# 1 Einführung

Seit der Entstehung des Begriffs »Industrie 4.0« im Jahre 2011 wurden viele der Konzepte in die Praxis überführt. Die Digitalisierung der Produktionswelt ist in vollem Gange, neue datenbasierte Geschäftsmodelle entstehen und die Vernetzung von Produktionsanlagen schreitet immer weiter fort. Damit werden Unternehmen zukunftsfähig gemacht und ihre internationale Wettbewerbsfähigkeit bleibt erhalten.

Auf der anderen Seite steigt mit einer zunehmenden Vernetzung aber auch die Verletzbarkeit von produzierenden Unternehmen durch Angriffe von außen, insbesondere über das Internet. Schon der Roman Blackout [EL12] illustriert sehr anschaulich, welche Anfälligkeit aus einer breiten Vernetzung entstehen kann. Wenngleich es in dem Buch um den Angriff auf eine kritische Infrastruktur (Stromnetz) und nicht um eine Produktionsanlage geht, so ist dem Autor nach eigenen Angaben die Idee zu dem Buch wohl gekommen, als ihm am Beispiel der Produktion einer elektrischen Zahnbürste klar wurde, wie vernetzt unsere Gesellschaft ist, eben auch im Bereich der Produktion. Im Roman wurde plastisch dargestellt, dass die Gesellschaft auf eine solche Attacke nicht vorbereitet ist. Das falsche Sicherheitsgefühl, das im Roman geschildert wird, ist teilweise auch in der Realität zu beobachten, auch wenn es um die Entwicklung von Produktionsstandorten in Richtung Industrie 4.0 geht. Der Begriff Industrie umfasst dabei nicht nur das produzierende Gewerbe mit diskreter Fertigung, sondern auch Prozessindustrie und Landwirtschaft. Nicht nur im Roman, auch in der Wirklichkeit können Cyber-Angriffe nicht nur Computer lahmlegen, sondern in der Folge durchaus auch zur Gefährdung von Gesundheit und Umwelt führen.

> »Das Hauptziel von Safety ist der Schutz der Umgebung vor dem Fehlverhalten des Systems. Im Fokus steht die Unversehrtheit von Umwelt und Mensch. Sichere Systeme müssen sich konform zu ihrer korrekten Spezifikation verhalten und eine hohe Zuverlässigkeit und Fehlersicherheit gewährleisten. Systematische Fehler müssen in der Entwicklung vermieden, das Auftreten von zufälligen Fehlern durch Überwachung im laufenden Betrieb erkannt und erkannte Fehler beherrschbar gemacht werden, indem der Übergang in einen als sicher definierten Zustand ermöglicht wird. Durch die Verknüpfung dieser physischen, vormals von der Umgebung abgeschotteten Systeme mit IT, entstehen jedoch neue Herausforderungen für Safety-Experten, um die Sicherheit dieser Systeme weiterhin gewährleisten zu können.« [MHKT15]

In der traditionellen Welt der Produktion wurde unter Sicherheit immer die Sicherheit für Menschen und Umgebung verstanden (wir benutzen für diese Bedeutung den

englischen Begriff Safety, [MHTK15]). Nun rückt aber mit der zunehmenden Digitalisierung von Maschinen und Anlagen und ihrer Vernetzung untereinander, mit der klassischen IT und mit Akteuren außerhalb des Unternehmens immer mehr der Aspekt der informationstechnischen Sicherheit (Security)[1] in den Blickpunkt, bei dem es um den Schutz von Anlagen, Produkten und Daten vor unbefugtem Zugang, Missbrauch, Manipulation etc. geht [MHTK15]. Während Safety-Maßnahmen üblicherweise ihre Wirkung behalten, solange das System nicht verändert wird, veralten Security-Maßnahmen mit der Zeit durch gesteigerte Möglichkeiten von Angreifern (z. B. das Brechen immer größerer Schlüssellängen).

Dabei haben schon die Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0 [KWH13] im Jahr 2013 Sicherheit als erfolgskritischen Faktor für Industrie 4.0 herausgestellt. Gerade der umfangreiche, oft zeitkritische Datenverkehr innerhalb und außerhalb von Produktionsanlagen, der für Industrie 4.0 kennzeichnend ist, muss ausreichend abgesichert werden. Schließlich steht Industrie 4.0 auch für die Auflösung der klassischen Produktionsketten und ihre Ablösung durch dynamische Wertschöpfungsnetzwerke, die auch einen intensiven, Unternehmensgrenzen überschreitenden Datenaustausch erfordern.

> »Die Umsetzung von Industrie 4.0 in kleinen und mittleren Unternehmen geht mit einem erheblichen Anstieg des Vernetzungsgrades zwischen allen Systemen der Produktion einher. So findet Kommunikation und Datentransfer nicht nur zwischen Geräten einer Anlage oder zwischen Anlagen und ganzen Anlagenverbünden statt, sondern es verschwimmen in zunehmendem Maße auch die vertikalen Grenzen der klassischen Automatisierungspyramide.
>
> Im Gegensatz zur Industrie 3.0 findet unternehmensübergreifende Kommunikation nun auch zwischen den einzelnen Komponenten der gleichen Ebene der Automatisierungspyramide statt, was als horizontale Vernetzung bezeichnet wird. Es wird insbesondere eine starke Zunahme von Maschine-zu-Maschine (M2M)-Kommunikation erwartet. So können sich einzelne Maschinen in verteilten Wertschöpfungsnetzwerken einbinden, um bspw. eine optimale Lastverteilung zu ermöglichen. Daraus ergibt sich eine hohe Dynamik der Anlagenverbünde.« [BM16a]

Abbildung 1-1 und 1-2 illustrieren diesen Wandel [BM16a].

Je mehr autonom agierende Komponenten in der Produktion mitwirken, desto kritischer wird auch deren sichere und zuverlässige Anbindung an korrekte, vertrauenswürdige Daten. Während also schon durch die zunehmende technische Komplexität der Bedarf steigt, Systeme in jeder Hinsicht abzusichern, nehmen auf der anderen Seite erfolgreiche (und für die Opfer oft sehr kostspielige) Cyber-Attacken zu, auch in Bezug auf den von den Angreifern investierten Aufwand [BSI19e]. In einem späteren Kapitel gehen wir auf einige prominente Beispiele aus der jüngsten Vergangenheit ein.

In einem internationalen Benchmark [GK16] wurde gezeigt, dass Sicherheit eines der kritischen Fokusthemen für Deutschland ist (▶ Abb. 1-3).

---

1 Im Folgenden werden wir den Begriff Sicherheit immer im Sinne von Security gebrauchen, wenn es nicht ausdrücklich anders gekennzeichnet ist.

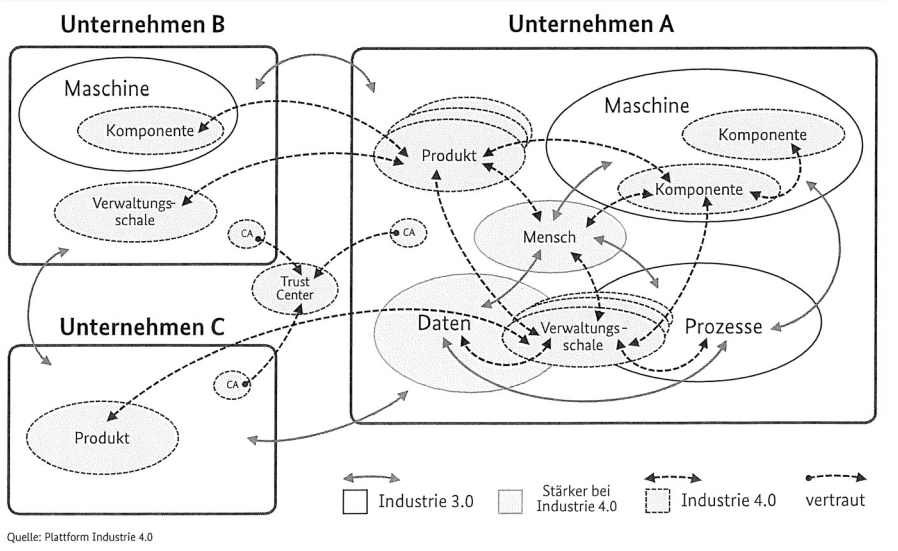


**Abb. 1-1:** Informationsfluss in Industrie 3.0 [BM16a]

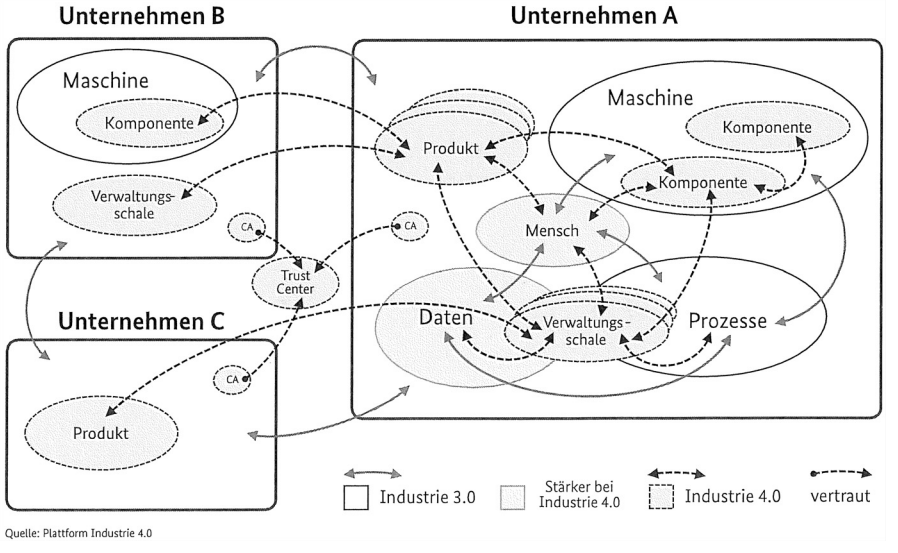


**Abb. 1-2:** Informationsfluss in Industrie 4.0 [BM16a]

Bereits in den erwähnten Umsetzungsempfehlungen wird Security by Design, d. h. das Einbeziehen umfänglicher Sicherheitsbetrachtungen als Entwurfsprinzip für Produktionsanlagen herausgestellt. Dort wurde ebenfalls gefordert, »IT-Sicherheitskonzepte, -architekturen und -standards zu entwickeln und zu etablieren, die für das

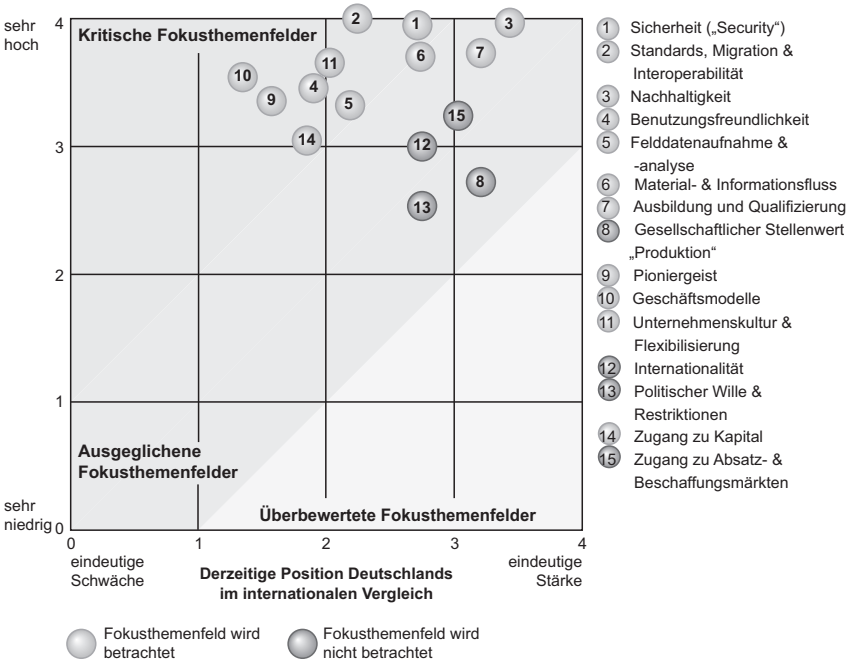


**Abb. 1-3:** Derzeitige Position Deutschlands im internationalen Vergleich [GK16]

Zusammenspiel dieser hochvernetzten, offenen, heterogenen Komponenten ein hohes Maß an Vertraulichkeit, Integrität und Verfügbarkeit herstellen«. Diesem Prinzip steht jedoch entgegen, dass die meisten Produktionsanlagen vor langer Zeit mit einem geringeren (oder nicht vorhandenen) Vernetzungsgrad und ohne Einbeziehung von Security-Überlegungen entworfen wurden. Für solche Anlagen müssen bei der Umstellung auf Industrie 4.0 auch adäquate Sicherheitsmaßnahmen getroffen werden. Erschwerend kommt hinzu, dass solche Sicherheitsmaßnahmen keinesfalls die Stabilität und Zuverlässigkeit der Produktion negativ beeinflussen oder die Produktionskosten spürbar steigern dürfen. Außerdem ist zu beachten, dass Sicherheitslösungen, die nicht benutzerfreundlich sind, zu ihrer Umgehung motivieren. Leichte Nutzbarkeit oder besser noch vom Benutzer unbemerkte Sicherheit sind also anzustreben. Dass Sicherheit für Industrie 4.0 nicht nur eine technische, sondern eine ganzheitliche Betrachtung erfordert, adressieren die Umsetzungsempfehlungen durch die ausdrückliche Nennung der Mitarbeiter, die bspw. entsprechend weitergebildet werden müssen, und durch den Hinweis auf die Relevanz von Datenschutzbestimmungen auch in diesem Umfeld. Dass gerade die Rolle der Mitarbeiter in Bezug auf Security nicht unterschätzt werden darf, zeigen die Top-10 Bedrohungen für »Industrial Control Systems« (also IT-Systeme im industriellen Einsatz), die das BSI 2019 veröffentlich hat [BSI19]. Hier steht menschliches Fehlverhalten auf Platz 3 mit stark steigender Tendenz (► Abb. 1-4)

| Top 10 Bedrohungen | Trend seit 2016 |
|---|---|
| Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware |  |
| Infektion mit Schadsoftware über Internet und Intranet |  |
| Menschliches Fehlverhalten und Sabotage |  |
| Kompromittierung von Extranet und Cloud-Komponenten |  |
| Social Engineering und Phishing |  |
| (D)DoS Angriffe |  |
| Internet-verbundene Steuerungskomponenten |  |
| Einbruch über Fernwartungszugänge |  |
| Technisches Fehlverhalten und höhere Gewalt |  |
| Kompromittierung von Smartphones im Produktionsumfeld |  |

**Abb. 1-4:** Die Top 10 Bedrohungen für Industrial Control Systems 2019 [BSI19]

Sicherlich haben auch die Umsetzungsempfehlungen dazu beigetragen, das Bewusstsein für die Wichtigkeit des Themas Security für Industrie 4.0 bei den Unternehmen zu erhöhen. Immer mehr wird verstanden, dass es nicht nur um den Schutz einzelner Systeme geht, sondern darum, das Kerngeschäft des Unternehmens zu schützen. Daher müsste Security eigentlich immer mitgedacht werden, wenn neue Geschäftsmodelle, Strategien, Services oder Produkte entwickelt werden. Es gibt jedoch noch keine Anzeichen, dass dieses tatsächlich in der Breite der Fall ist. Bedarf besteht allerdings, wie der Thread Intelligence Index 2019 zeigt [IBM19]. Dort wird angegeben, dass immerhin 10 % aller untersuchten Angriffe im Jahr 2018 sich gegen das produzierende Gewerbe richteten (▶ Abb. 1-5). Auch eine Untersuchung des TÜV Rheinland belegt eine Zunahme der Angriffe auf Operational Technology [TÜV19].

Das vorliegende Buch möchte Interessierten aus Lehre, Forschung und Praxis einen Überblick über die verschiedenen Aspekte des Themas Sicherheit (Security) für Industrie 4.0 geben. Dabei werden natürlich auch Bereiche angeschnitten, die nicht nur im Kontext Industrie 4.0 relevant sind. In jedem Fall soll aber der Bezug zu Industrie 4.0 klar herausgestellt und erläutert werden, welche Spezifika Industrie 4.0 im jeweiligen Kontext aufweist.

Es sollte deutlich werden, dass Sicherheit (Security) für Industrie 4.0 zum alles entscheidenden Nukleus wird [WK16], der die verbindliche Basis für die system-, unternehmens- und nationsübergreifenden Interoperabilität aller Prozessbeteiligten darstellt. Das Buch legt seinen Fokus auf die Erfassung und Modellierung von Bedrohungen und Risiken, weil nur ein Verständnis der Bedrohungen, daraus resultierenden Risiken und vor allem deren jeweilige Bewertung dazu führt, die Bemühungen um eine Erhöhung der Sicherheit auf die richtigen Fokuspunkte zu lenken. Wie wir zeigen werden, ist eine 100 %ige Absicherung nicht möglich. Gerade deshalb ist ein Bewusstsein über die jeweils zu adressierenden Schwerpunkte unumgänglich. Dabei gibt das Buch einen Überblick über die adressierten Themenfelder. Für sehr detaillierte Vertiefungen einzelner Aspekte verweisen wir jeweils auf

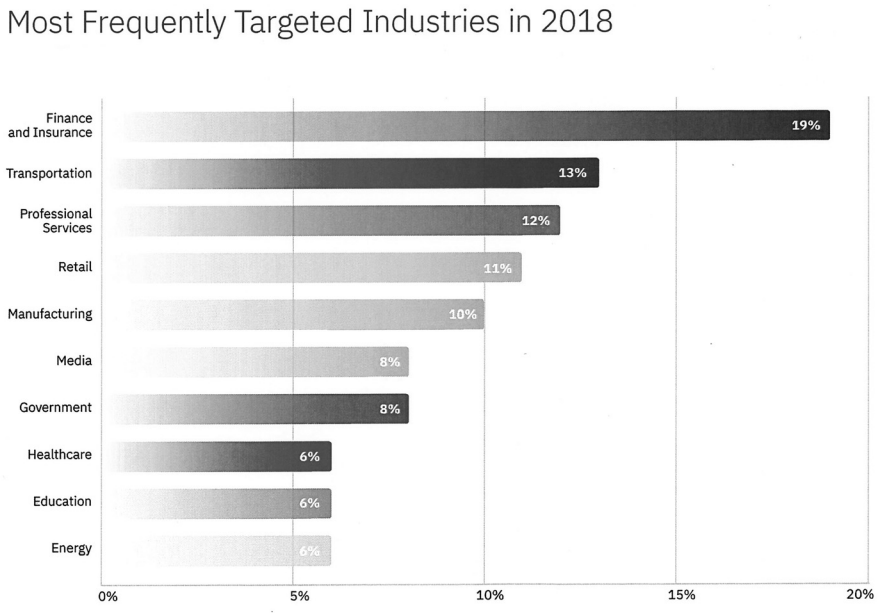


**Abb. 1-5:** Häufigste Angriffsziele 2019 [IBM19]

weiterführende Literatur. Gerade bei der Plattform Industrie 4.0[2] und den daran beteiligten Verbänden VDMA, ZVEI und BITKOM entstehen immer wieder neue Publikationen, in denen Aspekte von Industrie 4.0 vertieft werden, sei es in Bezug auf Architektur, Schnittstellen, Normen, Veränderungen der Arbeitswelt rechtliche Aspekte oder eben auch in Bezug auf Security.

Wir beginnen mit einer Heranführung, wie Security und Industrie 4.0 in Beziehung stehen. Dabei ist das Verständnis des durch Industrie 4.0 eingeleiteten Paradigmenwechsels grundlegend. Während Sicherheit im Sinne von Safety schon lange die industrielle Praxis bestimmt hat, gewinnt Security durch Industrie 4.0 immer mehr an Bedeutung. Wir legen dar, warum sich die aus der Office-IT bekannten Security-Konzepte leider nicht einfach auf Industrie 4.0 übertragen lassen. Nachdem wir gezeigt haben, dass es eine 100 %ige Sicherheit nicht geben kann, übertragen wir die Schutzziele der Security auf Industrie 4.0 und gehen auf Security By Design und Security At Large ein.

Für jedes Schutzziel zeigen wir Angriffsbeispiele, mit denen wir nicht nur verdeutlichen, dass die Bedrohung existiert und zunimmt, sondern auch, welchen wirtschaftlichen Schaden erfolgreiche Angriffe hervorrufen können.

Im Rahmen des Security by Design spielen die Begriffe Bedrohungsmodellierung und Bedrohungsanalyse eine wesentliche Rolle. Hinter beiden Begriffen steht die Idee,

2 https://www.plattform-i40.de

dass als grundlegende Voraussetzung für die Planung und Umsetzung adäquater Sicherheitsmaßnahmen zunächst ermittelt werden muss, welche Werte in einem Unternehmen, Prozess oder System überhaupt vorhanden sind und durch welche Gefahren diese Werte potentiell bedroht werden.

Die Bedrohungsanalyse eines Untersuchungsgegenstands liefert i. d. R. nicht einige wenige potentielle Bedrohungen, sondern eine Vielzahl möglicher Problemstellen. Jedoch besitzen nicht alle Bedrohungen die gleiche Relevanz hinsichtlich möglicher Schäden bzw. Verluste. Im Kontext begrenzter Ressourcen und Budgets ist es wichtig, Bedrohungen zu priorisieren und Maßnahmen zur Behebung der Bedrohungen effizient und ökonomisch planen und umsetzen zu können. Hierfür ist ein differenzierter Ansatz zur Modellierung und Analyse von Risiken notwendig.

Anschließend gehen wir auf verschiedene Aspekte der Umsetzung eines auf die Ergebnisse der Bedrohungsanalyse ausgerichteten Sicherheitskonzeptes ein, beginnend bei technischen Maßnahmen zur Erkennung von Sicherheitsvorfällen über Architekturen für die IT-Sicherheit bis hin zu organisatorischen Aspekten. Auch die Mitarbeiter sind ein wesentlicher Faktor für die Security.

Es gibt eine große Fülle von Normen und Standards, die im Kontext von Sicherheit in Industrie 4.0 relevant sind. Wir geben einen Überblick über die wichtigsten.

Anschließend werfen wir noch einen Blick auf rechtliche Fragestellungen, die mit IT-Sicherheit in Industrie 4.0 verbunden sind. Ein Begriff, den man traditionell nicht mit Produktion zusammendenkt, ist der Schutz personenbezogener Daten. Für Industrie 4.0 ist das Thema allerdings relevant, wie wir in einem eigenen Abschnitt darstellen. Neben den relevanten Grundlagen des Datenschutzrechts diskutieren wir die Berührungspunkte zu Industrie 4.0 und die speziellen Betrachtungen, die in diesem Umfeld nötig sind. Außerdem diskutieren wir, welche Implikationen das IT-Sicherheitsgesetz für das Thema Industrie 4.0 hat.

Abschließend wagen wir einen Ausblick auf die weitere Entwicklung der Security im Umfeld von Industrie 4.0.

# 2 Zum Begriff Security im Zusammenhang mit Industrie 4.0

In diesem Kapitel gehen wir darauf ein, warum die Einführung von Methoden und Konzepten der Industrie 4.0 überhaupt dazu führt, dass Security neu betrachtet werden muss. Hier spielt nicht nur eine neue Beziehung von Safety und Security zueinander eine Rolle, sondern auch die im Vergleich zur Office-IT, aus der die meisten IT-Sicherheits-Ansätze stammen, veränderte Gewichtung von Schutzzielen. Schließlich können manche Lösungen aus der klassischen IT im Umfeld von Industrie 4.0 nicht oder nur uneingeschränkt angewendet werden. Gerade im Industrie-4.0-Umfeld ist daher eine umfassende, ganzheitlich wirkende Betrachtung von Security erforderlich.

## 2.1 Paradigmenwechsel in der Produktion

Die vierte Industrielle Revolution bringt die Produktion zu Ihren Ursprüngen zurück, dem individuellen Produkt. Bisher auf Massenproduktion ausgerichtet, zielt die Industrie nun auf die wettbewerbsfähige Produktion kleiner Stückzahlen oder sogar Unikate. Hier schließt sich der Kreis zur handwerklichen Maßanfertigung unter Wahrung aller Industrialisierungsvorteile. Dem post-industrialisierten Europa eröffnet sich eine neue, agile und global wettbewerbsfähige industrielle Produktion.

### 2.1.1 Industrie gestern und heute

Die erste Industrielle Revolution ermöglichte es, große Stückzahlen von Produkten in hoher und gleichwertiger Qualität zu extrem günstigen Konditionen zu erzeugen. Die dafür entwickelten mechanischen Produktionsanlagen wurden in der zweiten Phase durch Elektrizität und Dampfkraft weiter beschleunigt und in eine komplett arbeitsteilige Organisation überführt. Heute, in der dritten Phase, ermöglichen speicherprogrammierbare Steuerungen und Enterprise Ressource Systeme die aktuelle Just-in-time- und On-demand-Fertigung.

Die Vision Industrie 4.0 verspricht als nächste Stufe die durchgehende Optimierung der industriellen Wertschöpfungskette von der Idee über die Entwicklung und Herstellung bis hin zur Lieferung, Wartung und Recycling durch konsequente digitale Vernetzung aller Wertschöpfungsinstanzen (▶ Abb. 2-1).


**Abb. 2-1:** Die Wertschöpfungskette

Vielfach wird Industrie 4.0 als neue Methode der Produktionsoptimierung verstanden. Diese Perspektive verkürzt den Blick auf die Entwicklung. Industrie 4.0 geht weit über reine Optimierung hinaus. Hier werden neue Produktionsweisen umgesetzt, die teilweise völlig neue Geschäftsfelder für die Akteure eröffnen. Darüber hinaus umfasst Industrie 4.0 auch das Treffen automatisierter Entscheidungen im Produktionsprozess aufgrund von Echtzeitdatenanalysen und Künstlicher Intelligenz. Auch eine neue Qualität der Maschine-zu-Maschine-Kommunikation und neuartige Mensch-Maschinen-Schnittstellen werden durch Industrie 4.0 möglich. Wie aber schon Abbildung 2-1 zeigt, umfasst Industrie 4.0 jedenfalls erstmals einen durchgängigen Produktlebenszyklus, der nicht nur Fernwartung und Service einschließt, sondern auch die Kommunikation mit dem Produkt *nach* der Produktion bis hin zum Recycling des Produkts. Schließlich bedeutet Industrie 4.0 zudem die Integration der Produktion mit der Betriebswirtschaft (also zusätzlich zu der klassischen Office-IT) und die Kommunikation (auch der Produktionssysteme) verschiedener Unternehmen untereinander bis hin zu dynamischen unternehmensübergreifenden Wertschöpfungsnetzen [BVZ15]. Sogar ein automatisierter Vertragsabschluss zwischen Maschinen ist Teil dieser Vision.

### 2.1.2 Paradigmenwechsel in der Produktion

In diesem Szenario werden Maschinen in der Produktionswelt von morgen viel autonomer interagieren, als wir uns gegenwärtig vorstellen können. Sie werden über eigene Identitäten verfügen, sich in Produktionsprozesse autonom integrieren, untereinander kommunizieren und Zugriff auf viele Informationen erhalten. Das führt wie bereits angesprochen schon heute teilweise zum Umdenken in Bezug auf mögliche neue Geschäftsmodelle. Daten werden in dieser Welt u.U. viel wertvoller sein als die Maschine, die sie erzeugt oder verarbeitet. Manche Hersteller von Werkzeugmaschinen haben das schon erkannt und setzen auf Vermarktungsstrategien für den Verkauf von Maschinendaten für Produktionsoptimierung. Die Maschine als »Asset« tritt in den Hintergrund, die Vermarktung von Dienstleistungen analog der Mobilfunkbranche wird sich mehr und mehr etablieren.

Das führt direkt zu Fragestellungen, die die Sicherheit von Daten, Maschinen und Produktionsumgebungen berühren. Wie können Konstruktions-, Produktions- und Kundendaten geschützt werden, durch welche Maßnahmen kann man die Integrität von Maschinen und deren Produktionsumgebung sicherstellen? Last but not least, wie schützt man eine völlig integrierte Produktionswelt von morgen gegen Angriffe, bei denen z. B. ein lokaler IT-Sicherheitsvorfall bei einem Produzenten die Produktion und Logistik des gesamten Bundesgebietes betreffen könnte?

## 2.2 Security meets Safety

Die digitale Transformation durchdringt mittlerweile fast alle Prozesse und Wertschöpfungsketten der Industrienationen. Dabei steigen der Grad der Automation und die damit einhergehende Autonomie der Systeme in bisher nicht vorstellbare Dimensionen. Durch Industrie 4.0 scheint es möglich zu werden, dass Maschinen ganz unter Ausschluss direkter menschlicher Interaktion Aufträge untereinander verhandeln. Im Bereich der Mobilität werden autonomes Fahren und autonomer Transport schon heute in bestimmten Bereichen sehr erfolgreich praktiziert. Zukünftig wird die Autonomie dieser Systeme weiter voranschreiten. Man kann mit Recht behaupten, dass autonome Systeme ein zentraler Innovationstreiber der Zukunft sein werden.

Wie jede Entwicklung birgt auch die fortschreitende Autonomie der Systeme Chancen und Risiken zugleich. Insbesondere die Fragestellung nach der Sicherheit der Systeme stellt sich unmittelbar. Während Sicherheit in der Vergangenheit oft als innovationsverlangsamend wahrgenommen wurden, bietet sich momentan die historische Gelegenheit, IT-Sicherheit als »Enabling-Factor« in dieser Entwicklung zu verankern. Es gibt nämlich zwei entscheidende Unterschiede zur Fragestellung der IT-Sicherheit in der klassischen IT. Zum einen können die Lessons-learned aus diesem Bereich nun gewinnbringend operationalisiert werden, zum anderen trifft IT-Sicherheit auf den bereits sehr etablierten Bereich der Safety dieser Systeme. Unter diesen Voraussetzungen ist leicht denkbar, dass IT-Sicherheit nun als Dimension der neuen Produktqualität »made in Germany« etabliert werden kann.

Natürlich muss dazu der Begriff Sicherheit neu gefasst und vor allen Dingen umfassend betrachtet werden. Es darf keine Trennung zwischen klassischer IT und I4.0-Systemen, sowie zwischen Safety und Security geben. In zunehmendem Maße können bei Industrie 4.0 Verletzungen der Security auch zu Verletzung der Safety führen. Ein einfaches Beispiel: Wenn die Unterbrechung einer Lichtschranke, die z. B. einen Gefahrenbereich abgrenzt, auf einem angreifbaren Weg an das verarbeitende System weitergeleitet wird und dieses Signal durch einen Angriff verloren geht, wird die Maschine im Gefahrenbereich fälschlicherweise nicht abgeschaltet werden, was zu einem Safety-Problem führt.

Die Autoren verstehen daher die Sicherheit der Zukunft als umfassende Sicherheit, die alles ganzheitlich betrachtet und gerade das Wechselspiel der Systeme berücksichtigt. Dabei umfasst Sicherheit ganz unterschiedliche Aspekte wie bspw. den Schutz des Betriebs (also den Schutz vor Sabotage), den Schutz geschäftsrelevanter und sensibler Informationen, den Schutz vor Systemen gegen unbefugte Zugriffe von außen und Datenschutz. Dieses Wechselspiel wird durch die zunehmende Vernetzung aller Systeme und Auslagerung von Daten und Diensten in Cloud-Umgebungen immer weiter voranschreiten.