Sichere IT-Systeme und sichere Kommunikation: zwei neuralgische Herausforderungen für Industrie 4.0

Stand des Artikels / der Informationen: 14. Oktober 2015

Inhaltsverzeichnis

Einleitung

Spätestens seitdem die Hannover Messe in den Jahren 2013 und 2014 das Thema „Industrie 4.0“ zum Leitmotto erklärte, wird die intelligente Vernetzung der Produktion als zentrales Zukunftsthema in Industrie, Politik, Presse und Wissenschaft kontrovers diskutiert.
Die sogenannte Industrie 4.0 basiert darauf, dass die Produkte selbst – z. B. per Barcode, RFID-Chip oder Smart Tags (das „Gedächtnis“ der Produkte) – die Maschinen informieren, was mit ihnen passieren soll. Das wird die gesamte Produktionslogik verändern: Intelligente Maschinen und Produkte, Lagersysteme und Betriebsmittel organisieren sich zukünftig selbstständig in echtzeitfähigen IT-Systemen – entlang der gesamten Wertschöpfungskette, von der Logistik über Produktion und Marketing bis zum Service und Qualitätsmanagement.

Auch wenn Anzahl und Tragweite der umgesetzten industriellen Lösungen den Versprechen einer revolutionären Entwicklung heute noch nicht standhalten, so wird die Digitalisierung und Automatisierung wesentliche Grundpfeiler unserer heutigen Arbeitswelt radikal verändern. Durch die Verbindung von physischer und virtueller Welt könnte Industrie 4.0 eine historische Zäsur darstellen, die das Format einer vierten industriellen Revolution hat und dauerhaft die Arbeitsbedingungen sowie wirtschaftlichen und sozialen Verhältnisse umgestalten wird. Gegenwärtig befinden wir uns auf dem Höhepunkt der dritten industriellen Revolution, bei der seit den 1970er-Jahren immer mehr Elektronik und Informationstechnologie eingesetzt wird, wodurch immer komplexere Produktionsabläufe wirtschaftlich werden.
Der durch Industrie 4.0 ausgelöste Strukturwandel wird wahrscheinlich gravierender und schneller ausfallen als die Veränderungen vergangener Jahrzehnte. Experten weisen Deutschland bei der Entwicklung eine Vorbildrolle zu, da durch den vergleichsweise hohen Industrieanteil die nötigen Voraussetzungen vorhanden sind, um Industrie 4.0 schnell voranzutreiben. Schon heute finden sich Anwendungen aus diesem Bereich bereits in vielen Unternehmen, besonders aus der Automobilbranche (53 Prozent), wie eine Umfrage des IT-Branchenverbandes BITKOM zeigte. Die Unschärfe des Begriffs Industrie 4.0 lässt zudem vermuten, dass weitere Projekte im Bereich echtzeitfähiger, intelligenter Vernetzung von Menschen, Maschinen und Objekten in den Unternehmen unter anderen Namen verfolgt werden. Doch welche Herausforderungen kommen damit generell und in Bezug auf Sicherheitsaspekte auf die Organisationen zu?

Im Folgenden geht es um Begrifflichkeiten, Ziele und Herausforderungen im Kontext von Industrie 4.0, aber vor allem sollen zentrale Aspekte zur Qualitätssicherung, Standardisierung und Informationssicherheit vorgestellt werden.

Begrifflichkeiten und Zielsetzungen im Kontext von Industrie 4.0

Eine allgemeingültige und verbindliche Definition des Begriffs „Industrie 4.0“, der 2011 erstmals in einem Beitrag für die VDI-Nachrichten verwendet wurde, gibt es bis heute nicht. Die Erklärungen reichen, je nach Blickwinkel und Interessenlage, von einer volkswirtschaftlichen Programmatik zur Stärkung des Industriestandorts Deutschland bis hin zur Umsetzung von Teilaspekten der Digitalisierung und Automatisierung industrieller Wertschöpfung. Am weitesten verbreitet ist die Arbeitsdefinition der von der Bundes-

regierung, Wirtschaftsvertretern, Gewerkschaftern und Wissenschaftlern betriebenen Plattform „Industrie 4.0“:

„Der Begriff Industrie 4.0 steht für (...) eine neue Stufe der Organisation und Steuerung der gesamten Wertschöpfungskette über den Lebenszyklus von Produkten. Dieser Zyklus orientiert sich an den zunehmend individualisierten Kundenwünschen und erstreckt sich von der Idee, dem Auftrag über die Entwicklung und Fertigung, die Auslieferung eines Produkts an den Endkunden bis hin zum Recycling, einschließlich der damit verbundenen Dienstleistungen.
Basis ist die Verfügbarkeit aller relevanten Informationen in Echtzeit durch Vernetzung aller an der Wertschöpfung beteiligten Instanzen sowie die Fähigkeit aus den Daten den zu jedem Zeitpunkt optimalen Wertschöpfungsfluss abzuleiten.
Durch die Verbindung von Menschen, Objekten und Systemen entstehen dynamische, echtzeitoptimierte und selbst organisierende, unternehmensübergreifende Wertschöpfungsnetzwerke, die sich nach unterschiedlichen Kriterien wie bspw. Kosten, Verfügbarkeit und Ressourcenverbrauch optimieren lassen.“ (Plattform Industrie 4.0: www.plattform-i40.de)

In der Vision von Industrie 4.0 kommunizieren vernetzte Werkstücke, Maschinen und Anlagen miteinander – entweder via Internet oder über Inhouse-Netze. Viele dazu notwendige Technologien sind bereits vorhanden, aber erst durch die Nutzung ihrer Synergieeffekte ergibt sich das revolutionäre Produktionsparadigma. Die technologischen Treiber, die Industrie 4.0 voranbringen, lassen sich dabei vier Kategorien zuordnen:

1. Cyber-physische (Produktions-)Systeme (CPS und CPPS):
   Miteinander vernetzte Maschinen und bewegliche Gegenstände, die mittels IT und kontinuierlichem Datenaustausch gesteuert werden. Das Produkt wird als intelligentes Werkstück zum aktiven Element im Produktionsprozess.
2. Integrierte Daten und Big Data:
   Die Vernetzung von Maschinen und Objekten für alle verfügbaren Daten – über die verschiedenen Stufen der Wertschöpfungskette (horizontal) und zwischen den Akteuren der Zulieferkette (vertikal). Große Datenmengen werden erfasst, in Echtzeit analysiert und für die Prozessanpassung zurückgeführt (Big Data).
3. Cloud-Technologien:
   Von jedem Ort aus Zugriff auf zentral gespeicherte Daten eines Prozesses über das Internet, die mittels bereitgestellter Verarbeitungs- und Analysesoftware bearbeitet werden können.
4. Additive Fertigungsverfahren:
   3D-Visualisierung und 3D-Druckverfahren. Dadurch wird es in vielen Fällen möglich, aus druckbarem Material Bauteile mit variablen Formen zu fertigen.

Zusammengenommen ermöglichen die beschriebenen Schlüsseltechnologien mittels laufender Auswertung von Daten aus der Produktion, Qualitätssicherung und Prozessparameter radikal veränderte Prozesse entlang der gesamten Wertschöpfungskette. Ziel ist letztendlich die intelligente Fabrik (Smart Factory), die sich durch Wandlungsfähigkeit, Ressourceneffizienz und Ergonomie auszeichnet. Mit ihren variablen und flexibleren, dezentral gesteuerten Produktionsanlagen erlaubt sie, individualisierte Lösungen mit einem geringeren Mehraufwand zu produzieren und zu verkaufen.

Zum Beispiel können die Eigenschaften von Produkten schon während der Entwicklungs- und Designphase getestet werden, was die Herstellung von Prototypen beschleunigt. Solche Simulationsverfahren, die sich in den vergangenen Jahren wesentlich weiterentwickelt haben, werden heute bereits u. a. in der Automobilindustrie genutzt. So lassen sich inzwischen nicht nur mehr einzelne Bauteile, sondern komplette Bauteilgruppen berechnen und optimieren. Der Trend geht sogar dahin, unterschiedliche Simulationsdisziplinen miteinander zu kombinieren (z. B. Strömungssimulation mit Festigkeitssimulation, Magnetfeldsimulation mit Thermischer Simulation). Dank schnellerer Rechner bzw. durch Einsatz von Rechen-Cluster lassen sich zudem die Simulationszeiten immer mehr verringern. Neben kürzeren Entwicklungszeiten ergibt sich darüber hinaus ein integrativer Entwicklungsansatz: Zulieferer und Hersteller arbeiten gemeinsam und parallel an der Produktentwicklung (Simultaneous Engineering). Im Ergebnis ist damit eine Kleinstserienfertigung bis hin zur „Losgröße 1“ ohne große Kostennachteile möglich.
Die oben beschriebenen Szenarien machen aber auch deutlich, wie sehr viel mehr als heute die Wertschöpfungsketten in Industrie 4.0 von hochverfügbaren und integren IT-Systemen abhängig sein werden. Deshalb muss die IT-Infrastruktur jedes Unternehmens betriebssicher genutzt werden – Stichworte sind hier Datenintegrität und Datenverlust – und es muss sichergestellt sein, dass die Anwendungen zur Verhinderung eines Produktionsstillstands stets einsatzbereit sind. Zu betrachtende Risiken sind etwa: Stromausfall, RZ-/Server-Ausfall, Netzwerkausfall, Attacken durch Schadprogramme (z. B. Stuxnet, Dudu und Flame) auf vernetzten Produktionsanlagen oder fehlerhafte Konfiguration von Maschinen (menschliches Versagen). Dementsprechend wird die Bedeutung von Informationssicherheit in Zukunft schon während der Planungs- bzw. Entwicklungsphase weiter zunehmen. Es gilt, eine digitale und organisatorische Sicherheit herzustellen, z. B. zur Vermeidung von Manipulation oder Diebstahl von vertraulichen Informationen. Die ISO 22301 (Business Continuity Management = BCM) und vor allem die ISO/IEC 27001 (Informationssicherheit) enthalten diesbezüglich bereits umfassende Herangehensweisen.

Im Zusammenhang von Industrie 4.0 darf ein Stichwort nicht fehlen: Das Internet der Dinge (Internet of Things = IoT), das zwar dem gleichen Themenkreis rund um Digitalisierung angehört, aber gegenüber Industrie 4.0 einen anderen Schwerpunkt setzt. Das Internet der Dinge strebt an, die Lücke zwischen realer und virtueller Welt zu schließen. Das geschieht über „intelligente Gegenstände“, sogenannte mit einer Sensorik ausgestattete Wearables, die in letzter Konsequenz den „klassischen“ Computer überflüssig machen. Bekannte Stichworte sind in diesem Zusammenhang beispielsweise Smart Home und Smart Car. Im besten Fall ist sich der Mensch der IT nicht mehr bewusst. So wird in diesem Sinne gerade die Datenbrille erprobt, doch erscheinen viele Projekte noch sehr zukunftsfern.
Bei Industrie 4.0 liegt der Schwerpunkt auf der Machine-to-Machine-Kommunikation (M2M) in der Entwicklung, Logistik und Fertigungstechnik, was vielerorts bereits in unterschiedlichen Zusammenhängen praktiziert wird. Angesichts der angestrebten und weiter oben beschriebenen intelligenten Fabrik ist Industrie 4.0 aber auch Teil des Internets der Dinge.

Industrie 4.0: eine Herausforderung für Unternehmen

Die intelligente Vernetzung der Produktion ist der nächste logische Schritt einer dynamischen, evolutionären Digitalisierung der weltweiten Wirtschaft. Diese Entwicklung hängt auch mit der heutigen Produktion zusammen, die in der Kapazitätsfalle steckt: d. h. Kunden kaufen nur Produkte, die ihren individuellen Anforderungen entsprechen. In den kommenden Jahren wird für Deutschland vor allem für die innerbetriebliche Logistik, die Fertigung und die indirekten Bereiche – also Bereiche, die nicht unmittelbar in die Erstellung der Leistung eingebunden sind (z. B. Verwaltung) – ein erheblicher Automatisierungsschub erwartet. Verglichen mit der medialen Präsenz des Themas und der Erwartungshaltung überrascht jedoch der derzeit geringe Durchdringungsgrad von Industrie 4.0. Die Unternehmen haben längst noch nicht mit der Umsetzung flächendeckend begonnen. Eine Umfrage, die das Fraunhofer Institut 2014 im Auftrag der Ingenics AG unter 518 Unternehmen vor allem der Automobilindustrie und aus dem Maschinen- und Anlagenbau durchführte, zeigte erstaunliche Ergebnisse: Es existiert nur in knapp einem Drittel (29 Prozent) der befragten Organisationen eine Strategie zu Industrie 4.0, die mehrheitlich von der Geschäftsführung verantwortet wird, und nur ein knappes Viertel hat ein Budget hierfür ausgewiesen. Als Haupt-hemmnisse werden die fehlende Veränderungsfähigkeit innerhalb der Organisation sowie fehlende technische Voraussetzungen angesehen. Fast ebenso viel Bedeutung wird dem Umgang mit der Arbeitnehmervertretung und dem Schutz mitarbeiterbezogener Daten beigemessen.

Zunächst jedoch ein Blick auf die Herausforderungen für die Unternehmen in Hinblick auf die Produktionsprozesse in einer Industrie-4.0-Umgebung: Die transparenten und flexibleren Abläufe machen es einfacher, Produktionsprozesse standortübergreifend zu optimieren – mit Blick auf ständig wechselnde Produktanforderungen, Qualität, Preis oder Ressourceneffizienz (flexible Fertigung). Aufgrund dieser Produktionsszenarien erwarten deshalb viele Unternehmen eine Effizienzsteigerung der Wertschöpfungskette, besonders eine effizientere Auftragsabwicklung. Gerade hier ergeben sich ganz neue Chancen für Produktion und Service: z. B. können individuelle Kundenwünsche dank der Rentabilität der Produktion von Kleinstmengen berücksichtigt werden.
Damit etablierte Anbieter nicht den Anschluss verlieren, müssen sie die Potenziale der Digitalisierung für ihre Produktions- und anderen Wertschöpfungsprozesse analysieren und nutzen. Der Abschlussbericht des „Arbeitskreises Industrie 4.0“ (April 2013) unterscheidet hier bei seinen Handlungsempfehlungen drei Stoßrichtungen:

1. Horizontale Integration über Wertschöpfungsnetzwerke
2. Durchgängigkeit des Engineering über die gesamte Wertschöpfungskette
3. Vertikale Integration und vernetzte Produktionssysteme

Bei einer optimalen Umsetzung fungieren die vernetzten Produktionsmodule als selbstständige Unternehmenseinheiten mit der Fähigkeit zur dynamischen Selbstorganisation, Selbstoptimierung und Integration in den Zielfindungsprozess. In Zeiten von Industrie 4.0 muss eine Produktionslinie dabei nicht auf ein Produkt festgelegt sein. Vorausgesetzt es gelingt eine intensive unternehmensübergreifende Kooperation zwischen Kunde und Zulieferer (vgl. Automobilindustrie), dann lassen sich die Bearbeitungsstationen auch flexibel an einen sich verändernden Produktmix anpassen – und Kapazitäten optimal auslasten (resiliente Fabrik).
Bevor das Potenzial von Industrie 4.0 jedoch voll ausgeschöpft werden kann, sind massive Investitionen in die IT-Systeme notwendig. Während die Netzwerk- und Breitband-Verfügbarkeit schon vielfach gegeben ist oder deren Ausbau vorangetrieben

wird, sind weitere Infrastrukturvoraussetzungen (IP-fähiger Maschinenpark, intuitive Benutzung oder Systeme zur Indoor-Ortung) erst in Grundzügen erkennbar. Darüber hinaus muss auch in die Datenqualität investiert werden. Dies betrifft zum Beispiel die Genauigkeit, Vollständigkeit und Aktualität der zur Verfügung stehenden Stammdaten der vielfach eingesetzten ERP- und MES-Systeme, die gegenwärtig vor allem offline genutzt werden.

Das revolutionäre Potenzial von Industrie 4.0 zeigt sich auch in den tiefgreifenden Veränderungen, die höchstwahrscheinlich auf die Arbeitswelt zukommen und von den Unternehmen auch so wahrgenommen werden (siehe Umfrageergebnisse weiter oben). So wird sich die Transformation der Geschäftsprozesse, nicht nur innerhalb des einzelnen Unternehmens, sondern auch von unternehmensübergreifenden Wertschöpfungsprozessen (Supply Chain), auf die Unternehmensorganisation und die Arbeitsprozesse der Mitarbeiter auswirken. Das betrifft vor allem den Einsatz der Ressource „Mensch“, denn aufgrund des hohen Automatisierungsniveaus durch CPS muss die Mensch-Maschine-Schnittstelle neu definiert werden: *„Die Technik ist nicht mehr länger passives Objekt, sondern wird zum handlungsfähigen Akteur (anpassungsintelligente Produktion).“* (Technische Universität Dortmund, Wandel von Produktionsarbeit – „Industrie 4.0“, Soziologisches Arbeitspapier Nr. 38/2014). Grundsätzlich stellt sich die Frage, inwieweit die Mitarbeiter zukünftig fähig sein werden, autonome Systeme zu kontrollieren, für diese verantwortlich zu sein und bei Störungen kompetent einzugreifen. Dies beinhaltet nicht nur eine IT-nahe Qualifikation und ein tiefes Prozess-Know-how, sondern auch die Einbindung von Erfahrungskompetenz, z. B. im Falle einer Störung, die nicht automatisiert abgebildet werden kann. Und trotzdem kann es passieren, dass der qualifizierte Facharbeiter möglicherweise nicht mehr gebraucht oder zu einfachen Hilfstätigkeiten, die nicht oder nur ineffizient automatisiert werden können, degradiert wird, weil seine Arbeitsschritte von intelligenten Produktionsmaschinen selbstständig geplant, gerüstet und ausgeführt werden. Hier werden sich bezüglich der Mitarbeiterqualifikation neue Dimensionen auftun. Um die Unternehmen auf diese anstehenden Entwicklungen vorzubereiten, sollten deshalb frühzeitig alle beteiligten Mitarbeiter eingebunden und Projekte zur Automatisierung und Digitalisierung der direkten und indirekten Geschäftsprozesse aufgesetzt werden. Eine Untersuchung der Bank Ing-DiBa lässt dabei vermuten, dass viele Berufsgruppen dem Risiko unterliegen, durch Industrie 4.0 in den nächsten 20 Jahren überflüssig zu werden; nicht nur Facharbeiter, sondern auch Ingenieure.
Wie in den gängigen Managementsystemen (ISO 9001 und ISO/IEC 27001) bereits gefordert, müssen die Unternehmen die notwendigen Kompetenzen der Mitarbeiter ermitteln und entsprechende Qualifizierungsprogramme aufsetzen. Das gilt insbesondere in Hinblick auf das Bewusstsein der Mitarbeiter, welche Auswirkung die eigene Tätigkeit auf die erbrachten Produkte und Dienstleistungen entlang der gesamten Prozesskette hat. Weitere Themen zur Einbindung der Mitarbeiter in den Umstellungsprozess auf Industrie 4.0 sind die betriebliche Mitbestimmung, flexiblere Arbeitszeitsysteme und individuellere Formen der Vergütung. Selbstorganisation und dezentrale Entscheidungsfindung gewinnen dabei an Bedeutung.

Die Automatisierung der Fertigungsprozesse (computer integrated manufacturing = CIM) macht bereits seit den 1990er-Jahren vielerorts Fortschritte, dagegen sind digitale Geschäftsmodelle nur in Ansätzen erkennbar. Dabei schätzt der Branchenverband HDE, dass der Anteil des Online-Handels am Einzelhandelsumsatz, derzeit bei rund 9 Prozent, bis 2020 auf 20 Prozent in Deutschland steigen wird. Und auch der

Branchenverband BITKOM rechnet bei cloudbasierten Dienstleistungen mit jährlichen Steigerungsraten von durchschnittlich 35 Prozent. Ähnliches gilt für die Vermarktung von Big Data, der Auswertung von Datenströmen intelligenter Objekte, auf deren Basis sich innovative Services und Angebote entwickeln lassen. Digitalisierung und Automatisierung eröffnen also neue Wege der unternehmerischen Ausrichtung, die das Potenzial für große Wachstumssprünge besitzen, weil sie den Vergleich, die Vermittlung und die Koordinierung von Diensten und Dienstleistern revolutionieren – über Social-Media-Analysen, Open-Innovation-Plattformen und Big-Data-Anwendungen. Weitere Stichworte in diesem Zusammenhang sind Shared Economy (Dienste, Produkte oder Inhalte werden gemeinsam genutzt) und „hybride" Geschäftsmodelle (Smart Services).
Das volle Potenzial von Industrie 4.0 wird sich hier am besten ausschöpfen lassen, wenn alle Akteure – kreative Start-ups und etablierte Unternehmen – auf der Basis eines Erfahrungsaustausches zusammenarbeiten. Ein Schritt in diese Richtung war die Gründung der Plattform „Industrie 4.0" durch die Branchenverbände VDMA, ZVEI und BITKOM im April 2013, die mittlerweile auch von der Bundesregierung, den Gewerkschaften und der Wissenschaft getragen wird und den anstehenden digitalen Strukturwandel in der Industrie koordinieren und geordnet gestalten soll.

Standardisierung

Mit der Aufnahme des Themas „Industrie 4.0" als eines von zehn Zukunftsprojekten in die Hightech-Strategie der Bundesregierung hat die deutsche Politik die Initiative ergriffen, um die digitale Transformation von Wirtschaft und Gesellschaft aktiv zu begleiten. Zunächst unterstützte das Bundesministerium für Bildung und Forschung (BMBF) den „Arbeitskreis Industrie 4.0", getragen von der Deutschen Akademie der Technikwissenschaften sowie den Branchenverbänden BITKOM, VDMA und ZVEI, der seinen Abschlussbericht 2013 an Bundeskanzlerin Angela Merkel übergeben konnte. Inzwischen beteiligen sich das BMBF und das BMWi (Bundesministerium für Wirtschaft und Energie) an der Plattform „Industrie 4.0". Aber auch darüber hinaus will die Bundesregierung aktiv sein: Weitere Maßnahmen sollen das Vertrauen in die für Industrie 4.0 so wichtige IT-Sicherheit stärken. So soll das im Juni 2015 verabschiedete IT-Sicherheitsgesetz nicht nur «kritische Infrastrukturen» (z. B. Krankenhäuser oder Energieversorger) besser vor Cyberangriffen schützen, sondern Unternehmen müssen in Zukunft Mindeststandards bei der IT-Sicherheit erfüllen.

Damit ein reibungsloser Informations- und Produktionsfluss gewährleistet ist, müssen sich alle Akteure und Elemente „verstehen". Maschinen unterschiedlicher Hersteller müssen miteinander arbeiten können, d. h. sichere, standardisierte Schnittstellen und Baukastensysteme werden notwendig. Hinzu kommen eine Vielzahl von Schnittstellen zu weiteren Leittechnik-Systemen, z. B. Fernwartungsschnittstellen zu Service Providern und Herstellern oder Schnittstellen zum Office-Netz. Das kann nur mit Standards in der Referenzarchitektur gelingen, die den Rahmen für die Entwicklung, Integration und den Betrieb der relevanten technischen Systeme bildet. Der Zugang zu verifizierbar vertrauenswürdigen Technologien ist deshalb von entscheidender Bedeutung für den Erfolg von Industrie 4.0.
Der Qualität als Zielgröße einer Industrie 4.0 kommt also gerade in Hinblick auf die IT-Sicherheit eine zentrale Rolle zu. Die Mehrzahl der vom Fraunhofer Institut befragten Unternehmen geht denn auch davon aus, dass die Bedeutung von Qualitätsthemen

und -prüfungen weiter zunehmen wird. Nicht von ungefähr erwartet das DIN-Institut Hunderte neuer Normen zu Industrie 4.0. Es will für eine Bündelung deutscher Interessen sorgen, indem es die relevanten Experten und Institutionen an einem Tisch zusammenführt. Die Ergebnisse sollen dann in internationale Normen und Standards einfließen. Deshalb engagiert sich das DIN-Institut auch besonders für die ISO-Strategiegruppe 4.0, die Anfang August 2015 vom Technical Management Board der International Standard Organization (ISO) eingerichtet wurde und die u. a. eine Bestandsermittlung der derzeit vorhandenen Normen in Hinblick auf Industrie 4.0 durchführen soll, um Normungslücken aufzudecken. In die gleiche Richtung weist der Ende Juli unterzeichnete Kooperationsvertrag mit dem US-basierten Industrial Internet Consortium (IIC), in dem die Identifizierung von Standards für Industrie 4.0 vereinbart wurde.

Wenn sich der gesamte industrielle Prozess durch Industrie 4.0 ändert, Innovationszyklen kürzer werden und neue Technologien genutzt werden, müssen sich die rechtlichen Regelungen, zum Beispiel beim Eigentums- und Urheberrecht, nicht nur wandeln. Sie müssen auch mit der Entwicklung neuer Geschäftsmodelle Schritt halten, denn dann geben sie Sicherheit, schaffen Akzeptanz und wirken innovationsfördernd. Die Voraussetzung dafür: Die rechtliche Analyse neuer Technologien muss frühzeitig beginnen – und nicht erst, wenn Industrie 4.0 angekommen ist. Bislang sind jedoch zentrale datenschutzrechtliche Fragen ungeklärt: Welche Daten werden erhoben und wem gehören sie? Wenn Daten zur Fernwartung ausgelesen werden, gehören die Daten dann dem Hersteller? Sind personenbezogene Daten auch betroffen? Es besteht, wie schon so oft, die Gefahr, dass Standards gesetzt werden und erst hinterher dafür Regeln geschaffen werden. Immerhin weist die internationale Norm für Datenschutz- und Datensicherheit beim Cloud-Computing, die ISO/IEC 27018 (veröffentlicht August 2014), hier in die richtige Richtung. Angesichts der steigenden Zahl cloudbasierter Dienstleistungen wird ihre Bedeutung in Zukunft sicher weiter zunehmen, denn die intelligenten Objekte, zentrales Merkmal der Digitalisierung, generieren zahlreiche Informationen, die über Firmengrenzen hinweg übermittelt werden.

Risiken und IT-Sicherheit im Zusammenhang mit Industrie 4.0

In der Industrie 4.0 müssen IT-Sicherheitsaspekte an Bedeutung gewinnen. Anlagen und Produkte, aber auch Daten und Know-how müssen verlässlich vor unbefugtem Zugriff und Missbrauch geschützt werden. Unternehmen gegen IT-Angriffe sichern! Das wird eine der zentralen Herausforderungen sein, deren akzeptable Lösung mit über den Erfolg von Industrie 4.0 entscheidet.

Die Dezentralisierung des Datenverkehrs fordert neue Strukturen und Technologien für Netzwerke und Datenmanagement. Hinsichtlich Performance und Latenzzeiten steht die prozessnahe IT höheren Anforderungen gegenüber: einmal, weil immer größer werdende Datenmengen schnell verarbeitet werden müssen, und zum anderen, weil die Anforderungen an Verfügbarkeit und Sicherheit der zu verarbeitenden Informationen (Integrität) gleichzeitig steigen. Deshalb wird es sicherlich Zielkonflikte zwischen IT-Sicherheit und Verfügbarkeit der Anlagen geben. Eine wesentliche Problematik der industriellen Steuerungssysteme (Industrial Control Systems = ICS: IT-System inkl. Netzwerke) besteht darin, dass sich bis dato noch keine Sicherheitskultur etabliert hat (im Vergleich zur kommerziellen IT). Prozessnahe IT-Systeme (z. B. Firmware) sind

Bestandteil der Anlagen und haben andere und zwar längere Zeithorizonte als die kommerzielle IT (bis zu 20 Jahren). Die IT-Sicherheit ist dabei meist nicht ein primäres Ziel der Anlagenhersteller. Andererseits hat der Betreiber der Anlage oft kein Detailwissen über die von ihm genutzten IT-Technologien. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat zu dieser Problematik das „ICS Security Kompendium" entwickelt, um die Betreiber von Industrieanlagen bei der Absicherung ihrer Produktions- und Steuerungssysteme zu unterstützen. Das Kompendium gibt einen Überblick über die wesentlichen Bedrohungen für industrielle Kontrollsysteme (organisatorische Bedrohungen, menschliche Fehlhandlungen und vorsätzliche Handlungen). Darüber hinaus werden Sicherheitsmaßnahmen (Best Practices) für die Planung, das Design und die Implementierung von ICS vorgestellt und es findet sich eine Darstellung zur Methodik von Audits bei ICS-Systemen.
Die häufig im Einsatz befindlichen SCADA-Systeme (Supervisory control and data acquisition) sind die Schnittstelle zwischen den Host-Systemen und den ICS-Netzwerken. Sie überwachen und kontrollieren die ICS-Komponenten. Bis dato waren diese SCADA-Systeme auf proprietären Plattformen angesiedelt, mit einer eigenen Kommunikationsinfrastruktur und ohne Internetanschluss. In Hinblick auf Industrie 4.0 streben IT-Spezialisten nun für solche Systeme eine übergreifende (Internet-) Vernetzung an, damit werden sie zukünftig aber auch den klassischen Gefahren der IT-Sicherheit ausgesetzt. Die einstigen Entwickler konnten dies jedoch nicht vorhersehen und so sind diese Systeme nie dafür ausgelegt und die oben dargestellten Bedrohungsszenarien nie betrachtet worden.
Hinzu kommt, dass bei der Steuerung von kompletten Fertigungsanlagen die Werte von Sensoren in Echtzeit vorliegen müssen; denn bei Störungen (z. B. Virenbefall) kann die Anlage meist nicht einfach so vom Netz genommen werden, ohne die Betriebssicherheit zu gefährden (z. B. Chemieindustrie, Kraftwerke). Wie ein solcher Störfall aussehen könnte, zeigte bereits vor einigen Jahren das Beispiel des erfolgreich in iranische Atomanlagen eingeschleusten Virus „Stuxnet“: Die Uranzentrifugen kamen sehr schnell in den roten Drehzahlbereich. Genutzt hatte Stuxnet übrigens Sicherheitslücken in den Steuerungssystemen von Siemens (Simatic S7).
Doch trotz der potenziellen Bedrohungen oder solcher beispielhaft genannten Vorfälle sind die Automatisierungs-, Prozesssteuerungs- und Prozessleitsysteme derzeit immer noch nicht im Fokus der IT-Sicherheit. Das muss sich für Industrie 4.0 grundlegend ändern!
Durch die Auflösung der „Insellösungen“ und der starken Vernetzung mit einer Vielzahl von anderen Systemen, einschließlich der Office-Umgebung, ergeben sich auch neue Anforderungen an die Netzwerkumgebung. Nicht nur die Verfügbarkeit des Netzwerkes, sondern ebenso die Netzwerksegmentierung als Schutzmaßnahme müssen Unternehmen in Betracht ziehen. Zugriffsberechtigungskonzepte, Authentifizierungsverfahren, Verwendung von sicheren Netzprotokollen, um nur einige Beispiele zu nennen, sind zu definieren und umzusetzen.

Mit der zunehmenden Vernetzung und dem Austausch großer Datenmengen in der Industrie 4.0 müssen die Sicherheitsanforderungen in jedem Unternehmen also steigen. Maßnahmen zur Steigerung der Angriffssicherheit werden aber bislang nur langsam und oft lediglich als Lösung von Teilaspekten realisiert, obwohl die Weiterentwicklung zur Industrie 4.0 Ansätze erfordert, die einen umfassenden Schutz der hochgradig vernetzten Systemstrukturen sowie des Daten- und Informationsaustausches sicherstellen. Betriebsbedingt stellt schon das regelmäßige und zeitnahe Patchen eine Herausforderung dar. Dabei erschweren die oft unzureichende Herstellerunterstützung

und die Kritikalität der Anlagen (Verfügbarkeit) zusätzlich ein geregeltes Patch-Management. Ein profundes Risikomanagement, schon bei der Planung und Implementierung der IT-Systeme, ist hier Voraussetzung für ein erfolgreiches Security-Management.
Um Informationssicherheit in der Industrie 4.0 zu gewährleisten, ist ein proaktives Vorgehen entscheidend, wie es heute schon die Norm ISO/IEC 27001 vorsieht, die einen ganzheitlichen Ansatz hat. Als Managementsystem konzentriert sie sich nicht nur auf die Implementierung von Sicherheitsmaßnahmen, sondern fordert ebenso Management Attention und ständige Anpassung zur Verbesserung des Systems. Zu diesem generischen Forderungskatalog stellt die ISO/IEC TR (Information security management guidelines based on ISO/IEC 27019 for process control systems specific to the energy utility) eine sinnvolle Ergänzung dar, die zu den Anforderungen eine Hilfestellung bei der Implementierung von technischen und organisatorischen Maßnahmen gibt.
Es genügt nicht, nachträglich Security-Funktionen in einem Managementsystem zu ergänzen, wenn es schon Sicherheitsvorfälle gab. Das Thema muss von Anfang an mitgedacht werden – zugeschnitten auf die Prozessabläufe im Unternehmen. Zudem ist mit der zunehmenden Vernetzung und Zusammenarbeit verschiedener Partner ein starkes Vertrauen in den jeweils anderen erforderlich. Verlässliche Konzepte, Architekturen und Standards im Bereich der IT-Sicherheit sollten diese Vertrauensbasis unterstützen, denn Hersteller und Betreiber benötigen die Sicherheit, dass ihr Know-how, ihr geistiges Eigentum und ihre Daten geschützt sind. Die Herausforderung für die Unternehmen besteht deshalb darin, bestehende Managementsysteme für die neuen Anforderungen von Industrie 4.0 auszurüsten und gleichzeitig Lösungen für neue Anlagen zu entwickeln.

Die Vorsorge auf Unternehmensebene ist umso wichtiger, als festzuhalten bleibt: Eine technische oder digitale Souveränität ist derzeit im Bereich IT-Sicherheit weder auf deutscher noch auf europäischer Ebene gegeben.
Deshalb will die Bundesregierung zumindest auf nationaler Ebene das Vertrauen in IT-Sicherheit stärken. Diesem Ziel und explizit in Hinblick auf Industrie 4.0 dient ein Referenzprojekt des BMBF zum Schutz der Produktion vor Cyberangriffen und Spionage. Im Zusammenwirken von deutscher Industrie und sieben Forschungseinrichtungen und Universitäten gilt es, verlässliche Lösungen zu entwickeln, die auch für kleine und mittlere Unternehmen funktionieren und entlang der gesamten Wertschöpfungskette genutzt werden können. Dieser Ansatz findet die volle Unterstützung des Verbands Deutscher Maschinen- und Anlagenbauer (VDMA), denn der jährliche Schaden durch Industriespionage in Deutschland beläuft sich laut einer Studie von Corporate Trust aus dem letzten Jahr auf 11,8 Milliarden Euro! Die im Projekt entwickelten IT-Sicherheitslösungen sollen standardisiert werden, um den Wettbewerb nicht zu behindern und kostengünstige Lösungen für kleine und mittlere Unternehmen zu schaffen.
Ziel aller Standardisierungen und aller technischen und organisatorischen Maßnahmen zur Informationssicherheit muss es sein, eine Balance zu finden, die Deutschlands hohe und bisweilen hart erkämpften Standards schützt, gleichzeitig aber genügend Raum für innovative Ideen und Konzepte lässt. Offenheit und Vertrauen sowie eine digitale Medienkompetenz der Nutzer müssen dabei vorausgesetzt werden. Das BMWi hat darüber hinaus gemeinsam mit dem IT-Branchenverband BITKOM im Juli 2015 die Plattform „Innovative Digitalisierung der Wirtschaft “ ins Leben gerufen, die die Arbeit

der Plattform „Industrie 4.0“ ergänzt. Die Ergebnisse, die dort gewonnen werden, sollen in einer „Digitalen Charta 2025“ zusammengefasst werden.

Fazit

Industrie 4.0 wird kommen, sie könnte die erste industrielle Revolution mit Ansage sein! Die fortschreitende Automatisierung und Digitalisierung hin zu einer Smart Factory, in der intelligente Objekte, Systeme und Menschen in einer dynamischen, echtzeitoptimierten und selbst organisierenden Weise miteinander vernetzt sind, wird künftig der wichtigste Innovationstreiber für die industrielle Wertschöpfung sein. Im Moment ist Industrie 4.0 jedoch noch eher die Vision eines evolutionären Prozesses in der Zukunft, dessen Wahrnehmung in Industrie, Politik und Gesellschaft aber stetig wächst.

Die digital vernetzten Produktionsumgebungen und intelligenten Wertschöpfungsketten werden die Produktionsweise, bestehende Geschäftsmodelle und die Arbeitswelt in Deutschland nachhaltig verändern. Relevante Produktivitätssteigerungen durch Industrie 4.0 sind aber erst zu erwarten, wenn sich die Technologienutzung in effektiveren und effizienteren Produktionsprozessen niederschlägt und die IT-Sicherheit der Unternehmen gewährleistet ist. Dabei kann es für die Einführung insgesamt keine einheitliche Umsetzung geben, da die individuellen Ausgangssituationen je nach Unternehmen, Branche, Unternehmenskultur sowie Fertigungsprozess verschiedene Implementierungszeiträume, Migrationsstrategien und IT-Systeme benötigen. Doch sollte schon heute jedes Unternehmen sein Leistungsangebot und das Portfolio auf innovative digitale Dienste und Produkte überprüfen und dementsprechend aufbauen.

Standardisierungsfragen werden bei der Herstellung einer technologischen Souveränität, die vor Cyberkriminalität schützt und sichere Daten gewährleistet, eine zentrale Rolle spielen, um verifizierbar vertrauenswürdige Technologien bereitzustellen. Die Industrial-Control-Systeme waren dabei nie auf die Anforderungen einer Industrie 4.0 ausgelegt. Eine hochverfügbare und vor allem sichere IT zu entwickeln, stellt deshalb die große technische Herausforderung für die digitalisierte und stark vernetzte Welt von morgen dar. Denn nur eine umfassende, durch Know-how und Standards abgesicherte IT-Sicherheit wird das weitgehend fehlerfreie Funktionieren von Industrie 4.0 gewährleisten können! US-amerikanische und asiatische Unternehmen haben hier bereits viele wichtige Standardisierungsentscheidungen getroffen. Europa muss deshalb dringend faire und gleiche Wettbewerbsbedingungen sowie hohe Standards für die Informationssicherheit schaffen, damit der Informations- und Datenschutz gewahrt bleibt. Die Sicherheit der Systeme und der Schutz der Daten sind somit zentrale Querschnittsthemen von Industrie 4.0 und jedes Unternehmen sollte schon im Vorfeld geeignete Maßnahmen hierzu entwickeln. Einer der Wegweiser kann dabei unter anderem die ISO/IEC 27001 sein.
IT-Sicherheit und Kommunikationssicherheit sind also die neuralgischen Punkte! Hier entscheidet sich, ob Industrie 4.0 ein Erfolg wird oder nicht.

Quellen und weiterführende Links

http://www.acatech.de/?id=2240

http://ap-verlag.de/industrie-4-0-anwendungen-fuehren-zur-digitalisierung-der-fabriken/8384/

http://www.bmwi.de/BMWi/Redaktion/PDF/I/industrie-4-0-und-digitale-wirtschaft.pdf

https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Themen/IKT-gestuetzte_Technologiebereiche/SCADA/scada_node.html

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security_kompendium_pdf.pdf?__blob=publicationFile

http://www.computerwoche.de/a/industrie-4-0-ist-das-internet-der-ingenieure,2538117

http://www.deutschlandfunk.de/industrie-4-0-entwickler-verlangen-mehr-sicherheitsforschung.684.de.html?dram:article_id=288574

http://www.daserste.de/information/wirtschaft-boerse/plusminus/sendung/industrie-revolution-roboter-jobs-gefahr100.html

http://www.dgq.de/wp-content/uploads/2014/03/Industrie4_0.pdf

https://www.enisa.europa.eu/media/press-releases/prs-in-german/konnen-wir-von-industriellen-Kontrollsystemen-scada-zwischenfsllen-lernen

http://www.ict5.de/index.php/industrie-4-0.html

https://www.ingenics.de/de/news/aktuelles/industrie40_ergebnisse.php

http://www.itwissen.info/definition/lexikon/supervisory-control-and-data-aquisition-SCADA.html

http://www.plattform-i40.de/

http://politik-digital.de/category/themen/internet-der-dinge-themen/

http://www.xing-news.com/reader/news/articles/98554?newsletter_id=7509&xng_share_origin=email

Abkürzungsverzeichnis

BCM: Business Continuity Management
BMBF: Bundesministerium für Bildung und Forschung
BSI: Bundesamt für Sicherheit in der Informationstechnik
BMWi: Bundesministerium für Wirtschaft und Energie

CIM: computer integrated manufacturing
CPS: Cyber-physische Systeme
CPPS: Cyber-physische Produktionssysteme

ICS: Industrial Control Systems
IIC: Industrial Internet Consortium
IoT: Internet of Things
IP: Internet-Protokoll
ISO: International Standard Organization
ISO/IEC TR: Information security management guidelines based on ISO/IEC 27019 for process control systems specific to the energy utility

SCADA-Systeme: Supervisory control and data acquisition systems

VDMA: Verband Deutscher Maschinen- und Anlagenbauer

ZVEI: Zentralverband Elektrotechnik- und Elektronikindustrie e.V.

Die Autoren

Andreas Altena, IT-Kaufmann und Betriebswirt, ist Geschäftsführer der **Sollence GmbH** in Krefeld. Seine Kernkompetenzen sind Qualitäts-, Informationssicherheit-, Datenschutz- und (IT-)Service-Managementsysteme, Service-Excellence sowie integrierte Systeme.
Über seine Tätigkeit als Geschäftsführer hinaus begutachtet er seit 2007 als DQS-Excellence-Auditor national und international Managementsysteme in den genannten Bereichen. Seit 2012 ist er Trainer und Experte für die DGQ-Weiterbildung in den Bereichen Qualitätsmanagement, Informationssicherheit und in der Auditorenausbildung.
Er ist Autor und Mitautor von verschiedenen Veröffentlichungen rund um die Themen Managementsysteme, Risikomanagement und Informationssicherheit. Zu Themen des Datenschutzes und der Datensicherheit ist er gern gefragter Experte des regionalen und überregionalen Fernsehens.

Sabine Roeb-Vollmer, selbstständig seit 1991, ist als Beraterin und DQS-Senior-Auditleiterin spezialisiert auf die Implementierung und Weiterentwicklung von Managementsystemen für Qualität, Informationssicherheit und Service Management.
Sie war bereits in zahlreichen multinationalen Konzernen erfolgreich tätig, unterstützt aber auch gerne kleine und mittelständische Unternehmen bei deren Zertifizierungsvorbereitungen.
Als systemischer Business- und Management-Coach für Führungskräfte, Projektmanager und Nachwuchsführungskräfte begleitet sie Menschen in Einzelcoachings.
Als Coach ist sie Sparringspartnerin ihrer Klienten und unterstützt die persönliche Weiterentwicklung im Sinne von verbesserter Selbstreflexion und Leistungssteigerung und hilft bei der Lösung von Konflikten im beruflichen und privaten Kontext.

Unternehmensinformationen

»**Die Sollence GmbH ist Ihr ganzheitlicher Partner zur exzellenten Organisationsentwicklung**«
Wir entwickeln die Kompetenz unserer Kunden auf Basis von international anerkannten Normen und Best-Practice-Ansätzen bei Managementsystemen weiter und unterstützen mit Beratung, Coaching, Training, Auditierung sowie der Erbringung weiterer Dienstleistungen im Bereich der Organisationsentwicklung.
Die Expertise umfasst dabei unter anderem Themen wie Qualität, Informationssicherheit, Compliance, Risikomanagement und agile Unternehmensführung. Das Kundenspektrum reicht von kleinen und mittelständischen Unternehmen bis hin zu Konzernen und deren Einheiten in den unterschiedlichsten Branchen.
Weitere Informationen erhalten Sie unter http://www.sollence.de

Weitere Informationen / Kontakt zu den Autoren

Sollence GmbH
Robert-Reichling-Straße 10
47807 Krefeld

Fon: +49 (0)2151.3617913
mail@sollence.de
https://www.sollence.de