen führt. Welche Auswirkungen dies mit sich bringt und wie damit in Cloud-basierten Umgebungen umgegangen werden kann, die Teile von CPPS sein können, ist einer der Aspekte, die im Rahmen dieser Arbeit diskutiert werden.

Anhang 2.3 – IT-Architekturen in der Produktion

Die in Abbildung 2.3 dargestellte Automatisierungspyramide stellt eine Unternehmens-IT-Architektur dar, wie sie immer noch in den meisten Unternehmen Bestand hat. Die darin

abgebildeten technischen Systeme wurden ihre Systemarchitektur betreffend in der Vergangenheit als monolithische Software konzipiert und implementiert (Becker 2011, S. 18). Dies gilt sowohl für die IT-Systeme als auch für die mechatronischen Systeme in der Feldebene, die als in sich geschlossene Funktionsblöcke ausgelegt wurden (Geisberger et al. 2012, S. 19). Diese Art der Umsetzung ist historisch durch den Stand der Technik begründet. Die IKT war schlichtweg nicht leistungsfähig genug, um zahlreiche Systeme leistungsfähig und ökonomisch sinnvoll zu vernetzen. Einzelne Systeme verfügten nicht über ausreichend Rechenkapazität und ihr Systementwurf unterlag somit bestimmten Zwängen, die beispielsweise die Umsetzung von echtzeitfähigen Anwendungen erschwerten oder unmöglich machten (Verl et al. 2014, S. 235; Horvath et al. 2012, S. 32).

Die Möglichkeiten der IKT letzten Jahre jedoch haben in diesem Bereich neue Muster der System- und Anwendungsentwicklung befördert. Tabelle 17 gibt eine Übersicht des Wandels der gängigen IT-Architekturen.

Tabelle 17 IT-Architekturmuster im Wandel der Zeit in Anlehnung an (Becker 2011, S. 18)

	1960-70	1980-90	1990+	1995+	2000+	2010+	2015+	2020+
Fokus	Marktanteile und Skaleneffekte	Effektivität	Dezentralisierung	Kundenbindung	Vernetztes Echtzeit-unternehmen	Integration extrem großer Daten-mengen	Verarbeitung großer Daten-mengen	Autonomisierung von Diensten und Systemen
Paradigma	Mainframe	Modul	Client-Server	Applikations-server / Objekt-orientierung	SOA	Micro-services	Serverless	Unikernel /KI/...
Struktur	Monolithisch 1 Schicht	Abteilungs-orientiert 1 Schicht	Arbeits-platz-orientiert 2 Schichten	Portale mit Backend-Systemen 3 Schichten	Modulare, dezentrale Services > 3 Schichten	Weltweit vernetzte Systeme > 3 Schichten	Edge-Cloud Strukturen > 3 Schichten	Hyper-Konvergenz > 3 Schichten
Treiber	Status quo, keine Skalierung	Sinkende CPU-Kosten	PC und Netzwerke	WWW	Web Services	Skalierbare Dienste für IoT und Cloud	Big Data, Data Science, ML/AI	Autonome Systeme

Insbesondere das Architekturmuster der Service-orientierten Architektur (SOA) hat die IT-Anwendungen in Unternehmen in den letzten Jahren stark geprägt. SOA basiert auf einer

losen Kopplung von modularen Diensten. Im Ansatz stellt SOA aktuell auch weiterhin den Stand der Technik dar. Die Art der Umsetzung und die eingesetzten Technologien haben sich über die Jahre jedoch graduell weiterentwickelt.

Ursprünglich diente SOA der Integration von Diensten in Unternehmen, die mittels einer Middleware (siehe Abschnitt 3.2.5) in Form eines Enterprise Service Bus (ESB) miteinander lose gekoppelt werden konnten. Middlewares lassen sich jedoch auch zu Anbindung von Maschinen und Anlagen nutzen, beispielsweise in Form eines Manufacturing Service Bus (MSB) (Schel et al. 2018). Microservices erweitern das SOA-Konzept um die Möglichkeit einer dezentralen Kommunikationsstruktur, in der die einzelnen Dienste direkt miteinander kommunizieren (vgl. Peer-to-Peer / P2P). Die beiden Ansätze sind in Abbildung A 6 gegenübergestellt.

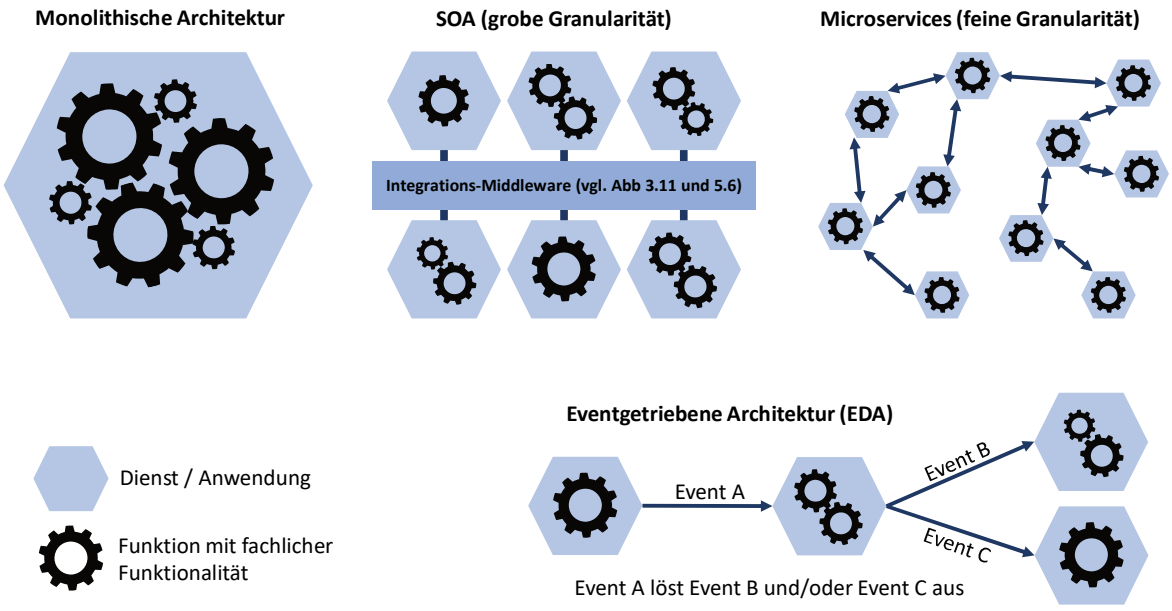


Abbildung A 6 Konzept von SOA, EDA und Microservices

SOA stellt zum heutigen Zeitpunkt den Stand der Technik in der Entwicklung verteilter Systeme dar. Das SoA-Konzept wird oft mit einer ereignisgesteuerten Architektur (engl.

Event-driven Architecture - EDA) gekoppelt. EDA hat einen Fokus auf Ereignisse und Ereignisnachrichten. Eine Ereignisquelle sendet eine Nachricht mit den Daten über das Auftreten eines Ereignisses an eine Middleware. Ein registrierter Empfänger (Ereignissenke) bemerkt die Ankunft einer Ereignisnachricht und verarbeitet sie unmittelbar. Das Ereignis selbst enthält keine Informationen über die weitere Verarbeitung. Das Konzept und Kommunikationsmuster, sich für den Empfang bestimmter Ereignisse zu registrieren, wird als Publish/Subscribe bezeichnet und ermöglich es einer Ereignisquelle mehrere Ereignissenken asynchron und nach dem Push-Prinzip mit Daten zu versorgen (Bruns et al. 2010, S. 36f). Auch die Implementierung von Diensten und Anwendungen in Form von Microservices ist oft das Mittel der Wahl moderner und skalierbarer Systeme. Die Umsetzung des in dieser Arbeit entwickelten Konzepts basiert ebenfalls auf diesen Prinzipien der modernen Software- und Systementwicklung.

Anhang 2.4 – Cloud-Plattformen für die Produktion

SOA und Microservices haben als Architekturmuster im Zuge der digitalen Transformation auf die Produktions-IT starken Einfluss genommen. Viele der Funktionen, die bisher als monolithische Systeme bestand hatten, können in Funktionsblöcke unterteilt und ihre fachliche Funktionalität in Form von kleinen schlanken Anwendungen (Apps) bereitgestellt werden (Bauer et al. 2017). Eines der ersten Beispiele dafür, wie die Kombination aus Cloud-Technologie- und Architektur die Produktions-IT beeinflusst hat, ist das Konzept der Plattform „Virtual Fort Knox" (VFK) (Holtewert et al. 2013).

Diese wurde konzipiert, um Dienste und Anwendungen für das Produktionsumfeld bereitzustellen und als föderative, offene und sichere Plattform ein PaaS-Angebot für freie Dienstanbieter bereitzustellen (Stock et al. 2014). Abbildung A 7 zeigt das Konzept und Die Plattform-Architektur der VFK-Plattform. Diese Plattform ist primär als PaaS-Angebot zu verstehen, da sie darauf ausgerichtet ist Dienste für das Produktionsumfeld bereitzustellen, die von unabhängigen Dienstanbietern (Independent Service Vendor - ISV) bereitgestellt werden.

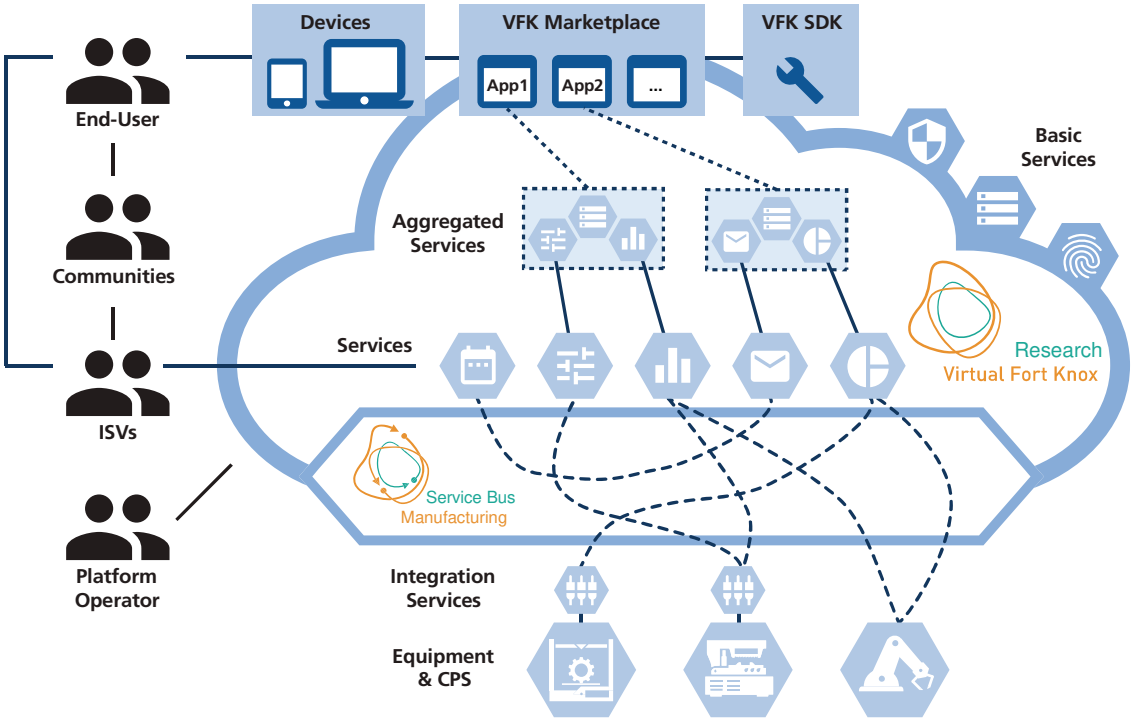


Abbildung A 7 "Virtual Fort Knox "– Manufacturing-Service Cloud-Konzept

Diese Dienste können zu höherwertigen Lösungen aggregiert werden, indem sie über eine Integrationsschicht in Form einer Middleware (MSB, siehe Anhang 2.3 und Abschnitt 3.2.5) orchestriert werden. Zudem können über diese Middleware auch Bestandanlagen über Vorschaltgeräte in Form von Cloud-Adaptern integriert werden. Handelt es sich bei diesen Anlagen um neuartige cyber-physische-Systeme (siehe Abschnitt 2.2), so können diese auch über standardisierte Schnittstellen direkt mit der Integrationsschicht kommunizieren und sich zu Diensten in einer Cloud verbinden und mit diesen Daten austauschen.

Cloud-Plattformen und die dahinterstehenden Prinzipien haben eine tragende Bedeutung für das Konzept dieser Arbeit, da diese einerseits ein Ökosystem bilden, das auf sichere Infrastruktur und verlässliche Transaktionen zwischen Teilnehmern in Form von Nutzern, Diensten und cyber-physischen-Systemen angewiesen ist. Andererseits bilden sie den technischen Unterbau, auf welchem das Konzept entwickelt, erprobt und genutzt wird.

Anhang 2.5 – Das Referenzarchitekturmodell Industrie 4.0 (RAMI 4.0)

Um die für die Industrie tauglichen Entwurfsmuster für Industrie 4.0 Anwendungen bzw. das Industrial Internet und die damit verbundenen zahlreichen Standards zusammenzuführen, hat die Plattform Industrie 4.0 ein Referenzarchitekturmodell entwickelt. Das Referenzarchitekturmodell Industrie 4.0 (RAMI 4.0) ist Abbildung A 8 abgebildet.

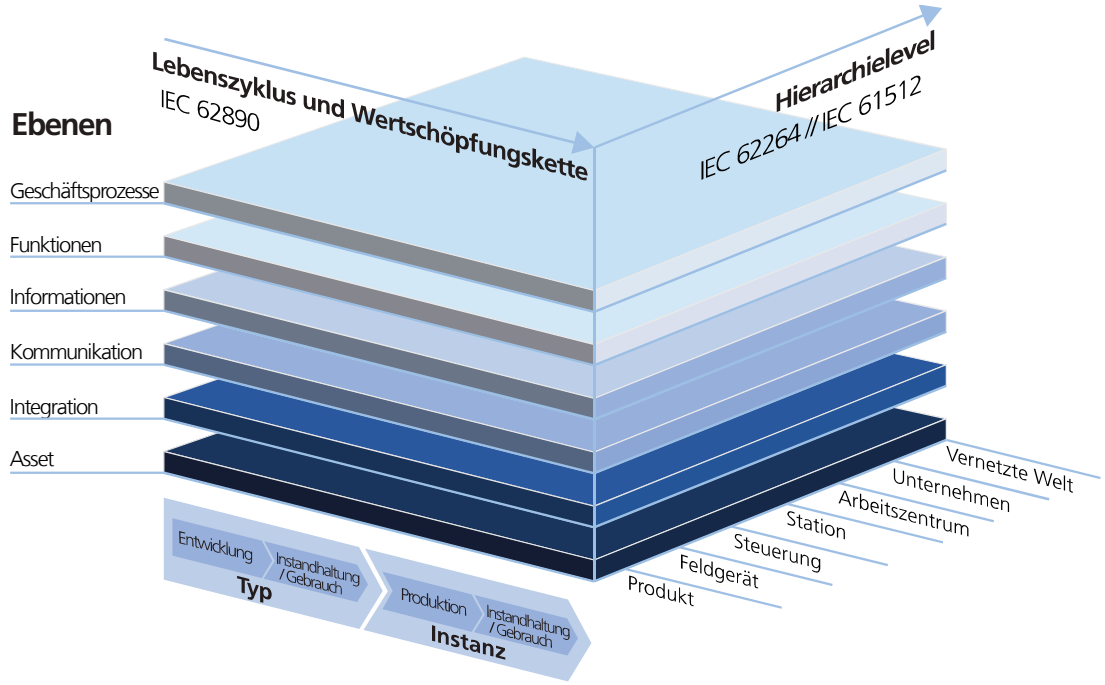


Abbildung A 8 Referenzarchitekturmodell Industrie 4.0 (RAMI 4.0)

Das Modell stellt einen Würfel dar, dessen Achsen alle wesentlichen Aspekte von Industrie 4.0 abbilden und folgende Bedeutung haben (Heidel et al. 2017, S. 45f; Bedenbender et al. 2019, S. 15):

- **„Lebenszyklus und Wertschöpfungskette"-Achse (links horizontal):**
  Hier wird der Lebenszyklus von Anlagen und Produkten dargestellt, der sich an der IEC 62890 zum Life-Cycle-Management orientiert. Dabei wird zwischen Typen und Instanzen von Produkten unterschieden, je nachdem ob sie sich noch in einer Planungs- und Fertigungsphase oder schon im Einsatz befinden.
- **„Hierarchielevel"-Achse (rechts horizontal):**
  Hier werden die gängigen Hierarchiestufen der Produktions-IT nach IEC 62264/ISA95 bzw. IEC 61512-1/ISA88 (vgl. Abschnitt 2.1.2) dargestellt. Allerdings wurden sie um die Stufe „Produkt" und „Connected World" erweitert, um den Vernetzungs- bzw. IoT-Aspekt einer I4.0-Umgebung abzubilden.
- **„(Architektur-)Ebenen"-Achse (vertikal):**
  In der IKT werden Schichtmodelle eingesetzt, um komplexe Sachverhalte in Bezug auf Systeme oder Produkte und ihre IT-Architektur darzustellen. Hier finden sich sechs Ebenen, die vom Asset, über die Integrations-, Kommunikations-, Informations-, funktionale und Businessschicht eingeteilt das digitale Abbild dieses Assets, beispielsweise einer Maschine als I4.0-Komponente, darstellen.

RAMI 4.0 ist in Form der DIN-SPEC 91345 als nationales Standarddokument verabschiedet (Norm DIN SPEC 91345) und wird über die IEC auch in die internationale Standardisierung eingebracht.

In ähnlicher Weise haben andere Länder ebenfalls eigene Referenzarchitekturmodelle entwickelt. Hier ist insbesondere die Industrial Internet Reference Architecture (IIRA) des Industrial Internet Consortium (IIC) zu nennen. Das IIC ist im Vergleich zur Plattform Industrie 4.0 nicht von einer Regierung eingesetzt, sondern stellt einen Verbund privater Unternehmen aus dem Bereich der IKT dar. Jedoch ist die IIRA ein umfangreiches Konzept mit Fokus auf „Ende zu Ende" IIoT-Anwendungen. RAMI 4.0 hat allerdings insbesondere im Hinblick auf die „Lebenszyklus und Wertstrom"-Achse eine Besonderheit aufzuweisen. Die Erschaffer des Modells hatten den Anspruch, den Lebenszyklus einer Industrie 4.0-Komponente komplett abzubilden und einzubeziehen. Eine Industrie 4.0-Komponente ist die Komposition aus Asset, also einer beliebigen Entität von Wert für ein Unternehmen,

und einer standardisierten virtuellen Repräsentation dieses Assets. Diese virtuelle Repräsentation ist eines der Kernkonzepte des RAMI 4.0 und wird als Verwaltungsschale bezeichnet, die in Abschnitt 3.2.3 im Detail diskutiert wird.

Die vorliegende Arbeit ist inhaltlich an diesen Kernkonzepten und Standards ausgerichtet. Dies ist einerseits persönlich durch die inhaltlichen Arbeiten des Autors an diesen Themen begründet, andererseits durch die unmittelbare Relevanz des zu entwickelnden Konzepts für die damit verbundenen industriellen Anwendungen.

Anhang 3 – Sicherheit in einer vernetzten Produktion

Die digitale Transformation der Produktion und die damit verbundene Vernetzung hat neben den in Anhang 1 genannten Vorteilen auch Nachteile mit sich gebracht. Diese Nachteile äußern sich hauptsächlich in Form verschiedener sicherheitsrelevanter Aspekte, die Einfluss auf das gesamte Unternehmen und sämtliche Assets auf allen Ebenen haben (Bachlechner et al. 2016, S. 13). Betroffen sind hier sowohl die Maschinen, IT-Systeme, geistiges Eigentum als auch Personen. Maschinen und somit die Produktion können beispielsweise durch unbefugte Dritte beschädigt, IT-Systeme manipuliert, geistiges Eigentum gestohlen und Daten von Mitarbeitern und Kunden missbraucht werden (Bitkom 2018, S. 20–21). Abbildung A 9 stellt u. a. dar, wie sich Zwischenfälle dieser Art in den letzten Jahren entwickelt haben.

Seit 2016 waren vor allem Ransomwares, die vernetzte IT-Systeme übernehmen und gegen Lösegeld ggf. wieder freigeben, für einen starken Anstieg der Zwischenfälle verantwortlich. Sicherheitsforscher prognostizieren das IoT als das nächste große Angriffsziel. Zudem sehen sie mehrstufige Authentifizierung und „Identity Intelligence", also den analytische Ansatz zur Absicherung der Identität einer Entität auf Basis möglichst vieler Informationen über die Entität, als möglichen effektiven Schutz gegen Cyber-Angriffe (Mcafee Labs 2018).

Die Wahrscheinlichkeit des Auftretens dieser definierten Gefahren in Kombination mit dem Ausmaß der Folgen des Auftretens werden als Risiko definiert (Kaplan et al. 1981).

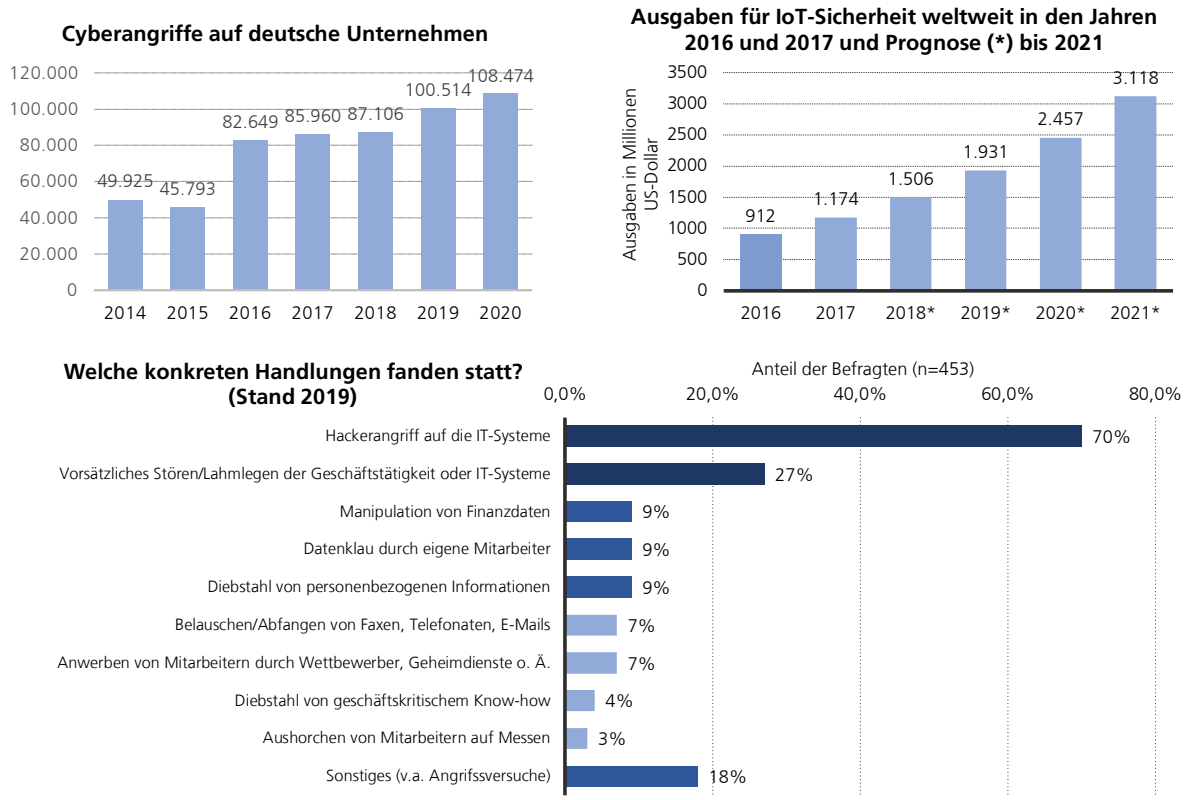


Abbildung A 9 Angriffe und Angriffsarten auf deutsche Unternehmen (Datenquellen: (Bundeskriminalamt 2021; Gartner 2017; Meseke et al. 2019))

Die vorliegende Arbeit hat zum Ziel dazu beizutragen, dieses Risiko zu mindern, indem die Wahrscheinlichkeit des Auftretens dieser Gefahren durch bestimmte Sicherheitsmaßnahmen reduziert wird. Allerdings ist Sicherheit im Umfeld der Produktion ein vielschichtiger Begriff und soll im folgenden Abschnitt in ihren jeweiligen Ausprägungen betrachtet und in Bezug gesetzt werden.

Anhang 3.1 – Sicherheit – Begriffsklärung

Der Begriff der Sicherheit wird in seiner allgemeinen Bedeutung als höchstmögliches Freisein von Gefährdungen definiert (Dudenredaktion 2019c). Im Kontext soziotechnischer Systeme ist im deutschsprachigen Sprachraum der Begriff jedoch zu undifferenziert. Im

Englischen wird zwischen der Security und Safety unterschieden. Daher wird im allgemeinen deutschen Sprachgebrauch in Bezug auf Sicherheit auch zwischen diesen beiden Begriffen unterschieden, um diese Unterscheidung nicht der Interpretation aus dem Kontext zu überlassen (Keller et al. 2019, S. 1). Safety (Betriebssicherheit) hat den Schutz der Umgebung vor einem Objekt oder dem Fehlverhalten des Systems zum Hauptziel.

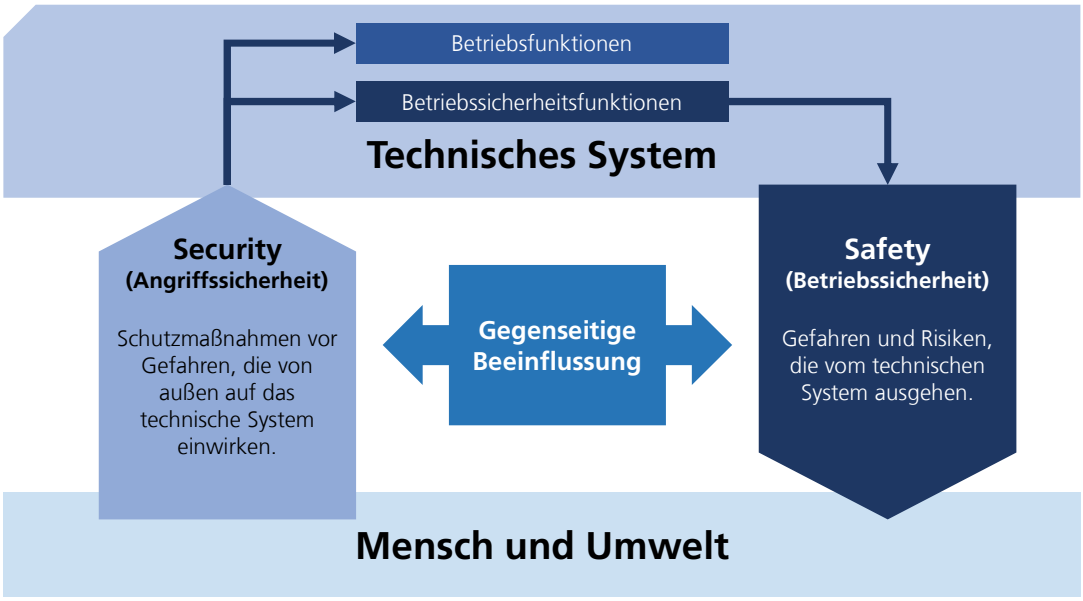


Abbildung A 10 Safety und Security eines technischen Systems in Anlehnung an (VDE 2019)

Die Unversehrtheit von Mensch und Umwelt steht hier an oberster Stelle, was durch Maßnahmen erreicht wird, die einen sicheren Betrieb einer Anlage ermöglichen (Menz et al. 2015, S. 7; Norm VDI/VDE 2182 Blatt 2.3). Dem gegenüber steht die Security (Angriffssicherheit), die den Schutz von Systemen vor unbefugten Zugriffen von außen sowie den Schutz sensibler Daten vor Verfälschung, Verlust und unbefugtem Zugriff zum Ziel hat, weshalb sie im Deutschen auch als Angriffssicherheit bezeichnet wird (Menz et al. 2015, S. 8; Bachlechner et al. 2016, S. 189). Abbildung A 10 stellt diesen Sachverhalt schematisch dar.

Weiterhin lässt sich Sicherheit in ihren Ausprägungen der Angriffssicherheit und Betriebssicherheit weiter differenzieren. So geht die zur Safety gehörende funktionale Sicherheit

davon aus, dass das betrachtete „sichere" System geschlossen ist und nur definierte Zustände einnehmen kann, die im Fall einer Fehlfunktion einen fehlerhaften Zustand vermeiden sollen (Keller et al. 2019, S. 1; Menz et al. 2015, S. 7).

Da jedoch vernetzte Systeme heutzutage grundsätzlich nicht mehr als geschlossen angenommen werden können, muss man in Hinblick auf funktionale Sicherheit auch untersuchen, wie sich ein System bei unbeabsichtigtem oder absichtlichem Fehlgebrauch gegenüber dem Sollzustand verhält. Dies wird im Rahmen der Gebrauchssicherheit (Safety-in-use) geprüft (Hölz 2018, S. 4).

Angriffssicherheit (Security) lässt sich unterteilen in:

- **Informationssicherheit** (Information Security) dient dem Schutz von Daten und Informationen aller Art und umfasst die gesamtheitlich dazu eingesetzten Maßnahmen.
- **IT-Sicherheit** (IT Security) beinhaltet alle technischen Maßnahmen und ist unterteilt in:
    - Physische IT-Sicherheit (Baulicher Schutz, Infrastruktur, Redundanz, technische Sicherheitssysteme)
    - Technische IT-Sicherheit (Redundanz, Diversifizierung, Verteilung)
    - Logische IT-Sicherheit (Organisation, Backup, Netzwerkdesign, Prozesse)
- **Datensicherheit** (Data Security) ist die Summe der Maßnahmen zur Sicherung von Daten.

Sollen im Gegensatz zur allgemeinen Datensicherheit personenbezogene Daten geschützt werden, spricht man von **Datenschutz** (Privacy).

Eine Erweiterung der IT-Sicherheit stellt die **Cyber-Sicherheit** (Cyber Security) dar. Diese befasst sich mit allen Facetten der Sicherheit in der Informations- und Kommunikationstechnik, weitet die Belange der Informationssicherheit jedoch auf den gesamten Cyber-Raum aus. Dieser besteht aus allen durch das Internet weltweit über territoriale Grenzen hinweg erreichbaren Informationsinfrastrukturen (BSI 2014, S. 15). Auf diesen werden Kommunikation, Anwendungen, Prozesse und Informationen ausgeführt, verarbeitet und transportiert. Daher liegt bei der Cyber-Sicherheit auch ein spezieller Fokus auf Cyber-

Angriffe, die den Cyber-Raum als Hauptangriffsweg nutzen oder selbst als Ziel eines Angriffs auslegen (BSI 2017b, S. 84).

Der Fokus dieser Ausarbeitung liegt auf der IT-Sicherheit bzw. Cyber-Sicherheit im Kontext global vernetzter CPS. Abbildung A 11 stellt die genannten Arten von Sicherheit zur besseren Übersicht in Bezug zueinander.

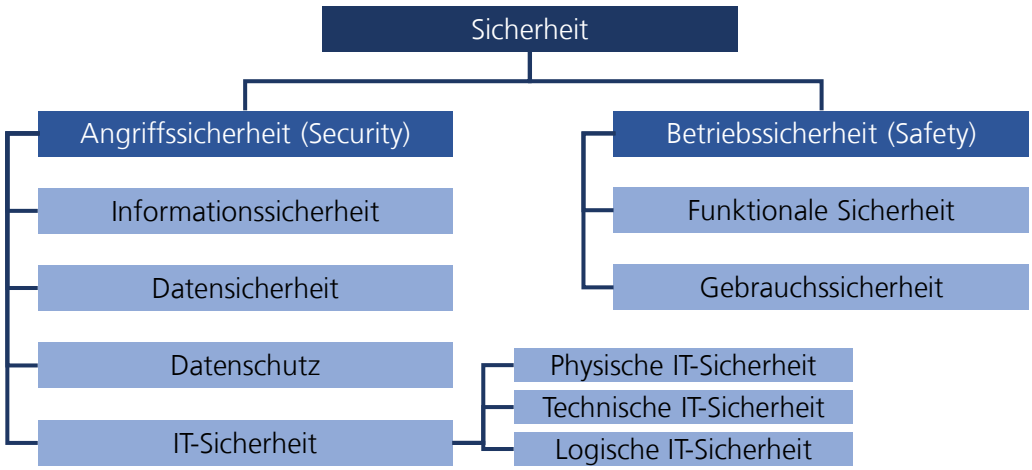


Abbildung A 11 Sicherheitsarten in Bezug zueinander

Es ist erkennbar, dass diese Aspekte der Sicherheit eines Systems nicht getrennt betrachtet werden können. Insbesondere durch willkürlichen Einfluss von außen auf die Maßnahmen der IT-Sicherheit wird mit hoher Wahrscheinlichkeit auch die Betriebssicherheit in Mitleidenschaft gezogen (Keller et al. 2019, S. 432; Jasperneite 2011).

In Hinblick auf das Risiko des Auftretens einer definierten Gefahr ist die sog. statistische Sicherheit ein Begriff, der im Kontext der IT-Sicherheit relevant ist. Aus der Sicht der IT-Sicherheit ist ein absolut sicheres System, also ein System dessen Maßnahmen für Angriffssicherheit für einen Angreifer unüberwindbar sind, zum aktuellen Zeitpunkt und auf absehbare Zeit technisch nicht realisierbar. Dies liegt daran, dass diese Maßnahmen oft in einem Zielkonflikt stehen und wirtschaftlich darstellbar sein müssen. Verfügt dieser An-

greifer über ausreichend Ressourcen, können diese Maßnahmen gebrochen und überwunden werden. Die statistische Sicherheit ist in diesem Kontext die Wahrscheinlichkeit, dass die technischen Maßnahmen zur Absicherung eines technischen Systems von einem Angreifer überwunden werden können. Die vorliegende Ausarbeitung möchte zum Zweck der Risikominderung eine Steigerung der statistischen Sicherheit erreichen. Dies soll durch zusätzliche Maßnahmen erreicht werden, die minimale oder keine Auswirkung auf die eingesetzten Ressourcen haben und zugleich die Aufwände des Angreifers unverhältnismäßig steigern, sodass das Risiko eines Eindringens stark verringert wird.

Anhang 3.2 – Cyber-Sicherheit und Schutzziele

Um eine umfassende Informationssicherheit garantieren zu können, wurden Schutzziele für die IT definiert, die dem Schutz der Systeme und Daten dienen. Insbesondere Cyber-Angriffe, also beabsichtigte böswillige Angriffe auf IT-Systeme stehen hier im Mittelpunkt (Whitman et al. 2011, S. 1). Die drei ursprünglichen Ziele werden auch als CIA-Triade bezeichnet, abgeleitet aus den Anfangsbuchstaben der Englischen Begriffe dieser Schutzziele (BSI 2013, S. 11; Landoll 2011, S. 6):

- **Vertraulichkeit (Confidentiality):**
  Sicherstellung, dass nur autorisierte Personen Zugriff auf bestimmte Daten und Informationen haben.
- **Verfügbarkeit (Availability):**
  Allzeitiger Zugriff auf Daten ist die Voraussetzung für die Funktion kritischer Anwendungen und Prozesse.
- **Integrität (Integrity):**
  Verhinderung, dass Daten auf unbefugte oder unerwünschte Weise geändert werden.

Diese drei Schutzziele der IT-Sicherheit allein reichen schon seit Langem nicht mehr aus, um den Herausforderungen der sich fortlaufend ändernden IT-Landschaft gerecht zu wer-

den (Whitman et al. 2011, S. 8). Daher gibt es mittlerweile weitere Schutzziele und Modelle, die die bisherigen erweitern. Ein Beispiel hierfür ist die Parker'sche Hexade, die drei weitere atomare Schutzziele definiert (Andress 2011, S. 7):

- **Besitz (Possession):**
  Daten und Informationen befinden sich auf einem physischen Medium oder Gerät. Gelingt dieses in die falschen Hände, ist das Besitz-Schutzziel verletzt.
- **Nützlichkeit (Utility):**
  Daten und Informationen können unterschiedlichen Nutzen haben. Verschlüsselte Daten sind für einen Angreifer nicht nützlich, wenn dieser keinen Schlüssel besitzt.
- **Authentizität (Authenticity):**
  Die korrekte Zuordnung zum Eigentümer oder Ersteller der betreffenden Daten stellt sicher, dass diese authentisch sind (vgl. Nachweisbarkeit).

Zusätzlich zur bereits genannten Authentizität nennt die Norm ISO 27002 zum Informationssicherheitsmanagement bzw. die ältere ISO/IEC 13335 weitere relevante Schutzziele (Norm ISO/IEC 27002; Norm ISO/IEC 13335-1), um den erweiterten Schutzraum der Cyber-Sicherheit gerecht werden zu können:

- **Zurechenbarkeit (Accountability):**
  Aktionen können auf den korrekten Verantwortlichen zurückverfolgt werden.
- **Nachweisbarkeit bzw. Nichtbestreitbarkeit (Non-Repudiation):**
  Die Fähigkeit, das Eintreten eines beanspruchten Ereignisses oder einer beanspruchten Handlung und seinen Ursprung einer Entität nachzuweisen.
- **Verlässlichkeit (Reliability):**
  Die Eigenschaft eines konsistenten beabsichtigten Verhaltens und Ergebnisses.
- **Resilienz (Resilience):**
  Widerstandsfähigkeit eines Systems, trotz massiver externer oder interner Störungen wieder in den Ausgangszustand zurückzukehren.

Der Schutz personenbezogener Daten ist (Datenschutz) eng mit dem Schutzziel der Vertraulichkeit verbunden und daher nicht erst seit Inkrafttreten der Datenschutz-Grundverordnung (DSGVO) im Jahr 2018 eine Herausforderung zum Erhalt der Informations- bzw. Cyber-Sicherheit.

Im Kontext der Vernetzung und Digitalisierung zeigt sich, dass eine industrielle Anlage nicht nur aus einem einzigen System, sondern aus einer Vielzahl miteinander kommunizierender Teilsysteme besteht. Durch die Kompromittierung nur eines Teilsystems oder der Kommunikation kann das Gesamtsystem durch unterschiedlich schwerwiegende Auswirkungen seine Integrität einbüßen (Dönicke et al. 2018, S. 8). Die vorliegende Arbeit befasst sich mit der Integrität eines Gesamtsystems in Form eines CPS und mit Ansätzen, wie die dieses geschützt werden kann, indem kompromittierte Teil- und Gesamtsysteme identifiziert werden können, wenn sie von ihrem erwarteten Verhalten abweichen. Die weiteren Schutzziele werden vom Autor als nachrangig betrachtet, da diese von einem System, dessen Integrität verletzt wurde, nicht mehr oder kaum eingehalten werden können.

Anhang 3.3 – Cyber-Sicherheit im industriellen Umfeld

Für das industrielle Umfeld im Speziellen gelten prinzipiell dieselben Schutzziele, wie sie im vorherigen Abschnitt für den Bereich der IKT vorgestellt wurden. Allerdings sind in Hinblick auf die OT die Prioritäten anders gelagert. Für allgemeine IT-Systeme sind die klassischen Schutzziele der Vertraulichkeit, Integrität und Verfügbarkeit in ebendieser Reihenfolge relevant. Die Normenreihe für Industrielle Kommunikationsnetze - IT-Sicherheit für Netze und Systeme ISA99/IEC 62443 - stellt die Verfügbarkeit und Integrität über die Vertraulichkeit (Norm IEC/TS 62443-1-1). Dies ist dadurch begründet, dass OT-Systeme in der Produktion verlässlich und mit hoher Verfügbarkeit unter Einhaltung harter Echtzeitanforderungen betrieben werden müssen. IT-Systeme, die in der Vergangenheit eher auf den oberen Ebenen der Unternehmens-IT-Architektur zu finden waren, verarbeiten hingegen oft kunden- und personenbezogene Daten. Hier wiegt die Vertraulichkeit höher als ein möglicher kurzzeitiger Ausfall der Verfügbarkeit oder verzögerter Informationsfluss.

Neben der IEC 62443 Norm behandelt auch die VDI/VDE-Richtlinienreihe 2182 die Informationssicherheit in der industriellen Automatisierung und beschreibt umfassende Maßnahmen zum Erhalt der Schutzziele (Norm VDI/VDE 2182 Blatt 1). Ein aktueller Ansatz des IIC, dem auch die vorliegende Arbeit in Hinblick mit Fokus auf die Systemintegrität folgt, befasst sich mit der Vertrauenswürdigkeit (Trustworthiness) als übergeordnete Systemeigenschaft wie sie Abbildung A 12 zu sehen ist (Durand et al. 2019).

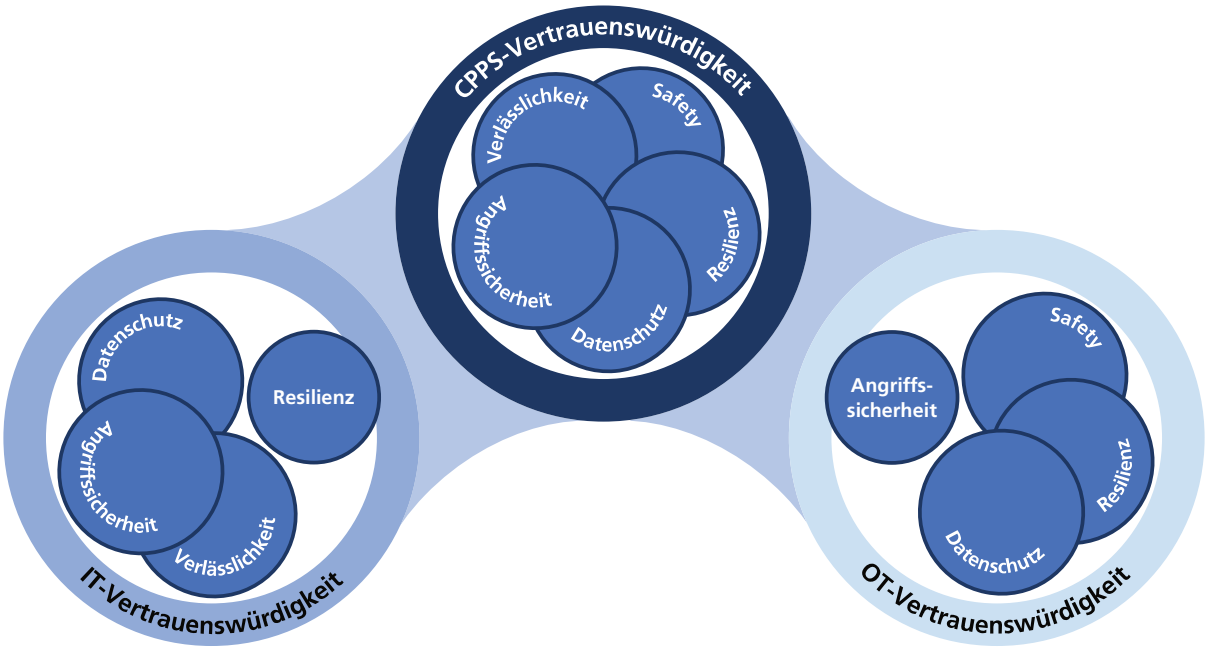


Abbildung A 12 Verschmelzen der OT- und IT-Schutzziele in Anlehnung an (Dönicke et al. 2018; Durand et al. 2019)

Vertrauenswürdigkeit ist eine abstrakte Eigenschaft, die von mehreren Faktoren abhängt. Einer dieser Faktoren sind technische und organisatorische Maßnahmen, die die Sicherheit von Systemen erhöhen. Als eine dieser Maßnahmen sollen Authentifizierungsverfahren auf Basis von Selbstbeschreibungsmerkmalen dazu beitragen durch eine Erhöhung der Vertrauenswürdigkeit die (Cyber-) Sicherheit zu stärken.

Anhang 3.4 – Akteure, Bedrohungsarten und Motivation von Cyber-Angriffen

Die globale Vernetzung ermöglicht Tätern schädliche Aktivitäten in Form von Cyber-Angriffen. Im Kontext der Informationssicherheit werden Angriffe, die darauf abzielen vorhandene Sicherheitsmechanismen zu überwinden, um in ein IKT-System einzudringen, seine Schwächen offen zulegen und es gegebenenfalls zu übernehmen, als Hacking bezeichnet (BSI 2011, S. 80).

Es gibt eine Reihe von Akteuren, die für die Verletzung der Schutzziele verantwortlich sein können. Diese unterscheiden sich grundsätzlich in ihrer Motivation und der Art der definierten Gefahr, die von ihnen ausgeht, da sie über unterschiedliche Fähigkeiten und Ressourcen verfügen (Rogers 2006). Obwohl die Anzahl der Angriffsziele und die Auswahl an Angriffsmethoden umfassend ist, kann die Motivation hinter einem Cyber-Angriff unter anderem häufig auf finanziellen Interessen, Diebstahl von Daten, gezielter Störung (Sabotage), Einflussnahme oder Durchsetzung politischer Interessen bis hin zu Terrorismus fußen (BSI 2012b, S. 3). Um diese Motivation durchzusetzen, werden die folgenden fünf grundlegenden Bedrohungsarten zur Verletzung der Schutzziele eingesetzt (vgl. Anhang 3.2) (BSI 2011, S. 25; Landoll 2011, S. 10; Andress 2011, S. 9):

- **Eindringen/Übernehmen (intrusion):**
  Angreifer dringen mittels Hacking in Systeme ein oder übernehmen diese. Dies dient dazu die Sicherheitsgrundwerte durch Angriffe auf die weiteren Punkte dieser Liste zu beeinträchtigen.
- **Abfangen/Ausspähen/Entwenden (interception):**
  Angreifer erhalten unautorisiert Zugriff auf Daten, wobei das Angriffsziel dies meist nicht mitbekommt.
- **Unterbrechen/Verhindern/Zerstören (interruption):**
  Angreifer verletzten die Verfügbarkeit und Integrität von Daten.
- **Modifizieren/Verändern (modification):**
  Angreifer verletzten die Integrität von bestehenden Daten, so dass das Angriffsziel der Annahme ist, diese seien technisch nicht kompromittiert.

- **Täuschen/Betrügen/Fälschen (fabrication):**
  Angreifer erzeugen Daten mit dem Ziel einen falschen Zustand oder Umstand darzustellen.

Risiken im Umfeld der Cyber-Sicherheit werden grundsätzlich durch beabsichtigte, aber auch durch unbeabsichtigte Ereignisse (events) beeinflusst. Dies sind Geschehnisse, die in irgendeiner Form, meist durch Logging, registriert werden. Das bedeutet, dass eine der in Tabelle 18 genannten Bedrohungen durch eine Aktion eines Akteurs ausgelöst werden kann, ohne dass dieser dies mitbekommt. Ein solches zufälliges Ereignis kann sowohl durch menschliches als auch technisches Versagen ausgelöst werden (Haas 2016, S. 36).

In diesem Fall kann auch davon ausgegangen werden, dass eine Motivation nicht vorhanden ist. Kommt es durch diese Ereignisse zu einem Vorfall (incident), also einem Ereignis, dessen Ursache aufgrund eines Verdachtsfalls aktiv nachgegangen wird, oder infolgedessen sogar zu einem Eindringen (intrusion), sind die Schutzziele dennoch unmittelbar bedroht.

Tabelle 18 Abbildung der Bedrohungen auf die Schutzziele in Anlehnung an (BSI 2011)

Bedrohung / Schutzziel	Eindringen	Abfangen	Unterbrechen	Modifizieren	Täuschen
Vertraulichkeit	•	•			
Integrität	•			•	•
Verfügbarkeit	•		•		
Besitz	•	•	•		
Authentizität	•			•	•
Nützlichkeit	•	•			
Zurechenbarkeit	•				•
Nachweisbarkeit	•				•
Verlässlichkeit	•				•

Die vorliegende Ausarbeitung bezieht sich primär auf beabsichtigte bzw. vorsätzliche Ereignisse bzw. Vorfälle, die im allgemeinen auch den größten Schaden verursachen

(Andress et al. 2013, S. 46). Opfer solcher Angriffe können sowohl staatliche und privatwirtschaftliche Einrichtungen und Infrastrukturen als auch Privatpersonen sein. Das Angriffsziel sind in allen diesen Fällen jedoch grundsätzlich Informationen, IT-Systeme und IT-Dienste in unterschiedlichster Ausprägung (BSI 2012b Anhang B).

Eine Übersicht der möglichen Akteure und ihrer Motivation, bevorzugter Angriffsarten und Ziele bzw. Schutzziele ist in Tabelle 19 dargestellt.

Tabelle 19 Akteure und Motivation von Cyberattacken
in Anlehnung an (Andress et al. 2013, S. 48f; Skopik 2017, S. 55f; BSI 2012b Anhang A S.1)

Art	Staatliche Akteure	Hacker (Individuen)	Kriminelle	Aktivisten	Unternehmen	Insider
Ausprägung	Staaten, Geheim-dienste, Cyber-Krieger	Skript Kiddies, Whitehats, Blackhats	Kleinkriminelle, organisierte Kriminalität	Hacktivisten (politisch, religiös), Cyber-Terroristen	Konkurrenten, Auftragshacker	Mitarbeiter, Dienstleister, Berater, Zulieferer
Motivation	Krieg, Spionage, Patriotismus	Bekanntheit, Neugier, finanzielles Interesse	finanzielles Interesse	Ideologie, Rache	Wirtschafts-spionage, finanzielles Interesse	Rache, finanzielles Interesse
Angriffszweck	Diebstahl, Veröffentlichung, Zerstörung, Erpressung, Sabotage, Spionage	Diebstahl, Erpressung, Ermittlung von Sicherheitslücken	Diebstahl, Erpressung	Veröffentlichung, Zerstörung, Erpressung, Sabotage	Betriebsstörung, Diebstahl, Veröffentlichung, Zerstörung, Erpressung, Sabotage, Spionage	Diebstahl, Erpressung, Sabotage, Ermittlung von Sicherheitslücken

Es ist anzumerken, dass diese Darstellung nicht definitiv ist, da eine Vielfalt von Ansätzen existiert Cyber-Angreifer taxonomisch aufgrund unterschiedlicher Faktoren zu gruppieren. Auch ist eine klare Trennung der Akteure nicht möglich, da zwischen den Gruppen Überschneidungen bis hin zu fließenden Übergängen auftreten.

Anhang 3.5 – Angriffsvektoren und -arten im Cyber-Raum

Angriffsvektoren sind Angriffspfade auf bestimmte Schwachstellen eines Ziels, die die Angriffsfläche bilden (Kruger et al. 2014). Angriffsvektoren können je nach Technologie sehr spezifisch werden. Tabelle 20 gibt eine Übersicht über die üblichen Angriffsvektoren in der IKT bzw. im Cyber-Raum und Tabelle 21 liefert einen beispielhaften Überblick über die dabei eingesetzten Werkzeuge und Methoden.

Tabelle 20 Verschiedene Arten von Angriffsvektoren im Cyber-Raum

Angriffsvektoren	Ausprägung	Angriffsfläche
Passwörter	Passwortdiebstahl, Berechtigungsverletzung	Social Engineering, Phishing, Browser, Email, Brute Force, Schadsoftware
Mitarbeiter	Social Engineering	Browser, Betriebssystem
Prozesse	Systemmanipulation und Ausfall	Betriebssysteme, Dienste, Geräte
Kommunikation	Abhören sensibler Daten	Drahtlose Interfaces, Wifi-Netzwerke
Applikationen	Ausnutzen von Schwachstellen, Drive-by-Attacken	Browser, Messaging-Dienste, Betriebssysteme, Anwender
Geräte	Datenschutz und Berechtigungs-verletzung, physische Angriffe	Baseband-Prozessor, SIM-Karten, Speicherkarten, USB-/ Hardwareschnittstellen, Speicher, Firmware
Cloud-Dienste	Unbefugter Zugriff	Betriebssysteme, Dienste, Geräte
Datenbanken	Unbefugter Zugriff, SQL-Injection	(Web-)Schnittstellen
Netzwerk	Portscans, Man-in-the-Middle, Sybil-Attacke	offene Ports, offene Netzwerke, Vortäuschung einer Geräteidentität

Durch den technischen Fortschritt und Wandel kommt es auch ständig zur Entwicklung neuer Angriffsvektoren (Hunt et al. 2020). Mobile Geräte, die für IoT-Anwendungen eingesetzt werden, nutzen meist automatische Anmeldeverfahren. Erlangt ein Angreifer physischen Zugriff auf das Gerät, kann er es so nutzen um Zutritt zu weiteren Angriffsvektoren zu bekommen (Blowers et al. 2016). Dies ermöglicht Advanced Persistent Threat (APT)-Attacken, bei denen ein Angreifer unbemerkt über einen längeren Zeitraum Zugriff

auf ein Firmennetzwerk und dessen Ressourcen erhält. Ein Beispiel hierfür ist der Stuxnet-Angriff, bei dem eine Urananreicherungsanlage mit Schadsoftware infiziert und über einen längeren Zeitraum unbemerkt die Steuerung der Zentrifugen manipuliert wurde (Karnouskos 2011).

Tabelle 21 Gängige Angriffsarten im Cyber-Raum in Anlehnung an (Andress et al. 2013, S. 49)

Typ	Ausprägung
Schadsoftware (Malware)	Viren, Würmer, Trojaner, Spyware, Rootkits, Adware, Ransomware
Exploits	Drive-by-Exploits, Backdoors
Angriffe auf Personen	Social Engineering, (Spear-)Phishing
Angriffe auf Infrastruktur	Botnetze, DDoS, Sniffing

Anhang 3.6 – Gegenmaßnahmen in der IT-Sicherheit

Ein absoluter Schutz ist zum aktuellen Zeitpunkt in nicht geschlossenen Systemen, wie es ein CPS per Definition ist, nicht umsetzbar (acatech et al. 2015, S. 11). Maßnahmen zur Erhöhung der Sicherheit wirken sich ab einem bestimmten Punkt oft exponentiell negativ auf Kosten der Wirtschaftlichkeit und Praktikabilität aus (Stephan et al. 2018, S. 83) und verringern die Effizienz der Systeme (Hilty et al. 2003, S. 255). Dieser Zusammenhang ist in Abbildung A 13 illustriert.

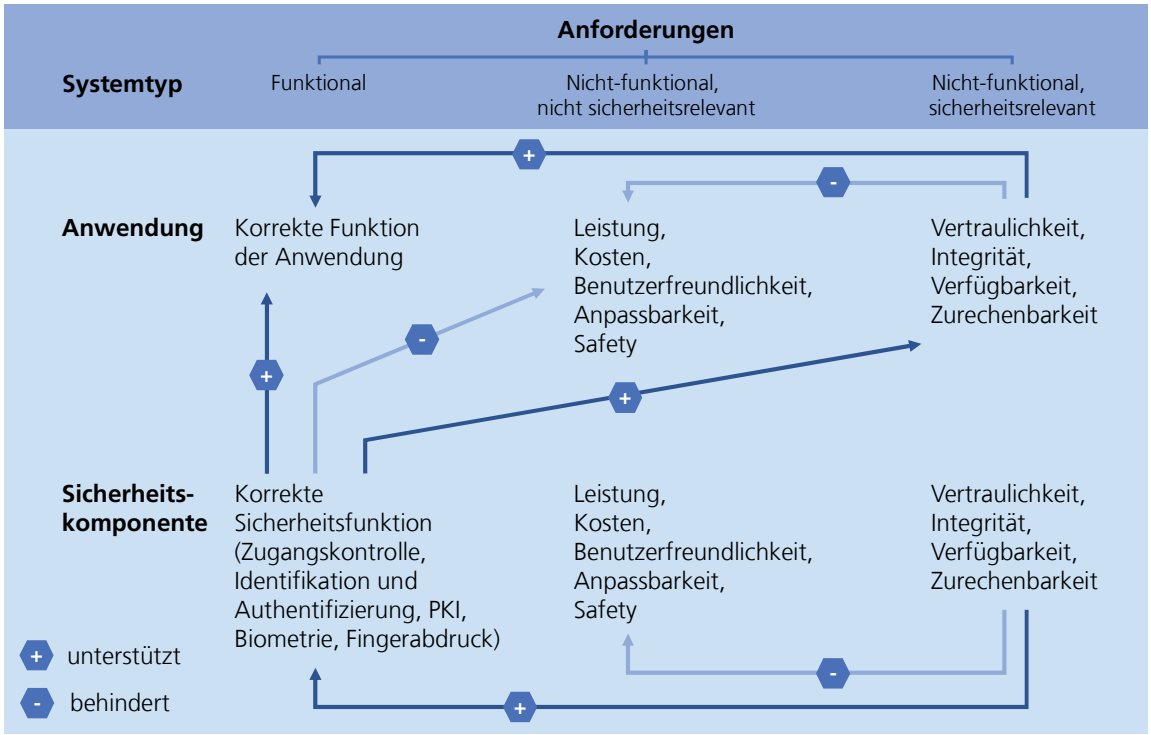


Abbildung A 13 Einfluss und Wechselwirkung von Sicherheitsmaßnahmen nach (Schumacher 2006, S. 33)

Es gibt Ansätze, die es erlauben die Risiken bzw. im Fall eines Cyber-Angriffs die Cyber-Risiken methodisch zu bewerten. Diese ermöglichen es ein sinnvolles Verhältnis zwischen einem akzeptablen Risiko und den Ressourcenaufwänden für Gegenmaßnahmen zu finden (Haas 2016). Die gängigsten Ansätze zum Schutz von IKT-Systemen sind in Tabelle

22 gelistet. Für industrielle Anwendungen von CPS bestehen jedoch weitere Herausforderungen, die die Sicherheitsstandards der Vergangenheit unzureichend abgedeckt haben und die Entwicklung neuer Strategien erfordert haben (Cardenas et al. 2009), die schon im Produktengineering beginnen (Kieseberg et al. 2018).

Tabelle 22 Taxonomie von Sicherheitsmechanismen
in Anlehnung an (Schumacher 2006, S. 18)

Dienste			
Sicherheitsdienste		**Unterstützende Sicherheitsdienste**	
Identifizierung und Authentifizierung, Abschreckung, Kontenverwaltung, Zugangskontrolle, Schutz von Systemgrenzen, Nachweisbarkeit, Systemwiederherstellung		Autorisierung, Systemsicherheitsrichtlinien, Sicherheitsplanung, Registrierung, Betriebswartung, Betriebskonzept, Kontinuität des Betriebs	
Mechanismen und Implementierung (Tools, Produkte oder Prozesse)			
Automatisierte Mechanismen	**Prozedurale Mechanismen**	**Managementgestützte Mechanismen**	**Physische Mechanismen**
Verschlüsselung, Filter Scanner, Firewalls, Proxies, Packet-Sniffer, Integritätsüberwachung, Hashing, Protokollierung, Parser, Kennzeichnung/ Labeling, An- und Abmeldung (Benutzer-ID und Passwörter), Biometrie, Token, Intrusion Detection/ Prevention Systeme, Anomaliedetektion, Zugriffskontrolllisten (ACL), RBAC, digitale Signaturen, Antivirus- und Endpunktschutz	Anmeldung, Backup, Wieder-herstellung, Löschung, Störfallreaktion, Handhabung, Schulung, Sicherheit, Verwaltung, Personal, Konfigurations-verfahren	Informationssystem-Sicherheitsrichtlinien, Schulung, Konfigurations-management, Katastrophenschutz, Wiederherstellung, Connection Service Agreements, Audit	Menschliche Sicherheitskräfte, Türen, Tresore, Schlösser, Sensoren, Wände

Anomalie-Detektion und Intrusion Detection Systeme (IDS) dienen dazu unautorisierte Aktivitäten im Netzwerk oder auf Hostsystemen zu erkennen (Kieseberg et al. 2018). Darüber hinaus existieren auch aktive Gegenmaßnahmen, wie z.B. Honeypots oder Honeynets. Dies sind Systeme, deren einziger Zweck es ist, technisch kompromittiert zu werden. Dies

wird durch absichtlich platzierte Sicherheitslücken erreicht, die Angreifern unter unbemerkter Beobachtung kontrollierten Zugriff ermöglichen, jedoch ohne die Möglichkeit tatsächlichen Schaden anzurichten. Honeypots ermöglichen es einerseits Schadsoftware und Angriffsmuster von Angreifern zu erkennen, zu studieren und Gegenmaßnahmen zu entwickeln. Andererseits können sie als Ablenkung oder zur Angriffserkennung dienen, da eine Aktivität auf einem Honeypot grundsätzlich unautorisiert ist. Somit kann ein „false positive", also ein Fehlalarm, ausgeschlossen werden (Fraunholz et al. 2016).

Der hier verfolge Ansatz ist in Teilen von der Anomalie-Detektion von IDS inspiriert, da Abweichungen von den in einer Selbstbeschreibung definierten Merkmalen ebenso als Anomalien betrachtet werden können.

Anhang 3.7 – Defense-in-Depth

Jede der im vorherigen Abschnitt genannten Maßnahmen ist als Einzelmaßnahme nicht ausreichend, um ein ausreichendes Sicherheitsniveau zu erreichen. Daher wird insbesondere im Bereich der Cyber-Sicherheit für industrielle Anwendungen und Unternehmen eine Defense-in-Depth-Strategie empfohlen, die darauf basiert Maßnahmen auf unterschiedlichen Ebenen zu kombinieren, wie Abbildung A 14 zeigt.

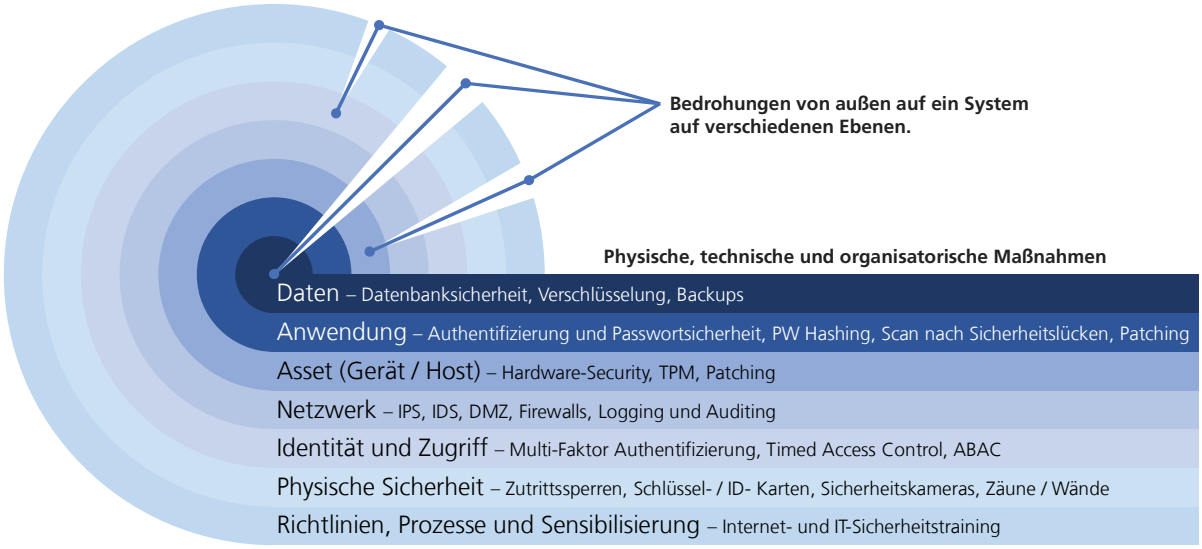


Abbildung A 14 Defense-in-Depth-Prinzip
in Anlehnung an (Andress 2011, S. 13; Norm IEC/TS 62443-1-1)

Dieses Konzept hat seinen Ursprung in der militärischen Strategie und dient dazu Hindernisse zu schaffen, die den Fortschritt von Eindringlingen zur Erreichung ihrer Ziele behindern. Gleichzeitig wird ihr Fortschritt überwacht und Gegenmaßnahmen für den Angriff entwickelt und umgesetzt, um sie abzuwehren (U.S. Department of Homeland Security 2016, S. 2). Grundsätzliche Strategien wie nach dem Defense-in-Depth-Prinzip in industriellen Anwendungen und Produkte umzusetzen sind, sind in der IEC 62443-4-1 Norm für die Anforderungen von Entwicklungslebenszyklen sicherer Produkte aufgeführt (Norm IEC

62443-4-1). Abbildung A 15 zeigt eine Übersicht der für Defense-in-Depth relevanten Aspekte in Form einer Mind-Map.

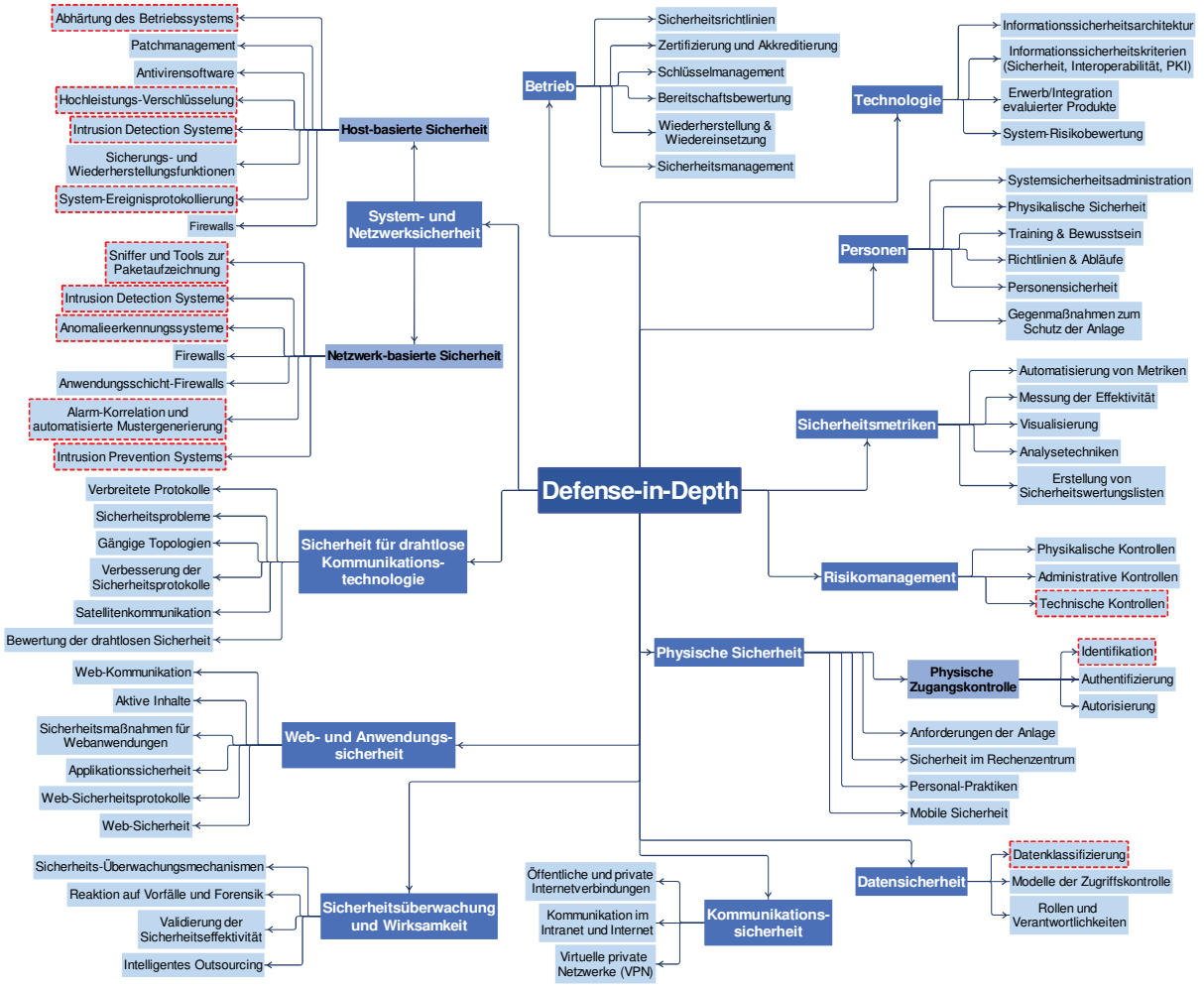


Abbildung A 15 Übersicht der Defense-in-Depth-Aspekte in Anlehnung an (Vacca 2013, S. 14)

Wenn ein Angriff einen Sicherheitsmechanismus zum Versagen bringt, können andere Mechanismen trotzdem die notwendige Sicherheit zum Schutz des Systems bieten.

Die Implementierung einer Verteidigungsstrategie kann die Komplexität einer Anwendung erhöhen, was dem in der Sicherheitsbranche häufig praktizierten Prinzip der Einfachheit zuwiderläuft. Das heißt man könnte argumentieren, dass das Hinzufügen neuer Schutzfunktionen zusätzliche Komplexität schafft, die neue Risiken mit sich bringen kann.

Das Gesamtrisiko für das System muss abgewogen werden. Mindestlängen für Passwörter erhöhen die Komplexität und können dazu führen, dass Benutzer ihre Passwörter aufschreiben, was die Gesamtsicherheit des Systems verringert. Eine Smartcard zur Authentifizierung würde jedoch die Sicherheit durch Hinzufügen einer zusätzlichen Schicht zum Authentifizierungsprozess erhöhen.

Der in der vorliegenden Ausarbeitung verfolge Ansatz ist als Teil einer Defense-in-Depth-Strategie konzipiert und soll somit bestehende Maßnahmen ergänzen. Die hierfür besonders relevanten Aspekte sind in Abbildung A 15 rot markiert. Identifizierung und Authentifizierung (vgl. Abschnitt 4.2.1 und 3.1) sind dabei im Fokus und werden mit Mechanismen und Methoden der in Kapitel 3 vorgestellten Ansätze adaptiert, kombiniert und integriert werden.

Anhang 4 – Selbstbeschreibungs-Beispiele

Abbildung A 16 stellt ein Beispiel für eine einfache Selbstbeschreibung eines CPS dar, welches sich als Smartes Objekt anmeldet. Die Selbstbeschreibung beinhaltet in diesem Fall nur ein Event, welches die Daten für die aktuelle Konzentration von Feinstaub-Partikeln in der Umgebungsluft übermittelt. Die Funktion, die das CPS anbietet, ist zuständig für das Auslesen des aktuellen Werts. Zudem erlaubt das CPS eine Anpassung des Mess- bzw. Sendeintervalls der Partikeldaten mittels eines einstellbaren Parameters.

```
{
   "@class": "SmartObject",
   "uuid": "40ad22ba-b55a-11ea-b75e-ac675d03262b",
   "name": "Particulate_Detector03262b",
   "description": "Detector for fine particulate matter.",
   "token": "03262b",
   "events": [
      {
         "eventId": "P_MATTER_CURRENT",
         "name": "Current particulate concentration",
         "description": "Contains the current reading of particulate matter.",
         "dataFormat": {
            "dataObject": {
               "type": "string"
            }
         },
         "@id": 1
      }
   ],
   "functions": [
      {
         "functionId": "READ_PARTICULATE",
         "name": "Read current particulate",
         "description": "This function reads the current particulate concentration.",
         "dataFormat": {
            "dataObject": {
               "type": "array",
               "items": {
                  "type": "string"
               }
            }
         }
      }
   ],
   "configuration": {
      "parameters": {
         "measurement_interval": {
            "type": "INTEGER",
            "format": "INT32",
            "value": 17
         }
      }
   }
}
```


Abbildung A 16 Einfache CPS Selbstbeschreibung

```
{
   "@class": "SmartObject",
   "uuid": "ef9e8cfd-0450-44be-a9fd-4c1582bdb2b9",
   "name": "Raspberry PI 3 + Enviro+ (1)",
   "description": "Raspberry PI 3 + Enviro+ sensor board",
   "token": "4c1582bdb2b9",
      "metaData": [
      {
         "value": null,
         "selector": "/",
         "name": "SEN",
         "description": "Sensor - device which, when excited by a physical phenomenon, produces an electric signal characterizing
the physical phenomenon",
         "dataFormat": null,
         "isArray": false,
                  "typeDescription": {
            "value": null,
            "identifier": "0112/2///61360_4#AAA103#001",
            "location":
"https://cdd.iec.ch/cdd/iec61360/iec61360.nsf/2a050a792eee78e1c12575560054b803/219d27329351ec25c1257dd300515f6
9",
            "typeDescriptor": "CDD",
            "@class": "TypeDescription"
         },
         "@class": "CustomMetaData"
      },
      {
         "value": null,
         "selector": "/",
         "name": "Fine Particle Sensor",
         "description": "Sensor which measures fine particles",
         "dataFormat": null,
         "isArray": false,
                  "typeDescription": {
            "value": null,
            "identifier": "0112/2///61360_4#AAA103#001-FEIN",
            "location": "",
            "typeDescriptor": "CUSTOM",
            "@class": "TypeDescription"
         },
         "@class": "CustomMetaData"
      },
      {
         "value": "METHOD_STUB_TO_GET_DATA",
         "selector": "/",
         "name": "MUP",
         "description": "CPU - processor whose elements have been miniaturized into an integrated circuit",
         "dataFormat": "string",
         "isArray": false,
                  "typeDescription": {
            "value": null,
            "identifier": "0112/2///61360_4#AAA062#001",
            "location":
"https://cdd.iec.ch/cdd/iec61360/iec61360.nsf/2a050a792eee78e1c12575560054b803/670dc436b7e157cac1257dd300515f41
",
            "typeDescriptor": "CDD",
            "@class": "TypeDescription"
         },
         "@class": "CustomMetaData"
      },
      {
         "value": "METHOD_STUB_TO_GET_DATA",
         "selector": "/",
         "name": "CPU_Architecture",
```


Abbildung A 17 Selbstbeschreibung mit Metadaten

```
if __name__ == "__main__":

    SERVICE_TYPE = "SmartObject"
    SO_UUID = "ef9e8cfd-0450-44be-a9fd-4c1582bdb2b9"
    SO_NAME = "Raspberry PI 3 + Enviro+ (1)"
    SO_DESCRIPTION = "Raspberry PI 3 + Enviro+ sensor board"
    SO_TOKEN = "4c1582bdb2b9"
    myMsbClient = MsbClient(
        SERVICE_TYPE,
        SO_UUID,
        SO_NAME,
        SO_DESCRIPTION,
        SO_TOKEN,
    )

    myMsbClient.addMetaData(CustomMetaData("SEN",
                            "Sensor - device which, when excited by a physical phenomenon, produces an electric signal charac-
terizing the physical phenomenon",
                            TypeDescription(TypeDescriptor.CDD,
                                    "0112/2///61360_4#AAA103#001",
                                    "https://cdd.iec.ch/cdd/iec61360/iec61360.nsf/2a050a792eee78e1c12575560054b803/2
19d27329351ec25c1257dd300515f69")))

    myMsbClient.addMetaData(CustomMetaData("Fine Particle Sensor",
                            "Sensor which measures fine particles",
                            TypeDescription(TypeDescriptor.CUSTOM,
                                    "0112/2///61360_4#AAA103#001-FEIN",
                                    "")))

    myMsbClient.addMetaData(CustomMetaData("MUP",
                            "CPU - processor whose elements have been miniaturized into an integrated circuit",
                            TypeDescription(TypeDescriptor.CDD,
                                    "0112/2///61360_4#AAA062#001",
                                    "https://cdd.iec.ch/cdd/iec61360/iec61360.nsf/2a050a792eee78e1c12575560054b803/6
70dc436b7e157cac1257dd300515f41"),
                            "/",
                            "METHOD_STUB_TO_GET_DATA",
                            DataType.STRING))

    myMsbClient.addMetaData(CustomMetaData("CPU_Architecture",
                            "CPU_Architecture",
                            TypeDescription(TypeDescriptor.CUSTOM,
                                    "0112/2///61360_4#AAA062#001",
                                    ""),
                            "/",
                            "METHOD_STUB_TO_GET_DATA",
                            DataType.STRING))

    myMsbClient.addMetaData(CustomMetaData("RAM",
                            "memory that permits access to any of its address locations in any desired sequence",
                            TypeDescription(TypeDescriptor.CDD,
                                    "0112/2///61360_4#AAA062#001",
                                    "https://cdd.iec.ch/cdd/iec61360/iec61360.nsf/2a050a792eee78e1c12575560054b803/6
70dc436b7e157cac1257dd300515f41"),
                            "/",
                            "METHOD_STUB_TO_GET_DATA",
                            DataType.DOUBLE))

    myMsbClient.addMetaData(CustomMetaData("OS_platform",
                            "Operating system platform",
                            TypeDescription(TypeDescriptor.CUSTOM,
                                    "OS_platform",
                                    "")
```

Abbildung A 18 Python Code-Beispiel zur programmatischen Erstellung einer CPPS-Selbstbeschreibung

Anhang 5 – Fingerprint-Teilmodell-Mapping

Das Mapping des internen MSB-Datenmodells auf ein VWS-Teilmodell wie in Abbildung A 19 dargestellt möglich.

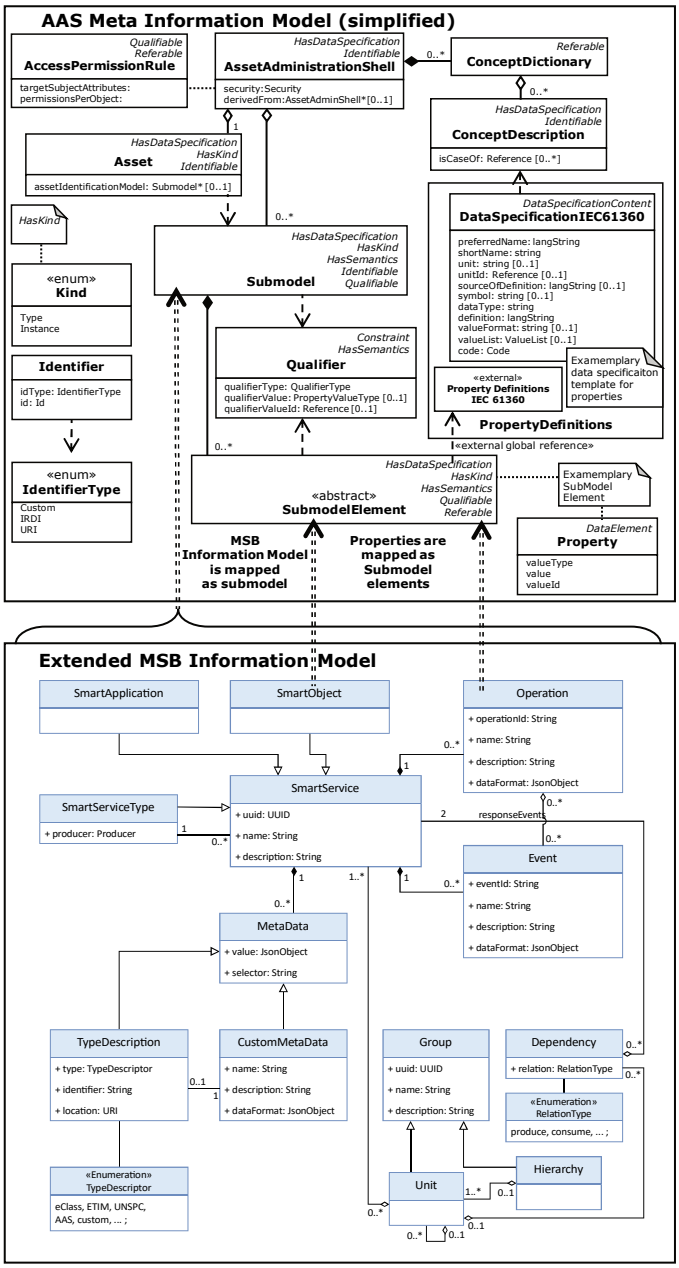


Abbildung A 19 Mapping des MSB-Datenmodells auf den hybriden Fingerabdruck im VWS-Teilmodell-Format

Anhang 6 – Übersicht eingebetteter Systeme für CPS-Prüfstand

Tabelle 23 listet die im Rahmen der Arbeit für eine Merkmalsprüfung verwendeten und zusätzliche x86-basierte Geräte. Dabei liegt das Hauptaugenmerk auf eingebetteten Systemen, die im CPS-Prüfstand integriert sind.

Tabelle 23 Übersicht eingebetteter Systeme für CPS-Prüfstand

Gerät	Hostname	Betriebssystem	SoC	CPU	Kerne	Frequenz	RAM
Onlogic ML100G-31	IIoTcenter	Ubuntu 18.04.4 LTS	Intel Core	i7-8650U	4(+4)	1,9/4,2 GHz	32 GB
Onlogic CL210G	Kalinuc	Kali GNU/Linux Rolling	Intel Celeron	N3350	2(+2)	1,1/2,4 GHz	4 GB
Raspberry Pi 1	Raspi-1	Raspbian GNU/Linux 10	BCM2835	ARM1176JZF-S	1	0,7 GHz	256 MB
Raspberry Pi 2	Raspi-2	Raspbian GNU/Linux 10	BCM2836	ARM Cortex-A7	4	0,9 GHz	1 GB
Raspberry Pi 3	Raspi-3	Raspbian GNU/Linux 10	BCM2837	ARM Cortex-A53	4	1,2 GHz	1 GB
Raspberry Pi 3 A+	Raspi-3-Ap	Raspbian GNU/Linux 10	BCM2837B0	ARM Cortex-A53	4	1,4 GHz	512 MB
Raspberry Pi 3 B+	Raspi-3-Bp	Raspbian GNU/Linux 10	BCM2837B0	ARM Cortex-A53	4	1,4 GHz	1 GB
Raspberry Pi 4 1GB	Raspi-4-1GB	Raspbian GNU/Linux 10	BCM2711	ARM Cortex-A72	4	1,5 GHz	1 GB
Raspberry Pi 4 2GB	Raspi-4-2GB	Raspbian GNU/Linux 10	BCM2711	ARM Cortex-A72	4	1,5 GHz	2 GB
Raspberry Pi 4 4GB (1)	Raspi-4-4GB-1	Raspbian GNU/Linux 10	BCM2711	ARM Cortex-A72	4	1,5 GHz	4 GB
Raspberry Pi 4 4GB (2)	Raspi-4-4GB-2	Raspbian GNU/Linux 10	BCM2711	ARM Cortex-A72	4	1,5 GHz	4 GB
Rasp. Pi Dev Board - CM1	Raspi-Dev-1	Raspbian GNU/Linux 10	BCM2835	ARM1176JZF-S	1	0,7 GHz	512 MB
Rasp. Pi Dev Board - CM3	Raspi-Dev-2	Raspbian GNU/Linux 10	BCM2837	ARM Cortex-A53	4	1,2 GHz	1 GB
Rasp. Pi Dev Board - CM3+	Raspi-Dev-3	Raspbian GNU/Linux 10	BCM2837B0	ARM Cortex-A53	4	1,2 Ghz	1 GB
Raspberry Pi CM4 IOBoard	Raspi-Dev-4	Raspbian GNU/Linux 10	BCM2711	ARM Cortex-A72	4	1,5 Ghz	8 GB
Raspberry Pi CM4 IOBoard	Raspi-Dev-5	Raspbian GNU/Linux 10	BCM2711	ARM Cortex-A72	4	1,5 Ghz	8 GB
Raspberry Pi Zero W 1	Raspi-Zero-W-1	Raspbian GNU/Linux 10	BCM2835	ARM1176JZF-S	1	1,0 GHz	512 MB
Raspberry Pi Zero W 2	Raspi-Zero-W-2	Raspbian GNU/Linux 10	BCM2835	ARM1176JZF-S	1	1,0 GHz	512 MB
Raspberry Pi Zero W 3	Raspi-Zero-W-3	Raspbian GNU/Linux 10	BCM2835	ARM1176JZF-S	1	1,0 GHz	512 MB
Raspberry Pi Zero W 4	Raspi-Zero-W-4	Raspbian GNU/Linux 10	BCM2835	ARM1176JZF-S	1	1,0 GHz	512 MB
Beaglebone Black	Beaglebone-Black	Debian GNU/Linux 10	AM3358/9	ARM Cortex-A8	1	1,0 GHz	512 MB
Raspberry PI 3 + Enviro+	Raspi-3-Particle-1	Raspbian GNU/Linux 10	BCM2837	ARM Cortex-A53	4	1,2 GHz	1 GB
Raspberry PI 3 + Enviro+	Raspi-3-Particle-2	Raspbian GNU/Linux 10	BCM2837	ARM Cortex-A53	4	1,2 GHz	1 GB
Raspberry Pi 4 4GB (3)	Raspi-4-4GB-3	Raspbian GNU/Linux 10	BCM2711	ARM Cortex-A72	4	1,5 GHz	4 GB
Raspberry Pi 4 4GB (4)	Raspi-4-4GB-4	Raspbian GNU/Linux 10	BCM2711	ARM Cortex-A72	4	1,5 GHz	4 GB
Raspberry Pi 4 8GB	Raspi-4-8GB	Raspbian GNU/Linux 10	BCM2711	ARM Cortex-A72	4	1,5 GHz	8 GB
Raspberry Pi 4 8GB (C)	Raspi-4-8GB-C	Raspbian GNU/Linux 10	BCM2711	ARM Cortex-A72	4	1,5 GHz	8 GB
Raspberry Pi 4 8GB (D)	Raspi-4-8GB-D	Raspbian GNU/Linux 10	BCM2711	ARM Cortex-A72	4	1,5 GHz	8 GB
Google Coral Dev Board	Coral-Dev-Board-1	Mendel GNU/Linux 4	NXP i.MX 8M	ARM Cortex-A53	4	1,5 GHz	1 GB
Banana Pi M2 Zero	Bananapi-M2-Zero	Armbian 20.08 Buster	Allwinner H2+	ARM Cortex-A7	4	1,2 GHz	512 MB
Banana Pi M2+	Bananapi-M2p	Raspbian GNU/Linux 9	Allwinner H3	ARM Cortex-A7	4	1,2 GHz	1 GB
Banana Pi M3	Bananapi-M3	Armbian 20.08 Buster	Allwinner A83T	ARM Cortex-A7	8	1,8 GHz	2 GB
Orange Pi Zero	Orangepi-Zero	Debian GNU/Linux 10	Allwinner H2+	ARM Cortex-A7	4	1,2 GHz	256 MB
Revolution Pi 1 (17747)	RevPi-1-17747	Raspbian GNU/Linux 9	BCM2835	ARM1176JZF-S	1	0,7 GHz	512 MB
Revolution Pi 3 (19181)	RevPi-3-19181	Raspbian GNU/Linux 9	BCM2837	ARM Cortex-A53	4	1,2 GHz	1 GB
Revolution Pi 3+ (32760)	RevPi-3p-32760	Raspbian GNU/Linux 9	BCM2837B0	ARM Cortex-A53	4	1,2 GHz	1 GB
Sotec CloudPlug Edge	SOCP2001-20011111	Poky (Yocto Dist.) 2.7.1	NXP i.MX 7	ARM Cortex-M4	2	1,2 GHz	1 GB
Siemens Simatic IOT2050	Siemens-Simatic-IOT2050	Debian GNU/Linux 10	TI AM6548 HS	ARM Cortex-A53	4	1,0 GHz	2 GB
Siemens Simatic IOT2040	Siemens-Simatic-IOT2040	IOT2000 Image V2.6.0	Intel Quark	x1020	1	0,4 GHz	1 GB
Siemens Simatic IOT2020	Siemens-Simatic-IOT2020	IOT2000 Image V2.6.0	Intel Quark	x1000	1	0,4 GHz	512 MB
***Lenovo ThinkPad P52**	IPA-WN1111	Windows 10 (Build 2004)	Intel Core	i7-8850H	6(+6)	2,6/4,3 Ghz	32 GB
***Dell XP15 9550**	nindev	Windows 10 (Build 2004)	Intel Core	i7-6700HQ	4(+4)	2,6/3,5 Ghz	32 GB
***Dell XPS13 9370**	ubuntudev	Ubuntu 18.04.4 LTS	Intel Core	i7-8550U	4(+4)	1,8/4.0 Ghz	16 GB
***Dell XPS13 7390 2in1**	ninice	Windows 10 (Build 2004)	Intel Core	i7-1065G7	4(+4)	1,3/3,9 Ghz	32 GB
***Intel NUC Kit NUC6i7KYK**	ultradevnuc	Ubuntu 20.04.1 LTS	Intel Core	i7-6770HQ	4(+4)	2.6/3,5 Ghz	32 GB

* Weitere Referenzgeräte mit denen Messungen durchgeführt wurden, die jedoch nicht Teil des CPS-Prüfstands sind.

Anhang 7 – Ergänzende Informationen zu Versuchsaufbau 1

Anhang 7.1 – Beispiel 1 – Systemdaten als Merkmal

Die in Anhang 6 gelisteten eingebetteten Systeme verfügen über unterschiedliche Systemdaten bzw. -konfigurationen. Diese Informationen lassen sich wie in Kapitel 3.3 beschrieben ebenfalls als Merkmale nutzen. Um die Informationen abzufragen, wurde ein Python-Skript verwendet, welches prinzipiell sowohl auf Linux- als auch auf Windows-Systemen ausführbar ist. Allerdings wurden im Versuchsaufbau nur Linux-basierte Hostsysteme verwendet. Einige Beispiele für die Systemdatenprofile sind im Folgenden in Abbildung A 20 gelistet. Die Informationen zu den Netzwerkschnittstellen wurden teilweise aus Platzgründen gekürzt.


```
{
   "hw": {
      "architecture": "i586",
      "cpu-cores": 1,
      "cpu-temp": "null",
      "cpu-use": "22.6",
      "processor": "Quark SoC X1000",
      "ram": {
         "free": "412.7",
         "total": "491.1",
         "used": "25.0"
      },
      "storage": {
         "free": "1.3G",
         "percentage": "10%",
         "remaining": "13G",
         "total": "14G"
      }
   },
   "network": {…  …},
   "os": {
      "hostname": "Siemens-Simatic-IOT2020",
      "platform": "Linux",
      "platform-release": "4.4.185-cip35",
      "platform-version": "#1 PREEMPT Thu Dec 26 06:28:31 UTC 2019",
      "serial": "0000000000000000",
      "uptime": 4191944.75
   }
}
```

```
{
   "hw": {
      "architecture": "armv7l",
      "cpu-cores": 4,
      "cpu-temp": 35.05,
      "cpu-use": "0.0",
      "processor": "ARMv7 Processor rev 3 (v7l)",
      "ram": {
         "free": "7692.7",
         "total": "8157.2",
         "used": "99.7"
      },
      "storage": {
         "free": "1.5G",
         "percentage": "11%",
         "remaining": "13G",
         "total": "15G"
      }
   },
   "network": {
      "eth0": {
         "10": [
            {
               "addr": "fe80::6561:6752:c717:1bf9%eth0",
               "netmask": "ffff:ffff:ffff:ffff::/64"
            }
         ],
         "17": [
            {
               "addr": "dc:a6:32:be:ce:0e",
               "broadcast": "ff:ff:ff:ff:ff:ff"
            }
         ],
         "2": [
            {
               "addr": "192.168.1.126",
               "broadcast": "192.168.1.255",
               "netmask": "255.255.255.0"
            }
         ]
      },
      "lo": {...}
   },
   "os": {
      "hostname": "Raspi-4-8GB-C",
      "platform": "Linux",
      "platform-release": "4.19.118-v7l+",
      "platform-version": "#1311 SMP Mon Apr 27 14:26:42 BST 2020",
      "serial": "10000000bda0ba18",
      "uptime": 48024.82
   }
}
```

```
{
   "hw": {
      "architecture": "x86_64",
      "cpu-cores": 8,
      "cpu-temp": "null",
      "cpu-use": "13,5",
      "processor": "Intel(R) Core(TM) i7-6770HQ CPU @ 2.60GHz",
      "ram": {
         "free": "27020.1",
         "total": "32771.2",
         "used": "1752.2"
      },
      "storage": {
         "free": "22G",
         "percentage": "5%",
         "remaining": "413G",
         "total": "457G"
      }
   },
   "network": {
      "docker0": {…},
      "eno1": {
         "10": [
            {
               "addr": "fe80::aa24:12c1:68d1:e56f%eno1",
               "netmask": "ffff:ffff:ffff:ffff::"
            }
         ],
         "17": [
            {
               "addr": "00:1f:c6:9b:b0:b2",
               "broadcast": "ff:ff:ff:ff:ff:ff"
            }
         ],
         "2": [
            {
               "addr": "172.21.5.78",
               "broadcast": "172.21.5.255",
               "netmask": "255.255.255.0"
            }
         ]
      },
      "lo": {…},
      "wlp3s0": {…}
   },
   "os": {
      "hostname": "ultradevnuc",
      "platform": "Linux",
      "platform-release": "5.4.0-42-generic",
      "platform-version": "#46-Ubuntu SMP Fri Jul 10 00:24:02 UTC 2020",
      "serial": "0000000000000000",
      "uptime": 228010.36
   }
}
```


Abbildung A 20 Strukturierte Informationen zu den Systemdaten eines eingebetteten Systems

Anhang 7.2 – Beispiel 2 – Speicherleistung als Merkmal

Bei vielen eingebetteten Systemen kommen SD-Karten als Speicher zum Einsatz. Wie bereits erwähnt unterscheiden sich diese in ihren Leistungsdaten stark. Zudem kann der integrierte Flash-Speicher, der beispielsweise auf den industrietauglichen Raspberry Pi Compute Modulen zum Einsatz kommt, sogar bessere Leistungsdaten aufweisen als leistungsfähige SD-Karten-Modelle. Abbildung A 21 zeigt eine Auswahl von Speicherkarten und Modulen, die für eine Leistungsdatenmessung benutzt wurden, um ihre Eignung als Merkmal zu untersuchen.

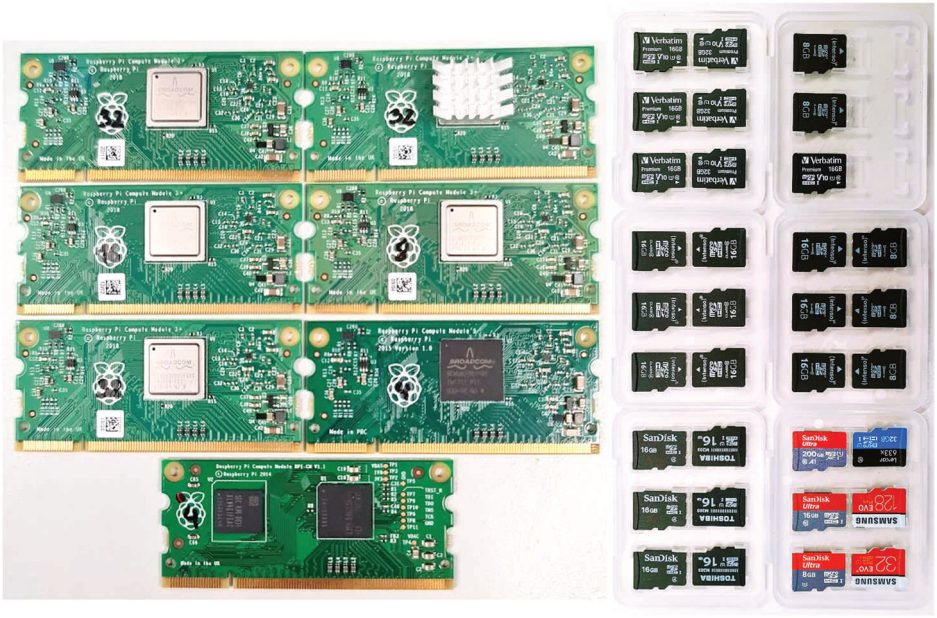


Abbildung A 21 Auswahl SD-Karten und Raspberry Pi Compute Module

Die Messergebnisse sind in den folgenden Diagrammen abgebildet, die zeigen, dass sich selbst die Speicherkartenmodelle desselben Herstellers ähneln, jedoch auch stark unterscheiden können. Zudem ist zu erkennen, dass die Art des Speichers starken Einfluss hat. So ist der Compute Module Flash-Speicher schneller und konsistenter in den ausgeführten Schreibvorgängen. Zieht man als Vergleichswert die Daten einer SSD-Festplatte eines PCs heran, so erreicht dieser sogar noch höhere Werte. Im Folgenden sind Diagramme der

Messreihen dargestellt, die mit den in Abbildung A 21 gezeigten SD-Karten bzw. Compute Modulen gemessen wurden. Hierzu wird ein Python-Skript verwendet, welches eine Reihe von Schreibvorgängen auf dem Speicher ausführt und die Dauer jedes Schreibvorgangs erfasst. Sämtliche Karten wurden in einem Raspberry Pi 4 mit 4 GB RAM getestet. Charakteristisch ist hier nicht nur die Geschwindigkeit eines jeden Speichers bzw. der Speicherart, sondern auch die Konstanz der Schreibraten, wie in Abbildung A 22 zu erkennen ist.

Abbildung A 22 Darstellung charakteristischer Speicher-Schreibraten

Zusätzlich wurde eine Messreihe mit jedem individuellen Gerät auf dem CPS-Prüfstand und der in diesem zufällig platzierten SD-Karte durchgeführt. Dies ermöglicht es systemische Einflüsse eines einzelnen Boards zu vermeiden und erzeugt sogar durch eine 1: 1 Kopplung ein charakteristisches Schreibverhalten, da die Kombination des Geräts bzw. des darin verbauten Kartenlesers mit einer bestimmten SD-Karte hierauf Einfluss haben kann. Auch hier sind neben den grundsätzlichen Unterschieden in der Schreibleistung

insbesondere Muster zu erkennen, die durch eine Schwankung in der Schreibgeschwindigkeit verursacht werden. Abbildung A 23 bis Abbildung A 28 zeigen die unterschiedlichen Systeme und ihre Messergebnisse. Auch hier sind meist eindeutige Unterschiede und Muster zu erkennen. Eine Merkmalsprüfung kann hier z. B. über einen Ähnlichkeitsvergleich der Messreihen über einen Nearest-Neighbor-Algorithmus durchgeführt werden.

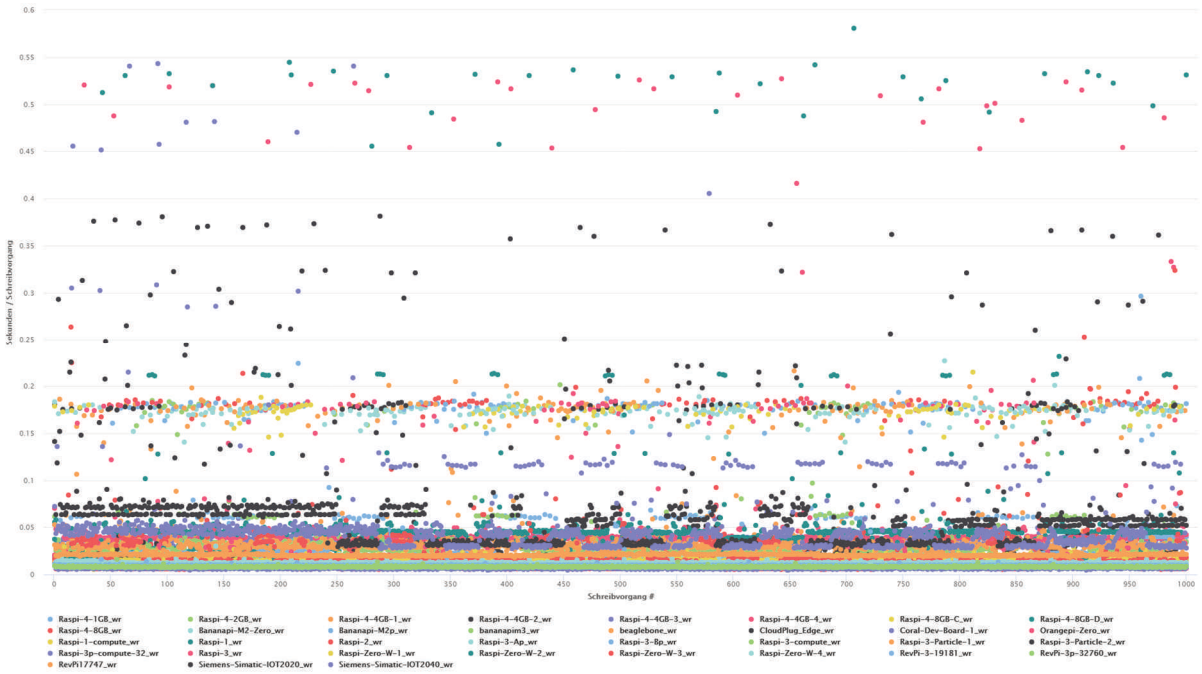


Abbildung A 23 Schreibraten aller geprüften Systeme

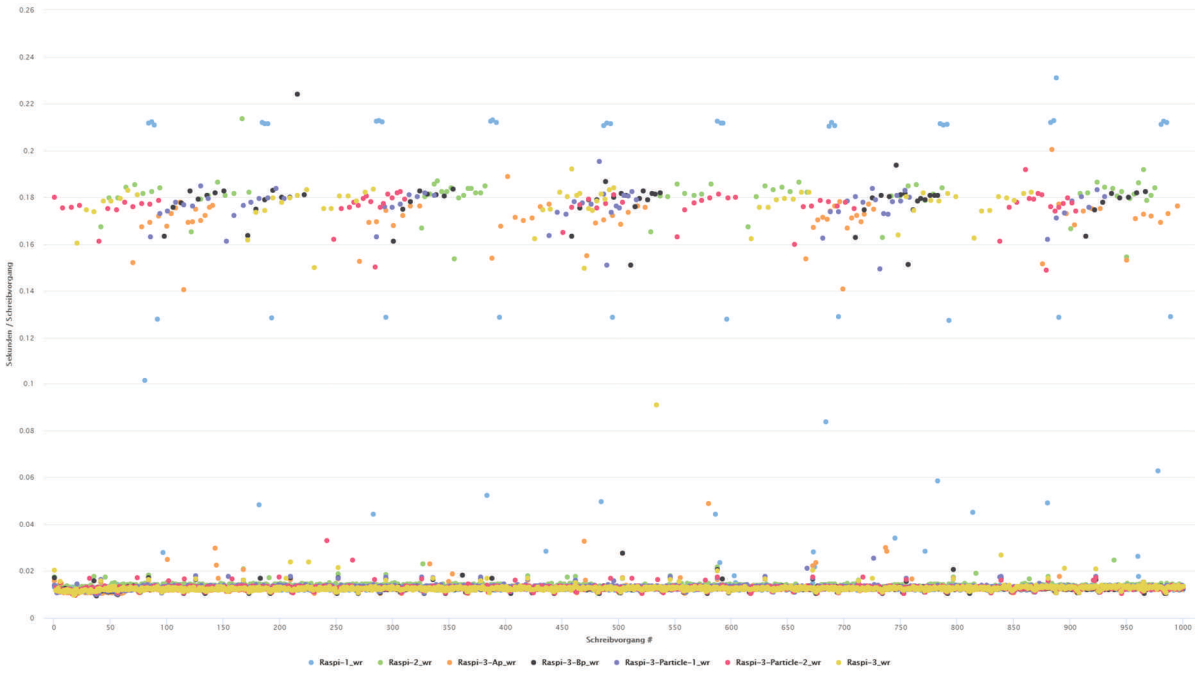


Abbildung A 24 Messwerte der Raspberry Pi (1-3) Systeme

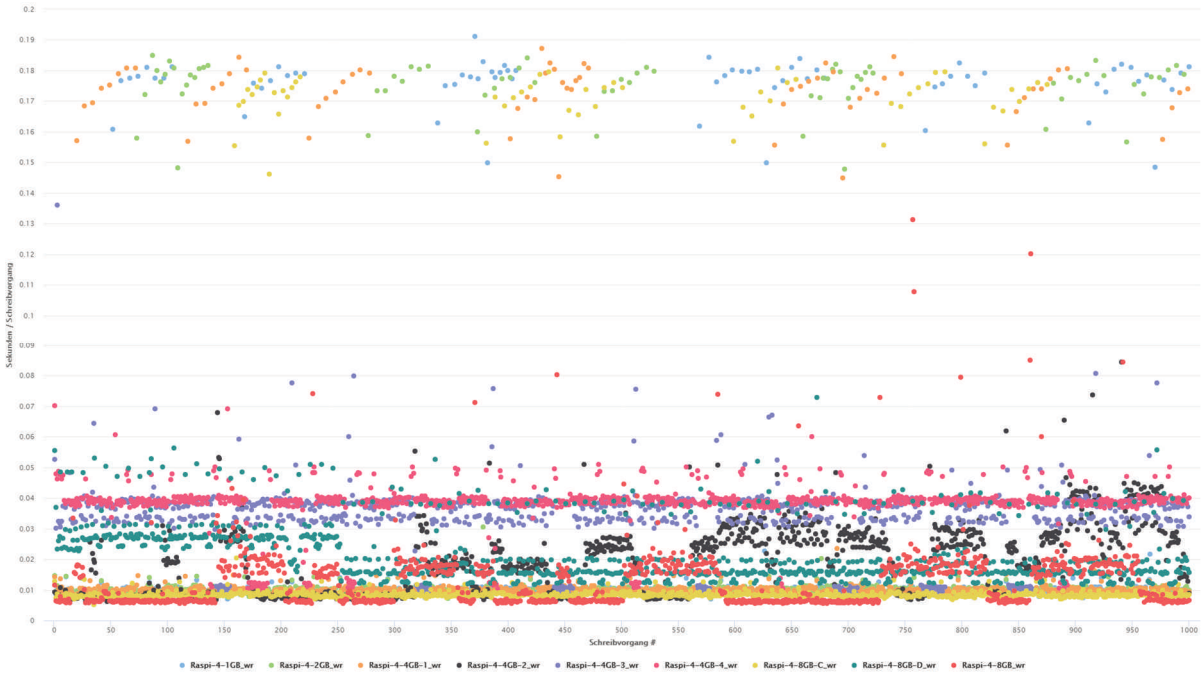


Abbildung A 25 Messwerte der Raspberry Pi 4 Systeme

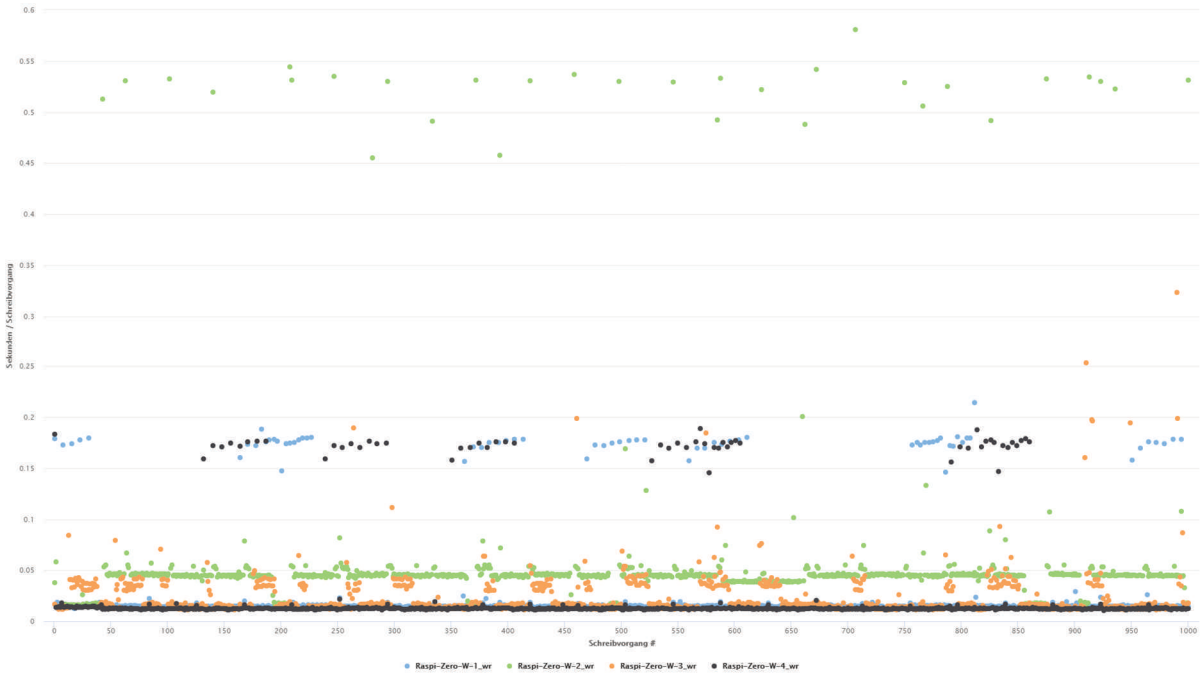


Abbildung A 26 Messwerte der Raspberry Pi Zero Systeme

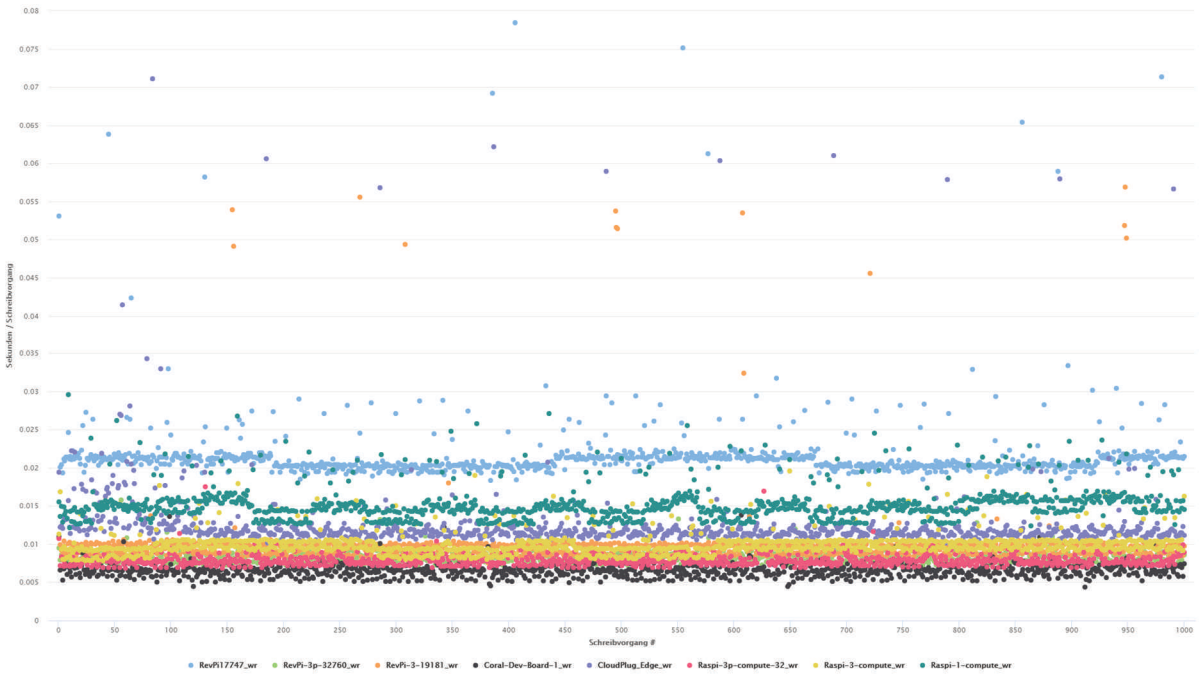


Abbildung A 27 Messwerte der Systeme mit integriertem Flash-Speicher

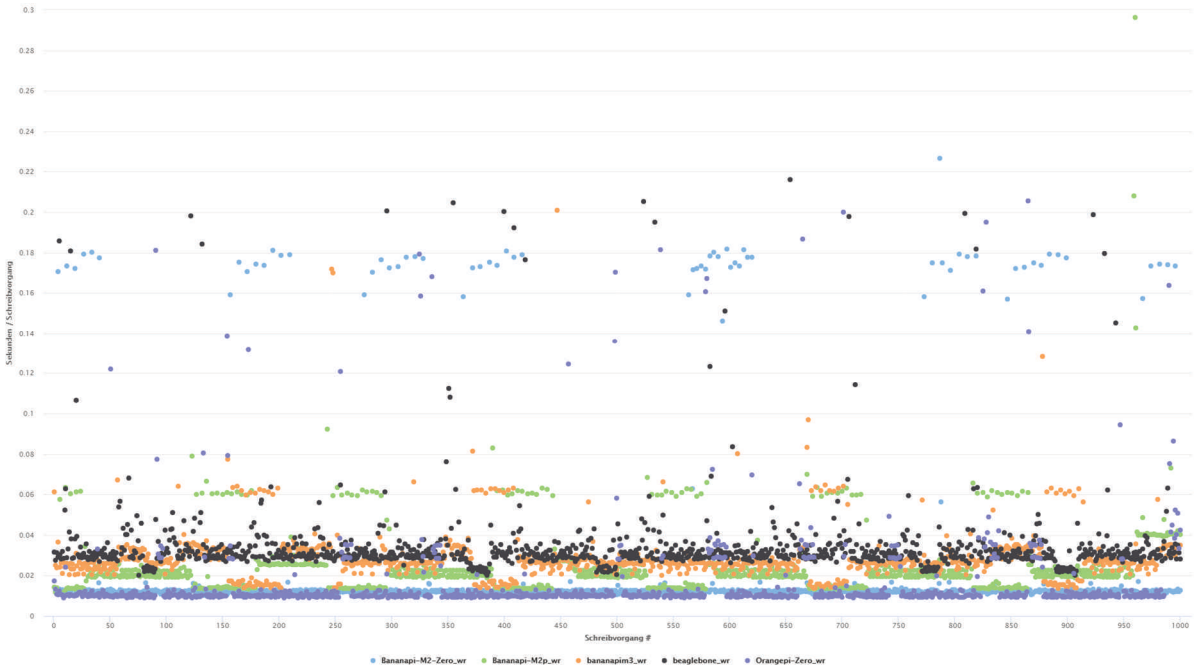


Abbildung A 28 Messwerte der Raspberry Pi-ähnlichen Boards

Anhang 7.3 – Beispiel 3 – CPU-Rechenleistung als Merkmal

Die in Anhang 7.1 dargestellten Systeminformationen geben unter anderem Auskunft über die CPU-Architektur und das Modell. Die Geschwindigkeit, die sich aus der Modellbezeichnung der CPU bzw. der erwarteten Modellkonfiguration eines bestimmten Geräts eines Herstellers ergeben sollte, lässt sich als Merkmal ablegen und erfassen bzw. ableiten. Allerdings sind dies statische Informationen, die sich zusätzlich mittels dynamischer Daten der CPU-Rechenleistung durch eine aktive Merkmalsprüfung erfassen lassen. Hierfür wird ein Python-Skript benutzt, welches auf allen eingebetteten Systemen die gleiche (parametrisierbare) Rechenoperation ausführt. Die Leistung der CPU ergibt sich implizit aus der Zeit, die das Skript für einen vollständigen Durchlauf benötigt. Die Ergebnisse mehrerer Messreihen sind in Abbildung A 29 dargestellt.

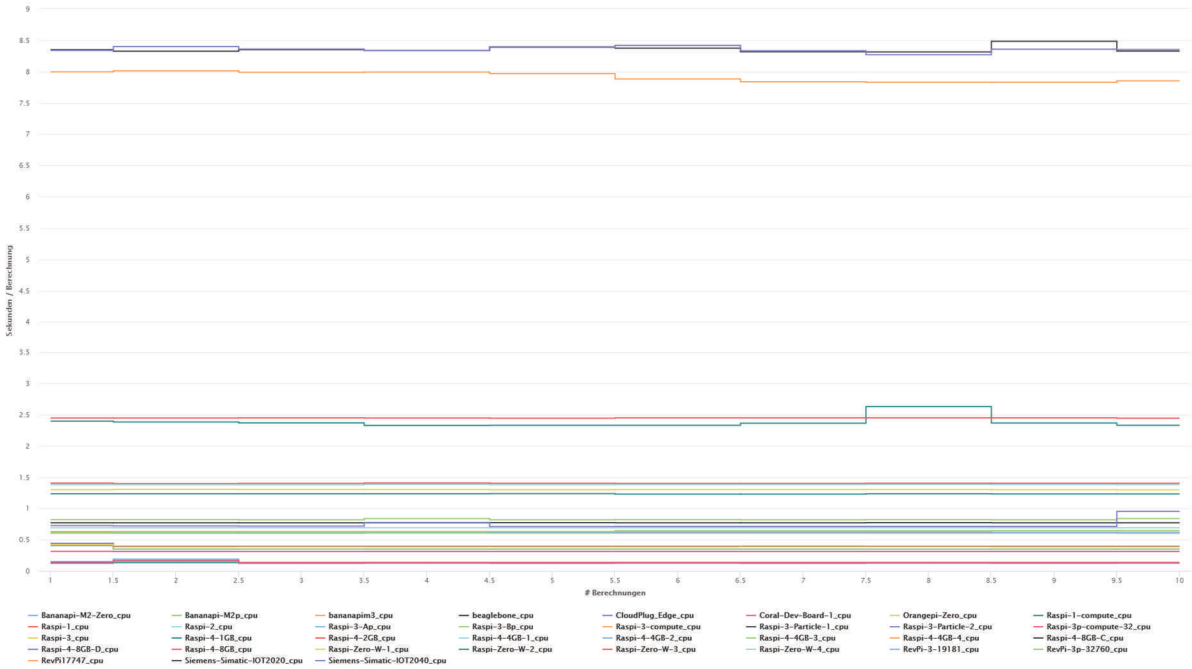


Abbildung A 29 Gemessene Rechenleistung der eingebetteten Systeme

Anhang 7.4 – Beispiel 4 – Systemtemperatur als Merkmal

Die Systemtemperatur, die bei den meisten Geräten über einen Sensor im Prozessor abgefragt werden kann, eignet sich ebenfalls als Merkmal. Zwar ist diese ggf. starken Schwankungen unterlegen, da die Umgebungstemperatur direkten Einfluss auf die Systemtemperatur hat. Allerdings lässt sich dieser Einfluss zur Merkmalsstärkung nutzen, da eine zusätzliche Messung der Umgebungstemperatur oder die unabhängige Messung eines anderen CPPS als ortsabhängiges kontextbasiertes Wertmerkmal herangezogen werden kann. Einige Systeme unterstützen auch keine Temperaturabfrage, was in diesem Fall dieses Merkmal ausschließt, es aber umgekehrt bei Systemen, die diese Fähigkeit besitzen, diese zu einer charakteristischen Fähigkeit machen. Neben der Umgebungstemperatur ist allerdings die Bauweise des eingebetteten Systems bzw. die ggf. eingesetzte Kühllösung ein Einflussfaktor. Oft sind die SoCs nicht zusätzlich gekühlt. Meist wird höchstens ein passives Kühlelement auf dem Chip angebracht. Aktive Kühler mit Lüfter und höher Kühlleistung sind selten können so dazu führen, dass eine niedrige Systemtemperatur erreicht werden kann, die weit unter der für ein Gerät mit einfacher oder keiner Kühlung liegt und somit auch sehr charakteristisch ist. Tabelle 24 listet die Systemtemperaturen der betrachteten eingebetteten Systeme und die eingesetzte Kühllösung bzw. deren Bauweise.

Tabelle 24 CPPS-Komponenten, Systemtemperatur und Kühllösung

#	System	Kühllösung	Temperatur [°C]
1	Raspberry Pi 4 8 GB	Kupfer/Alu-Kühler mit Heatpipe und Lüfter	35,5
2	Raspberry Pi 4 4 GB	Passives Kühlkörper-Gehäuse	43,4
3	Raspberry Pi 4 4 GB	Aktives Kühlkörper-Gehäuse	38,5
4	Google Coral Dev Board	Aluminium-Kühlkörper + Lüfter	65,0
5	Raspberry Pi 2	Passive Kühlkörpervariante auf SoC	44,4
6	Raspberry Pi 4 4 GB	Keine zusätzliche Kühlung	58,9
7	Raspberry Pi 4 2 GB	Passive Kühlkörpervariante auf SoC	53,1
8	Raspberry Pi 4 4 GB	Lüfter ohne direkten Kontakt	41,4

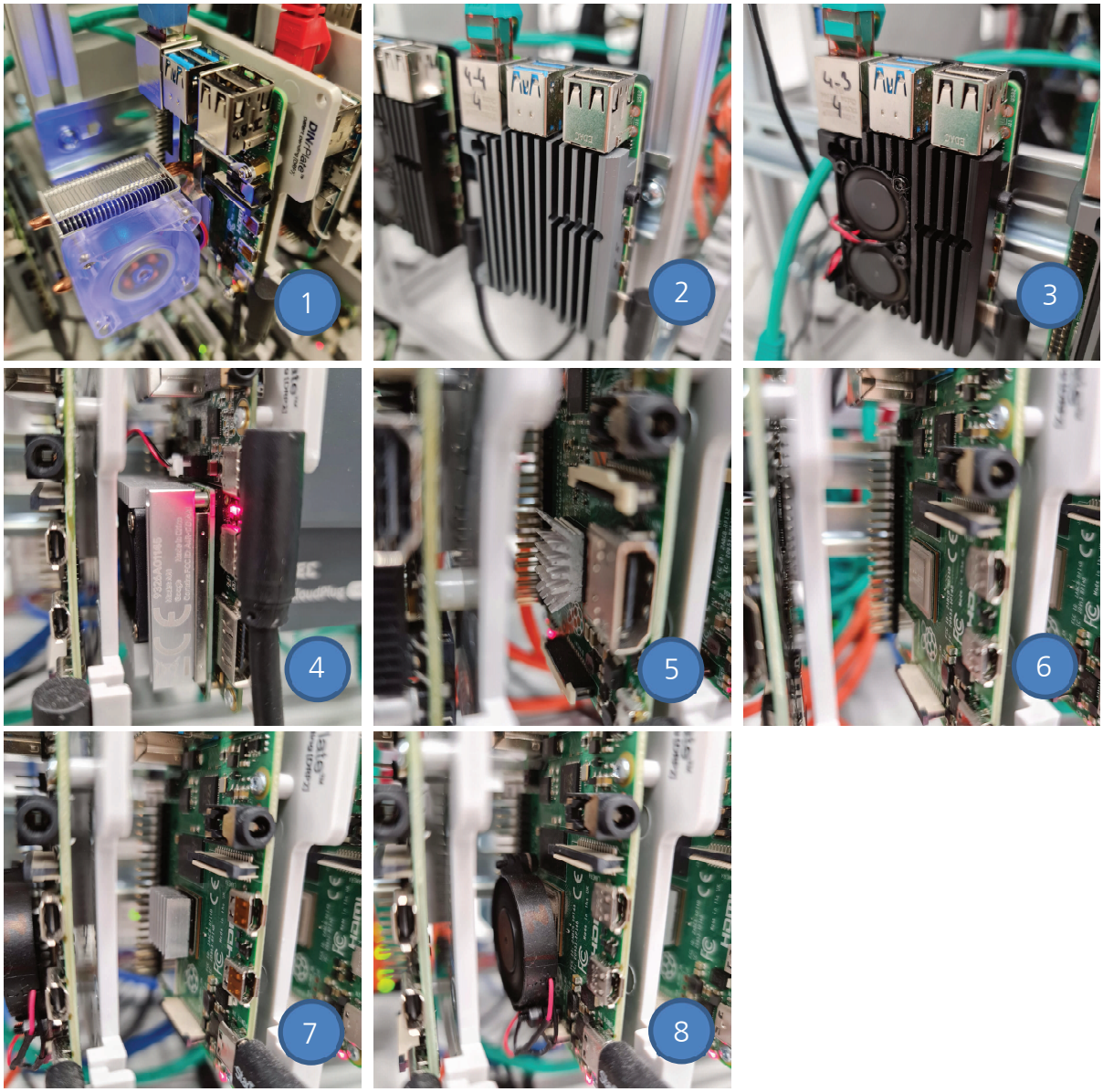


Abbildung A 30 Auswahl und Übersicht unterschiedlicher Kühllösungen

Anhang 7.5 – Beispiel 5 – Sensor- bzw. Umgebungsdaten als Merkmal

Einige der verwendeten eingebetteten Systeme sind zusätzlich mit Sensoren zur Wahrnehmung ihrer Umgebung ausgestattet, womit sie erst zu CPS im eigentlichen Sinn werden. Abbildung A 31 zeigt eine Auswahl von Sensoren: (1) Gassensor (CO, NO2, NH3), (2) Feinpartikelsensor, (3) Mikrofon zur Messung eines Klangprofils der Umgebung, (4) Lichtsensor, (5) Licht-/Farbsensor, (6) Accelerometer z. B. zur Erfassung von Vibrationen oder Bewegungsmustern, (7) Temperatursensor, Hygro- und Barometer. Die Fähigkeit andere CPS in der Umgebung zu detektieren, beispielsweise visuell oder durch Funkdaten (z. B. Bluetooth) wird hierzu gezählt. Insbesondere CPPS, die sehr spezifische Aufgaben erfüllen, können mit entsprechend spezifischen Sensoren ausgestattet sein. Zwar können neben Hardware-Sensoren zum Zweck des „general-purpose sensing" auch virtuelle und Software-Sensoren verwendet werden, allerdings erhöht die Spezifizität der Sensoren auch die Spezifizität der Identität des CPPS.

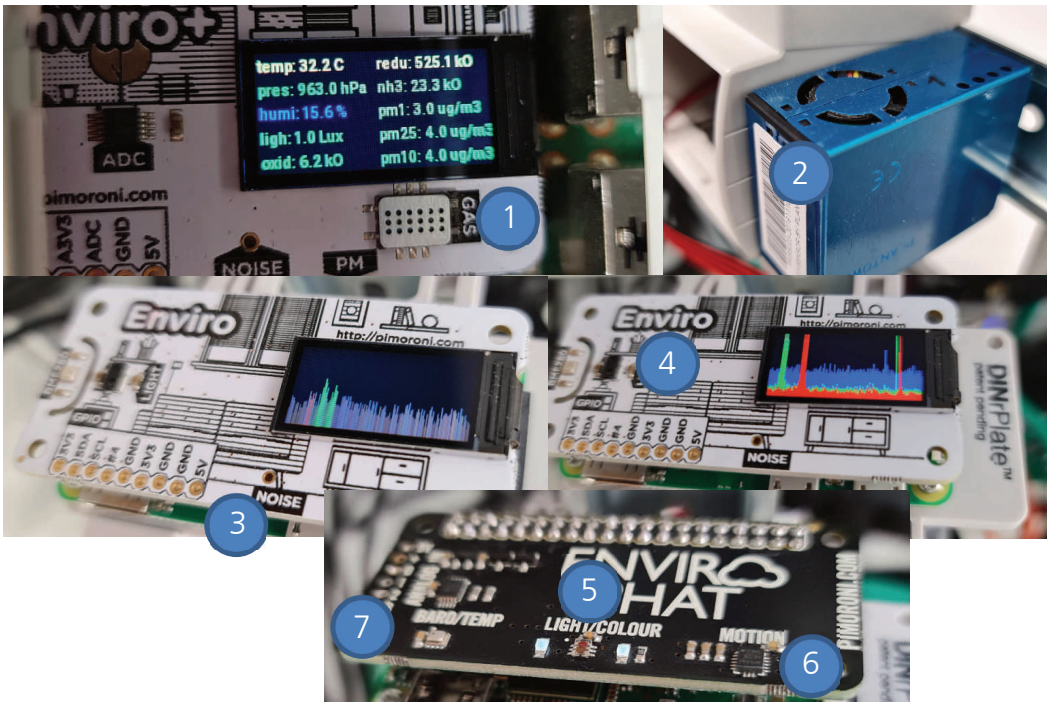


Abbildung A 31 Beispiele für zusätzliche Sensorik

Anhang 8 – Ergänzende Informationen zu Versuchsaufbau 2

Dieser Versuchsaufbau fokussiert sich auf die kontinuierliche Authentifizierung mittels komplexer Merkmale, die sich aus der Korrelation einzelner Merkmale ergeben. Im Folgenden sind zusätzlich die spezifischen prozessabhängigen Verhaltensmuster, die sich aus den Sensordaten ergeben, dargestellt. Die besonderen Merkmale sind in Abbildung A 32 farblich mit Pfeilen markiert. Da diese Merkmalswerte meist Ereignis-, Orts- und Zeit-abhängig sind, wird auch der Bezug zur Anlage dargestellt bzw. an welcher Stelle diese Merkmale auftreten.

1. Grün und Blau: Das Steuerungsereignis, welches den Wendeprozess im Greifer-Modul auslöst, kann zeitlich mit einer Veränderung der Sensordaten des Accelerometers, des Gyroskops, des Magnetometers und Lichtsensors korreliert werden.
2. Gelb: Der aktuelle Standort während des Pressvorgangs, der durch das entsprechende Ereignis der Steuerung markiert werden kann, kann durch eine charakteristische Veränderung der Magnetfeldmessung bestätigt werden, da sich die Presse innerhalb eines metallischen Gehäuses befindet, das starken Einfluss auf die elektromagnetische Messung hat.
3. Rot: Die Lage des Produkts kann anhand mehrerer Sensoren korreliert werden, so bestätigen der Messwert der Erdbeschleunigung des Accelerometers gemeinsam mit den Werten des Magnetometers und Lichtsensors die Lage des Produkts. Der Lichtsensor kann beispielsweise nur Licht erfassen, wenn das Produkt mit der Öffnung nach oben platziert ist.
4. Lila: Die Bewegung des Produkts bzw. des Werkstückträgers kann an den 90° Abbiegestellen nachverfolgt werden, da hier die Lagesensoren eine entsprechende Veränderung auf der entsprechenden Achse erfassen. Diese Daten können zusätzlich mit den Standortdaten der RFID-Leser korreliert werden.

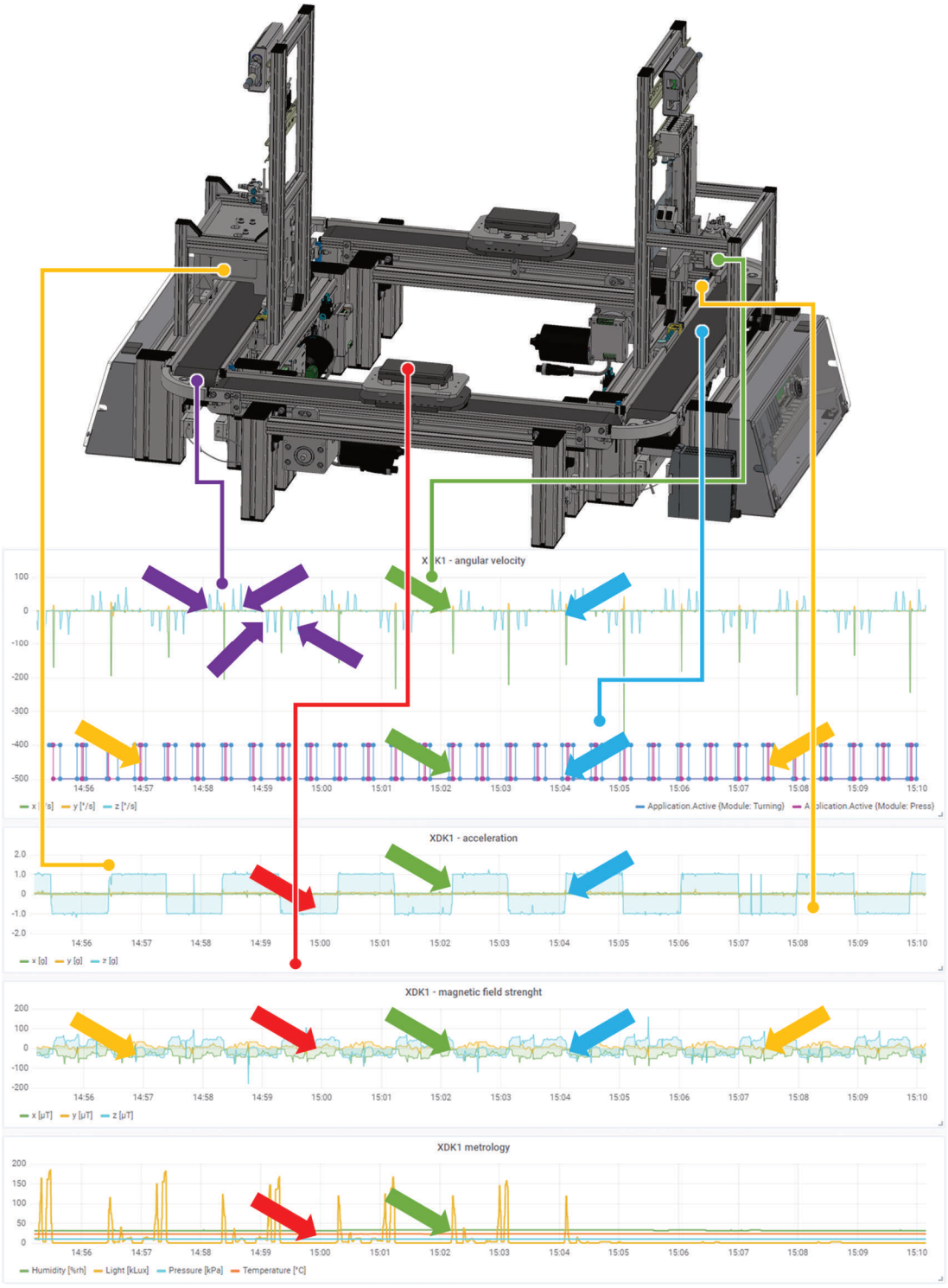


Abbildung A 32 Erläuterung der Sensordaten-Charakteristik