

# SecurePLUGandWORK - Abschlussbericht



Projektkonsortium SecurePLUGandWORK

Karlsruhe, 10. Juli 2017

<u>Inhalt</u>	<u>Seite</u>
<b>1 EINLEITUNG .....</b>	<b>4</b>
1.1 AUSGANGSSITUATION.....	4
1.2 MOTIVATION .....	4
1.3 HERAUSFORDERUNG INDUSTRIE 4.0: BABYLONISCHE SPRACHVIELFALT.....	5
1.4 SELBSTBESCHREIBUNG VON MASCHINEN UND ANLAGEN .....	5
1.5 BESCHREIBUNG VON MASCHINENKOMPONENTEN.....	7
<b>2 VERBUNDPROJEKT SECUREPLUGANDWORK .....</b>	<b>9</b>
2.1 PROJEKTZIELE .....	9
2.2 PROJEKTPARTNER .....	9
2.3 INDUSTRIEARBEITSKREIS .....	10
<b>3 ARCHITEKTUR.....</b>	<b>11</b>
3.1 VERWENDETE STANDARDS.....	11
3.1.1 AutomationML.....	11
3.1.2 OPC Unified Architecture (OPC UA) .....	11
3.2 LÖSUNGSANSATZ.....	12
3.3 SYSTEMARCHITEKTUR.....	13
<b>4 SECUREPLUGANDWORK-ADAPTER.....</b>	<b>15</b>
4.1 KONZEPTION.....	15
4.2 VALIDIERUNG.....	19
4.3 ZUSAMMENFASSUNG UND EINSATZ .....	20
4.4 ANDERE ‚INDUSTRIE 4.0-ADAPTER‘ .....	21
4.4.1 Ergebnisse einer Umfrage unter Anwendern .....	23
4.4.2 Anbieter von ‚Industrie 4.0-Adaptern‘ .....	28
<b>5 SECUREPLUGANDWORK-INTEGRATIONSSERVER .....</b>	<b>30</b>
<b>6 ASSISTENZTOOL.....</b>	<b>31</b>
<b>7 SECUREPLUGANDWORK-MIDDLEWARE .....</b>	<b>32</b>
7.1 ENTWICKLUNGSARBEITEN.....	32
7.2 PARALLELE STANDARDISIERUNG.....	34
<b>8 INFORMATIONSSICHERHEIT .....</b>	<b>36</b>
8.1 BEDROHUNGSANALYSE .....	36
8.2 SICHERHEITSCHIP (ZERTIFIKATE, KOMMUNIKATION, DONGLE, ETC.).....	37
8.3 DIGITALE ZERTIFIKATE .....	37
8.4 ZERTIFIKATE UND DER OPC-UA STANDARD.....	37
8.4.1 Generieren und Ausrollen der Zertifikate mit Licence Central und Zertifizierungsinstanz .....	37
8.4.2 Authentifizierung.....	38
8.4.3 Vertraulichkeit der Daten .....	38
8.4.4 Aufwand auf der Seite der Schutzkomponenten .....	38
8.4.5 Zusammenfassung der Schutzziele .....	40
8.4.6 Beispielablauf UseCase Spindel .....	40
<b>9 STANDARDS UND STANDARDISIERUNG .....</b>	<b>42</b>
9.1 EINHEITLICHER DATENAUSTAUSCHSTANDARD .....	42
9.2 EINHEITLICHER KOMMUNIKATIONSSTANDARD .....	42
9.2.1 Allgemeines .....	42
9.2.2 IT-Sicherheit in OPC UA.....	42
9.3 KOMBINATION VON AUTOMATIONML UND OPC UA.....	44
9.3.1 Companion Specification OPC UA for AutomationML .....	44
9.3.2 DIN SPEC 16592.....	44
9.4 AUTOMATIONML BPR DATAVARIABLE .....	44
<b>10 ANWENDUNGSBEISPIELE .....</b>	<b>46</b>

---

10.1	WERKZEUGMASCHINE UND IHRE KOMPONENTEN .....	46
10.1.1	Werkzeugmaschine .....	46
10.1.2	Motorspindel .....	47
10.1.3	Winkelbohrkopf .....	56
10.1.4	Werkzeugmagazin .....	58
10.1.5	Kugelgewindetrieb .....	59
10.2	INDUSTRIELLE WASCHANLAGEN ZUR TEILEREINIGUNG .....	65
10.3	GREIFER .....	69
10.3.1	Ausgangssituation .....	69
10.3.2	Lösungsansatz.....	69
10.3.3	Systemkomponenten und AutomationML-Modell.....	70
10.3.4	Prüfstand/Achsvermessung.....	71
10.3.5	Integration Maschinenebene – Schunk-Arm .....	74
10.3.6	Ergebnisse und deren Verwertung .....	75
10.4	SMARTFACTORYOWL.....	77
10.5	MOBILE DEMONSTRATOREN .....	78
10.5.1	Mobiler SecurePLUGandWORK-Demonstrator .....	78
10.5.2	Tischaufbau (Demo Funktionalität).....	78
<b>11</b>	<b>GESCHÄFTSMODELLE .....</b>	<b>79</b>
11.1	LITERATURRECHERCHE ZU INDUSTRIE 4.0-GESCHÄFTSMODELLEN .....	79
11.2	INDUSTRIE 4.0-GESCHÄFTSMODELLE IN DER PRAXIS .....	81
11.3	INDUSTRIE 4.0 GESCHÄFTSMODELLE IM ZWIESPALT ZWISCHEN RECHT UND TECHNIK .....	82
11.3.1	Rolle von Information und Know-how.....	83
11.3.2	Implikationen für neue Geschäftsmodelle .....	84
11.3.3	Kein direkter Schutz von Geschäftsmodellen.....	84
11.4	IDEENSAMMLUNG UND DISKUSSION VON BEST PRACTICES UND ANSÄTZEN ANDERER UNTERNEHMEN.....	91
11.5	DISKUSSION UND KONKRETISIERUNG DER GESCHÄFTSMODELLE .....	93
11.5.1	Bewertungsmethode.....	94
11.5.2	Businesspläne .....	96
11.5.3	Kompetenzentwicklung.....	97
<b>12</b>	<b>LITERATUR .....</b>	<b>100</b>
<b>13</b>	<b>ABBILDUNGSVERZEICHNIS .....</b>	<b>103</b>

## 1 Einleitung

### 1.1 Ausgangssituation

In der Industrie 4.0 sind Maschinen, Anlagenkomponenten und IT-Systeme miteinander vernetzt, so dass jede Komponente der Fabrik über die relevanten ‚Partner‘ informiert ist. Schon seit vielen Jahren sind in der Fertigung IT-Systeme verbreitet, die Maschinen- und Betriebsdaten erfassen, die Qualität regeln oder mit denen Unternehmen Produkte und Zwischenerzeugnisse während des Lebenszyklus verfolgen. Diese produktionsnahen IT-Systeme werden als Manufacturing Execution Systeme (MES) bezeichnet. Die VDI-Richtlinienreihe 5600 definiert die Aufgaben und wichtigsten Funktionen solcher IT-Systeme. Wichtigster Nutzen dieser Werkzeuge ist es, Fertigung und Montage für die einzelnen Beteiligten einer Fabrik transparent zu machen und letztlich günstiger zu produzieren, höhere Qualität zu erzeugen oder schneller zu liefern. Dieser Nutzen entsteht allerdings erst dann, wenn ein großer Teil der Fertigungseinrichtungen mit dem MES verbunden ist.

Parallel zur Fertigungswelt und getrieben durch große IKT-Anbieter entstehen derzeit verschiedene Plattformen für das Industrielle Internet der Dinge (IIOT). Mit ihnen soll es möglich sein, Daten aus der Fertigung zu sammeln, auszuwerten und mit Hilfe von Algorithmen letztlich die Verfügbarkeit von Maschine und Anlagen zu verbessern. Trotz großer Leistungsfähigkeit in der Verarbeitung der Daten leiden viele dieser Plattformen daran, dass der Zugang zu Daten aus Maschinen und Produktionsanlagen schwierig ist. Einer der Gründe dafür ist, dass viele kleine und mittelständische Ausrüster hochproduktive und zuverlässige Maschinen und Anlagen liefern, mit denen weltweit qualitativ hochwertige Produkte hergestellt werden. Diese mittelständischen Unternehmen bilden das Rückgrat der deutschen Industrie: sie sind hochspezialisiert und bieten teilweise maßgeschneiderte Lösungen für genau eine Fertigungsaufgabe an. Sie beherrschen die Mechanik, Mechatronik und Automatisierungstechnik ihrer Maschine, Anlagenkomponente oder Fördertechnik-Einrichtung. Mit den Daten, die die Maschinen und Anlagen während des Fertigungsprozesses erzeugen, rücken datenbasierte Dienstleistungen rund um die eigentlichen Produktionsanlagen in den Fokus des Interesses. Schlüssel zu solchen neuen produktbegleitenden Dienstleistungen sind Informations- und Kommunikationstechnologien (IKT). Sie durchdringen den traditionellen Maschinen- und Anlagenbau immer stärker und schaffen Potentiale für innovative Dienstleistungen. Es liegt also auf der Hand, dass sich mittelständische Maschinen- und Anlagenbauer zukünftig viel stärker als heute mit den Themen IT-Anwendungen, Schnittstellen, Kommunikation, IT-Sicherheit, etc. auseinander setzen, Kooperationspartner finden und neue Dienstleistungen aufbauen.

Industrie 4.0 umfasst unter anderem intelligente Anlagenkomponenten, Maschinen und Anlagen sowie IT-Systeme, die miteinander vernetzt und über die relevanten ‚Partner‘ mit ihren Fähigkeiten informiert sind. Bei einem Neuaufbau oder Umbau von Anlagen, Maschinen und Komponenten können alle Partner auf die Veränderung entsprechend reagieren. Änderungen sind beispielsweise in der eingebetteten Software der Feldgeräte, im Programmcode der Steuerungen, aber auch in überlagerten IT-Systemen wie bspw. MES nötig.

### 1.2 Motivation

Diese Veränderungen werden heute häufig manuell durchgeführt und sind daher zeitintensiv und fehleranfällig. Im Rahmen von Industrie 4.0 sollen die Änderungen (teil-)automatisiert ablaufen, ähnlich wie bei einer USB-Schnittstelle und USB-Geräten am PC. Die Situation im

Umfeld der Produktion ist allerdings erheblich komplexer. Alle Änderungen sollen »secure« erfolgen. Das Verbundprojekt SecurePLUGandWORK betrachtete zwei Anwendungsszenarien auf unterschiedlichen Hierarchie- und Komplexitätsebenen:

- Anwendungsszenario Integration Komponente – Maschine, z.B. Kugelgewindetrieb wird in Werkzeugmaschine integriert. Konkret im Projekt zu integrierende Komponenten in eine Werkzeugmaschine waren
  - Motorspindel,
  - Winkelbohrkopf,
  - Kugelgewindetrieb.
- Anwendungsszenario Integration Maschine – Anlage, z.B. Einzelmodule werden zu Waschmaschine vereinigt. Konkret im Projekt zu integrierende Anlagenteile zu einer Gesamtanlage waren
  - Module von Industriewaschmaschinen zur Reinigung von kühlenschmiermittelbehafteten Teilen, z.B. aus einer Zerspanung,
  - Greifer eines Leichtbau-Roboterarmes und ein
  - Werkzeugmagazin.

### **1.3 Herausforderung Industrie 4.0: Babylonische Sprachvielfalt**

Genau hier beginnt die Herausforderung: die angestrebte internetbasierte Vernetzung in der Industrie 4.0 erfordert, dass Maschinen und ihre Komponenten als Datenquellen eine maschinenlesbare Selbstbeschreibung mitbringen, die den Inhalt der Daten beschreibt, die eine Maschine bereitstellen kann: eine Art ‚Maschinentreiber‘. Diese ‚Treiber‘ sind zwingend erforderlich, wenn Maschinen und Anlagen miteinander vernetzt oder an ein überlagertes SCADA-, Leit- oder MES-System angeschlossen werden. Gibt es, wie heute, diese ‚Maschinentreiber‘ kaum, muss sich der Betreiber oder Systemintegrator mit der sprichwörtlichen babylonischen Sprachvielfalt seiner Maschinen und Anlagen plagen (Bild 1). Außer den verschiedenen Maschinen, deren Steuerungen und damit proprietären Datenbezeichnungen existieren in der Fabrik viele heterogene IT-Systeme mit meist proprietären Schnittstellen, die bei jeder Änderung manuell angepasst werden. Schnittstellenanpassungen sind aufwändig und fehleranfällig. Wenn sich Industrie 4.0 also zielgerichtet und auf breiter Basis durchsetzen soll, muss die produzierende Industrie die Sprachvielfalt beherrschen.

### **1.4 Selbstbeschreibung von Maschinen und Anlagen**

Die Herausforderung, verkettete Maschinen und Anlagen mit einem übergeordneten IT-System zu verbinden, ist oben bereits skizziert: heute erfolgt diese Konfiguration des IT-Systems zum großen Teil manuell. Die Gründe dafür liegen darin, dass heute Produktionsprozesse und -anlagen in vielen Unternehmen ausgeschrieben und von spezialisierten Anlagenherstellern zugekauft werden. Der Maschinen- und Anlagenbau ist mittelständisch geprägt, so dass Produktionsbetriebe ihre Anlagen von diversen Lieferanten erhalten. Dementsprechend sind die Anlagen heterogen ausgestattet: mit unterschiedlichen Steuerungen, diversen Kommunikationsprotokollen und/oder Feldbussystemen, etc. Ein Plug-and-play mit automatischen Konfigurationsverfahren wie beispielsweise in der Unterhaltungselektronik oder der PC-Welt mit USB-Anschlüssen existiert nicht. Die Verbindung zwischen Anlagensteuerung und überlagertem IT-System ist weitgehend starr und anlagenspezifisch konfigu-

riert. Daraus resultiert ein hoher Konfigurationsaufwand bei der Erstinbetriebnahme und bei jeder Anpassung der Produktionsanlage an neue Randbedingungen. Wandlungsfähig im Sinne von Industrie 4.0 ist ein solches Gebilde bestenfalls auf der mechanischen Seite, nicht aber auf Seiten der Software.

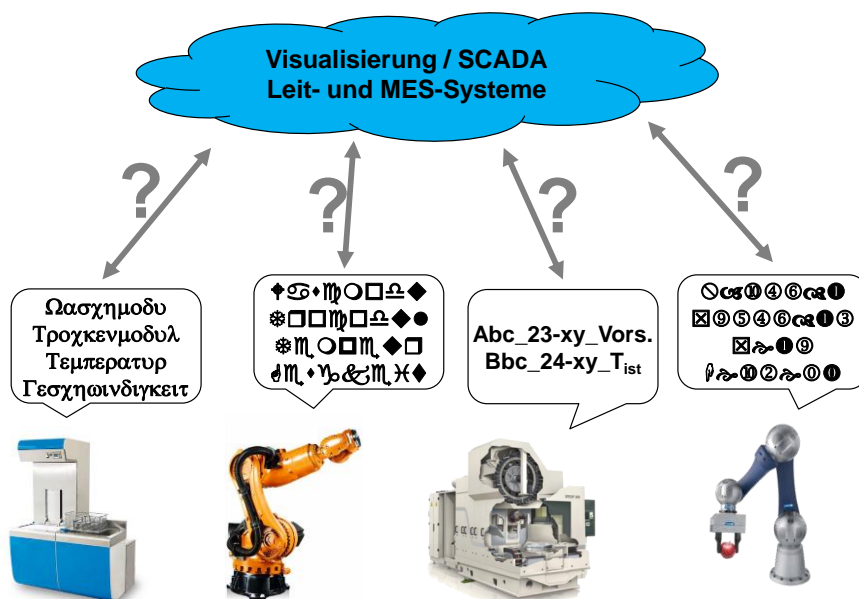


Bild 1: Herausforderung der ‚Sprachvielfalt‘ in der Produktion

In einem Beispiel hat ein Anwender seine Anlagen mechanisch in funktionsfähige Module aufgeteilt: basierend auf einem standardisierten Grundträger werden Module mit verschiedenen Funktionen zur Gesamtanlage kombiniert. Eine Gesamtanlage kann aus bis zu 15 Einzelmodulen bestehen. Bezogen auf die Software ist die aktuelle Situation jedoch dadurch gekennzeichnet, dass alle Module an einen einzigen zentralen Schaltschrank angeschlossen sind, der die jeweiligen Module ansteuert. Bei Erweiterungen oder Änderungen an der Anlage muss die komplette Verkabelung entfernt und die Steuerung manuell umprogrammiert und getestet werden. Ziel des Herstellers ist es nun, auch die Software zu modularisieren, indem jedes Hardware-Modul mit einer eigenen Steuerung ausgestattet wird, die außerdem die Beschreibung des Moduls enthält. Änderungen oder Umbauten der Gesamtanlage sind dann erheblich einfacher, da zukünftig nur noch einzelne Module einschließlich ihrer Steuerung eingefügt werden müssen. Eine zentrale Verkabelung existiert nicht mehr.

Die Schwierigkeit für mittelständische Hersteller von Maschinen liegt darin, dass sie sich zunehmend an die Vorgaben ihrer Kunden zum Thema ‚MES-Anbindung‘ anpassen müssen; eine eigene Standardisierung der Bezeichnungen der MES-bezogenen Signale ist daher nur dann sinnvoll, wenn das MES sich aus einem ‚sprechenden‘ Datenhaushalt bedienen kann, d.h. wenn die Bedeutung einzelner Datenpunkte allgemein verständlich und maschinenlesbar beschrieben ist.

Zwei Anwendungsfälle der Selbstbeschreibung sind zu unterscheiden:

1. Im Entwicklungsprozess der Maschine wird im Zuge des Engineering-Prozesses eine Selbstbeschreibung in Form eines Modells erstellt.
2. Für eine bereits installierte Maschine soll nachträglich eine Selbstbeschreibung erstellt werden, und zwar auf Basis der Datenpunkte, die bereits in der Maschine existieren.

## 1.5 Beschreibung von Maschinenkomponenten

Die Inbetriebnahme von (Werkzeug-) Maschinen ist heute einer der zeitaufwendigsten Schritte und in ihrem Aufwand oftmals schwer im Voraus zu kalkulieren. So folgt bei einer modernen Produktionsstraße auf die bis zu sechs Wochen dauernde Fertigung und Montage der Einzelmaschinen ein annähernd gleich zeitaufwendiger Prozess zur Inbetriebnahme der Gesamtanlage, der je nach Projektlage beim Hersteller oder bereits beim Kunden auf der Baustelle stattfindet. Einen Großteil dieser Zeit benötigt der Maschinenbauer, um Komponenteneigenschaften manuell in der Maschinensteuerung zu ermitteln und zu hinterlegen, z.B. den Steigungsfehler von Kugelgewindetrieben (siehe auch Bild 2 links, aufgrund der oben beschriebenen Form der Datenweitergabe als pdf-Datei oder auf Papier). Bei der Inbetriebnahme von Komponenten in einer Werkzeugmaschine müssen Spezifikation wie beispielsweise die Steigung des Kugelgewindetriebs (KGT), die Lagerabstände und die elektrischen Kennwerte der Hauptspindel in der Maschinensteuerung manuell hinterlegt werden. Durch den manuellen Anteil ist dieser Vorgang zeitaufwendig und fehlerbehaftet. Um die geforderte Prozessfähigkeit zu gewährleisten, müssen bauteilspezifische Fehler kompensiert werden. Beispielsweise werden geometrische Fehler bei Kugelgewindetrieben durch Kreisformtests identifiziert und die daraus ermittelten Kompensationswerte in der Steuerung hinterlegt. Bei einer Hauptspindel müssen Verschiebungen des Bearbeitungswerkzeuges, aufgrund von temperaturbedingten Einflüssen, durch entsprechende externe Messeinrichtungen identifiziert und kompensiert werden.

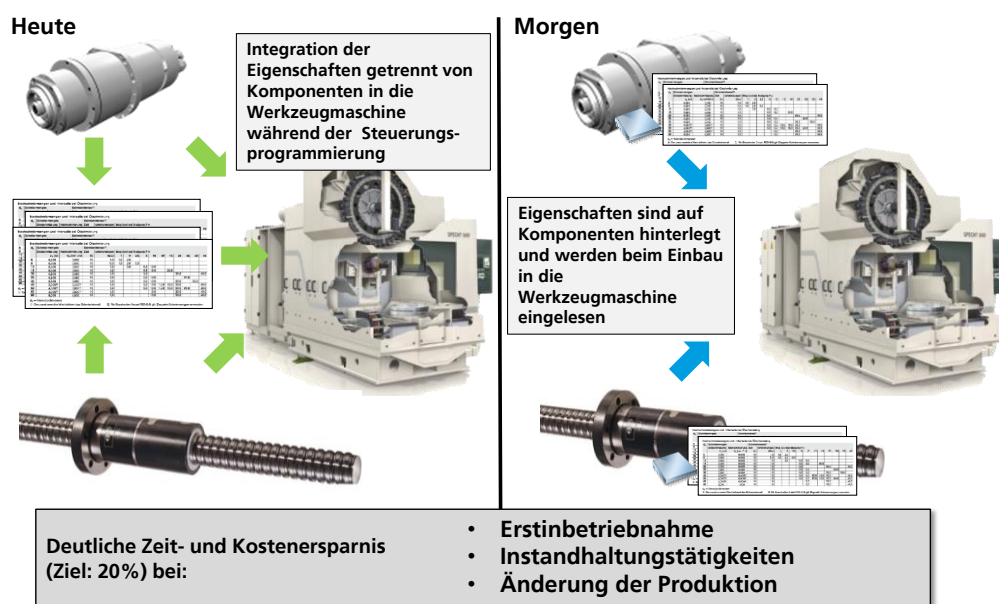


Bild 2: Komponentenintegration am Beispiel von Werkzeugmaschinen heute und morgen

Beispielsweise befindet sich zur Identifizierung von Kugelgewindetrieben auf der Mutter ein 7stelliger Zahlencode. Dieser mit einem Laser aufgebrachte Code wird benötigt, um die Kugelgewindetriebe mit den Inbetriebnahmedaten der jeweiligen Komponenten zu verbinden. Hier sind z.B. Steigungsfehlerschriebe, Reibmomentkurven, Steifigkeiten, Geometriedaten bis hin zu Prüfzeugnissen für die jeweiligen Kugelgewindetriebe notwendig. Diese Daten werden in unterschiedlichen Datenformaten, separat vom Kugelgewindetrieb, an den Kunden weiter gegeben. Die Daten aus den Prüfmessungen an den Prüfständen werden in unterschiedlichen Datenformaten erzeugt. Der dabei entstehende hohe manuelle Aufwand ist heute ein Kostentreiber bei der Inbetriebnahme von Werkzeugmaschinen.

Auch die Inbetriebnahme von Erweiterungssystemen wie Greifersystemen, die für Werkstückmanipulationen zum Einsatz kommen, ist heute noch aufwendig. Hier müssen beispielsweise die möglichen Bewegungsräume in der übergeordneten Steuerung hinterlegt werden. Außerdem wird für hochgenaue Positioniervorgänge die Positionierungsgenauigkeit im Arbeitsraum hinterlegt. Eine Werkzeugmaschine kann mit verschiedenen Werkzeugmagazinen (WZMM) ausgestattet werden. Bei der Inbetriebnahme muss hierbei die Anzahl, Position und der Zustand der einzelnen Werkzeuge, bei großen Magazinen bis zu 100, manuell in der Steuerung hinterlegt werden.



## 2 Verbundprojekt SecurePLUGandWORK

### 2.1 Projektziele

Das Projekt SecurePLUGandWORK hatte zum Ziel, PLUGandWORK-Mechanismen mit integrierter Sicherheitstechnologie auf Basis marktgängiger Standards für verschiedene Anwendungsfälle zu entwickeln. Dabei werden die Integration von Komponenten in Werkzeugmaschinen und die Integration von Maschinen in Anlagen/MES betrachtet.

Ziel ist die Vereinfachung, Fehlerreduktion, Qualitätssteigerung und Zeiteinsparung / Einsparung manueller Aufwände.

Das Projekt ermöglicht die PLUGandWORK-Fähigkeit in den produktionsnahen Softwarekomponenten durchgängig über die verschiedenen Ebenen der Fertigungshierarchie. Dies geschieht unter Nutzung offener Standards, die bereits heute in der Industrie eingesetzt werden. Unter anderem sollen Maschinen und Anlagen so schneller in Betrieb genommen werden. In der SecurePLUGandWORK-Architektur werden auch nicht-I4.0-kommunikationsfähige Komponenten mit I4.0-Eigenschaften ausgestattet. Diese Funktionalität wird mit im Projekt entwickelter Software basierend auf den Standards OPC UA und AutomationML, sowie Hardware in Form eines Produktgedächtnisses nachgerüstet.

Neben der Anforderung nach Wandlungsfähigkeit steht die Forderung nach Sicherheit (Security) komplexer vernetzter Anlagen. Schutz vor Manipulation von Steuerdaten und Reverse-Engineering von einzelnen Komponenten bedeuten gleichzeitig Robustheit gegen mögliche Cyber-Attacken in einer hochvernetzten und daher angreifbareren Automatisierungswelt. Darum wurden als weitere Projektziele softwarebasierte und damit automatisierte Authentifizierung von Komponenten des Produktionssystems und Verschlüsselung der Kommunikation verfolgt, ebenfalls unter Nutzung offener Standards wie OPC-UA.

### 2.2 Projektpartner

Die Partner des Verbundprojekts sind in Bild 3 im Überblick dargestellt.

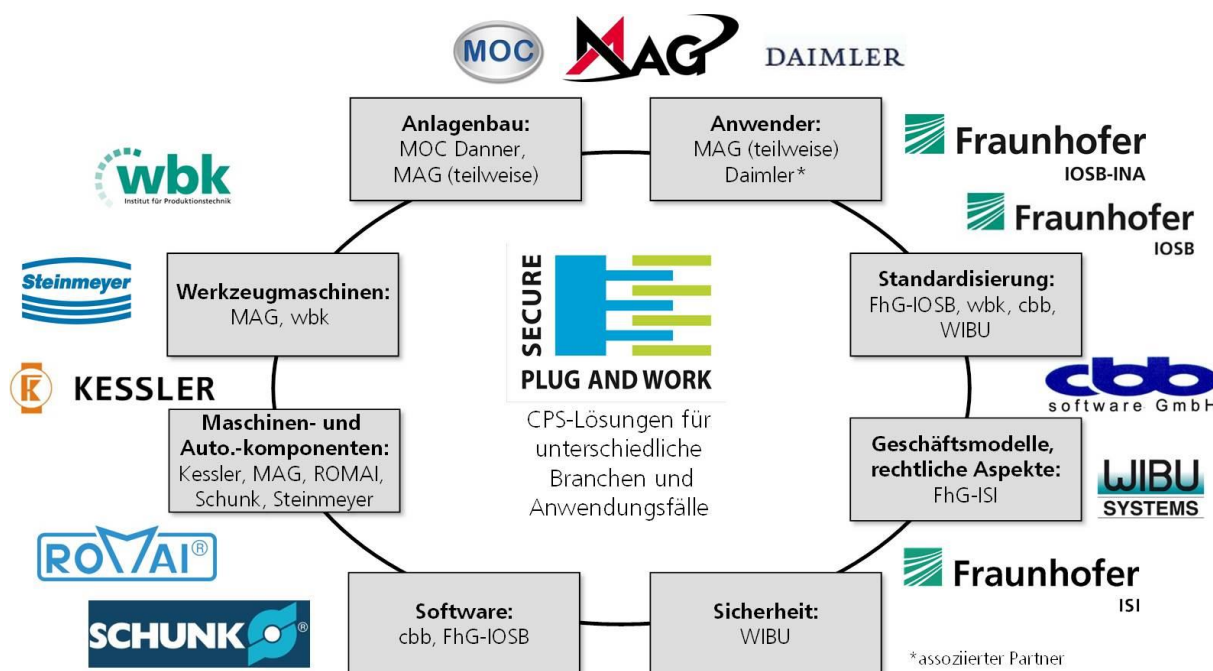


Bild 3: Projektpartner

### **2.3 Industriearbeitskreis**

Um die Projektergebnisse einer breiten Öffentlichkeit zugänglich zu machen und den Austausch der Ergebnisse zwischen verschiedenen Industrie 4.0-Verbundprojekten zu fördern, wurde im Projektverlauf ein Industriearbeitskreis eingerichtet, der mehrfach tagte. Im Einzelnen beteiligten sich die Industrie 4.0-Konsortien der Projekte CSC, eApps4Production, It's OWL, piCASSO, SecurePLUGandWORK (siehe [http://www.iosb.fraunhofer.de/?secureplugandwork\\_arbeitskreis](http://www.iosb.fraunhofer.de/?secureplugandwork_arbeitskreis)).

## 3 Architektur

### 3.1 Verwendete Standards

#### 3.1.1 AutomationML

Ursprünglich als Austauschformat für Engineering-Daten gestartet, haben die Industrie- und Forschungspartner des AutomationML-Vereins AutomationML™ zu einem mächtigen Beschreibungsformat entwickelt und in die internationale Standardisierung (IEC 62714) gebracht. AutomationML ist ein offener Standard, d.h. jedes Unternehmen kann es sofort und kostenfrei verwenden. Im SecurePLUGandWORK-Kontext wird AutomationML genutzt zur Selbstbeschreibung von Geräten, Maschinen und Anlagen sowie von Steuerungen und Netzwerkkomponenten, entsprechend einer Gliederung nach Produkten, Prozessen und Ressourcen. Dies umfasst die Geometrie und Kinematik der Objekte einer Fabrik, deren Logik und Verhalten sowie logische und physische Schnittstellen. Auch Rollen und damit Zugriffsrechte auf Daten können über AutomationML bis auf Datenpunktebene beschrieben werden. Ein übergeordnetes AutomationML-Modell integriert die Einzelmodelle. Es bildet das Zusammenspiel von Fabrik, Linien, Anlagen, der Topologie und der Einbindung in das Fabriknetzwerk ab. AutomationML hat das Potential, sich zu einem Basisformat zur Beschreibung von Industrie 4.0-Komponenten zu entwickeln. In Kombination mit dem Kommunikationsprotokoll OPC UA bildet es eine Schlüsselkomponente für semantische Interoperabilität, d.h. für verständlichen, durchgängigen und echtzeitfähigen Datenaustausch für das Industrielle Internet der Dinge.

#### 3.1.2 OPC Unified Architecture (OPC UA)

Mit der OPC Unified Architecture (OPC UA) steht ein moderner und leistungsfähiger Kommunikationsstandard zur Verfügung, der sich stetig in der produzierenden Industrie weltweit durchsetzt. Dieser Standard nach IEC 62541 bietet vernetzte Informationsmodelle und erlaubt ereignisgesteuerte Kommunikation zwischen Servern und Clients der industriellen Informationstechnik. OPC UA umfasst zukunftsorientierte IT-Sicherheitsmechanismen, sodass die Daten sicher zwischen verschiedenen Standorten verschickt werden können. Modelle aus der Planung, z.B. AutomationML, können entsprechend der gemeinsamen »Companion Specification« von AutomationML e.V. und der OPC Foundation in ein Informationsmodell von OPC UA überführt werden. Dass OPC UA bis auf Chip-Ebene skalierbar ist und darum auf eingebetteten Systemen eingesetzt werden kann, haben Entwickler des Centrums für Industrial IT (CIIT) am Beispiel des dort entwickelten Tiger-Chips gezeigt. Für industrielle Anwendungen in der Industrie 4.0 hat OPC UA seine Leistungsfähigkeit unter Beweis gestellt und verbreitet sich in produzierenden Unternehmen.

Beide im Projekt genutzten Standards, AutomationML und OPC UA, haben das Potential, Industrie 4.0-Komponenten so zu beschreiben, dass sie interoperabel eingesetzt werden. AutomationML könnte beispielsweise eingesetzt werden, um das sog. Manifest einer Industrie 4.0-Komponente zu beschreiben („extern zugänglicher definierter Satz von Metainformationen, der Auskunft über die funktionalen und nicht-funktionalen Eigenschaften der I4.0-Komponente gibt“) [1]. OPC UA kann für den sog. Komponenten-Manager genutzt werden. Natürlich ist die Beschreibung der Industrie 4.0-Verwaltungsschale nicht allein auf diese zwei Standards beschränkt.

### 3.2 Lösungsansatz

Basierend auf den bestehenden AutomationML-Konstrukten wie Rollenkonzepten und Anlagenbeschreibungen entwickelten die Partner im Projekt ein Anlagenmodell, das außerdem die Zertifikate und die Digitalen Rechte der einzelnen SecurePLUGandWORK-Teilnehmer verwaltet und überwacht. Das Anlagenmodell soll es den Projektpartner ermöglichen, Beschreibungen von Komponenten und Maschinen einschließlich der jeweiligen Sicherheitsmodule im Sinne einer mechatronischen Bibliothek abzulegen. Das Anlagenmodell setzt sich aus verschiedenen Komponenten zusammen, die über stark typisierte Links verbunden sind:

- a. Topologie (Attribute und Beziehungen von Objekten in ihrer hierarchischen Anlagenstruktur) implementiert mit CAEX (Computer Aided Engineering Exchange),
- b. Geometrie (grafische Attribute und 3D-Information) implementiert mit COLLADA<sup>1</sup>,
- c. Kinematik (Verbindungen und Abhängigkeiten von Objekten, um Bewegungsplanung zu beschreiben) implementiert mit COLLADA,
- d. Logik (Ablaufsequenzen, internes Verhalten und I/O-Verbindungen) implementiert mit PLCopen<sup>2</sup>
- e. Umweltbedingungen und –einflüsse bzw. Informationen über die Umgebung
- f. Sicherheit (Nutzer, (X509-)Zertifikate, Datenbesitz, ...)

Außerdem entwickelten die Projektpartner eine Softwarekomponente, die Funktionen eines Änderungsmanagers übernimmt, z.B. Versionsverwaltung eingespielter Änderungen, Abgleich von Software-Versionsständen, Logging durchgeführter Revisionsarbeiten an den realen Komponenten der Fabrik, Aktualisierung von Modellen der Digitalen Fabrik, etc. Der Umfang dieses zu implementierenden Änderungsmanagers war in Phase 1 detailliert zu spezifizieren.

Einbringen der Sicherheitsmechanismen und Selbstbeschreibungen auf den Komponenten

1. Passiv, nur Identifizierung an Komponente/Maschine/Anlage und Datenhaltung der Selbstbeschreibung und Sicherheitsmechanismen zentral (Bsp.: Kleber mit QR-Code oder passive RFID).
2. Aktiv auf kontaktlosen oder kontaktbehafteten Chips an Komponente/Maschine/Anlage (z.B. Chips nach ISO/IEC 14443 oder ISO/IEC 18000-3, Kommunikation per NFC)
3. Aktiv auf Datenspeicher an Steuerung der Komponenten/Maschine, z.B. über einen Dongle
4. Datenverbindung für Selbstbeschreibung durch einfaches System zur Selbstbeschreibung an der Komponenten/Maschine anbringen, z.B. Speicherbaustein durch einfaches Bussystem angebunden)
5. Bestehende Datenverbindung zur Komponente/Maschine nutzen und auf dieser aufsetzen. Informationen/Daten können räumlich getrennt gespeichert werden, an Komponente/Maschine kann aber ein Server existieren, der diese verteilt.

Ablage der Beschreibungen und Sicherheitsmechanismen auf den Komponenten des Projekts:

---

<sup>1</sup> COLLADA: <https://www.khronos.org/collada/> [letzter Zugriff: 28.06.2017]

<sup>2</sup> PLCopen: <http://www.plcopen.org/> [letzter Zugriff: 28.06.2017]

- Passive Komponente (Kugelgewindetrieb, usw.). Die Komponente besteht nur aus einem mechanischen System. Mögliche Speichermedien: 1), 2), 3)
- Aktive Komponente (Spindel, Winkelbohrkopf, usw...): Diese Komponente kann Signale in Aktionen umsetzen, die geschieht im Beispiel einer Spindel über elektrische Signale. Mögliche Speichermedien: 3), 4), 5)
- Teilsystem (Greifer, Werkzeugwechsellmagazin, usw...): Das System verfügt über eine eigene Steuerung, kann also aktiv eine Umsetzung von Signalen betreiben. Ein Teilsystem erweitert ein Gesamtsystem (Werkzeugmaschine) um eine Funktionalität. Mögliche Speichermedien: 4), 5)

### 3.3 Systemarchitektur

Die im Projekt in mehreren Iterationen entwickelte Software-Systemarchitektur ist in Bild 4 zusammengefasst. Baugruppen und Maschinen müssen sich vor ihrem Einbau authentifizieren und können erst dann in die Maschine eingebaut oder ans MES angebunden werden. In den Zwischenberichten zum Projekt sind Details der Architektur bereits ausführlich beschrieben.

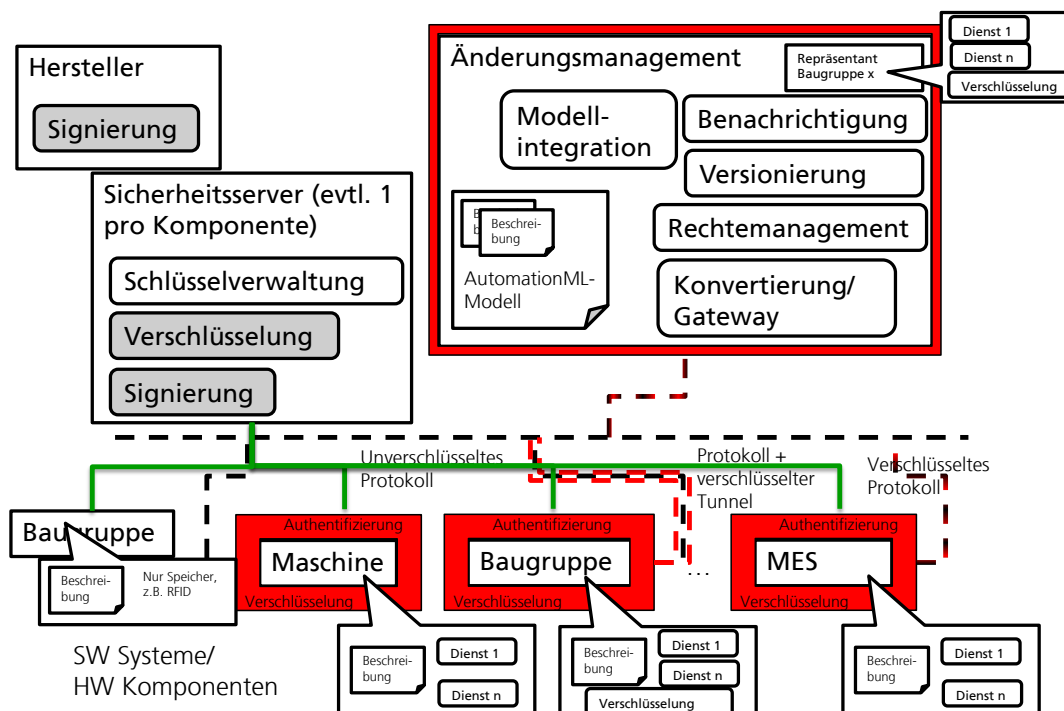


Bild 4: Komponenten/Bausteine der Architektur (1)

Weitere wichtige Bausteine der Architektur sind in Bild 5 aufgeführt. So sorgt die Middleware eMiCo der Fa. cbb dafür, dass verschiedene Quellprotokolle auf OPC UA umgesetzt werden. Eingangsprotokolle, AutomationML-Selbstbeschreibungen, der Vertrauensanker zur Authentifizierung und Verschlüsselung sowie der OPC UA-Server laufen sämtlich auf dem SecurePLUGandWORK-Adapter, der im nachfolgenden Abschnitt erläutert und in den unten aufgeführten Anwendungsbeispielen immer wieder erwähnt wird. Der SecurePLUGandWORK Integrationsserver fasst die OPC UA-Einzelmodell zusammen und stellt sie der ‚Außenwelt (Connected World)‘ zur Verfügung.

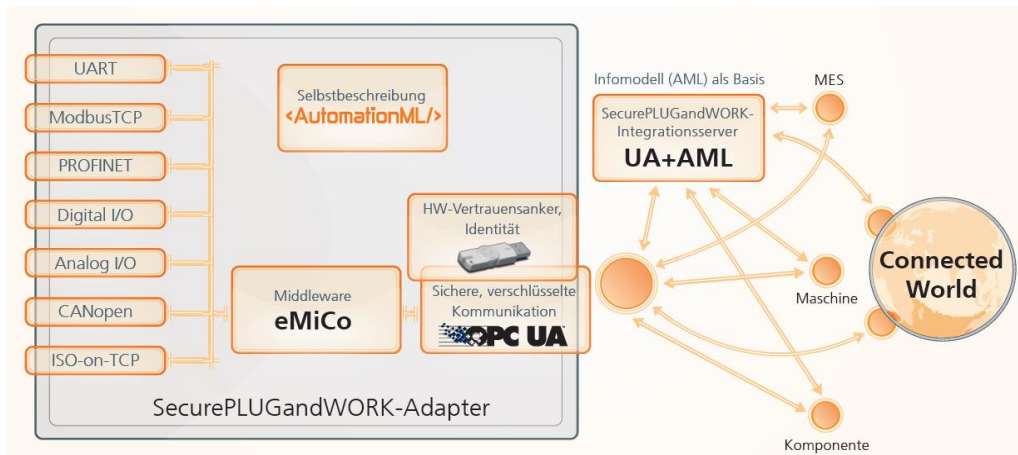


Bild 5: Komponenten/Bausteine der Architektur (2)

## 4 SecurePLUGandWORK-Adapter

Die vorangehend erläuterten Anwendungsfälle führen dazu, dass eine Anbindung zwischen dem physikalischen Prozess und dem Managementsystem erforderlich ist. Physikalische Prozesse werden über Sensoren aufgenommen und können über Aktoren beeinflusst werden. Managementsysteme sind in der Regel in zentralen Architekturen verortet, die über Standard-Ethernet hochgradig mit Mensch und Maschine vernetzt sind. Ein Adapter ist notwendig, um die Schnittstellen zwischen physikalischen Prozessen mit Managementsystemen zu koppeln. Die Konzeption und Umsetzung eines solchen SecurePLUGandWORK-Adapters wird nachfolgend erläutert.

### 4.1 Konzeption

Aus den hier vorliegenden Anwendungsfällen wurden Anforderungen gesammelt und analysiert, die im Anhang im Einzelnen aufgelistet werden. In Tabelle 1 werden die zusammengefassten Analyseergebnisse inklusive einem Lösungsansatz aufgezeigt.

Tabelle 1: Anforderungen an einen SecurePLUGandWORK-Adapter

Nr.	Anforderungsbeschreibung	Lösungsansatz
1	Spannungsversorgung muss industriekompatibel sein und zwischen 5- 36 VDC liegen	Einsatz eines Spannungswandlers (18-36 VDC), 5 VDC im eingeschränkten Betrieb möglich
2	Protokollspezifischen Kommunikation: CAN, SPI, I2C, Ethernet-Vernetzung mit dem Internet und Office Netz per Standard-Ethernet, Anbindung an hochklassige Echtzeit-Ethernetsysteme	Nutzung des eines eingebetteten Systems mit Ethernet-Anschluss, Nutzung eines PROFINET IRT Adapters (TPS1), Implementierung eines CAN-Transceivers, Implementierung eines OPC-UA-Servers
3	4 analoge Eingänge, die zwischen 1-10 V liegen	Nutzung einer Operationsverstärkerschaltung zur Pegelanpassung
4	Zwischen 2-8 digitale Ein- und Ausgänge, die echtzeitfähig Zugriff ermöglichen, Eingangsschwellen nach EN 61131-2 (24 V-Logik) und TTL (2,5-5 V-Logik)	Nutzung von „General Purpose Inputs and Outputs“ mit einer Pegelwandlererweiterung mit einer Schwellenanpassung
5	Industriekompatibles Format: Hutschienenbefestigung, stoßsichere Einhausung, Erdungsschutz, Überspannungssicherung, Verpolungssicherung, Einfacher Anschluss von Eingangs- und Ausgangssignalen	Metallgehäuse mit Hutschienenbefestigung, Klemmblock Anschlüsse
6	Möglichkeit der Vorverarbeitung von Signalen	Nutzung digitaler Signalprozessoren und Softwarefilterung

Im Fokus der Anforderungen stehen Schnittstellenvielfalt, Echtzeitfähigkeit, Vorverarbeitung bei maximaler Systemverfügbarkeit und Robustheit. Aus diesen Anforderungen wurde entnommen, dass im Kern eine leistungsfähige Verarbeitungseinheit mit einem Betriebssystem stehen muss, um die notwendigen Signalvorverarbeitungsschritte durchzuführen, wie auch

die geforderten Protokolle bedienen zu können. Nach diesem Ansatz wurden unterschiedliche eingebettete Systeme hinsichtlich Ihrer Leistungsfähigkeit und Anbindbarkeit verglichen. Aus den bekanntesten Einplatinencomputerlösungen wie RaspberryPI, Odroid, u.a. wurde das BeagleBoneBlack (BBB) ausgewählt. Diese Plattformlösung ist vollständig offen, basiert auf einem Linux System und verfügt über ausreichend Schnittstellen und Rechenleistung für die hier beschriebenen Anforderungen. Die hier fehlende Industriekompatibilität (z.B. Signalpegel bei maximal 3,3 V ohne Absicherung) sollen mit so genannten Capes hergestellt werden, die als aufsteckbare Platinen die Plattform erweitern. Da keine bekannten, kommerziellen Lösungen diese Produktionsanforderungen erfüllen, wurde eine Eigenentwicklung von Platinen, und Gehäuse durchgeführt. Im Folgenden werden anhand der Anforderungen die Designentscheidungen erläutert:

Industriekompatible Spannungsversorgung zwischen 5-36VDC: Spannungsversorgungen, die mit einer größtmöglichen Spannweite von Eingangsspannungen arbeiten können, sind die Klasse der Spannungswandler. Eine Marktrecherche zeigte, dass relevante, kommerzielle Spannungswandler einen maximalen Arbeitsbereich zwischen 18-36 V aufweisen. Da die Anforderungen aus unterschiedlichen Use-Cases gesammelt wurden, ist es zulässig den fehlenden, niedrigen Spannungsbereich, eines reinen 5 V Systems als Design-/Bestückungsalternative zu verwenden. Für die gesamte Plattform ist eine Versorgungsspannung von 5 VDC notwendig, für die digitalen Ausgänge 24 VDC. In Bild 6 ist der entsprechende Schaltplanentwurf dargestellt, der einen Spannungsregler enthält, der mit dem Spannungswandler als Bestückungsvariante ausgetauscht werden kann.

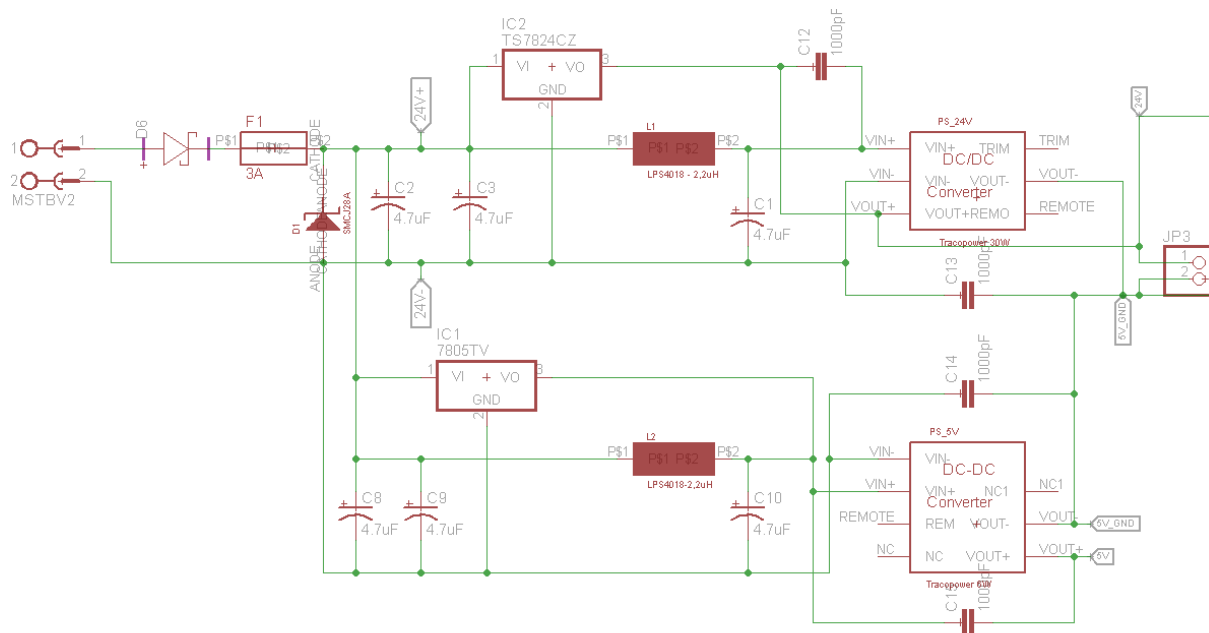


Bild 6: Schaltung zur Spannungsversorgung des Adapters

Mit diesem Design wird erreicht, dass 5 VDC sowie der Bereich zwischen 18-36 VDC zur Spannungsversorgung verwendet werden können. Mit entsprechenden Filter und Kompensationselementen können alle notwendigen Systemspannungen störungsfrei realisiert werden.

Protokollspezifische Kommunikation: Auf dem BeagleBoneBlack sind bereits SPI-, I2C- und eine Standard-Ethernet-Schnittstelle vorhanden. OPC-UA wird als Server installiert, wodurch ein direkter Durchgriff auf die Sensoren und Aktoren möglich ist. Die Kommunikation zu ei-



nem hochklassigen Feldbussystem wird mittels des Moduls TPS1 per PROFINET IRT hergestellt. Per SPI können so z.B. Sensordaten und Steuerdaten mit echtzeitfähigen Steuerungen ausgetauscht werden. Ein CAN-Transceiver wird in die Capes integriert, um eine vollumfängliche Schnittstellenvielfalt zu unterstützen.

Analoge Messtechnik: Das BeagleBoneBlack enthält 4 Analogeingänge, die einen maximalen Pegel bis zu 1,8 V unterstützen. In Bild 7 ist die hierfür erarbeitete Verstärkerschaltung eines Operationsverstärkers dargestellt. Die Eingangspiegel sind mit einer Diode gegen Überspannung gesichert. Außerdem ist die Spannungsmessung über den verbauten Innenwiderstand von 1 M $\Omega$  so ausgelegt, dass ein, gegenüber der konventionellen Messung mit dem BeagleBone, ein deutlich minimierter Strom durch die Messung entsteht.

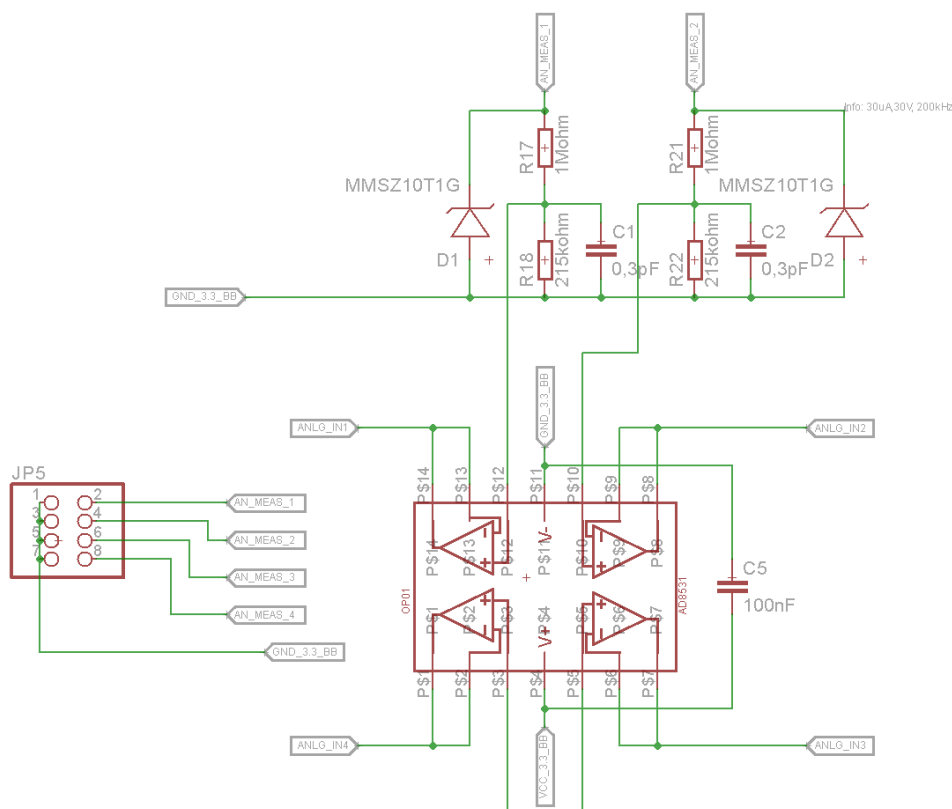


Bild 7: Pegelerweiterung der analogen Spannungsmesseingänge

Es können somit Spannungen zwischen 0-30 V gemessen werden, wobei der Adapter gegen Überspannung geschützt wird.

#### Schaltbare Digitale I/O: IO

Die Eingangssignale sollten unterschiedliche Logiklevel unterstützen und dies adaptiv umsetzen. Ein kommerziell erhältliches Gerät, welches dies ermöglicht, existiert heute nicht. Eine eigene Schaltung wurde daher entsprechend ausgelegt, die in Bild 8 dargestellt wird.

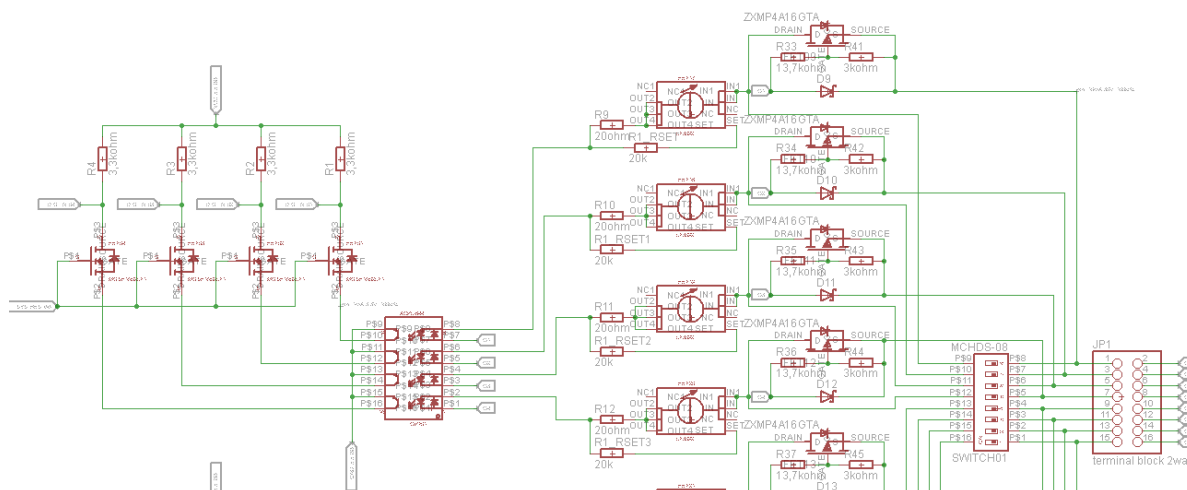


Bild 8: Schaltplanausschnitt der umschaltbaren Eingangslogik

Seitens des BeagleBoneBlack werden die General-Purpose-I/Os (GPIOs) über einen Pull-Up-Widerstand auf 3,3 V-Systemspannung gehalten. Ein Transistor, der auf die Systemfreigabe durch ein Resetsignal reagiert, schaltet die GPIOs auf einen Optokopplerausgang, der die eigentlichen Eingangssignale und die GPIO-Pegel galvanisch trennt. Der Optokoppler verhält sich dabei stromsensitiv: Liegt ein Eingangssignal an, veranlasst ein definierter Strom den Optokoppler zur Signalübertragung. Die Generierung dieses definierten Stroms aus dem Eingangssignal wird mit einem J-Fet realisiert, das als Konstantstromquelle beschaltet wird. Die Hardware wird so gegenüber Schwankungen im Spannungspegel des Eingangssignals abgesichert. Um auch TTL-Logik Spannungspegel zu unterstützen wird die Eingangsspannung über eine Brückenschaltung abgegriffen. Liegt eine TTL-kompatible Spannung an, entspricht die Brückenspannung der Schwellspannung eines Leistungstransistors, der durchschaltet und das Eingangssignal an den J-FET durchleitet. Mit einem Schalter, kann diese Brückenschaltung überbrückt werden, so dass der ursprüngliche Pegel unterstützt wird, wie in Bild 9 dargestellt wird.

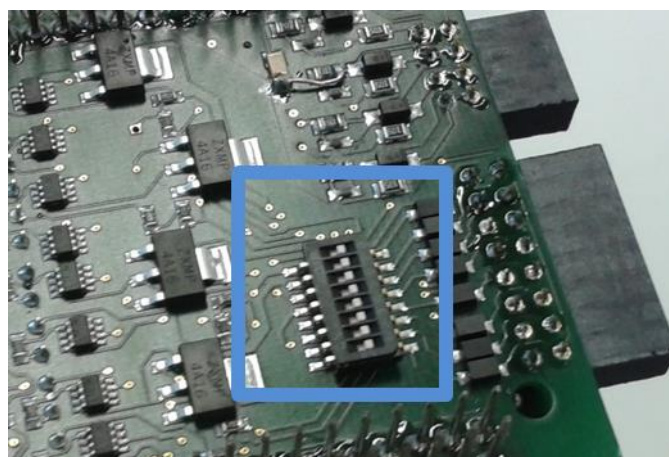


Bild 9: Pegelumschaltung zwischen 24 V- und TTL-Logik

Neben den digitalen Eingängen wurden auch digitale Ausgänge implementiert. Genau wie die Eingänge wurde eine galvanische Trennung durch einen Optokoppler erzeugt, der wiederum eine kommerziell erhältliche Treiberstufe ansteuert.

Industriekompatibles Format: Da der Adapter in Schaltschränken und an Geräten in unterschiedlichen Umgebungen Verwendung finden soll, wurde dieser mit einem Metallgehäuse

ausgestattet. Die Konstruktion wurde derart ausgeführt, dass eine HutschieneMontage möglich ist, die Öffnung eines Deckels einen Eingriff erlaubt und ein Klemmblock aufsteckbar ist. In Bild 10 sind das 3D-Modell und der reale, angeschlossene Adapter dargestellt.

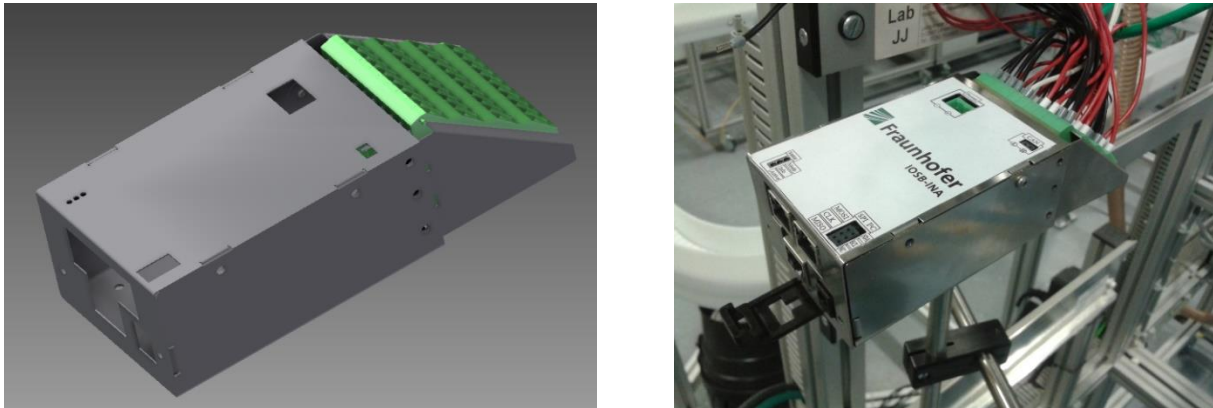


Bild 10: Konstruktion und Realisierung des SecurePLUGandWORK-Adapters

Signalvorverarbeitung: Die Messung von analogen Sensorwerten kann mittels der in den BeagleBoneBlack integrierten Signalprozessoren unternommen werden. Hier sind vielfältige Filtermöglichkeiten programmierbar, die Hardwarebasiert eine Signalverarbeitung ermöglicht. Durch die Middleware kann außerdem eine Softwarebasierte Signalverarbeitung erfolgen.

Gemäß der dargestellten Konzeption wurden zwei doppelagige Capes entwickelt und hergestellt. Nach einem Prototypen und einer Designanpassung wurde der vollständige Adapter für alle Partner und Use-Cases gefertigt.

## 4.2 Validierung

Um die Leistungsfähigkeit des entwickelten SecurePLUGandWORK-Adapters zu bestätigen, wurden zahlreiche Tests durchgeführt. Ein erster Prototyp wurde hinsichtlich seiner Funktionen im Detail messtechnisch erfasst. Getestet wurden die folgenden Eigenschaften:

1. Digitale Outputs: Latenzen, Flankensteilheit, Pegeltreue, Übersprechfaktor, induktives Übersprechen, Belastbarkeit (0-30W Ausgangsleistung im 24-Stunden-Dauerversuch), belastete und unbelastete maximale Steuerfrequenz(10 Hz, 500 Hz, 1,5 kHz).
2. Digitale Inputs: Latenzen, Flankensteilheit, Übersprechfaktor, induktives Übersprechen, unterschiedliche Eingangsspannungslevel (2,5 V, 3,3 V, 5 V 16 V, 24 V).
3. I2C, SPI, CAN, PROFINET-Kommunikation: Tests der maximalen Taktfrequenz (1 kHz-33 MHz), Spannungspegel am Stecker, Übertragung und Empfang von Daten zu einem Gegengerät.
4. Spannungsversorgung: Verpolungssicherung, Versorgung mit Über-, Unterspannung, Spannungseinbrüche.
5. Analogeingänge: Eingangsspannung zwischen 0-10 V. Ausgangsspannung verhält sich linear zwischen 0-1,8 V.

Sämtliche Tests haben die Prototypen erfolgreich bestanden. Für die abschließende korrekte Übergabe der Adapter für die Use-Cases wurden erfolgreich vor Auslieferung fünf weitere Tests durchgeführt.

1. Gesamtleistungsaufnahme wurde gemessen

2. Versorgungsspannungen wurden variiert
3. Funktion der digitalen Outputs bei 60 Hz
4. Funktion der digitalen Inputs bei 1,5 kHz, und unterschiedlichen Spannungspegeln
5. Funktion der analogen Inputs bei Spannungen von 0-10 V

Zur Gesamtintegration wurde weiterhin ein OPC-UA-Server auf dem BeagleBoneBlack installiert, der Sensoreingänge auslesen und GPIOs ansteuern konnte. Die Integration in eine PROFINET Netzwerk wurde ebenfalls erfolgreich mit einer eigenen Gerätebeschreibung durchgeführt. Um das System handhabbar für die Partner zu gestalten, wurde außerdem eine Gebrauchsanleitung verfasst, die die elektronischen Spezifika aufzeigt, Beispielschaltungen für Sensoren und Aktoren darstellt und in einer Beschreibung der Softwareansteuerung in Linux mündet.

### 4.3 Zusammenfassung und Einsatz

Die hier entwickelte Hardware-Test-Plattform für das Projekt SecurePLUGandWORK kann für Forschungs- und Testzwecke genutzt werden. Sie darf nur auf eigenes Risiko im produktiven Umfeld zum Einsatz kommen. Das Fraunhofer IOSB übernimmt hierfür keine Haftung. Insgesamt konnten die folgenden Funktionalitäten und Leistungen mit dem SecurePLUGandWORK-Adapter erreicht werden:

- Versorgungsspannung:
  - Input 18-36VDC (nominal 24VDC)
- Digitale Ausgänge:
  - 8-Kanäle
  - 24VDC abei 30W(pro Kanal max 0,8A, -norm 0,15A, normale Version: 24VDC at 4,8W)
  - Kurzschlussicherheit
  - Induktive Lasten
  - Maximale Ausgangsfrequenz zwischen 1,5-1,8kHz (abhängig von der Lastsituation)
  - Galvanische Trennung
- Digitale Eingänge:
  - 8-Kanäle
  - Logic levels für jeden Kanal separat einstellbar
  - Unterstützung der Logik Level: TTL-, CMOS-, LV-Logic, 24 V
  - Maximale Eingangsfrequenz von 5,5kHz
  - Galvanische Trennung
  - Kurzschlussicherheit
  - Leistungsaufnahme bei maximal 15+/-1.8mA pro Kanal
- Analog Eingänge:
  - 4-Kanäle
  - Spannung bis zu 10V (Erweiterbar bis zu 30V)
  - Kurzschlussicherheit
  - Hohe Eingangsimpedanz (>1,2M $\Omega$ )
- CAN Interface
- SPI Interface supported
- I<sup>2</sup>C Interface supported
- Profinet<sup>®</sup> Interface unterstützt
  - by TPS1- $\mu$ Board (Company OWITA) expansion

Der SecurePLUGandWORK-Adapter wurde als Steuerung in einem modularen Produktionssystem in der SmartFactoryOWL, einer Initiative des Fraunhofer IOSB-INA und der Hochschule OWL, eingesetzt. Auf der Hannovermesse 2015 wurde außerdem zwei Exponate im Bereich Modularität und Sicherheit durch den Adapter demonstriert. Der Einsatz in einem echtzeitfähigen, Ethernet-basierten Netzwerk wurde hierbei evaluiert.

Die Integration von Anlagen/Sensoren/Aktoren mit SecurePLUGandWORK-Adapter wurde durchgeführt. Für den Fall, dass es sich um ein WLAN-basiertes System handelt, ist die Integration beispielhaft in Bild 11 dargestellt:

1. Modul wird hinzugefügt: UA-Server verbindet sich mit dem Global Discovery Server (RegisterServer)
2. UA-Client ruft Status vom GDS ab und erkennt, dass ein neuer UA-Server vorhanden ist (FindServers)
3. UA-Client verbindet sich mit UA-Server des Moduls
4. Kommunikation gemäß EA-Modell

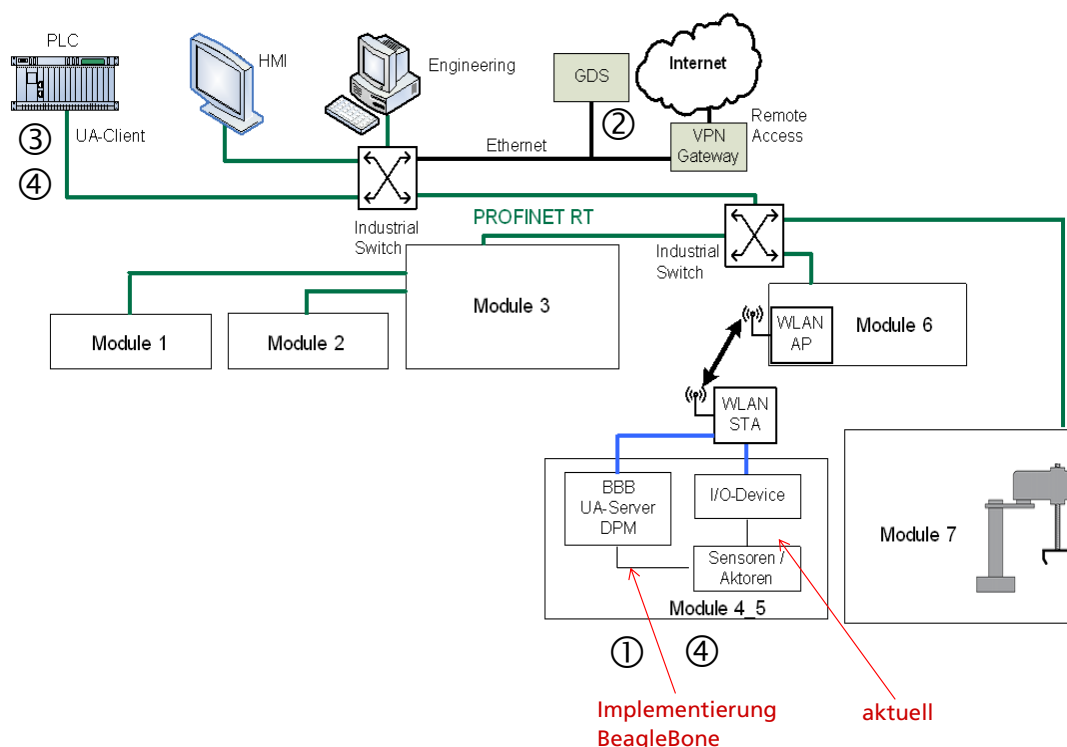


Bild 11: Beispielintegration des SecurePLUGandWORK-Adapters (BBB) per WLAN

In diesem Fall wird ein WLAN-Adapter an das BeagleBoneBlack angeschlossen und so eine Funkverbindung aufgebaut. Ein zusätzliches IO-Device kann hierdurch ersetzt werden.

#### 4.4 Andere ‚Industrie 4.0-Adapter‘

Eine besondere Herausforderung von Industrie 4.0 liegt darin, bestehende Maschinen und Anlagen kommunikationsfähig zu machen – im Gegensatz zu SecurePLUGandWORK, das anwendbar auf neue Komponenten und Maschinen ist. Während Hersteller in Neuanlagen geeignete Kommunikationsschnittstellen wie die hier entwickelten Lösungen einbauen und liefern können, müssen Bestandsanlagen ggfs. nachgerüstet werden.

Hauptschwierigkeiten dabei sind, den laufenden Betrieb nicht zu stören und die Gewährleistung des Maschinenlieferanten zu erhalten. Die Maschinen müssen also nachträglich so befähigt werden, dass die Betreiber einfach einen ‚Adapter‘ nachrüsten, mit dem die Maschine Daten nach außen kommunizieren kann. Diese Nachrüstlösungen werden heute unter den Bezeichnungen IIoT-Adapter, Gateways oder Middleware-Lösungen beworben. Im Kern geht es dabei darum, die Forderung nach Interoperabilität zu erfüllen. Die meisten marktgängigen

Produkte setzen darauf, OPC UA als Kommunikationsstandard für Industrie 4.0 zu nutzen und vorhandene Protokolle bestehender Maschinen und Anlagen einfach auf OPC UA umzusetzen, z.B. Modbus, CanOpen, Profinet, Profibus, IOLink oder Ethercat. Allerdings ist es für Industrie 4.0 nicht ausreichend, Geräte allein zum Datenaustausch zu befähigen. In der Kommunikation muss auch klar sein, was die ausgetauschten Daten bedeuten. Also benötigt man für Industrie 4.0 eine semantische Beschreibung von Maschinen und Produktionsanlagen. Aufgrund der oben beschriebenen Vielfalt an Geräten, Maschinen, Steuerungen und Engineering-Werkzeugen, z.B. zur Steuerungsprogrammierung, bietet es sich daher an, ein universelles Datenaustauschformat zu nutzen. Beispielsweise können Ingenieure und Planer Fähigkeiten und Datenbedeutungen von Maschinen und Anlagen wie oben beschrieben mit AutomationML nach IEC 62714 beschreiben, so dass auch andere Datenabnehmer sie verstehen und verarbeiten können. Anwendungsmöglichkeiten solcher Selbstbeschreibungen sind schnellere Inbetriebnahmen, das Mitliefern der Dokumentation zur Maschine oder Anlage und die Nutzung der Selbstbeschreibungen zur Konfiguration anderer IT-Systeme, z.B. Visualisierungen oder Leitsysteme.

Wirklich Industrie 4.0-taugliche Nachrüstlösungen umfassen also eine modellhafte Beschreibung der Maschinen und Anlagen und deren Daten und eine geeignete zukunftsfähige Kommunikationslösung. Auch hierfür ist bereits eine mögliche Lösung verfügbar, die auf den im Projekt erarbeiteten Lösungen aufbaut: der „PLUGandWORK-Cube“. Mit ihm können produzierende Unternehmen ihre Maschinen nachrüsten, so dass sie den Kommunikationsstandard OPC UA 'sprechen', und zwar inklusive der Gerätebeschreibung als AutomationML-Modell. Das Abbild der Maschinen und Anlagen steckt also als Informationsmodell nach der OPC UA Companion Specification »OPC Unified Architecture for AutomationML« [2] im PLUGandWORK-Cube. Dieser baut automatisch seinen Adressraum mittels Informationsmodell nach AutomationML auf und bietet eine vereinheitlichte Kommunikation nach außen über OPC UA, z.B. zum MES. Über verschiedene Kommunikationskanäle wird die Prozessankopplung realisiert, z.B. wenn Steuerungen unterschiedlicher Hersteller angekoppelt werden sollen. Die Performanz ist dabei beispielsweise abhängig von der Anzahl der SPS-Variablen oder dem Abfragezyklus zur SPS. Schon heute sind folgenden Kanäle verfügbar: OPC UA Client, Siemens S7, ODBC, OPC DA. Die aktuelle Hardware-Basis des PLUGandWORK-Cubes ist ein kompakter SIMATIC Industrie-PC (IPC227E) mit dem Betriebssystem Windows, aber darauf nicht beschränkt.

Mit dem PLUGandWORK-Cube sind weitere Dienste nutzbar, beispielsweise die Generierung von WinCC- oder ProVis.Visu-Prozessführungsbildern auf Basis der AutomationML Modelle einschließlich der Kopplung an den aggregierenden OPC UA-Server des Cubes. Auch die Konvertierung von AutomationML-Modellen in die XML-Repräsentation der OPC UA-Informationsmodelle nach den Regeln in [2] kann als Dienst erfolgen. Weiterhin sind zur Erstellung der benötigten AutomationML-Modelle verschiedene Assistenztools verfügbar, z.B.

- Plugins für den offiziellen AutomationML-Editor, z.B. zur geführten Erstellung von AutomationML-Modellen nach individuellen Vorgaben oder zur Zusammenführung mehrerer AutomationML-Modelle,
- Prüfung der Modelle auf Konformität zur IEC Spezifikation IEC62714-1, den zugehörigen XML-Schemata sowie Hinweise zur Korrektur der Modelle und Autokorrekturmechanismen bei Abweichungen von der Spezifikation,

Importfunktionen für weitere toolspezifische Schnittstellen, z.B. Grafikdaten (Format DXF), csv, XML, Microsoft-Excel, Datenbank, API, etc.

#### 4.4.1 Ergebnisse einer Umfrage unter Anwendern

Diverse Anwenderunternehmen wurden im Verlauf des Projekts befragt, welche IoT-Adapter und –Lösungen sie einsetzen bzw. einzusetzen planen. Die Ergebnisse der Online-Befragung sind hier kurz dargestellt.

34 Unternehmen aus unterschiedlichen Branchen haben an der Umfrage teilgenommen

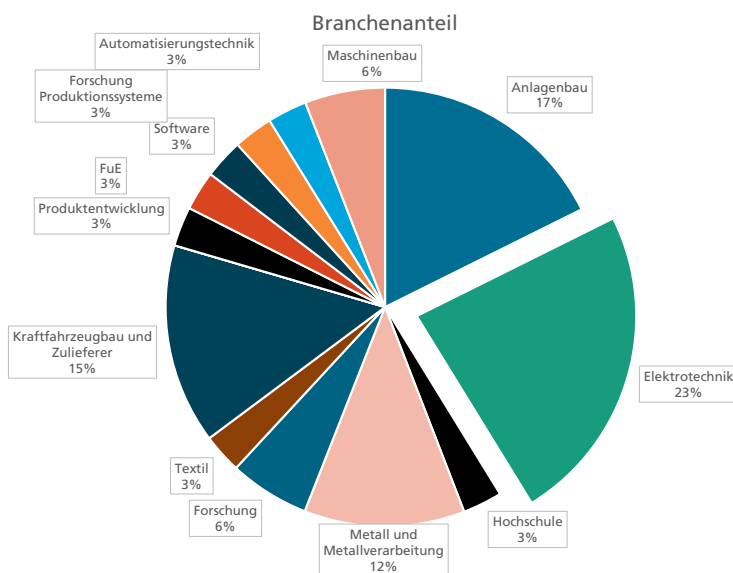


Bild 12: Herkunftsbranchen der Umfrageteilnehmer

Die Mehrzahl der teilgenommenen Unternehmen hat mehr als 5000 Mitarbeiter.

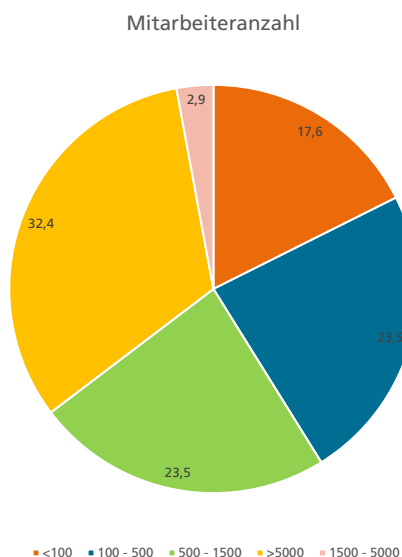


Bild 13: Unternehmensgröße

97% der Unternehmen können sich vorstellen, Daten ihrer Maschinen und Anlagen systematisch zu erfassen und zu nutzen.

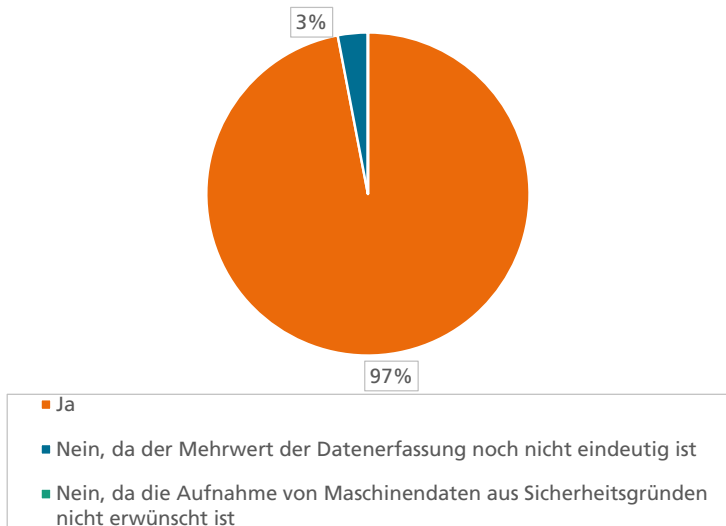


Bild 14: Wunsch nach Datennutzung eindeutig

Die Unternehmen sehen einen unterschiedlichen Nutzen bei der Auswertung und Sammlung von Maschinendaten.

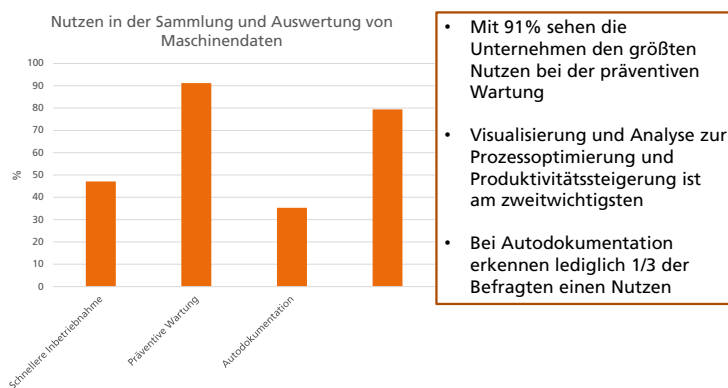


Bild 15: Vermutete Nutzenpotentiale bei den Umfrageteilnehmern

Condition Monitoring und Datenauswertung ist schon bei 81% der Unternehmen im Einsatz oder geplant.

### Condition Monitoring

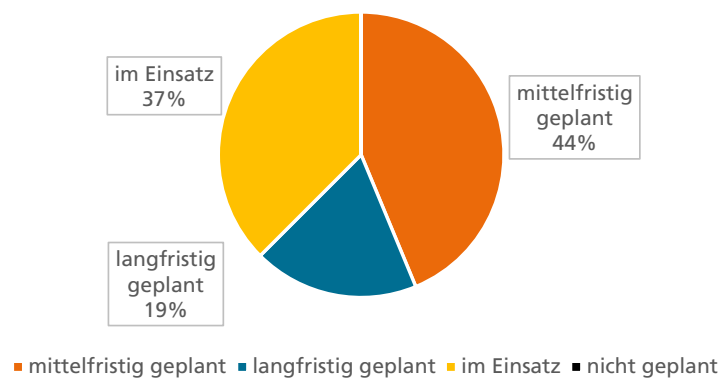


Bild 16: Datenbasiertes Condition Monitoring als Haupteinsatzfeld



Fast die Hälfte der befragten Unternehmen plant mittelfristig Industrie 4.0 Geschäftsmodelle einzusetzen.

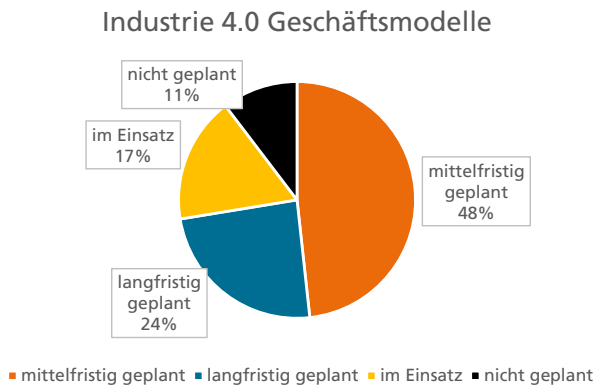


Bild 17: Planung des Einsatzes Industrie 4.0-basierter Geschäftsmodelle

Kommunikation von der Produktion bis in den Office Bereich ist bei allen auf der Agenda oder schon längst umgesetzt.

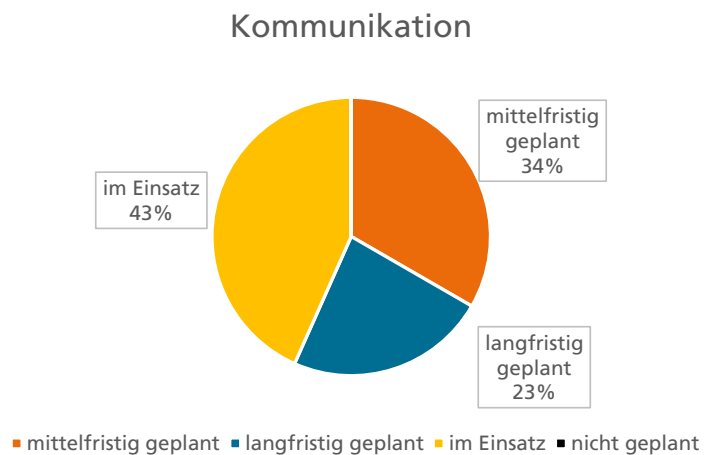


Bild 18: Durchgängige Kommunikation geplant oder umgesetzt

Nur 28% der Befragten gaben an, Cloud/Fog Computing in Zukunft nicht geplant zu haben.

Fernwartung ist in der Produktion mit fast 60% weit verbreitet.

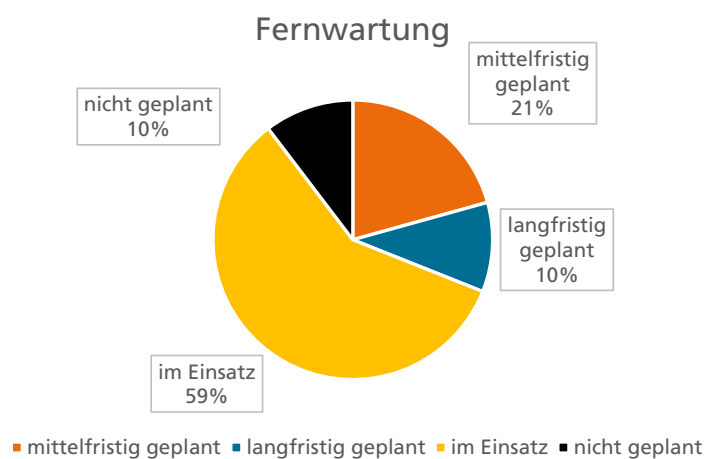


Bild 19: Einsatz von Fernwartung bei den Umfrageteilnehmern

Autonome Systeme stehen mittelfristig bei 40% der Unternehmen auf der Agenda.

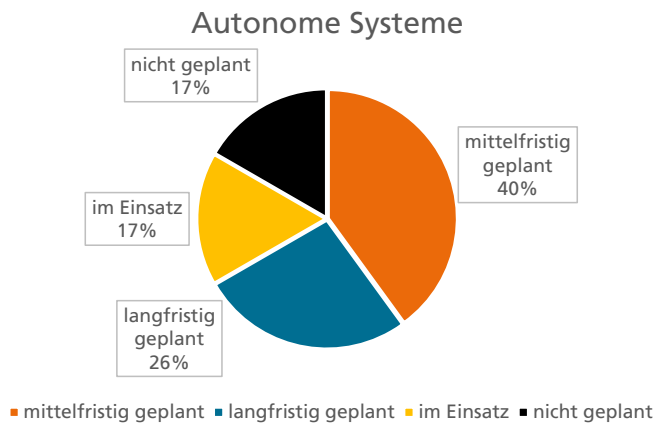


Bild 20: Einsatz autonomer Systeme bei den Umfrageteilnehmern

Eine Vielzahl unterschiedlicher Speicherprogrammierbarer Steuerungen (SPS) werden in den Unternehmen eingesetzt.

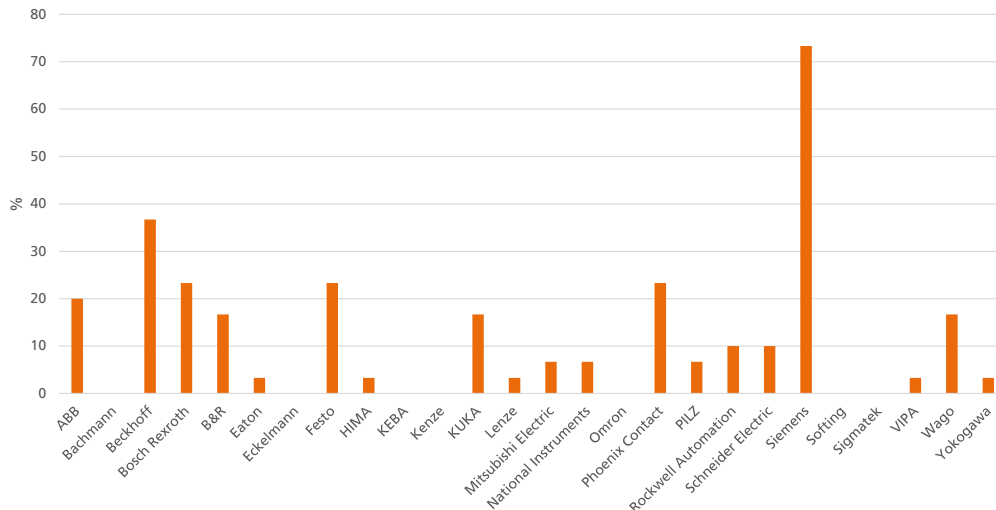


Bild 21: Eingesetzte SPSen bei den Umfrageteilnehmern

Viele Maschinen sind schon im Intranet, aber noch nicht an das Internet angeschlossen.

Sind ihre Maschinen an das Intranet angebunden?

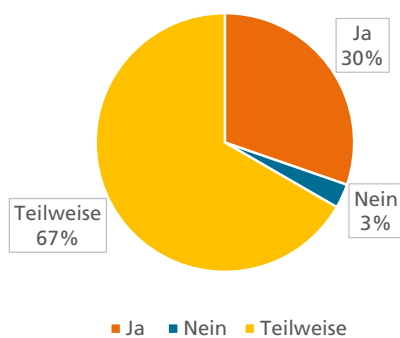


Bild 22: Grad der Vernetzung von Maschinen

Sind ihre Maschinen an das Internet(z.B.Cloud) angebunden?

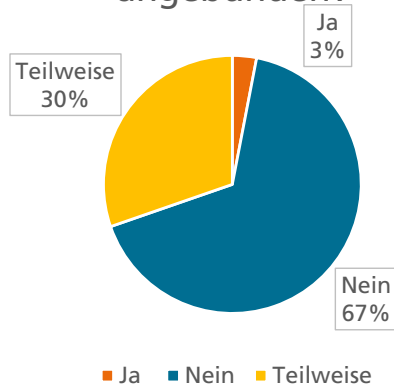


Bild 23: Skepsis bei Einsatz von Clouds

Eine Anbindung an das Intranet und/oder das Internet realisieren die Unternehmen durch folgende Protokolle/Bussysteme:

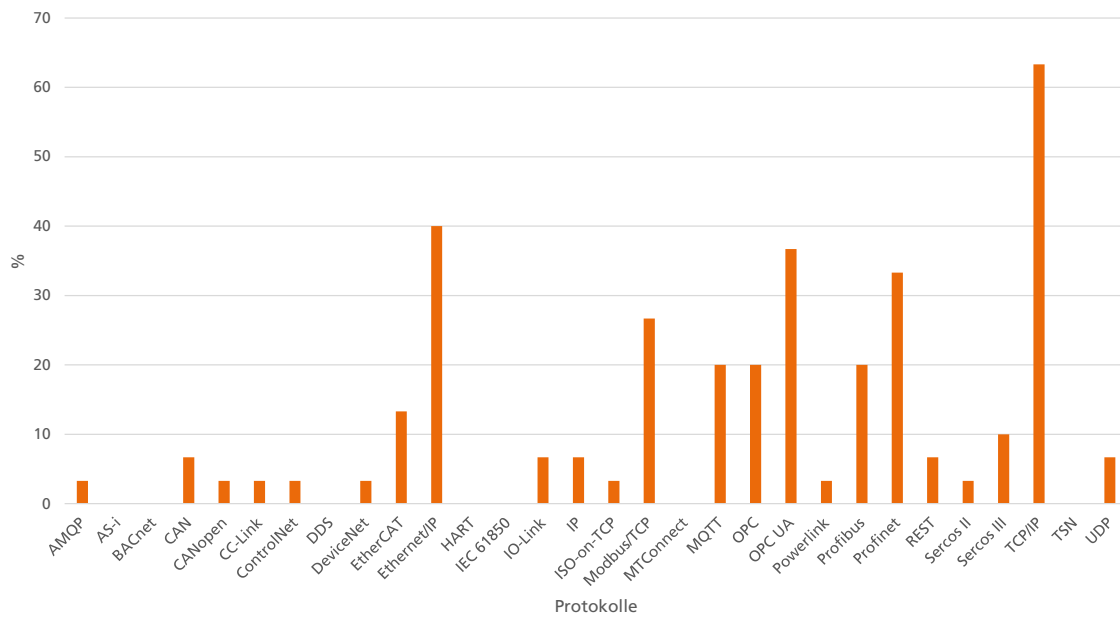


Bild 24: Eingesetzte Protokolle

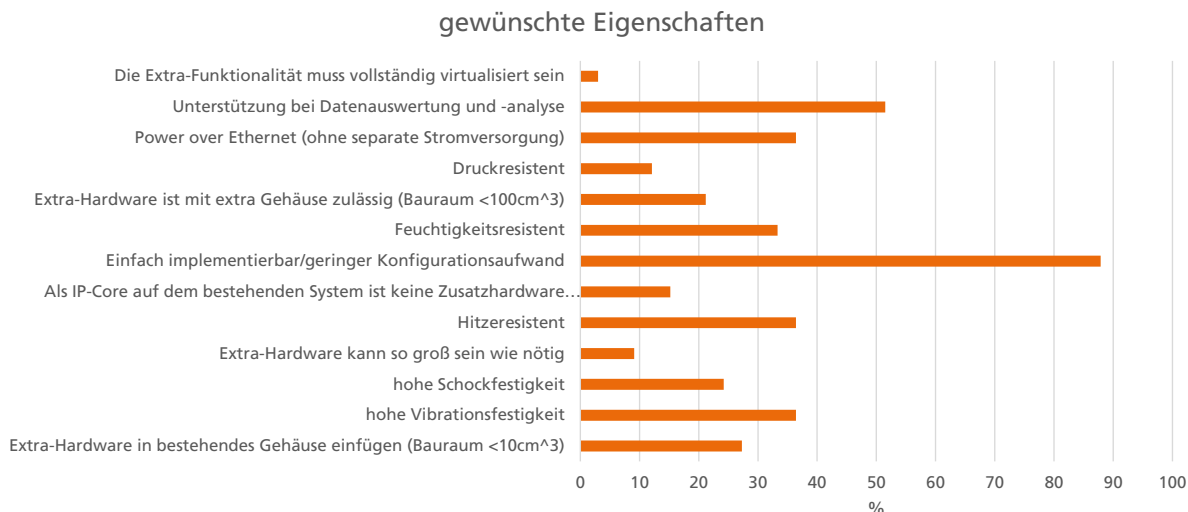


Bild 25: Gewünschte Eigenschaften von Adaptern

85% der Befragten gaben an, dass eine einfache Implementierung und ein geringer Konfigurationsaufwand am meisten gewünscht werden. Die Extra-Hardware würde am liebsten in ein bestehendes Gehäuse eingefügt werden.

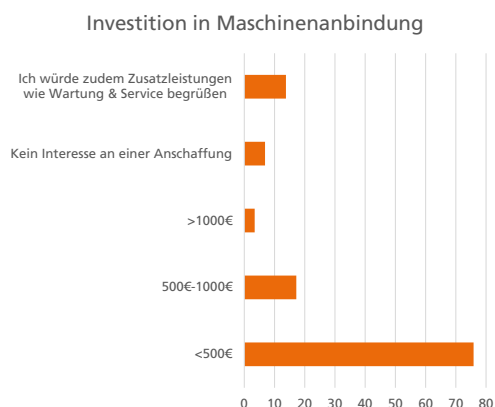


Bild 26: Zahlungsbereitschaft für eine nachträgliche Vernetzung

75% würden weniger als 500€ für eine Maschinenanbindung ins Netz bezahlen, nur 14% würden Zusatzleistungen wie Wartung und Service begrüßen. Die komplette Auswertung findet man auf der Webseite <http://iosb.fraunhofer.de/?i40plattform>.

#### 4.4.2 Anbieter von ‚Industrie 4.0-Adaptern‘

Ebenso wie die Anwender wurden auch Anbieter von IoT-Gateways, Adaptern o.ä. befragt. Im Folgenden sind die Ergebnisse zusammengefasst. Die Auswertung ist ebenfalls auf der o.g. Webseite zu finden.

Service-oriented Architecture		Client/Server			Pub/Sub			proprietär
Box	Hersteller	OPC UA (SOAP/HTTP?)	REST	CoAP	DDS	MQTT	AMQP	oneM2M
BlackBox 2	autem							
netIoT Edge	Hilscher	x						
OPC UA Gateway	HMS	x						
CloudPlug	SOTEC	x						
Tixi Cloud Gateways	Tixi							
MICA Base	Harting	x				x		
Comprosys	Contec	x						
IoT Gateway	Bosch Rexroth	x	x					
atvise scada + box	CERTEC EDV	x						
HB-DataHub	HB-Softsolution e.U.	x	x					
IBH Link UA	IBHsoftec	x						
echocollect	softing	x						
dataFEED uaGate	SOFTING Industrial	x				x		
Spectra PowerBox 100-IOT	Spectra	x				x		
eWON Flexy	eWON (HMS)	x	x					
OpenIoTfog	Fraunhofer Fokus	geplant	x	x	geplant	x		x
SIMATIC IOT2000	Siemens							

Bild 27: Untersuchte Adapterlösungen

Feldbusse			
Box	Hersteller	ProfiBus	Can Bus
BlackBox 2	autem		
netIoT Edge	Hilscher		
OPC UA Gateway	HMS		
CloudPlug	SOTEC	x	x
Tixi Cloud Gateways	Tixi		
MICA Base	Harting		
Comprosys	Contec		
IoT Gateway	Bosch Rexroth		
atvise scada + box	CERTEC EDV		
HB-DataHub	HB-Softsolution e.U.		
IBH Link UA	IBHsoftec		
echocollect	softing		
dataFEED uaGate	SOFTING Industrial		
Spectra PowerBox 100-IOT	Spectra	x	x
eWON Flexy	eWON (HMS)	x	
OpenIoTfog	Fraunhofer Fokus		
SIMATIC IOT2000	Siemens		

Bild 28: Unterstützte Feldbusse der Adapter (1)

Ethernet								
Box	Hersteller	ProfiNet	EtherCAT	Powerlink	Ethernet/IP	Sercos 3	CC-Link	Modbus/TCP
BlackBox 2	autem							
netIoT Edge	Hilscher	x	x (nur netX)					
OPC UA Gateway	HMS							
CloudPlug	SOTEC							
Tixi Cloud Gateways	Tixi							
MICA Base	Harting	x	x		x			x
Comprosys	Contec		x		x			x
IoT Gateway	Bosch Rexroth					x		
atvise scada + box	CERTEC EDV							
HB-DataHub	HB-Softsolution e.U.				x			x
IBH Link UA	IBHsoftec	x						
echocollect	softing							x
dataFEED uaGate	SOFTING Industrial							
Spectra PowerBox 100-IOT	Spectra	x	x	x	x	x	x	x
eWON Flexy	eWON (HMS)				x			x
OpenIoTfog	Fraunhofer Fokus	x	geplant				x	
SIMATIC IOT2000	Siemens							

Bild 29: Unterstützte Feldbusse der Adapter (2)

## 5 SecurePLUGandWORK-Integrationsserver

Der PLUGandWORK-Integrationsserver (Bild 30) ist eine der Kernkomponenten der von den Partnern definierten Software-Architektur (siehe Bild 4) und besteht aus den im Folgenden kurz aufgeführten Komponenten, entwickelt vom Fraunhofer IOSB.

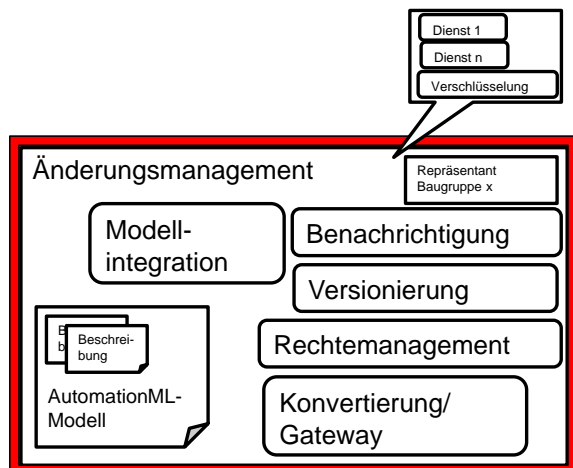


Bild 30: Funktionalität Integrationsserver

### Kommunikation

Der Integrationsserver verfügt über eine Kommunikationsschnittstelle, die ereignisgesteuert reagiert und bei der sich Tools für Benachrichtigungen bei Änderungen an interessanten Stellen registrieren können. Außerdem übernimmt der Kommunikationsteil die Verschlüsselung/Signierung von Datentelegrammen.

### Änderungsmanagement

Dieser Teil des Integrationsserver erledigt die Integration und Harmonisierung verschiedener Modelle aktiver Komponenten im Integrationsserver. Änderungen in Anlagenkonfigurationen werden erkannt und an beteiligte/andere interessierte Kommunikationspartner übermittelt. Dies beinhaltet die Beschreibung der Änderungen in einem standardisierten Datenaustauschformat.

### Rechtemanagement/Rollenbasierte Zugriffskontrolle auf Informationen (online)

Dieser Teil des Integrationsserver besteht zunächst aus dem ‚RoleManager‘, einem Software-Tool zur Definition von Rollen. Es ist in Integration in AML und wird von Konverter in UA XML übersetzt. Die Auswertung und Ausführung der beschriebenen Rollen und Zugriffsberechtigungen erfolgt dann im Integrationsserver. Im Detail sind die hier verfügbaren Funktionen in [3] beschrieben.

## 6 Assistenztool

Ein weiteres wichtiges Werkzeug im Projekt, das ebenfalls das Fraunhofer IOSB entwickelte und den Partner zur Verfügung stellte, ist ein assistierendes Werkzeug, mit dem die Partner ihre AutomationML-Modelle in die jeweiligen OPC UA-Server konvertieren. Es umfasst im einzelnen folgende Funktionen:

- Plugin für den AutomationML-Editor, mit dem Modelle erstellt, visualisiert und/oder geändert werden,
- Konvertiert das Datenaustauschformat in ein Importformat, das vom jeweiligen Zielsystem akzeptiert wird, und zwar
  - AutomationML zu systemspezifischem XML (Middleware-Konfiguration) und
  - AutomationML zu OPC UA.
- Schnittstelle zum SecurePLUGandWORK-Adapter.

## 7 SecurePLUGandWORK-Middleware

### 7.1 Entwicklungsarbeiten

Die Aufgabe der Middleware liegt darin, die gesamte Kommunikation zwischen den unterschiedlichen Sensoren, z.B. Temperaturfühler, Druckfühler, Drehzahlmesser, Lichtschranken, und Aktoren, z.B. Motoren, Ventile, Magnetschalter, Heiz- oder Kühlelemente, durchzuführen. Hier bietet die Middleware eine effiziente Lösung. Für jeden Teilnehmer im System (Sensoren, Aktoren) wird nur einmalig eine Bibliothek für seine spezifischen Eigenschaften programmiert. Anschließend kann dieser Teilnehmer im Sinne einer „PLUGandWORK“ Funktionalität, ähnlich wie ein USB-Gerät am PC, auf einfache Weise mit dem Controller zusammenarbeiten. Die herstellereigenen Protokoll-Eigenschaften spielen dann keine Rolle mehr.

Es erfolgte die Integration des OPC UA Servers in die eMiCo Middleware. Als geeignete Plattform für den SecurePLUGandWORK-Adapter ist ein Beagle Bone Black ausgewählt worden. Bild 31 zeigt den Beagle Bone Black.

Beagle Bone Black and TPS-1 TIGER chip

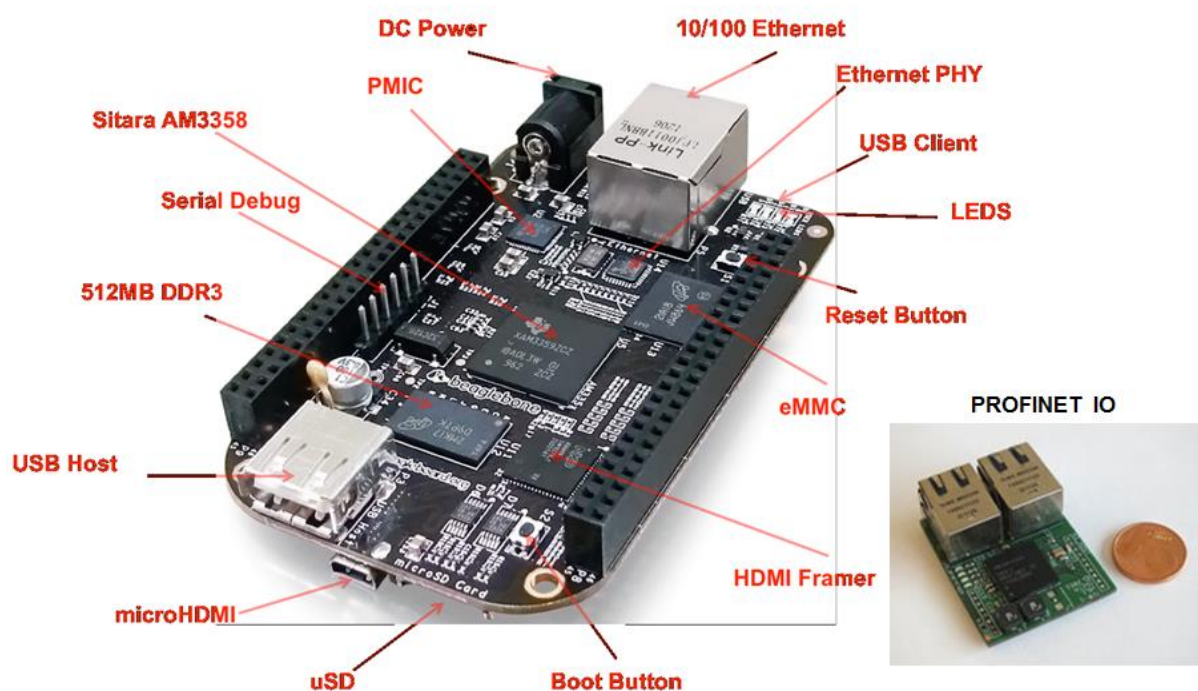


Bild 31: BeagleBoneBlack (BBB)

Der Beagle Bone Black ist ausgestattet mit einem AM335x 1GHz ARM® Cortex-A8 Prozessor. Er besitzt 512MB DDR3 RAM, einen µSD-Karten-Slot, USB Host, Ethernet, HDMI und 2x 46 Pin-Buchsenleisten.

Im nachfolgenden Bild 32 ist eine schematische Übersicht der in der Middleware implementierten Schnittstellen dargestellt, welche im Projekt Verwendung finden.



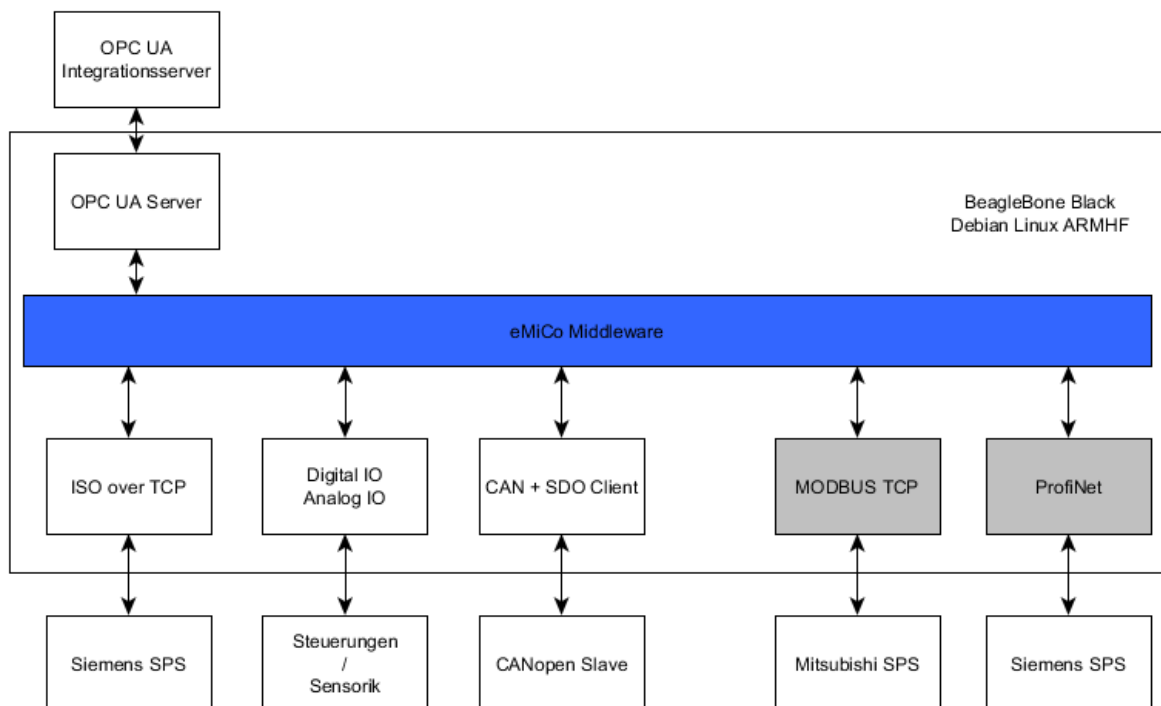


Bild 32: Übersicht der implementierten Schnittstellen

Für das Projekt wurden Konfigurationen für die Middleware-Schnittstelle ISO over TCP bereitgestellt und getestet. Für Digital I/O und Analog I/O wurde eine Middleware-Schnittstelle geschaffen, welche die Schnittstellen des ARM-SoC bedient. Die Entwicklung an der CANopen-Schnittstelle wurde durchgeführt. Außerdem wurde die Integration der ProfiNET-Schnittstelle auf Basis des Tiger-Chips durchgeführt. Ferner erfolgte die Integration des WIBU Security SDKs in die OPC-UA-Server-Komponente. Des Weiteren wurde eine Modbus/TCP-Schnittstelle entwickelt.

Anhand der an den spezifischen Hardwareschnittstellen durchgeführten Tests wurde die Middleware eMiCo entsprechend angepasst. Es wurde die eMiCo-Middleware auf der Projekthardware integriert und mit den entsprechenden Hardwareschnittstellen verbunden. Testweise wurden Beispielfiguren für die Anlagen der Projektpartner entwickelt.

Es wurde ein Prototyp für ein finales Betriebssystem-Image für den SecurePLUGandWORK-Adapter erstellt. Dieses wurde in Abstimmung und in Zusammenarbeit mit dem IOSB definiert und umgesetzt. In Kooperation mit dem IOSB wurden Beispielfiguren für die Middleware erzeugt. Diese dienen als Grundlage für die automatische Erzeugung der Middleware-Konfigurationen durch den Integrationsserver. Im weiteren Verlauf wurde die automatische Konfigurationserzeugung optimiert. Dies gilt für die Interfaces zu den zu steuernden Anlagen ITOT, CANopen, Digital / Analog I/O, Modbus/TCP sowie der Schnittstelle zum Integrationsserver OPC-UA.

Die Security-Konfiguration wurde beispielhaft dargestellt und wurde für die weitere Security-Umsetzung verwendet. Des Weiteren erfolgten umfangreiche Anwendungs-Tests am SecurePLUGandWORK-Adapter vorgenommen, um dessen Funktionsfähigkeit zu prüfen.

## 7.2 Parallele Standardisierung

In der im Januar 2013 herausgegebene VDE/VDI Richtlinie 2657 Blatt 1 „Middleware in der Automatisierungstechnik - Grundlagen“, in der die Bedeutung der Middleware-Technologie für die Automatisierungstechnik erkannt und empfohlen wird, wird unsere Middleware Lab-Map<sup>®</sup> namentlich genannt und empfohlen. Die Ideen und Ansätze unserer Middleware Lab-Map dienen als Grundlage für die Entwicklung des eMiCo.

Basierend auf den Projektergebnissen wurde diese VDE/VDI Richtlinie im September 2016 um Blatt 2 „Middleware in der Automatisierungstechnik - Vorgehensmodell für den Middleware-Engineering-Prozess“ erweitert. Hier wurde in der Beschreibung der technischen Architektur unsere Middleware LabMap als Beispiel verwendet.

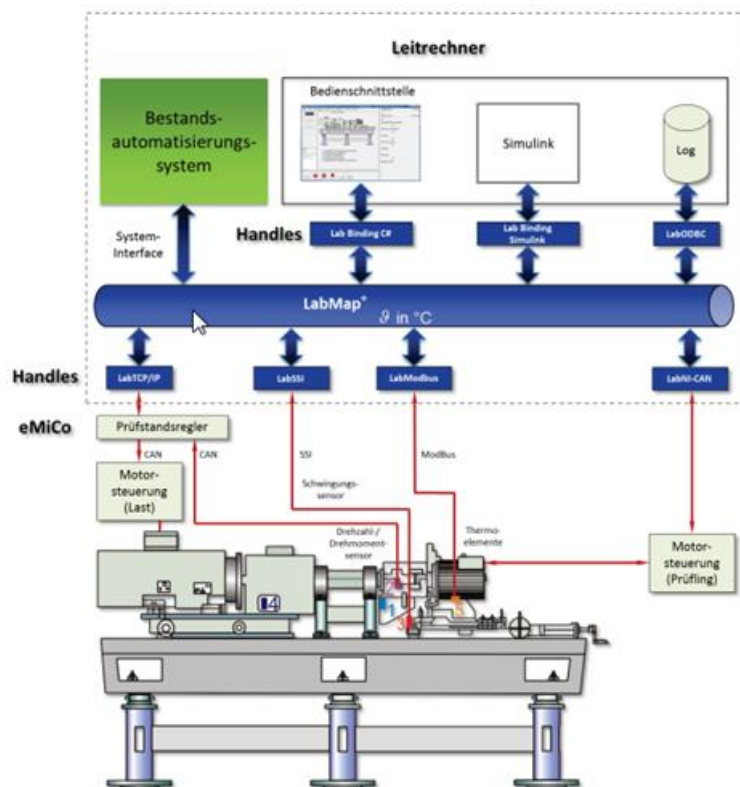


Bild 33: Logische Architektur einer Automatisierungsanwendung (Quelle: VDE/VDI Richtlinie 2657 „Middleware in der Automatisierungstechnik“)

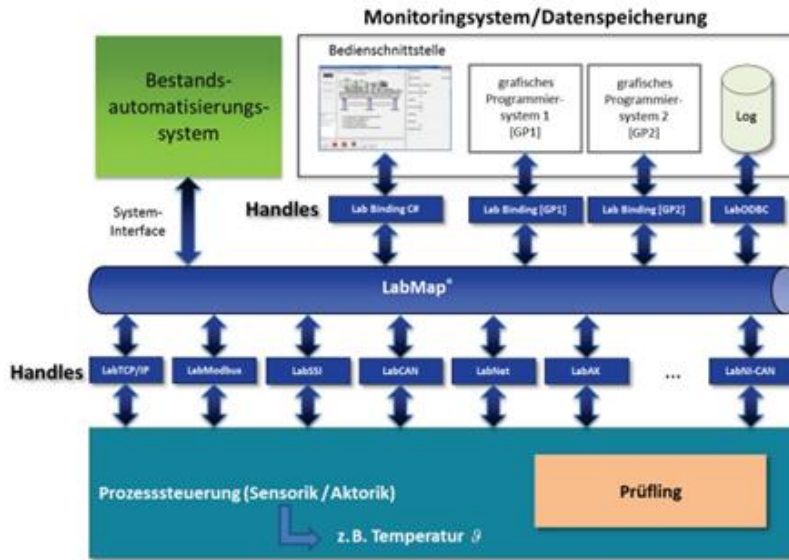


Bild 34: Technische Architektur der Middleware (Quelle: VDE/VDI Richtlinie 2657 „Middleware in der Automatisierungstechnik“)

## 8 Informationssicherheit

Wibu-Systems stellte den Projektpartnern für die Arbeiten in SecurePLUGandWORK die CodeMeter (CM)-Systemkomponenten und Entwicklungstools zur Verfügung. Zum Einsatz kommen die unterschiedlichen Hardware-Komponenten (Bild 35) je nach Verwendungszweck in einem Embedded System, einem Desktop oder in einem portablen Gerät, auf das die Selbstbeschreibung von Mehrspindelkopf, Spindel, Kugelgewindetrieb sowie Erweiterungssystem aufgebracht wird. Die geeignete CodeMeter-Hardware-Komponente wird steuerungsspezifisch ausgewählt, je nachdem, welche elektrische Schnittstelle für die Hardwarekomponente von der Steuerung zur Verfügung gestellt wird. Es war Aufgabe des Projekts herauszuarbeiten, welche Variante für welche(s) Komponente/Feldgerät eingesetzt werden kann.



Bild 35: Varianten der CodeMeter-HW/SW-Komponenten für den Einsatz an Maschinen oder in der IT-Security

Der höchste erzielbare Sicherheitslevel im Rahmen des Vorhabens erstreckt sich auf alle beteiligten Systeme, solange CodeMeter HW-Komponenten eingesetzt werden können. Die in Hardware eingebetteten Lizenzcontainer speichern geschützt vor Manipulation unter anderem die für das Ausrollen OPC-UA-Architektur wichtigen Zertifikate. Der Demonstrator 1 zeigt die konfigurierten, sicher von Ebene zu Ebene kommunizierenden Systemkomponenten. Sie werden in einer einheitlichen, hardwarebasierten OPC-UA-Sicherheitszone zusammengefasst. In bisher bekannten Demonstratoren für Plug and Play-Szenarien spielten Aspekte einer Schutzhardware keinerlei Rolle. Dagegen unterstützen in diesem Projekt unterschiedliche Bauformen eine Plug-and-Work-Integration auch bei bestehenden Infrastrukturen innerhalb der Maschinenebene. Für Feldgeräte oder Komponenten, in denen keine Hardware-Schnittstellen für die Aufnahme der physischen CodeMeter-Security-Module bestehen, wird per Virtualisierung ein Lizenzcontainer per Software in der Steuerungskomponente abgebildet. Eine Lizenz wird für den Fall in einem CMAct-Lizenzcontainer gespeichert (CMAct License). Im Folgenden beschreiben wir kurz die einzelnen Schritte, die in Bezug auf IT-Security im Projekt bearbeitet wurden.

### 8.1 Bedrohungsanalyse

Zunächst erarbeiteten die Partner eine Bedrohungsanalyse mit Ermittlung von Gefährdungspotenzialen für jeden Systemteilnehmer; sie umfasst

- Möglichkeiten zur Kommunikation,
- Speichermöglichkeit,

- Identifikation/Betriebsdaten/Konfigurationsdaten: hier waren insbesondere das Gefährdungspotenzial und der Schutzanspruch der zur Komponenten zugehörigen Konfigurationsdaten zu beschreiben.

Ergebnis war ein vierstufiges Sicherheitskonzept mit Methoden und Hürden für potenzielle Angreifer.

## **8.2 Sicherheitschip (Zertifikate, Kommunikation, Dongle, etc.)**

CodeMeter wird als Sicherheitskomponente über die gesamte SP&W-Infrastruktur eingesetzt. Sie verfügt als HW-Komponente (Dongle/Karte/ASIC) oder virtualisierte HW-Komponente (SW + verschlüsselter Datenfile) über einen oder mehrere Lizenzcontainer, in denen kryptographische (geheime) Schlüssel, Nutzungsrechte (Zähler, zeitliche Begrenzungen) und Zertifikate gespeichert werden. Die Speicher für kritische Informationen befinden sich in einem besonders geschützten Bereich eines Smartcard Chips, der nur unter sehr hohem technischen Aufwand angegriffen werden kann. Die Bauformen der HW-Ausführungen und deren Software-Aktivierungsvariante CmAct (CmActLicense) sind im Bild 35 dargestellt.

Alle diese Bauformen bzw. deren Software-Variante CmAct können je nach Kompatibilität bis zur untersten Steuerungsebene angewendet werden. Ist eine mechanische Komponente (KGT) rein passiv ohne elektrische Verbindung im Sinne von SP&W zu integrieren, so muss ein elektronischer Speicher (RFID/NFC-Chip) verbindungsfest hinzugefügt werden, damit ein weiterer, virtueller passiver Lizenzcontainer (ohne CPU) in Analogie zu den anderen HW-Komponenten zur Verfügung gestellt werden kann. Dadurch können auch die rein mechanischen Anlagenkomponenten in das Gesamtsicherheitskonzept von SP&W einbezogen werden.

## **8.3 Digitale Zertifikate**

Sie sind eine grundlegende Voraussetzung, damit ein Netzwerk vertrauenswürdig betrieben werden kann. Zertifikate und Nutzungsrechte werden für die Installation von Software benötigt, ferner spielen sie für den Zugang von Nutzern zu den einzelnen Komponenten eine wichtige Rolle. Ein Zertifikat ist Bestätigung der Identität eines Anwenders oder einer Komponente und damit so etwas wie sein Ausweis. Es enthält Angaben zur Identität sowie den „Stempel“ der zertifizierenden Stelle.

## **8.4 Zertifikate und der OPC-UA Standard**

Über die Anwendung des OPC UA-Standards kann eine sichere Netzwerk- und Software-Architektur installiert, flexibel angepasst oder ausgebaut werden. Das sichere Genieren und Verteilen von Zertifikaten auf die einzelnen SecurePLUGandWORK-Komponenten ist also die Grundvoraussetzung dafür, dass eine Sicherheitsarchitektur gemäß Best Practice umgesetzt werden kann und die erforderliche Robustheit gegen bekannte Bedrohungsszenarien implementiert wird. Der OPC UA-Standard legt in verschiedenen Sicherheitsprofilen fest, wie sich in der OPC UA-Client-Server-Architektur jede Client-Komponente mit jeder Server-Komponente interoperabel auf einen festgelegten Profil vernetzen kann.

### **8.4.1 Generieren und Ausrollen der Zertifikate mit Licence Central und Zertifizierungsinstanz**

Die Licence Central (LC, siehe Bild 36) ist eine Zentrale, die mit der zertifizierenden Stelle zusammenarbeitet. Über einen Master-Dongle werden Zertifikate verteilt. Die Zertifikate kön-

nen mittels der LC über die zunächst ungesicherte Kommunikation unter Anwendung von CM-Datenfiles in den entfernten LC-Container übertragen werden. Nur Autorisierte Benutzer (Administrator) können Generieren und Speicherung von Zertifikaten am Zielort (Container an den Endpunkten) auslösen.

Im Übrigen kann der Dongle auch als SW-Container realisiert werden; der Schlüssel liegt dann in einem gesicherten Bereich, man hat ohne entsprechendes Programm keinen Zugriff.

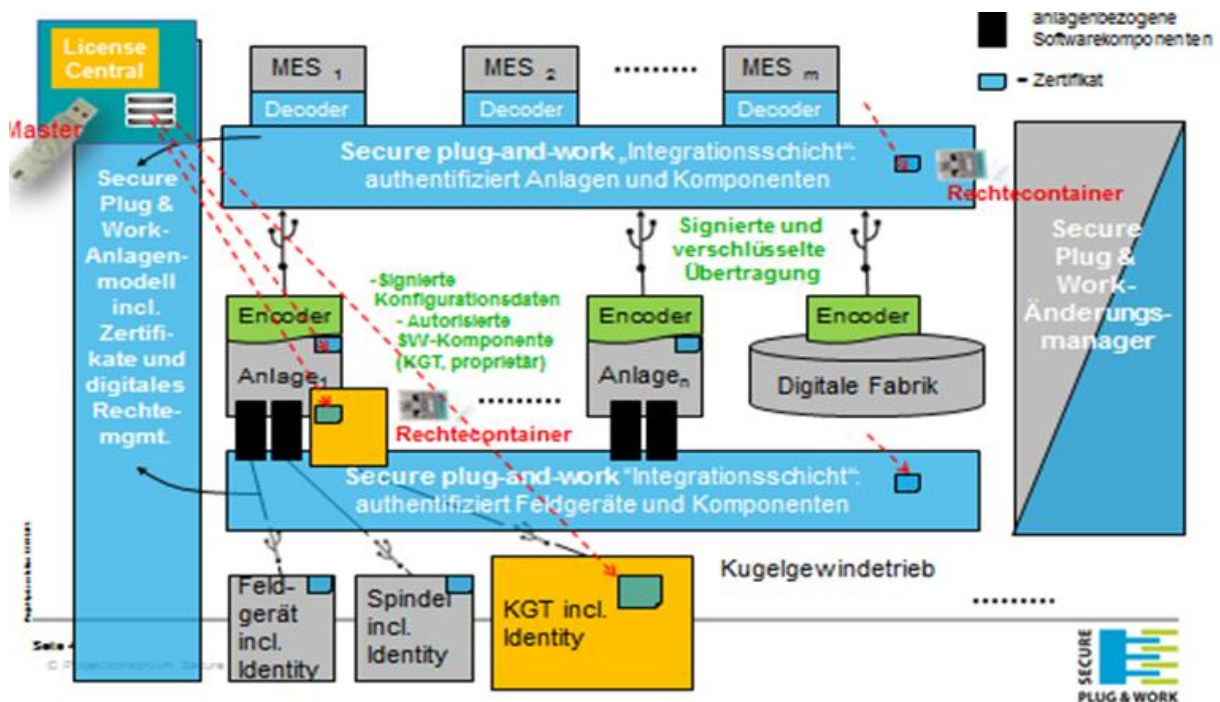


Bild 36: Licence Central in SecurePLUGandWORK

#### 8.4.2 Authentifizierung

Auf der Basis der Zertifikate, die mit CodeMeter sicher ausgerollt werden, findet eine gegenseitige Identifikation und Authentifizierung der Kommunikationsendpunkte sowie der kommunizierenden Anwendungen statt. Lediglich bei den passiven RFID-Tags ist nur eine einseitige Authentifizierung des Tags auf der Leserseite möglich. Über Passwort-Schutz ist allerdings ein autorisierter Zugriff auf verifizierbare Daten (Identitäten) abgesichert.

Jede Komponente mit Identität (auch mechanische Komponente) braucht Minispeicher für gesicherte Identität, z.B. einen RFID Chip.

#### 8.4.3 Vertraulichkeit der Daten

Zwischen den Endpunkten einer Kommunikationsbeziehung findet gemäß dem OPC UA-Standard eine vertrauliche Kommunikation statt. Dazu werden beim Herstellen einer Kommunikationsverbindung (Session) Schlüssel für einen „Trusted Channel“ generiert. Bei jeder Verbindung haben diese Schlüssel andere Werte. Lauschangriffe werden dadurch erschwert.

#### 8.4.4 Aufwand auf der Seite der Schutzkomponenten

CodeMeter ist ein aktives Schutzsystem (Smartcard Chip) und kann mittels der bereitgestellten Entwicklungsumgebungen alle schützenswerten IT-Komponenten mit Best Practice absichern. Überall dort, wo Steuerungskomponenten ISO-Standards und Industriestandards (Be-

triebssystem- und Programmentwicklungsplattformen) unterstützen, ist eine Integration der aktiven Schutzkomponenten möglich (Bild 37).

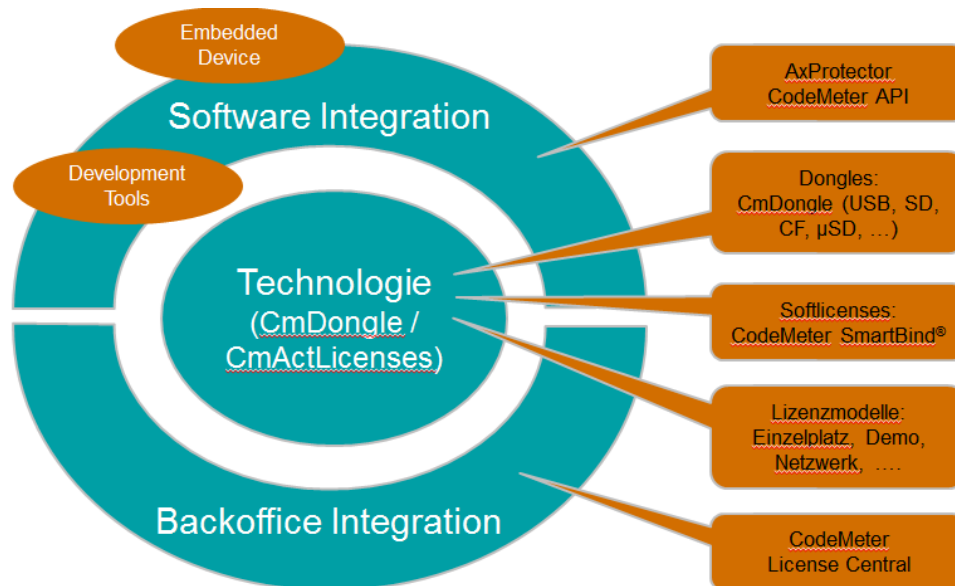


Bild 37: Optionen und Ausprägungen der CodeMeter-Technologie, die in SecurePLUGandWORK genutzt wurden

Die passiv ausgeführten Schutzkomponenten wie RFID-Tags, die batterieles über das Energy Harvesting Prinzip als Transponder arbeiten, können mit allerdings nur begrenzt zur Verfügung stehendem Speicherplatz (2 kB) für den elektronischen Schutz von Identitäten, Konfigurations- und Betriebsdaten vorteilhaft an mechanischen Baugruppen wie Spindeln oder Kugelgewindetriebe (Bild 38) aufgebracht werden. RFID-Tags sind dann kostengünstig, wenn andere elektronische Lösungen aus welchen Gründen auch immer (technisch schwierig oder aufwendig bzw. alternativ aktive Tags mit Batterien) vergleichsweise zu kostenaufwendig sind. Aus der Vielfalt der Tag-Varianten ist allerdings passgenau für den Einsatzfall diejenige Tag-Type auszuwählen, die den Einsatzbedingungen (Anforderungen an Robustheit) an der mechanischen Komponente am Einsatzort am besten entsprechen kann. Die Auswahl des Tags kann in iterativen Schritten ggf. am Demonstrator ermittelt werden. In jedem Fall sollten ISO-Standards für das Leseprotokoll am RF-Leser gelten.

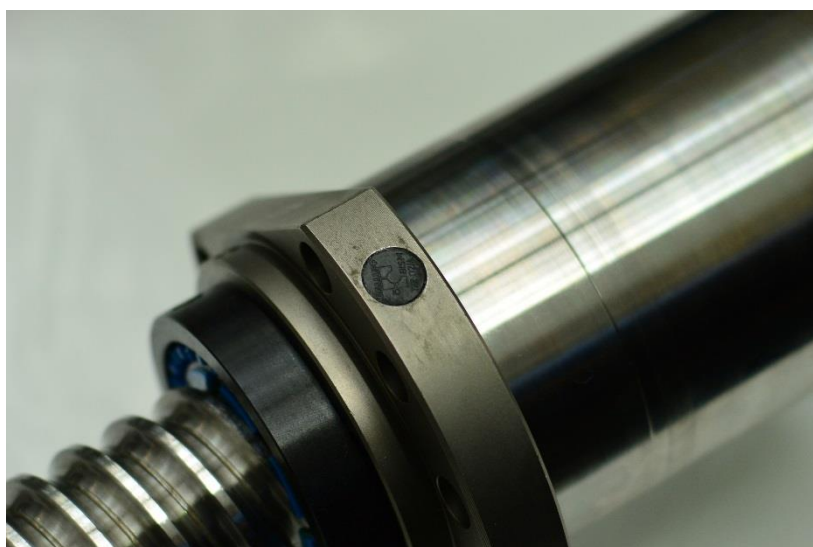


Bild 38: Kugelgewindetrieb mit aufgebrachtem RFID-Chip

### 8.4.5 Zusammenfassung der Schutzziele

Im folgenden sind die im Projekt verfolgten Schutzziele stichpunktartig aufgeführt:

1. Schutz vor Kopiermöglichkeit/Nachbau
2. Allgemeine Schutzziele
3. Implementieren von Daten- und Plagiatsschutz
4. Vertraulichkeit, Integrität und Authentizität der Daten
5. Schutz von geistigem Eigentum durch Kopierschutz, Schutz gegen Reverse-Engineering, Gewährleistung von Integrität und Authentizität von Software
6. Sichere Kommunikation über Internet basierende Protokolle (TCP/IP) und gesicherte Verteilung von Zertifikaten
7. Sichere Kommunikation über Feldbus

#### Ansatz: Security by Design

- a. Kopierschutz durch Verschlüsselung und sicheres Speichern der Schlüssel
- b. Know-how-Schutz durch Verschlüsselung
- c. Schutz der Konfigurations- und Betriebsdaten durch Verschlüsselung
- d. Funktionen modular freischalten und neue Geschäftsmodelle ermöglichen durch sichere Lizenzierung der Software
- e. Zugangsschutz: Authentifizierung der Komponenten und Benutzer durch Verschlüsselung und PKI-Verfahren
- f. Integritätsschutz durch Codesignaturen und Prüfung gegen Zertifikate
  - g. Sicheres Online-Management von Zertifikaten mit Licence Central in webbasierten Netzwerken auch bei ungeschützter Ende-zu-Ende-Kommunikation

### 8.4.6 Beispielablauf UseCase Spindel

Am Beispiel der Motorspindel, deren Konfigurationsdaten auf dem SecurePLUGandWORK-Adapter abgelegt werden und die dann in die Steuerung der Werkzeugmaschine eingelesen werden, ist der Security-Ansatz in den folgenden Stichpunkten aufgeführt.

- 1) Konfigurationsparameter auf Spindel schreiben
  - a. Daten signieren mit privatem Schlüssel
  - b. Klartextdaten und Signatur, sowie öffentlichen Schlüssel auf Spindel übertragen
- 2) Korrektheit der Daten prüfen/Integrität der Konfigurationsdaten
  - a. Controller auf Spindel
  - b. Spindel in Werkzeugmaschine
  - c. Spindel hat Daten und Signatur (verschlüsselter Hashwert, berechnet durch Hersteller), sowie öffentlichen Schlüssel
  - d. SPS (Prüfstand o.ä.) bekommt Befehl: lies Spindel Daten aus
  - e. SecurePLUGandWORK-Adapter auf Spindel überträgt Datei mit Konfigurationsdaten und Signatur
  - f. SPS hat Dongle und prüft Signatur → Integrität der Daten sichergestellt
- 3) Betriebsdaten verschlüsselt
  - a. Hersteller spielt öffentlichen Schlüssel vor Auslieferung auf Spindel (bzw. in Dongle)
  - b. SPS hat Betriebsdaten mitgeschrieben, Daten auf Spindel speichern (Achtung: Speicherüberlauf)
  - c. Daten zur Laufzeit auf Controller/SecurePLUGandWORK-Adapter übertragen



- 
- d. Zufallszahl (Session Key, Transport Key) auf Daten auf dem Controller berechnen
  - e. Controller verschlüsselt mit öffentlichem Schlüssel des Spindelherstellers oder des Spindelbetreibers
    - Variante A: Rollenbasierte Verschlüsselung auf Spindel, aufwändiger, weniger Netz-Traffic
    - Variante B: Kompletterschlüsselung und rollenbasierte Verarbeitung in SW, weniger aufwändig, mehr Netz-Traffic
- 4) Verschlüsselten Betriebsdaten werden ausgelesen (Spindelhersteller)
- a. Verschlüsselten Daten werden aus der Spindel ausgelesen
  - b. Daten werden mit Hilfe von privatem Schlüssel entschlüsselt (privater Schlüssel nur beim Hersteller).

## **9 Standards und Standardisierung**

### **9.1 Einheitlicher Datenaustauschstandard**

Der Datenaustausch wird mit Hilfe des XML-Formats AutomationML (IEC CDV 62714-1) unterstützt. AutomationML bietet die Möglichkeit, Produktionsanlagen und ihre Komponenten in verschiedenen Aspekten (Anlagenhierarchie, Geometrie, Kinematik, Ablaufplanung und Verhalten) einheitlich zu beschreiben. Dazu wird auf bestehende Standards zurückgegriffen, z.B. Collada für Geometriedaten, CAEX für Strukturdaten und PLCopen für Logikdaten. AutomationML trifft zusätzliche Einschränkungen für diese Formate und legt fest, wie diese verwendet und kombiniert werden.

Im Projekt stellt AutomationML die Grundlage für hersteller-unabhängige und tool-neutrale Modellierung der Komponenten und Systeme und die Beschreibung ihrer Fähigkeiten dar.

### **9.2 Einheitlicher Kommunikationsstandard**

#### **9.2.1 Allgemeines**

OPC UA (IEC 62541) ist ein Standard zur serviceorientierten Kommunikation in der Produktion, der mittlerweile eine hohe Verbreitung gefunden hat. OPC UA ist ein Kommunikationsprotokoll. Es stehen (ähnlich wie in AutomationML) Techniken zur Modellierung eines Informationsmodells zur Verfügung, etwa die Erzeugung von neuen Datentypen und komplexen Objekten. Das aktuelle Datenmodell (der ‚Addressraum‘) eines OPC UA-Servers kann von extern durch Mechanismen der Selbstbeschreibung erkundet werden. Dadurch, dass Objekte im Addressraum Methoden enthalten können, die von extern aufrufbar sind, lassen sich serviceorientierte Architekturen über OPC UA abbilden. Weiterhin können Änderungen an Objekten und Variablen von Klienten „abonniert“ werden, sodass sie Änderungen über einen Publish/Subscribe-Mechanismus informiert werden. Neben der binären Transportschicht ist eine XML-Serialisierung und Kommunikation über HTTP Teil des OPC UA Standards. Einige Sicherheitsmechanismen werden bereits unterstützt. Etwa die Verschlüsselung der Kommunikation mittels Public-Key Kryptographie und die Authentifizierung einer Identität über Zertifikate.

Im Projekt stellt OPC UA die Grundlage für sicheren Datenaustausch und serviceorientierte Kommunikation dar.

#### **9.2.2 IT-Sicherheit in OPC UA**

Die OPC UA-Spezifikationen [4] benennen mögliche Angriffsszenarien, wie z.B. das unerlaubte Eindringen in das System, die Verfälschung/Manipulation von Werten, Nachrichten und Anmeldedaten, das unerlaubte Abhören der Kommunikation oder die Kompromittierung von OPC UA-Servern durch eine Nachrichtenflut sowie explizite umsetzbare Gegenmaßnahmen. OPC UA implementiert ein Cyber Security Management System (CSMS) mit einem Sicherheitsmodell auf drei Ebenen.

Die Nutzer-Authentifizierung in OPC UA erfolgt mit einer Benutzer-Passwort-Kombination oder basierend auf einem Sicherheitsschlüssel (Security token). Hierfür wird der Einsatz von Zertifikaten vorgeschlagen, z.B. X.509v3, oder – wie oben beschrieben – über CodeMeter. Auch Server und Clients erhalten eine eigene Identität basierend auf einem solchen Zertifikat. Dabei spielt es keine Rolle, ob dies selbst-signierte oder von einer Zertifizierungsstelle (Trusted Authority) verifizierte Zertifikate sind. Während Local Discovery Server (LDS) Infor-

mationen über alle Server vorhalten, die bei ihnen registriert wurden, kann ein Global Discovery Server (GDS) [5] auch Discovery-Informationen über Applikationen in einem Unternehmen bereitstellen. Der GDS übernimmt auch das Zertifikatsmanagement, die Verteilung und das Management von Zertifikaten und realisiert Trust- und Revocation List. Dabei muss die Erstverteilung ebenso wie die Erneuerung von Zertifikaten unterstützt werden.

Für Nutzer oder Gruppen kann der Zugriff auf einen OPC UA-Server oder seine Knoten geregelt werden. Diese Autorisierungsmechanismen regeln den lesenden (read, historyRead), schreibenden (write, historyWrite) oder ausführenden Zugriff (execute) auf Daten. Wird der Zugriff verweigert, gibt es hierfür entsprechende vordefinierte Status-Codes, z.B.

„Bad\_UserAccessDenied“. So kann für Personen mit bestimmten Rollen, z.B. den Inbetriebnehmer, den Servicetechniker, oder den Anlagenbetreiber, der Zugriff auf wichtige Produktionsinformationen geregelt werden. Diese Mechanismen wurden in SecurePLUGandWORK genutzt (siehe Bild 39).

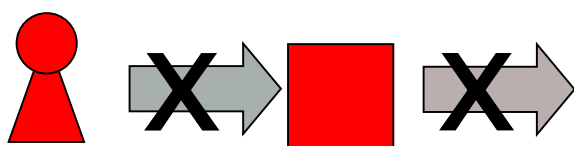


Bild 39: Zugriffsbeschränkungen für einen Nutzer (rot markiert, links) oder eine Anwendung (rot markiert, rechts)

Auch die Integrität der Daten muss sichergestellt werden: Ein Empfänger muss sicher sein, dass die Daten ohne jegliche Verfälschung bei ihm eintreffen – gerade so, wie sie der Sender verschickt hat. Dazu werden Daten ‚signiert‘. Hierfür werden symmetrische und asymmetrische Signaturen genutzt. Gleichzeitig enthält jede Request-/Response-Nachricht in OPC UA eindeutige Session IDs, Secure Channel IDs, Zeitstempel, Sequenznummern und Request IDs, auf Basis derer geprüft werden kann, ob Nachrichten verfälscht wurden.

Um die Vertraulichkeit der auf einem spezifischen Kommunikationskanal (SecureChannel) zwischen zwei Partnern übermittelten und verwalteten Informationen sicherzustellen, wird eine asymmetrische Verschlüsselung genutzt (Bild 40). Dies verhindert das ungewollte Abhören von Nachrichten.

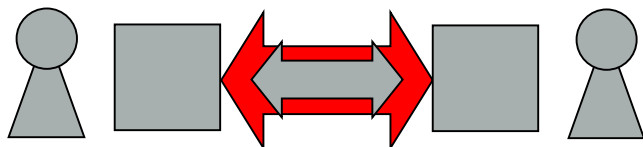


Bild 40: Abgesicherter Kommunikationskanal (SecureChannel, rot markiert) zwischen zwei Applikationen, betrieben durch zwei unterschiedliche Nutzer

Der Kompromittierung von OPC UA-Servern auf Grund von Nachrichtenfluten wirkt OPC UA entgegen, indem nur eine vordefinierte maximale Anzahl an Sessions von einem Server akzeptiert wird und gleichzeitig die Verfügbarkeit der Server auf Basis von Redundanzmechanismen sichergestellt wird.

Zusätzlich zur vorbeugenden Sicherung gilt es auch, den aktuellen Zustand, Aktionen und Ergebnisse als Audit-Spuren (audit trails) zu dokumentieren und nachvollziehen zu können, um im Nachgang einer Kommunikation die sog. Prüffähigkeit (Auditability) zu gewährleisten.

Daher werden mit OPC UA erfolgreiche und erfolglose Verbindungsversuche ebenso ausgezeichnet wie Konfigurationsänderungen, Zurückweisungen von Sessions, etc.. Anhand der Audit-Spuren kann beispielsweise das versuchte Eindringen von Angreifern frühzeitig erkannt [6] und klassifiziert [7] werden. Diese Mechanismen nutzt das IOSB beispielsweise innerhalb eines Frühwarnsystems für Cyber-Attacken auf IT-Systeme kritischer Infrastrukturen.

OPC UA bietet also eine Vielzahl von Möglichkeiten für die IT-Sicherheit; allerdings müssen sie bezogen auf den Anwendungsfall und mögliche Bedrohungen ausgewählt und umgesetzt werden.

### **9.3 Kombination von AutomationML und OPC UA**

#### **9.3.1 Companion Specification OPC UA for AutomationML**

Eine gemeinsame Arbeitsgruppe des AutomationML e.V. und der OPC Foundation unter Leitung von Frau Dr.-Ing. Miriam Schleipen des Fraunhofer IOSB befasst sich seit Beginn 2014 mit der Aufgabe, AutomationML und OPC UA zu vereinen. Als erstes Ergebnis der gemeinsamen Arbeitsgruppe wurde am 22. Februar 2016 die Companion Specification "AutomationML for OPC UA" veröffentlicht: <https://opcfoundation.org/developer-tools/specifications-unified-architecture/opc-unified-architecture-for-automationml/>.

Sie beschreibt Regeln, wie AutomationML-Modelle verketteter Produktionssysteme in OPC UA-Informationsmodelle überführt werden können, um beispielsweise aggregierende OPC UA-Server für verkettete Produktionssysteme zu realisieren.

SecurePLUGandWORK hat mit seinen Anwendungsfällen maßgeblich zur Erprobung des companion specification im Integrationsserver beigetragen.

#### **9.3.2 DIN SPEC 16592**

Als weiteres Ergebnis der DIN SPEC Arbeitsgruppe zum Thema "Combining OPC Unified Architecture and Automation Markup Language" wurde die DIN SPEC 16592 im Dezember 2016 veröffentlicht: <https://www.beuth.de/de/technische-regel/din-spec-16592/265597431>.

Die DIN SPEC 16592 beschreibt die Kombination von AutomationML Engineeringdaten mit OPC UA-Online-Informationen, wie z.B. Prozessdaten und Diagnoseinformationen. Sie erweitert und detailliert das ursprüngliche Mapping der Companion Specification und definiert darüber hinaus, wie OPC UA-Konfigurationsinformationen in ein AutomationML-Modell integriert können. Außerdem werden mögliche Anwendungsfälle für die Kombination beider Standards beschrieben, und Hilfestellung für die Einbindung weiterer externer Standards, z.B. CANopen und STEP, gegeben.

Im SecurePLUGandWORK-Assistenztool wurde das neuste Mapping von AutomationML und OPC UA Ende 2016 integriert.

### **9.4 AutomationML BPR DataVariable**

Die Vorstufen zur jetzigen DataVariable („aml-ua-variable“, ProcessVariable) wurden im Projekt im jeweiligen Entwicklungsstand genutzt und erprobt. Durch das Projekt kam der Wunsch auf, die aml-ua-variable allgemein für verschiedene Kommunikationsstandards und Protokolle zu nutzen. Dies wurde in Anwender- und Standardisierungsgremien diskutiert und ist in der jetzigen Best Practice Recommendation „DataVariable“ umgesetzt.

Rückmeldungen wurden mit in die aktuell erstellte Best Practice Recommendation „DataVariable“ zurückgespeist.

Der SecurePLUGandWORK-Integrationsserver baut seine Client-Subscriptions auf die unterlagerten OPC UA-Server der Maschinen und Komponenten automatisch an Hand der Beschreibung der entsprechenden DataVariables im AutomationML-Modell auf. Weiterhin erzeugt das SecurePLUGandWORK-Assistenztool die komplette Middleware-Konfigurations-Datei zur automatischen Konfiguration der eMiCo-Middleware für die Komponenten und Maschinen ebenfalls aus den DataVariables im AutomationML-Modell.

## 10 Anwendungsbeispiele

Wichtigste Nachweise, dass die entwickelten Konzepte, Technologien, SW-Werkzeuge etc. einsatzfähig sind und Industrie 4.0-Ziele unterstützen, sind die Demonstratoren. Die Demonstrationsszenarien sind in den folgenden Abschnitten beschrieben.

Die Komponentenslieferanten im Projekt entwickelten gemeinsam mit dem Werkzeugmaschinenhersteller MAG das Anwendungsszenario „Integration Komponente – Maschine“, z.B. Kugelgewindetrieb wird in Werkzeugmaschine integriert. Beteiligt daran sind Werkzeugmaschine, Spindel, Winkelbohrkopf und Kugelgewindetrieb.

Die Projektpartner, die eher die Integration von Modulen zu kompletten Anlagen oder Automatisierungslösungen verfolgen, entwickelten das Anwendungsszenario „Integration Maschine – Anlage“, z.B. Einzelmodule werden zu einer Industriewaschmaschine vereinigt. Beteiligt daran sind Waschmaschinen, Greifer und Werkzeugmagazin.

### 10.1 Werkzeugmaschine und ihre Komponenten

#### 10.1.1 Werkzeugmaschine

MAG stellte eine Maschine vom Typ E-Specht 600 (Bild 41) zur Verfügung, die die Arbeiten zur Integration von Komponenten in Maschinen demonstrieren konnte. Diese Maschine zeichnet sich dadurch aus, dass hydraulische Aktuatoren (z.B. Hydraulik-Zylinder, die elektrisch angesteuert werden) komplett durch elektromechanische ‚E-Aktuatoren‘ ersetzt sind. Diese kommen beim Werkzeughandling, im Rundtisch, den Spannsystemen, der Spindel und beim Palettenwechsler zum Einsatz. Im ursprünglichen Stand waren alle Einzelkomponenten klassisch und manuell in die Maschine zu integrieren. Im Rahmen des Projekts wurden zusätzlich zum Stand der Technik die neuen, mit SecurePLUGandWORK-Adaptoren versehenen, Komponenten angebaut. Die Werkzeugmaschinenkomponenten Werkzeugmagazin, Spindel, Winkelbohrkopf und Kugelgewindetrieb konnten damit bezüglich dem automatischen Auslesen von Eigenschaften der Komponenten und in Hinblick auf eine schnellere und fehlerärmere Inbetriebnahme erprobt werden.

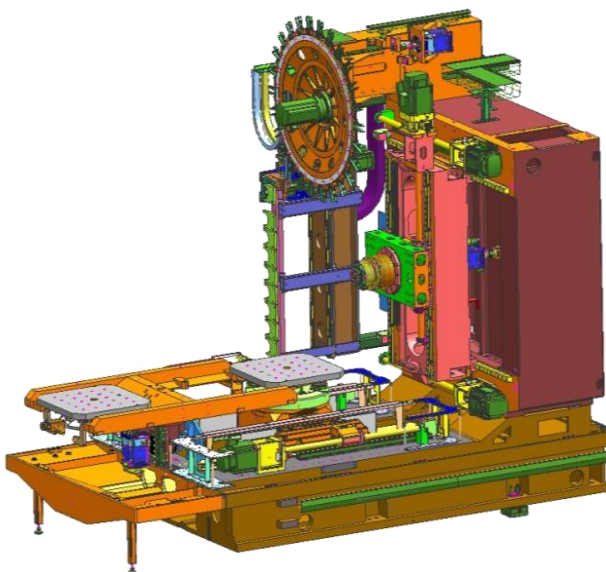


Bild 41: E-SPECHT 600 (vollelektrische Maschine)

## **10.1.2 Motorspindel**

### **10.1.2.1 Teilziele der Fa. Kessler**

Das Teilziel des Verbundprojektes für Kessler war es, die Inbetriebnahme der Kessler Produkte zu vereinfachen und damit zeitlich schneller zu erlauben. Dabei eingeschlossen sollte der Schutz der Maschinenkomponenten vor unzulässigen Betriebsbedingungen und der Aufzeichnung von Überschreitungen der vorausbestimmten Grenzen sein. Hierzu müssen die Betriebsbedingungen definiert werden und geeignete Messtechnik in die Komponenten integriert werden.

Zur Erreichung dieses Teilziels muss von Kessler eine geeignete Schnittstelle zu den Maschinenkomponenten definiert und entsprechende Datenformate und Dateninhalte festgelegt werden (physische und informelle Definition). Kessler verfolgt dabei das Ziel, seine Komponenten methodisch und in einem möglichst offenen, das heißt kostengünstigen Format zu beschreiben, um seine Kundenbasis zu erweitern. Hier ist die Zusammenarbeit mit MAG und dem wbk zur Gestaltung der Schnittstelle von besonderer Bedeutung. Zur Validierung der Forschungsergebnisse wurde Demonstrator gebaut. Als Ergebnis erwartet Kessler eine Standardisierung der neuen Komponentenschnittstelle, die auch in die entsprechenden DIN Gremien als Normungsvorschlag eingebracht werden soll.

Mit Anwendung der neuen Schnittstelle erwartet Kessler eine verkürzte Inbetriebnahmezeit beim Einbau der Maschinenkomponenten in die Werkzeugmaschinen und damit einen deutlichen Kundenvorteil. Der Schutz der Komponenten vor unzulässigen Betriebsbedingungen beugt einem Ausfall der Komponenten vor. Die Aufzeichnung der Überschreitung zulässiger Betriebsbedingungen bei nicht vermeidbaren Ereignissen schützt Kessler vor nicht zutreffenden Garantieleistungen. Nach Durchführung des Vorhabens verfügt Kessler über einen Demonstrator an dem weitere grundlegende Untersuchungen in Zusammenarbeit mit anderen Werkzeugmaschinenherstellern durchgeführt werden können.

### **10.1.2.2 Ressourcen für das Projekt**

Für dieses Projekt musste eine neue Spindel entwickelt werden, welche die SecurePLUGandWORK Eigenschaften bereitstellt. Diese Spindel wurde über die Neuentwicklungsprozesse der Firma Kessler ausgearbeitet und die kompletten vollen Entwicklungsprozesse eingebunden: Projektplanung, Auftragsmanagement, Konstruktion, Fertigung, Prüfstände Endkontrolle, Qualitätsmanagement und Versand. Es wurden aus den Entwicklungsabteilungen der Firma Kessler Ressourcen zur Bauraumuntersuchung für Elektronik Komponenten abgestellt sowie zusätzliche Messungen, die die thermische Belastung von Elektronikkomponenten in einer Motorspindel untersuchten.

### **10.1.2.3 Einbindung in die Unternehmens Strategien**

Dieses Projekt spiegelt die Unternehmens Strategien der Firma Kessler direkt wieder. Kessler ist einer der führenden Produzenten von Motorspindeln. Durch das Ausarbeiten von Lösungen, die in Zusammenhang mit dem IoT (Industrie 4.0) stehen, wird die Kessler auch diesen Status in der Zukunft behalten können. Mit PLUGandWORK-fähigen Komponenten werden für Kunden vielfältige Möglichkeiten eröffnet. Durch schnellere Tauschlösungen der Komponenten können Endkunden Kosten einsparen und somit werden diese Lösungen in Zukunft die herkömmlichen Komponenten ablösen.

#### 10.1.2.4 Technischer Stand zu Beginn des Projekts

Die Kompetenzfelder der Franz Kessler GmbH sind Motoren, Lagerungen, Werkzeugspann- und Lösetechnik, Medienzufuhr und Sensorik. Erweitert wird das Produktportfolio durch direktangetriebene Spindelschwenkköpfe und Werkstückachsen sowie Sonderlösungen nach Kundenvorstellung. Eine breite Auswahl an Standardmodulen steht dem Kunden zur Auswahl. Auf Wunsch werden auch Sonderkonstruktionen zusammen mit dem Kunden erarbeitet und realisiert. Abgerundet wird das Portfolio durch eine leistungsfähige Service- und Reparaturabteilung mit integriertem Ersatzteilservice. Wie die Firma Steinmeyer war auch die Franz Kessler GmbH schon vor Beginn des Projekts Lieferant von MAG und erwartete von der Kooperation in diesem Projekt signifikante Verbesserungen bei Inbetriebnahme bzw. der Konfiguration der Hauptspindeln in Zusammenspiel mit der kompletten Werkzeugmaschine. Die Problemstellung hierbei war, dass die Hauptspindeln der Firma Kessler noch keine standardisierten Schnittstellen zum Übertrag von Parametern und Konfigurationsdaten besaßen. Die Hauptspindeln sollten daher zukünftig mit einer Datenverarbeitungs- und Speichermöglichkeit ausgestattet werden.

Die Datenaufnahme für Inbetriebnahme- und Kompensationsdaten sollten in standardisierten Prüfständen erfolgen, welche die Komponenten in AutomationML charakterisieren. Die Schnittstelle aus dem Projekt SecurePLUGandWORK erlaubt die Anbindung an die übergeordnete Maschinensteuerung. Des Weiteren können Sensorinformationen, die während des Betriebs gesammelt werden, übertragen werden. Dies dient im Schaden- oder Servicefall einer besseren Fehlersuche.

Geplante Mehrwerte durch das Projekt das Projekt waren im Einzelnen:

- Erfüllen neuer Anforderungen von Systemintegratoren und Anlagenbetreibern, neues Verkaufsargument, exakte Dokumentation der gelieferten Komponente.
- Im Schadensfall einer Komponente wird durch den Einbau eines selbstbeschreibenden Ersatzteils die Inbetriebnahmezeit reduziert und damit die Stillstandszeit beim Kunden minimiert.
- Kessler übergibt die Maschinenkomponenten mit definierten Datensätzen an die Kunden (Maschinenhersteller). Diese können dann die Inbetriebnahme einfacher und schneller vornehmen (Kundenvorteil mit Auswirkung als Verkaufsargument).
- Überschreitungen von technischen Grenzwerten können vermieden werden oder zumindest aufgezeichnet werden. Hierdurch ist das Eintreten von Schäden vermieden bzw. falls sie dennoch eingetreten sind, sind sie zumindest nachweisbar keine Garantiefälle (Vermeidung von Kosten).
- Veröffentlichung (Produktkatalog) elektronischer Produktspezifikationen in standardisiertem Format (AutomationML).

#### 10.1.2.5 Erarbeiteter Demonstrator

MAG stellte eine Maschine vom Typ E-Specht 600 zur Verfügung, die die Arbeiten zur Integration von Komponenten in Maschinen demonstrieren konnte. In diese Maschine wird eine mit einer Selbstbeschreibung ausgerüstete Spindel eingebaut. Eine Spindel ist hinsichtlich der geometrischen Daten ein Unikat, auf das die Steuerung der Maschine angepasst werden muss, bzw. die Steuerung gleicht die Ungenauigkeiten der Spindel aus. Eine Veränderung der Spindel führt zu einer notwendigen Neuanpassung der Steuerung.



Es wird unterschieden zwischen serienspezifische Eigenschaften und Sacheigenschaften. Die Komponenten werden durch Prüfläufe und Verwendung abgenutzt, Anbauten können eventuell geschädigt werden. Die im Projekt genutzten Hardware-Komponenten konnten nach Ende des Projekts also nicht mehr anderweitig genutzt werden.

Allgemein zu demonstrieren waren

- Automatische Datenübertragung an die Werkzeugmaschine,
- Übermittlung von Messgrößen direkt aus der Spindel,
- Anbindung der Spindel an Prozessleitsysteme,
- Verkürzte und fehlerreduzierte Inbetriebnahme bei Neumaschinen und Maschinenerweiterungen,
- Reduktion der Stillstandszeit beim Kunden durch selbstbeschriebenes Ersatzteil,
- Betriebsdatenerfassung auf Motorspindel über deren Lebensdauer,
- Reduzierung des Verdrahtungsaufwands.

Speziell auf die Nutzung der Spindel wurde folgendes gezeigt:

- Übermittlung von Zuständen der Spindel,
- Warnungen bei Überlast,
- Warnung bei Verschleiß,
- Reduktion der Herstellungskosten,
- Reduktion der Stillstandszeit beim Kunden,
- Garantieverlängerung durch Betriebsdatenerfassung,

Benötigte Software-/Hardware-Komponenten.

- Motorspindel,
- SecurePLUGandWORK-Adapter,
- SPS und NC-Steuerung,
- OPC UA Integrationsserver,
- OPC UA-Client,
- Profinet-Schnittstelle,
- SecurePLUGandWORK fähiges Maschinen-Steuerungsprogramm.

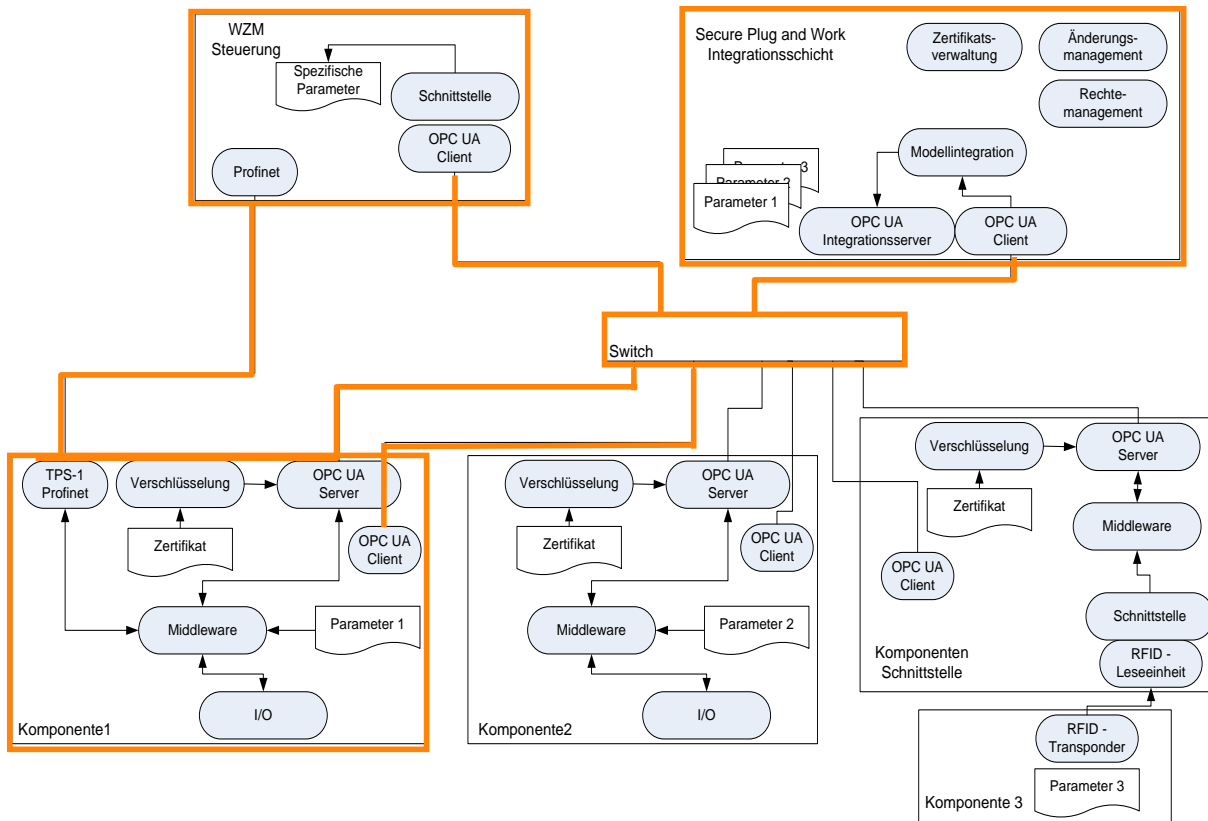


Bild 42: Verknüpfung zwischen Komponenten und Werkzeugmaschine

### 10.1.2.6 Projektergebnisse

Es wurde untersucht, inwiefern es möglich ist, in der Spindel einen möglichst sicheren Ort zur Unterbringung einer Elektronik zu schaffen. Dazu wurde eine Bauraumuntersuchung im Bereich des Wickelkopfs des Motors durchgeführt, um insbesondere die thermischen Verhältnisse in diesem Bereich zu identifizieren. Innerhalb der gegebenen Platzverhältnisse wurden drei Probanden (siehe Bild 43) quasi als Platzhalter für eine spätere Elektronik definiert und mit Temperatursensoren ausgestattet. Die Probanden wurden im Kühlgehäuse im Bereich des Motorwickelkopfs eingebaut und vergossen (siehe Bild 44).



Bild 43: Probanden

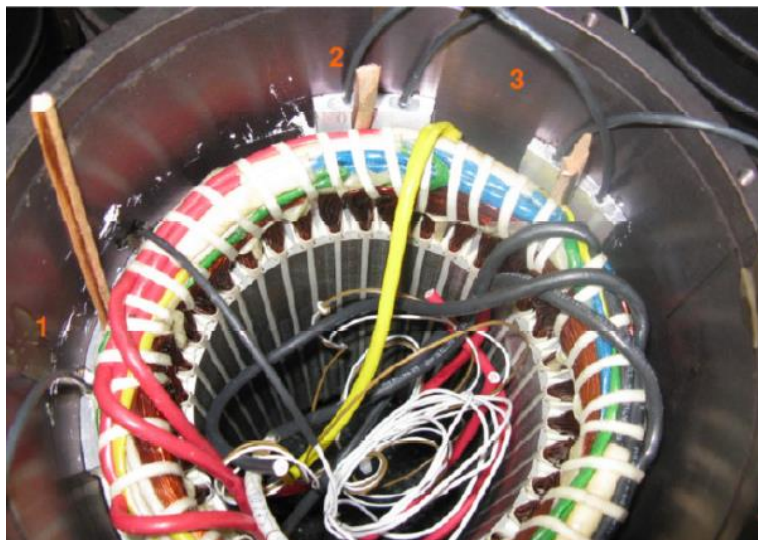


Bild 44: Eingebaute Probanden

Danach wurde der Stator mittels Frequenzumrichter bestromt und dadurch erwärmt. Hierbei wurde darauf geachtet, dass die Temperatur im Bereich der Wicklung bis kurz unterhalb der thermischen Dauerfestigkeitsgrenze der Isolierstoffklasse F (155 °C) geführt wurde. Der Stator wurde dabei wassergekühlt. Die sich ergebenden Temperaturen entsprechen dem thermisch eingeschwungenen Zustand (Bild 45).

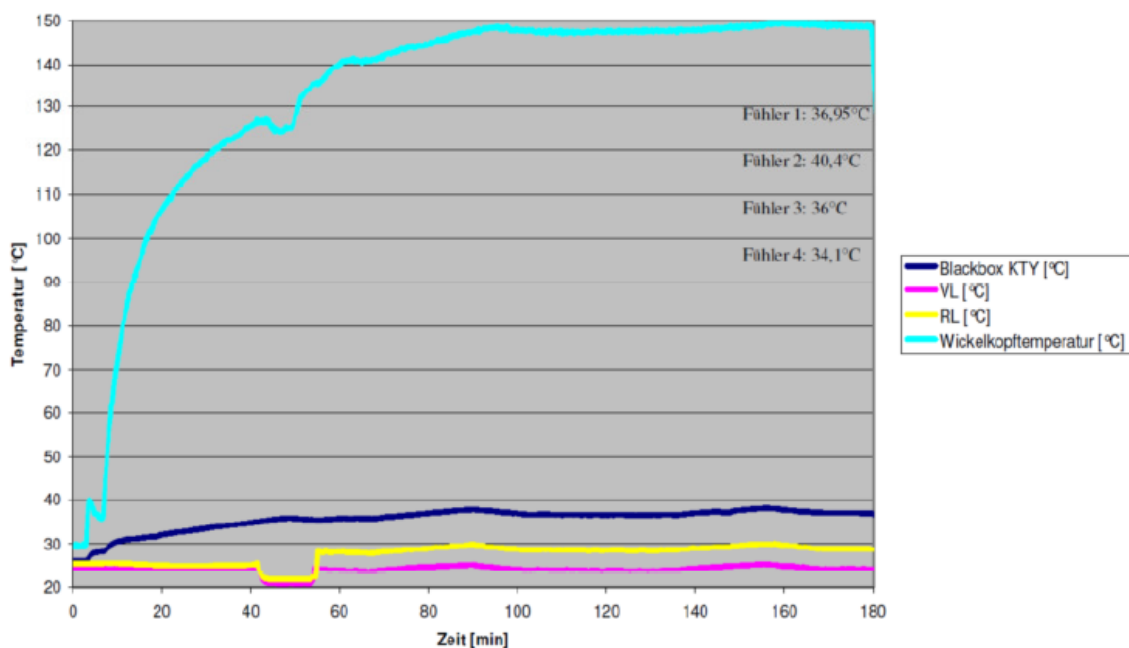


Bild 45: Temperaturverlauf bis Beharrung

Aus thermischen Gesichtspunkten sind der Einbau und der sichere Betrieb einer Elektronik im Bereich des Wickelkopfs des Motors in den aufgezeigten Größenverhältnissen möglich. Es ist darauf zu achten, dass ein derartiges Element thermisch gut an das Kühlgehäuse angebunden ist.

Für den ersten Test der Verbindung von Spindel-Sensorik und BeagleBone war die Produktion eines Spindel-Prototyps erforderlich. Von besonderer Relevanz war im Vorfeld die Auswahl eines geeigneten Sensors zur Temperaturmessung, welcher die folgenden Anforderungen zu erfüllen hatten:

- Kompakte Baugröße kleiner 5 x 2 x 2mm (LBH)
- Messbereich von -20 bis +150°C
- Messtoleranz +/- 1°C

Die Wahl fiel auf den Sensor PT1000, welcher die Anforderungen vollumfänglich erfüllt. Er ist durch die folgende Mess-Kennlinie gekennzeichnet (Bild 46):

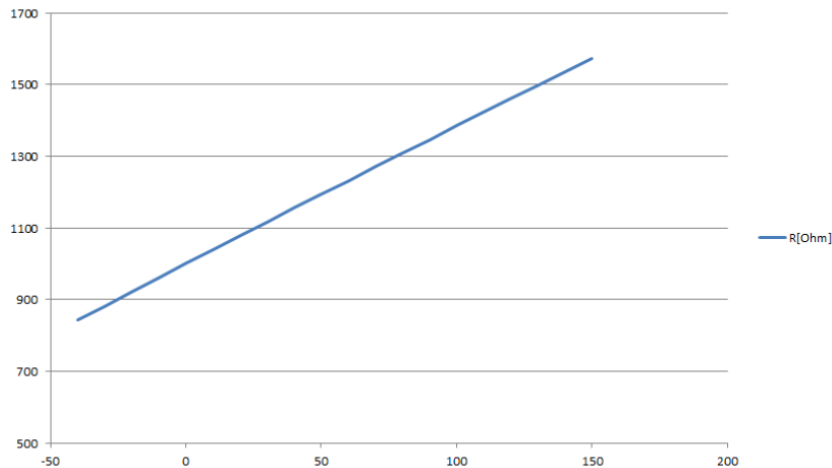


Bild 46: PT1000 Temperaturkurve

Nach Auswahl des geeigneten Sensors konnte die Produktion des Prototyps erfolgen. Um Kosten zu sparen, wurde ein defekter Spindel-Rückläufer des Typs „Konzern-Spindel“ als Grundlage und Bauteil-Quelle verwendet. Diese Spindel wurde zunächst vollständig zerlegt und anschließend gereinigt. Nicht weiterzuverwenden war das Statorpaket, daher wurde dieses neu produziert und anschließend jeweils ein Temperatursensor in die drei Wicklungsphasen eingebracht, in Bild 47 sind die Zuleitungen im Vordergrund zu erkennen.



Bild 47: zerlegte Spindel (links) und Statorpaket inklusive Sensoren (rechts)

Im nachfolgenden Arbeitsschritt wurde das Gehäuse aufgeschumpft und der Wickelkopf mit den sechs Zuleitungen für Strom sowie den sechs für die Temperatursensoren mit Vergussmasse vergossen. In den finalen Schritten wurde die Spindel wieder vollständig zusammengesetzt (Bild 48).

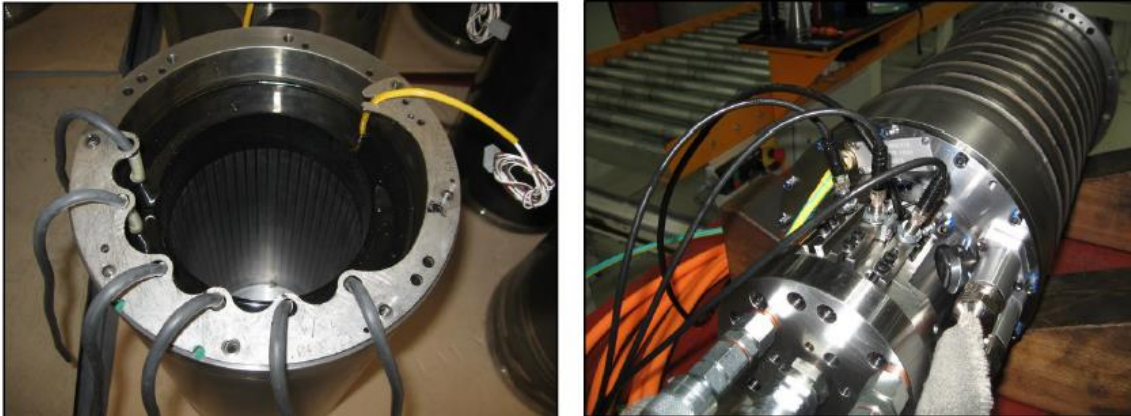


Bild 48: Spindel im Verguss (links) und fertig montierter Prototyp (rechts)

Als nächstes war es erforderlich, sich mit dem Hersteller MAG, welcher für das Projekt die Werkzeugmaschine bereitstellte, genau abzustimmen und eine geeignete Spindel für den späteren Demonstrator zu bestimmen und gegebenenfalls Änderungen vorzunehmen. Basierend auf ersten Informationen von MAG bezüglich der angestrebten Abmessungen der Spindel wurde aus den mehr als 2.000 Spindeln und Varianten, die Kessler im Programm hat, die geeignetste und passendste ausgewählt. MAG nutzt in der Konstruktion 3D-CAD-Modelle, die ausgewählte Spindel lag allerdings noch als 2D-Zeichnung vor. Daher wurde zunächst ein einfaches Hüllenmodell der Spindelgeometrie (Bild 49) erstellt und MAG zur Verfügung gestellt.

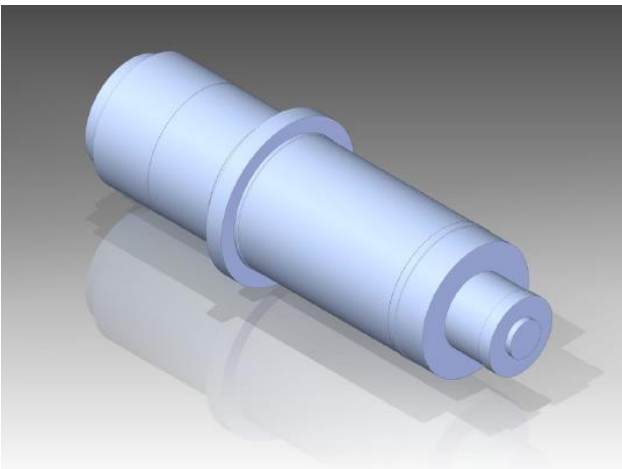


Bild 49: Einfaches Hüllenmodell der Spindel

Dieses Modell erwies sich für die konkrete Änderungskonstruktion als zu wenig detailliert für die Anforderungen von MAG, daher wurden in einer Änderungsrunde sämtliche Konstruktionsdetails wie Anschluss-Stecker, Flansch, Gewindebohrungen zur Befestigung etc. in das 3D-Modell integriert bzw. detaillierter ausgearbeitet (Bild 50).

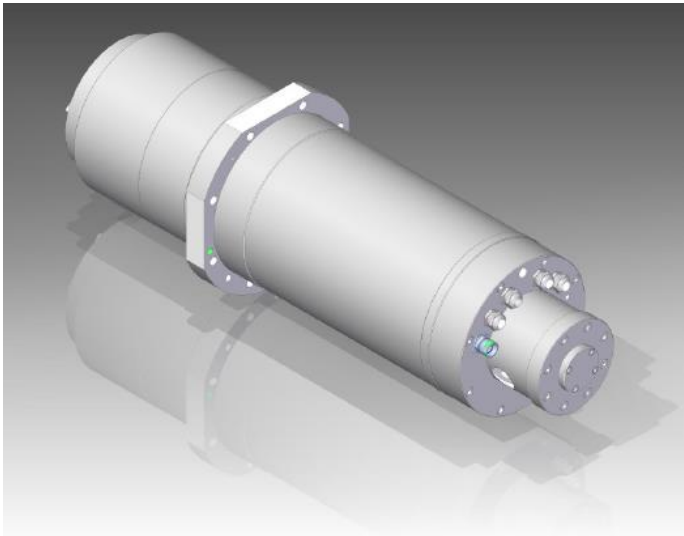


Bild 50: Detailliertes Hüllenmodell

Zur Kommunikation zwischen den BeagleBones der einzelnen Komponenten (Spindel Kessler, Spindel CORCOM) und der Werkzeugmaschine musste ein gemeinsamer Datensatz definiert werden. Für die Schnittstelle Kessler-MAG wurde der Grundstein während eines ganztägigen Abstimmungsgesprächs gelegt, im Laufe des Projekts wurde der Datensatz immer weiter überarbeitet und verfeinert. Stand heute besteht der Datensatz aus 84 Konstanten oder Variablen, aufgeteilt in die Bereiche „Initialisierungs-Daten“, „Betriebsdaten“ und „Sensordaten“. Neben der Bezeichnung, der zu verwendenden Maßeinheit und einem eindeutigen Bezeichner zur Verwendung im OPC UA Modell, sind für jeden Parameter Datentyp, Speicherbedarf und Zugriffsrechte definiert. Außerdem ist festgelegt, in welchem Format die einzelnen Parameter von den beteiligten Firmen mit Inhalten befüllt werden.

Nach Lieferung des BBB zu Kessler wurde dieser in Betrieb genommen. Hierfür wurde ein Stecker Netzteil für die 24V Spannungsversorgung an den BBB angeschlossen. Zur Inbetriebnahme wurde ein Aufbau direkt am PC realisiert und die für die Erstinbetriebnahme benötigten Einstellungen wie das aktuelle Datum und die Uhrzeit über Putty eingestellt, um den internen OPC UA Server verbinden zu können. Für weitere Tests wie das Anbringen der Sensorik an den BBB wurde ein weiteres Anschlusskästchen erstellt, an dem man auch die Spannungsversorgung der Sensorik abgreifen konnte. Um die PT 1000 Sensoren direkt auf einen Referenzwert zu skalieren wurden hierfür Umsetzer-Module der Firma IFM beschafft.

Da nun die Sensorik alle über M12 Schraub-Steck-Verbinder verfügten, wurden an das Anschlussgehäuse Kabel mit M12 Schraub-Steck-Verbindern angebracht. Folglich wurde ein Tischaufbau realisiert (siehe Bild 51).



Bild 51: Kessler Versuchsaufbau

Mit diesem Test Aufbau wurde die Kommunikation zwischen Sensor und OPC UA-Client getestet. Nach den prototypischen Versuchen 2015 wurde im Jahr 2016 eine Spindel mit den für das Projekt benötigten Sensoren bei der Firma Kessler angefertigt. Es wurde eine Spindel vom Typ SMS 112.84-695.481 gewählt.

In diese Spindel wurde die gewählte Sensorik verbaut, die zur Kommunikation über den SecurePLUGandWORK-Adapter gewählt wurde. Zum einen wurde ein Balluff-Sensor vom Typ BAW M18ME-UAC48BBP01,5-GS04-003 verwendet. Dieser Sensor misst einen Weg von maximal 4,8 mm mit einem Spannungsbereich von 0 – 10V. Der Sensor wird wie der BBB auch mit 24 V versorgt. Für die weitere Sensorik wurden PT 1000 Temperaturwiderstände in der Spindel verbaut.

Drei dieser Sensoren wurden in den Bauraum zwischen Wickelkopf und Kühlgehäuse eingebracht, um Rückschlüsse auf den Temperaturverlauf einer Spindel zu ziehen. Zwei weitere Sensoren sind an den Standard Einbaupositionen zur Überwachung der Lagertemperatur und der Wickelkopfperatur verbaut.

Um die Server-Client-Schnittstelle zu testen, wurde das Programm UAExpert auf einem Rechner bei Kessler installiert. Mit diesem Programm ist es möglich über den OPC UA Server, der sich auf dem BBB befindet, zu kommunizieren. Die Verbindung wurde direkt über eine Ethernet-Leitung zum BBB hergestellt. Über die Verbindung wurde das Analogsignal des Balluff-Sensors übertragen und anschließend auf Plausibilität geprüft. Die Anbindung aller analogen Sensoren wurde bei den Integrationstreffen in Eislingen und Karlsruhe bearbeitet und bereitgestellt. Hierbei wurde ausschließlich der oben beschriebene Versuchsaufbau verwendet.

Im Jahr 2017 war die technische Realisierung im Hause Kessler abgeschlossen. Es musste nur noch der Demonstrator für die Abschlussdemonstration bei MAG in Eislingen vorbereitet werden. Dieser Demonstrator bestand aus der produzierten SecurePLUGandWORK-Spindel und dem SecurePLUGandWORK-Adapter der Firma Kessler. Für den Demonstrator wurden die Sensorabgänge der Spindel mit Industriesteckern versehen, welche sich einfach an den Adapter anschließen ließen. Für den Abschlusstermin wurde eine Demonstratormaschine bei der Firma MAG in Eislingen erstellt. Hierbei wurden alle Komponenten des Projekts mit einer Werkzeugmaschine verbunden und die Funktionalität der SecurePLUGandWORK-Adapter

vorgeführt. Es wurden das Tauschen einer Corcom-Spindel und einer Kessler-Spindel (Bild 52), der Einbau eines Romai-Mehrspindelkopfes, das Anmelden eines Werkzeugwechslers und der Tausch eines Kugelgewindetribs an der Werkzeugmaschine gezeigt. Des Weiteren stellten alle Projektpartner bei dieser Veranstaltung ihre Ergebnisse und die im Projekt ausgearbeiteten Demonstratoren vor.

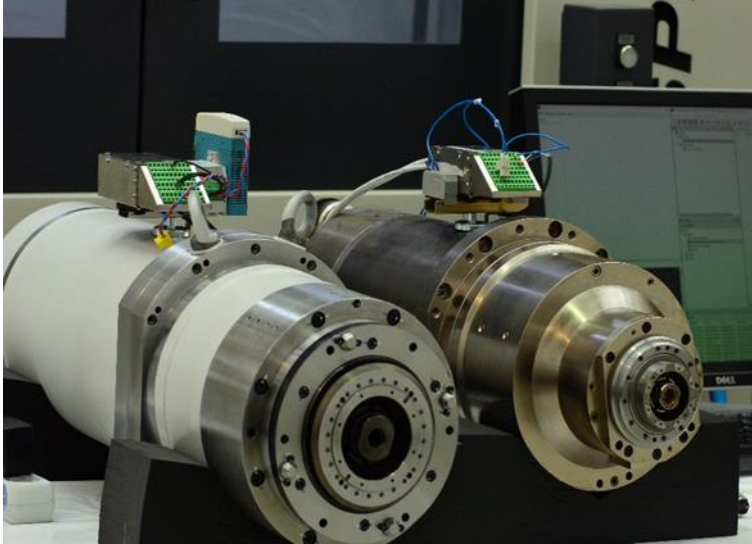


Bild 52: zu tauschende Spindeln zweier unterschiedlicher Hersteller mit SecurePLUGandWORK-Adapttern

#### 10.1.2.7 Nutzen für die Firma Kessler

Die ausgearbeiteten Ergebnisse werden der Firma Kessler zur Weiterentwicklung der eigenen Produkte im Rahmen des IoT-Umfelds (Industrie 4.0) von großem Nutzen sein. Das Erarbeiten eines aussagekräftigen Spindel-Modells in AutomationML muss noch in den zuständigen Gremien des VDW und VDMA behandelt werden. Für die Hersteller von Motorspindeln käme die Einigung auf ein Standardmodell einer Revolution gleich.

Der entwickelte SecurePLUGandWORK-Adapter kann für weitere Tests zur PLUGandWORK-Funktionalität bei KESSLER weiter verwendet werden. Der Einbau des Adapters in ein Produkt ist allerdings aufgrund der nicht industriefähigen Elektronikkomponente Beaglebone Black und des nicht passenden Formfaktors nicht realisierbar. Die Schnittstellen des Geräts sind aber für die Firma KESSLER von großem Wert zur Weiterentwicklung aller Produkte.

#### 10.1.3 Winkelbohrkopf

ROMAI hat einen Winkelbohrkopf mit integrierten Sensoren entwickelt (Bild 53) und diesen mit einem I4.0 tauglichen SecurePLUGandWORK-Adapter ausgestattet.

Im Rahmen des Projektes SecurePLUGandWORK wurde die sichere Integration in eine Werkzeugmaschine erprobt. Eindeutige Identifikationsdaten, Geometrie IST-Daten sowie Kenngrößen für den Betrieb können mittels einem entwickelten AML-Modell an einen OPC-UA-Server übergeben werden und mit Hilfe der Profi-Bus Schnittstelle an die Werkzeugmaschine bzw. an die Steuerung übergeben werden und ermöglichen eine sichere, verkürzte Inbetriebnahme.



Laufende Betriebsdaten werden erfasst und können von dem Adapter oder der Steuerung ausgewertet werden.

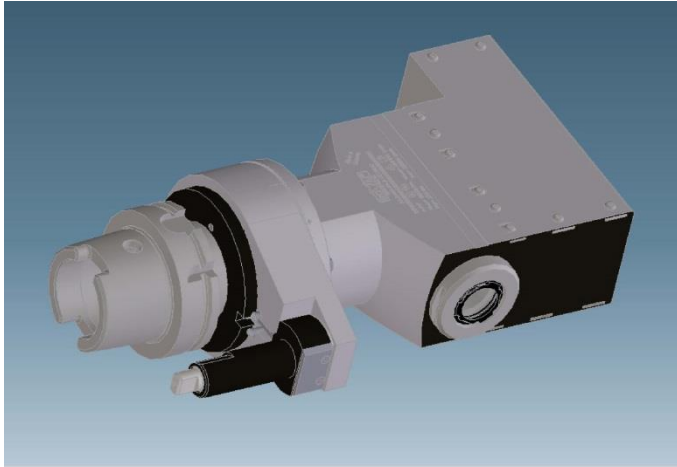


Bild 53: Prinzipbild eines Winkelbohrkopfes

Ausgehend von der Motivation

- Verkürzen der Inbetriebnahme (Daten on Board – PLUGandWORK),
- Sichere Inbetriebnahme (Daten ohne Übertragungsfehler),
- Betriebsdaten Logger mit gesicherten Daten für Wartung und Reparatur,
- Integrierte Sicherheitstechnologie

ergibt sich mit dieser Umsetzung ein mehrfacher Nutzen, der in der Zukunft zu abgewandelten Geschäftsmodellen führen kann.

- Mehrwert durch Just in Time Wartung,
- optionale Garantieverlängerung durch Belastungsprofil,
- Mehrwert durch Abgrenzung Garantie / Kulanz / Reparatur,
- I4.0-Anbindung an MES Systeme,

Die benötigten SW-/Hardware-Komponenten sind getestet und müssen in weiteren Umsetzungen fortentwickelt werden:

- Beaglebone Black mit Licensing Dongle,
- AML Model mit UA Server / Client,
- 24 V / Netzwerk.

Die grobe Architektur zur Verbindung von Winkelbohrkopf und Maschine entspricht derjenigen in Bild 42.

Insbesondere durch die Applikation des SecurePLUGandWORK-Adapters in das weitere Lieferspektrum der Fa. ROMAI, das auch größere 2-Achs-Vorsatzköpfe mit integrierter Motorspindel für Groß-Bearbeitungsmaschinen umfasst, kann hier zur Standortsicherung ein weiterer Ausbau der produktbegleitenden Dienstleistungen im Bereich der I4.0-Anwendungen erfolgen (Bild 54).



Bild 54: Beispiel eines 2-Achs-Vorsatzkopfes

#### 10.1.4 Werkzeugmagazin

Ein sogenanntes Erweiterungssystem bestehend aus Werkzeugmagazin und Greifersystem konnte ebenfalls an der Werkzeugmaschine erprobt werden. Das Erweiterungssystem ist ebenfalls in der Lage, SecurePLUGandWORK Funktionen zu erfüllen. Beim Inbetriebnahmeprozess werden die Daten des Werkzeugmagazins vom SecurePLUGandWORK-Adapter an die Steuerung der Werkzeugmaschine übermittelt, womit das Steuerungsprogramm und die Werkzeugverwaltung konfiguriert werden.

##### Motivation

- Verkürzte und fehlerreduzierte Inbetriebnahme bei Neumaschinen und Maschinenerweiterungen,
- Reduktion der Stillstandszeit beim Kunden durch selbstbeschreibende Komponente,
- Betriebsdatenerfassung auf Werkzeugmagazin über dessen Lebensdauer.

##### Nutzung/Geschäftsmodell

- Reduktion der Herstellungskosten,
- Reduktion der Stillstandszeit beim Kunden durch schnelleren Umbau,
- Garantieverlängerung durch Betriebsdatenerfassung.

##### Benötigte SW-/Hardware-Komponenten

- Werkzeugmagazin,
- SecurePLUGandWORK-Adapter,
- SPS und NC-Steuerung,
- OPC UA-Integrationsserver,
- OPC UA-Client,
- SecurePLUGandWORK-fähiges Maschinensteuerungsprogramm.

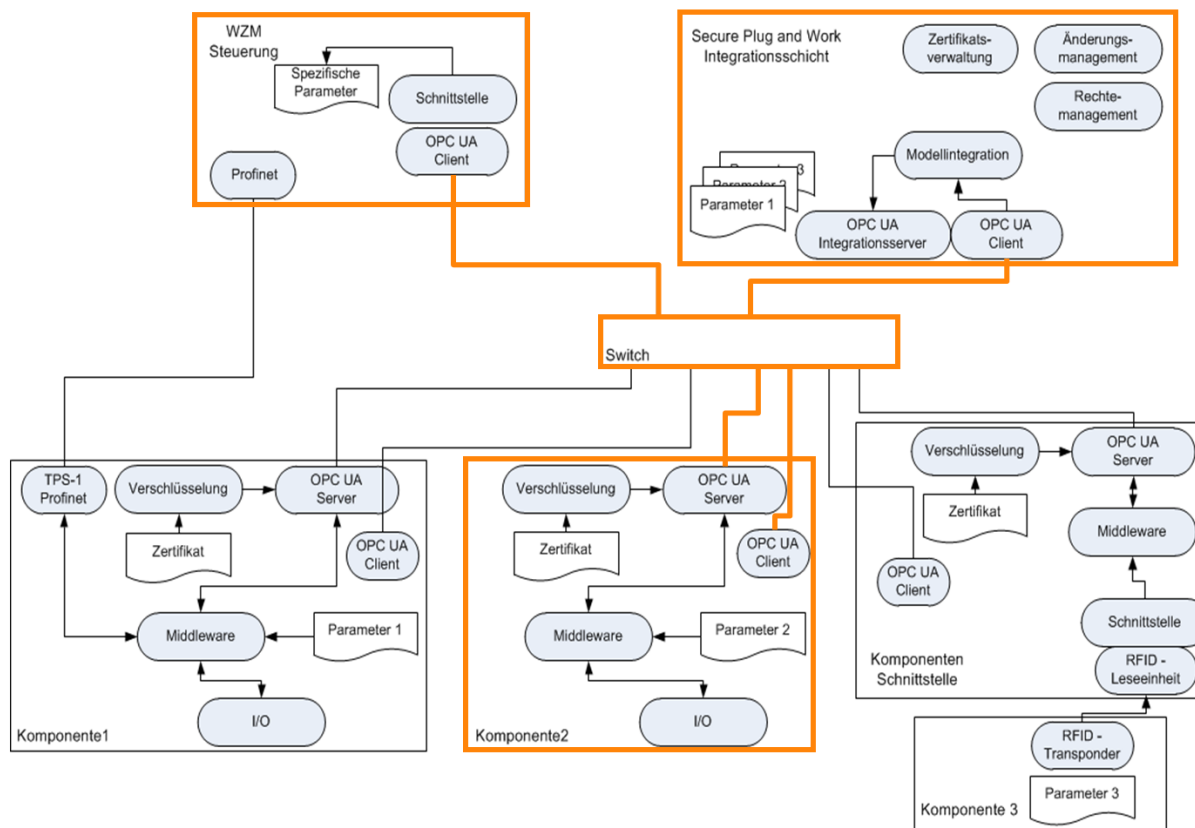


Bild 55: Architekturbild Werkzeugmagazin

### 10.1.5 Kugelgewindetrieb

Der Kugelgewindetrieb (KGT) dient in den Vorschubachsen der Werkzeugmaschine dazu, die rotatorische Bewegung eines elektrischen Motors in eine lineare Vorschubbewegung umzuwandeln. Die Vorschubbewegung hat einen maßgeblichen Einfluss auf die Produktivität einer Werkzeugmaschine sowie auf die Qualität der bearbeiteten Werkstücke. Daraus ergeben sich hohe funktionale Anforderungen an die Komponenten der Vorschubachse und somit auch an den KGT. Zur Gewährleistung der geforderten Eigenschaften ist bei Montage und Inbetriebnahme derzeit ein hoher manueller Aufwand notwendig. Dieser Aufwand besteht unter anderem darin, Komponentendaten aus Datenblättern, die in Papierform vorliegen, in die Maschinensteuerung einzugeben. Es kann auch notwendig sein, diese Daten durch Messungen an der eingebauten Komponente zu ergänzen.

In diesem Projekt wurde der KGT um eine PLUGandWORK-Funktionalität erweitert, indem alle relevanten Daten direkt auf der Komponente gespeichert und elektronisch an die Maschinensteuerung übertragen werden. Dabei soll sowohl für den Komponentenhersteller als auch für seine Kunden ein Nutzen erzielt werden. Zunächst muss die Liste der relevanten Daten erarbeitet werden und in einer strukturierten Beschreibungssprache abgebildet werden. Zur Speicherung und Übertragung der Daten müssen geeignete Technologien und Einbaorte definiert werden. Um die Komponentendaten zu erfassen wird ein Prüfstand konzipiert und aufgebaut.

#### 10.1.5.1 Auswahl der relevanten Komponentendaten

Die Merkmale und Daten, die einen individuellen Kugelgewindetrieb charakterisieren, entstehen in verschiedenen Phasen des Komponentenlebenszyklus:

- Konfigurationsdaten bestimmen schon vor der Herstellung den Typ des KGT.
- In der Fertigung entstehen stochastische Abweichungen der mechanischen Eigenschaften innerhalb eines Toleranzbereichs, die in einer nachgelagerten Prüfung gemessen werden können (Bild 56).
- Bei der Montage durch den Maschinenhersteller oder den Maschinenanwender wird der Kugelgewindetrieb einer individuellen Maschine und einer Bewegungsachse zugewiesen.
- Bei der Inbetriebnahme können weitere Eigenschaften des KGT im eingebauten Zustand ermittelt werden (Berücksichtigung des Einflusses der umgebenden Komponenten).

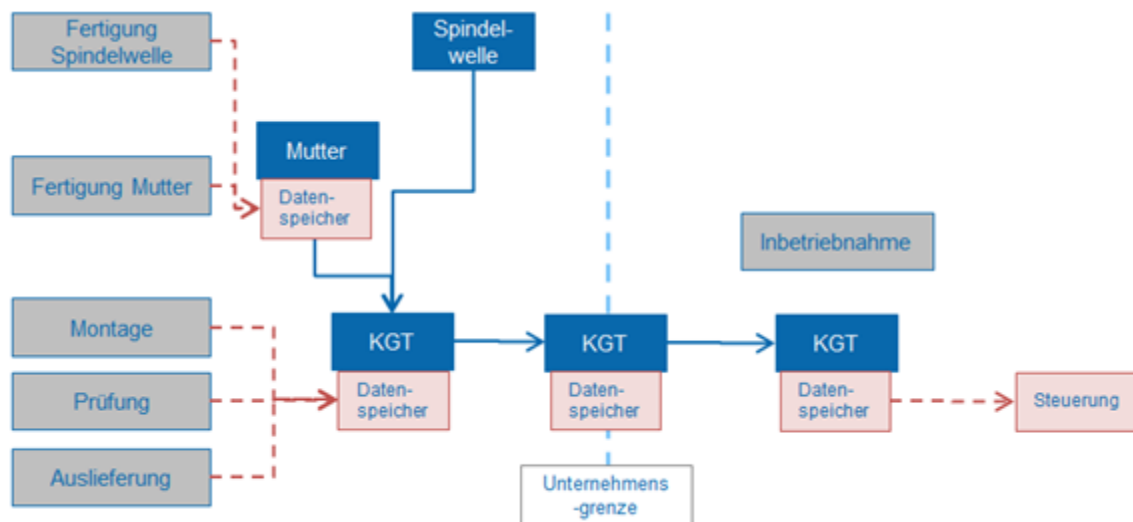


Bild 56: Datenentstehung und Übertragung im Lebenszyklus eines Kugelgewindetriebs

Im Betrieb können Daten wie die Betriebsdauer und die auftretenden Lasten aufgenommen werden, die Aussagen über den Verschleiß und den späteren Ausfall des KGT erlauben.

In Abstimmung zwischen wbk, Steinmeyer und MAG wurde ermittelt, welche Eigenschaften von Kugelgewindetriebs erfasst werden können. Die Merkmale können verschiedene Zwecke erfüllen:

- Eindeutige Identifikation der individuellen Komponente,
- Prüfung der Eignung der Komponente für den Einsatzzweck (Kompatibilität und Leistungseigenschaften),
- Unterstützung der Maschinenhersteller oder –anwender beim Ersteinbau und Austausch,
- Betrachtung durch den Komponentenhersteller der Einsatzbedingungen bei Reklamation oder Überholung.

Die ausgewählten Merkmale sind in der nachfolgenden Tabelle aufgeführt. Diese werden wie in den anderen Anwendungsbeispielen dieses Projekts im Format AutomationML strukturiert abgespeichert.

Merkmalsname	Einheit
<b>Typidentifikation</b>	
Hersteller	String
Artikelnummer (Maschinenhersteller, hier MAG)	String
Zeichnungsnummer (Komponentenhersteller, hier Steinmeyer)	String

<b>Einzelteilidentifikation</b>	
Seriennummer (Komponentenhersteller, hier Steinmeyer)	Integer
Herstelldatum des KGT	Datum
letzte Überholung des KGT	Datum
<b>Konfigurationsdaten</b>	
KGT Nenndurchmesser (D)	mm
KGT Steigung	mm
max. möglicher Verfahrensweg	mm
Steifigkeit (nominal)	N/ $\mu\text{m}$
Maximal zulässige Drehzahl	U/min
Maximal zulässige Beschleunigung	m/s <sup>2</sup>
Maximal zulässiger Ruck	m/s <sup>3</sup>
Maximal zulässige Vorschubkraft	N
<b>Messdaten</b>	
Reibmomentverlauf (Anfang, Ende, Abstand, n Reibmomente)	mm, mm, mm, Nm
Steigungsverlauf (Anfang, Ende, Abstand, n Abweichungen)	mm, mm, mm, $\mu\text{m}$
<b>Betriebsdaten</b>	
Anzahl der Umdrehungen (=Laufweg)	Integer
Maximal aufgetretenes Drehmoment	Nm
Ersteinsatzdatum	Datum
max. Leerlaufmoment	Zeitstempel, Nm
min. Leerlaufmoment	Zeitstempel, Nm
Produktionszeit der Maschine	h

### 10.1.5.2 Datenspeicherung und Übertragung

Für die Komponentendaten musste eine geeignete Technologie zur Speicherung und Übertragung gefunden werden. Durch den Wunsch, den Datenträger direkt auf der Komponente zu befestigen, ergeben sich besondere Herausforderungen:

- Beschränkter Bauraum,
- Mechanische Belastung durch hohe Beschleunigungen,
- Medienbeständigkeit (Öl, Kühlschmiermittel).

Ausgewählt wurden RFID-Datenträger, die sich bei ähnlichen Einsatzbedingungen zur Identifikation von Werkzeugen in Bearbeitungszentren bewährt haben. Hierbei ist zu beachten, dass der im Kugelgewindetrieb eingesetzte Stahl durch eine abschirmende Wirkung die Datenübertragung stören kann. Es wurden aber eine Einbaulage und ein System aus RFID-Datenträger und Lesegerät gefunden, die eine zuverlässige Datenübertragung erlauben. Der Datenträger ist zylindrisch, mit einem Durchmesser von 10 mm und einer Höhe von 4,5 mm. Dieser kann in Stahlbauteile eingesenkt werden, so dass er bündig mit der Stahloberfläche abschließt. Um die Zugänglichkeit zu gewährleisten, ohne die Funktion des KGT zu beeinträchtigen, wurde eine Einbaulage im Flansch der KGT-Mutter gewählt, in einer radial eingebrachten Bohrung (Bild 57). Der Datenträger erlaubt das Schreiben und Lesen von 2.000 Bytes.

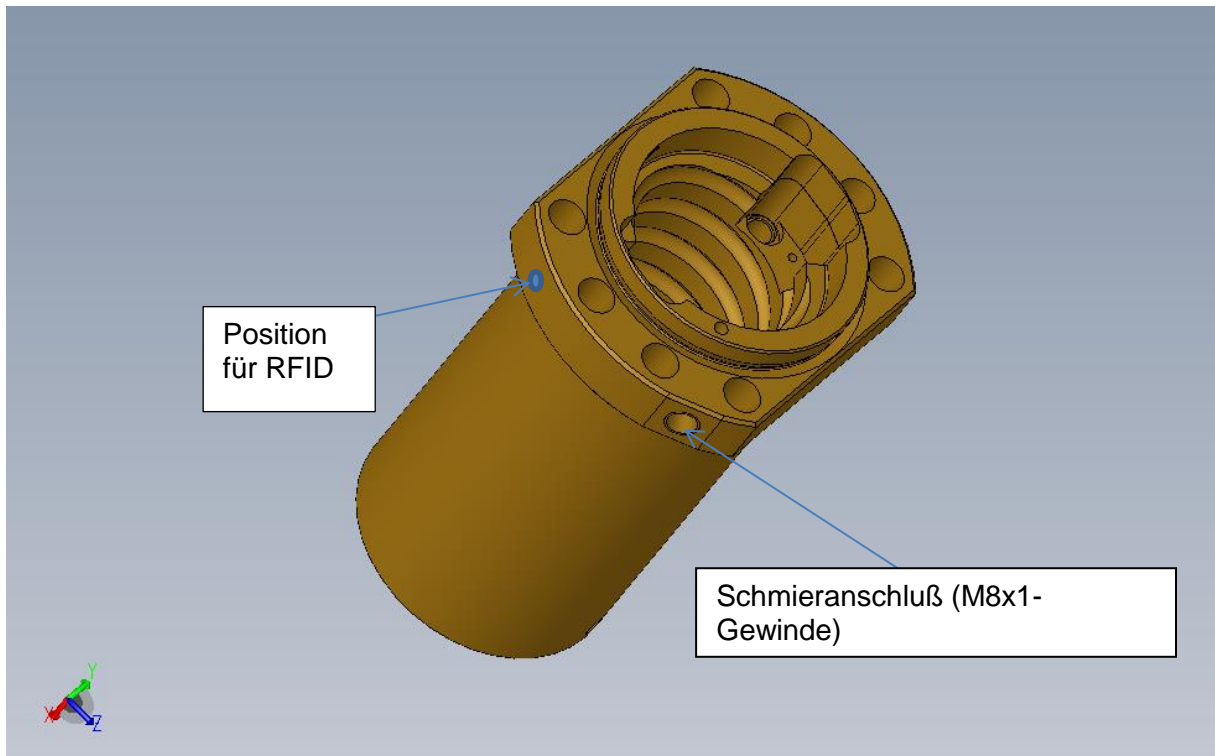


Bild 57: Position des RFID-Datenträgers in der KGT-Mutter

Zur Anbindung des Auswertegeräts und die weitere Informationsübertragung wird der Einplatinenrechner BeagleBone verwendet, der auch im SecurePLUGandWORK-Adapter zum Einsatz kommt. Am wbk wurde ein Programm erstellt, um die Komponentendaten von Kugelgewindetrieben auf RFID-Datenträger zu schreiben und zu lesen. Um die begrenzte Speicherkapazität des Datenträgers besser auszunutzen, werden die Daten aus der Beschreibung in AutomationML in ein kompakteres Textformat umgewandelt. Beim Lesen wird wieder eine vollwertige AutomationML-Datei aus den gespeicherten Daten erzeugt.

Auf dem BeagleBone werden die Daten durch einen OPC UA-Server im Netzwerk freigegeben. So können diese im Integrationsserver aggregiert werden. Der Kommunikationsablauf für das Anwendungsbeispiel KGT ist in Bild 58 zu sehen, während Bild 59 die Einbindung in den übergeordneten Anwendungsfall Werkzeugmaschine darstellt.

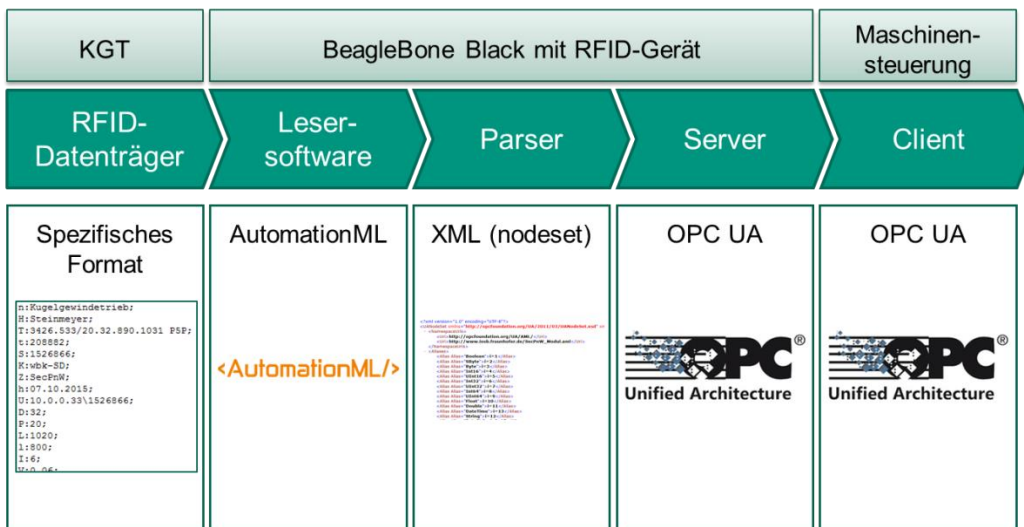


Bild 58: Kommunikationsablauf im Anwendungsbeispiel KGT

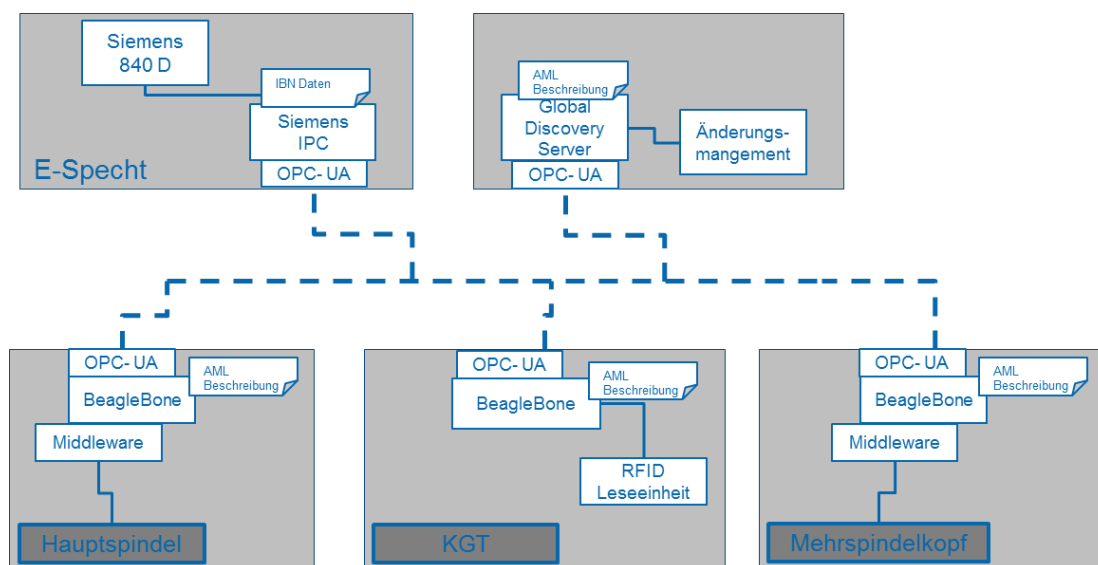


Bild 59: Einordnung des KGT im Anwendungsfall Werkzeugmaschine

Vor dem mechanischen Einbau eines neuen KGT werden zunächst die Daten mithilfe eines RFID-Lesegeräts auf den BeagleBone geladen. Der BeagleBone wird im lokalen Netzwerk mit dem Integrationsserver verbunden und signalisiert per OPC UA an die Steuerung der Werkzeugmaschine, dass neue KGT-Daten geladen werden können. Die Steuerung ruft die Daten ab, um eine Kompensationstabelle automatisch anzulegen. Mithilfe dieser Tabelle können die Steigungsfehler des KGT bei der Abarbeitung von NC-Programmen berücksichtigt werden. Beim Ausbau eines KGTs können Betriebsdaten aus der Steuerung wieder an den BeagleBone gesendet und auf den RFID-Datenträger geschrieben werden.

Der BeagleBone wird im Anwendungsbeispiel KGT nur beim Ein- und Ausbau des KGT benötigt und kann sukzessiv für mehrere Maschinen verwendet werden, während die BeagleBones für die anderen Komponenten (Werkzeugmagazin, Hauptspindel, Winkelbohrkopf) in der Maschine verbleiben.

### 10.1.5.3 KGT Prüfstand

Zur Messung der individuellen (Instanz-spezifischen) Eigenschaften von Kugelgewindetrieben wurde am wbk ein Prüfstand aufgebaut. Der Verlauf des Reibmoments sowie die Positionsabweichung des Kugelgewindetriebs sollen über die Länge des Gewindes gemessen werden. Beide Untersuchungen erfolgen am selben Prüfstand, wobei eine kurze Umbauphase zum Wechsel des Prüfmodus notwendig ist.

Der Prüfstand ist auf einem steifen Bett aus Stahl aufgebaut (Bild 60). Die Spindel des Kugelgewindetriebs wird an einem Ende mit einem Spindellager aufgenommen (Festlager) und am anderen Ende mit einem als Loslager fungierenden Rillenkugellager. Der Kugelgewindetrieb wird über eine Balgkupplung durch einen Synchronmotor angetrieben. Ein Drehgeber erfasst den Winkel des Kugelgewindetriebs. Daraus lässt sich die ideale Bewegung der Mutter berechnen (ohne Steigungsfehler). Zur Bestimmung der Steigungsfehler wird die Mutter des KGT an einen linear beweglichen Schlitten befestigt (Bild 61). Die Position des Schlittens wird durch ein direktes Messsystem in Form eines Glasmaßstabs erfasst. Somit können für jede angefahrte Position die Messwerte des Glasmaßstabs mit den Positionen verglichen werden, die sich bei idealer Steigung aus dem durch den Drehgeber gemessenen Winkel

ergeben. Die Differenz entspricht der Wegabweichung infolge Steigungsabweichungen (Bild 62).

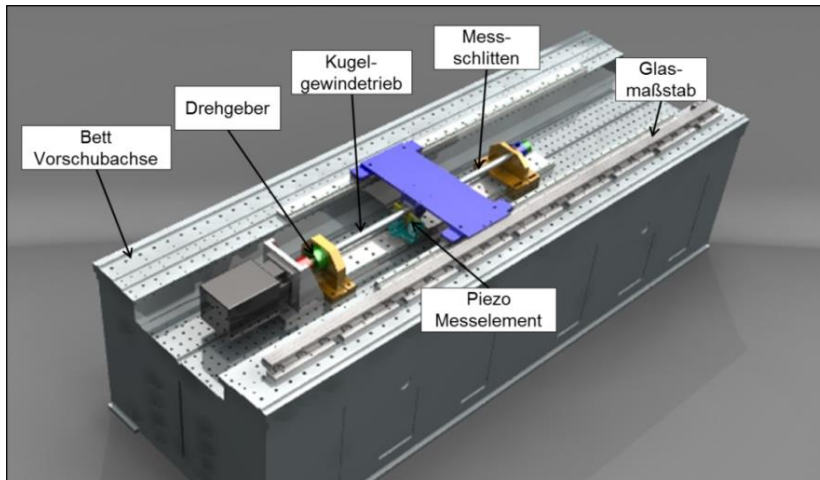


Bild 60: Aufbau des Prüfstands zur Vermessung von Kugelgewindetrieben

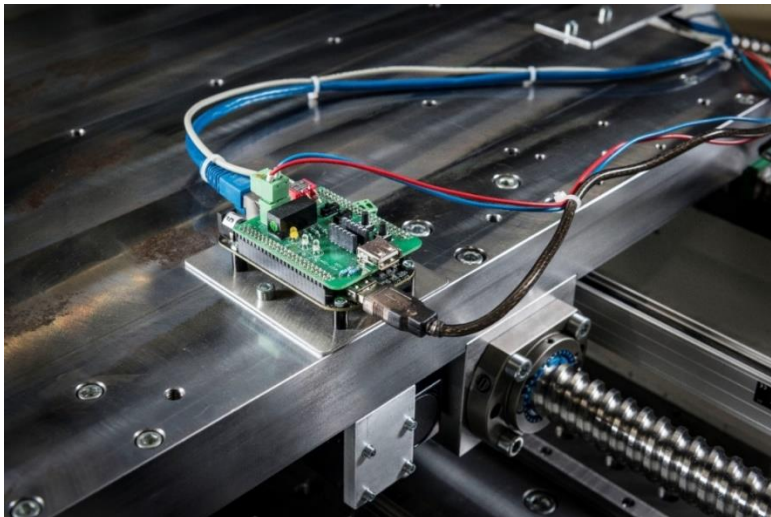


Bild 61: Einplatinenrechner BeagleBone und Prüfstands Aufbau zur Messung der Wegabweichungen

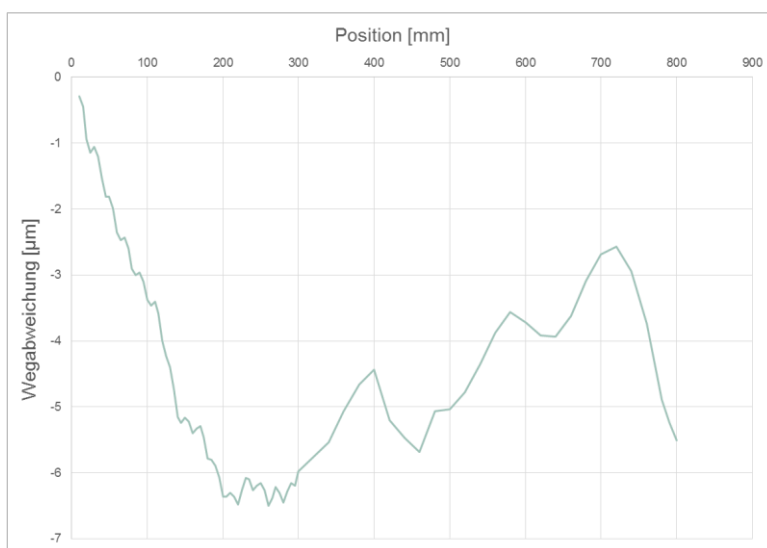


Bild 62: Wegabweichungen für einen im Projekt untersuchten KGT



Um das Reibmoment zu messen, wird die Mutter vom Hauptschlitten gelöst und mit einem kleineren Schlitten verbunden (Bild 63). Eine mit einem Gewinde versehene Halbschale greift in das Gewinde der KGT-Spindel ein, somit bewegt sich der Messschlitten bei einer Drehung der KGT-Spindel synchron mit der Mutter. Am Flansch der KGT-Mutter wird ein Hebel angebracht, dessen Ende eine lineare Kraft auf einen piezoelektrischen Kraftsensor aufbringt. So kann während der Verfahrbewegung das Reibmoment bestimmt werden (Bild 64).



Bild 63: Aufbau zur Messung des Reibmoments

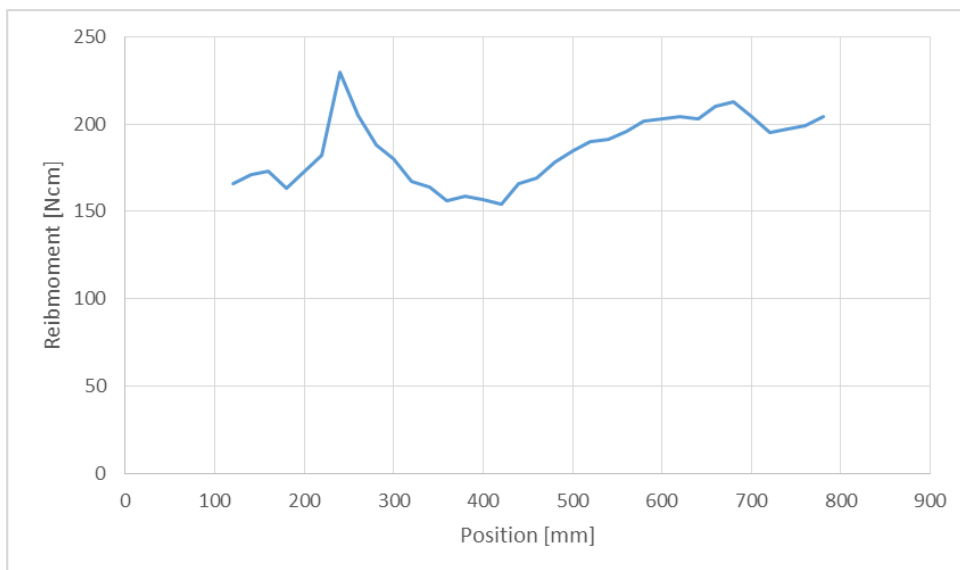


Bild 64: Verlauf des Reibmoments für einen im Projekt untersuchten Kugelgewindetrieb

## 10.2 Industrielle Waschanlagen zur Teilereinigung

Entsprechend ihrer Möglichkeiten stellte die Fa. MOC Danner Module seiner Dolphin-Serie (Bild 65) als Testumgebung und Demonstrator zur Verfügung, die über SecurePLUGandWORK-Mechanismen miteinander gekoppelt wurden und darüber hinaus für die Anbindung an ein überlagertes Leitsystem vorbereitet wurden. Dieser Demonstrator, der aus den drei Modulen Waschmodul, Spülmodul, Trocknungsmodul bestand, illustriert damit die Arbeiten zur Integration von Maschinen in eine Gesamtanlage bzw. in ein MES. Zusätzlich zum Stand der Technik wurde die heute zentrale Steuerung durch dezentrale Steuerungseinheiten aus-

getauscht, so dass steckerfertige Module entstehen, die mechanisch, elektrisch und logisch zur Gesamtanlage zusammengesteckt werden. Auch diese Module werden mit Code-Meter-Hardware-Komponenten versehen. Ein zentraler Kabelbaum sowie der Schaltschrank in der heutigen Form entfallen. Ein Beispiel für eine solche Komplettanlage zeigt Bild 66. Maschine und Produktionsfunktionalität bleiben dabei gleich, aber der Aufwand für die Integration und Erstinbetriebnahme sind geringer und senken dadurch die TCO.



Bild 65: Industriewaschmaschine bestehend auf vier Modulen



Bild 66: Aus mehreren Modulen bestehende Anlage

Anhand dieses Szenarios ist im Folgenden kurz beschrieben, welche Arbeiten konkret für einen solchen Demonstrator anfallen und welche Komponenten (Bild 67) dabei zum Einsatz kamen.

Projektziele der Fa. MOC Danner waren

- Ermöglichen eines wirtschaftlichen Umbaus von Anlagen, z.B. bei Erweiterungen,
- Verkürzung der Inbetriebnahmezeit von verketteten Anlagen,
- schnelle Anbindung an ein kundenspezifisches Leitsystem,

- Veröffentlichung (Produktkatalog) elektronischer Produktspezifikationen in einem standardisierten Format, und zwar AutomationML.

Wie sich im Projektverlauf zeigte, ergaben sich weitere Nutzenpotenziale für MOC Danner, z.B. verbesserte Ressourceneffizienz für den Hersteller und den Kunden. Durch den Einbau des SecurePLUGandWORK-Adapters erhält MOC Danner die Möglichkeit, Daten und Parameter aus dem tatsächlichen Betrieb beim Kunden zu erhalten und darauf aufbauend neue datenbasierte Dienstleistungen anzubieten.

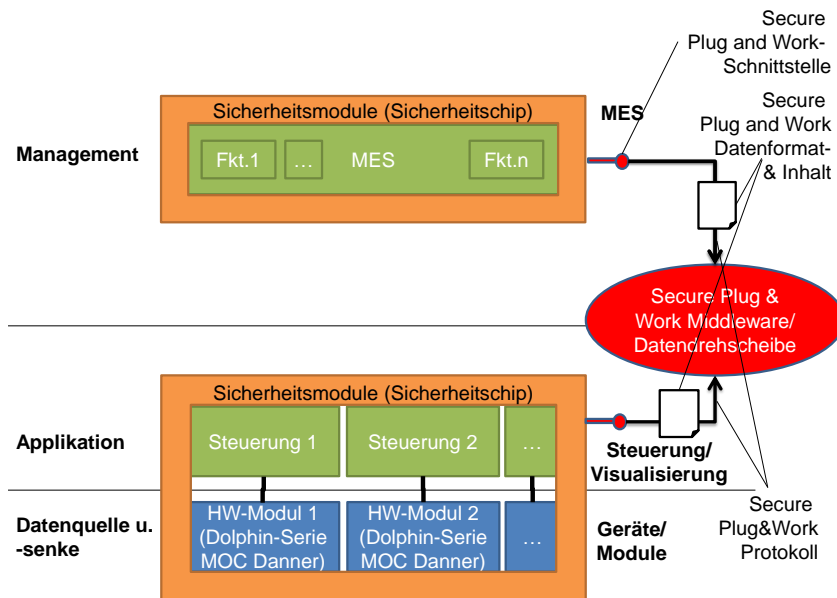


Bild 67: Übersicht Komponenten und Schnittstellen Demonstrator 2 MOC Danner – Dolphin  
Eingesetzte Software-/Hardware-Komponenten waren

- Steuerungen
  - Siemens SPS CPU1214C DC/DC/DC
  - Mitsubishi SPS FX3G (+ENET P502)
- Automation ML-Modell
- BeagleBone Black mit SecurePLUGandWORK-Komponenten (Integrationsclient, Middleware)
- Laptop mit
  - SecurePLUGandWORK-Komponenten (Integrationsserver, Distributionsclient, AutomationML-Assistenztool (Plugin für AutomationML Editor))
  - TIA Portal/GX Works2
  - ProVis.Visu
  - UAExpert.

Im Gegensatz zur Komponentenintegration, bei dem die Steuerung der Maschine direkt mit der jeweiligen Komponente (Spindel, Kugelgewindtrieb) kommuniziert, ist bei der verketteten Anlage eine Kommunikation der dezentralen Steuerungen der Module mit dem überlagerten MES erforderlich. In Bild 67 sind die einzelnen Teile, die im Projekt entwickelt werden, aufgeführt.

- Die SecurePLUGandWORK-Schnittstelle, die jeder Teilnehmer im Produktionssystem benötigt, um sich überhaupt an der Kommunikation dem Datenaustausch beteiligen zu können.

- Das SecurePLUGandWORK-Protokoll (=der Kommunikationskanal), über das die Inhalte, z.B. die Fähigkeitsbeschreibungen der Anlagenmodule, ausgetauscht werden.
- Das SecurePLUGandWORK-Datenformat, in dem die Fähigkeiten der Module beschrieben sind. Hiermit ist im engeren Sinne die in diesem Antrag immer wieder genannte Selbstbeschreibung gemeint. Hierfür verwenden die Partner vorzugsweise AutomationML, mit dem die Rolle einer Komponente oder eines Moduls, seine Attribute und ihre Wertebereiche sowie weitere semantische Informationen beschrieben werden. Dazu zählen beispielsweise Informationen aus Fabrikplanungssystemen, die ebenfalls benötigt werden, z.B. Vorgänger-Nachfolger-Beziehungen in einem Layout, so dass erkannte Komponenten an den richtigen Stellen in einem Visualisierungsbild positioniert werden oder Konfigurationsdaten zur korrekten Parametrisierung einer Werkzeugmaschinensteuerung.
- Um die Authentizität und Integrität der Parameter zu gewährleisten, wurden diese signiert und – wenn sie als sensible Information schützenswert sind – auch ggfs. verschlüsselt. Die für die Waschmaschinen genutzten Elemente für Security sind in Bild 69 zusammengefasst.
- Die SecurePLUGandWORK-Middleware, über die beispielsweise ein oder mehrere MES-Systeme sich aus den Fähigkeitsbeschreibungen 'bedienen' können, um sich zu konfigurieren.
- Sowohl das MES als auch die einzelnen Module der Gesamtanlage erhalten Sicherheitschips (siehe Kapitel 8.2 **Fehler! Verweisquelle konnte nicht gefunden werden.**), über die die Authentifizierung und die Kommunikation gesichert erfolgt. Diese Chips sind für Anlagenmodule bzw. komplette Maschinen RFID-Chips, für Maschinenkomponenten aufklebbare Codes.

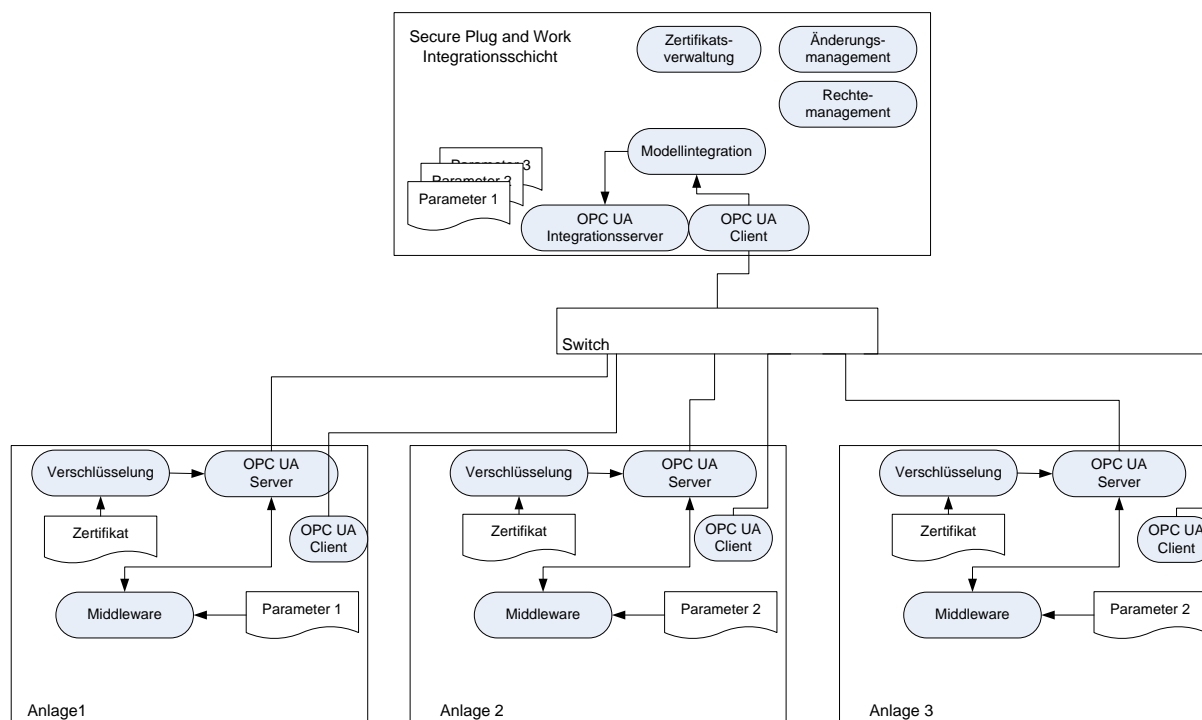


Bild 68: SecurePLUGandWORK-Architektur zur Integration von Anlagenteilen an überlagerte IT-Systeme

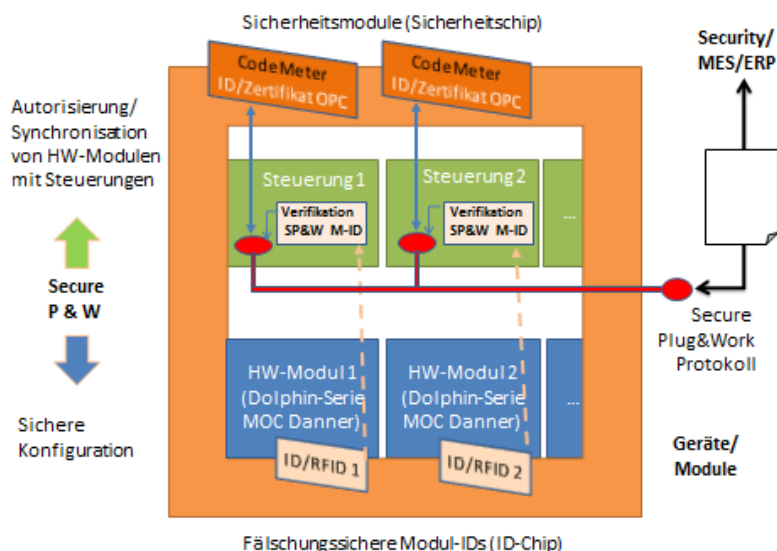


Bild 69: Übersicht Security-Komponenten auf Steuerungs-/ HW-Modulebene

## 10.3 Greifer

### 10.3.1 Ausgangssituation

SecurePLUGandWORK betrachtet verschiedene Anwendungsszenarien auf unterschiedlichen Hierarchie- und Komplexitätsebenen. Für SCHUNK relevant ist das Anwendungsszenario Integration Maschine in Anlage (z. B. Einzelmodule werden zu einem Greifersystem bestehend aus Manipulatorarm mit Greifer vereinigt). Die Inbetriebnahme von Erweitungssystemen wie Greifersystem (GS), welche beispielsweise für Werkstückmanipulationen zum Einsatz kommen, ist sehr aufwendig. Hier müssen beispielsweise die möglichen Bewegungsräume in der übergeordneten Steuerung hinterlegt werden. Außerdem wird für hochgenaue Positioniervorgänge die Positionierungsgenauigkeit im Arbeitsraum hinterlegt.

### 10.3.2 Lösungsansatz

Basierend auf den bestehenden AutomationML-Konstrukten wie Rollenkonzepten und Anlagenbeschreibungen wurde ein Anlagenmodell entwickelt, das außerdem die Zertifikate und die Digitalen Rechte der einzelnen SecurePLUGandWORK-Teilnehmer verwaltet und überwacht. Das Anlagenmodell soll es den Projektpartner ermöglichen, Beschreibungen von Komponenten und Maschinen einschließlich der jeweiligen Sicherheitsmodule im Sinne einer mechatronischen Bibliothek abzulegen. Insbesondere bei der Robotertechnik ist unter Sicherheit sowohl das Thema Safety als auch Security eine echte Herausforderung, gerade durch die automatisierte Datenübermittlung. Korrupte Daten führen hier nicht nur zu verzögerter Inbetriebnahme, sondern auch zu Gefahren für den Menschen. Dieses muss in einer Safety-Betrachtung separat untersucht werden.

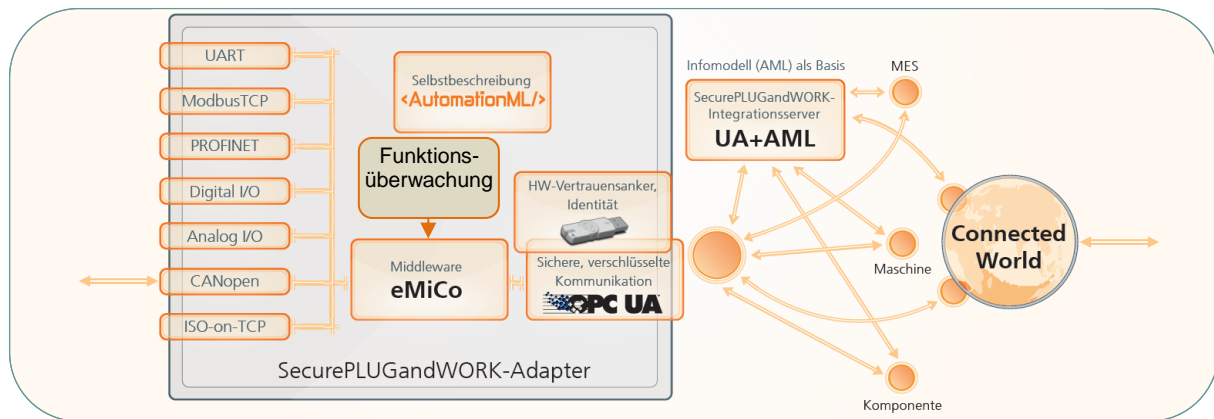


Bild 70: Schematische Darstellung des SecurePLUGandWork Adapters mit integrierter Funktionsüberwachung für den robusten Betrieb. Bei den SCHUNK spezifischen Demonstratoren wurde vom linken Teil des SecurePLUGandWORK-Adapters lediglich die CANopen-Konnektivität verwendet.

### 10.3.3 Systemkomponenten und AutomationML-Modell

Folgende Systemkomponenten wurden von Schunk im Projekt umgesetzt:

- Modell
- HW-Adapter
- Integrationsserver/Änderungsmanager (Verteilung der Komponenten, Logbuch, ...)
  - Konsistenzchecks auf z.B. Vollständigkeit, Plausibilität; Rückfall auf Standardparameter bei Umkonfiguration im Fehlerfall
- Middleware
- Assistenztool
- Hilfstools wie Integrationsclient, Distribution-Client, WriteClient, ... zur Ergänzung der zentralen eMiCo-Komponente (Middleware).

Im AutomationML-Modell wurde Folgendes beschrieben:

- Beschreibung der Fähigkeiten (Semantik); abstrakte Beschreibungen der Prozesse: RoleClassLibrary
- Typen-/ Herstellerbibliothek; Vormodellierung des Herstellers inkl. Beschreibung der Fähigkeiten (Konkret); „Ich kann Greifen“: SystemUnitClass
- Konkrete Anlage; Instanz beim Kunden: InstanceHierarchy
- Topologie, Topographie, Verhalten, Geometrie, Kinematik, Logik

Die OPC-UA Kommunikationsfähigkeit der SCHUNK-Komponente im Projekt wurde mittels kleinem Einplatinen-Computer (Beagle Bone) realisiert. Die Bereitstellung der Hardware mit der erforderlichen CANopen Konnektivität, sowie der Basissoftware erfolgte vom Projektpartner IOSB-INA. Die konkrete Integration in den Demonstrator erfolgte von SCHUNK in enger Kooperation mit dem IOSB.

### 10.3.4 Prüfstand/Achsvermessung

#### 10.3.4.1 Vermessung und Kompensation der Positionierfehler

Die Wiederholgenauigkeit ist bei typischen Roboterarmen ausreichend, um nach einer Online-Programmierung (Teachen) eine Handhabungsaufgabe zuverlässig durchzuführen. Allerdings besitzt jeder Roboter systematische Positionierfehler, die eine Übertragung des Programms auf einen anderen Roboter erschweren. So entsteht ein zusätzlicher Aufwand beim Austausch eines Roboters oder bei der Inbetriebnahme einer baugleichen Automatisierungsanwendung. Diesen gilt es hier im Sinne eines PLUGandWORK-Ansatzes zu reduzieren, indem ein Fehlermodell für jeden individuellen Roboter hinterlegt wird. Hierzu wurde am wbk ein Prüfstand zur automatisierten Vermessung von Positionierfehlern konzipiert und aufgebaut, am Beispiel des von Schunk hergestellten LWA 4P. Die notwendigen kinematischen Modelle wurden aufbereitet und eine Software zur Berechnung der Position anhand von Kamerabildern wurde erstellt.

#### 10.3.4.2 Prüfstandkonzept und Aufbau

Der Roboter muss in einem Prüfstand eingespannt werden, damit unterschiedliche Gelenkwinkel angefahren werden. Dabei werden für jede Position statische Aufnahmen des Roboters durch eine Kamera erfasst und zur Verarbeitung an einen Rechner übermittelt. Der Prüfstand soll die folgenden Anforderungen erfüllen:

- Wenig Aufwand für Ein- und Ausbau des Roboters.
- Eindeutige reproduzierbare Positionierung des Roboters relativ zu einer feststehenden Kamera.
- Vernachlässigbar kleine Verformung des Prüfstandgestells für alle Positionen des Roboters.
- Wenige Störkonturen im Arbeitsraum des Roboters.

Zur Bildaufnahme wird eine Kamera von Basler des Typs ace2500-14u eingesetzt. Diese besitzt einen CMOS-Sensor mit einer Auflösung von 2590 x 1942 Pixel und einer Pixelgröße von 2,2  $\mu\text{m}$  x 2,2  $\mu\text{m}$ . Mit dem Objektiv C125-0618-5M (Brennweite  $f = 6$  mm) entstehen Blickwinkeln von ca. 53° horizontal und 40° vertikal.

Das Gestell ist aus Aluminiumprofilen gebaut, um eine hohe Steifigkeit gegenüber Biegebelastungen sicherzustellen. Dieses besteht aus einem Grundrahmen mit Füßen, einem Podest für den Roboter und einer Aufnahme für die Kamera. Der Roboter wird mithilfe zwei Stifte auf dem Podest positioniert und durch Schrauben gesichert. Nach dem mechanischen Einbau müssen zwei Kabel mit Steckern angeschlossen werden, um den Roboter mit Energie (24V DC) und Signalen (CANopen) zu versorgen. Die Kamera wird so angebracht, dass ihre Position in allen drei Raumrichtungen manuell angepasst werden kann. Der resultierende Gesamtaufbau ist in Bild 71 dargestellt.

Zur besseren Erkennung der Pose des Roboters (Position und Orientierung) wird am Roboterflansch ein speziell konstruierter Endeffektor (Bild 72) als Target angebracht. Dieser ist würfelförmig ausgeführt und trägt auf fünf Flächen jeweils ein Schachbrettmuster. In die sechste Fläche des Würfels ist ein an den LWA 4P angepassten Flansch integriert, um den Würfel schnell und reproduzierbar an den Roboterflansch zu befestigen.

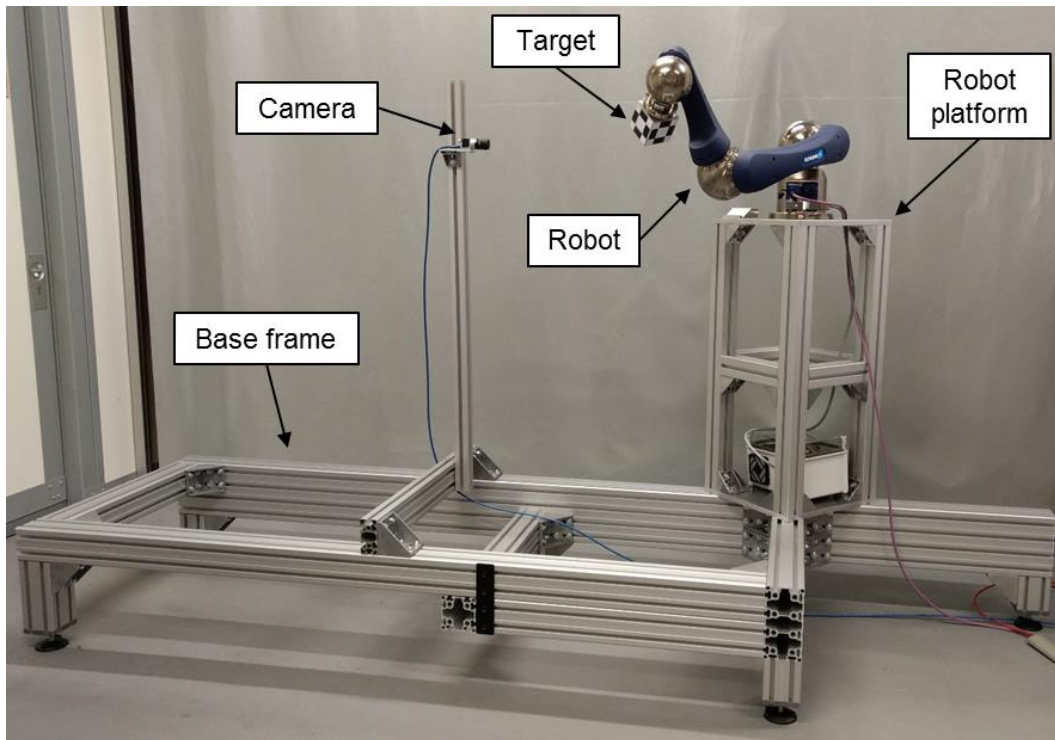


Bild 71: Gesamtaufbau Roboterprüfstand



Bild 72: Würfel-Endeffektor mit Muster für die Bildverarbeitung

#### 10.3.4.3 Kinematisches Modell

Zur Identifizierung der Positionierfehler muss zunächst die Kinematik des Greifarms modelliert werden. Die Achsen der zweiten und dritten Gelenke sind parallel angeordnet. Dies führt im klassischen Denavit-Hartenberg-Modell dazu, dass kleine Abweichungen in der Ausrichtung der Achsen große Abweichungen in den Modellparameter verursachen. Um dies zu vermeiden, wird die Formulierung nach Hayati und Mirmirani gewählt. Die Position der Gelenke wird mithilfe von Rotationsmatrizen berechnet. Diese werden für einen beliebigen Rotationswinkel  $\alpha$  wie folgt notiert:

$$R_x(\alpha) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos \alpha & -\sin \alpha \\ 0 & \sin \alpha & \cos \alpha \end{bmatrix} \quad (1)$$



$$R_y(\alpha) = \begin{bmatrix} \cos \alpha & 0 & \sin \alpha \\ 0 & 1 & 0 \\ -\sin \alpha & 0 & \cos \alpha \end{bmatrix} \quad (2)$$

$$R_z(\alpha) = \begin{bmatrix} \cos \alpha & -\sin \alpha & 0 \\ \sin \alpha & \cos \alpha & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad (3)$$

Die Position  $p_0$  eines Punktes des Endeffektors bezüglich des Basiskoordinatensystems kann bestimmt werden, indem die Position  $p_E$  in Endeffektor-Koordinaten sukzessiv in das Koordinatensystem jedes Gelenks transformiert wird. So entstehen die folgenden Gleichungen:

$$p_0 = \begin{pmatrix} 0 \\ 0 \\ d_0 \end{pmatrix} + p_1 \quad (4)$$

$$p_1 = R_z(\theta_1) \cdot \left[ \begin{pmatrix} a_1 \\ 0 \\ d_1 \end{pmatrix} + R_x\left(-\frac{\pi}{2}\right) \cdot p_2 \right] \quad (5)$$

$$p_2 = R_z\left(\theta_2 - \frac{\pi}{4}\right) \cdot \left[ \begin{pmatrix} a_2 \\ 0 \\ 0 \end{pmatrix} + R_y\left(\frac{\pi}{2}\right) \cdot p_3 \right] \quad (6)$$

$$p_3 = R_z\left(\theta_3 + \frac{\pi}{4}\right) \cdot \left[ \begin{pmatrix} a_3 \\ 0 \\ d_3 \end{pmatrix} + R_x\left(-\frac{\pi}{2}\right) \cdot p_4 \right] \quad (7)$$

$$p_4 = R_z(\theta_4) \cdot \left[ \begin{pmatrix} a_4 \\ 0 \\ d_4 \end{pmatrix} + R_x\left(\frac{\pi}{2}\right) \cdot p_5 \right] \quad (8)$$

$$p_5 = R_z(\theta_5) \cdot \left[ \begin{pmatrix} a_5 \\ 0 \\ d_5 \end{pmatrix} + R_x\left(-\frac{\pi}{2}\right) \cdot p_6 \right] \quad (9)$$

$$p_6 = R_z(\theta_6) \cdot \left[ \begin{pmatrix} a_6 \\ 0 \\ d_6 \end{pmatrix} + p_E \right]$$

Dieses Modell muss noch um Parameter erweitert werden, die eine Korrektur der individuellen Fehler ermöglichen. In ersten Untersuchungen konnten die Positionierfehler deutlich reduziert werden, indem die Nulllagenfehler in den Gelenken modelliert und kompensiert wurden. Aus diesem Grund wird weiterhin dieses einfache Fehlermodell eingesetzt. Die Modellparameter sind jeweils ein Versatz  $\varphi_i$  in jedem der sechs Gelenke:

$$\theta_i = \theta_i^* + \varphi_i \quad (11)$$

$\theta_i$  bezeichnet hier den Istwert des Gelenkwinkels  $i$  und  $\theta_i^*$  den durch die Steuerung vorgegebenen Sollwinkel.

#### 10.3.4.4 Posenmessung

Um die Pose (Position und Orientierung) des Endeffektors zu messen, müssen zunächst im aufgenommenen Bild Merkmale erkannt werden, die bekannten Punkten des Endeffektors entsprechen. Hier werden die Ecken im Schachbrettmuster benutzt, in denen sich zwei helle

und zwei dunkle Felder treffen. Die Position jeder Ecke im Bild wird mit Subpixel-Genauigkeit erfasst, indem nach einer Glättung die Sattelpunkte der Intensität (Helligkeit) ermittelt werden (Bild 73). Aus der Eckpunkterkennung ergeben sich bis zu 12 Punkte in einem Bild. Aus diesen Punkten wird anschließend unter Berücksichtigung der Perspektive die Position und Orientierung des Würfels bestimmt (Bild 74).

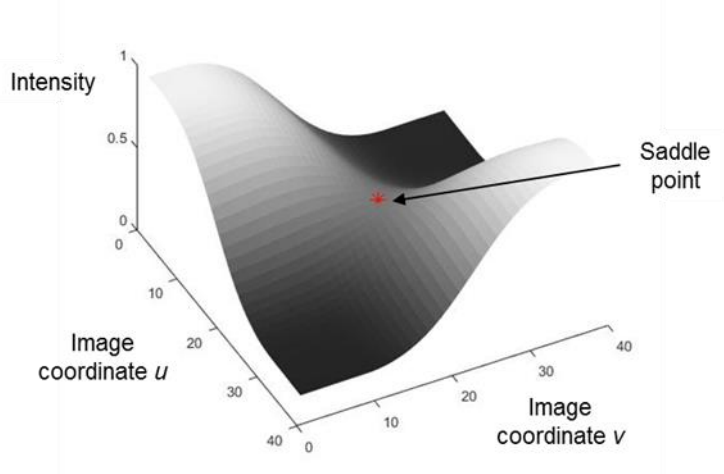


Bild 73: Prinzip der Eckpunkterkennung

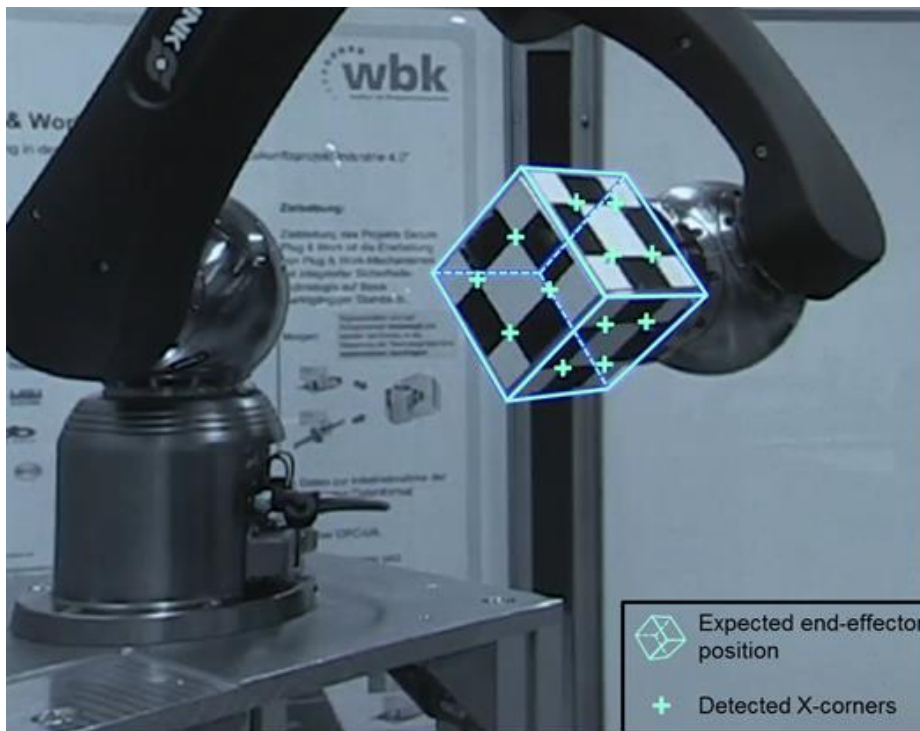


Bild 74: Kamerabild nach der Verarbeitung

### 10.3.5 Integration Maschinenebene – Schunk-Arm

Hier kommt ein UA Server auf dem SecurePLUGandWORK Adapter auf Basis eines BeagleBoneBlack (mit CAN Schnittstelle) zum Einsatz. Das zunächst vorgesehene Konzept auch die SPS bzw. die CANopen-Robotersteuerung ebenfalls mit einem UA Server auszustatten wurde aufgrund des geringen Mehrwerts für den Demonstrator nicht weiterverfolgt. Dongles für die sichere Kommunikation gibt es hier im auf USB-Basis im SecurePLUGandWORK-Adapter.

Der OPC-UA-Server ist die sichere Schnittstelle nach außen.

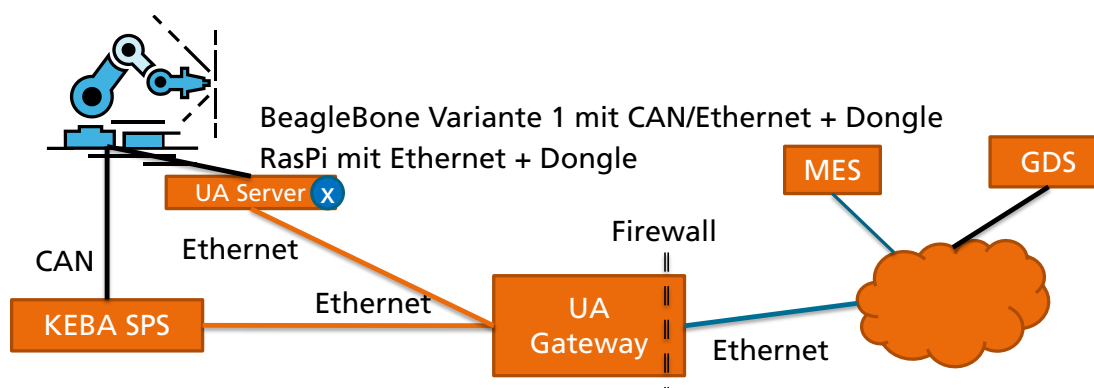


Bild 75: Realisierte Komponenten des Schunk-Demonstrators

### 10.3.6 Ergebnisse und deren Verwertung

Konkrete Ergebnisse des Projekts sind verschiedene Demonstratoren, anhand derer die SecurePLUGandWORK-Mechanismen präsentiert wurden. SCHUNK spezifisch sind zwei Demonstratoren:

1. Ein Prüfstand zur optischen Vermessung eines SCHUNK-Leichtbauarms zur Bestimmung von Gelenkwinkeloffsets am WBK
2. Ein portabler SCHUNK-Leichtbauarm mit integriertem SecurePLUGandWORK-Adapter zur Demonstration der Industrie-4.0 konformen Anbindung über OPC-UA und AutomationML.

Es werden vermehrt Aktivitäten im Bereich von OPC-UA TSN (Time Sensitive Networking) beobachtet. Diese neue Erweiterung des Ethernet Standards nimmt immer mehr Fahrt auf und wird von Branchenexperten als das Kommunikationsprotokoll für Industrie 4.0 angesehen, siehe [https://de.wikipedia.org/wiki/OPC-UA\\_TSN](https://de.wikipedia.org/wiki/OPC-UA_TSN). Dies bestärkt den Eindruck mit der frühzeitigen Konzentration auf OPC UA in SecurePLUGandWORK auf die richtige Technologie gesetzt zu haben.

### Eingesetzte Hardware- und Softwarekomponenten

- Für die SCHUNK spezifischen Demonstratoren in SecurePLUGandWORK wurden SCHUNK Greifsysteme bestehend aus LWA4 Leichtbauarm mit einer PC-basierten einfachen Robotersteuerung verwendet.
- Der im Projekt entwickelte SecurePLUGandWORK-Adapter mit der eMiCo Middleware und Integrationsclient fungiert als CANopen / OPC-UA Gateway und ermöglicht die Ankopplung von Komponenten mit CANopen-Feldbus basierter Kommunikation an gesicherte OPC-UA Kommunikation mit Hardware-Verschlüsselung.
- Der ebenfalls im Projekt entwickelte OPC-UA Integrationsserver zur Datenaggregation und mobilem Zugriff läuft auf handelsüblichen PCs, verwendet aber ebenfalls hardwarebasierte Verschlüsselung zur Sicherung der Kommunikation.

### SCHUNK spezifische Anpassungen des SecurePLUGandWORK Adapters

In Bild 70 ist der SecurePLUGandWORK Adapter nochmals schematisch dargestellt. Neben den von den Projektpartnern bereitgestellten Anteilen wie der BeagleBoneBlack basierten Hardwarebasis, der eMiCo Middleware sowie der hardwarebasierten Sicherheit (Security)

hat auch SCHUNK Softwarekomponenten bereitgestellt, die für den Betrieb im Demonstrator erforderlich sind. Dies betrifft insbesondere interne Überwachungsroutrinen, um Fehlerfälle zu diagnostizieren oder gar automatisch behandeln zu können. Diese zusätzliche Funktionalität erhöht die Robustheit ganz erheblich und ist daher nicht nur für das Demonstrator-Szenario relevant, sondern zeigt dass neben der eigentlichen Funktionalität zusätzliche und weitere Maßnahmen erforderlich sind, um einen zuverlässigen Betrieb im Feld zu ermöglichen.

### **Verwertbarkeit für CANopen basierte SCHUNK Komponenten**

Die in SecurePLUGandWork gewonnen Erkenntnisse lassen sich direkt und unmittelbar für alle SCHUNK Komponenten welche CANopen basierte Feldbuskommunikation verwenden verwerten. Neben den verwendeten zweiachsigen Schwenk- und Greifmodulen ERB145 und ERB115 bzw. PG+70 betrifft dies auch noch alle PRL+ Schwenkmodule. Die beschriebenen Vorteile wie Selbstbeschreibung und OPC-UA Kommunikation ließen sich hier direkt nutzen, es müssten lediglich die Parameter der AutomationML Selbstbeschreibung angepasst werden, nicht jedoch das zugrunde liegende Modell.

### **Verwertbarkeit für andere mechatronische SCHUNK Komponenten**

Andere mechatronische SCHUNK-Komponenten verwenden alternative Kommunikationskanäle wie Profibus, Profinet, DIO oder RS232. Je nach Unterstützung dieser Feldbusse durch den SecurePLUGandWORK-Adapter in Hard- und Software können die SecurePLUGandWORK-Erkenntnisse mit mehr oder weniger, aber vermutlich überschaubarem Aufwand genutzt werden. Neben den Parametern der AutomationML-Selbstbeschreibung muss dabei dann aber auch das zugrunde liegende Modell angepasst werden.

### **Verwertbarkeit für nicht mechatronische SCHUNK Komponenten**

Neben mechatronischen Komponenten bietet SCHUNK auch andere, i.W. pneumatische oder hydraulische Automatisierungskomponenten wie Greifer oder Schwenkeinheiten sowie Spannsysteme oder gar ganz einfache unaktivierte mechanische Komponenten wie Spannbacken an. Da diese über keine Elektronik verfügen können hier die in SecurePLUGandWORK ebenfalls gewonnen Erkenntnisse für passive Bauelemente genutzt werden. Dabei muss das einer Selbstbeschreibung zugrunde liegende Modell entsprechend angepasst bzw. grundsätzlich neu erstellt werden.

Unabhängig von einer Industrie 4.0- bzw. OPC UA-konformen Ertüchtigung solcher Komponenten kann auch schon die AutomationML basierte Selbstbeschreibung ein erheblicher Gewinn in Bezug auf (Wieder-)Inbetriebnahme oder Wartung sein.

### **Geschäftsmodelle**

In Kooperation mit dem Projektpartner Fraunhofer ISI wurden Geschäftsmodelle erarbeitet, die sich im Zusammenhang mit SecurePLUGandWORK für Schunk ergeben (siehe Bild 76).

- Erstellung von Businessplänen inklusive einer Kostenrechnung für zwei ausgewählte Geschäftsmodelle,
- Erarbeitung einer multikriteriellen Bewertungsmethode zum Vergleich alternativer Geschäftsmodelle und zur Auswahl des passenden Geschäftsmodells.

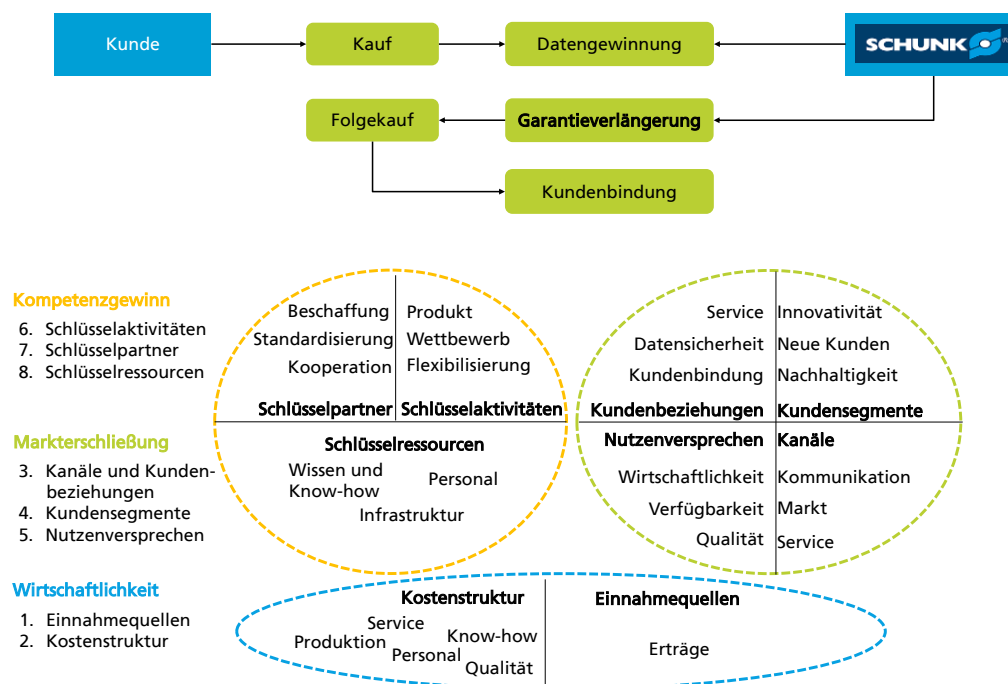


Bild 76: Visuelle Darstellung der Untersuchung von Industrie 4.0-spezifischen Geschäftsmodellen für SCHUNK

Diesen Aspekt hat SCHUNK nun als hinreichend wichtig erkannt, um eine eigene Abteilung ‚Smart Factory Engineering‘ zu gründen. Hier wird an diesem und mittlerweile einigen weiteren Geschäftsmodellen intensiv gearbeitet. Auf der HMI 2017 konnte das Thema des automatischen Datenabgleichs mit SAP und Rückführung der in HANA ermittelten Ergebnisse an die Maschine eindrucksvoll aufgezeigt werden.

### 10.4 SmartFactoryOWL

SmartFactoryOWL: Ein weiterer Demonstrator für die Projektergebnisse ist die SmartFactoryOWL, eine Initiative des Fraunhofer IOSB-INA und der Hochschule OWL (Bild 77). Hier können vom Feldgerät bis zur Leitwarte sämtliche SecurePLUGandWORK-Komponenten in einer realitätsnahen modular aufgebauten Produktionsanlage gezeigt werden und das Zusammenspiel bzw. die Abgrenzung zu Projektergebnissen des Spitzenclusters it'sOWL dargestellt werden. Durch die Projektergebnisse wird die Fähigkeit der sicheren und automatischen Rekonfiguration der beteiligten Steuerungs- und Leitsysteme, die in der SmartFactoryOWL verbaut sind, bei einem Produktwechsel demonstriert. An einem ausgewählten Szenario wird gezeigt, dass die Inbetriebnahmezeit neuer Produktions- oder Logistikmodule aus Sicht der Automatisierungstechnik auf wenige Minuten reduziert werden kann. Werkzeugmaschinen waren zum Projektstart 2013 noch nicht Teil der SmartFactoryOWL, so dass die Ergebnisse des Demonstrators 1 aus dem Werkzeugmaschinenbau auf andere Feldgeräte, z.B. Motoren für Materialflusssystem, Energiemesszähler, etc., übertragen werden müssen, die in der SmartFactoryOWL verbaut sind. Außerdem ist die SmartFactoryOWL aus modularen Komponenten aufgebaut, die jeweils eine eigene Steuerung haben. Die SecurePLUGandWORK-Anbindung dieser Module an verschiedene Leitsysteme der SmartFactoryOWL (ProVis.Agent, ABB-Leitsystem) wurde ebenfalls durchgeführt.



Bild 77: SmartFactoryOWL (siehe auch [www.smartfactory-owl.de](http://www.smartfactory-owl.de))

## 10.5 Mobile Demonstratoren

### 10.5.1 Mobiler SecurePLUGandWORK-Demonstrator

Zusätzlich verfügt das IOSB über den auf dem BMBF-Stand der Hannover Messe 2013 gezeigten Demonstrator SecurePLUGandWORK, auf den die Ergebnisse des Projekts übertragen werden, so dass weiterhin ein mobiler Demonstrator zum Einsatz auf Messen oder anderen Veranstaltungen zur Verfügung steht. Hier ist konkret geplant, zwischen den zwei bestehenden Modulen ‚Abfüllung‘ und ‚Greifer‘, die jeweils mit einer eigenen Siemens-Steuerung ausgestattet sind, die Security-Ergebnisse des Projekts zu demonstrieren. Beide Module sind an ein übergeordnetes Leitsystem (ProVis.Agent) angeschlossen, so dass die Integration eines neuen Moduls (‚Greifer‘) in den Demonstrator einfach und verständlich visualisiert werden kann.

### 10.5.2 Tischaufbau (Demo Funktionalität)

Weiterhin wurde am Fraunhofer IOSB am Ende des Projekts ein weiterer mobiler Demonstrator mit einer Ampel-Licht-Schaltung aufgebaut, der alle zentral entwickelten Komponenten (Integrationsserver, Integrationsclient, Middleware, Assistentztool) demonstrierbar macht.

## 11 Geschäftsmodelle

Die Entwicklung neuer Geschäftsmodelle erfolgte nicht demonstratorbezogen, sondern querliegend zu den o.g. Funktionen und Demonstratoren. Diese Vorgehensweise ermöglicht eine maximale Transfermöglichkeit auf andere Anwendungsbereiche und Branchen. Vorstellbar sind hier vor allem ergebnis- und nutzungsbezogene Geschäftsmodelle, die zu ihrer Umsetzung softwaretechnische Zusatzfunktionen in den Steuerungen benötigen. So kann z.B. erreicht werden, dass Funktionen bedarfsorientiert zugeschaltet und vergütet werden. Ebenso sind freischaltbare Zusatzmodule auf der Hardware möglich oder temporäre Kapazitätserhöhungen, die unter die vom Hersteller garantierte Lebensdauer fallen. Ziel dieser Arbeiten war also die systematische Entwicklung von innovativen, dienstleistungsorientierten Geschäftsmodellen für SecurePLUGandWORK-Technologien.

Folgende Motivation lag den Arbeiten zu Geschäftsmodellen zu Grunde:

- SecurePLUGandWORK-Technologien ermöglichen die Erfassung umfassender Betriebsdaten über die Nutzung eines Produkts (Komponente bis Anlage),
- Die Erfassung, Nutzung und Auswertung der Betriebsdaten ermöglicht innovative, dienstleistungsorientierte Geschäftsmodelle,
- Zentrale Frage: Wie kann ich die gewonnenen Daten nutzen?

Dabei wurde das in Bild 78 zusammengefasste Vorgehen gewählt.

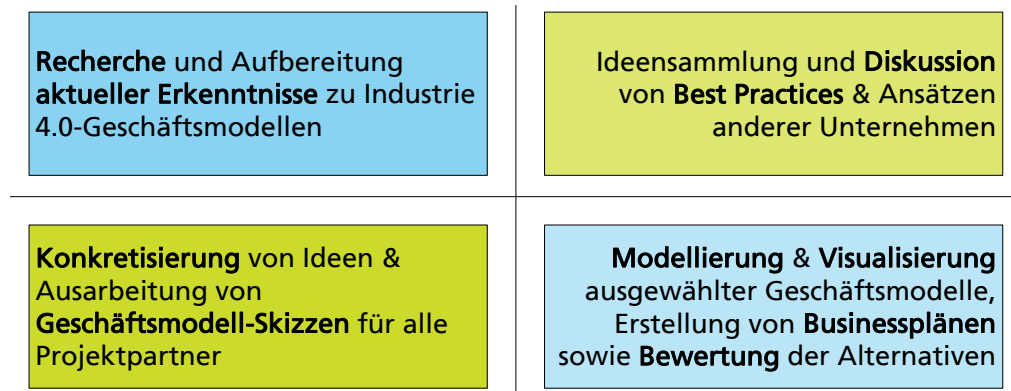


Bild 78: Vorgehen zur Generierung von Geschäftsmodellen in Projekt

### 11.1 Literaturrecherche zu Industrie 4.0-Geschäftsmodellen

Bild 79 zeigt die Ergebnisse einer Literaturanalyse mit der Fragestellung, welche Geschäftsmodellkonzepte im Maschinen- und Anlagenbau für Industrie 4.0 aktuell existieren. Ein spezielles Augenmerk der Untersuchungen ist dabei auf die Situation von kleinen und mittleren Unternehmen (KMU) gerichtet. Um herauszufinden, welche konkreten Geschäftsmodellkonzepte KMU aktuell zur Verfügung stehen, wurden Publikationen zum Thema Industrie 4.0 auf die Nennung von Geschäftskonzepten sowie von bereits umgesetzten Industrie 4.0-Geschäftsmodellen für den Maschinen- und Anlagenbau untersucht. Ausgangsbasis für die Analyse ist eine im Herbst 2014 für eine projektbezogene Marktanalyse erstellte und gepflegte Datenbank von Publikationen zum Themenfeld Digitalisierung der Industrie. Die Datenbank enthält 152 Beiträge in deutscher und englischer Sprache aus dem Zeitraum 2002 bis 2014. Die Mehrheit der Beiträge stammt jedoch aus den Jahren 2012 – 2014, beschreibt Entwicklungen unter dem Stichwort Industrie 4.0 und ist in deutscher Sprache verfasst.

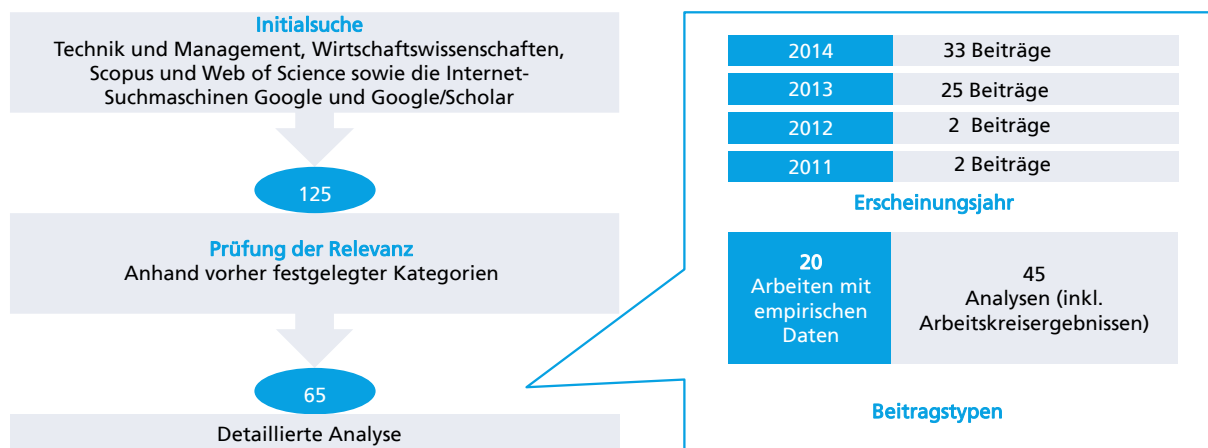


Bild 79: Ergebnisse der Literaturanalyse

Sämtliche in der Datenbank enthaltenen Artikel wurden auf Inhalte zu dem Begriff „Geschäftsmodell“ bzw. „business model“ durchsucht. Relevant für die Untersuchung waren Geschäftsmodelle für den Maschinen- und Anlagenbau, die einen neuen Nutzen oder eine Optimierung bestehender Leistungen an den Kunden formulieren. Konzepte oder Praxisbeispiele, die sich auf die Optimierung interner Prozesse beziehen, wie Verbesserung der Termineinhaltung oder Qualitätsprüfung wurden nicht betrachtet. Von den 152 Beiträgen thematisierten 77 konkrete Geschäftsmodelle im Zusammenhang mit Industrie 4.0. Diese Beiträge wurden detailliert überprüft auf die Beschreibung von Geschäftsmodellkonzepten oder Praxisbeispielen im Branchenkontext des Maschinen- und Anlagenbaus. In 18 Beiträgen wurden konkrete Umsetzungskonzepte identifiziert.

In 18 Beiträgen fanden sich konkretere Ausführungen zu Geschäftsmodellen, hierbei wurden entweder theoretische Konzepte beschrieben oder von bereits umgesetzten Beispielen berichtet. Die identifizierten Geschäftsideen für Industrie 4.0 unterscheiden sich in ihrer Detailtiefe. Eine ausführliche Beschreibung der Geschäftsmodellbeispiele und -konzepte für Industrie 4.0, welche detailliert auf die einzelnen Geschäftsmodellbestandteile, Nutzenversprechen, Wertschöpfungsarchitektur und Ertragsmodell eingehen, findet sich, mit einer Ausnahme, in keinem der Beiträge. Beschrieben wird zumeist grob das Nutzenversprechen für den Abnehmer und die neue Industrie 4.0-Technologie, welche die Erfüllung des Nutzenversprechens erst ermöglicht. In einigen Beiträgen werden zusätzlich noch der Nutzen für weitere Beteiligte des Geschäftsmodells ausgeführt sowie passfähige Ertragsmodelle vorgeschlagen.

Es kann festgehalten werden, dass die Diskussion um die Entwicklung von Geschäftsmodellen für Industrie 4.0 mit dieser der Technologieentwicklung im Rahmen von Industrie 4.0 nicht Schritt halten kann. Für die Umsetzung in marktfähige Angebote gilt es die Vorteile zu benennen, die technische Entwicklungen für verschiedene Anwenderkreise bringen. Ferner ist zu untersuchen, welche Herausforderungen mit der wirtschaftlichen Umsetzung einhergehen und welche Investitionen abseits der Technologie in die Änderungen bestehender Geschäftsmodelle und Organisationsstrukturen getätigt werden müssen. Ideen für neue Geschäftsmodellkonzepte für Industrie 4.0 werden bislang allgemein formuliert. Besonderheiten in der Umsetzung, die speziell auf die Situation von KMU im deutschen Maschinenbau zugeschnitten sind, werden in der Literatur noch nicht thematisiert.



## 11.2 Industrie 4.0-Geschäftsmodelle in der Praxis

Im Zuge des Forschungsprojekts wurde eine eigenständige Unternehmensbefragung durchgeführt, die zum Ziel hatte, mit einer hohen Detailtiefe den aktuellen Stand der Umsetzung von Industrie 4.0, erwartete Auswirkungen von Industrie 4.0 auf Wertschöpfungskette und Dienstleistungsangebot sowie Chancen, Risiken, Treiber und Hemmnisse im Zusammenhang mit Industrie 4.0 bei Unternehmen des verarbeitenden Gewerbes zu erfassen.

Insgesamt wurden Experteninterviews mit Vertretern von 14 Unternehmen sowie einem Verbandsvertreter geführt. Zwei der befragten Unternehmen waren Hersteller von Elektronikkomponenten. Sie wurden in die Befragung inkludiert, um die Zulieferer- und Ausrüstersicht bei Industrie 4.0-Lösungen zu berücksichtigen. Der Verband steht stellvertretend für die Automatisierungsindustrie, die übrigen Unternehmen sind dem Maschinen- und Anlagenbau zuzuordnen. Die befragten Unternehmen verteilen sich über ganz Deutschland und teilen sich nahezu hälftig zwischen KMU (bis 250 Mitarbeitern) und großen Unternehmen auf, was eine differenzierte Betrachtung der beiden Kategorien ermöglichte. Um ein hohes Maß an Vergleichbarkeit erzielen und gleichzeitig den Besonderheiten der Unternehmen Rechnung tragen zu können, lag den etwa einstündigen Interviews ein strukturierter Fragebogen mit sowohl offenen als auch geschlossenen Fragen zugrunde.

Viele der befragten Unternehmen befassen sich nur am Rande mit Industrie 4.0 und haben selbst nur in sehr geringem Umfang konkrete Erfahrungen mit neuen technischen Lösungen gemacht. Selbst Konzepte, wie Fernzugriff auf Produktionsanlagen durch den Hersteller, welche eher als Vorstufe zu Industrie 4.0 anstatt als Industrie 4.0 selbst zu betrachten sind und für die praktikable technische Lösungen seit längerer Zeit existieren, sind wenig verbreitet. Dies ist aber weniger auf mangelndes Interesse oder Engagement der Komponenten- oder Anlagenhersteller, sondern vielmehr auf mitunter nachvollziehbare Bedenken bezüglich der (Daten-)Sicherheit auf Seiten der Endkunden zurückzuführen. Nach aktuellem Stand gestaltet sich der Informationsaustausch zum Einsatz des Produkts beim Kunden sehr inhomogen. Einige, vor allem große Unternehmen, erhalten bereits verschiedene Betriebsdaten (Lastdaten, Daten zu Verfügbarkeiten, Stör-, Produktions- und Umrüstzeiten) von ihren Kunden, teilweise auch per Fernzugriff. Andere, vor allem KMU, erhalten lediglich während der Angebotserstellung oder im Rahmen von Serviceeinsätzen Informationen zu den Einsatzbedingungen ihrer Produkte. Dieser Informationsaustausch erfolgt meist weder automatisiert noch digital, sondern über informelle Gespräche mit dem Kunden. Fast alle Unternehmen wünschen sich einen höheren Informationsrücklauf vom Kunden. So könnten sie Daten zur Verfügbarkeit und Auslastung sowie Produkt- und Prozessparameter zur Produktoptimierung, Vermeidung von Ausfällen, Kostensenkung, aber auch zur Entwicklung neuer Geschäftsmodelle bzw. Dienstleistungen (z. B. Condition-based Maintenance) verwenden.

Es zeigt sich jedoch auch, dass erste kleine Schritte hin zur Industrie 4.0 unternommen wurden. Viele Unternehmen geben an, die Digitalisierung der Wertschöpfungskette voranzutreiben. Hauptaugenmerk liegt in den meisten Fällen auf der Einführung von Softwarelösungen wie Product Data Management (PDM), Enterprise Resource Planning (ERP) und Produktionsplanungs- und Steuerungssystemen (PPS), um die Transparenz zu verbessern und die Leistungsfähigkeit zu erhöhen. Dies ist zunächst als ein grundlegender Schritt zur Digitalisierung der Wertschöpfungskette zu betrachten. Nur einzelne Unternehmen haben bisher keine derartigen Anstrengungen getätigt. Zur Erbringung von Dienstleistungen wird Informations- und Kommunikationstechnologie (IKT) in sehr unterschiedlichem Umfang eingesetzt. Ungefähr ein Drittel der Unternehmen nutzt IKT sehr spärlich oder gar nicht. Die übrigen Unter-

nehmen nutzen Laptops, Smartphones und Software Diagnose Tools bei Serviceeinsätzen vor Ort. Darüber hinaus nutzen einige Befragte VPN-Verbindungen zur Fernwartung von Maschinen und Anlagen. Auffällig ist, dass bei Komponentenherstellern der IKT-Einsatz geringer ist. Die gilt auch für die übergeordnete Gruppe der KMU.

Zum aktuellen Dienstleistungsangebot gehören bei fast allen befragten Unternehmen Planung, Beratung, Montage und Inbetriebnahme sowie die Erstellung einer technischen Dokumentation - jedoch ohne nennenswerte Elemente von Industrie 4.0. Neuartige Geschäftsmodelle, wie nutzungs- oder leistungsbezogene Vergütung, z. B. das Bezahlen pro Outputeinheit, Arbeitsgang, nach Nutzungsdauer oder Verfügbarkeit spielen sowohl auf der Angebotsseite als auch auf der Nachfrageseite kaum eine Rolle. Lediglich ein Unternehmen stellte bereits konkrete Überlegungen bezüglich eines Betreibermodells mit einer Vergütung basierend auf der Zahl der Arbeitszyklen an, verwarf dieses Geschäftsmodell aber wieder aufgrund momentan nicht zu erfüllender technischer Voraussetzungen des Produkts.

Es gilt jedoch in der Zukunft noch einige Hürden zu überwinden, was letztlich dazu führt, dass sich insbesondere KMU derzeit noch in Zurückhaltung üben. Einer der Gründe hierfür besteht darin, dass sich eine Vielzahl der Industrie 4.0-Technologien noch in der Grundlagen- und Evaluierungsphase befinden. Dies birgt nicht nur erhöhte Fehlerquellen, sondern auch ein schwer kalkulierbares Investitionsrisiko. Vor allem für den Mittelstand ist es problematisch, da die Zeitspanne bis zur Marktreife zu groß ist. Die Investitionsbereitschaft auf Seiten der KMU fällt zudem momentan noch relativ gering aus, da nicht nur in die Hardware und Software investiert werden muss, sondern beispielsweise auch in die Schulung der Mitarbeiter. Hierbei muss nicht nur das fehlende Know-how der Mitarbeiter, sondern auch die generelle Altersstruktur des Unternehmens berücksichtigt werden. Aufgrund fehlender Erfahrungen ist es außerdem noch schwer abzuschätzen, in welchem Ausmaß die in diesem Zusammenhang benötigten Investitionen ausfallen werden. Zusammenfassend lässt sich festhalten, dass Industrie 4.0 vor allem bei KMU bisher nur in Ansätzen realisiert wurde, wenngleich der zunehmende Trend zur Digitalisierung der Wertschöpfungskette als Basis für die Implementierung von Industrie 4.0-Lösungen dienen kann.

### **11.3 Industrie 4.0 Geschäftsmodelle im Zwiespalt zwischen Recht und Technik**

Die Thematik der unerwünschten Nachahmung von Produkten und des Inverkehrbringens von Plagiaten wurde in den letzten Jahren vermehrt unter dem Begriff der Produktpiraterie beleuchtet<sup>3</sup>. Angesichts der Menge der Autoren, die sich bereits mit diesem Thema aus den verschiedensten Perspektiven beschäftigt haben, ist es jedoch auffällig, dass noch niemand den Informationsaustausch im Rahmen von M2M-Kommunikation in seine Überlegungen einbezogen hat. Sobald Maschinen untereinander, Maschinen mit Komponenten und Menschen mit Maschinen und/oder Komponenten Betriebsdaten und Informationen über Produktionsprozesse austauschen mit dem Ziel, folgende Leistungen effizienter und schneller zu erbringen, sind diese Informationen auch für Dritte interessant. Gerade das wirtschaftliche Potenzial des industriellen Dienstleistungssektors<sup>4</sup> und die damit einhergehenden wissens-

---

<sup>3</sup> So z.B. von den BMBF-geförderten Projekten PiratPro, Pro-Protect, PROACTIVE, MobilAuthent, ProAuthent, KoPiKomp, Pro Original und KoPira; Welser v. und González 2006; Wildemann et al. 2007; [8] Abele et al. 2011; Fuchs 2006 [9]; Fusan 2009 [10]; Krüger et al. [11]; Sokianos 2006 [12]; Kleine 2010 u.a. [13].

<sup>4</sup> Lightfoot und Gebauer 2011, S. 665; Kinkel et al. 2011, S. 268 [14]

und kommunikationsintensiven Prozesse<sup>5</sup> könnten zu einem erhöhten Risiko für Informationsdiebstahl und Datensicherheit des Unternehmens über den Weg der eingesetzten IuK-Technologie führen.

Das aus technischer Sicht extrem dynamische Umfeld macht es unumgänglich, das Thema aus verschiedenen Perspektiven gleichzeitig zu betrachten, um geeignete Lösungsansätze zu finden. Recht ist ein System aus demokratisch gesetzten Spielregeln, die für Gerechtigkeit sorgen sollen und helfen, Konflikte zu vermeiden oder sie zu regulieren.<sup>6</sup> Ein rein juristischer Ansatz wäre wohl schon vor den notwendigen gesetzlichen Anpassungen veraltet, wenn er die Technik zum Zeitpunkt X zugrunde legt und damit die Dynamik der IuK-Technologie verkennt. Ein rein technischer Ansatz kann zu gesellschaftlichen Entwicklungen führen, die nicht den demokratisch legitimierten Zielsetzungen der Gesellschaft entsprechen. Das Rechtssystem könnte in diesem Fall nur noch nachhinkend reagieren<sup>7</sup> und seiner Steuerungsfunktion nicht mehr nachkommen.<sup>8</sup> Wie auch schon Roßnagel/ Banzhaf/ Grimm<sup>9</sup> ihrem Werk vorausschicken, passen „technische Möglichkeiten, rechtliches Sollen und wirtschaftliche Praxis ... nicht nahtlos zueinander“. Daher ist es wichtig, die rechtlichen und technischen/ organisatorischen Maßnahmen als Maßnahmenbündel zu verstehen und auch als solches zu betrachten.<sup>10</sup> Dressel/ Scheffler<sup>11</sup> sprechen sogar von einer Funktion des Rechts als „Steuerungsinstrument für technische Lebenssachverhalte“. Hierbei ist es für die zukünftige Sicherung der Wettbewerbsfähigkeit deutscher Unternehmen wesentlich, dass das Rechtssystem nicht nur als Hemmschwelle oder Fußangel<sup>12</sup>, sondern eben als „Befähiger“ von der Industrie wahrgenommen wird.

An dieser Stelle greifen die bisher in der Literatur vorgestellten Konzepte gegen Produktpiraterie und Industriespionage zu kurz, da sie sich zwar auch mit juristischen Fragestellungen auseinandersetzen, allerdings vornehmlich aus der ex-post-Perspektive, d.h. den Möglichkeiten der Rechtsverfolgung und Rechtsdurchsetzung im Falle einer Verletzungshandlung von Verträgen, Patent- und Markenrechten. Der Dreiklang von Recht, Technik und Betriebswirtschaft als Steuerungsinstrument für neue Geschäftsmodelle findet hier noch keine Beachtung.

### 11.3.1 Rolle von Information und Know-how

Allen Darstellungen gemein ist die zentrale Bedeutung von Informationen. Informationen als immaterielles Gut lösen materielle Ressourcen in Ihrer Bedeutung ab. Informationen und deren Verwertung in Form von Wissen sind der bedeutendste Erfolgsfaktor von nationalen Ökonomien und Unternehmen.<sup>13</sup> Der Wert der Information ist anzusetzen entsprechend der Qualität und der strategischen Bedeutung für das innehabende Unternehmen.<sup>14</sup> Informationen, und darüber spezifisches Wissen, zu erlangen ist das Ziel der Industrie- und Wirtschaftsspionage. Kennzeichnend im Projekt SecurePLUGandWORK ist die automatisierte

---

<sup>5</sup> Helbig in Sokianos 2006, S. 150 oben [12]

<sup>6</sup> Roßnagel 2009, S. 15 [15]

<sup>7</sup> Wildemann et al. 2007 [16], S. 8; Fuchs 2006, S. 117 [9].

<sup>8</sup> Roßnagel 2009, S. 15 [15]

<sup>9</sup> Roßnagel et al. 2003, S. 8 [17]

<sup>10</sup> Roßnagel 2009, S. 15-20 [15]; Wildemann et al. 2007, S. XII [16]

<sup>11</sup> Dressel und Scheffler 2003, S. VI. [18]

<sup>12</sup> so bezeichnet von Wegerich in Roßnagel et al. 2003, S. 5 [17]

<sup>13</sup> Lux und Peske 2002, S. 14 [19]

<sup>14</sup> Hummelt 1997, S. 6 [20]

Verknüpfung mehrerer Vorgänge – in Serie oder parallel, ohne dass ein Mensch eingreifen muss. Es kann sich dabei um die Inbetriebnahme mit der Kombination von mehreren Anlagenteilen oder von der Anlage mit neuen Komponenten und/oder Werkzeugen handeln oder auch um zeitlich nachgelagerte Wartungs- und Instandhaltungsprozesse. Es ist damit mehr als eine elektronisch übertragene Frage, die von einem (menschlichen) Kommunikationspartner beantwortet wird und kann soweit gehen, dass eine Delegation dahingehend erfolgt, dass „die Techniksysteme den Handlungsraum selbst in eine bestimmte Gestalt bringen, etwa indem sie den Mitteleinsatz strategisch bestimmen, selbst koordinieren und an die Verfügbarkeit von Ressourcen anpassen“<sup>15</sup>. Die so neu entstehenden Geschäftsprozesse ermöglichen auch zahlreiche neue Dienstleistungen über den gesamten Lebenszyklus der Anlagen.<sup>16</sup>

### 11.3.2 Implikationen für neue Geschäftsmodelle

Auf dieser Basis neu entstehende Geschäftsmodelle sind gekennzeichnet durch zwei relevante Datenströme: Die klassischen vom Anbieter zum Kunden und der Datenrückfluss zum Anbieter. Letzterer gewinnt z.B. für neue Dienstleistungen zunehmend an Bedeutung,<sup>17</sup> z.B. indem Diagnosedaten direkt zum Anbieter übertragen werden und dort dann automatisch ein Prüfbericht erstellt und Maßnahmen eingeleitet werden. Die Mensch-Mensch-Kommunikation wird im Rahmen von SecurePLUGandWORK zu großen Teilen abgelöst durch Mensch-zu-Maschine und/oder Maschine-zu-Maschine-Kommunikation. Die hierbei gesammelten Daten aus unterschiedlichen Quellen werden in dynamischen Datenbanken zusammengeführt und zu unterschiedlichen Zwecken wieder vom Unternehmen eingesetzt. Genau diese Daten, die ein enormes Wissen über Anlagen, Kunden und Märkte in kodifizierter Form enthalten, sind auch interessant für Mitbewerber und somit ein potenzielles Ziel für Angriffe.<sup>18</sup> Büllsbach<sup>19</sup> bezeichnet diese Informationen bereits als den vierten Produktionsfaktor (neben Arbeit, Kapital und Rohstoffen) und stellt fest, dass Unternehmen der globalen wirtschaftlichen Entwicklung nicht mehr folgen können ohne einen gezielten Einsatz der gesammelten und verarbeiteten Informationen in der Produktion.

Mit der steigenden Bedeutung des bidirektionalen Datenflusses sind zukünftig kontroverse Diskussionen zwischen Anbietern und Kunden über die Art und Weise der Datennutzung und dem Eigentum an den Informationen zu erwarten.<sup>20</sup> Berechtigte Bedenken beider Seiten über einen möglichen Abfluss des Prozess-Know-hows nicht nur an den Geschäftspartner sondern auch an Dritte gilt es durch sichere Prozessgestaltung, einen klaren Rechtsrahmen, Verträge und eine gute Vertrauensbasis zu zerschlagen.

### 11.3.3 Kein direkter Schutz von Geschäftsmodellen

Ein innovatives Geschäftsmodell ist, wie alle Konzepte oder Geschäftsmethoden, nach deutschem Recht nicht geschützt, da Geschäftsideen in Deutschland nicht Gegenstand von Schutzrechten sein können.<sup>21</sup> Erlangt jedoch ein Wettbewerber auf nicht legale Weise Informationen darüber, welche Informationen vom Anbieter in welchem Umfang erhoben und

---

<sup>15</sup> Roßnagel 2007, S. 17 [15]

<sup>16</sup> Mattern 2003, S. 27 [21]

<sup>17</sup> s. Körner 2002, S. 34 [22]

<sup>18</sup> vgl. Brentani 2001, S. 173 [23]

<sup>19</sup> s. Büllsbach 2002, S. 45 [24]

<sup>20</sup> s. Körner 2002, S. 35 u. 73 [22]

<sup>21</sup> s. Gillert 2006, S. 206 u. 209 [25]

verarbeitet werden und welche Kommunikationskanäle genutzt werden, so wird er erst dadurch in die Lage versetzt, dieses Geschäftsmodell nachzuahmen. Ob dann der Standpunkt vertretbar ist, es handele sich nicht um Piraterie, zumal ja mangels Schutzzfähigkeit auch keine Rechtsverletzung vorliege<sup>22</sup>, soll an dieser Stelle dahingestellt bleiben. Auch die Diskussion um die Patentierbarkeit von Geschäftsmodellen und/oder Software mit oder ohne direkten Zusammenhang mit einer technischen Einrichtung in Deutschland kann hier dahinstehen, da es in den interessanten Fällen nicht um die Nachahmung des Geschäftsmodells an sich, sondern um den ungewollten Datenabfluss von Anlagen- und Produktions-/Unternehmensdaten geht, der über Patente nicht erreicht werden kann.

### 11.3.3.1 Schutz der einzelnen Informationen

Folglich sind die Bedeutung und der Schutz der einzelnen Informationen näher zu betrachten als möglicher Ansatzpunkt für das Zusammenspiel von Recht und Technik. Zu klären sind neben der Situation bei den tatsächlichen Angriffen von Dritten auf die Informationen auch die Zugriffe bzw. die Zugriffsberechtigung der verschiedenen (Mit-) Glieder der Wertschöpfungskette (Stichwort: Eigentum an den Betriebsdaten). Gerade im letzteren Fall ist es möglich, dass keine vertragliche Vereinbarung – wie z.B. zwischen dem Anlagenhersteller und dem Käufer – existiert, in deren Rahmen die Datenerhebung und –Nutzung geregelt werden könnte. Ein Beispiel dazu ist der Hersteller der in der Anlage verbauten Spindel, der keinerlei vertragliche Beziehung zum Käufer der Anlage unterhält, der aber u.U. ein nachvollziehbares Interesse daran hat, Betriebsdaten und –Zustände der Spindel zu erfassen und auszuwerten. Ebenso soll die Bedeutung der Erfassung personenbezogener Daten im B2B-Geschäft zumindest kurz angesprochen werden.

#### a) Angriffe

Unter einem Angriff lassen sich vielfältige Arten zusammenfassen: Zum einen kann es sich um die Erstellung einer Kopie bzw. um eine Nutzung von fremden Daten handeln, wobei kennzeichnend ist, dass die Originaldaten im Herrschaftsbereich des Berechtigten verbleiben. Diese Angriffsform wird im Volksmund und in der nicht-juristischen Literatur oftmals auch als Datendiebstahl bezeichnet.<sup>23</sup> Aus der juristischen Perspektive muss allerdings festgestellt werden, dass es sich dabei um keinen Diebstahl im Sinne des § 242 StGB handelt. § 242 StGB setzt die Wegnahme eines körperlichen Gegenstands, einer Sache i.S.v. § 90 BGB voraus. Damit sind digitale Güter schon vom Wortlaut her nicht umfasst, die Bezeichnung Datendiebstahl ist irreführend. § 242 StGB kann den Schutz von Daten wenn überhaupt nur indirekt über das Eigentum am Datenträger gewährleisten. Juristisch korrekt muss die beschriebene Handlung als „unrechtmäßiges Kopieren“ von Daten, möglicherweise in Tateinheit mit dem Straftatbestand des § 202a StGB „Ausspähen von Daten“ – sofern es unter Überwindung einer Zugangssicherung erfolgt - bezeichnet werden.

Ähnlich verhält es sich bei der Datenmanipulation: Hier wird nicht lediglich eine Kopie der vorhandenen Daten veranlasst, sondern zusätzlich eine Veränderung der Originaldaten herbeigeführt. Diese Veränderungen können erheblichen Folgeschaden anrichten. Vor allem in automatisierten Geschäftsabläufen wird zur Entscheidungsfindung und Ablaufbestimmung auf verschiedene Datenquellen zurückgegriffen ohne die Daten selbst zu verifizieren. Eine

---

<sup>22</sup> vgl. Gillert 2006, S. 206 [25]

<sup>23</sup> vgl. Gabler Verlag (Hrsg.): Stichwort „Ausspähen von Daten“ – hier wird Datendiebstahl synonym benutzt; s. Pierrot in Ernst 2004, Rn. 25 [26]

Manipulation am übermittelten Sensormesswert kann u.U. dazu führen, dass durch die Überschreitung von Schwellenwerten ein Sicherheitsprozess ausgelöst wird, der die Anlage zum Schutz vor Schäden ausschaltet oder die gesamte Produktion stoppt.<sup>24</sup>

### **b) Eigentum an den Betriebsdaten?**

Eine wesentliche Voraussetzung, um den Schutz und die dazu nötigen Maßnahmen bewirken zu können, ist die Klärung der Nutzungsmöglichkeiten bzw. des Eigentums an den erhobenen Daten. In diesem Zusammenhang ist nur eine einzige Konstellation unproblematisch: Der Eigentümer und gleichzeitig Betreiber der Anlage ermächtigt den Hersteller bzw. den Servicetechniker ausdrücklich (z.B. im Rahmen eines Vertrags), bestimmte Daten aus der Anlage auszulesen und weiter zu verarbeiten. Eine Einbettung in die Betriebsanleitung wird auf keinen Fall ausreichend sein.

In allen anderen Fällen kann man über das Eigentum wie auch über die Nutzungsberechtigung an den erhobenen Betriebsdaten durchaus streiten: Zunächst sind Betriebsdaten keine bewegliche Sache i.S.d. § 90 BGB, so dass kein Sacheigentum an den Daten entstehen kann und damit auch keine Eigentumsübertragung möglich ist. Daher muss auf den erweiterten Eigentumsbegriff des Art. 14 GG zurückgegriffen werden. In Betracht kommt eine Zuordnung aus dem Recht am Gewerbebetrieb bzw. aus der Berufsfreiheit Art. 12 GG (streitig). Ein allgemeiner Vermögensschutz kann jedoch über Art. 14 GG nicht erreicht werden. In Betracht kommen ferner zahlreiche, über verschiedene Gesetze verteilte Regelungen zur Zuordnung von bzw. Nutzungsberechtigung an Daten wie z.B. im UWG, UrhG, TKG... über die letztlich Datenbanken (UrhG) oder zumindest der Zugang zu einzelnen Informationen geregelt ist. Die einzelne Information als solche ist jedoch nirgendwo geschützt.

Ansatzpunkt könnte hier die Übertragung des Sacheigentums an der Anlage sein – in dem Moment, wo Einigung und Übergabe erfolgt sind, könnte der neue Eigentümer automatisch auch Verfügungs- und Nutzungsrechte an den Betriebsdaten kraft Kaufvertrags erwerben. Dies wird jedoch abzulehnen sein, da zum Zeitpunkt des dinglichen Erwerbs überhaupt noch keine Betriebsdaten existieren, an denen der Käufer Rechte erwerben kann. Ohne ausdrückliche Regelung ist auch der Kaufvertrag nicht auf zukünftige Leistungen gerichtet. Denkbar ist jedoch die Annahme, dass die Informationen, die die Anlage bzw. in ihr verbaute Komponenten während des neuen Eigentumsverhältnisses „produziert“ auch rechtlich dem Eigentümer der Anlage zustehen. Auch dies wird ohne zusätzliche Vereinbarung nicht automatisch anzunehmen sein. Man muss allerdings davon ausgehen, dass für jegliche Nutzung (nicht Erfassung) von Daten ein Einwilligungserfordernis für den Eigentümer der Anlage besteht, so dass dieser die Erhebung faktisch nicht verhindern kann (außer durch einen Sacheingriff in seine Anlage), aber die weitere Nutzung und das Auslesen der Informationen aus seinem „Hoheitsgebiet“ durchaus seiner Einwilligung bedarf. Anders herum darf jedoch auch der Eigentümer der Anlage kein gegen Zugriff geschütztes Speichermedium des Herstellers auslesen, da er ohne separate Vereinbarung keine Verfügungs- und Nutzungsrechte an den Daten hat. Sind die Daten jedoch frei zugänglich, gilt die Allgemeinfreiheit der Information und er darf sie auch nutzen. In allen anderen Fällen muss eine vertragliche Vereinbarung herbeigeführt werden.

---

<sup>24</sup> s. Kotarski 2014, S. 25 [27]

### c) Schutz personenbezogener Daten

Rechtlich weniger relevant im B2B-Umfeld ist das Kontrollpotenzial, das sich aus dieser Art der automatisierten Datensammlung und –Verarbeitung ergibt. Natürlich kann der Hersteller theoretisch die Zustandsdaten der Anlage jederzeit auslesen und damit Informationen über die Produktion und damit über Mengen- etc. gewinnen, doch zum einen ist sich der Kunde darüber bewusst und stimmt dem im Rahmen des Vertrages (z.B. condition monitoring) ausdrücklich zu und zum anderen hat er ja durch den faktischen Zugriff auf die Anlage jederzeit die Möglichkeit, diese Datensammlung und Verarbeitung zu unterbinden (Chip ausbauen, Internetverbindung trennen...). Eine Sammlung und Nutzung der Daten zur vollautomatischen Überprüfung von menschlichen Verhaltensweisen<sup>25</sup>, z.B. der des Anlagenführers anhand von manuellen Eingriffen, Not-Stopps, Dauer der Stillstandszeiten..., wie es von Schaar<sup>26</sup> als ubiquitous computing beschrieben wird, ist in diesem Kontext wenig wahrscheinlich und auch nur von geringer Aussagekraft, so dass es hier nicht weiter verfolgt wird.

#### 11.3.3.2 Präventiver Schutz durch das Rechtssystem?

In Deutschland existieren keine Rechtsvorschriften, die explizit die Thematik der elektronischen Industriespionage abdecken.<sup>27</sup> Das deutsche Recht kennt die Begriffe Industrie- od. Wirtschaftsspionage nicht im Sinne einer Legaldefinition, so dass sich die Analyse des Rechtsschutzes über zahlreiche Gesetze erstreckt. Eine wichtige Diskussion in diesem Kontext beginnt sogar schon einen Schritt früher: Die Diskussion um eine eventuelle Subsidiarität rechtlicher Maßnahmen gegenüber technischen Schutzmöglichkeiten, die immer dann wieder auftaucht, wenn neue Technologien auf den Markt kommen und die Missbrauchsmöglichkeiten diskutiert werden.<sup>28</sup> Der Ansatzpunkt ist dabei, dass es digitale Piraterie überhaupt erst gibt, weil a) technische Schutzmöglichkeiten noch nicht möglich oder b) nicht ausreichend ausgeschöpft werden. Lapidar formuliert lautet die Anforderung an die Industrie, sich zunächst technisch zu rüsten und entsprechende Entwicklungen voranzutreiben, bevor rechtliche Maßnahmen in Anspruch genommen werden können. Begründet wird dies mit den Prinzipien der Subsidiarität und der Eigenverantwortlichkeit, so dass der Selbstschutz als gleichgeeignetes aber milderer Mittel verpflichtend vorrangig eingesetzt werden muss.<sup>29</sup> Unabhängig von dieser in der Literatur existierenden aber nicht haltbaren Forderung sind Normen zum Schutz von Informationen quer über die ganze Rechtsordnung verteilt. Angesichts der Tatsache, dass die IKT gerade ein Mittel ist, um weltweit Leistungen auf digitalem Weg zu erbringen und damit über organisatorische und geografische Grenzen hinweg zu operieren, wäre es fatal davon auszugehen, eine nationale Rechtsordnung alleine könnte hier ausreichend Schutz gewähren. Zudem sind Fragen des Datenschutzes auch Gegenstand von internationalen und supranationalen Regelungen.<sup>30</sup> Änderungen im nationalen Datenschutzrecht sind nicht zuletzt auf Harmonisierungsbestrebungen der EU und anderer Organisationen zurückzuführen.<sup>31</sup> An dieser Stelle wird daher nur ein Auszug aus den relevanten Normen vorgestellt:

---

<sup>25</sup> vgl. Roßnagel 2007, S. 22 [15]

<sup>26</sup> vgl. Schaar 2006 [28]

<sup>27</sup> s. auch Meissinger 2005, S. 15 [29]

<sup>28</sup> s. Scheffler in Gounalakis 2003, § 57, Rn. 8 ff. [30]

<sup>29</sup> s. Hassemer 1981, Schutzbedürftigkeit S. 22 ff.; s. Amelung 1977, S. 17 [31]

<sup>30</sup> s. Tinnefeld et al. 2005. S. 97 [32]

<sup>31</sup> s. Scholz 2003, S. 113 [33]

## a) BDSG

Zunächst und weil begrifflich sehr naheliegend soll der Schutz über das nationale Datenschutz- bzw. Informationsrecht untersucht werden. In Wortlaut und Reichweite sehr umfassend geregelt ist der Schutz von Daten, die von Privatpersonen vorgehalten und ausgetauscht werden, z.B. durch das Gesetz zum Schutz vor Missbrauch personenbezogener Daten bei der Datenverarbeitung (Bundesdatenschutzgesetz - BDSG). Dieses Gesetz legt jedoch in § 3 Abs. 1 BDSG fest, dass

*"Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person (Betroffener)."*

Damit ist es derzeit in Deutschland noch herrschende Meinung, dass Unternehmensdaten, insbesondere aus der Produktion, keine Daten sind, die unter das BDSG fallen. In anderen Ländern, auch innerhalb der EU ist dies z.T. anders geregelt.<sup>32</sup>

## b) Telekommunikationsgesetz (TKG)

Das TKG stellt eine der vielen Spezialregelungen zum BDSG dar, indem es sich mit dem rein technischen Vorgang der Kommunikation, also insbesondere dem Netz, über das verschiedene Dienste angeboten werden sowie den Telekommunikationsdiensten befasst. Hier fallen neben Bestands-, Verbindungs- und Abrechnungsdaten insbesondere auf der Ebene der Telekommunikationsdienste auch qualifizierte Nutzungsdaten an.<sup>33</sup> Im Unterschied zum BDSG, welches nur Einzelangaben natürlicher Personen schützt, stellt das TKG in § 91 Abs. 1 Einzelangaben über juristische Personen und Personengesellschaften den Angaben über natürliche Personen gleich. Unternehmen genießen somit denselben Schutz wie natürliche Personen.

Die Auswirkungen für den Schutz von Unternehmensdaten werden in den §§ 88 f. TKG deutlich: § 88 TKG enthält eine einfachgesetzliche Umsetzung des Fernmeldegeheimnisses aus Art. 10 GG für die Inhalte der Telekommunikation. Unter Telekommunikation ist dabei gem. § 3 Nr. 22 TKG der technische Vorgang des Aussendens, Übermittels und Empfangens von Signalen mittels Telekommunikationsanlagen zu verstehen. Signale können dabei in Form von Zeichen, Sprache, Bildern oder Tönen vorliegen.<sup>34</sup> Telekommunikationsanlagen umfassen gem. Nr. 23 technische Einrichtungen oder Systeme, die als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können. Darunter werden auch Elemente der M2M-Kommunikation zu verstehen sein, wie z.B. Transponder und Lesegeräte für RFID-Chips,<sup>35</sup> da es um den Schutz der Inhalte geht und es dabei keine Rolle spielen kann, ob die Kommunikation automatisiert erfolgt oder vom Menschen direkt initiiert wird – der auszutauschende Inhalt bleibt dabei stets gleich.<sup>36</sup> Unabhängig von den Vorschriften zum Datenschutz innerhalb des TKG (§§ 91 ff.), schützt das Fernmeldegeheimnis neben den techni-

<sup>32</sup> s. z.B. in Österreich: § 4 Nr. 1 DSG 2000.

<sup>33</sup> s. Bergmann/Möhrle/Herb, Datenschutzrecht 1977->, Datenschutzrecht Bd. III Teil 6, Vorb. 1.4.6 u. 1.5 [34]

<sup>34</sup> s. Hoeren 2013, S. 425 [35]

<sup>35</sup> s. Theißen 2009, S. 288 [36]

<sup>36</sup> Dies ergibt sich auch aus der Gesetzesbegründung, wonach § 89 TKG gerade auch die Besonderheiten neuer Informations- und Kommunikationstechniken erfassen und bei gleicher Interessenlage den gleichen Schutz gewährleisten soll. s. die vom Wortlaut identische Vorgängernorm § 86 TKG, BT-Drs. 13/443.



schen Daten der Verbindung auch den Inhalt der Kommunikation,<sup>37</sup> ohne dabei einen Personenbezug zu fordern.

### c) UWG

Den wohl umfassendsten präventiven Schutz erfahren Unternehmen durch das Rechtssystem über das Gesetz gegen den unlauteren Wettbewerb. Das UWG hat das Ziel, fairen Wettbewerb mit zivilrechtlichen Mitteln zu gewährleisten. Da für Informationen in der hier diskutierten Form kein Sonderrechtsschutz in Betracht kommt, kann über das UWG zumindest ein Schutz vor Handlungsunrecht erlangt werden. Verstöße gegen das Lauterbarkeitsrecht können nämlich zivilrechtliche Ansprüche auf Unterlassung, Beseitigung, Gewinnabschöpfung und Schadensersatz (§§ 8 ff. UWG) nach sich ziehen.<sup>38</sup> Damit spielt das UWG eine wichtige Rolle beim Schutz von Know-how in Form von Unternehmensdaten. Im Rahmen des UWG ist Know-how weit definiert als „jeder wirtschaftlich relevante Wissensvorsprung“. <sup>39</sup> Dazu gehören neben Prozessinformationen, Konstruktionspläne, Betriebsdaten, Kalkulationsunterlagen, Lieferanten- und Kundenlisten etc. auch die Servicedaten.

Insbesondere § 4 UWG erweist sich als hinreichend flexibel, um auch die mit der Digitalisierung einhergehenden neuen Problemstellungen bewältigen zu können. Zudem bietet das UWG zusammen mit den Mitteln des einstweiligen Rechtsschutzes die Möglichkeit, schnell und proaktiv auf Angriffe zu agieren und so den Schaden gering zu halten.

### d) BGB

Der Unternehmer kann in Fällen der Verletzung der ihm zustehenden Unternehmensgeheimnisse Schadensersatz für den konkret erlittenen Schaden und auch Unterlassung gem. §§ 823 Abs. 1 BGB; 823 Abs. 2 BGB i.V.m. § 17 UWG; 826 BGB, 1 UWG bzw. Wertersatz gem. § 812 Abs. 1, Satz 1, 2. Alternative BGB oder den Verletzergewinn gem. §§ 687 Abs. 2, 681, 667, 684 BGB einfordern.

Im Rahmen des § 823 Abs. 2 BGB kann durch strafrechtliche Vorschriften in mehrfacher Hinsicht Schutz vor Spionageangriffen auf Unternehmensgeheimnisse erlangt werden. Im Bereich der Prävention und der Schadensvermeidung erweist sich der Unterlassungsanspruch aus § 823 Abs. 2 BGB i.V.m. § 17 UWG als sehr effektiv, sofern der Angriff erkannt wird und der Angreifer identifiziert werden kann, bevor ein Schaden entsteht.

#### 11.3.3.3 Repressiver Schutz durch das Rechtssystem

§ 303a StGB bietet umfassenden Schutz vor Datensabotage und Eingriffen in die Produktionsabläufe, während § 303b StGB mit der Wesentlichkeit der Auswirkungen auf die Funktionstüchtigkeit des Unternehmens eine nicht unerhebliche Schwelle aufweist, oberhalb allerdings einen wirksamen Schutz bietet. Auch die §§ 202a und 202b StGB bieten einen wirksamen Schutz für Unternehmensdaten: § 202b StGB schützt während eines laufenden Übertragungsvorgangs während § 202a StGB jede Art von unbefugtem Zugriff auf zugangsgeschützte Daten verhindern soll und damit auch im Bereich der Datenübertragung mit RFID oder Bluetooth 4.0 Anwendung finden kann. Lediglich § 263a StGB könnte zwar in einigen Fällen zumindest theoretisch relevant werden, wird jedoch aufgrund der praktischen Beweis-

<sup>37</sup> s. Spindler 2007, Rn. 432 [37]

<sup>38</sup> s. Müller 2011, S. 128 f. [38]

<sup>39</sup> Welser v. und González 2006, S. 106 [39]

probleme bei der geforderten Stoffgleichheit zwischen Vermögensschaden und angestrebtem Vermögensvorteil kaum Anwendung finden.

### Fazit

Es wird deutlich, dass es im deutschen Recht formal nicht an Schutzmöglichkeiten mangelt. Der Schutz setzt allerdings nicht an der Nutzung der Information an sich an, sondern an der Überwindung des faktischen (Geheim-) Schutzes, den der Informationsinhaber wählt,<sup>40</sup> bzw. an seiner tatsächlichen Beziehung zur Information.<sup>41</sup> Die anwendbaren Vorschriften mögen zwar verstreut über zahlreiche Gesetze sein, ergeben aber in ihrer Gesamtheit durchaus einen sinnvollen Schutz für Unternehmensgeheimnisse gegenüber Angriffshandlungen.<sup>42</sup> Wenn Kleine<sup>43</sup> von einem „Versagen“ juristischer Maßnahmen als Mittel zur Eindämmung von Produktpiraterie spricht, so liegt dem eine rein betriebswirtschaftliche Betrachtung bezogen auf absolute geistige Eigentumsrechte im Kontext von Produktpiraterie zu Grunde. Es liegt in der Materie des Rechts, dass hier stets nur Rahmenbedingungen geschaffen werden können, die eben nicht mit physischen, nicht zu überwindenden Bauwerken vergleichbar sind. Schon deshalb ist der Rechtsrahmen nicht mit den betriebswirtschaftlichen Messgrößen der Effektivität und der Effizienz bewertbar.<sup>44</sup>

Vor allem die Möglichkeiten bereits über den vorbeugenden Rechtsschutz Unterlassung zu verlangen, geben den Unternehmen „schnelle“ Instrumente an die Hand. Es bleibt jedoch die Situation, dass kein Normensystem in der Lage ist, kriminelle Handlungen und ihre Folgen zu verhindern. Der Schaden tritt aber bereits bei einem ersten Angriff auf und die Folgen sind für die Unternehmen kaum kalkulierbar, da, sofern der Angriff überhaupt zeitnah erkannt wird, nicht nachzuvollziehen ist, wer zu welchem Zweck Informationen manipuliert oder kopiert hat. Diese Unkenntnis der Person des Angreifers ist eines der zentralen Probleme im Rahmen von Cyberpiraterie und Recht, denn zur Durchsetzung eines Anspruchs oder zur Verfolgung einer Straftat wird stets eine (natürliche) Person benötigt, der die Handlung nachweisbar zuzurechnen ist. Das Medium Internet bietet unzählige Möglichkeiten, die Rückverfolgung von Aktivitäten über IP-Adressen zu verschleiern<sup>45</sup> oder durch die Ausnutzung der fehlenden Gesetze zum Datenschutz bzw. zur Datenspeicherung anderer Länder<sup>46</sup> faktisch unmöglich zu machen,<sup>47</sup> so dass es nur in einem verschwindend kleinen Bruchteil aller bekannte Fälle überhaupt möglich ist, eine Person zu ermitteln, die eine Aktion veranlasst hat. Daher erweisen sich die vom Gesetzgeber vorgesehenen Schutzmöglichkeiten als wenig praktikabel zur Prävention vor Piraterieangriffen auf Unternehmensdaten, da eine Re-

---

<sup>40</sup> s. Ann 2007, S. 40 [40]

<sup>41</sup> s. Müller 2011, S. 121 [38]

<sup>42</sup> s. Brenner 2006, S. 281; a.A. Gottschalk et al. 2002, S. 95 f., wo von einem Bedeutungsverlust juristischer Schutzmaßnahmen berichtet wird [41]

<sup>43</sup> s. Kleine 2010, S. 41 unter Verweis auf die empirische Untersuchung bei Voigt et al. 2008 [42]

<sup>44</sup> a.A. Kleine 2010, S. 41 [42]

<sup>45</sup> s. z.B. das Tor-Netzwerk zur Anonymisierung von Verbindungsdaten ([www.torproject.org](http://www.torproject.org)). Es basiert darauf, dass eine zufällige, sich alle zehn Minuten ändernde verschlüsselte Verbindung über drei Tor-Knoten zum Ziel aufgebaut wird, so dass eine quasi-anonyme Nutzung des Internets möglich ist.

<sup>46</sup> z.B. sog. Offshore-Server in Belize, Bahamas, Malaysia oder Panama.

<sup>47</sup> so wird ein Rechtshilfeersuchen von vielen Ländern abgelehnt werden mangels einer Eingriffsgrundlage z.B. für den Zugriff auf Netzwerke. s. Schuster 2000, S. 77 ff. [43]

aktionsmöglichkeit zumeist erst dann gegeben ist, wenn der Schaden bereits entstanden ist.<sup>48</sup>

Neben einzelnen notwendigen Veränderungen im Rechtssystem ist vor allem eine Synthese mit der aktuellen IKT und damit eine Kombination von verschiedenen Maßnahmen unumgänglich,<sup>49</sup> um ein wirkungsvolles Schutzsystem aufzubauen.<sup>50</sup> Setzt man wieder die betriebswirtschaftliche Brille auf, so liegt es auf der Hand, dass der technische Datenschutz gegenüber dem rein rechtlichen Informationsschutz deutlich effektiver ist, denn was bereits technisch verhindert wird, muss nicht mehr verboten oder rechtlich verfolgt werden.<sup>51</sup> Wenn das Zusammenspiel zwischen Recht und Technik derart gestaltet werden kann, dass das Rechtssystem zum Schutz von Informationen die Voraussetzungen für einen technischen Schutz schafft, indem es Pflichten generiert und Anreize schafft, dann kann auch ein faktischer, präventiver Schutz erreicht werden.

#### 11.4 Ideensammlung und Diskussion von Best Practices und Ansätzen anderer Unternehmen

Im Rahmen von Workshops und Industriearbeitskreisen wurden die Ideen zu Industrie 4.0-Geschäftsmodellen gesammelt und Best Practices über Diskussionen mit anderen Unternehmen identifiziert.

##### Was ist ein Geschäftsmodell?

- Vereinfachte Darstellung der Geschäftslogik d.h. eine vereinfachte Beschreibung wie ein Unternehmen Profit erwirtschaftet
- Zur Vereinfachung wird ein Geschäftsmodell in verschiedene Bestandteile unterteilt:



- Änderungen im Unternehmensumfeld/im Unternehmen führen zu Chancen und Risiken, denen durch Anpassungen im bestehenden Geschäftsmodell oder Aufbau eines neuen Geschäftsmodells entsprochen werden kann.

Bild 80: Definition Geschäftsmodell

Daraus resultiert eine Sammlung von 12 Tätigkeitsfeldern für Industrie 4.0-Geschäftsmodelle für Komponenten- und Anlagenhersteller (Bild 81), die jeweils über das Nutzenversprechen, die Wertschöpfungsarchitektur und das Erlösmodell beschrieben werden.

<sup>48</sup> s. Wildemann et al. 2007, S. 8 [16]

<sup>49</sup> s. Wildemann et al. 2007, S. I [16]

<sup>50</sup> s. Roßnagel 2007, S. 158 [44]

<sup>51</sup> s. Ebenda, S. 185 [44]

**Ideen für Geschäftsmodelle im Rahmen von SecurePLUGandWork**

- |   |                                 |
|---|---------------------------------|
| 1. Verfügbarkeitsgarantie                   | 8. Neuartige Abrechnungsmodelle |
| 2. Verkürzung der <u>Inbetriebnahmezeit</u> | 9. Genauere Ausfallprognosen    |
| 3. Ausschussgarantie                        | 10. Flexible Produktionslinie   |
| 4. Nutzungsabhängige Vergütung              | 11. Technologiedaten            |
| 5. Wandlungsfähige Produkte                 | 12. Anlagenoptimierung          |
| 6. Nutzungsabhängige Produktgarantie        |                                 |
| 7. Ressourceneffizienz                      |                                 |

Bild 81: identifizierte Geschäftsmodelle

Die folgenden Beispiele zeigen die Art der Beschreibung:

**Beispiel 1: Nutzungsabhängige Vergütung**

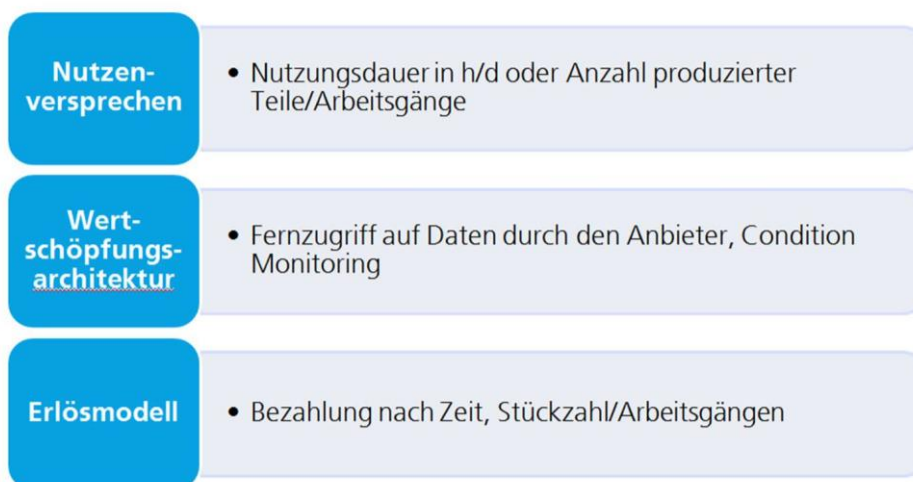


Bild 82: Geschäftsmodell nutzungsabhängige Vergütung

**Beispiel 2: Verkürzung der Inbetriebnahmezeit**

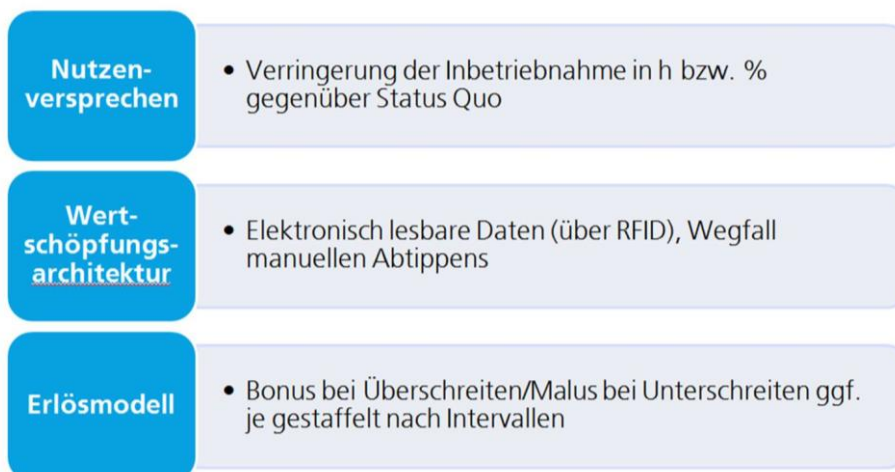


Bild 83: Geschäftsmodell Verkürzung der Inbetriebnahmezeit

### 11.5 Diskussion und Konkretisierung der Geschäftsmodelle

Im Rahmen von strukturierten Kleingruppen-Workshops wurden zunächst die Punkte: Aktueller Informationsrückfluss und Informationsverwertung, Anvisierte Datenverwendung, Kundenwert/eigener Nutzen und der „Daten-Nutzen“ diskutiert, um dann Ideen für „eigene“ Geschäftsmodelle zu entwickeln und diese auf Passfähigkeit hin zu prüfen.

**Geschäftsmodell-Workshops mit den Komponentenherstellern:**

- Schunk  } Karlsruhe, 23.03.2015
- MAG/Corcom  }
- Romai  }
- Steinmeyer  Karlsruhe, 10.04.2015
- Kessler,  Bad Buchau, 27.04.2015



**Geschäftsmodell-Workshops mit den Anlagenherstellern:**

- MAG  Eisingen, 30.04.2015
- MOC  Ammerbuch, 24.06.2015



Bild 84: Erarbeitung von Geschäftsmodellen mit den Projektpartnern

Jeder Projektpartner konnte mindestens ein potenzielles Geschäftsmodell identifizieren. Die Geschäftsmodelle sind im Projektkontext als sehr passfähig anzusehen und besitzen unterschiedliche Anforderungen an die Hard- und Software. Bereits in diesem Rahmen konnten erste Ideen zur unternehmensspezifischen Ausgestaltung der Geschäftsmodelle erarbeitet werden. Genaue Inhalte der Ideen können aus Gründen des Wettbewerbsschutzes der beteiligten Unternehmen nicht genannt werden.

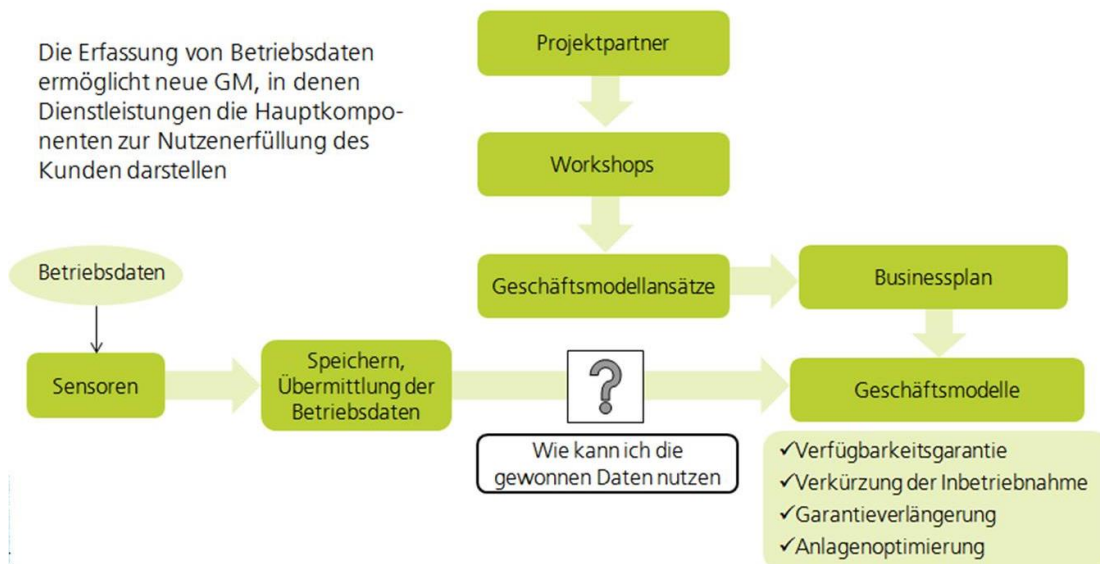


Bild 85: Wie werden aus Betriebsdaten Geschäftsmodelle

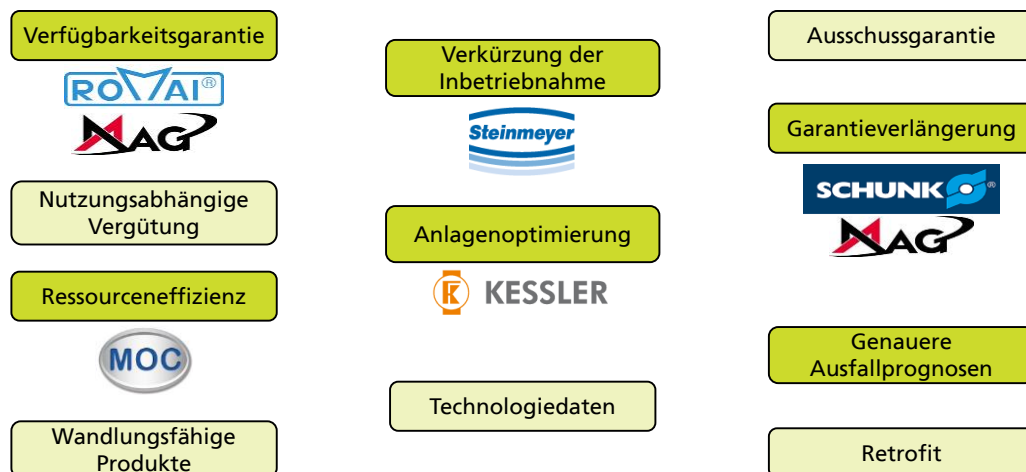


Bild 86: Geschäftsmodelle für die Projektpartner

### 11.5.1 Bewertungsmethode

Im Rahmen des Projektes kam die Frage nach der Bewertung von Geschäftsmodellen auf - welche Alternative ist für ein Unternehmen zu präferieren, insbesondere, wenn eine Entwicklung in verschiedene Richtungen möglich ist? Der zentrale Ansatzpunkt für jegliche Bewertungs- und Entscheidungsfragen ist das digitale Dienstleistungskonzept selbst: Ein solches umfasst stets drei Dimensionen: Die Wertschöpfungsarchitektur, das Nutzenversprechen und das Ertragsmodell. Lediglich die Erträge sind der rein quantitativen Prognose und Messung zugänglich. Der realisierbare Nutzen dagegen ist vielschichtig und nur schwer zu quantifizieren. Als Beispiele mögen hier die geringeren und planbaren Ausfallzeiten der Maschinen beim Kunden im Falle des condition monitoring oder auch die besseren Möglichkeiten der Personaleinsatzplanung für Servicemitarbeiter seitens des Anbieters dienen. Viel genannt ist auch der Datenrückfluss zum Anbieter zwecks Generierung von Betriebsdaten für Zulassungszwecke z. B. im Bereich der Arbeitssicherheit (Fallzahlen als Indiz) oder Kenntniserlangung über die Einsatzbedingungen von Komponenten zum Zweck der Produkt(weiter)entwicklung und Individualisierung. Neben direkten Nutzen sind auch indirekte Nutzen auf andere Unternehmensbereiche / -Produkte zu verzeichnen, die sich ebenfalls nur schwer messen lassen.

Dies führt zu der Notwendigkeit, ein neues Geschäftsmodell auch strukturiert und in verschiedenen Dimensionen zu bewerten, um die Vorteilhaftigkeit für das Unternehmen feststellen zu können, bzw. um eine Entscheidung zwischen verschiedenen Modellen fundiert treffen zu können. Für die Arbeit mit Geschäftsmodellen, hat sich in der Praxis die Business-Model-Canvas-Methode (BMC) von Osterwalder und Pigneur bewährt. "Sie gilt mittlerweile weltweit als Mittel der Wahl, um innovative Geschäftsmodelle zu finden und veraltete auf den Kopf zu stellen"<sup>52</sup>. Diese Methode liefert neun für Geschäftsmodelle gleichermaßen relevante Felder und damit auch zugleich einen ersten Anhaltspunkt für Zielkriterien zur Bewertung von Industrie 4.0-Geschäftsmodellen. So können Aussagen zu den Kundenbeziehungen und Kundenwerten, den Finanzen und den Ressourcen des Unternehmens getroffen werden.

Im BMC-Modell zeichnen sie sich wie folgt ab: Das Ertragsmodell umfasst die Felder Kostenstruktur und Einnahmequellen und damit das strategische Ziel der Wirtschaftlichkeit. Das zweite Oberziel ist die Markterschließung, welche durch die BMC-Felder Kundensegmente,

<sup>52</sup> Osterwalder/Pigneur 2013 [45]

Kundenbeziehungen und Kanäle dargestellt wird. Als drittes Ziel wird abweichend vom gängigen Begriff der Produktivität der Kompetenz(zu)gewinn benutzt, welcher durch die verbleibenden BMC-Felder der Schlüsselressourcen, -aktivitäten und -partner dargestellt wird. Ein Kompetenz(zu)gewinn gerade im Bereich der neuen Geschäftsmodelle zielt nämlich direkt auf die Steigerung der unternehmerischen Produktivität und damit auf die Leistungsfähigkeit ab.

### OBERZIELE IM BUSINESS MODEL CANVAS

#### Kompetenzgewinn

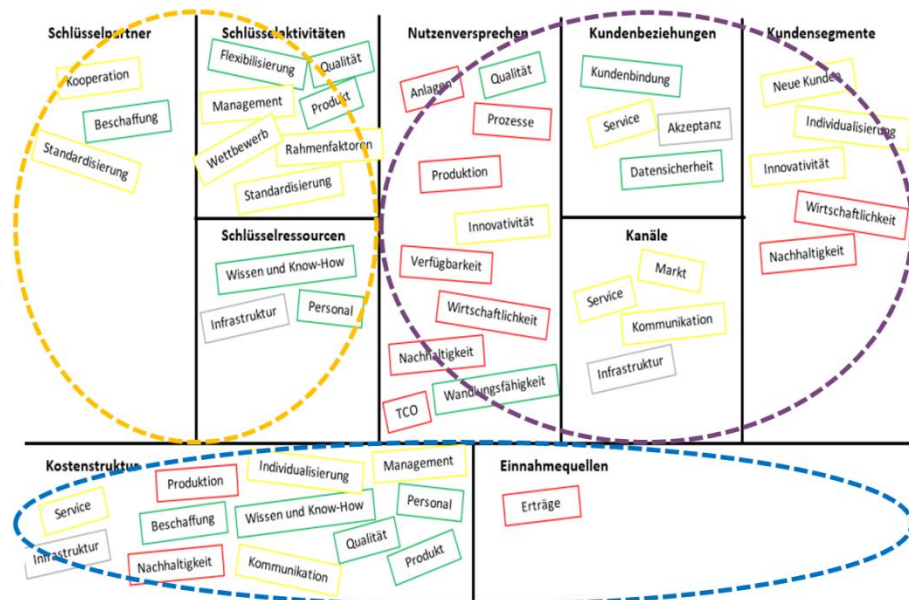
- 6. Schlüsselaktivitäten
- 7. Schlüsselpartner
- 8. Schlüsselressourcen

#### Markterschließung

- 3. Kanäle und Kundenbeziehungen
- 4. Kundensegmente
- 5. Nutzenversprechen

#### Wirtschaftlichkeit

- 1. Einnahmequellen
- 2. Kostenstruktur



(In Anlehnung an: Otserwalder, A.; Pigneur, Y.: Business Model Generation (2010))

Bild 87: Oberziele im Business Model Canvas

Darüber hinaus stellt sich jedoch die Frage, inwiefern das Modell ebenso dazu dienen kann, verschiedene Geschäftsmodelle miteinander zu vergleichen. In der Praxis liegen oftmals nur sehr wenige „belastbare Daten“ dazu vor: Umsatzerwartungen und/ oder Zeiteinsparungen oder eine bessere Planbarkeit der Reparaturarbeiten zu prognostizieren, gleicht einem Blick in die Glaskugel, hingegen sind Investitionen in die Technologie und/oder in Personal leichter zu beziffern.

Als geeigneter Ansatz zur Bewertung von Werten unterschiedlicher Natur wurde die multikriterielle Bewertung gewählt. Die identifizierten Ziele sind sowohl qualitativer als auch quantitativer Natur und müssen somit mit verschiedenen Skalen gemessen werden. Beispielsweise können Kosten, Zeiten und Veränderungen mit Zahlen (kardinalskaliert) bemessen werden, während Risiken, Fähigkeiten, Potenziale und Beurteilungen mit Worten beschrieben werden können. Eine Kombination solch verschiedener Ziele erlauben Outranking-Verfahren wie PROMETHEE oder ELECTRE. Das genutzte PROMETHEE-Verfahren ermittelt in seiner Anwendung aus den Kriterienausprägungen, dem gewichteten Mittel der zugehörigen Präferenzfunktionen und dem Gewicht, welches die Wichtigkeit des Zielkriteriums gegenüber den anderen Zielkriterien ausdrückt, eine Outranking-Relation. Damit wird eine Aussage über die betrachtete Alternative getroffen, welche zeigt, inwieweit diese von anderen Alternativen dominiert wird.

Eine Anwendungsmöglichkeit, die im Projekt erfolgreich erprobt wurde, sieht so aus, dass aus den Zielen Fragen abgeleitet werden, deren Beantwortung mit Hilfe der verschiedenen Skalen möglich und erforderlich ist. Zusätzlich wählt der Entscheider einen individuellen

Schwerpunkt seiner Optimierung aus den Oberzielen Wirtschaftlichkeit, Kompetenzgewinn und Markterschließung. Anhand dieser Schwerpunktsetzung ist eine systemgestützte Vorgewichtung der zugehörigen Ziele möglich. Diese Vorgewichtung kann jedoch durch die individuelle Beurteilung des Entscheiders im Rahmen jeder einzelnen Frage noch beeinflusst werden.

Die Ausgabe des Ergebnisses erfolgt als ein Präferenzwert. Je näher der Wert an 0 und je weiter er von 1 entfernt ist, desto schwerer ist es, eine eindeutige Handlungsempfehlung auszusprechen. Daher bietet sich eine inhaltliche Verfeinerung der Ergebnisdarstellung ebenso an wie eine grafische Ausgabe zur Visualisierung der Ergebnisse, wie in Bild 88 dargestellt. Im ersten Fall (links) ergibt sich keine Präferenz, die digitalen Dienstleistungskonzepte sind gleichwertig hinsichtlich der gewählten Fokussierung. Im zweiten Fall (Mitte) ergibt sich eine schwache Präferenz des „blauen“ Modells im Bereich der eigenen Einnahmequellen und im dritten Fall eine deutliche Präferenz des „roten“ Modells in allen Bereichen, besonders deutlich jedoch im Bereich der eigenen Schlüsselpartner. Es bietet sich an, diese Art der Interpretation auf der Ebene der drei Oberziele weiter zu vertiefen, um die spezifischen Stärken und Schwächen der Geschäftsmodelle besser identifizieren und anschließend die Modelle verfeinern und weiterentwickeln zu können. Eine noch tiefergehende Betrachtung auf der Detailebene aller 47 Zielkriterien erscheint hingegen nicht sinnvoll.

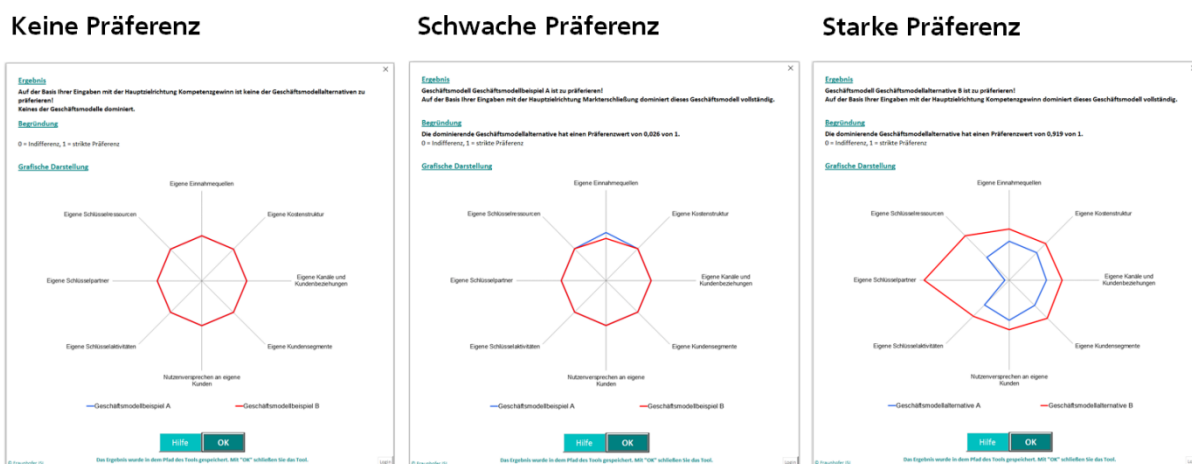


Bild 88: Visualisierung der Präferenz

Als Beispiel für die Aussagekraft mag ein Ergebnis dienen, welches von einem Geschäftsmodell in den Bereichen Wirtschaftlichkeit und Markterschließung dominiert wird. Das Konzept ist sehr fokussiert auf den Kunden, was jedoch mit einer hohen Beanspruchung der eigenen Ressourcen und finanziellen Mittel einhergeht und wenig Synergiepotenziale durch externe Partner bietet. Jedoch sind die Chancen auf hohe Einnahmen und Ausweitung der Kundenstruktur mit hervorragend bewertet worden, so dass dieses Geschäftsmodell für eine angestrebte Markt-Pull-Strategie geeignet ist.

Als Ergebnis lässt sich daher festhalten, dass eine sinnvolle Bewertung von Industrie 4.0-Geschäftsmodellen im Maschinen- und Anlagenbau über die identifizierten Ziele und mit Hilfe der entwickelten Bewertungsmethode sinnvoll und möglich ist.

### 11.5.2 Businesspläne

Im Projekt wurden zwei ausgewählte Geschäftsmodellideen bis zur Umsetzungsreife weiterentwickelt und in Form je eines Businessplans dokumentiert. Die erste Idee betrifft die Res-



sourceneffizienz beim Anlageneinsatz der Anlagen von MOC Danner: Das Problem ist, dass viele Unternehmen ihre Reinigungsanlagen nicht mit optimalen Parametern betreiben. Sie verschwenden Ressourcen und erzeugen übermäßig viel Abwasser. Die Komponenten der Reinigungsanlage werden stärker beansprucht als erforderlich und erreichen somit schneller das Ende ihrer Lebensdauer. Der Lösungsansatz liegt darin, das Nutzungsverhalten des Kunden kennenzulernen, zu analysieren und ihm aktiv eine Lösung anzubieten, die zu messbaren Einsparungen an Ressourcen führt. Dabei zeigt die Erfahrung des Herstellers, dass für ein qualitativ gleichbleibendes Reinigungsergebnis meist ein deutlich geringerer Ressourceneinsatz ausreichend ist. MOC Danner verfügt sowohl über die Erfahrungswerte, als auch über das technische Know-how eine Optimierung der Betriebsparameter herbeizuführen, benötigt hierfür jedoch umfassende Betriebsdaten des Kunden. Mit Hilfe eines mobilen Datenerfassungskoffers werden diese kurzfristig im direkten Anlagenbetrieb erfasst, anschließend ausgewertet und zu einer individuellen Kundenempfehlung ausgearbeitet.

Das zweite Geschäftsmodell soll das Problem lösen, das die Produkte des Unternehmens, wie z. B. Greifarme, aufgrund fehlender Kenntnisse beim Einkäufer des Kunden oftmals überdimensioniert werden. Zudem erfolgt ein zu früher Austausch, da die Minimierung des Ausfallrisiko für den Kunden Priorität hat. Für den Anbieter erschweren derzeit ein fehlendes Feedback sowie große Sicherheitsbedenken bezüglich der Offenlegung von Betriebsdaten auf Kundenseite, eine Verbesserung der Produkte. Das Geschäftsmodell setzt genau dort an: Der Hersteller bietet seinen Kunden eine Funktionsgarantie für Greifer, die auch sämtliche Ersatz- und Verschleißteile innerhalb der Garantiezeit umfasst und somit zu einer erhöhten Planungssicherheit beim Kunden führt. Im Gegenzug erhält der Hersteller protokollierte und gespeicherte Betriebsdaten zum Einsatz der Greifer über den Zeitraum der Funktionsgarantie. Der Folgekauf eines einsatzoptimierten Greifers kann dann zudem vergünstigt erfolgen.

Die Businesspläne selbst enthalten sensitive Unternehmensdaten und können daher hier nicht veröffentlicht werden.

### **11.5.3 Kompetenzentwicklung**

Die zunehmende Digitalisierung und Vernetzung der Produktion sowie die disziplinübergreifende Entwicklung von innovativen Technologien, Produkten und Dienstleistungen erfordern massive Veränderungen der Arbeitswelt im Verarbeitenden Gewerbe. Höhere Komplexität der Aufgaben, gesteigerte Anforderungen an die Leistungsfähigkeit und Flexibilität der Mitarbeiter sowie die Erfordernis von Kenntnissen aus verschiedenen Fachdisziplinen sind in diesem Zusammenhang als zentrale Herausforderungen zu nennen. Darüber hinaus wächst die Anzahl der unternehmensinternen und -externen Kommunikationsschnittstellen. Entsprechend ergeben sich dadurch gesteigerte Anforderungen an die Qualifikation und an spezielle Kompetenzen der Mitarbeiter, die in vielen Unternehmen erst noch aufgebaut werden müssen. Die Unternehmen können diese entweder zukaufen oder selbst aufbauen. Es gilt, gerade bei eigenständigem Kompetenzaufbau, Fortbildungs- und Mitarbeiterentwicklungskonzepte in die Unternehmensphilosophie und -strategie zu integrieren, um vorhandene Kompetenzen auf dem aktuellem Stand zu halten und den Aufbau neuer Kompetenzen zu unterstützen.

Wer rechtzeitig weiß, welche Mitarbeiter wo und mit welchen Kompetenzen benötigt werden und inwieweit diese bereits vorhanden sind, kann seine Strategie zur Erreichung des angestrebten Kompetenzlevels planen und rechtzeitig agieren. Ein strategisches Kompetenzma-

nagement ist dabei ein geeignetes Mittel, die unternehmerischen Entscheidungen zu unterstützen, um Unternehmen des Verarbeitenden Gewerbes für Industrie 4.0 zu wappnen.

Im Rahmen des Projektes entstand daher ein Leitfaden für die Verbundpartner zum Einstieg in ein systematisches Kompetenzmanagement. Dazu ist er inhaltlich an die Bedürfnisse und Anforderungen von KMU angepasst und stellt einige Ansätze und Methoden vor, die sowohl der Problematik im Maschinen- und Anlagenbau als auch der Unternehmensgröße angemessen sind. Nach einer kurzen Definition von Kompetenz und strategischem Kompetenzmanagement zeigen aktuelle Studien Zukunftsszenarien hinsichtlich des möglichen Kompetenzbedarfs für Industrie 4.0 auf. Auf dieser Grundlage werden für Industrie 4.0 relevante Kompetenzen ermittelt und Kompetenzprofile für verschiedene Funktionen erarbeitet. Anschließend wird aufgezeigt, wie sich die Interaktion zwischen den einzelnen Akteuren durch Industrie 4.0 verändern kann. Im Weiteren wird ein Vorgehensmodell zum strategischen Kompetenzmanagement vorgestellt. Zusätzlich werden Methoden und Instrumente des strategischen Kompetenzmanagements betrachtet. Abschließend werden Hinweise zur Entscheidungsfindung bezüglich der Kompetenzentwicklung in einem Unternehmen gegeben.

Beispielhaft wurde ein Kompetenzprofil für einen Facharbeiter / Maschinenführer erarbeitet (Bild 89):

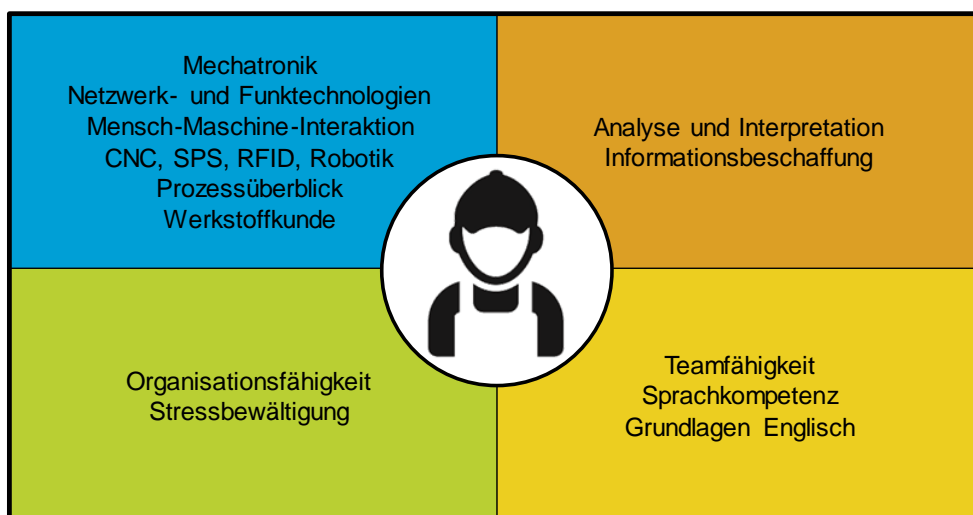


Bild 89: Kompetenzprofil Facharbeiter / Maschinenführer

Durch zunehmende Automatisierung und Hybridisierung der Produktionsprozesse ist mit einer Zunahme an Komplexität zu rechnen. Es ist eine Höherqualifizierung, insbesondere in Bereichen der Mechatronik, der Netzwerk- und Funktechnologien und der Robotik erforderlich. Zur Bedienung komplexer Maschinen werden zukünftig verstärkt Erfahrungen in CNC-Steuerung sowie speicherprogrammierbaren Steuerungen und Kenntnisse über RFID-Technologien benötigt. Hinsichtlich der Steuerung der Maschinen wird sich ein Wandel weg von der eigenständigen Interpretation, hin zur reinen Umsetzung der maschinell angezeigten Anweisungen und Informationen ergeben. Es wird der Fokus auf Qualitätssicherung verstärkt, was einen generellen Überblick über die Prozessabläufe, über den eigenen Fachbereich hinaus, nötig macht. Intelligente Werkstoffe müssen anders gehandhabt werden als bisherige, was Wissen um moderne Werkstoffkunde erfordert.

Zur Beseitigung von Störungen in komplexen Maschinen werden Fähigkeiten zur Analyse und Interpretation benötigt. Überfachlich werden fundierte Kenntnisse über Produktionsabläufe, Strukturen und Wertschöpfungsketten vorausgesetzt. Es werden verstärkt organisato-

rische, prozessuale und planerische Aufgaben zu erledigen sein, was Fähigkeiten wie Kommunikation, Interpretation, Selbstständigkeit, eigenständige Informationsbeschaffung und Fremdsprachenkompetenz erfordert. Um komplexere Sachverhalte verständlich zu vermitteln wird eine gewisse Sprachkompetenz im Sinne von Ausdrucksfähigkeit benötigt. Es werden quantitativ mehr Maschinen einzurichten und zu steuern sein und es kommen neue Aufgaben wie Softwarewartung und Einspielung von Software hinzu. Neue und komplexe Aufgaben sowie Mehrleistung erfordern ein hohes Maß an Organisationsfähigkeit und machen Kenntnisse über Methoden zur Stressbewältigung erforderlich.

Die komplette Präsentation zum Thema Kompetenzentwicklung ist abzurufen unter: <http://www.isi.fraunhofer.de/isi-de/t/projekte/be-securePLUGandWORK-Industrie-4.0.php>.

## 12 Literatur

- [1] VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik: Industrie 4.0 – Technical Assets. Grundlegende Begriffe, Konzepte, Lebenszyklen und Verwaltung, VDI Status-report Industrie 4.0, Nov. 2015.
- [2] OPC Unified Architecture for AutomationML, OPC UA Companion Specification, <https://opcfoundation.org/developer-tools/specifications-unified-architecture/opc-unified-architecture-for-automationml/>, February, 2016.
- [3] Schleipen, M.; Selyansky, E.; Henßen, R.; Bischoff, T.: Multi-level user and role concept for a secure plug & work based on OPC UA and AutomationML, IEEE Conference ETF A, Luxemburg, September, 2015.
- [4] OPC UA Specification: Part 2 – Security Model
- [5] Global Discovery Server V1.02 Part 12
- [6] Christoph Thomalla: Ontologie-basierte Erkennung von Cyber-Attacken. visIT IT-Sicherheit in der Produktion, S.12/13, ISSN 1616-8240, 2014.
- [7] Jörg Kippe: Cyber-Security in kritischen Infrastrukturen. visIT IT-Sicherheit in der Produktion, S.10/11, ISSN 1616-8240, 2014.
- [8] Abele, Eberhard; Kuske, Philipp; Lang, Horst (2011): Schutz vor Produktpiraterie. Ein Handbuch für den Maschinen- und Anlagenbau. Heidelberg.
- [9] Fuchs, Hans Joachim (2006): Piraten, Fälscher und Kopierer. Strategien und Instrumente zum Schutz geistigen Eigentums in der Volksrepublik China. Wiesbaden: Gabler.
- [10] Fusan, Carsten (Hrsg.) (2009): Managementmaßnahmen gegen Produktpiraterie und Industriespionage. 1. Aufl. Wiesbaden: Gabler
- [11] Krüger, Jörg; Nickolay, Bertram; Verhasselt, Jochen: Marken- und Produktpiraterie 2006 - Wahrnehmung von Marken- und Produktpiraterie und Akzeptanz technologischer Schutzinstrumente. Fraunhofer IPK. Berlin.
- [12] Sokianos, Nicolas P. (Hrsg.) (2006): Produkt- und Konzeptpiraterie erkennen, vorbeugen, abwehren, nutzen, dulden. Wiesbaden.
- [13] Kleine, Oliver (2010): Strategisches Management der Produktpiraterie – Qualitätssicherung in der Konzeption ganzheitlicher Schutzstrategien. In: Industrie Management 26 (4), S. 65–69.
- [14] Lightfoot, Howard W.; Gebauer, Heiko (2011): Exploring the alignment between service strategy and service innovation. In: Journal of Service Management (Vol. 22 No. 5), S. 664–683.
- [15] Roßnagel, Alexander (2009): Mobilität und Kontext - Zukunftsentwicklung der mobilen Kommunikation in Recht und Technik. In: Schriftenreihe des Instituts für Europäisches Medienrecht (EMR) (Band 38).
- [16] Wildemann, Horst; Ann, Christoph; Broy, Manfred; Günthner, Willibald A.; Lindemann Udo (2007): Plagiatschutz: Handlungsspielräume der produzierenden Industrie gegen Produktpiraterie. 1. Aufl. TCW Transfer-Centrum. München.

- 
- [17] Roßnagel, Alexander; Banzhaf, Jürgen; Grimm, Rüdiger (2003): Datenschutz im Electronic Commerce. Technik - Recht - Praxis. Heidelberg: Verlag Recht und Wirtschaft GmbH (Schriftenreihe Kommunikation und Recht, 18).
- [18] Dressel, Christian; Scheffler, Hauke (Hg.) (2003): Rechtsschutz gegen Dienstpiraterie. München.
- [19] Lux, Christian; Peske, Thorsten (2002): Competitive Intelligence und Wirtschaftsspionage. Analyse, Praxis, Strategie. 1. Aufl. Wiesbaden: Gabler.
- [20] Hummelt, Roman (1997): Wirtschaftsspionage auf dem Datenhighway. Strategische Risiken und Spionageabwehr. München: Hanser.
- [21] Mattern, Friedemann (2003): Vom Verschwinden des Computers – Die Vision des Ubiquitous Computing. In: Friedemann Mattern (Hg.): Total vernetzt. Szenarien einer informatisierten Welt. Berlin, Heidelberg [u.a.]: Springer, S. 1–42.
- [22] Körner, Mike (2002): E-Service-Support im Maschinen und Anlagenbau. Ausgewählte Aspekte zum erfolgreichen Management von e-Service-Leistungen. Frankfurt am Main: VDMA-Verlag
- [23] Brentani, Ulrike de (2001): Innovative versus incremental new business services: Different keys for achieving success. In: Journal of Product Innovation Management 18, S. 169–187.
- [24] Büllesbach, Alfred (2002): Premium Privacy. In: v. Mutius, Helmut Bäumler und Albert von Mutius (Hg.): Datenschutz als Wettbewerbsvorteil. Privacy sells: Mit modernen Datenschutzkomponenten Erfolg beim Kunden. 1. Aufl. Neuwied: Vieweg (DuD-Fachbeiträge), S. 45–57.
- [25] Gillert, Olaf (2006): Juristische Gesichtspunkte der Produkt- und Konzeptpiraterie. In: Nicolas P. Sokianos (Hg.): Produkt- und Konzeptpiraterie erkennen, vorbeugen, abwehren, nutzen, dulden. Wiesbaden, S. 205–222.
- [26] Gabler Verlag (Hrsg.): Gabler Wirtschaftslexikon. Stichwort: Ausspähen von Daten. Online verfügbar unter <http://wirtschaftslexikon.gabler.de/Archiv/606/ausspaehen-von-daten-v7.html>, zuletzt geprüft am 01.02.2013.
- [27] Kotarski, David (2014): Fabriksicherheit für Industrie 4.0. In: PRODUCTIVITY Management (19), S. 25–27.
- [28] Schaar, Peter (2006): Datenschutz im Spannungsfeld von Privatsphärenschutz, Sicherheit und Informationsfreiheit. In: RDV (1), S. 1–5.
- [29] Meissinger, Jan (2005): Gefahren und Bedrohungen durch Wirtschafts- und Industriespionage in Deutschland. Hamburg.
- [30] Gounalakis, Georgios (2003): Rechtshandbuch Electronic Business. München.
- [31] Hassemer (1981): Schutzbedürftigkeit des Opfers und Strafrechtsdogmatik. Berlin.
- [32] Tinnefeld, Marie-Theres; Ehmman, Eugen; Gerling, Rainer W. (2005): Einführung in das Datenschutzrecht. Datenschutz und Informationsfreiheit in europäischer Sicht. 4. Aufl. München: Oldenbourg.

- [33] Scholz, Philip (2003): Datenschutz beim Internet-Einkauf. Gefährdungen-Anforderungen-Gestaltungen. 1. Aufl. Baden-Baden: Nomos (Der elektronische Rechtsverkehr, 8).
- [34] Datenschutzrecht. Handkommentar, Bundesdatenschutzgesetz, Datenschutzgesetze der Länder und Kirchen, Bereichsspezifischer Datenschutz. 45. EL 2012. Begründet von Lutz Bergmann, Roland Möhrle und Armin Herb. Stuttgart, München: R. Boorberg.
- [35] Hoeren, Thomas (2013): Internetrecht. Stand Oktober 2013. Universität Münster. Münster. Online verfügbar unter [http://vg01.met.vgwort.de/na/0347f56c827c491aa8d5783d2670a0e4?l=http://www.uni-muenster.de/Jura.itm/hoeren/itm/wp-content/uploads/Skript-Internetrecht\\_Oktober2013.pdf](http://vg01.met.vgwort.de/na/0347f56c827c491aa8d5783d2670a0e4?l=http://www.uni-muenster.de/Jura.itm/hoeren/itm/wp-content/uploads/Skript-Internetrecht_Oktober2013.pdf), zuletzt geprüft am 3.1.14.
- [36] Theißen, Sascha (2009): Risiken informations- und kommunikationstechnischer (IKT-) Implantate im Hinblick auf Datenschutz und Datensicherheit. Karlsruhe.
- [37] Spindler, Gerald (2007): Verantwortlichkeit von IT-Herstellern, Nutzern und Intermediären. Gutachten im Auftrag des BSI. o.O. Online verfügbar unter [https://www.bsi.bund.de/ContentBSI/Publikationen/Studien/recht/Gutachten\\_pdf.pdf](https://www.bsi.bund.de/ContentBSI/Publikationen/Studien/recht/Gutachten_pdf.pdf), zuletzt geprüft am 19.12.2011.
- [38] Müller, Stefan (2011): Der Schutz von Unternehmensgeheimnissen. In: Jürgen Ensthaller und Patrick Wege (Hg.): Management geistigen Eigentums. Die unternehmerische Gestaltung des Technologieverwertungsrechts. 1. Aufl. Berlin: Springer, S. 111–136.
- [39] Welser v., Marcus; González, Alexander (2006): Marken- und Produktpiraterie : Strategien und Lösungsansätze zu ihrer Bekämpfung. Weinheim: Wiley.
- [40] Ann, Christoph (2007): Know-how - Stiefkind des Geistigen Eigentums. In: GRUR, S. 39–43.
- [41] Brenner, Christian (2006): Schutzmaßnahmen gegen Produktpiraterie in der Praxis. In: Nicolas P. Sokianos (Hg.): Produkt- und Konzeptpiraterie erkennen, vorbeugen, abwehren, nutzen, dulden. Wiesbaden, S. 275–290.
- [42] Kleine, Oliver (2010): Strategisches Management der Produktpiraterie – Qualitätssicherung in der Konzeption ganzheitlicher Schutzstrategien. In: Industrie Management 26 (4), S. 65–69.
- [43] Schuster, Leopold (2000): Die Grenzen polizeilicher Ermittlungen. In: Helmut Bäumler (Hg.): E-Privacy. Datenschutz im Internet. 1. Aufl. Braunschweig, Wiesbaden: Vieweg, S. 77 ff.
- [44] Roßnagel, Alexander (2007): Datenschutz in einem informatisierten Alltag. Gutachten im Auftrag der Friedrich-Ebert-Stiftung. Berlin.
- [45] Osterwalder, A.; Pigneur, Y.: Business Model Generation: Ein Handbuch für Visionäre, Spielveränderer und Herausforderer, Campus Verlag.

### 13 Abbildungsverzeichnis

Bild 1: Herausforderung der ‚Sprachvielfalt‘ in der Produktion .....	6
Bild 2: Komponentenintegration am Beispiel von Werkzeugmaschinen heute und morgen .....	7
Bild 3: Projektpartner .....	9
Bild 4: Komponenten/Bausteine der Architektur (1) .....	13
Bild 5: Komponenten/Bausteine der Architektur (2) .....	14
Bild 6: Schaltung zur Spannungsversorgung des Adapters .....	16
Bild 7: Pegelerweiterung der analogen Spannungsmesseingänge .....	17
Bild 8: Schaltplanausschnitt der umschaltbaren Eingangslogik.....	18
Bild 9: Pegelumschaltung zwischen 24 V- und TTL-Logik .....	18
Bild 10: Konstruktion und Realisierung des SecurePLUGandWORK-Adapters.....	19
Bild 11: Beispielintegration des SecurePLUGandWORK-Adapters (BBB) per WLAN ..	21
Bild 12: Herkunftsbranchen der Umfrageteilnehmer .....	23
Bild 13: Unternehmensgröße.....	23
Bild 14: Wunsch nach Datennutzung eindeutig.....	24
Bild 15: Vermutete Nutzenpotentiale bei den Umfrageteilnehmern .....	24
Bild 16: Datenbasiertes Condition Monitoring als Haupteinsatzfeld .....	24
Bild 17: Planung des Einsatzes Industrie 4.0-basierter Geschäftsmodelle.....	25
Bild 18: Durchgängige Kommunikation geplant oder umgesetzt .....	25
Bild 19: Einsatz von Fernwartung bei den Umfrageteilnehmern.....	25
Bild 20: Einsatz autonomer Systeme bei den Umfrageteilnehmern.....	26
Bild 21: Eingesetzte SPSen bei den Umfrageteilnehmern .....	26
Bild 22: Grad der Vernetzung von Maschinen .....	26
Bild 23: Skepsis bei Einsatz von Clouds .....	27
Bild 24: Eingesetzte Protokolle .....	27
Bild 25: Gewünschte Eigenschaften von Adapters .....	28
Bild 26: Zahlungsbereitschaft für eine nachträgliche Vernetzung.....	28
Bild 27: Untersuchte Adapterlösungen .....	29
Bild 28: Unterstützte Feldbusse der Adapter (1) .....	29
Bild 29: Unterstützte Feldbusse der Adapter (2) .....	29
Bild 30: Funktionalität Integrationsserver .....	30
Bild 31: BeagleBoneBlack (BBB) .....	32
Bild 32: Übersicht der implementierten Schnittstellen .....	33
Bild 33: Logische Architektur einer Automatisierungsanwendung (Quelle: VDE/VDI Richtlinie 2657 „Middleware in der Automatisierungstechnik“) .....	34
Bild 34: Technische Architektur der Middleware (Quelle: VDE/VDI Richtlinie 2657 „Middleware in der Automatisierungstechnik“) .....	35

---

Bild 35: Varianten der CodeMeter-HW/SW-Komponenten für den Einsatz an Maschinen oder in der IT-Security .....	36
Bild 36: Licence Central in SecurePLUGandWORK .....	38
Bild 37: Optionen und Ausprägungen der CodeMeter-Technologie, die in SecurePLUGandWORK genutzt wurden .....	39
Bild 38: Kugelgewindetrieb mit aufgebrachtem RFID-Chip .....	39
Bild 39: Zugriffsbeschränkungen für einen Nutzer (rot markiert, links) oder eine Anwendung (rot markiert, rechts).....	43
Bild 40: Abgesicherter Kommunikationskanal (SecureChannel, rot markiert) zwischen zwei Applikationen, betrieben durch zwei unterschiedliche Nutzer .	43
Bild 41: E-SPECHT 600 (vollelektrische Maschine).....	46
Bild 42: Verknüpfung zwischen Komponenten und Werkzeugmaschine .....	50
Bild 43: Probanden.....	50
Bild 44: Eingebaute Probanden .....	51
Bild 45: Temperaturverlauf bis Beharrung .....	51
Bild 46: PT1000 Temperaturkurve .....	52
Bild 47: zerlegte Spindel (links) und Statorpaket inklusive Sensoren (rechts) .....	52
Bild 48: Spindel im Verguss (links) und fertig montierter Prototyp (rechts).....	53
Bild 49: Einfaches Hüllenmodell der Spindel .....	53
Bild 50: Detailliertes Hüllenmodell .....	54
Bild 51: Kessler Versuchsaufbau .....	55
Bild 52: zu tauschende Spindeln zweier unterschiedlicher Hersteller mit SecurePLUGandWORK-Adaptern .....	56
Bild 53: Prinzipbild eines Winkelbohrkopfes .....	57
Bild 54: Beispiel eines 2-Achs-Vorsatzkopfes .....	58
Bild 55: Architekturbild Werkzeugmagazin.....	59
Bild 56: Datenentstehung und Übertragung im Lebenszyklus eines Kugelgewindetriebs .....	60
Bild 57: Position des RFID-Datenträgers in der KGT-Mutter .....	62
Bild 58: Kommunikationsablauf im Anwendungsbeispiel KGT .....	62
Bild 59: Einordnung des KGT im Anwendungsfall Werkzeugmaschine.....	63
Bild 60: Aufbau des Prüfstands zur Vermessung von Kugelgewindetrieben .....	64
Bild 61: Einplatinenrechner BeagleBone und Prüfstandsaufbau zur Messung der Wegabweichungen .....	64
Bild 62: Wegabweichungen für einen im Projekt untersuchten KGT .....	64
Bild 63: Aufbau zur Messung des Reibmoments .....	65
Bild 64: Verlauf des Reibmoments für einen im Projekt untersuchten Kugelgewindetrieb .....	65
Bild 65: Industriewaschmaschine bestehend auf vier Modulen .....	66
Bild 66: Aus mehreren Modulen bestehende Anlage .....	66



---

Bild 67: Übersicht Komponenten und Schnittstellen Demonstrator 2 MOC Danner – Dolphin .....	67
Bild 68: SecurePLUGandWORK-Architektur zur Integration von Anlagenteilen an überlagerte IT-Systeme .....	68
Bild 69: Übersicht Security-Komponenten auf Steuerungs-/ HW-Modulebene .....	69
Bild 70: Schematische Darstellung des SecurePLUGandWork Adapters mit integrierter Funktionsüberwachung für den robusten Betrieb. Bei den SCHUNK spezifischen Demonstratoren wurde vom linken Teil des SecurePLUGandWORK-Adapters lediglich die CANopen-Konnektivität verwendet. ....	70
Bild 71: Gesamtaufbau Roboterprüfstand.....	72
Bild 72: Würfel-Endeffektor mit Muster für die Bildverarbeitung .....	72
Bild 73: Prinzip der Eckpunkterkennung .....	74
Bild 74: Kamerabild nach der Verarbeitung .....	74
Bild 75: Realisierte Komponenten des Schunk-Demonstrators.....	75
Bild 76: Visuelle Darstellung der Untersuchung von Industrie 4.0-spezifischen Geschäftsmodellen für SCHUNK .....	77
Bild 77: SmartFactoryOWL (siehe auch <a href="http://www.smartfactory-owl.de">www.smartfactory-owl.de</a> ) .....	78
Bild 78: Vorgehen zur Generierung von Geschäftsmodellen in Projekt.....	79
Bild 79: Ergebnisse der Literaturanalyse .....	80
Bild 80: Definition Geschäftsmodell .....	91
Bild 81: identifizierte Geschäftsmodelle .....	92
Bild 82: Geschäftsmodell nutzungsabhängige Vergütung.....	92
Bild 83: Geschäftsmodell Verkürzung der Inbetriebnahmezeit.....	92
Bild 84: Erarbeitung von Geschäftsmodellen mit den Projektpartnern .....	93
Bild 85: Wie werden aus Betriebsdaten Geschäftsmodelle .....	93
Bild 86: Geschäftsmodelle für die Projektpartner .....	94
Bild 87: Oberziele im Business Model Canvas.....	95
Bild 88: Visualisierung der Präferenz.....	96
Bild 89: Kompetenzprofil Facharbeiter / Maschinenführer.....	98