

Die Smart Factory und ihre Risiken

Frank Herrmann

Ostbayerische Technische Hochschule Regensburg (OTH Regensburg)
Innovationszentrum für Produktionslogistik und Fabrikplanung
Postfach 120327
93025 Regensburg
E-Mail: Frank.Herrmann@OTH-Regensburg.de

Schlüsselwörter

Industrie 4.0, Smart Factory, Risiken

Abstrakt

In dieser Arbeit werden die Risiken einer Smart Factory untersucht und dargestellt, um den Status der Realisierung von Smart Factories aufzuzeigen. Dazu werden im Detail die entscheidenden technischen Komponenten vorgestellt und im Hinblick auf ihre Risiken analysiert. Generell wird eine ganzheitliche Sichtweise auf eine Smart Factory eingenommen. Ganzheitlich werden die ökonomischen Risiken erhoben. Diese komplette Risikoanalyse zeigt, dass der größte Handlungsbedarf im technologischen Bereich liegt. Dabei wurden die Themen Standardisierung, Informationssicherheit, Verfügbarkeit der IT-Infrastruktur, Verfügbarkeit von schnellem Internet und komplexen Systemen als am Wichtigsten eingestuft, und diese werden im Detail weiter analysiert. Ebenso weiter analysiert werden die organisatorischen und finanziellen Risiken, welche ebenfalls eine wichtige Rolle bei einer Transformation in eine Smart Factory spielen.

1. Einleitung

Um den Kundenerwartungen in der heutigen Zeit gerecht zu werden, bedarf es selbst bei Losgröße eins einer flexibleren Produktion. Um dieses Ziel zu erreichen, sollte eine neue Stufe der Automatisierung durch die Einführung von Methoden der Selbstoptimierung, Selbstkonfiguration, Selbstdiagnose, Kognition und intelligenten Support der Arbeitnehmer bei ihrer zunehmend komplexen Arbeit realisiert werden. Dies wird unter dem Begriff "Smart Factory" oder „Industrie 4.0“ zusammengefasst. In einer traditionellen Fabrik ist die Bereitstellung von qualitativ hochwertigen Dienstleistungen oder Produkten mit möglichst geringen Kosten der Schlüssel zum Erfolg. Industriefabriken versuchen hierbei, so viel Leistung wie möglich zu erzielen, um sowohl ihren Gewinn zu steigern als auch ihren Ruf zu verbessern. Im Gegensatz dazu können Komponenten und Systeme in einer Fabrik der Industrie 4.0 zusätzlich zur Zustandsveränderung, Fehlerdiagnose, Selbstwahrnehmung und Selbstvorhersage lernen, wodurch dem Management ein besserer Einblick in den Status der Fabrik ermöglicht wird.

Darüber hinaus ermöglicht der Peer-to-Peer-Vergleich und die Verbindung von Zustandsinformationen aus verschiedenen Komponenten eine präzise Zustandsprognose auf Komponenten- und Systemebene und zwingen das Fabrikmanagement, die erforderliche Wartung zum bestmöglichen Zeitpunkt auszulösen, um eine Just-in-Time-Wartung zu ermöglichen und Ausfallzeiten nahe Null zu erreichen. Es existieren bereits viele Publikationen über die intelligente Fabrik – Literaturüberblicke sowie Analysen von Forschungsarbeiten. Diese Publikation erweitert die Literaturüberblicke, indem die Risiken einer Smart Factory, die aus eben den vorhandenen Publikationen gefolgert wurden, zusammengefasst und bewertet werden. Möglicherweise steigt dadurch das Bewusstsein für diesen Fertigungstrend – vor allem für Anwender.

Der Rest dieser Arbeit ist wie folgt strukturiert. Zunächst werden Smart Factory bzw. Industrie 4.0 vorgestellt. Als nächstes werden die Technologien innerhalb einer Smart Factory erläutert. Dabei wird besonders auf Künstliche Intelligenz eingegangen. In Abschnitt 4 werden die Risiken, basierend auf einer Literaturübersicht, für diese Technologien aufgelistet und analysiert. Abschließend werden einige Schlussfolgerungen gezogen.

2. Industrie 4.0

In der industriellen Revolution, s. auch die Abbildung 1, brachte die Dampfmaschine, das Fließband und der Computer tiefgreifende wirtschaftliche Veränderungen. Nun stehen wir vor dem nächsten gewaltigen industriellen Wandel, der sogenannten 4. Industriellen Revolution oder kurz, Industrie 4.0.

Die Idee der vierten industriellen Revolution besteht darin, dass sich die Produktion mit modernsten Informations- und Kommunikationstechniken verzahnt. So entsteht die Möglichkeit, Produkte nach individuellen Kundenwünschen zu fertigen und diese in Losgröße eins zum Preis von Massenware zu produzieren. Die technischen Grundlagen bilden intelligente, digital vernetzte Systeme und Produktionsprozesse. Des Weiteren bestimmt die Industrie 4.0 die gesamte Lebensphase eines Produktes. Sie befasst sich mit der Idee, der Entwicklung, der Fertigung, der Nutzung und der Wartung bis hin zum Recycling des Produktes (Bundesministerium für Wirtschaft und Energie).

Alle vier Revolutionsstufen haben eine Gemeinsamkeit. Sie haben alle eine Auswirkung auf das wirtschaftliche und das gesellschaftliche Leben. Ebenfalls steigt die Produktivität an und schafft Veränderung in den Arbeitsprozessen und Arbeitsbedingungen. Für die Industriemitarbeiter bedeutet dies, eine höhere Qualifikationsanforderung. Mit diesen Veränderungen muss auch in der bereits anstehenden vierten Revolution gerechnet werden; s. (Kelkar et al. 2014, S. 2).

Unternehmen einen hohen Digitalisierungsgrad ihrer Wertschöpfungskette. Aktuell nutzen bereits 20 Prozent der deutschen Unternehmen selbststeuernde Anlagen; s. (Bundesministerium für Wirtschaft und Energie).

Durch die stärkere, innerbetriebliche sowie überbetriebliche Vernetzung, wird eine völlig neue Art der wirtschaftlichen Produktion geschaffen. Dies stellt deutsche und weltweite Unternehmen vor großen Herausforderungen, da Industrie 4.0 alle Dimensionen, wie Technik, Or-

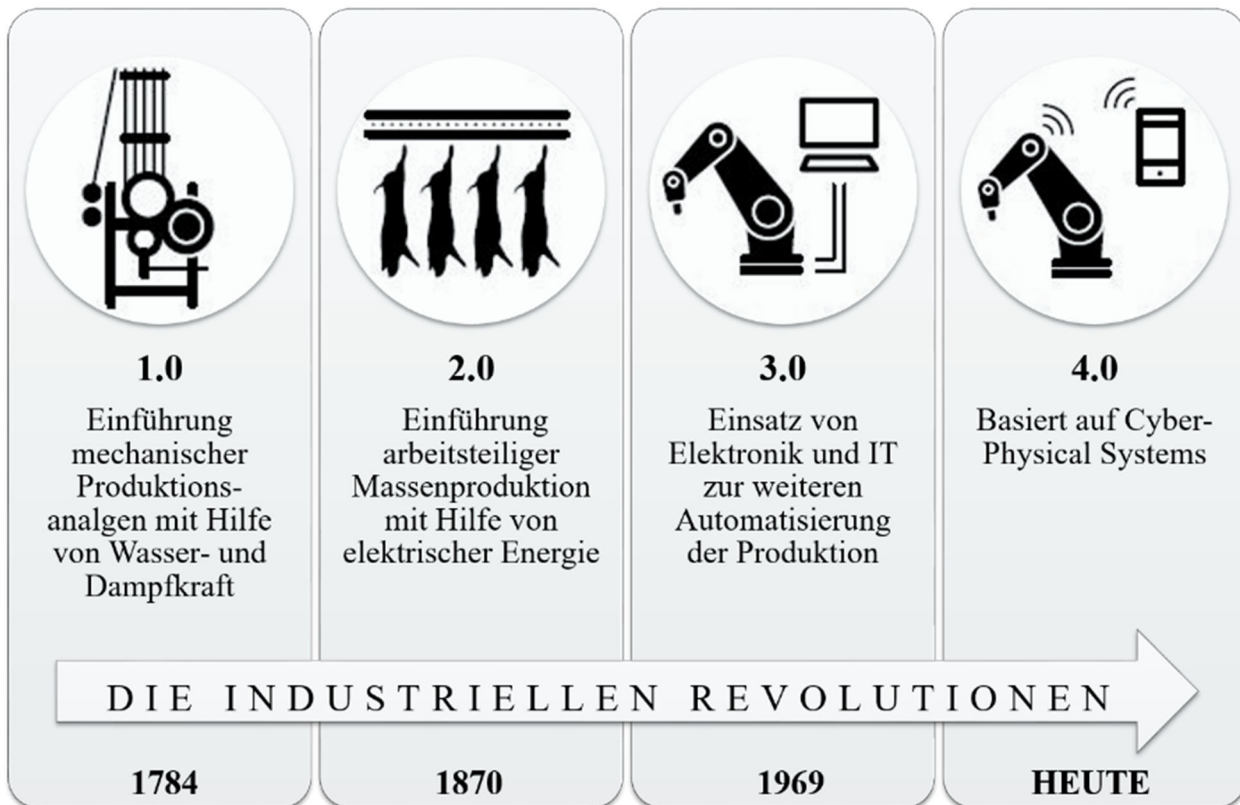


Abbildung 1: Industrielle Revolutionen im Überblick. (Eigene Darstellung)

Den Herausforderungen der Industrie 4.0 und der Umstellung der Produktion auf einen vernetzten Betrieb müssen sich deutsche Unternehmen stellen. Gelingt dies nicht, so besteht die Gefahr, dass deutsche Unternehmen den wirtschaftlichen Anschluss verlieren; s. (Bischoff 2015, S. 3).

Werden jedoch aktuelle Zahlen der Industrie 4.0 für den Standort Deutschland betrachtet, so lässt sich eine positive Entwicklung hin zur Industrie 4.0 erkennen. Laut dem Bundesministerium für Wirtschaft und Energie werden bis zum Jahr 2020 jährlich Investitionen von 40 Milliarden Euro in Industrie 4.0 Anwendungen geplant. Ebenfalls wird ein zusätzliches volkswirtschaftliches Wachstum von über 153 Milliarden Euro bis 2020 erwartet. Bis zum Jahr 2020 sehen 83 Prozent der deutschen

Unternehmen, Menschen und Geschäftsmodelle, betrifft; s. (Bischoff 2015, S. 1).

Um die Risiken und Herausforderungen für Unternehmen in der Industrie 4.0 genauer betrachten zu können, wird nun vorab die moderne Produktionsumgebung mit dem aktuellen technischen Stand beschrieben.

3. Technologien innerhalb einer Smart Factory

Im Zentrum der Industrie 4.0 steht die Smart Factory (intelligente Fabrik). Grundsätzlich geht es bei der Smart Factory um die Vernetzung von Maschinen und Anlagen mittels Software, so dass eine intelligente Kommunikation miteinander ermöglicht wird und die Arbeitsschritte automatisiert aufeinander abgestimmt werden können. Damit dies realisiert werden kann, müssen grundlegende

Technologien eingesetzt werden. Die technologischen Voraussetzungen werden in diesem Kapitel erläutert; s. (Zillmann 2016, S. 8).

Um die technischen Voraussetzungen einer Smart Factory aufzuzeigen, müssen vorerst die Cyber-Physical Systems (CPS), welche die Grundlage einer Smart Factory bilden, beschrieben werden; s. (Bauernhansl et al. 2014, S. 15f.). Das Schlagwort CPS tauchte erstmals in Amerika im Jahr 2006 auf. Systeme erhalten den Zusatz „Cyber“, wenn sie zur diskreten Verarbeitung von Informationen und zur Kommunikation genutzt werden. Daneben werden die realen Systeme als „physical“ bezeichnet. Dies bedeutet, die CPS sind autonom und können sich eigenständig konfigurieren und erweitern; s. (Jasperneite 2012). Ein weiteres wesentliches Merkmal der CPS ist, dass sie sich über offene und globale Informationsnetze, wie das Internet, verbinden können. Somit können sich Systeme beliebig koppeln, ihre Verbindungen während der Betriebszeit verändern, beenden und neu aufbauen. Es entsteht die Möglichkeit, verfügbare Daten, Informationen und Dienste an beliebiger Stelle im CPS bereitzustellen und zu verwenden; s. (VDI/VDE-Gesellschaft 2013, S. 2). CPS können Objekte, Produkte, Geräte, Gebäude, Produktionsanlagen oder Logistikkomponenten sein, die eingebettete Systeme enthalten; s. (Bauernhansl et al. 2014, S. 15f.).

Eingebettete Systeme bzw. Embedded Systems sind Mikroprozessoren oder kleine Rechner. Sie sind ein zentrales Thema bei der Umsetzung von CPS. Durch die Kombination von Hardware- und Softwarekomponenten wird das entsprechende System gesteuert, geregelt oder überwacht. Mit Hilfe dieser Technologie entstehen die oben beschriebenen flexiblen und intelligenten Systeme (CPS); s. (Mauerer 2016).

Die Embedded Systems sind mit *Sensoren* und *Aktoren* ausgestattet. Über Sensoren werden die Produktionsdaten erfasst. Die gesammelten Daten werden mit verfügbaren Daten und Diensten ausgewertet und abgespeichert. Durch die Verwendung von Aktoren besitzt ein CPS die Möglichkeit, physikalisch auf seine Umwelt einzuwirken; s. (Bauernhansl et al. 2014, S. 15f.). Die Kommunikation der CPS erfolgt über das Internet oder Intranet. Sie können Internetdienste nutzen und / oder diese selbst anbieten.

Die Bezeichnung *Internet of Things* (IoT) wurde im Jahr 1999 zum ersten Mal verwendet. Das klassische Internet wurde umfassend erweitert. Dies hat zur Folge, dass die virtuelle und reale Welt durch die Vernetzung von und mit Alltagsgegenständen, immer mehr miteinander verschmelzen. Physische Objekte (things) werden eindeutig identifizierbar, erhalten eine virtuelle Repräsentation und können über das Internet kommunizieren; s. (Mauerer 2016). Die Kommunikation erfolgt über offene und globale Informationsplattformen. Über diese Netze werden Dienste und Daten genutzt und zur Verfügung gestellt. Solche Dienste werden in der Literatur als *Internet of*

Things and Services (IoTS) bezeichnet. Es entsteht die Vision von adaptiven und flexiblen Produktionsanlagen, die sich selbst konfigurieren und teilweise selbst organisieren; s. (VDI/VDE-Gesellschaft 2013, S. 3).

Zur Steuerung von intelligenten Produktionsanlagen sind innerhalb einer Produktionsumgebung *Cyber Physical Production Systems* (CPPS) notwendig. Die Aufgabe des CPPS besteht darin, die einzelnen CPS zu koordinieren und die Veränderungen in der Produktion zu steuern (Huber 2016a, S. 39). Mit Hilfe dieser Plattform können die drei verschiedenen Internetarten miteinander verbunden werden. Im Internet des Menschen vernetzt sich der Mensch mit den sozialen Netzwerken. Des Weiteren gibt es das zuvor beschriebene Internet der Dinge (IoT) und das Internet der Dinge und Dienste (IoTS); s. (Bauernhansl et al. 2014, S. 16).

Auch wenn das Ziel der Smart Factory eine vernetzte, selbstorganisierte Produktionsumgebung ist, darf der Mensch in diesem Szenario nicht fehlen. Der Mensch muss weiterhin im Mittelpunkt stehen, wobei sich sein Aufgabengebiet allerdings sehr stark ändern wird. Hauptsächlich müssen Menschen kontrollierende Tätigkeiten wahrnehmen, während die operativen Aufgaben in den Hintergrund treten. Für die Ausführung dieser Tätigkeiten muss der Mensch über eine multimodale Schnittstelle, auch *Human-Machine-Interface* (HMI) genannt, mit den CPS verbunden sein; s. (Huber 2016a, S. 286). Ein CPS kann beispielsweise über Sprache oder Touch Displays gesteuert werden. Zukünftig kann der Mensch auch über Gesten entsprechend einwirken; s. (Bauernhansl et al. 2014, S. 16). Durch mobile Endgeräte wird der Mensch direkt in das Kommunikationsnetz der Smart Factory eingebunden; s. (Zillmann 2016, S. 13). Geeignete mobile Endgeräte sind Tablets oder Smartphones, wodurch die intuitive Benutzung dieser Devices eine Vereinfachung für den Mitarbeiter darstellt. Das Schlagwort *Augmented Reality* (AR) dient als Hilfsmittel für den Produktionsmitarbeiter. Augmented Reality bildet die reale Welt mit zusätzlichen Informationen aus der virtuellen Welt ab. Die angezeigten Informationen werden in der richtigen Größe und an der korrekten Position dargestellt. Diese neue Technologie wird in Smart Glasses oder in Datenhandschuhen verwendet, welche mit dem Backend-System verbunden werden; s. (Huber 2016a, S. 78).

Beim Thema CPS muss auch die *Machine-to-Machine-Communication* (M2M-Kommunikation) erwähnt werden. Hier kann nicht nur der Mensch mit der Maschine kommunizieren, sondern die Maschine kann selbstständig mit anderen Maschinen oder Werkzeugen in Kontakt treten. Durch diese Lösung können Maschinen- und Produktionsdaten erfasst, und in Echtzeit weitergeleitet werden; s. (Zillmann 2016, S. 13).

Die Echtzeitverarbeitung von Informationen wird auch *Real Time Enterprise* (RTE) genannt und ist ein zentrales

Element innerhalb einer Smart Factory. Die Informationen sollten dem Anwender immer rechtzeitig vorliegen. Bei der Verarbeitung großer Datenmengen spielt das Schlagwort Big Data eine wichtige Rolle; s. (Huber 2016a, S. 11).

Big Data wird oftmals als „Rohstoff des 21. Jahrhunderts“ bezeichnet. Die Grundvoraussetzung hierbei ist das Sammeln, Speichern, Filtern, Analysieren, Verdichten und Visualisieren großer Datenmengen. Es kann sowohl mit strukturierten, als auch mit unstrukturierten Daten gearbeitet werden. Die Hauptaufgabe ist es, Muster und Kausalitäten zu erkennen. Bei dem richtigen Einsatz von Big Data zeigt sich, dass mit zunehmender Datenmenge auch die Aussagekraft steigt.

Technisch können Big Data-Systeme auf Not Only SQL (NoSQL)-Datenbanken oder auf einem Hadoop Framework basieren. Hadoop ist ein Open-Source-Framework und dient zur Speicherung großer Datenmengen auf verteilten Systemen. Ein weiteres Big Data-System ist die In-Memory-Datenbank. Diese wird für schnelle Auswertungen eingesetzt. Hier dient der Arbeitsspeicher eines Computers als Datenspeicher. Die SAP SE ist einer der bekanntesten In-Memory-Datenbank-Anbieter; s. (Huber 2016a, S 54ff.).

Damit eine gemeinsame Vernetzung und Kommunikation zwischen verschiedenen Umgebungen und Objektarten erfolgen kann, müssen akzeptierte *Standards und Schnittstellen* eingesetzt werden. Dazu wurde im Jahr 2012 das Internet-Protokoll IPv6 eingeführt. Mit Hilfe des IPv6 Protokolls stehen für Ressourcen, Informationen, Objekte und Menschen in einer Smart Factory eine ausreichende Anzahl an Adressen zur Verfügung. Es entsteht somit eine flächendeckende Vernetzung; s. (Kelkar et al. 2014, S. 8).

Innerhalb einer Smart Factory bilden *Cloud-Computing-Lösungen* eine wichtige Komponente. Hierbei wird eine bedarfsgerechte und flexible Nutzung von unterschiedlichen IT-Leistungen über das Internet in Form von Diensten angeboten. Allgemein betrachtet werden bei einem Cloud-Ansatz Daten oder Dienste an einen internen oder externen Dienstleister ausgelagert; s. (Huber 2016a, S. 60g.). Die Abrechnung solcher Services erfolgt immer nutzungsabhängig. Es können drei Service-Elemente unterschieden werden. Unter *Infrastruktur-as-a-Service (IaaS)* versteht man die Bereitstellung von Rechen-, Speicher- und Netzkapazität durch einen Cloud-Provider. Bei dem Service-Element *Platform-as-a-Service (PaaS)* wird dem Anwender eine Entwicklungsumgebung in Form eines technischen Frameworks über einen Internetanbieter zur Verfügung gestellt. Hierbei handelt es sich um standardisierte Umgebungen. Diese vereinfachen und beschleunigen die Softwareentwicklung, indem die angebotene Umgebung nicht implementiert werden muss. *Software-as-a-Service (SaaS)* stellt standardisierte Anwendungsservices über eine Cloud zur Verfügung und

kann von Endanwendern genutzt werden; s. (Münzl et al. 2015, S. 10ff.).

Durch die vorangegangenen Definitionen wird deutlich, dass ohne *Automatisierung* eine Produktion im Sinne einer Smart Factory nicht erfolgen kann. Mittels der Automatisierung werden Produktionsprozesse beschleunigt und optimiert. Dies geschieht durch die Übertragung der Produktionsprozessfunktionen an künstliche Systeme. Als Automat wird eine Maschine bezeichnet, welche bestimmte und vorher festgelegte Abläufe selbstständig beziehungsweise automatisch ausführt. Je nach Grad der Automatisierung wird von Teil- oder Vollautomatisierung gesprochen. Im Bereich der Smart Factory wird eine Vollautomatisierung gefordert. Dies bedeutet, dass keine vollständige Weitergabe von starren und wiederkehrenden Produktionsabläufen an Maschinen erfolgt. In einer Smart Factory werden die Prozesse mit unterschiedlichen Aufgabenstellungen durch flexible Fertigungssysteme ausgeführt; s. (Maurer 2016).

Die *sensitiven Roboter* gelten als Inbegriff der Automatisierung und sind eng mit den Themen CPS und M2M-Kommunikation verknüpft. Ein sensitiver Roboter wird mit feinfühligem Gelenksensoren ausgestattet, um somit Tätigkeiten in Verbindung mit menschlichen Kollegen durchzuführen. Innerhalb einer Smart Factory bewegen sich die Roboter frei und werden nicht durch Gitterzäune vom Menschen getrennt. Diese Zusammenarbeit wird *Mensch-Roboter-Kollaboration* bezeichnet; s. (Reinhart, Gunther et al. 2018). Der Mensch wird durch die enge Zusammenarbeit von körperlich schweren Arbeiten entlastet oder bei ergonomisch ungünstigen Tätigkeiten unterstützt; s. (Huber 2016a, S. 50).

Als *digitales Produktgedächtnis* wird ein zu fertigendes Produkt mit einem automatisch auslesbaren Datenträger bezeichnet, welches dazu beiträgt, ein vollständig dezentralisiertes Produktionsumfeld zu erreichen. Somit werden die Produkte selbst zum Informationsträger. Die relevanten Daten werden unabhängig von Server-Systemen an die bearbeitenden Maschinen weitergegeben. Das digitale Produktgedächtnis ist für die autonome, dezentrale Produktion und für individualisierten Produkte ein entscheidender Schritt. Es ermöglicht eine durchgängige Produktdokumentation über die gesamte Produktlebensphase. Die Produktdaten sind jederzeit auslesbar und bei Problemen können fehlerhafte Bauteile sofort identifiziert werden. Durch das digitale Produktgedächtnis wird eine optimale Ressourcenoptimierung ermöglicht; s. (Kelkar et al. 2014, S. 8).

Im Zusammenhang einer flexiblen und effizienten Produktion muss die neue Technologie des *3D-Druckers* erwähnt werden. Durch diese Technik werden additive Fertigungsverfahren ermöglicht. Additiv bedeutet in diesem Umfeld die Erzeugung eines Bauteils über schichtweises Hinzufügen eines Werkstoffes. Das gewünschte Objekt wird Schicht für Schicht auf Basis eines 3D-Modells aus

den gewünschten Materialien erzeugt. Die Vorteile gegenüber einer konventionellen Fertigung sind enorm. Kleinserien können wirtschaftlich und rentabel produziert werden und die Herstellung schwieriger Bauteile wird erleichtert. Ein weiterer positiver Aspekt ist die Minimierung des Materialeinsatzes und das Entfallen der Fertigungsschritte. Das Produktionsumfeld der Smart Factory lässt sich mit Hilfe dieser neuen Technologie einfacher und flexibler umsetzen und gestalten; s. (Huber 2016a, S 33ff.).

In einer Smart Factory haben *robuste Netze* eine hohe Bedeutung. Damit die CPS miteinander kommunizieren können, ist eine hohe Verfügbarkeit der kabel- und funkgestützten Netzwerke unabdingbar. Die Herausforderung der Datenfülle und der damit verbundenen hohen Datenübertragungsrate darf nicht unterschätzt werden. Um dieses Problem zu bewältigen, werden Breitbandnetzwerke eingesetzt. Eine besondere Rolle spielen Wireless LANs (Local Area Network), so dass die Mobilität von Robotern und Automaten gewährleistet werden kann. Im Bereich Funknetzwerken besteht derzeit noch Entwicklungsbedarf (Kelkar et al. 2014, S. 9).

Durch diese Technologien hat eine Smart Factory ein komplexes Umfeld und es treten hohe technischen Anforderungen auf. Diese Überlegungen werden durch die Abbildung 2 vervollständigt. Sie dient zusätzlich der Einordnung der Begrifflichkeiten, die üblicherweise mit der Smart Factory in Verbindung gebracht werden. Einige

der genannten Technologien existieren bereits und manche befinden sich noch in der Entwicklung. Dennoch sind die genannten Technologien und Methoden noch nicht in dem gewünschten Ausmaß und Zusammenspiel eingesetzt. Eine zentrale Rolle für die Umsetzung der Zusammenarbeit der einzelnen Technologien spielt die IT. Sie sorgt für die notwendige Vernetzung und die benötigten Architekturen. Erst durch den richtigen Einsatz der IT werden all diese Komponenten steuerbar. Durch die ansteigende Vernetzung der Technologien treten viele Risiken auf und erfordern neue Konzepte und Mechanismen in Unternehmen. Welche Risiken auftreten können, werden im Kapitel „Risiken innerhalb einer Smart Factory“ erläutert. Zuvor wird auf immer intensiver genutzte Künstliche Intelligenz in einer Smart Factory näher eingegangen.

4. Künstliche Intelligenz

Industrie 4.0 ist die erste industrielle Revolution, die nicht nach ihrem Ende definiert wurde, sondern während ihrer Laufzeit antizipiert wird. Sie lässt sich in drei aufeinander aufbauenden Stufen einteilen, welche im Folgenden beschrieben sind. Der Bereich Künstliche Intelligenz bildet mit drei Phasen die letzte Form der industriellen Revolution, s. (Botthof, Alfons et al. 2015, S. 24f.): Die erste Stufe innerhalb der Industrie 4.0 ist die Flexibilisierung. Cyber-physische-Systeme vernetzen hierbei die Prozesse der Produktion, Logistik, Internetdienste, des Engineerings und des Managements miteinander.

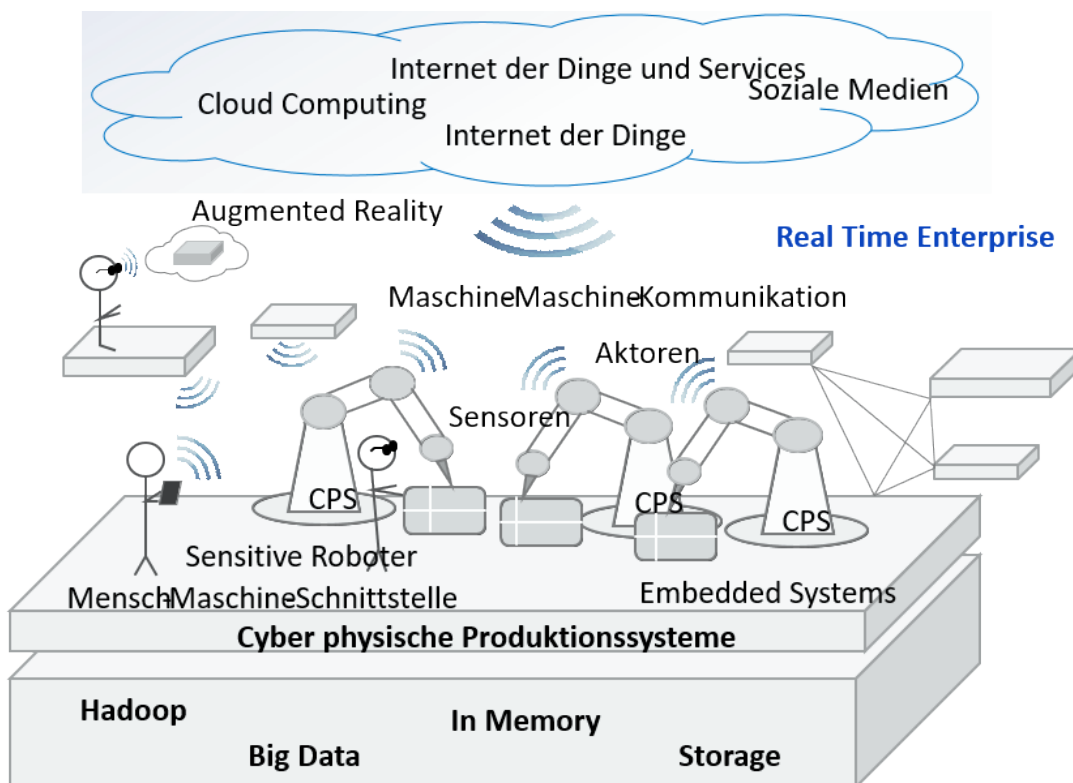


Abbildung 2: Begrifflichkeiten innerhalb einer Smart Factory. (Eigene Darstellung)

Dadurch werden Informationen selbstständig mittels Sensoren erfasst und ausgetauscht. Die transferierten Informationen ermöglichen den Start von Aktionen und somit eine eigenständige und gegenseitige Steuerung. Allerdings handelt es sich an dieser Stelle noch nicht um eine Digitalisierung, jedoch ist Vernetzung die Grundlage dafür; s. (Ruskowski, 2019).

Die Humanisierung bzw. Kognition stellt die zweite Ebene dar. Die bestehenden cyber-physischen Systeme werden humanisiert, indem sie mit kognitiven Eigenschaften wie Sehen und Hören erweitert werden. Dies kann durch Bilderkennungssysteme in der Produktion erfolgen, die beispielsweise dabei helfen, Ware mit Qualitätsmängeln zu identifizieren. Ein weiteres Beispiel der Kognition ist der Einsatz von Spracherkennungssystemen, die eine Steuerung der Maschinen mittels der Stimme ermöglichen; s. (Ruskowski, 2019).

Der letzten Stufe der Industrie 4.0, der Agilität, wird die Künstliche Intelligenz zugeordnet. Bei der autonomen Herstellung der Produkte durchlaufen Bauteile die einzelnen Produktionsstufen ohne menschliche Hilfe. Durch den Schritt der Humanisierung der Maschinen wissen diese, um welches Bauteil es sich handelt und welche Arbeitsschritte an ihm ausgeführt werden sollen. Das führt schließlich dazu, dass Produktion und Logistik durch die ganzheitliche Einführung von KI ineinander einfließen; s. (Ruskowski, 2019).

Dennoch: eine allgemeingültige Definition des Begriffs „Künstliche Intelligenz“ existiert auf Grund seiner Anpassung an die technischen Möglichkeiten seit der Begriffsbildung in den 1950er Jahren nicht. Das Fraunhofer Institut beschreibt Künstliche Intelligenz in einer Studie als „ein Teilgebiet der Informatik, das versucht, mit Hilfe von Algorithmen kognitive Fähigkeiten wie Lernen, Planen oder Problemlösen in Computersystemen zu realisieren.“; s. (Bauer et al. 2018, S. 11) Somit handelt es sich hierbei um Technologien, welche gewisse Ausprägungen der menschlichen Intelligenz adoptieren (Krüger et al., 2019). Die Merkmale dieser Systeme lassen sich in die vier folgenden Kernbereiche unterteilen; s. (Termer, 2019):

Wahrnehmen – In Unternehmen müssen IT-Systeme die Daten der verschiedenen Abteilungen aufnehmen, um diese in den weiteren Schritten verarbeiten zu können. Durch den weiter steigenden Fortschritt der Digitalisierung sind der Menge und der Art von Daten kaum Grenzen gesetzt. Einerseits stützt dies die Zuverlässigkeit der Aussage, welche das Ergebnis der Datenverarbeitung liefert, andererseits haben nicht alle Daten die gleiche Relevanz für die entsprechenden Systeme. Daher ist es eine gründliche Filterung der Daten notwendig, welche für den Verarbeitungsprozess erforderlich sind.

Verstehen – Die wahrgenommenen Daten sollen automatisiert erkannt und zugeordnet werden. Dies kann mittels

Erweiterungen durch Deep Learning bzw. Machine Learning realisiert werden. Immer weiter steigt hierbei die Nachfrage an Sprachverständnis-Tools, die beispielsweise bei der Bearbeitung von Kundenanliegen als Unterstützung dienen. Man betrachte nun ein hypothetisches Unternehmen, welches täglich eine hohe Zahl an Produktionsaufträgen erhält und diese automatisiert an die betreffenden Produktionsabteilungen weiterleiten möchte. Wird eine definierte Abteilung in dem Auftrag erkannt, so kann dieser problemlos zugeordnet werden. Wenn allerdings ein neuer Auftrag keine bekannte Struktur aufweist, da beispielsweise eine Sonderbestellung hinzugefügt wurde, muss die KI zunächst den Wunsch verstehen können. Trainierte Systeme erfüllen bereits heutzutage diese Aufgabe.

Handeln – KI-Systeme ermöglichen eine intelligente Prozess- bzw. Gerätesteuerung in der Produktion. Auswirkungen eben solcher intelligenter Prozess- und Gerätesteuerungen auf den Herstellungsprozess, sollen unter anderem Diskussionsthema dieser Arbeit sein.

Lernen – In der Entwicklungsphase der Künstlichen Intelligenz werden dem System Daten injiziert, um bestimmte Strukturen zu erlernen. Der Lernprozess beschränkt sich jedoch nicht nur auf die sogenannte Trainingsphase, sondern streckt sich bis in den laufenden Betrieb. Folglich handelt es sich bei Künstlicher Intelligenz um ein System, welches durch ständige Datenerfassung kontinuierlich lernt und sich dadurch optimal an die Anforderungen der Unternehmen anpasst.

5. Risiken innerhalb einer Smart Factory

Da die Industrie 4.0 zunehmend an Form gewinnt, kristallisieren sich neben den vielen Vorteilen auch immer mehr Risiken heraus. Diese näher zu beleuchten ist essentiell, um im Nachgang den Stand der Smart Factory zu bewerten. Die Risiken zum Thema Industrie 4.0 können in die Bereiche technische, organisatorische und wirtschaftliche Risiken gruppiert werden. Da die Industrie 4.0 ein stark technologisch getriebenes Thema ist, werden im Folgenden die technologischen Risiken genauer betrachtet. Die organisatorischen und wirtschaftlichen Risiken werden zur Vollständigkeit danach nur kurz behandelt.

In den Smart Factories werden sehr viele Technologien eingesetzt, weswegen sich auf diejenigen beschränkt wurde, die in der Literatur am intensivsten behandelt werden und dadurch als am Wichtigsten eingestuft werden können. Sie lauten: Standardisierung, IT-Sicherheit, Verfügbarkeit der IT-Infrastruktur, Verfügbarkeit von schnellem Internet und komplexe Systeme beschränkt, da die in der Literatur am intensivsten behandelt werden und deswegen als am Wichtigsten eingestuft

5.1 Standardisierung

Zum Thema Industrie 4.0 existieren keine internationalen Standards und Normen. Diese sind jedoch Voraussetzung

für eine hohe Anzahl von Vernetzungspartnern und der Erschließung des wirtschaftlichen Potenzials der Industrie 4.0. Größtenteils passen sich die zuliefernden Unternehmen den Standards der größeren Unternehmen an, was zur Folge hat, dass die Handlungsmöglichkeiten der kleineren Unternehmen gehemmt werden. Ebenso entstehen zu hohe Investitionsausgaben, wenn Unternehmen auf nicht zukunftsorientierte Technologien setzen; s. (Schröder 2016, S. 12). Um eine Smart Factory zu verwirklichen und eine Grundlage für die Standardisierung vorzugeben, wurde ein Referenzarchitekturmodell für die Industrie 4.0 (RAMI 4.0) entwickelt; s. (Zillmann 2016, S. 11). Dieses wurde erstmals auf der Hannover Messe 2015 vorgestellt und von den Industrieverbänden Bitkom, VDMA und ZVEI gemeinsam definiert; s. (Schewe 2016). Anhand des Modells soll ein gemeinsames Verständnis geschaffen werden, welche Standards, Use Cases und Normen für eine Smart Factory notwendig sind. Das Ziel des Referenzarchitekturmodells ist es, möglichst wenig Standards einzusetzen und ein anschauliches und einfaches Architekturmodell als Referenz zu schaffen; s. (Plattform Industrie 4.0 2015, S. 41f.).

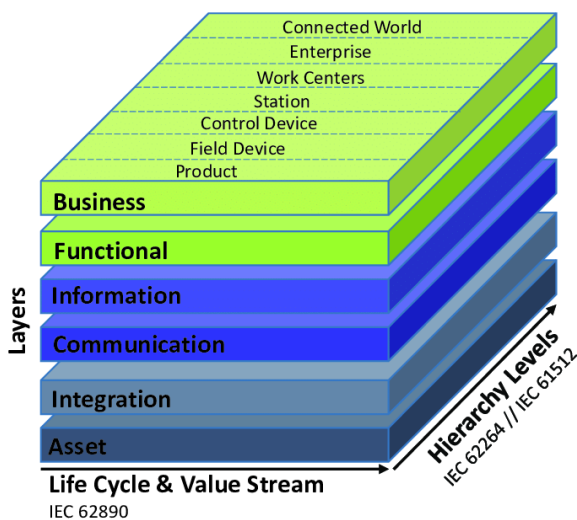


Abbildung 3: RAMI 4.0 (Eigene Darstellung)

Das Modell besteht aus einem dreidimensionalen Koordinatensystem. Die Achse „Hierarchy Levels“ stellen die unterschiedlichen Funktionalitäten und Verantwortlichkeiten innerhalb einer Fabrik oder einer Anlage dar. Die waagrechte Achse „Life Cycle & Value Stream“ bildet den Lebenszyklus und Wertschöpfungsketten von Anlagen und Produkten ab. Hier wird zwischen Typ und Instanz unterschieden. Ein Typ befindet sich in der Entwicklung oder Prototypenfertigung. Wenn das Produkt gefertigt wird, wird es als Instanz bezeichnet. Anschließend muss die senkrechte Achse „Layers“ betrachtet werden. Hier wird das digitale Abbild der betrachtenden Industrie 4.0-Technologie strukturiert Schicht für Schicht beschrieben. Es werden die sechs Schichten Geschäftsprozesse, Funktionen, Daten, Kommunikation, Integration und die realen Dinge dargestellt. Durch die drei beschriebenen Achsen können alle Aspekte von Industrie

4.0 abgebildet werden und dienen als Basis für weitere Arbeitsschritte; s. (Hankel und Rexroth 2015).

Die Hard- und Softwarekomponenten in der Produktion werden Industrie 4.0-fähig, wenn sie die Kommunikationsfähigkeit der realen Objekte mit den jeweiligen Daten und Funktionen umsetzen. Eine wichtige Voraussetzung dafür ist, dass die Industrie 4.0-Komponenten während ihres gesamten Lebenszyklus, die Daten in einem abgesicherten elektronischen Container sammeln und mit sich tragen. Der elektronische Container kann auch als Verwaltungsschale bezeichnet werden. Alle relevanten Daten einer Hard- oder Softwarekomponente sind in der Verwaltungsschale gespeichert, und ergeben zusammen ein virtuelles Abbild. Dadurch entstehen neue Möglichkeiten der vernetzten Produktion und liefern einen Mehrwert für alle, die am Wertschöpfungsprozess beteiligt sind.

Damit die Kommunikation entlang der Wertschöpfungskette funktioniert, ist die Open Platform Communications Unified Architecture, kurz OPC UA, eine grundlegende Voraussetzung. Dieses Kommunikationsprotokoll ist für M2M- und PC-to-Machine Kommunikation entwickelt worden und wurde im Jahr 2006, als Standardprotokoll im Rahmen der Industrie 4.0, vorgestellt. OPC UA kann Maschinendaten transportieren und diese ebenfalls maschinenlesbar semantisch beschreiben. Dies unterscheidet OPC UA von herkömmlichen Kommunikationsprotokollen; s. (Kagermann et al. 2013, S. 104).

Die aufgezeigten Beispiele zum Thema „Standardisierung“ sind nur ein kleiner Einblick und der Beginn für die Umsetzung einer vernetzten Smart Factory. Es besteht die dringende Notwendigkeit, internationale Standards und Normen in naher Zukunft zu erarbeiten, wobei auf die bereits bestehenden Technologien und Schnittstellen zurückzugreifen ist.

5.2 IT-Sicherheit

Eines der größten technischen Risiken innerhalb einer Smart Factory stellt die „IT-Sicherheit“ dar. In den letzten Jahren nahmen die Cyber-Attacken gegen Unternehmen sowie auch gegen Privatpersonen stetig zu; s. (Huber 2016b). Aufgrund des mangelnden Ausbaus von Datenschutz und Datensicherheit entstehen durch Cyber-Attacken hohe finanzielle Schäden. Auch die Ausbreitung neuer Geschäftsmodelle und der Einsatz von Cloud-Lösungen werden durch die aufkommenden Gefahren gehemmt; s. (Kelkar et al. 2014, S. 56). Mittels der CPS-basierten Produktionssysteme entstehen neue Sicherheitsanforderungen, da sie einen hohen Vernetzungsgrad aufweisen. Sie sind vernetzt mit einer Vielzahl an beteiligten Maschinen, IT-Systemen und Automatisierungskomponenten. Die technischen Systemkomponenten agieren teilweise autonom mit einem zeitkritischen Daten- und Informationsaustausch, wobei zugleich mehrere Akteure entlang der Wertschöpfungskette beteiligt sind. Es lässt sich somit feststellen, dass das Thema Industrie

4.0 einen völlig neuen Blickwinkel auf den Bereich der Sicherheit wirft; s. (Kagermann et al. 2013, S. 50).

Grundsätzlich lässt sich das Thema Sicherheit in zwei Bereiche aufteilen. Zum einen muss das Thema der Betriebssicherheit (Safety) und zum anderen die Thematik der Angriffssicherheit (Security) berücksichtigt werden. Bei dem Thema Betriebssicherheit dürfen Maschinen, Produktionsanlagen, Werkstücke und Produkte zu keinem Zeitpunkt eine Gefahr für den Menschen darstellen. Die funktionale Sicherheit (Functional Safety) und eine hohe Zuverlässigkeit (Reliability) sind Voraussetzung für die Betriebssicherheit. Eine Sicherstellung dieser Bedingungen erweist sich als komplex, da hohe Anforderungen an verteilte IT-Architekturen in einer Produktion bestehen. Es wird erwartet, dass die Anlagen in der Produktion ohne Unterbrechung über mehrere Jahre hinweg laufen.

Der zweite Bereich ist das Thema Security und schützt Daten und Dienste in Systemen gegen Missbrauch, unbefugten Zugriff, Veränderungen und Zerstörungen. Das Ziel von Security ist die Erhöhung der Vertraulichkeit und der Integrität; s. (Zillmann 2016, S. 22).

Damit das Konzept der Industrie 4.0 realisiert und umgesetzt werden kann, müssen alle relevanten Risikobereiche der Sicherheit betrachtet werden. Zu diesen gehören Produktion und Fertigung mit ihren Embedded Systems, Big Data, Cloud-Computing und die mobilen Lösungen. Hieraus lässt sich erkennen, dass neue Formen der Zusammenarbeit entstehen und neue, zumindest angepasste IT-Sicherheitskonzepte erforderlich werden.

Mögliche Gefahren im Industrie 4.0-Bereich sind die Infektion mittels Schadsoftware über das Internet oder Intranet und über externe Hardware. Neben den gezielten Angriffen müssen sich Unternehmen auch gegen unabsichtlich herbeigeführte Probleme wappnen, wie beispielsweise dem menschlichen Fehlverhalten. Außerdem stellen die Fernwartungszugänge, die Nutzung mobiler Endgeräte und Distributed-Denial-of-Service (DDoS) weitere Gefahren innerhalb einer modernen Produktionsumgebung dar; s. (Huber 2016a, S. 65ff.). DDoS-Angriffe sind ein schwer abzuschermendes Risiko für jede extern erreichbare Schnittstelle. Es werden viele Anfragen an einen Empfänger gestellt, so dass eine Überlastung der Server und Netzwerke vorliegt und legitime Anfragen nicht mehr bearbeitet werden können; s. (Bundesamt für Sicherheit in der Informationstechnik 2016, S. 28).

Ein weiteres Bedrohungsszenario geht einher mit der angestrebten Standardisierung der Anlagen und Maschinen. Die Informationen über Systeme und deren Spezifikationen werden im Internet weltweit verfügbar sein und sind folglich leicht manipulierbar; s. (Huber 2016a, S. 66).

Der Schutz von personenbezogenen Daten ist ein weiterer wichtiger Aspekt. Aufgrund der starken Vernetzung der Prozesse und der Digitalisierung muss dem Thema

große Aufmerksamkeit geschenkt werden (Huber 2016a, S. 68).

Der Ansatz BYOD (Bring your own Device) bringt ebenfalls viele Bedrohungen mit sich. Im Jahr 2013 nutzten circa 23 Prozent der Mitarbeiter in deutschen Unternehmen ihr eigenes mobiles Endgerät für Unternehmenszwecke. Dieser Trend verursacht eine Kostenersparnis für die Unternehmen, da die Anschaffungskosten für Mobile Devices entfallen. Die Mitarbeiter sind bereits mit ihrem mobilen Endgerät vertraut, wodurch die Mitarbeiterzufriedenheit gesteigert werden kann. Nicht zuletzt bringt die ortsungebundene Arbeit mehr Flexibilität und Produktivität in den Arbeitsalltag der Mitarbeiter. Neben den Vorteilen lassen sich auch viele Gefahren aufzeigen. Eine übergreifende Kontrolle kann nicht erfolgen und basiert lediglich auf dem entgegengebrachten Vertrauen an die Mitarbeiter, welche sich an die vereinbarten Richtlinien halten müssen. Des Weiteren sind auf jedem mobilen Device persönliche und viele unternehmensbezogene Daten gespeichert; s. (Stoitsi 2015). Mit Hilfe der zentralen Verwaltungsplattform MDM (Mobile Device Management) und EMM (Enterprise Mobile Management) können mobile Geräte mit zusätzlichem Tracking und Reporting in die Unternehmensinfrastruktur miteingebunden werden. Das MDM-System muss standardmäßig die Datenverschlüsselung von Datenträgern vornehmen, um somit die Sicherheit von Endgeräten gewährleisten zu können; s. (Huber 2016a, S. 65). Zur Unterstützung der Unternehmen werden bereits unternehmensbezogene Software und Applikationen für Mobile Devices entwickelt; s. (Stoitsi 2015).

Damit die die Produktionsstabilität innerhalb einer Smart Factory gewährleistet werden kann, müssen die Automatisierungsnetzwerke segmentiert werden. Die Automatisierungsnetzwerke werden in kleine Zellen aufgeteilt, zwischen denen Firewalls die Kontrolle übernehmen; s. (Huber 2016a, S. 67). Es ist sinnvoll, Firewalls mit Deep Packet Inspection (DPI)-Fähigkeit bei betriebskritischen Geräten einzusetzen. Bei DPI werden spezielle Befehle oder Anfragen geprüft, ob diese durch die Firewall gelassen werden dürfen oder nicht. So können unzulässige Zugriffe auf Produktionsobjekte vermieden werden; s. (Jenker 2014). Grundsätzlich sollten jedoch die altbekannten Maßnahmen nicht vergessen werden, wie beispielsweise Kameras, Kartenlesegeräte, organisatorische Maßnahmen und Passwortkontrolle. Ebenfalls sind Positivlisten ein einfacher Schutz gegen unkontrollierte Zugriffe. Hier erfolgt die Festlegung, auf welchem Rechner welche Prozesse, Programme oder Operationen laufen dürfen. Ein weiterer Ansatz zur Erhöhung der Sicherheit, ist das sogenannte Security by Design. Es ist von Vorteil, bereits bei der Produktentwicklung gewisse Sicherheitsaspekte zu berücksichtigen. Oftmals ist es nicht ausreichend, die CPS-basierten Produktionssysteme nachträglich um Security-Funktionen anzureichern; s. (Huber 2016a, S. 67f.).

Mit Hilfe des Security by Design-Ansatzes, wurde das plattformunabhängige und weltweit anerkannte Kommunikationsprotokoll OPC UA (Unified Architecture) entwickelt (siehe Kapitel „Standardisierung“). Dadurch entsteht eine sichere Vernetzung der Produktionsprozesse und stellt einen zentralen Baustein auf dem Weg zur Industrie 4.0 dar; s. (Bundesamt für Sicherheit in der Informationstechnik 2016, S. 52f.).

Viele Ansätze zur Einführung von geeigneten IT-Sicherheitsmaßnahmen kommen vom Bundesamt für Sicherheit und Informationstechnik (BSI). Das BSI beschäftigt sich mit sehr vielen IT-Sicherheitsthemen, von denen die meisten jedoch noch in der Entwicklungsphase stecken. Grundlegend können der IT-Grundschutz, das ICS-Security-Kompendium (Industrial Control Systems) und LARIS ICS als Hauptthemen für das BSI genannt werden. Der IT-Grundschutz ist der meistgenutzte Standard für Informationssicherheit in Deutschland und befindet sich gerade in einem Modernisierungsprozess. Das ICS-Security-Kompendium enthält die Grundlagen der IT-Sicherheit und die relevanten Normen und Standards. Des Weiteren beinhaltet es Best Practices und Empfehlungen zum Thema Cyber-Security für Anlagenbetreiber. Die Software LARIS ICS ist dagegen wie ein Tool aufgebaut, welches einen Fragebogen sowie Empfehlungen für weitere Maßnahmen umfasst. Das Tool trägt dazu bei, ein umfassendes IT-Sicherheitsmanagement in Unternehmen erarbeiten zu können; s. (Schonscheck 2015a).

Die IT-Sicherheitserfahrung in Industriebetrieben kann aktuell als eher gering eingeschätzt werden. Aus diesem Grund muss das BSI weitere Entwicklungs- und Optimierungsphasen durchlaufen, um den Unternehmen den Einstieg in die industrielle IT-Sicherheit so einfach wie

möglich zu gestalten; s. (Schonscheck 2015b). Dennoch bleibt die IT-Sicherheit eine individuelle Aufgabe jedes einzelnen Unternehmens. Diese müssen sich zum Ziel setzen, ein System mit einer inhärenten IT-Sicherheit zu konzeptionieren. Festzuhalten ist aber, dass es noch viele offene Baustellen im Bereich der IT-Sicherheit gibt und viele Ansätze noch nicht reif für den produktiven Einsatz sind; s. (Huber 2016a, S. 68).

5.3 Verfügbarkeit der IT-Infrastruktur

Eine weitere Herausforderung im Industrie 4.0-Umfeld ist die Verfügbarkeit der IT-Infrastruktur. Durch die stärkere Verwendung von Software und vernetzten Maschinen und Anlagen, steigt die Abhängigkeit der Unternehmen von einer leistungsstarken, skalierbaren und verfügbaren IT-Infrastruktur; s. (Huber 2016b). Aus diesem Grund muss die IT eine moderne und virtualisierte IT-Landschaft schaffen. Mit Hilfe von Standardisierung und Konsolidierung der IT-Systeme kann dies ermöglicht werden. Des Weiteren muss eine Vernetzung aller Komponenten und Systeme im Unternehmen erfolgen sowie die Gewährleistung der Verfügbarkeit von konsistenten Daten. Um diesen Anforderungen gerecht zu werden, muss eine Auflösung der klassischen Automatisierungspyramide, s. die Abbildung 4 erfolgen; s. (Zillmann 2016, S. 20).

Aktuell wird die Kommunikation in Unternehmen durch das hierarchische System der Automatisierungspyramide widerspiegelt. Das Ziel der Automatisierungspyramide ist es, die Komplexität der industriellen Fertigung zu minimieren. Dies wird durch die Einteilung der Unternehmensprozesse in die einzelnen Ebenen erreicht. Die ver-

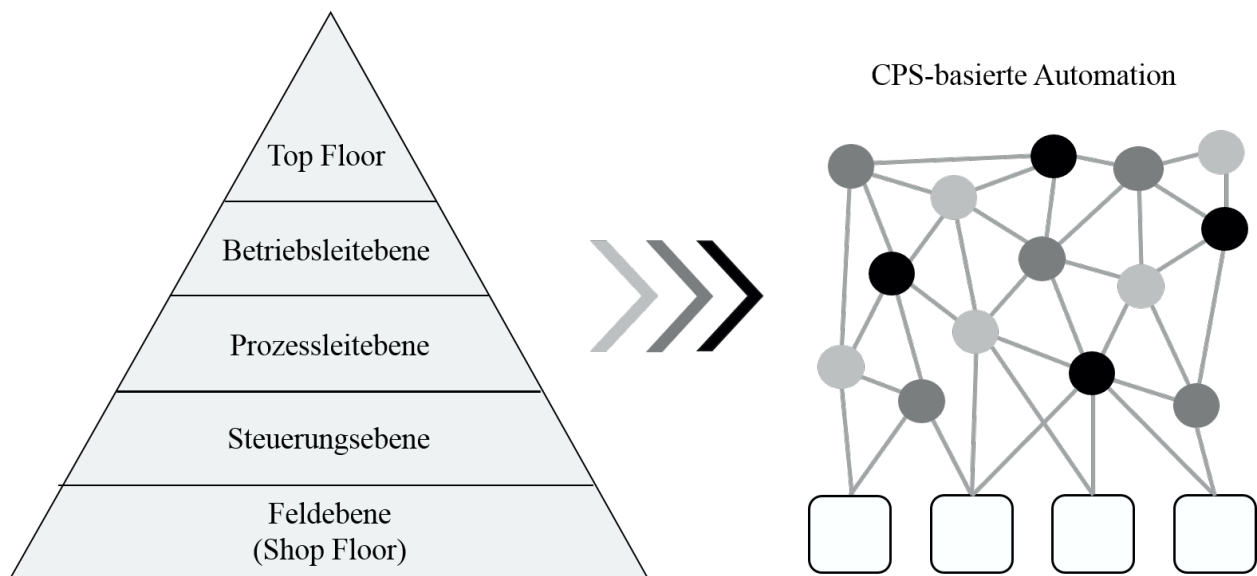


Abbildung 4: Traditionelle Automatisierungs-Pyramide und CPS-basierte Automatisierung (Eigene Darstellung)

schiedenen Ebenen werden jeweils durch unterschiedliche Systeme unterstützt; s. (Meudt et al. 2017, S. 7). Eine Unterstützung erfolgt in der Unternehmensleitebene mittels der Enterprise Resource Planning (ERP) Software und wird als Informationssystem in allen Bereichen eines Unternehmens für wirtschaftliche Tätigkeiten eingesetzt. Des Weiteren wird in der Betriebsleitebene die Software Manufacturing Execution System (MES) genutzt und ist mit den Aufgaben Produktionssteuerung, -lenkung und -kontrolle vertraut. Darunter befindet sich die Produktionsleitebene, in der die kurzfristige Produktionsplanung erfolgt. Dies geschieht mit Hilfe von Systemen, wie beispielsweise dem Supervisory Control and Data Acquisition (SCADA)-System. Während dessen befinden sich in der Prozessleitebene die Steuer- und Regelsysteme, wie die sogenannte speicherprogrammierbare Steuerung (SPS). In dieser Ebene werden die Signale von der Feldebene ausgewertet und weiterverarbeitet an die Feldebene zurückgegeben. Die Feldebene ist mit Sensoren und Aktoren ausgestattet und liefert produktionsrelevante Daten an die übergeordneten Ebenen; s. (Heinrich 2017, S. 5).

Heutzutage erfolgt die Kommunikation noch hierarchisch über wenige Schnittstellen zwischen den einzelnen Ebenen. Aus diesem Grund erfolgt die Betrachtungsweise und die Steuerung der Ebenen in der Regel noch isoliert; s. (Bauernhansl et al. 2014, S. 544). Der Schritt zu einer übergreifenden Vernetzung ist derzeit im Bereich der Automatisierungstechnik kaum vollzogen. Bereits heute liegen sehr große Mengen an Informationen über Produktionsmittel, Produkte und Prozesse in den IT-Systemen der Unternehmen vor. Ebenfalls existieren in Unternehmen meist eine Vielzahl an IT-Systemen und Maschinen nebeneinander, welche nur eine bedingte Vernetzung aufweisen oder welche aufgrund unterschiedlicher Semantik keine Datenmigration erlauben; s. (Bauernhansl et al. 2014, S. 39). Durch die Isolation der Informationsquellen werden Medienbrüche verursacht. Es lässt sich feststellen, dass der Nutzen der Informationsinterpretation in einer konkreten Anwendung erst dann erfolgen kann, wenn unterschiedliche Subsysteme gemeinsam integriert werden; s. (Bauernhansl et al. 2014, S. 79). Zudem kommt das Problem, dass die Systeme, Maschinen und Anlagen meist von unterschiedlichen Herstellern bezogen werden und ein unterschiedliches Alter aufweisen. Aus diesen Gründen ist das Umrüsten der Automatisierungssoftware sehr aufwändig, um die benötigte Kompatibilität herzustellen. Eine weitere Herausforderung ist es, den Datenfluss zu angrenzenden internen und externen Bereichen herzustellen; s. (Schröder 2016, S. 11). Ein ideales Ergebnis wird erst erreicht, wenn die Auflösung der starren hierarchischen Automatisierungspyramide erfolgt. Dies impliziert jedoch nicht das vollständige Verschwinden der Systeme auf den unterschiedlichen Ebenen. Der Fokus liegt hier vielmehr auf einer nahtlosen Verbindung zwischen den Ebenen zu einer Netzwerkstruktur. Damit dieses Ziel erreicht werden kann, müssen zeit- und finanztechnische Bemühungen der Integration erbracht werden; s. (Meudt et al.

2017, S. 7). Bei dem Thema Integration werden die flexible An- und Abkoppelbarkeit der einzelnen Komponenten, die programmieretechnischen Aufwände sowie die IT-Sicherheit der verteilten Informationen betrachtet. Für die anwendungsspezifische Verteilung von Informationen werden sogenannte Middleware-Systeme eingesetzt und führen Informationen aus verschiedene Quellsysteme zusammen. Diese werden über einheitliche Schnittstellen in technologieunabhängiger Form für Interpretationssysteme zur Verfügung gestellt. Wird der initiale Aufbau einer solchen Kommunikationsarchitektur aus Sicht der zu tätigen Investitionen betrachtet, so stellt dies den größten Aufwand dar. Ist die grundlegende Architektur realisiert, so können an die bestehende Infrastruktur weitere Datenquellen oder Interpretationssysteme mit überschaubarem Aufwand angebunden werden. Andererseits stellen bei den technischen Umsetzungen von Anwendungen die Identifikation der auszutauschenden Daten, die Umsetzung der Anbindung von Datenquellen und die Interpretationssysteme derzeit die größten Aufwände dar. In aktuellen Projekten, wie beispielsweise dem Forschungsprojekt CyProS (Cyber-Physische Produktionssysteme), wird an Komponenten geforscht, die die Umsetzbarkeit solcher Architekturen entscheidend beschleunigen; s. (Bauernhansl et al. 2014, S. 79ff.).

Grundsätzlich bedarf es nationale und internationale Abstimmungen bezüglich Standards für die Kommunikation zwischen den einzelnen Hardware- und Software-Applikationen. Daher muss den Unternehmen von Eigenentwicklungen abgeraten werden, da für eine verfügbare und sichere IT-Struktur internationale Standards benötigt werden; s. (Meudt et al. 2017, S. 7). Damit die Auflösung der Automatisierungspyramide und somit ein Aufbau einer verfügbaren IT-Infrastruktur gelingt, bedarf es noch einige Zeit.

5.4 Verfügbarkeit von schnellem Internet

Ein ebenso wichtiges Thema ist die Verfügbarkeit von schnellem Internet. Bezüglich des Ausbaus und der Verfügbarkeit der Breitbandnetze, befindet sich Deutschland im internationalen Vergleich auf den hinteren Plätzen. Doch gerade im Zeichen der Industrie 4.0 und der Digitalisierung ist der Zustand „Always on“ ein absolutes Muss; s. (Huber 2016b). Ein flächendeckender Einsatz von CPS setzt eine Infrastruktur voraus, mit der ein höherer und qualitativ hochwertigerer Austausch der Daten ermöglicht wird. Damit eine geringe Latenzzeit, eine hohe Ausfallsicherheit, eine hohe Qualität und ein umfassendes Breitbandnetz umgesetzt werden können, muss ein Ausbau der bestehenden Kommunikationsnetze erfolgen; s. (Kagermann et al. 2013, S. 49f.). Als Breitbandverbindung definiert die International Telecommunication Unit (ITU) bereits eine Übertragungsrate von zwei Megabit pro Sekunde. Diese festgelegte Übertragungsgeschwindigkeit ist nicht ausreichend, um unternehmensübergreifend und internetbasiert eine Produktion zu organisieren oder nachgelagerte Dienstleistungen zu definieren. Aus diesem Grund sind stabile Hochleistungsübertragungswege über Glasfaserkabel notwendig.

Ein weiteres Argument, den Glasfaserausbau voranzutreiben, ist, dass dieser nach heutigem Stand der Technik alternativlos ist. Ohne Glasfaserkabeln kann eine Smart Factory nicht realisiert werden und macht den Ausbau der Breitbandverbindung somit unabdingbar; s. (Schröder 2016, S. 1).

Die Bundesregierung erkennt den dringenden Bedarf an schnellem Internet und reagiert mit Förderungsprogrammen, Gesetzen und Strategien. Das Ziel der Bundesregierung ist, dass alle Haushalte bis zum Jahr 2018 einen Zugang zu schnellem Internet mit einer Übertragungsrates von mindestens 50 Megabit pro Sekunde haben. Des Weiteren setzt sich die Regierung dafür ein, bis 2025 ein flächendeckendes Breitbandnetz zu errichten, um auch Gewerbe-, Industriegebiete und Häfen an das Glasfasernetz anzuschließen. Die öffentlich zugänglichen Flächen der Gewerbe- und Industriegebiete werden zugleich mit kostenlosem WLAN (Wireless Local Area Network) ausgestattet. Das Gesetz „Gesetz zur Erleichterung des Ausbaus digitaler Hochgeschwindigkeitsnetze“ (DigiNetz-Gesetz) wurde 2016 von der deutschen Bundesregierung verabschiedet und fördert den Breitbandausbau in noch nicht erschlossenen Gebieten. Mittels dem DigiNetz-Gesetz werden bei einer Neuerschließung von Wohn- und Gewerbegebieten die Glasfaserleitungen künftig immer mitverlegt.

Auch in der Mobilfunktechnik gibt es einige Neuerungen. Im Jahr 2015 stellte Deutschland bereits Frequenzen im 700 Megahertz-Bereich für den Mobilfunk bereit und etablierte sich so zum europäischen Vorreiter. Doch aktuell wird eine neue Generation des Mobilfunks, namens 5G-Netzstandard, entwickelt. Mit dieser neuen Technologie lassen sich Datenmengen zuverlässig mit bis zu 20 Gigabit pro Sekunde übertragen. Aus diesen Gründen entwickelte die Bundesregierung die „5G-Strategie Deutschland“. Die 5. Generation des Mobilfunks wird damit zur digitalen Schlüsseltechnologie im Zeitalter der Vernetzung und ermöglicht eine Vielzahl an neuen Geschäftsmodellen, wie beispielsweise dem autonomen und vernetzten Fahren und der Industrie 4.0. Die 5G-Technik wird laut Bundesregierung bis 2020 marktreif sein; s. (Die Bundesregierung 2017).

5.5 Komplexe Systeme

Das nächste Problem, welches mit der Industrie 4.0 einhergeht, ist die zunehmende Komplexität innerhalb einer Smart Factory. Aufgrund der technologischen Entwicklungen in den letzten Jahrzehnten, ist die Komplexität der Produkte und Systeme bereits sehr stark gewachsen. Dies hat zur Folge, dass auch die Komplexität der industriellen Prozesse der Entwicklung und Fertigung stark ansteigen. Die Entwicklung und Produktion der Güter erscheint somit immer weniger beherrschbar; s. (Sendler 2013, S. 16).

Dass ein zu hohes Maß an IT und Automatisierung keine Allheilmittel sind, hat sich bereits in der Vergangenheit

herausgestellt. Die neu eingeführten Technologien können nicht mehr ausreichend beherrscht werden und die Unternehmen werden zunehmend unflexibel; s. (Huber 2016b). Die Rede ist vom Computer Integrated Manufacturing Ansatz (CIM Ansatz), welcher in den 80er Jahren verfolgt wurde. Beginnend von der Planung bis hin zur Fertigung sollte eine Vollautomatisierung erfolgen. Der Ansatz scheiterte, weil zum damaligen Zeitpunkt die erforderlichen Technologien nicht vorhanden oder zu unerschwinglichen Preisen erhältlich waren. Es wurde eine überzüchtete und überteuerte Produktion geschaffen, welche nur noch schwer beherrschbar war. Aufgrund der Komplexitätsprobleme und mangelnder Wirtschaftlichkeit wurde der Ansatz zu dieser Zeit nicht weiterverfolgt; s. (Bauernhansl et al. 2014, S. 85f.).

Im Laufe der Zeit verbesserte sich die Leistungsfähigkeit der Technologien und ebenso die Fähigkeiten der Entwickler. Zum heutigen Zeitpunkt haben genau hier die Ingenieure in der Mitte Europas eine gute Position, da sie die Verbindung von Embedded Software mit industriellen Produkten verschiedenster Arten sehr gut beherrschen. Manche Unternehmen schaffen die Verbindung von Software und Elektronik mit Mechanik besser als andere und sichern sich somit einen Platz an der Spitze des Weltmarkts. Dieser Vorsprung beruht auf den Erfahrungen, die sich über die letzten Jahrzehnte in der Industrie angesammelt haben. Es wird aber deutlich, dass der Vorsprung nicht langfristig gesichert ist. Die Voraussetzungen sind jedoch sehr gut, diesen zu halten oder sogar auszubauen. Der Industrie muss die Anpassung der Fähigkeiten, Methoden, Prozessen und Geschäftsmodellen an den Herausforderungen vernetzter, softwaregesteuerter Systeme gelingen. Ist dieser Prozess der Veränderung erfolgreich, so kann ein globaler Wettbewerbsvorteil entstehen. Die europäischen Produkte und Systeme würden neben der hohen Qualität, Langlebigkeit und Umweltverträglichkeit ebenfalls wegen Sicherheit punkten, da eine zukünftige Zusammenarbeit von vielen Fachdisziplinen bei Entwicklung und Bau der Systeme erfolgt. Durch diese Kooperation können komplexe Systeme problemlos ablaufen und Prozesse so einfach wie möglich gestaltet werden. Zudem lernen die Ingenieure die Komplexität einer Smart Factory zu steuern. Grundlegend dafür ist das Verständnis des Zusammenspiels der verschiedenen Disziplinen innerhalb einer modernen Produktionsumgebung. Es muss den Ingenieuren gelingen, die einfache Bedienung der heutigen mobilen Endgeräte auf die Prozesse und Produkte der industriellen Entwicklung und Produktion zu übertragen. Dieser Vorgang wird oftmals als *Simplicity* bezeichnet; s. (Sendler 2013, S. 16f.).

5.6 Organisatorische Risiken

Im Allgemeinen reduziert sich der Bereich der Smart Factory fast ausschließlich auf die Einführung neuer Technologien. Dennoch müssen organisatorische Risiken abgewogen werden. Wird dies nicht getan, besteht die Gefahr, dass die durch die Industrie 4.0 herbeigehenden

den Veränderungen zu erheblichen Problemen, fallendem Potential und Verzögerungen in der Implementierung von Industrie 4.0 führen; s. (Huber 2016b).

Die Aufbauorganisation eines Unternehmens spielt besonders in seiner höchsten Hierarchieebene eine signifikante Rolle. Hier muss das Management eine klare Strategie und einen Plan zur Digitalisierung definieren, um das Verständnis für die IT und die Prozesse aufzuzeigen. Organisationsmodelle müssen außerdem Kooperationen ebenso wie die Kommunikation zwischen allen Teilnehmern (Menschen und Maschinen) ohne Hierarchiehürden ermöglichen. Um die Mitarbeiter entsprechend auf die neuen Aufgaben in einer Smart Factory einstellen zu können, muss das Management ein Change-Team bzw. eine Change-Abteilung aufstellen – in der Realität wird dies oftmals nicht umgesetzt. Dies hat eine Art Neophobie zur Folge, wobei die neuen Aufgabenbereiche zunächst sehr kritisch betrachtet werden. Außerdem ist häufig eine sinkende Zufriedenheit der Mitarbeiter zu beobachten. Aus diesem Grund muss das Change-Team dafür sorgen, dass Kompetenzen ebenso wie die Qualifizierung der Angestellten des Unternehmens gegeben ist; s. (Huber 2016b).

Die neuen Technologien von Industrie 4.0 ändern sowohl die Arbeitsabläufe und -anforderungen der Ausbildungsplätze als auch das Berufsbild der einzelnen Tätigkeiten als solches. In der Produktion wird weitaus mehr Fachpersonal benötigt, gleichzeitig sinkt der Anteil der Mitarbeiter mit geringeren Qualifikationen, was auf die Digitalisierung zurückzuführen ist. Aktuell haben Unternehmen das Problem, dass viele ihrer Angestellten nicht in der Lage sind die neuen Technologien anzuwenden, da sie die neuen Prozesse nicht verstehen. „Lifelong learning“, Veränderungen in der Arbeitsorganisation, Teamzusammensetzung und Wissensmanagement werden auch noch in der Zukunft eine signifikante Rolle spielen; s. (Huber 2016b).

5.7 Wirtschaftliche Risiken

Zusätzlich zu den technischen und organisatorischen Risiken müssen nun die wirtschaftlichen Risiken abgewogen werden. Dazu wurden verschiedene Herausforderungen berücksichtigt. Die erste Hürde ist der fehlende Wille zu investieren – obwohl Investitionen in Industrie 4.0 im Moment relativ kostengünstig sind. Das größte Problem stellt jedoch die fehlende Transparenz des wirtschaftlichen Mehrwerts dar. So müssen Unternehmen in der Maschinenbau- und Anlagenindustrie schon heute zum Zeitpunkt der Investition die Anforderungen erwägen, die Produkte in der Zukunft haben werden. Grundsätzlich lässt sich feststellen, dass die Unternehmen die Relevanz von Investitionen in Industrie 4.0 in allen Sektoren schon lange erkannt und wahrgenommen haben. Unternehmen müssen die notwendigen Mittel für Investitionen und Ressourcen bereitstellen, damit eine Smart Factory umgesetzt werden kann. Studien zeigen, dass in Deutschland

jährlich 40 Milliarden Euro in Industrie 4.0-Anwendungen investiert werden; s. (Huber 2016b).

Ein weiteres Risiko ist der Verlust von Arbeitsplätzen innerhalb einer Smart Factory, da einfache Produktionsarbeiten durch die Digitalisierung ersetzt werden. Ziel der Einführung einer Smart Factory sollte es jedoch sein, die Automatisierung zu erhöhen und die Kosten zu senken und nicht, die Zahl der Arbeitsplätze zu reduzieren (Huber 2016b). Die Einführung einer Smart Factory verlangt den flexiblen Einsatz von Personal. Es gibt bereits starke Schwankungen im Personalbedarf. In Zukunft werden diese Schwankungen noch größer sein. Auch die Anforderungen an den Produktionsmitarbeiter in Bezug auf die Qualifikation ändern sich; s. (Huber 2016b). Akademischen Berufe wie Mathematiker, Informatiker, Berufe im Bereich der Naturwissenschaften und Technik müssen ebenso wie die nicht-akademischen Berufe der Mechatronik und Automatisierungstechnik weiter gefördert werden, um die hohe Nachfrage in der Wirtschaft zu befriedigen. Die Ausbilder müssen die Fähigkeiten der Auszubildenden in den Bereichen der Industrie 4.0-Technologien steigern. Durch interne Aus- und Weiterbildung wird sichergestellt, dass die Mitarbeiter in der Produktion auf dem neuesten Stand der Technik sind. Die Einführung der Smart Factory ermutigt die Mitarbeiter, sich selbst zu organisieren und damit mehr Eigenverantwortung zu übernehmen; s. (Huber 2016b).

Folglich kann der Verlust einiger Geschäftsbereiche als ein wirtschaftliches Risiko bezeichnet werden. Die neuen Marktteilnehmer verdrängen etablierte Hersteller wie Buchhandlungen und Verlage während sogenannte Start-ups den Herstellern neue Wege öffnen. Zudem ist die mangelnde Unterstützung der Forschung ein großes Hindernis. Deutschland investiert gut in Forschung und Finanzierung, jedoch investieren Länder wie China und Japan durch ihre höhere Investitionsbereitschaft besser im selben Bereich; s. (Huber 2016b).

Die festgestellten wirtschaftlichen Risiken deuten darauf hin, dass ohne Berücksichtigung dieser Fragen keine wettbewerbsfähige und vernetzte Produktionsumgebung entstehen kann.

6. Fazit

Dieses Dokument gibt dem Leser einen strukturierten Überblick über die Risiken, die in einer Intelligenten Fabrik auftreten können. Es werden verschiedene Risiken in den Bereichen Technologie, Organisation und Wirtschaft betrachtet. Befasst man sich etwas genauer mit den verschiedenen Risikobereichen wird allerdings deutlich, dass in vielen Bereichen noch Handlungsbedarf besteht. Unternehmen sind vor allem in den technischen Bereichen auf (Bundes-)Hilfen angewiesen, um die Digitalisierung der Wirtschaft voranzutreiben.

Die Implementierung von Industrie 4.0 gelingt nicht einzig durch die Hilfe der Bundesregierung, sondern erfor-

dert auch die Unterstützung der Unternehmen. Es ist notwendig, dass die Unternehmen und ihr Management für das Thema Smart Factory und Digitalisierung sensibilisiert werden und die Dringlichkeit einer Veränderung in der Produktion wahrnehmen. Wenn dies von den deutschen Unternehmen nicht berücksichtigt wird, wird sich diese Nichtbeachtung in den kommenden Jahren negativ auf die Wettbewerbsfähigkeit Deutschlands auswirken. Eine Anpassung der Produktionsmitarbeiter innerhalb der Smart Factory ist ebenfalls erforderlich.

Da die vierte industrielle Revolution erst am Anfang steht und noch die Möglichkeit besteht, die sich abzeichnenden Risiken klar zu erörtern, können so geeignete Gegenmaßnahmen ergriffen werden. Auf diese Weise können die Themen von Industry 4.0 erfolgreich umgesetzt und die sich abzeichnenden Potenziale genutzt werden.

Es konnten nicht alle Risiken einer vernetzten Produktionsumgebung angegangen werden. Ebenso wurden nicht alle Risiken detailliert und vollständig dargestellt. Es wurden ausgewählte Risiken beschrieben, die als relevant eingestuft wurden. Da dieses Thema sehr aktuell ist und sich noch in der Entwicklungsphase befindet, müssen die Untersuchungen parallel zum Entwicklungsfortschritt vorangetrieben werden. Aus diesem Grund sind weitere Untersuchungen in diesem Bereich notwendig und empfehlenswert, um einen vollständigen Überblick über die Intelligente Fabrik und ihren Status zu erhalten.

Literaturverzeichnis

Bauer, Wilhelm et al. (2018): Künstliche Intelligenz in der Unternehmenspraxis – Studie zu Auswirkungen auf Dienstleistung und Produktion

Bauernhansl, Thomas; Hompel, Michael ten; Vogel-Heuser, Birgit (Hg.) (2014): Industrie 4.0 in Produktion, Automatisierung und Logistik. Anwendung, Technologien, Migration. Wiesbaden: Springer Vieweg (SpringerLink). Online verfügbar unter <http://dx.doi.org/10.1007/978-3-658-04682-8>.

Botthof, Alfons et al. (2015): Zukunft der Arbeit in Industrie 4.0

Bundesamt für Sicherheit in der Informationstechnik (2016): Die Lage der IT-Sicherheit in Deutschland 2016. Hg. v. Bundesamt für Sicherheit in der Informationstechnik. Online verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2016.pdf?__blob=publicationFile&v=4, zuletzt geprüft am 06.12.2020.

Bundesministerium für Wirtschaft und Energie: Dossier "Industrie 4.0". Digitale Transformation in der Industrie. Unter Mitarbeit von Bundesministerium für Wirtschaft und Energie. Hg. v. Bundesministerium für Wirtschaft und Energie. Online verfügbar unter <https://www.bmwi.de/Redaktion/DE/Dossier/industrie-40.html>, zuletzt geprüft am 07.12.2020.

Die Bundesregierung (2017): Von der digitalen zur Gigabit-Gesellschaft. Breitbandausbau. Hg. v. Die Bundesregierung. Online verfügbar unter <https://www.bundesregierung.de/Content/DE/Artikel/2017/08/2017-08-30-breitbandausbau.html>, zuletzt geprüft am 06.11.2020.

Bischoff, Jürgen (Hg.) (2015): Studie "Erschließung der Potenziale der Anwendung von "Industrie 4.0" im Mittelstand". Studie im Auftrag des Bundesministeriums für Wirtschaft und Energie (BMWi). Unter Mitarbeit von agiplan GmbH, Fraunhofer IML und ZENIT GmbH. Online verfügbar unter http://www.zenit.de/fileadmin/Downloads/Studie_im_Auftrag_des_BMWi_Industrie_4.0_2015_agiplan_fraunhofer_iml_zenit_Langfassung.pdf, zuletzt geprüft am 25.11.2020.

Hankel, Martin; Rexroth, Bosch (2015): Industrie 4.0: Das Referenzarchitekturmodell Industrie 4.0 (RAMI 4.0). Hg. v. ZVEI - Zentralverband Elektrotechnik- und Elektronikindustrie e. V. Online verfügbar unter https://www.zvei.org/fileadmin/user_upload/Themen/Industrie_4.0/Das_Referenzarchitekturmodell_RAMI_4.0_und_die_Industrie_4.0-Komponente/pdf/ZVEI-Faktenblatt-Industrie4_0-RAMI-4_0.pdf, zuletzt geprüft am 02.12.2020.

Heinrich, Berthold (2017): Grundlagen zur Automatisierung: Springer Fachmedien (SpringerLink). Online verfügbar unter 10.1007/978-3-658-17582-5_1, zuletzt geprüft am 06.12.2020.

Huber, Walter (2016a): Industrie 4.0 in der Automobilproduktion. Ein Praxisbuch. Wiesbaden: Springer Vieweg.

Huber, Walter (2016b): Industrie 4.0 und die Risiken. Online verfügbar unter <https://www.computerwoche.de/a/industrie-4-0-und-die-risiken,3324008>, zuletzt geprüft am 15.11.2020.

Jasperneite, Jürgen (2012): Was hinter Begriffen wie Industrie 4.0 steckt. Internet und Automation. Online verfügbar unter <http://www.computer-automation.de/steuerungsebene/steuern-regeln/artikel/93559/>, zuletzt geprüft am 30.11.2020.

Jenker, Martin (2014): Cyber-Sicherheit für Steuer- und Regelungsnetzwerke. Cell-Zone-Site-Konzept. Hg. v. SPS Magazin. Online verfügbar unter http://www.spsmagazin.de/?inc=artikel/article_show&nr=87493, zuletzt geprüft am 06.12.2020.

Kagermann, Henning; Wahlster, Wolfgang; Helbig, Johannes (2013): Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0. Deutschlands Zukunft als Produktionsstandort sichern - Abschlussbericht des Arbeitskreises Industrie 4.0. Online verfügbar unter https://www.bmbf.de/files/Umsetzungsempfehlungen_Industrie4_0.pdf, zuletzt geprüft am 30.11.2020.

Kelkar, Oliver; Heger, Roland; Dao, Dan-Khanh (2014): Studie Industrie 4.0 - Eine Standortbestimmung der Automobil- und Fertigungsindustrie. Hg. v.

Mieschke Hofmann und Partner (MHP). Online verfügbar unter https://www.mhp.com/fileadmin/mhp.de/assets/studien/MHP-Studie_Industrie4.0_V1.0.pdf, zuletzt geprüft am 15.11.2020.

Krüger, Jörg et al. (2019): WGP Standpunkt, KI in der Produktion – Künstliche Intelligenz erschließen für Unternehmen

Mauerer, Jürgen (2016): Was ist was bei Industrie 4.0? Begriffe rund um die vernetzte Produktion. Online verfügbar unter <http://www.computerwoche.de/a/was-ist-was-bei-industrie-4-0,3313199>, zuletzt geprüft am 12.11.2020.

Meudt, Tobias; Pohl, Malte; Metternich, Joachim (2017): Die Automatisierungspyramide - Ein Literaturüberblick. Hg. v. Technische Universität Darmstadt. Online verfügbar unter <http://tuprints.ulb.tu-darmstadt.de/6298/1/2017%20-%20Die%20Automatisierungspyramide%20-%20Ein%20Literatur%C3%BCberblick-2.pdf>, zuletzt geprüft am 06.12.2020.

Münzl, Gerald; Pauly, Michael; Reti, Martin (Hg.) (2015): Cloud Computing als neue Herausforderung für Management und IT. Berlin: Springer Vieweg (essentials).

Plattform Industrie 4.0 (2015): Umsetzungsstrategie Industrie 4.0. Ergebnisbericht der Plattform Industrie 4.0. Online verfügbar unter <https://www.bitkom.org/Publikationen/2015/Leitfaden/Umsetzungsstrategie-Industrie-40/150410-Umsetzungsstrategie-0.pdf>, zuletzt geprüft am 12.11.2020.

Reinhart, Gunther et al.: Industrieroboter: Planung - Integration - Trends Ein Leitfaden für KMU, Würzburg 2018.

Ruskowski, Martin (2020): Von Industrie 4.0 zur KI in Service und Produktion. Vortrag. 16. Empolis Executive Forum 2019 in Berlin: 19.11.2020.

Schewe, Frank (2016): Was hinter der Referenzarchitektur RAMI 4.0 steckt. Industrie 4.0. Hg. v. computer-automation.de. Online verfügbar unter <http://www.computer-automation.de/steuerungsebene/steuern-regeln/artikel/129204/>, zuletzt geprüft am 06.12.2020.

Schonscheck, Oliver (2015a): Security-Konzept im Praxis-Check. IT-Sicherheit & Industrie 4.0. Spezielle Sicherheitskonzepte sind in Arbeit. Hg. v. Computerwoche. Online verfügbar unter <https://www.computerwoche.de/a/security-konzepte-im-praxis-check,3211303,2>, zuletzt geprüft am 06.12.2020.

Schonscheck, Oliver (2015b): Security-Konzepte im Praxis-Check. IT-Sicherheit & Industrie 4.0. IT-Sicherheitskonzepte noch nicht reif für die Industrie. Hg. v. Computerwoche. Online verfügbar unter <https://www.computerwoche.de/a/security-konzepte-im-praxis-check,3211303,3>, zuletzt geprüft am 06.12.2020.

Schröder, Christian (2016): Herausforderungen von Industrie 4.0 für den Mittelstand. Hg. v. Friedrich-Ebert-Stiftung. Online verfügbar unter

<http://library.fes.de/pdf-files/wiso/12277.pdf>, zuletzt geprüft am 06.12.2020.

Sendler, Ulrich (Hg.) (2013): Industrie 4.0. Beherrschung der industriellen Komplexität mit SysLM. Berlin, Heidelberg, s.l.: Springer Berlin Heidelberg (Xpert.press).

Stoitsi, Maria (2015): Die Vor- und Nachteile von ByoD. Enterprise Mobility Management. Hg. v. Computerwoche. Online verfügbar unter <https://www.computerwoche.de/a/die-vor-und-nachteile-von-byod,3213991>, zuletzt geprüft am 06.12.2020.

Termer, Frank (2019): Künstliche Intelligenz und ERP. Online verfügbar unter <https://www.bitkom.org/Bitkom/Publikationen/Kuenstliche-Intelligenz-und-ERP>, zuletzt geprüft am 10.11.2020

VDI/VDE-Gesellschaft (2013): Thesen und Handlungsfelder. Cyber-Physical Systems: Chancen und Nutzen aus Sicht der Automation. Online verfügbar unter https://www.vdi.de/uploads/media/Stellungnahme_Cyber-Physical_Systems.pdf, zuletzt geprüft am 30.11.2020.

Zillmann, Mario (2016): Smart Factory - Wie die Digitalisierung Fabriken verändert. Transformation von der Werkshalle bis zur Unternehmensleitung. Hg. v. Lünen-donk GmbH in Zusammenarbeit mit T-Systems und Produktion. Online verfügbar unter <http://luegendonk-shop.de/Luegendonk-Publikationen/Luegendonk-Whitepaper-Smart-Factory-Wie-die-Digitalisierung-Fabriken-veraendert.html>.