Umsetzungsstrategie Industrie 4.0

Ergebnisbericht der Plattform Industrie 4.0

April 2015

Impressum

Plattform Industrie 4.0 (2013-2015)
ist ein gemeinsames Projekt der Verbände
BITKOM e.V., VDMA e.V. und ZVEI e.V.

Herausgeberkreis

BITKOM e.V.
Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e. V.
Albrechtstraße 10
10117 Berlin-Mitte

Tel.: 030.27576-0
bitkom@bitkom.org
www.bitkom.org

VDMA e.V.
Verband Deutscher Maschinen- und Anlagenbau e.V.
Lyoner Straße 18
60528 Frankfurt am Main

Tel.: 069.6603-0
zvei@zvei.org
www.vdma.org

ZVEI e.V.
Zentralverband Elektrotechnik- und
Elektronikindustrie e.V.
Lyoner Straße 9
60528 Frankfurt am Main

Tel.: 069.6302-0
kommunikation@vdma.org
www.zvei.org

Koordination, Redaktion und Lektorat

Wolfgang Dorst, BITKOM e.V.

Layout und Satz

Astrid Scheibe, BITKOM e.V.

Grafiken

Astrid Scheibe, BITKOM e.V.

Druck

Kehrberg Druck Produktion Service

Bildnachweise

Abbildung 17: Bildquelle: Mensch als Dirigent der Wertschöpfung: FESTO AG & Co. KG; Abbildung 22: Bildquelle Maschine: FESTO AG & Co. KG, Bildquelle Klemmenblock: PHOENIX CONTACT GmbH & Co. KG, Bildquelle Elektr. Achse links: FESTO AG & Co. KG, Bildquelle Elektr. Achse rechts: FESTO AG & Co. KG; Abbildung 24 und 31: Bildquelle Maschine1 und 2: FESTO AG & Co. KG, Bildquelle Klemmenblock: PHOENIX CONTACT GmbH; Abbildung 25: Bildquelle Elektr. Achse links: FESTO AG & Co. KG, Bildquelle Elektr. Achse rechts: FESTO AG & Co. KG; Abbildung 26: Bildquelle Sensor: Pepperl+Fuchs GmbH, Bildquelle Steuerung: Bosch Rextoth AG, Bildquelle Elektr. Achse links: FESTO AG & Co. KG, Bildquelle Elektr. Achse rechts: FESTO AG & Co. KG; Abbildung 27: Bildquelle Auslegung: FESTO AG & Co. KG,Bildquelle Handbücher links: FESTO AG & Co. KG, Bildquelle Handbücher rechts: FESTO AG & Co. KG, Bildquelle Elektr. Achse, Mitte 1: FESTO AG & Co. KG, Bildquelle Elektr. Achse, Mitte 2: FESTO AG & Co. KG, Bildquelle Elektr. Achse, Mitte 3: FESTO AG & Co. KG, Bildquelle Elektr. Achse, Mitte 4: FESTO AG & Co. KG, Bildquelle Elektr. Achse, unten 1: Pepperl+Fuchs GmbH, Bildquelle Elektr. Achse, unten 2: FESTO AG & Co. KG; Abbildung 28: Bildquelle Maschine: FESTO AG & Co. KG, Bildquelle Klemmenblock: PHOENIX CONTACT GmbH & Co. KG,- Bildquelle Elektr. Achse links: FESTO AG & Co. KG, Bildquelle Elektr. Achse rechts: FESTO AG & Co. KG.

Veröffentlicht April 2015


Plattform
INDUSTRIE 4.0

Inhalt

Vorwort

1 Vorwort

Physische und virtuelle Welt wachsen zunehmend zusammen. Immer mehr physische Objekte verfügen über intelligente Sensor- und Aktor-Technologie und werden durch die Entwicklung des Internets der Dinge vernetzt. Die Verfügbarkeit aller relevanten Informationen in Echtzeit mittels Vernetzung aller an der Wertschöpfung beteiligten Instanzen sowie die Fähigkeit aus den Daten den zu jedem Zeitpunkt optimalen Wertschöpfungsfluss abzuleiten, löst die nächste Stufe der industriellen Revolution aus, die als Industrie 4.0 bezeichnet wird. Dies wird evolutionäre Auswirkungen auf die Technologien, aber revolutionäre Auswirkungen auf existierende Geschäftsprozesse haben und neue Geschäftsmodelle ermöglichen. Dabei steht die Optimierung der folgenden industriellen Kernprozesse im Fokus: Entwicklung, Produktion, Logistik und Service.

Die vorliegende Umsetzungsstrategie Industrie 4.0 wurde durch die Plattform Industrie 4.0 (organisiert über die Verbände BITKOM, VDMA, ZVEI) und in Zusammenarbeit mit den Unternehmen der Deutschen Industrie sowie weiteren Verbänden erarbeitet. Sie sichert damit die Zukunftsfähigkeit des Standorts Deutschland und seiner Industrie.

Wesentliche Kernbausteine für Industrie 4.0 werden in Kapitel 4 beschrieben. Aufsetzend werden in dem Kapitel 5 „Forschung und Innovation“ wichtige Forschungsbedarfe abgeleitet und in Form von Forschungsroadmaps und Steckbriefen beschrieben. Die Forschungsroadmaps bieten eine gute Orientierung für eine sinnvolle Weiterentwicklung des Themas Industrie 4.0 mittels geeigneter Maßnahmen und Förderinstrumente durch Politik und Unternehmen (Spitzencluster, Demo-Labs, Demo-Anlagen, Demo-Fabriken, usw.).

Ein Referenzarchitektur-Modell für Industrie 4.0 (kurz RAMI 4.0) wird in Kapitel 6 vorgestellt. Darin werden die Industrie 4.0-Komponenten in ihrem Aufbau und ihrer Arbeitsweise definiert. Wo es sinnvoll ist, setzen Teile des Referenzarchitektur-Modells und der Industrie 4.0-Komponenten auf bestehende und relevante Normen auf, um schneller handlungsfähig zu sein. Wo notwendig wurden in der Umsetzungsstrategie zusätzliche identifizierte Standardisierungsbedarfe identifiziert und beschrieben.

Aufgrund der zunehmenden Vernetzung und Steuerbarkeit von physischen Objekten und der gleichzeitig steigenden Bedrohungslage durch Hacker, Geheimdienste, Spionage etc. ergeben sich besondere Sicherheitsanforderungen. Diese werden im Kapitel 7 umrissen.

Die Umsetzungsstrategie wendet sich an Leser aus der deutschen Industrie, den relevanten technologieorientierten Branchen, der Forschung und der Politik. Im Besonderen sind Führungskräfte, Fachkräfte und Berater angesprochen sowie alle Personen, die an einem Zukunftsbild der Industrie 4.0 in Deutschland interessiert sind oder dieses mitgestalten wollen.

Übergreifende Darstellung Industrie 4.0

2 Übergreifende Darstellung Industrie 4.0

2.1 Definition Industrie 4.0

Der Begriff Industrie 4.0 steht für die vierte industrielle Revolution, einer neuen 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 beispielsweise Kosten, Verfügbarkeit und Ressourcenverbrauch optimieren lassen.

2.2 Strategie und Ziele

Die Industrieverbände BITKOM, VDMA und ZVEI hatten zur Fortführung der Aktivitäten der Forschungsunion Wirtschaft-Wissenschaft und zur Sicherung eines koordinierten und branchenübergreifenden Vorgehens die gemeinsame Initiative Plattform Industrie 4.0 etabliert. Das wichtigstes Ziel der Plattform Industrie 4.0 ist es die Vision Industrie 4.0 durch die Verbände BITKOM, VDMA und ZVEI in Richtung Industrie voranzutrieben. Damit soll Deutschlands Zukunft als Produktionsstandort gesichert und ausgebaut werden.

Der Abschlussbericht der Forschungsunion Wirtschaft-Wissenschaft zu Industrie 4.0 vom April 2013 beschreibt Umsetzungsempfehlungen [3], erläutert Forschungsbedarfe und nennt acht Handlungsfelder, die hier – ergänzt um einen Nutzenaspekt – zur Darstellung der Ausgangslage aufgelistet werden:

1. Standardisierung, Offene Standards für eine Referenzarchitektur
   Ermöglicht firmenübergreifende Vernetzung und Integration über Wertschöpfungsnetzwerke.
2. Beherrschung komplexer Systeme
   Nutzen von Modellen zur Automatisierung von Tätigkeiten und einer Intergration der digitalen und realen Welt.
3. Flächendeckende Breitband-Infrastruktur für die Industrie
   Sicherstellung der Anforderungen bei Industrie 4.0 an den Datenaustausch bzgl. Volumen, Qualität und Zeit.
4. Sicherheit
   Das Ziel ist hier die Gewährleistung der Betriebssicherheit (engl. Safety), des Datenschutzes (engl. Privacy) und der IT-Sicherheit (engl. Security).
5. Arbeitsorganisation und Arbeitsplatzgestaltung
   Klärung der Implikationen für den Menschen und Arbeitnehmer als Planer und Entscheider in den Industrie 4.0 Szenarien.
6. Aus- und Weiterbildung
   Formulierung der Inhalte und innovativer Ansätze für die Aus- und Weiterbildung.
7. Rechtliche Rahmenbedingungen
   Das Ziel ist die Schaffung erforderlicher – möglichst europaweit einheitlicher – rechtlicher Rahmenbedinungen für Industrie 4.0 (Schutz digitaler Güter, Vertragsrecht bei zwischen Systemen geschlossenen Verträgen, Haftungsfragen, ...).
8. Ressourceneffizienz
   Verantwortungsvoller Umgang mit allen Ressourcen (personelle und finanzielle Ressourcen sowie Roh-, Hilfs- und Betriebsstoffe) als Erfolgsfaktor für die zukünftige industrielle Produktion.

Damit die Transformation der industriellen Produktion hin zu Industrie 4.0 gelingt, wird in Deutschland eine duale Strategie verfolgt:

- Die deutsche Ausrüsterindustrie soll weiterhin führend auf dem Weltmarkt bleiben, indem sie durch das konsequente Zusammenführen der Informations- und Kommunikationstechnologie mit ihren klassischen Hochtechnologieansätzen zum Leitanbieter für intelligente Produktionstechnologien wird. Neue Leitmärkte für CPS-Technologien[1] und -Produkte sind zu gestalten und zu bedienen.
- Gleichzeitig gilt es, die Produktion in Deutschland durch effiziente und die Resourcen schonende Produktionstechnologien attraktiv und wettbewerbsfähig weiter zu entwickeln. Ziel ist der Ausbau der Wettbewerbsvorteile von Unternehmen in Deutschland, die durch die räumliche Nähe und aktive Vernetzung der Anwender und Hersteller durch das Internet entsteht. Automatisierungs-, Prozess- und Produktionstechnik in Deutschland haben von dieser Strategie gleichermaßen Vorteile.
- Der Weg zu Industrie 4.0 ist ein evolutionärer Prozess. Es bedarf der Weiterentwicklung der vorhandenen Basistechnologien um die Erfahrungen und Besonderheiten der Optimierung der gesamten Wertschöpfungskette zu erreichen. Die Umsetzung neuer Geschäftsmodelle über Dienste im Internet hat disruptiven Charakter. Erfolgreiche Unternehmen mit guten Produkten oder Dienstleistungen sowie wachsender Nachfrage in ihren Absatzmärkten sollen hohen Bereitschaft zu disruptiven Veränderungen entwickeln. Und zwar bei der Weiterentwicklung bestehender Prozesse im Unternehmen und bei der Entwicklung neuer Geschäftsmodelle.

1 Definition aus den Umsetzungsempfehlungen [3]: Cyber-Physical Systems (CPS): CPS umfassen eingebettete Systeme, Produktions-, Logistik-, Engineering-, Koordinations- und Managementprozesse sowie Internetdienste, die mittels Sensoren unmittelbar physikalische Daten erfassen und mittels Aktoren auf physikalische Vorgänge einwirken, mittels digitaler Netze untereinander verbunden sind, weltweit verfügbare Daten und Dienste nutzen und über multimodale Mensch-Maschine-Schnittstellen verfügen. Cyber-Physical Systems sind offene soziotechnische Systeme und ermöglichen eine Reihe von neuartigen Funktionen, Diensten und Eigenschaften.

2.3 Nutzen

Der Nutzen für die entlang der Wertschöpfungskette Beteiligten ist vielfältig. Die Fähigkeit auf induvidualisierte Kundenwünsche einzugehen wird verbessert und die Produktion von Einzelstücken und Kleinstmengen wird rentabler. Die Flexibilisierung schreitet durch die dynamische Gestaltung der Geschäftsprozesse über das Internet in unterschiedlichen Dimensionen sowie agilen Engineering-Prozessen voran. Aufgrund der Informationen, die Industrie 4.0 zusammen mit zum Beispiel Big Data, Social Media, und Cloud Computing bereitstellt, werden eine optimierte Entscheidungsfindung, eine frühzeitige Absicherung von Entwurfsentscheidungen und eine flexible Reaktion auf Störungen, sowie die standortübergreifende globale Optimierung aller Ressourcen ermöglicht.

Die Produktionseffizienz wird sich steigern – einerseits durch Erhöhung der Produktivität, andererseits durch effizientere Nutzung von Ressourcen (Maschinen, Energie etc.).

Es ergeben sich neue Potenziale durch neue Formen von Wertschöpfung und Beschäftigung, zum Beispiel durch nachgelagerte Dienstleistungen, also den Services, die komplementär zum eigentlichen Produkt dem Anwender angeboten werden können, nachdem das Produkt die Produktionseinrichtung verlassen hat.

Auch für die Gestaltung der Arbeit unter Berücksichtigung des demografischen Wandels ergeben sich Vorteile. So ist die Unterstützung der körperlichen Möglichkeiten sowie der kognitiven Fähigkeiten ein entscheidender Mehrwert von Industrie 4.0-Konzepten. Um in wissensbasierten Unternehmen mit hohem Ausbildungsstand das Wissen und die Erfahrung der Mitarbeiter zu erhalten, sind durch Industrie 4.0 für die Personalentwicklung flexible und vielfältige Laufbahnmodelle neben der Führungslaufbahn vor allem Fachlaufbahnen möglich. Durch Soziale Medien werden Produktionsplanung und Arbeitszeitgestaltung flexibler. Die Auslastung im Produktionsprozess wird optimiert und Ressourcen werden besser genutzt. Zudem kann man auch kurzfristig auf Kundenwünsche reagieren. Nicht zuletzt können Mitarbeiter durch die stärkere Einbindung in die Personaleinsatzplanung, ihre Arbeit besser mit Familie und Freizeit in Einklang bringen.

Industrie 4.0 stärkt die Wettbewerbsfähigkeit Deutschlands als Hochlohnstandort, ermöglicht die Positionierung der Unternehmen als Leitanbieter und lässt Deutschland zum Leitmarkt für Industrie 4.0-Lösungen werden.

Mit unserem Wissen in Deutschland im Industriesektor haben wir einen Vorsprung – sei es bei den führenden Unternehmen, sei es bei dem gut aufgestellten KMU-Bereich, sei es bei den Lieferanten von Industrie-Automatisierung, sei es bei IT-Unternehmen, sei es bei dem Werkzeug-/Maschinen-Bau – um nur einige zu nennen.

2.4 Wettbewerb

Die Vision Industrie 4.0 setzt eine sichere Kommunikation und Kooperation aller Teilnehmer firmenübergreifend in Echtzeit für die gesamte Lebendszeit des Produktes voraus, die durch Internet-basierte Plattformen ermöglicht werden soll. Auf diesen digitalen Plattformen bauen neue, innovative Wertschöpfungsketten auf, die den Nutzen von Industrie 4.0 erbringen.

Für die Aufgabe, diese firmenübergreifende sichere „horizontalen“ Kommunikations- und Kooperations-Plattformen im vorwettbewerblichen Bereich gemeinsam zu definieren und samt allen Randbedingungen und weiteren Forschungsbedarfen festzulegen, wurde die Initiative Plattform Industrie 4.0 ins Leben gerufen.

Aber dies ist nicht alles, auch durch die mögliche Durchgängigkeit von Produkt-Produktion-Service mit einem jeweiligen virtuellen Abbild der physikalischen Welt und deren Simulation sind neue Technlogien in Entwicklung.

Ferner ergeben sich mit einer verbesserten vertikalen Kommunikation, neue Möglichkeiten der sinnvollen und sicheren Nutzung von Technlogien des „Internets der Dinge“ in der Produktion.

Die Industrieunternehmen der Plattform Industrie 4.0, der Wissenschaftliche Beirat und die Trägerverbände BITKOM, VDMA und ZVEI haben in technisch orientierten Arbeitsgruppen gemeinsam notwendige oder geeignete Standards für ein Modell einer oder mehrerer Referenzarchitekturen evaluiert, notwendige Rahmenbedingen aufgezeigt und lohnende Forschungfelder benannt. Auf der Basis des in der Plattform Industrie 4.0 erstellten Orientierungswissens können einzelne Unternehmen aus eigener Entscheidung, ausserhalb der Verbändeplattform neue Wertschöpfungsketten und innovative Geschäftsmodelle anbieten, die im Wettbewerb zueinander im Markt stehen.

Die Plattform Industrie 4.0 stimmt sich regelmässig mit relevanten Gremien und Vereinigungen ab, die in vergleichbaren Themen engagiert sind und für einzelne Arbeitspunkte der eigenen Arbeit in der Verbändeplattform relevant sind. Die Abstimmung erfolgt über benannte und entsprechend beauftragte Mitglieder.

Thesen des Wissenschaftlichen Beirates

3 Thesen des Wissenschaftlichen Beirates

Der Wissenschaftliche Beirat berät die Plattform Industrie 4.0 in allen wissenschaftlichen und programmatischen Forschungsfragen im engen Austausch mit der Begleitforschung. Im Beirat aktiv sind 16 Professorinnen und Professoren aus den Fachbereichen Produktion und Automatisierung, Informatik sowie Jura und Arbeitssoziologie.

Zur Hannovermesse 2014 (Stand 3. April 2014) hat der Wissenschaftliche Beirat seine Thesen veröffentlicht [12], die über die Webseite der Plattform öffentlich verfügbar sind. Die nachfolgend zitierten Thesen sind in die Abschnitte Mensch, Technik und Organisation strukturiert:

Mensch

1. Vielfältige Möglichkeiten für eine humanorientierte Gestaltung der Arbeitsorganisation werden entstehen, auch im Sinne von Selbstorganisation und Autonomie. Insbesondere eröffnen sich Chancen für eine alterns- und altersgerechte Arbeitsgestaltung
2. Industrie 4.0 als soziotechnisches System bietet die Chance, das Aufgabenspektrum der Mitarbeiter zu erweitern, ihre Qualifikationen und Handlungsspielräume zu erhöhen und ihren Zugang zu Wissen deutlich zu verbessern.
3. Lernförderliche Arbeitsmittel (Learnstruments) und kommunizierbare Arbeitsformen (Community of Practice) erhöhen die Lehr- und Lernproduktivität, neue Ausbildungsinhalte mit einem zunehmend hohen Anteil an IT-Kompetenzen entstehen.
4. Lernzeuge – gebrauchstaugliche, lernförderliche Atefakte – vermitteln dem Nutzer ihre Funktionalität automatisch.

Technik

5. Industrie 4.0-Systeme sind für den Anwender einfach zu verstehen, intuitiv zu bedienen, sie sind lernförderlich und reagieren verlässlich.
6. Allgemein zugängliche Lösungsmuster erlauben es vielen Akteuren, Industrie 4.0-Systeme zu entwerfen, zu realisieren und zu betreiben (Industrie 4.0 by Design).
7. Die Vernetzung und Individualisierung der Produkte und Geschäftsprozesse erzeugt Komplexität, die z. B. durch Modellierung, Simulation und Selbstorganisation bewirtschaftet wird. Ein größerer Lösungsraum kann schneller analysiert und Lösungen können schneller gefunden werden.
8. Die Ressourceneffektivität und -effizienz kann kontinuierlich geplant, umgesetzt, überwacht und autonom optimiert werden.
9. Intelligente Produkte sind aktive Informationsträger und über alle Lebenszyklusphasen adressier- und identifizierbar.
10. Systemkomponenten sind auch innerhalb von Produktionsmitteln adressier- und identifizierbar. Sie unterstützen die virtuelle Planung von Produktionssystemen und –prozessen.
11. Neue Systemkomponenten verfügen mindestens über die Fähigkeiten der zu ersetzenden und können deren Funktion kompatibel übernehmen.
12. Systemkomponenten bieten ihre Funktionalitäten als Dienste an, auf die andere zugreifen können.
13. Eine neue Sicherheitskultur führt zu vertrauenswürdigen, resilienten und gesellschaftlich akzeptierten Industrie 4.0-Systemen.

Organisation

14. Neue und etablierte Wertschöpfungsnetze mit Mehrwert integrieren Produkt, Produktion und Service und ermöglichen die dynamische Variation der Arbeitsteilung.

15. Zusammenarbeit und Wettbewerb (Competition) führt betriebswirtschaftlich und rechtlich zu neuen Strukturen.

16. Systemstrukturen und Geschäftsprozesse werden auf dem jeweils gültigen Rechtsrahmen abbildbar; neue rechtliche Lösungen ermöglichen neue Vertragsmodelle.

17. Es entstehen Chancen für die Vermittlung regionaler Wertschöpfung – auch in sich entwickelnden Märkten.

In einem von der Plattform ebenfalls zur Hannovermesse 2014 veröffentlichten „Whitepaper FuE Themen“ werden die, für die Umsetzung der Thesen notwendigen, verschiedenen Themenfelder bezüglich ihrer Inhalte und Ziele vorgestellt. Weiterhin wird ein grober Zeitplan für die Beabeitung der Themenfelder gezeigt. Themenfelder und Zeitplan (siehe Kapitel 4 und 5) sind in die Arbeit der Plattform Arbeitsgruppen eingeflossen.

Umsetzungstrategie Industrie 4.0

4 Umsetzungstrategie Industrie 4.0

Zur Stärkung des Wirtschaftsstandortes Deutschland hat die „Plattform Industrie 4.0“ das Ziel eine Umsetzungsstrategie für Industrie 4.0 zu erarbeiten. Dazu wird einerseits in einem branchenübergreifenden Ansatz an Konzepten für Technologie, Standards, Geschäfts- und Organisationsmodellen gearbeitet, andererseits ein Schulterschluss zwischen Universitäten, Forschungseinrichtungen mit KMU und Industrieunternehmen geschlossen, der auch die praktische Umsetzung vorantreibt.

Durch Industrie 4.0 entstehen neue Wertschöpfungsketten und -netzwerke, die durch die weiter zunehmende Digitalisierung automatisiert werden. Als wichtige Kernbausteine, siehe Abbildung, werden entsprechend die Bereiche:

- Forschung und Innovation,
- Referenzarchitektur, Standardisierung und Normung sowie
- Sicherheit vernetzter Systeme

gesehen, die in spezifischen Arbeitsgruppen der Plattform Industrie 4.0 bearbeitet werden. Hinzu kommt:

- die Schaffung rechtlicher Rahmenbedingungen.

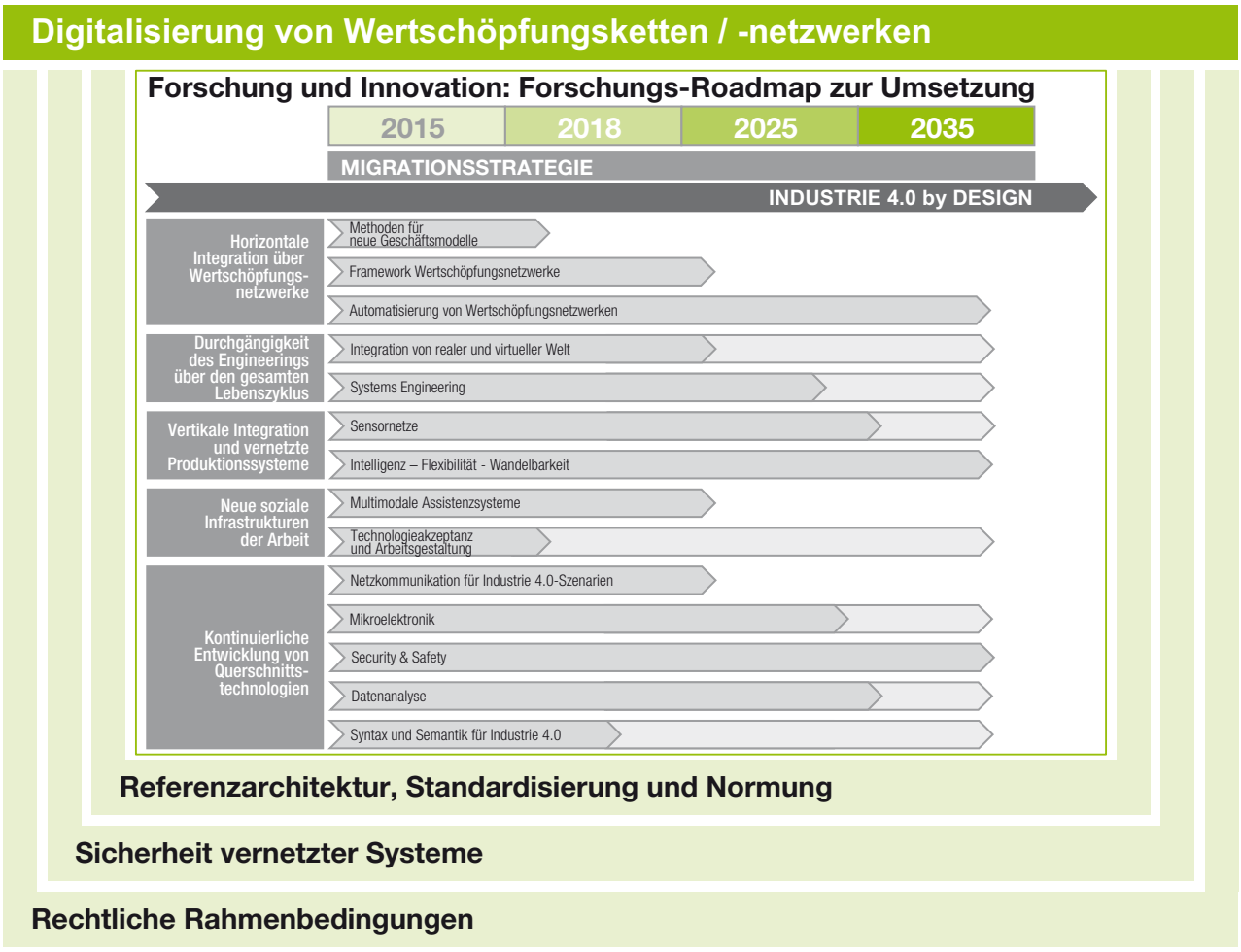


Abbildung 1: Kernbausteine Industrie 4.0

Dieses Thema wird nicht durch die Plattform Industrie 4.0 angegangen sondern insbesondere durch Arbeitskreise des BDI behandelt.

Im Bereich Forschung und Innovation wird in Abstimmung mit dem Wissenschaftlichen Beirat die zur Umsetzung von Industrie 4.0 erforderliche Forschungs- und Innovations-Roadmap erstellt und erforderliche Innovations- und Forschungsaktivitäten und deren Förderung aus Sicht der Industrie abgestimmt und koordiniert. Die wichtigsten Themenfelder sind dabei (siehe Kapitel 5):

- Horizontale Integration über Wertschöpfungsnetzwerke
  Der Schwerpunkt liegt in der Ausgestaltung der unternehmensübergreifenden Kollaboration (Lieferanten, KMU's, produzierendes Gewerbe – um nur einige zu nennen). Dies schliesst Aspekte und Methoden für neue Geschäftsmodelle ein.
- Durchgängigkeit des Engineering über den gesamten Lebenszyklus
  Zentrale Themen sind hier das PLM-gestützte Engineering, welches das Produkt- und Produktionsdesign verbindet und eine durchgängige Unterstützung über die gesamte Wertschöpfung hinweg ermöglicht. Dies adressiert fachliche Punkte wie die integrierte Betrachtung von Systems Engineering, Modellierung und Simulation.
- Vertikale Integration und vernetzte Produktionssysteme
  Das Kernthema bildet hierbei die Vernetzung der Produktion, die vielfach auch Echtzeitanforderungen bedingt. Wichtige Punkte sind hierbei, dass die erforderliche Wandlungsfähigkeit und die produktionstechnischen Sicherheitsanforderungen (z. B. Redundanz und Fehlertoleranz) gewahrt und sichergestellt werden können. Dies erfordert sowohl die Weiterentwicklung der zugehörigen Komponenten und Systeme, z. B. Sesornetze, als auch der Methoden wie beispielsweise Predictive Analytics.
- Neue soziale Infrastrukturen der Arbeit
  Der ausschlaggebende Erfolgsfaktor ist und bleibt der Mensch. Damit ist die Sicherstellung einer positiven Entwicklung der Veränderung der Arbeitswelt, gestützt und getrieben von allen Beteiligten (u.a. Gewerkschaften und Arbeitgeberverbände) von zentraler Bedeutung. Neben der Veränderung und Verbesserung der Aus- und Weiterbildung gibt es hier technische Aspkete wie die Einführung neuer Human-to-Machine Systeme und allgemein von Assistenzsystemen.
- Kontinuierliche Entwicklung von Querschnittstechnologien
  Für die Realisierung von Industrie 4.0 sind unterschiedliche technologische Voraussetzungen zu schaffen bzw. in die industrielle Anwendung zu bringen. Wichtige Technolgien sind Netzkommunikation, Breitband-Vernetzung, Cloud Computing, Data Analytics, Cyber Security, sichere Endgeräte sowie Machine-to-Machine Lösungen (inkl. Semantik).

Im Themenkomplex Referenzarchitekturen, Standardisierung und Normung geht es um die Erstellung einer lösungsneutralen Referenzarchitektur unter Nutzung von Normen und Standards und deren Etablierung (siehe Kapitel 6).

Im Bereich Sicherheit vernetzter Systeme wird auf Basis von exemplarischen Wertschöpfungsketten an konzeptuellen Beiträgen zur Gewährleistung der IT-Sicherheit innerhalb der horizontalen (Kunden/Zulieferer) und vertikalen (unternehmensinternen) Vernetzung gearbeitet. Dies dient der Identifikation von allgemeinen Anforderungen und Security-Prinzipien (siehe Kapitel 7). Die Ausgestaltung erfolgt dann in einem iterativen Prozess, der auch Forschungs- und Standardisierungsaspekte einbezieht und somit Beiträge für die Schaffung einer Industrie 4.0 Referenzarchitektur leistet.

Das Thema der rechtlichen Rahmenbedingungen adressiert die rechtsmäßige Gestaltung der neuen Produktionsprozesse und horizontalen Geschäftsnetzwerke. Zu den Herausforderungen zählen das Vertragsrecht (dynamischer Abschluss in automatisierten Wertschöpfungsketten), der Schutz von Unternehmensdaten, die Behandlung digitaler Güter, Haftungsfragen und der Umgang mit personenbezogenen Daten.

Forschung und Innovation

5 Forschung und Innovation

5.1 Einleitung

Die Platform Industrie 4.0 spricht sich dafür aus, Forschungsaktivitäten im Umfeld von Industrie 4.0 noch klarer als bislang zu bündeln und im Sinne einer strukturierten und priorisierten Forschungsagenda zu bearbeiten. Als Grundlage dafür sollen die von der Verbändeplattform in diesem Kapitel dargestellten Forschungs-Roadmaps dienen. Weiterhin ist ein dem Potenzial des Themas angemessenes und im internationalen Vergleich wettbewerbsfähiges Förderbudget des Bundes für die Durchführung der anstehenden Forschungsaufgaben bereitzustellen. Dieses ergänzt die von den beteiligten Unternehmen bereits jetzt in signifikanter Höhe eingesetzten Mittel und ist eine wichtige Voraussetzung für die gezielte Bearbeitung der anstehenden Aufgaben zur raschen Umsetzung von Industrie 4.0.

Darüber hinaus muss die Politik durch geeignete Maßnahmen und Förderinstrumente (Spitzencluster, Demo-Labs, Demo-Anlagen, Demo-Fabriken, usw.) die weitere Vernetzung und Zusammenarbeit zwischen Unternehmen und Wissenschaft sowie zwischen Unternehmen unterschiedlicher Größe und aus verschiedenen Branchen unterstützen, intensivieren und einfordern.

Industrie 4.0 wird sich letztendlich nicht durch die staatlich gelenkte Umsetzung einer vorgegebenen Roadmap erreichen lassen, zumal sich eine exakte Vision von Industrie 4.0 angesichts der unterschiedlichen Interessen und Sichtweisen der verschiedenen Firmen schwerlich festlegen lassen wird. Vielmehr wird Industrie 4.0 das Ergebnis inkrementeller Entwicklungen zur Realisierung konkreter Anwendungsfälle (inklusive Analyse von Nutzen- und Wertschöpfungspotenzialen) sein. Es ist wünschenswert, auch diese eher praktisch ausgerichteten Projekte für eine Förderung durch den Bund in Betracht zu ziehen. Die Förderung sollte damit den kompletten Innovationspfad von der Erforschung neuer Methoden und Technologien bis zu deren Einsatz in universitätsnahen Demoanlagen und industrienahen Pilotfabriken unterstützen.

Dieses Kapitel beschreibt die Forschungs- und Innovationsthemen zu Industrie 4.0. und basiert u.a. auf den Thesen des wissentschaftlichen Beirats. Erste Ergebnisse wurden bereits in dem „Whitepaper FuE-Themen“ zur Hannovermesse 2014 veröffentlicht. Seitdem wurde weiter an der Spezifikation relevanter Themen gearbeitet. Nachfolgend wird der überarbeitete Stand vom Februar 2015 dokumentiert (zu den Themenfeldern existieren jeweils detaillierte Steckbriefe, die über die in diesem Dokument geschriebenen Inhalte hinausgehen und jeweils in den Plattform Industrie 4.0 Arbeitsgruppen aktualisiert werden). Im ersten Halbjahr 2015 wird parallel auch eine neue Version des „Whitepapers FuE-Themen“ veröffentlicht, das diesbzgl. detaillierter auf diese Themen eingeht.

Nachfolgend werden zu jedem Themenfeld kurz (1) die Inhalte von Forschung und Innovation erläutert, (2) die angestrebten Ergebnisse und (3) die wesentlichen Meilensteine.

5.2 Themenfeld: Horizontale Integration über Wertschöpfungsnetzwerke

Unter horizontaler Integration verstehen wir die Integration der verschiedenen IT-Systeme für die Unterstützung bzw. Durchführung der unterschiedlichen Wertschöpfungsprozesse (beispielsweise Fertigung, Logistik, Vermarktung, Engineering, Service) sowohl innerhalb eines produzierenden Unternehmens als auch über Unternehmensgrenzen hinweg zu einer durchgängigen Lösung.

5.2.1 Methoden für neue Geschäftsmodelle

5.2.1.1 Inhalte von Forschung und Innovation

Ein Geschäftsmodell ist eine vereinfachte Darstellung, wie das Geschäft und die Wertschöpfung innerhalb eines Unternehmens funktionieren, und somit eine abstrakte Beschreibung, wie mit welchen Partnern, in welchen Märkten und mit welchen Kundengruppen Geld verdient wird. Im Kontext von Industrie 4.0 werden in Unternehmen aufgrund neuer Wertschöpfungsprozesse und einer sich verändernden Rollenverteilung in Wertschöpfungsnetzwerken neue Geschäftsmodelle entstehen.

Zu berücksichtigende Aspekte sind:

- Go-To-Market-Ansätze (GTMs)
- Methoden zur Bedarfsanalyse und -generierung sowie zur Potenzialermittlung
- Zahlungs- und Abrechnungsmodelle
- Nutzen- und Risikobewertung für jeden einzelnen Akteur im Netzwerk
- rechtliche Aspekte
- Anreiz- und Akzeptanzsysteme

5.2.1.2 Angestrebte Ergebnisse von Forschung und Innovation

Ein gemeinsames Verständnis der Geschäftsmodelle ist die Voraussetzung für die nachhaltige Nutzung der Potenziale einer firmenübergreifenden Vernetzung. Methodische Ansätze sollten vereinheitlicht und konsolidiert werden, Best Practices und Erfahrungen – insbesondere auch aus den jeweils anderen Branchen – systematisch erfasst werden. Dann erfolgen eine Übertragung auf die Produktion und die Analyse der sich daraus ergebenden Konsequenzen. Dabei sind die unterschiedlichen Rollen innerhalb von Wertschöpfungsnetzwerken zu betrachten.

Folgende Ergebnisse werden erwartet:

- exemplarische Go-to-Market-Ansätze für die unterschiedlichen Anbieterrollen innerhalb eines Netzwerkes, abgeleitet aus Best Practices
- ein auf die Bedarfe von Industrie 4.0 abgestimmter Geschäftsmodellansatz, der die Aspekte von Wertschöpfungsnetzwerken berücksichtigt
- exemplarische Zahlungs-, Abrechnungs- und Lizenzmodelle
- Leitfaden zur Bewertung des Industrie 4.0-typischen Nutzens und der entsprechenden Risiken
- Leitfaden für die rechtlichen Aspekte (u.a. Haftungsfragen insbesondere bei Service Level Agreements (SLAs) für Software as a Service (SaaS) und Platform as a Service (PaaS)).

5.2.1.3 Die wesentlichen Meilensteine

Methodik
1.4 Leitfaden zur Bewertung des Industrie 4.0-typischen Nutzens und der Risiken 1.5 Leitfaden für rechtliche Aspekte
Lösungen
1.1 Best Practices und Erfahrungen sowie Übertragung auf Produktion 1.2 Exemplarische Go-to-Market-Ansätze 1.3 Exemplarische Zahlungs-, Abrechnungs- und Lizenzmodelle 1.6 Auf Industrie 4.0 abgestimmter Geschäftsmodellansatz mit Berücksichtigung des Aspekts „Wertschöpfungsnetzwerke“ 1.7 Pilotierung (neuer) Geschäftsstrategien, -modelle und -prozesse
Voraussetzungen
2.3 Referenzarchitektur Wertschöpfungsnetzwerke für unterschiedliche Organisationsformen

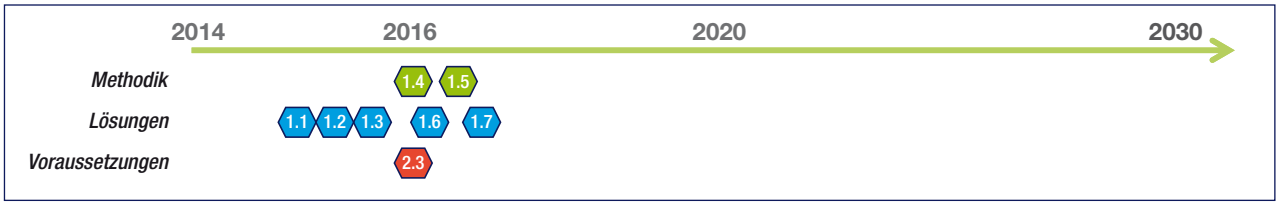


Abbildung 2: Meilensteine für die Forschung an Methoden für neue Geschäftsmodelle

5.2.2 Framework Wertschöpfungsnetzwerke

5.2.2.1 Inhalte von Forschung und Innovation

Ein Wertschöpfungsnetzwerk beschreibt ein System aus einzelnen Wertschöpfungsprozessen und deren prozesstechnische Abhängigkeit. Die einzelnen Wertschöpfungsprozesse werden durch autonome, rechtlich selbstständige Akteure realisiert. Sie sind über das Wertschöpfungsnetzwerk durch komplexe wechselseitige Beziehungen miteinander verbunden und bilden eine Interessengemeinschaft von Wertschöpfungspartnern, die auf einen nachhaltigen, ökonomischen Mehrwert ausgerichtet sind.

Zu berücksichtigende Aspekte sind:

- Voraussetzungen, Treiber, Konsequenzen für die Entstehung neuer Wertschöpfungsnetzwerke
- wirtschaftliche Rolle von CPS-Plattformen als Integrator von Wertschöpfungsnetzwerken
- mögliche geschäftliche Bedrohungen und resultierende Konsequenzen
- Organisationsformen von Wertschöpfungsnetzwerken, deren unterschiedliche Komponenten und Rollen sowie deren rechtliche Implementierung

5.2.2.2 Angestrebte Ergebnisse von Forschung und Innovation

Es sollen Konzepte für die Implementierung von Wertschöpfungsnetzwerken entstehen und in Pilotprojekten angewendet werden, damit Themen wie (neue) Geschäftsstrategien, -modelle und -prozesse unter stärkerer Einbeziehung von Kunden, Lieferanten, Partnern und Markt praktisch beleuchtet werden. Dazu werden für die konkreten Beispiele Business-Pläne erstellt und Erfahrungen bezüglich einer „Orchestrierung“ gesammelt, die auch als zukünftige Anforderungen an CPS-Plattformen zur Unterstützung von Wertschöpfungsnetzwerken veröffentlicht werden sollen.

Folgende Ergebnisse werden erwartet:

- die flexible Integration von Wertschöpfungsnetzen in der Produktion
- Methoden zur Analyse und Bewertung wirtschaftlicher und technologischer Potenziale aus Sicht der Netzwerkpartner und deren Kunden
- Mobilisierung insbesondere mittelständischer Unternehmen für die Kooperation in Netzwerken

- Eröffnung neuer Geschäftsmöglichkeiten
- Win-Win-Wertschöpfungspartnerschaften und damit nachhaltige, „integrierte“ Geschäftsmodelle

5.2.2.3 Die wesentlichen Meilensteine

Methodik
2.1 Formale Beschreibung und Standards (Semantik) einzelner Prozessschritte in einem einheitlichem Modell 2.2 Formale Beschreibung und Standards (Semantik) Schnittstellen und Gesamtnetzwerk in einem einheitlichem Modell 2.3 Referenzarchitektur Wertschöpfungsnetzwerke für unterschiedliche Organisationsformen 2.4 Analyse und Bewertung der wirtschaftlichen und technologischen Potenziale verkoppelter Wertschöpfungsnetzwerke 2.5 Leitfaden Voraussetzungen, Treiber, Konsequenzen und Vorgehensweise zur Implementierung 2.6 Anforderungen an CPS-Plattformen zur Unterstützung von Wertschöpfungsnetzen
Lösungen
2.7 Allgemeingültiges einheitliches Modell 2.8 Grundlegendes Verständnis zu Zusammenhängen, Modellen, Voraussetzungen, Treibern und Konsequenzen
Voraussetzungen
1.6 Auf Industrie 4.0 abgestimmter Geschäftsmodellansatz mit Berücksichtigung des Aspekts „Wertschöpfungsnetzwerke“

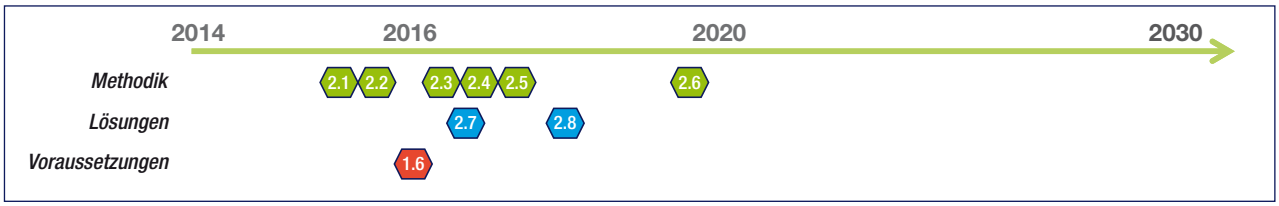


Abbildung 3: Meilensteine für die Forschung zum Thema „Framework Wertschöpfungsnetzwerke“

5.2.3 Automatisierung von Wertschöpfungsnetzwerken

5.2.3.1 Inhalte von Forschung und Innovation

Der Automatisierungsgrad der horizontalen Integration wird erhöht, indem Wertschöpfungsstufen automatisiert durchlaufen werden. Im Vordergrund stehen dabei Stufen, in denen die Wertschöpfung automatisiert erbracht wird oder rein in der „digitalen“ Welt erfolgt.

Zu berücksichtigende Aspekte sind:

- Durchgängigkeit der Informationsflüsse
- Einsatz von Verfahren zur Modellierung, Berechnung, Simulation und Optimierung
- Integration von Anwendungen wie PLM, APS, MES, SCM und ERP
- Einbindung des Menschen als kreativen Akteur in den globalen Wertstrom
- Gestaltung der Mensch-Maschine-Schnittstelle
- Abhängigkeit von Qualifizierungsmaßnahmen und Migrationsprozessen

5.2.3.2 Angestrebte Ergebnisse von Forschung und Innovation

Die Wertschöpfung soll effizienter und flexibler erbracht werden und sicher prognostizierbar sein. Menschen werden von nicht-kreativen Tätigkeiten entlastet. Produktivitätssteigerung, Ressourceneffizienz und Automatisierung stehen im Fokus. Durch die weitere Automatisierung einzelner Teilschritte komplexer Planungsprozesse werden die übergeordneten Wertschöpfungsketten und -netze sowie der operative Betrieb hinsichtlich global definierbarer Zielgrößen optimiert. Dabei werden Abhängigkeiten

berücksichtigt und Synergieeffekte erzielt. Dies wird möglich, indem ehemals hierarchisch-sequenziell organisierte Prozesse entweder integriert und teilweise synchron oder autonom durchgeführt werden.

Folgende Ergebnisse werden erwartet:

- eine Methodik, die die direkten und indirekten Zusammenhänge und Abhängigkeiten aller Unternehmensprozesse (z. B. PLM, ERP, APS, MES) beschreibt
- ein gemeinsames Zielhierarchiesystem, das die Auswirkung aller Tätigkeiten und Prozesse auf global definierte Ziele referenziert
- Prozesse und Tätigkeiten, die unter Berücksichtigung der o.g. Zusammenhänge und Abhängigkeiten hinsichtlich einer möglichst optimalen globalen Zielerreichung gestaltet und organisiert sind
- einfach anwendbare und integrierbare, autonom beschriebene Module
- Werkzeuge und Programme, die die Anwender durch eine einfache, intuitive Darstellung und kontinuierliche Simulationsmöglichkeiten unterstützen

5.2.3.3 Die wesentlichen Meilensteine

Methodik
3.1 Optimierungsmethoden 3.2 Strategische Vorgaben – Zielhierarchiesystem – Prozessmodellierung 3.3 Komplexitätsbeherrschung und Anwendbarkeit 3.4 Durchgängige Transparenz über den derzeitigen und geplanten Zustand aller Prozessschritte
Lösungen
3.5 Pilotierung Geschäftsstrategien, -modelle, -prozesse unter Einbeziehung von Kunden, Lieferanten, Partnern und Markt 3.6 Durchgängige Integration und flexible Verkopplung von Wertschöpfungsnetzen und optimale Entscheidungen
Voraussetzungen
2.1 Formale Beschreibung und Standards (Semantik) einzelner Prozessschritte in einem einheitlichem Modell 2.2 Formale Beschreibung und Standards (Semantik) Schnittstellen und Informationsflüsse in einem einheitlichem Modell 2.3 Referenzarchitektur Wertschöpfungsnetzwerke für unterschiedliche Organisationsformen 2.8 Grundlegendes Verständnis zu Zusammenhängen, Modellen, Voraussetzungen, Treibern und Konsequenzen

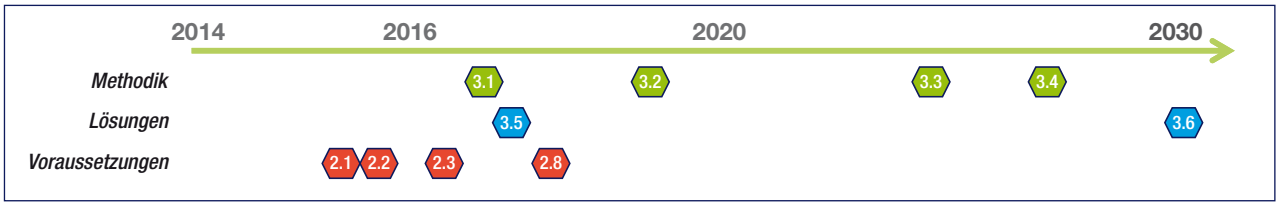


Abbildung 4: Meilensteine für die Forschung zur Automatisierung von Wertschöpfungsnetzwerken

5.3 Themenfeld: Durchgängigkeit des Engineerings über den gesamten Lebenszyklus

Unter dem Lebenszyklus eines Produkts verstehen wir die Entwicklung des Produkts sowie das Engineering des zugehörigen Produktionssystems, die Produktion des Produkts durch das Produktionssystem, die Nutzung des produzierten Produkts durch den Anwender sowie das Recycling bzw. den Rückbau des Produkts. Alle Informationen, die entlang dieses Lebenszyklus anfallen, sollen durchgängig verknüpft werden.

5.3.1 Integration von realer und virtueller Welt

5.3.1.1 Inhalte von Forschung und Innovation

Das Zusammenspiel von realer und virtueller/digitaler Welt rückt in der Industrie 4.0 stärker in den Mittelpunkt. Alle Objekte haben ein digitales Abbild (Modell). Die reale Welt ist in diesem Zusammenhang in der Regel charakterisiert durch zu lösende Problemstellungen und Entscheidungsfindungsprozesse. Wesentliche Elemente der virtuellen/digitalen Welt sind Simulationen, Planungs- und Beschreibungsmodelle. Die Co-Modellierung betrachtet darüber hinaus maßgeblich die Schnittstellen zwischen beiden Welten auf unterschiedlichen Skalen.

Planungsmodelle sind die Grundlage, um überhaupt komplexe Systeme erstellen zu können. Erklärungsmodelle ermöglichen die Analyse komplexer Systeme und führen somit über einen menschlichen Transferprozess zu Lösungen oder Entscheidungen. Insofern übt die virtuelle Welt bei beiden Modellansätzen einen signifikanten Einfluss auf den Entwurf der realen Welt aus. Gleichzeitig liegen die Sachverhalte, für die Modelle gebildet werden, sowie die Anforderungen bzw. Zielsetzungen, denen Rechnung zu tragen ist, in der realen Welt, sodass diese Einfluss auf die virtuelle Welt nimmt.

Benötigt wird hierzu ein wissenschaftliches Fundament im Sinne einer produktionstechnischen Modellierungstheorie für den Maschinen- und Anlagenbau. Bewährte Theorien, Beschreibungsmittel und Methoden einschließlich damit verbundener Basistechnologien aus der Informatik sind im Hinblick auf einen breiten Einsatz in den Ingenieurwissenschaften durch geeignete Adaption, Erweiterung und Kombination zu ertüchtigen. Hierbei spielt die adressatengerechte Integration in bekannte, domänenspezifische Arbeitsansätze und Softwarewerkzeuge eine Schlüsselrolle.

Wichtige zu berücksichtigende Aspekte sind:

- Die Modellierungstheorie muss die Grundlage bilden, um Fragestellungen wie „Was sind gute Modelle?“ (Einschließlich der Unsicherheitsabschätzungen), „Wie finde ich passende Modelle?“, „Was realisiere ich in der digitalen und was in der realen Welt?“ und „Wie können Schnittstellen zwischen virtueller und realer Welt gestaltet werden?“ fundiert beantworten zu können. Bestehende Modelle müssen dabei berücksichtigt werden.
- In der Modellierungstheorie müssen Konzepte und Leitgedanken wie beispielsweise Abstraktion, Durchgängigkeit, Sichten, Abhängigkeiten, Typ vs. Instanz, Modularisierung, Modellierungstiefe und modellgetriebene Architekturen auf Basis einer definierten Semantik festgelegt werden.
- Wirtschaftlichkeit von Modellierung: Neben dem Aufwand für die Erstellung von Modellen ist der nutzenstiftende Modell-Einsatz über den gesamten Lebenszyklus zu betrachten. Hierbei ist von großem Interesse, wie Modelle während ihrer Lebensdauer „mitwachsen“ können. Auch die Anreicherung aus bestehenden Datenquellen unter Erhaltung der Referenzen zur späteren konsistenten Zuordnung stellt einen relevanten Aspekt dar.

Konkret sind folgende Ergebnisse zu erarbeiten:

- Modellierungstheorie einschließlich daraus abgeleiteter Anforderungen an Werkzeuge und Daten- bzw. Informationsflüsse (auf allen Ebenen der Automatisierungspyramide)
- Verfahren für den Wirtschaftlichkeitsnachweis sowie Fallbeispiele
- Praxistaugliche Modellierungsvorschriften
- Allgemeines, werkzeugunterstütztes Meta-Modell

5.3.1.2 Angestrebte Ergebnisse von Forschung und Innovation

Die notwendige Grundlage ist ein einheitliches Verständnis von Modellen im Maschinenbau, in der Elektrotechnik und der Informatik im Umfeld der Produktion. Langfristiges Ziel ist die Befähigung produzierender Unternehmen zur wirtschaftlichen, nutzenstiftenden, bidirektionalen Modellierung. Damit sollen Elemente aus virtuellen Welten mit der realen Welt auf einem hohen semantischen Niveau interdisziplinär verknüpft werden können, um die Effizienz der internen Auftragsabwicklung sowie die Sicherheit von Entscheidungen signifikant zu erhöhen.

Folgende Ergebnisse werden erwartet:

- Modellierungstheorie einschließlich daraus abgeleiteter Anforderungen an Werkzeuge und Daten- bzw. Informationsflüsse (auf allen Ebenen der Automatisierungspyramide)
- Verfahren für den Wirtschaftlichkeitsnachweis sowie Fallbeispiele
- praxistaugliche Modellierungsvorschriften
- allgemeines werkzeugunterstütztes Meta-Modell

5.3.1.3 Die wesentlichen Meilensteine

Methodik
4.1 Erste Version einer Modellierungstheorie komplexer Systeme einschließlich Anforderungen an Werkzeuge 4.3 Praxistaugliche Anwendungsbeispiele und Modellierungsvorschriften 4.4 Verfahren für Wirtschaftlichkeitsnachweis einzelner Fall- bzw. Anwendungsbeispiele
Lösungen
4.2 Identifikation von „Best in Class“ Unternehmen 4.5 Erste Version eines Modellierungsframeworks 4.6 Allgemeines, werkzeugunterstütztes Meta-Modell
Voraussetzungen
4.a Etablierung einer branchenübergreifenden Community 4.b Schaffung von Akzeptanz für Modellierung in der breiten Masse 4.c Werkzeuge und Methoden zur Skalierung von Modellierungstiefen; Sicherstellung vertikaler und horizontaler Konsistenz 4.d Konzepte für Werkzeugunterstützung unter Nutzung erster Referenzarchitekturen im Einklang mit der realen Welt

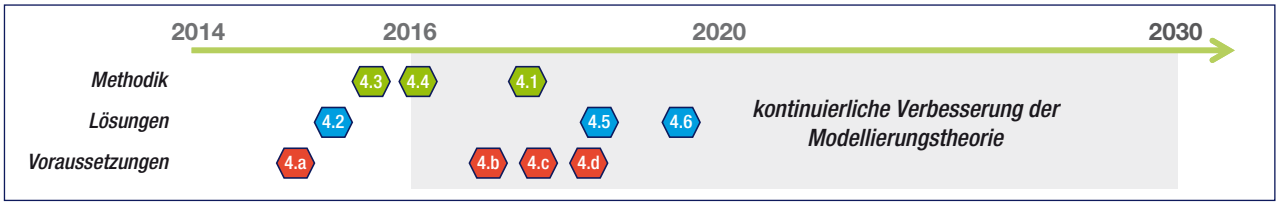


Abbildung 5: Meilensteine für die Forschung zur Durchgängigkeit des Engineerings über den gesamten Lebenszyklus

5.3.2 Systems Engineering

5.3.2.1 Inhalte von Forschung und Innovation

Systems Engineering ist eine durchgängige fachübergreifende Disziplin zur Entwicklung technischer Systeme, die alle Aspekte ins Kalkül zieht. Es stellt das multidisziplinäre System in den Mittelpunkt und umfasst die Gesamtheit aller Entwicklungsaktivitäten.

Zu berücksichtigende Aspekte sind:

- integrative Entwicklung von Produkt, Prozess und Produktionssystem. Von Beginn an müssen alle Aspekte in einem engen Wechselspiel entwickelt und über den Marktzyklus des Produkts kontinuierlich fortentwickelt werden
- Erprobung und Validierung von Entwurfsentscheidungen in „frühen“ Phasen, auch im Hinblick darauf, welche intendierten Funktionen später mechanisch, elektrisch, durch Firmware, Software oder durch Dienstleistungen umgesetzt werden
- Verfügbarkeit aller relevanten Daten und Prozesse über Systemgrenzen (Teilsystem, Maschine/Prozess, Produktionsanlage, Fabrik) und Firmengrenzen hinweg, sowie deren Bereitstellung in skalierbaren Systemen
- Modularisierung und Wiederverwendung der Anlagen und Systeme für die Beherrschung der zunehmenden Komplexität und Skalierbarkeit
- Rückfluss von Erfahrungen aus dem Einsatz der Anlagen und Systeme in die Entwicklung bzw. das Engineering und den Betrieb
- Die verwendeten Methoden lassen eine interoperable Engineering-Kette entstehen, die eine sichere Nutzung (Austausch von Daten, Rollenmodelle, Zugriffsverfahren) der Engineering-, Simulations- und für den Betrieb genutzten Systeme, deren Einbettung in Geschäftsmodelle (z. B. Lizenzen, Abrechnungssysteme) versionsorientiert ermöglichen

5.3.2.2 Angestrebte Ergebnisse von Forschung und Innovation

Ziel muss es sein, dass ein ganzheitlicher fachdisziplinübergreifender Entwurf eines komplexen Systems im Zuge der weiteren Konkretisierung in die etablierten Entwicklungsmethoden und die entsprechenden Toolumgebungen der betroffenen Domänen wie Mechanik, Elektrotechnik, Softwaretechnik sowie Anlagen- und Prozesstechnik mündet.

Das Systems Engineering soll – insbesondere in KMU – mehr Akzeptanz erhalten und dort zunehmend kooperativ genutzt werden. Die zunehmende Komplexität von Industrie 4.0-Systemen wird damit beherrscht und ermöglicht die effiziente und effektive Abwicklung von Projekten im Engineering- und Produktionsverbund.

Folgende Ergebnisse werden erwartet:

- aufeinander abgestimmte Methoden sowie abgestimmte Werkzeugketten und Entwicklungsumgebungen
- System- und ortsunabhängige Nutzung der Werkzeuge
- Semantik der applikativen Schnittstellen
- Disziplinübergreifendes, durchgängiges Anforderungsmanagement in komplexen Systemen

5.3.2.3 Die wesentlichen Meilensteine

Methodik
5.2 Praxistaugliche Leitfäden sowie Aus- und Weiterbildungsprogramme 5.3 Durchgängiges Anforderungsmanagement in komplexen Systemen entlang der vertikalen Integration 5.6 Branchenunabhängiges Referenzmodell für Entwicklung intelligenter technischer Systeme
Lösungen
5.1 Erstes aufeinander abgestimmtes Methodenset; erste aufeinander abgestimmte Werkzeugkette 5.4 System-, Mandanten- und ortsunabhängige Werkzeug-Nutzung 5.5 Semantik der applikativen Schnittstellen
Voraussetzungen
5.a Aufnahme von technischen und produktionstechnischen Anforderungen in frühen Entwicklungsphasen 4.1 Erste Modellierungstheorie zur Entwicklung von komplexen automatisierungs- bzw. produktionstechnischen Systemen 5.c Disziplinübergreifende Modularisierung von technischen Systemen 5.d Erweiterung bestehender Standards zur produktionszentrierten Beschreibung von Produkten

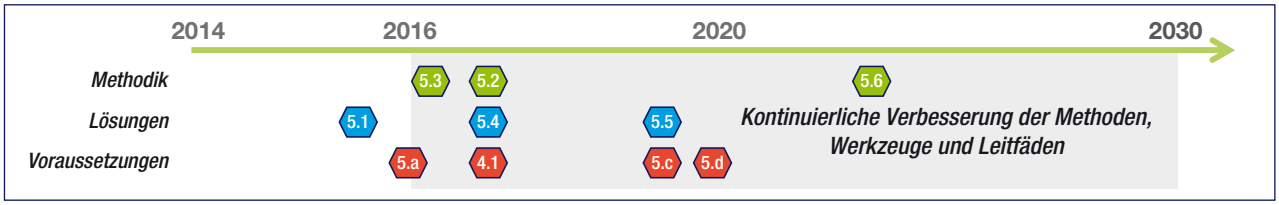


Abbildung 6: Meilensteine für die Forschung zum Thema „Systems Engineering“

5.4 Themenfeld: Vertikale Integration und vernetzte Produktionssysteme

Unter vertikaler Integration verstehen wir die Integration der verschiedenen IT-Systeme auf den unterschiedlichen Hierarchieebenen eines Produktionssystems (beispielsweise die Aktor- und Sensorebene, Steuerungsebene, Produktionsleitebene, Manufacturing und Execution-Ebene, Unternehmensplanungsebene) zu einer durchgängigen Lösung.

5.4.1 Sensornetze

5.4.1.1 Inhalte von Forschung und Innovation

Die zentrale Motivation hinter der Sensordatenanalyse ist die kontinuierliche Erfassung von Informationen über einen (technischen) Prozess entweder als Basis für dessen Steuerung und Regelung oder für eine Diagnose, Alarmierung etc. So können beispielsweise bei einem reaktivem Eingriff Prozessparameter angepasst werden oder bei Diagnosen Maschinendefekte signalisiert werden.

Die Verknüpfung der diversen Sensoren und deren Auswertung (teilweise unter kritischen Echtzeitbedingungen) ist eine zentrale Herausforderung.

Zu berücksichtigende Fragen sind:

- Wie kann Data Acquisition bei einer großen Anzahl von Sensoren in der Praxis gestaltet werden?
- Wo wird Data Manipulation sinnvollerweise durchgeführt?
- Wie kann der qualitative und quantitative Zusammenhang zwischen gemessenen Werten und auftretenden Effekten erkannt und in ein (Zustands-)Modell überführt werden?

5.4.1.2 Angestrebte Ergebnisse von Forschung und Innovation

Es soll ein Gerüst entwickelt werden für die Umsetzung von zustandsabhängigen Überwachungen und Steuerungen in Industrie 4.0-Szenarien. Der Zugriff auf die Hauptkomponenten (Layer) der Sensordatenverarbeitung soll, soweit möglich, standardisiert werden. Es wird eine Softwarearchitektur entstehen, die den Zugriff auf Sensordaten ermöglicht, ohne Kenntnisse über die physische Sensorebene besitzen zu müssen (Kapselung). Insbesondere ist die Einbindung kabelloser Sensoren zu berücksichtigen. Die Inbetriebnahme und Konfiguration soll grafisch und interaktiv mittels Plug-and-Play-Ansatz realisiert werden. Die Auswertung mehrerer Sensordatenströme im Sinne von Datenfusion muss ermöglicht werden, ohne dass jeder Anwendungsfall individuell entwickelt werden muss. Um einen möglichst hohen Grad an Autonomie des Sensornetzes zu erreichen, sollen die Sensoren mit semantischen Beschreibungen angereichert werden (Semantic Sensor Network Technologie).

Folgende Ergebnisse werden erwartet:

- erweiterte und verfeinerte Modelle zur Feststellung des System-/Produktzustands, die die Ableitung zuverlässiger Handlungsempfehlungen ermöglichen
- Online-Regelung eines Fertigungsprozesses in Abhängigkeit von den rückgeführten Echtzeitdaten aus dem Prozess sowie der Qualität des Prozessoutputs
- Einführung fallspezifischer, adaptiver Messstrategien in die Qualitätssicherung
- Etablierung einer branchenübergreifenden Community

5.4.1.3 Die wesentlichen Meilensteine

Methodik
6.1 Transparenter Zugriff auf Sensordaten über universelle Schnittstellen / Beschreibung der Sensoren mit Metadaten 6.3 Selbstorganisierende Kommunikationskonzepte
Lösungen
6.2 Interaktiver Inbetriebnahmeprozess mittels Plug-and-Play Ansatz 6.4 Algorithmen zur dezentralen Datenanalyse (Fog-Computing), Amalgamation mit Cloud-Computing-Ansatz 6.5 Dynamische Regelung komplexer Fertigungsprozesse, vertikale Integration mit betriebswirtschaftlichen Prozessen
Voraussetzungen
6.a Lokale Datenerfassung, -verarbeitung und -speicherung in dezentralen Sensorknoten 6.b Vernetzte Produktionssysteme (Internet der Dinge und Dienste) 6.c Verfügbarkeit energieautarker Sensoren

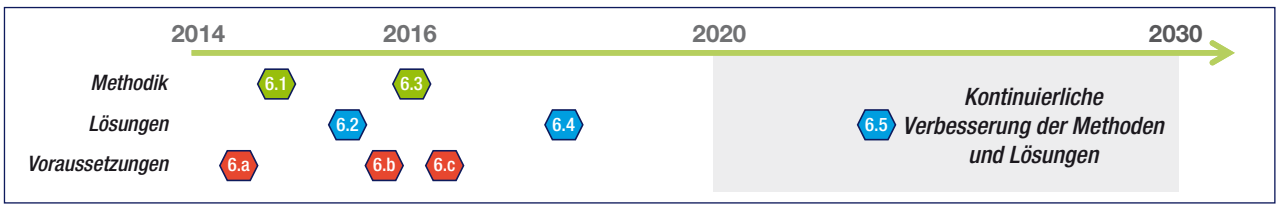


Abbildung 7: Meilensteine für die Forschung zu Sensornetzwerken

5.4.2 Intelligenz – Flexibilität – Wandelbarkeit

5.4.2.1 Inhalte von Forschung und Innovation

Intelligente Produktionssysteme sind adaptiv. Das heißt, sie interagieren auf Basis des integrierten Modellwissens mit ihrer Umgebung und passen sich ihr selbstständig an. Sie sind robust. Sie bewältigen auch unerwartete, vom Entwickler nicht berücksichtigte Situationen in einem sich stetig ändernden Umfeld, ohne ihre Leistungsniveau zu reduzieren. Sie sind aber auch vorausschauend. Sie antizipieren auf der Basis von Erfahrungswissen die Wirkungen unterschiedlicher Einflüsse. Und sie sind schließlich auch benutzungsfreundlich. Sie berücksichtigen sowohl das unterschiedliche Verhalten von Anwendern als auch den unterschiedlichen Informationsbedarf und passen sich diesem selbstständig an. Flexibilität bedeutet, dass Prozesse bzw. Systeme in definierten und begrenzten Korridoren vorgedacht wurden, um ein möglichst breites Spektrum an Anforderungen abzudecken. Im Produktionsumfeld bedeutet das ein flexibles Zusammenspiel von Menschen, Maschinen, Produktionssystemen und Wertschöpfungsnetzen in Bezug auf die Fertigung unterschiedlicher Produkte bzw. Varianten. Wandelbarkeit bedeutet, Grenzen der Flexibilitätskorridore zu verschieben. Damit können Prozesse und Systeme über einen konstruktiven Schritt geändert bzw. umgebaut werden. Im Produktionsumfeld, bezogen auf eine Maschine, ist das ein „einfaches“ Umbauen zur Fertigung neuer Produkte und Varianten, bezogen auf ein Produktionssystem ein „einfaches“ Ändern des Aufbaus.

Zu berücksichtigende Aspekte sind:

- Identifikation, Formalisierung und Beschreibung der direkt und indirekt auf die globalen Ziele wirkenden Flexibilisierungs- und Wandlungsmöglichkeiten
- Standardisierung der Schnittstellen und Fähigkeiten von Einheiten (Modulen) zum Aufbau einer flexiblen und wandelbaren Produktion
- soziale, ethische, ökologische und ergonomische Auswirkungen

Engineering und Testen von autonomen Systemen im Produktionsumfeld; die Entwickler autonomer Systeme müssen entsprechend geschult und ausgebildet werden

5.4.2.2 Angestrebte Ergebnisse von Forschung und Innovation

Durch Intelligenz entfalten Produkte und Produktionssysteme neue Funktionalitäten und entlasten ihre Benutzer. Es werden Entwicklung, Engineering, Wartung und Lebenszyklusmanagement verbessert und es erhöhen sich Zuverlässigkeit, Sicherheit und Verfügbarkeit von Produkten und Produktionssystemen. Darüber hinaus werden Ressourcen wie Energie und Material effizienter eingesetzt und ermöglichen so äußerst flexible und einfach wandelbare Produktionsprozesse und -systeme.

Folgende Ergebnisse werden erwartet:

- Identifikation von autonomen, wiederverwendbaren Einheiten (Modulen) innerhalb einer Produktion und Ableitung der Anforderungen und Potenziale für Arbeitsmodelle
- robuste, zuverlässige Algorithmen für zentrale und dezentrale Intelligenz
- Strategien für die Verhandlung zwischen intelligenten Systemen im Produktionsumfeld
- Technologien und Anwendungsbeispiele für eine intuitive Mensch-Maschine-Interaktion
- Migrationsstrategien hin zu flexiblen und wandelbaren Produktionen

5.4.2.3 Die wesentlichen Meilensteine

Methodik
7.1 Analyse von Flexibilisierungs- und Wandlungsmöglichkeiten sowie deren Auswirkungen auf Arbeitsmodelle 7.2 Migrationsstrategien in Richtung einer flexiblen und wandelbaren Produktion 7.3 Methoden und Beschreibungsmittel für das Engineering und Testen von autonomen Systemen
Lösungen
7.4 Technologien und Anwendungsbespiele für eine intuitive Mensch-Maschine-Interaktion 7.5 Standardisierung der Kooperation zwischen intelligenten Systemen im Produktionsumfeld 7.6 Robuste, zuverlässige Algorithmen für zentrale und dezentrale Intelligenz
Voraussetzungen
3.2 Strategische Vorgaben – Zielhierarchiesystem – Prozessmodellierung 9.5 Modelle für Beteiligung der betroffenen Mitarbeiter und des Betriebsrats am Implementationsprozess von Industrie 4.0 3.3 Komplexitätsbeherrschung und Anwendbarkeit

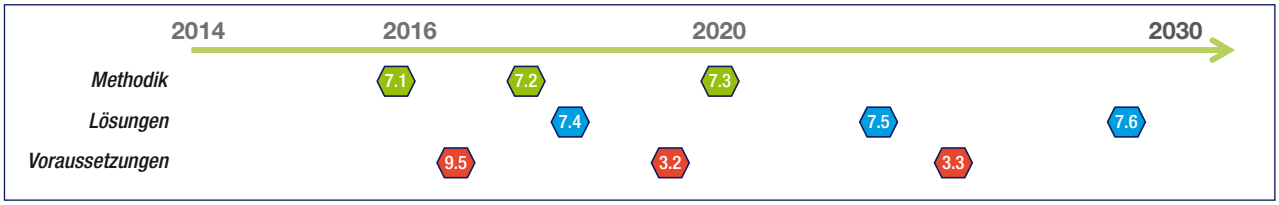


Abbildung 8: Meilensteine für die Forschung zu Intelligenz – Flexibilität – Wandelbarkeit

5.5 Themenfeld: Neue soziale Infrastrukturen der Arbeit

AG3 kann aufgrund seiner Kompetenzen und Erfahrungen FuE-Bedarf nur zu technischen Aspekten benennen. Die inhaltlichen Themen in diesem Abschnitt werden deshalb vom wissenschaftlichen Beirat beigesteuert.

5.5.1 Multimodale Assistenzsysteme

5.5.1.1 Inhalte von Forschung und Innovation

Grundsätzlich adressiert dieses Themenfeld eine humanzentrierte Auslegung der Mensch-Maschine-Schnittstelle. Im Rahmen von Industrie 4.0 wird sich die Mensch-Technik-Interaktion verändern: Die Maschinen passen sich den Menschen an – und nicht umgekehrt. Intelligente industrielle Assistenzsysteme mit multimodalen, bedienungsfreundlichen Benutzerschnittstellen können die Beschäftigten bei ihrer Arbeit unterstützen und bringen digitale Lerntechnologien direkt an den Arbeitsplatz.

Zu berücksichtigende Aspekte bei der Interaktionsgestaltung sind:

- Sinnfälligkeit der Ein-/Ausgaben
- Wahrnehmbarkeit, auch unter ungünstigen Bedingungen
- Identifizierbarkeit, Verwechslungssicherheit
- Aufgabenangemessenheit
- Selbstbeschreibungsfähigkeit
- Steuerbarkeit
- Erwartungskonformität

5.5.1.2 Angestrebte Ergebnisse von Forschung und Innovation

In der Fabrik sollen neue Formen der kollaborativen Arbeit entstehen, gestützt durch intelligente Assistenzsysteme. Methoden und Techniken der erweiterten Realität (Augmented Reality), der Dualwelttechnologie (Dual Reality) und der synchronisierten und multiplen Welten – also der Echtzeitsynchronisation von sensomotorischen und semanti-

schen Fabrikmodellen mit realen Fabriken – ermöglichen kollaborative Teleoperationen von hochkomplexen Komponenten, etwa bei der Fehlersuche. Die Zusammenarbeit der Beschäftigten wird sich damit grundlegend verändern. Kooperation und Kollaboration, zum Beispiel über angepasste soziale Netzwerke und soziale Medien, werden auch über Unternehmens- und Bildungsniveaugrenzen hinaus möglich. Leicht adaptierbare Interaktionssysteme werden der Heterogenität der Belegschaft Rechnung tragen, weil sie personalisiert und für spezielle Zielgruppen entwickelt sind.

Folgende Ergebnisse werden erwartet:

- Integration virtueller Menschmodelle zur Unterstützung der Simulation maschineller Produktionsabläufe
- Voraussetzungen für die Nutzung und den Erhalt von Erfahrungswissen der Beschäftigten als Bedingung eines stabilen Systembetriebs
- Herstellung und Sicherung von Transparenz über den Systemstatus für die Beschäftigten
- Absicherung der Qualifizierung für alle Beschäftigtengruppen
  - Förderung digitaler Lerntechniken
  - Weiterentwicklung digitaler Lerntechniken

5.5.1.3 Die wesentlichen Meilensteine

Methodik
8.1 Definition von industriellen Anwendungsfällen für eine sinnvolle multimodale Unterstützung von Arbeitsschritten 8.3 Allgemeine Methodik zur Bewertung der Interaktion
Lösungen
8.2 Praxistaugliche Leitfäden für eine aufgabenbezogene Interaktionsgestaltung in allen Phasen des Produktlebenszyklus 8.4 Präzisierung der Gestaltungsrichtlinien der Mensch-Maschine-Schnittstelle
Voraussetzungen
8.a Praxistaugliche Endgeräte für den Einsatz im Augmented Reality bzw. Dual Reality im Anwendungsfeld der Industrie 8.b Vernetzung von PLM-Systemen und Entwurf von Engineeringkonzepten für AR-/DR-Anwendungen 8.c Bereitschaft zur Flexibilisierung von Beschäftigungsverhältnissen 8.d Bereitschaft zur Gestaltung von Interaktionssystemen, die der Heterogenität der Belegschaft Rechnung trägt 8.e Sicherstellung des Qualifizierungszugangs für alle Beschäftigungsgruppen

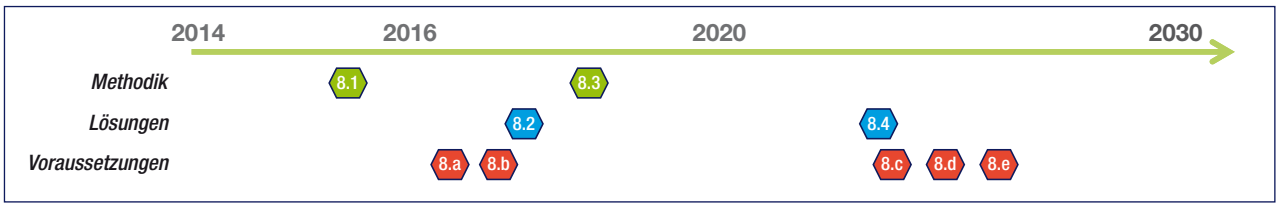


Abbildung 9: Meilensteine für die Forschung zu multimodalen Assistenzsystemen

5.5.2 Technologieakzeptanz und Arbeitsgestaltung

5.5.2.1 Inhalte von Forschung und Innovation

Industrie 4.0 muss von den Mitarbeitern in der Produktion akzeptiert werden. Die Voraussetzung dafür sind Arbeitsbedingungen, die eine Flexibilität im Sinne der Mitarbeiter ermöglichen und ihre Kreativität und Lernfähigkeit unterstützen. „Multimodale Assistenzsysteme“ werden dafür die technologische Voraussetzung schaffen. Im Fokus dieses Themenfelds sind auch die Qualifikationsentwicklung und die Arbeitsorganisation sowie die Gestaltung der Arbeitsmittel im Rahmen von Industrie 4.0-Systemen.

Zu berücksichtigende Aspekte sind:

- grundlegendes Verständnis von Industrie 4.0 als sozio-technisches System, in dem Technik, Organisation und Personal systematisch aufeinander abgestimmt werden müssen
- Arbeitsgestaltung, die die Akzeptanz, Leistungs- und Entwicklungsfähigkeit, das Wohlbefinden und die Gesundheit arbeitender Menschen unterstützt
- Beteiligung der Mitarbeiter und Gremien der Arbeitnehmervertretung an Einführungsprozessen

5.5.2.2 Angestrebte Ergebnisse von Forschung und Innovation

Das Aufgabenspektrum der Mitarbeiter soll erweitert werden, ihre Qualifikationen und Handlungsspielräume sollen erhöht und ihr Zugang zu Wissen deutlich verbessert werden. Auszugehen ist davon, dass neuartige kollaborative Formen von Produktionsarbeit möglich und systembedingt erforderlich werden. Damit bietet Industrie 4.0 die Chance, die Attraktivität von Produktionsarbeit zu steigern und dem absehbaren Fachkräftemangel entgegenzuwirken. Schließlich werden gute Voraussetzungen geschaffen, durch entsprechende Maßnahmen der Arbeitsgestaltung den wachsenden Anforderungen einer alternden Belegschaft gerecht zu werden.

Folgende Ergebnisse werden erwartet:

- Konzepte für Tätigkeits- und Aufgabenstrukturen, die an Akzeptanz, Leistungs- und Entwicklungsfähigkeit, Wohlbefinden und Gesundheit arbeitender Menschen ausgerichtet sind
- Vorschläge für die Integration von planenden, organisierenden, durchführenden und kontrollierenden Tätigkeiten an einem Arbeitsplatz
- Modelle für ein angemessenes Verhältnis zwischen anspruchsarmen Routineaufgaben und anspruchsvolleren problemlösenden Aufgaben
- lernförderliche Arbeitsmittel, die die Arbeitsorganisation unterstützen
- Modelle für die Beteiligung sowohl der betroffenen Mitarbeiter als auch des Betriebsrats am Implementationsprozess von Industrie 4.0

5.5.2.3 Die wesentlichen Meilensteine

Methodik
-
Lösungen
9.1 Konzepte für geeignete Tätigkeits- und Aufgabenstrukturen 9.2 Vorschläge für die Integration von planenden, organisierenden, durchführenden und kontrollierenden Tätigkeiten 9.3 Modelle für angemessenes Verhältnis zwischen anspruchsarmen Routineaufgaben und anspruchsvolleren Aufgaben 9.4 lernförderliche Arbeitsmittel, die die Arbeitsorganisation unterstützen 9.5 Modelle für Beteiligung der betroffenen Mitarbeiter und des Betriebsrats am Implementationsprozess von Industrie 4.0
Voraussetzungen
-

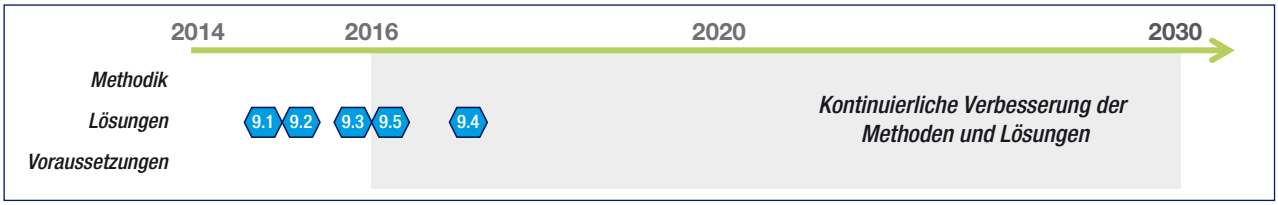


Abbildung 10: Meilensteine für die Forschung zu Technologieakzeptanz und Arbeitsgestaltung

5.6 Themenfeld: Querschnittstechnologien für Industrie 4.0

Die Liste der Querschnittstechnologien in diesem Kapitel erhebt keinen Anspruch auf Vollständigkeit und ist erweiterbar. Wichtig für Erweiterungen um weitere Technologien ist, jeweils die Bedeutung der Querschnittstechnologie speziell für Industrie 4.0 deutlich herauszuarbeiten.

5.6.1 Netzkommunikation für Industrie 4.0-Szenarien

5.6.1.1 Inhalte von Forschung und Innovation

Dieses Themenfeld adressiert die Netzkommunikation der involvierten stationären und mobilen Komponenten von Cyber-Physical Systems. Das sind Komponenten, Dienstleistungs- und Produktivsysteme im Shopfloor und in den Hintergrund-Systemen des Unternehmens, in denen der Austausch von Daten über die damit verbundenen Lieferketten und die Phasen des Lebenszyklus hinweg möglich ist.

Zu berücksichtigende Aspekte sind:

- Anforderungsgerechte Nutzung der drahtlosen Kommunikation im Büro und Shopfloor
- Koexistenz verschiedenster drahtloser und drahtgebundener Kommunikationssysteme und proprietärer Systeme
- Interoperabilität verschiedenster drahtloser Kommunikationssysteme
- vorausschauende Wirkungsanalyse bei sich ändernden Systemkonfigurationen
- weltweiter Einsatz der Produkte in den verfügbaren Bändern
- Anforderungsmanagement der Bandbreite, Deterministik und Echtzeit
- skalierbare und durchgängige Nutzung in einer interoperablen Engineering-Kette
- Security und Safety

5.6.1.2 Angestrebte Ergebnisse von Forschung und Innovation

Um den Anforderungskatalog für den Einsatz in Industrie 4.0-Produktionsszenarien zu erfüllen, sollen Vernetzungs- und Anbindungslösungen für den branchenübergreifenden Einsatz entwickelt und bewertet werden. Insbesondere die

Anforderungen an die Übertragungsleistung, Robustheit, die Security und Safety sowie die Zuverlässigkeit, Wirtschaftlichkeit und die internationale Ausrollbarkeit sind Ziele dieses Themenfelds.

Folgende Ergebnisse werden erwartet:

- Kosten-Effizienz und Akzeptanz von Industrie 4.0 durch standardisierte Lösungen, deren Standards die Ziele Interoperabilität, Skalierbarkeit, Kostensensitivität (z. B. auch für den teuren Sensor in geringer Stückzahl) und Anforderungsakzeptanz berücksichtigen. Standards sind durch Mechanismen zu qualifizieren, die in den üblichen Entwicklungsprozessen nutzbar sind und keine kostenerhöhenden Zertifikate (weder technisch noch räumlich getrieben) beinhalten. Hier sind z. B. offene Verfahren wie die CE „Selbsterklärung der Hersteller“ anzustreben.
- Bewertung der Möglichkeiten heutiger und zukünftiger
  - öffentlicher Netze im Industrie 4.0-Kontext
  - WLAN-Technologien und möglicher Alternativen wie z. B. Bluetooth im Industrie 4.0-Kontext
  - Nahfeld-Technologien im Industrie 4.0-Kontext
- Identifikation von Anforderungen an spezifische
  - Funklösungen, Netzwerktechnologien öffentlicher Netze, proprietäre Lösungen und Identifikation möglicher Alternativen
  - Applikationsfelder wie Gebäude, Prozesstechnik oder Infrastruktur (Energie, Wasser, Transportwesen)

5.6.1.3 Die wesentlichen Meilensteine

Methodik
10.1 Redesign öffentlicher Netze, Ableitung neuer Funktechnologien & Frequenzplanung in Public-Private Partnership 10.3 Standardisierung SDN-basierter Virtualisierung von Netzwerkressourcen 10.5 Evolutionäre Weiterentwicklung der Funkstandards, Nahfeldtechnologien und adaptiver Antennensysteme
Lösungen
10.2 100 Gbit/s 5G Netzwerkinfrastruktur in öffentlichen Netzen verfügbar 10.4 SDN im produktiven Einsatz 10.6 Nutzung neuer Funkstandards, Nahfeldtechnologien und adaptiver Antennensysteme in I40 Anwendungen
Voraussetzungen
10.a Design und Standardisierung der 5G Netzwerkinfrastruktur sowie neuer Funkstandards und Nahfeldtechnologien 10.b Verfügbarkeit von Standardhardware für SDN-basierte Netzwerk-Virtualisierung 10.c Industrialisierung neuer Antennentechnik für flexible Funknetzwerke 10.d Standardisierung von Koexistenzverfahren inkl. Interferenzdetektion, -unterdrückung und -vermeidung

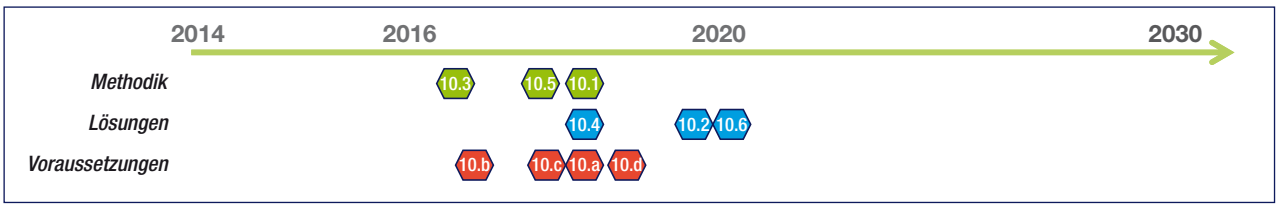


Abbildung 11: Meilensteine für die Forschung zu Netzkommunikation für Industrie 4.0-Szenarien

5.6.2 Mikroelektronik

5.6.2.1 Inhalte von Forschung und Innovation

Die Mikroelektronik ist die Basis für die CPS-Hardware zur intelligenten Steuerung, Überwachung und Identifikation von Produktions- und Logistikprozessen in der Industrie 4.0. Sie stellt einen umfangreichen Baukasten bereit, um Elemente der Industrie 4.0-Szenarien schrittweise umzusetzen. In diesem Zusammenhang steht die Mikroelektronik sowohl für „Moore“ als auch für „More than Moore“-Technologien, denen eine besondere Bedeutung zukommt, da die Technologien zur Systemintegration (z. B. 3D-Integration auf Waferlevel, Selbstdiagnosefähigkeit, Energieeffizienz) hier eine Schlüsselrolle spielen.

Die wichtigsten Forschungsthemen sind:

- Mikro-Elektro-Mechanische Systeme (MEMS) inkl. Sensoren und Aktoren
- Embedded Systems on Chip inkl. Spezialprozessoren, spezielle echtzeitfähige Mikrocontroller und Hightech-Speicher mit hoher Leistung und minimaler Leistungsaufnahme sowie Multi-Core-Architekturen
- Leistungselektronik für effizient arbeitende Aktuator-Systeme
- Funkkommunikation (low power, low latency)
- Energy Harvesting mit höchstmöglicher Ausbeute
- Systemintegration
- Embedded IT-Security Architektur
- Robustheit und Alterungsresistenz

5.6.2.2 Angestrebte Ergebnisse von Forschung und Innovation

Die Mikroelektronik ist eine der Schlüsseltechnologien, um Industrie-4.0-Ziele wie Flexibilität, Produktivitätserhöhung und Kostenreduktion zu verwirklichen. Hierzu ist ein optimiertes Zusammenspiel von spezieller elektronischer Hardware und intelligenter Software Voraussetzung. Die Umsetzung von Industrie 4.0-Szenarien hängt von der Verfügbarkeit geeigneter mikroelektronischer Bausteine und Systeme ab. Es besteht daher Bedarf an kontinuierlicher Forschung und Entwicklung, um neue Komponenten der Mikroelektronik zu entwickeln und bestehende an die konkreten Anforderungen im Industrie-4.0-Umfeld anzupassen.

5.6.2.3 Die wesentlichen Meilensteine

Methodik
11.1 Systemintegration 11.2 Robustheit und Alterungsresistenz 11.3 Energy Harvesting mit höchstmöglicher Ausbeute 11.4 Embedded Systems on Chip, spezielle echtzeitfähige Mikrocontroller und Hightech-Speicher
Lösungen
11.5 Mikro-Elektro-Mechanische Systeme (MEMS) inkl. Sensoren und Aktoren 11.6 Embedded IT-Security 11.7 Leistungselektronik für effizient arbeitende Aktuator-Systeme 11.8 Funkkommunikation (low power, low latency)
Voraussetzungen
5.1 Erstes aufeinander abgestimmtes Methodenset; erste aufeinander abgestimmte Werkzeugkette 10.5 Evolutionäre Weiterentwicklung der Funkstandards, Nahfeldtechnologien und adaptiver Antennensysteme

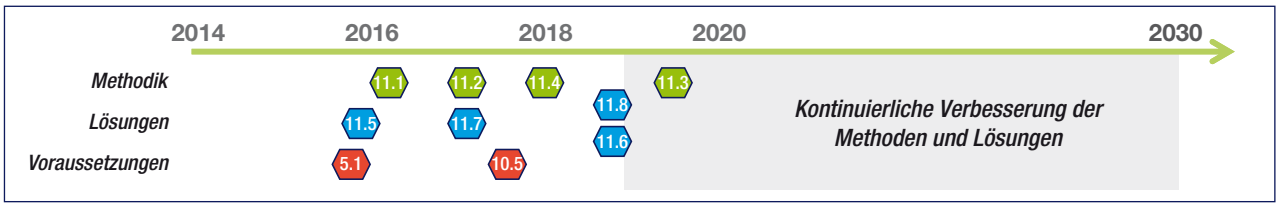


Abbildung 12: Meilensteine für die Forschung zur Mikroelektronik

5.6.3 Safety & Security

5.6.3.1 Inhalte von Forschung und Innovation

Security („Informationssicherheit“, engl.: „information security“) stellt die Verfügbarkeit, Integrität und Vertraulichkeit der Informationen in Industrie 4.0-Anlagen und -Systemen sicher. Bei Security geht es darum, Gefahren abzuwehren, die auf die Anlage bzw. deren Funktionen einwirken. Insbesondere sind explizite und nicht intendierte Angriffe eingeschlossen. Sicherzustellen ist die Informationssicherheit für alle Funktionalitäten, sowohl für Betriebsfunktionen als auch für Überwachungsfunktionen und Schutzfunktionen (z. B. Safety).

Bei Safety („Funktionale Sicherheit“, engl.: „functional safety“) für Systeme geht es darum, durch geeignete Maßnahmen sicherzustellen, dass von der Funktion einer Maschine oder Anlage keine Gefahr für Menschen oder Umwelt ausgeht. Safety ist ein Teil der Schutzfunktionen zur Betriebssicherheit.

Für Produkte, Komponenten und Industrie 4.0-Anlagen sind folgende Schutzziele zu berücksichtigen:

- Verfügbarkeit und Integrität
- Betriebssicherheit
- Know-how-Schutz
- Datenschutz

Der sichere Nachweis der Identität ist bei Industrie 4.0 von besonderer Bedeutung.

Wichtige zu berücksichtigende Aspekte sind:

- Bewertungsverfahren für Bedrohungspotenziale und Risiken inklusive Kosten/Nutzen-Abschätzung von Sicherheitsmaßnahmen
- Schutz von Schnittstellen im Außen- und im Innenverhältnis
- Schutz von Kommunikationssystemen in der Anlage
- Auswirkung von Security-Lücken auf Gefahren für die Betriebssicherheit
- Wechselwirkung mit rechtlichen Vorgaben z. B. zu Datenschutz
- Security-by-Design
- Langzeittauglichkeit von Sicherheitslösungen
- Angriffsdetektion und -analyse

Dabei sind folgende Randbedingungen zu berücksichtigen:

- Ausrichtung der Sicherheitsbetrachtung an den betroffenen horizontalen und vertikalen Wertschöpfungsnetzen
- Ausrichtung an konkreten Use Cases und zeitnahe Übertragung in anwendbare Ergebnisse, die die Praxistauglichkeit beweisen
- Berücksichtigung des „Faktors Mensch”: Transparenz, Usability, Nutzerakzeptanz, Datenschutz

5.6.3.2 Angestrebte Ergebnisse von Forschung und Innovation

Bereits heute sind vielfältige Standards und Technologien vorhanden, wobei im industriellen Umfeld bisher nur wenig umgesetzt ist. Die Gründe hierfür sind vielfältig, im Wesentlichen ist aber festzustellen, dass der Hauptzweck einer Automatisierungslösung nicht Security-Funktionen sind. Für die Anbieter verteuern Security-bezogene Prozesse Entwicklung und Fertigung und erfordern heute häufig nicht vorhandene Kenntnisse. Für die Betreiber stellen Security-Konzepte häufig entsprechende Hürden bezüglich Aufwand und Akzeptanz seitens des Bedienpersonals dar.

Um eine hohe Akzeptanz aller Parteien zu erreichen, sind Lösungen zu realisieren, die bedienerfreundlich für die Anwender sind, Entwickler durch Tools entlasten und effiziente Methoden zu einer Security-Bewertung bereitstellen.

Folgende Ergebnisse werden erwartet:

- Einfach handhabbare und benutzerfreundliche Security-Methoden.
- Skalierbare Security-Infrastrukturen für industrielle Domänen
- Einfach anwendbare Methoden und Bewertungsverfahren hinsichtlich der Security-Eigenschaften einzelner Komponenten und deren Komposition zu einer Industrie 4.0-Anlage. Zu berücksichtigen sind dabei

„Plug&Operate“ und die autonome, dynamische Konfiguration

- Methoden zur dynamischen Ermittlung und Bewertung der Safety-Funktionen einer Anlage unter Berücksichtigung der Wirkung des erzielten Security-Niveaus auf Restrisiken im Sinne von Safety
- Vorbereitung der Security-Standardisierung
- Erstellung geeigneter Maßnahmen-Kataloge für den Eintrittsfall von Sicherheitslücken, z. B. nach CERT-Methoden

5.6.3.3 Die wesentlichen Meilensteine

Die Definition von Meilensteinen für die längerfristige Planung der Forschung zum Thema „Security & Safety“ in Form von Methoden, Lösungen und die dafür notwendigen Voraussetzungen steht noch aus.

5.6.4 Datenanalyse

5.6.4.1 Inhalte von Forschung und Innovation

Zentrale Motivation für die Datenanalyse ist einerseits die sich damit bietende Möglichkeit zum Generieren von (neuen) Erkenntnissen. Andererseits dient „actionable“ Datenanalyse zur Entscheidungsunterstützung sowie für autonome Entscheidungen (Welche Information an wen und wann zur Verfügung stellen), was dann Unternehmen hilft, die Qualität ihrer Produkte und die Effizienz ihrer Produktion zu erhöhen und mögliche Fehlerentwicklungen frühzeitig zu erkennen. Dies dient insbesondere auch als Basis für neue Geschäftsmodelle. Zur Anwendung kommen hierzu Methoden der prädiktiven Analyse. Sie umfassen eine Vielzahl grundlegender Techniken aus der Statistik, dem maschinellen Lernen und Data Mining. Gegenwärtige und historische Messwerte, aber auch „unstrukturierte“ Daten beispielsweise aus sozialen Netzen, werden analysiert, um daraus bisher unbekannte Zusammenhänge offenzulegen (descriptive analytics) oder auch Abschätzungen über zukünftiges Systemverhalten bzw. Effekte ableiten zu können (predictive analytics). Die neu gewonnenen Erkenntnisse ermöglichen letztlich die Beurteilung verschiedener Handlungsalternativen und damit eine kontinuierliche Optimierung von Systemen, Prozessen und Strategien (prescriptive analytics). Die Ableitung von Handlungsempfehlungen oder direkten Maßnahmen auf Basis der Datenanalyse ist die eigentliche Herausforderung.

Das Thema „Datenanalyse“ beinhaltet die folgenden Aspekte:

- Data Manipulation
- State Detection
- Prognostic Assessment
- Advisory Generation

5.6.4.2 Angestrebte Ergebnisse von Forschung und Innovation

Es soll ein Kriterienkatalog für den Einsatz von Datenanalysen entwickelt werden, der die Umsetzung der folgenden Prinzipien ermöglicht:

- Zugriff auf Daten, ohne Kenntnisse über die konkrete (physische) Herkunft (Kapselung resp. Virtualisierung)
- Einbinden neuer Datenquellen über standardisierte Schnittstellen mittels Plug&Use Ansatz (semantische Beschreibung)
- Nutzung der Daten in einem branchenübergreifenden Wertschöpfungsnetzwerk
- Eine breite und kontinuierlich erweiterbare Prozessbasis soll erstellt werden, die die Ableitung neuer Anwendungsfälle erlaubt
- Rechtssicherheit (Wer hat welche Rechte an welchen Daten und daraus resultierenden Erkenntnissen)

Dazu sollen Prinzipien entwickelt werden, die einer Softwarearchitektur und entsprechenden Schnittstellen die Auswertung mehrerer Datenströme im Sinne von Datenfusion auf einer Metaebene ermöglicht, ohne dass jeder Anwendungsfall individuell entwickelt werden muss.

- Modelle zur Beschreibung von Zuständen sollen entwickelt werden, die die Prädiktion zukünftiger Zustände ermöglichen
- Verfahren und Algorithmen sollen entwickelt werden, die die stetig steigenden Datenmengen effektiv und effizient analysieren können

5.6.4.3 Die wesentlichen Meilensteine

Methodik
13.2 Anwendungsleitfaden zur Nutzung von Datenanalyse im Umfeld der Produktion 13.4 Analytics Technologien zur online Anpassung und Optimierung von Produktionsprozessen
Lösungen
13.1 Technologien und Anwendungsbeispiele für Datenanalyse 13.3 Algorithmen zur dezentralen Datenanalyse (Fog-Computing), Amalgamation mit Cloud-Computing-Ansatz 13.5 Dynamische Regelung komplexer Fertigungsprozesse, vertikale Integration mit betriebswirtschaftlichen Prozessen
Voraussetzungen
13.a Juristische Klärung des Eigentums- und Verfügungsverhältnisses an den Daten 13.b Theoretische Grundlagen zu descriptive-, predictive- und prescriptive analytics

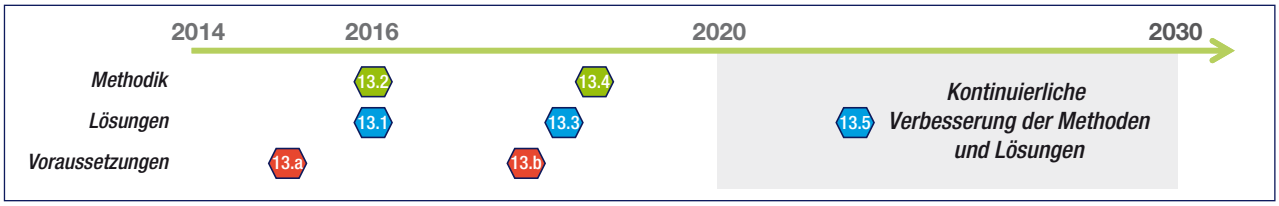


Abbildung 13: Meilensteine für die Forschung zum Thema „Datenanaylse“

5.6.5 Syntax und Semantik für Industrie 4.0

5.6.5.1 Inhalte von Forschung und Innovation

Die Realisierung von Industrie 4.0-Szenarien setzt voraus, dass die beteiligten Objekte (beispielsweise Maschinen, Maschinenkomponenten, Produkte- und Produktbeschreibungen oder Ressourcen im Sinne der Digitalen Fabrik) von den handelnden Subjekten (z. B. Menschen, Software-Werkzeugen, Software-Agenten, Leitsystemen, Software-Diensten) interpretiert, d.h. identifiziert und verstanden werden können. Dafür müssen die jeweils relevanten Eigenschaften der Objekte in Form von Merkmalen in einem Modell und die Aufgaben der Objekte in Bezug auf Rollen beschrieben werden. Die Basis dafür sind Informationsmodelle; damit diese in Computern verarbeitet werden können, werden im Produktionsumfeld (Daten-)Modelle, Modellsysteme, Erklärungsmodelle, Planungsmodelle sowie Komponentenmodelle benötigt.

Die Syntax beschreibt gültige Symbole, die zur Beschreibung von Dokumenten und Daten verwendet werden dürfen (z. B. Buchstaben, Ziffern, Sonderzeichen, graphische Symbole), und wie diese Zeichen korrekt miteinander zu Symbolketten verbunden werden.

Die Semantik stellt eine Beziehung zwischen Symbolen und Modellen her, dadurch bekommen Symbolketten bzw. Daten eine Bedeutung, und aus Daten werden Informationen. Eine solche Beziehung ist z. B. die Vereinbarung, dass eine bestimmte Zeichenkette in einer Datei ein bestimmtes Merkmal eines Modells beschreibt, welche Attribute dieses Merkmals näher beschreiben und welche Ausprägungen diese Attribute haben dürfen. Zudem müssen auch die Interdependenzen zwischen den Merkmalen und den Attributen beschrieben werden.

5.6.5.2 Angestrebte Ergebnisse von Forschung und Innovation

Ziel ist es, für Industrie 4.0-Szenarien eine formale, computer-verarbeitbare Form der Beschreibung als gemeinsame Semantik zu entwickeln und damit auf Anwendungs- und Nutzungsebene eine domänenspezifische „Sprache“ zu spezifizieren, die alle Objekte, Subjekte und deren Verkettungen (also Prozesse, Kommunikations- und Wertschöpfungsnetzwerke) im Verbund nutzen können. Dabei gilt es, die Durchgängigkeit von Informationsflüssen in und zwischen den Wertschöpfungsketten sicherzustellen und auf den erwähnten bestehenden Normen aufzusetzen, diese weiterzuentwickeln und erkannte Normungslücken zu schließen.

- Semantik und Syntax schaffen eine wesentliche Grundvoraussetzung für herstellerübergreifende Interoperabilität von Datenspeicherung, Datenübertragung und Datenverarbeitung
- Genormte semantische Beschreibungen legen die Basis für selbstoptimierendes Verhalten und die Automatisierung von Wertschöpfungsketten
- Dies ermöglicht die Einbindung von Modellen in den vollständigen Lebenszyklus (Da die Beschreibung von Produkt, Prozess und Ressourcen im Engineering als Semantik vorliegt)
- Mithilfe von Syntax und Semantik ist die Erstellung von generischen Werkzeugen bzw. Werkzeug-Funktionalitäten möglich
- Semantik und Syntax ermöglichen Plug-and-Produce-Funktionalitäten von Industrie 4.0-Komponenten und somit Flexibilität und Anpassbarkeit

Die Herausforderung wird sein, einerseits rasch Ergebnisse bei der Ausgestaltung von Syntax und Semantik für Industrie 4.0 zu erzielen und gleichzeitig einen größtmöglichen Anwendungsbereich (im Sinne eines Industry Footprints) zu erreichen.

5.7 Die Abhängigkeiten und Relevanz der Themen

Die verschiedenen Forschungsthemen stehen nicht für sich allein, sondern es ergeben sich Abhängigkeiten der Forschungsergebnisse untereinander. So beeinflussen neue Ergebnisse in einem Forschungsbereich die Forschung eines andern Bereiches. Die AG3 arbeitet zurzeit in Zusammenarbeit mit dem wissenschaftlichen Beirat an einer Analyse der gegenseitigen Beeinflussung und der Relevanz der Themen. Dabei werden die Methoden der Szenarioanalyse von Prof. Gausemeier angewendet. Die Ergebnisse dieser Analyse werden in Laufe des Jahres veröffentlicht, allerdings lässt sich jetzt schon feststellen, dass Forschungsergebnisse der folgenden Themen großen Einfluss auf die jeweils anderen Forschungsergebnisse haben werden:

- „Flexibilität, Intelligenz und Wandelbarkeit“
- „Sensornetzwerke“
- „Framework Wertschöpfungsnetzwerke“
- „Security & Safety“

5.6.5.3 Die wesentlichen Meilensteine

Methodik
14.8 Anwendungsleitfaden im Hinblick auf den Umgang von Syntax und Semantik bei Industrie 4.0
Lösungen
14.1 Ist-Analyse der Standardisierung/Normung im Umfeld von Syntax und Semantik 14.2 Ist-Analyse und Bewertung relevanter Konzepte im Umfeld von Syntax und Semantik 14.3 Industrie 4.0-Anforderungskatalog zu Syntax und Semantik 14.4 Benennung von Forschungsthemen auf Basis von Anwendungsfällen und –Wertschöpfungsketten 14.5 Normungslücken und Aufnahme entsprechender Standardisierungsbedarfe in Standardisierungs-/Normungsroadmaps 14.6 Realisierung von ausgewählten Interoperabilitäts-Demonstratoren 14.7 Integrationskonzepte in bestehende Kommunikationsstandards, konzeptionelle Erweiterung von Software-Werkzeugen
Voraussetzungen
14.a Anforderungen an Daten und Informationsmodelle abgeleitet aus Anwendungsfällen und Wertschöpfungsketten

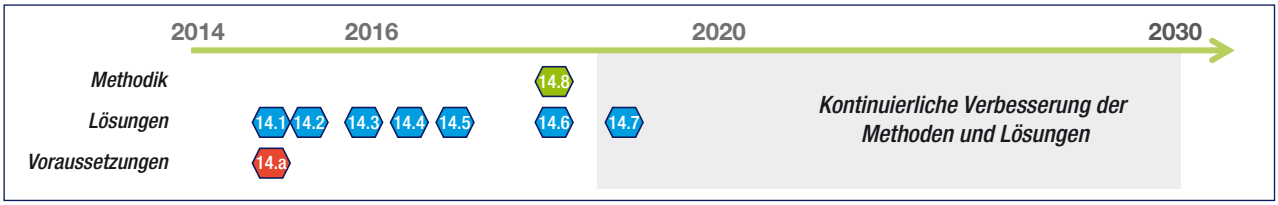


Abbildung 14: Meilensteine für die Forschung zu Syntax und Semantik für Industrie 4.0

Referenzarchitektur, Standardisierung, Normung

6 Referenzarchitektur, Standardisierung, Normung

In diesem Kapitel sind die in Kooperation mehrerer Institutionen[2] entstandenen Ergebnisse im Hinblick auf die grundlegende Referenzarchitektur für Industrie 4.0 sowie die daraus abgeleiteten Notwendigkeiten für eine Standardisierung und Normung zusammengefasst.

Damit fiel der Plattform Industrie 4.0 die Rolle der Koordination der Aktivitäten in den zahlreichen Untergremien und die Sicherstellung einer konsistenten Linie zu. So hat die Plattform ihrer zugedachten Aufgabe, ein konzertiertes Vorgehen unterschiedlichster Organisationen und Verbände sicherzustellen, entsprochen. Die nachfolgend vorgestellten breit getragenen Ergebnisse sind damit ein wichtiger Schritt zur Wahrung der Wettbewerbsfähigkeit der deutschen Industrie.

6.1 Einleitung

Einer der grundlegenden Gedanken zur Referenzarchitektur von Industrie 4.0 ist das Zusammenführen unterschiedlichster Aspekte in einem gemeinsamen Modell. Die vertikale Integration innerhalb der Fabrik beschreibt die Vernetzung von Produktionsmitteln z. B. von Automatisierungsgeräten oder Diensten untereinander. Als neuer Aspekt kommt bei Industrie 4.0 die Einbeziehung des Produktes bzw. Werkstücks hinzu. Das zugehörige Modell muss dies reflektieren. Doch Industrie 4.0 geht noch deutlich weiter. Mit durchgängigem Engineering über die ganze Wertschöpfungskette ist gemeint, dass technische, administrative und kommerzielle Daten, die rund um ein Produktionsmittel oder auch das Werkstück entstehen über die komplette Wertschöpfungskette konsistent gehalten werden und jederzeit über das Netzwerk zugreifbar sind. Ein dritter Aspekt bei Industrie 4.0 ist die horizontale Integration über Wertschöpfungsnetzwerke, die über den einzelnen Fabrikstandort hinausgeht und die dynamische Bildung von Wertschöpfungsnetzwerken ermöglicht. Die Aufgabe, diese Aspekte in einem Modell darzustellen, war zu lösen. Schließlich sollen Regelkreise mit Abtastungen im Millisekundentakt, die dynamische Kooperation mehrerer Fabriken untereinander innerhalb eines gemeinsamen Wertschöpfungsnetzwerks mit zusätzlichen kommerziellen Fragestellungen in einem Modell darstellbar sein. Hier galt es, die Sichtweisen aus den unterschiedlichen Anwendungsdomänen zu verstehen, das Wesentliche zu erfassen und in einem gemeinsamen Modell zu vereinen.

Bevor die eigentlichen Arbeiten zum Referenzarchitekturmodell RAMI4.0 begonnen werden konnten, war es daher notwendig einen Überblick über vorhandene Ansätze und Methoden zu gewinnen. Schnell wurde klar, dass es bereits eine Reihe existierender und nutzbarer Ansätze gibt, die allerdings in der Regel nur Teilaspekte der oben beschriebenen ganzheitlichen Sicht auf Industrie 4.0 adressieren. Im Einzelnen wurden folgende Ansätze näher betrachtet:

Ansatz für die Realisierung eines Communication Layers

- OPC UA: Basis IEC 62541

Ansatz für die Realisierung des Information Layers

- IEC Common Data Dictionary (IEC 61360Series/ ISO13584-42)
- Merkmale, Klassifikation und Werkzeuge nach eCl@ss
- Electronic Device Description (EDD)
- Field Device Tool (FDT)

Ansatz für die Realisierung von Functional und Information Layer

- Field Device Integration (FDI) als Integrationstechnologie

2 Die in der Gesellschaft Mess- und Automatisierungstechnik (GMA) von VDI und VDE mitarbeitenden Experten boten sich als hervorragende Partner für die Ausarbeitung der Ansätze an. Hier sind inbesondere die Fachausschüsse 7.21 „Industrie 4.0“ und 7.20 „Cyber-Physical Systems“ zu nennen.
Parallel wurde im ZVEI das Spiegelgremium SG2 gegründet, welches sich ebenfalls inhaltlich in den Verbund eingebracht hat. Durch entsprechende Vertreter in der SG2 wurde zudem noch die DKE (Deutsche Kommission Elektrotechnik) einbezogen, so dass auch die Normung Teil des Verbundes wurde.

Ansatz für das durchgängige Engineering

- AutomationML
- ProSTEP iViP
- eCl@ss (Merkmale)

Im ersten Schritt ging es dabei um die grundsätzliche Prüfung, ob diese Ansätze zum im folgenden Kapitel vorgestellten Referenzarchitekturmodell passen. Dies wird grundsätzlich bejaht, allerdings bedürfen die betrachteten Konzepte und Methoden noch detaillierteren Betrachtungen.

6.2 Das Referenzarchitekturmodell Industrie 4.0 (RAMI4.0)

In der Diskussion über Industrie 4.0 kommen ganz unterschiedliche Interessen zusammen. Branchen von Prozess- bis Fabrikautomation mit unterschiedlichsten Standards, die Technologien der Informations- und Kommunikationstechnik und die Automatisierungstechnik, die Verbände BITKOM, VDMA, ZVEI und VDI sowie die Normungsorganisationen IEC und ISO mit ihren nationalen Spiegelgremien DKE und DIN.

Zum Zweck eines gemeinsamen Verständnisses, welche Standards, Use Cases, Normen, etc. für Industrie 4.0 notwendig sind, entstand die Notwendigkeit ein einheitliches Architekturmodell als Referenz zu entwickeln, anhand dessen Zusammenhänge und Details diskutiert werden können.

Das Ergebnis ist das Referenzarchitekturmodell Industrie 4.0 (RAMI4.0).

Es beinhaltet die wesentlichen Aspekte aus Industrie 4.0. Es ergänzt die Hierarchiestufen aus IEC 62264 am unteren Ende um die Stufe des Produkts bzw. Werkstücks („Product“) und am oberen Ende über die einzelne Fabrik hinaus um die „Connected World“. Die waagrechte Achse dient der Darstellung des Lebenszyklus von Anlagen bzw. Produkten, wobei auch der Aspekt der Unterscheidung zwischen Typ und Instanz abgebildet wird. Über die sechs Layer wird schlussendlich die IT-Repräsentanz einer Industrie 4.0-Komponente strukturiert beschrieben.

Somit sind die besonderen Charakteristika des Referenzarchitekturmodells die Kombination von Lebenszyklus und Wertschöpfungskette mit einem hierarchisch strukturierten Ansatz für die Definition von Industrie 4.0-Komponenten. Damit ist ein Höchstmaß an Flexibilität zur Beschreibung einer Industrie 4.0-Umgebung gegeben. Der Ansatz erlaubt auch die sinnvolle Kapselung von Funktionalitäten.

Somit sind die Voraussetzungen geschaffen mittels des Referenzarchitekturmodells hoch flexible Konzepte zu beschreiben und zu realisieren. Dabei erlaubt das Modell die schrittweise Migration aus der heutigen in die Industrie 4.0-Welt und die Definition von Anwendungsdomänen mit speziellen Vorgaben und Anforderungen.

Das Referenzarchitekturmodell RAMI4.0 wird als DIN SPEC 91345 der Normung zugeführt.

6.2.1 Anforderungen und Ziele

Ziele

Industrie 4.0 ist eine Spezialisierung des „Internet of Things and Services“. Es sind ca. 15 Branchen in die Überlegungen einzubeziehen. Mit dem Referenzarchitekturmodell können Aufgaben und Abläufe in überschaubare Teile zerlegt werden. Es soll einen Sachverhalt so anschaulich machen, dass eine zielgerichtete Diskussion z. B. bzgl. Standardisierung und Normung möglich wird. Es sollen also auch die in Frage kommenden vorhandenen Standards und Normen verortet werden können, damit sichtbar wird, wo eventuell noch Erweiterungs-/Modifizierungsbedarf besteht, bzw. Normen und Standards fehlen. Überschneidungen werden dabei ebenfalls sichtbar und können diskutiert werden. Existieren für denselben oder ähnlichen Sachverhalt aus der Modellbetrachtung heraus mehrere Standards, kann ein Vorzugsstandard im Referenzarchitekturmodell diskutiert werden.

Ziel ist mit möglichst wenigen Standards auszukommen.

Erfüllung von Standards

Die ausgewählten Normen und Standards werden daraufhin geprüft, in wieweit deren beschriebene Komzepte und Methoden für die Anwendungen im Umfeld von Industrie 4.0 geeignet sind. Für eine erste Industrie 4.0-Anwendung kann die Umsetzung einer Teilmenge einer Norm / eines Standards genügen. Dies würde die Umsetzung und Einführung von herstellerübergreifenden Lösungen, wie sie für Indus-

trie 4.0 unerlässlich sind, beschleunigen und auch kleineren Unternehmen die Chance eröffnen, die Umsetzung und Anpassung an Industrie 4.0 schneller zu bewältigen.

Use Cases

Das Referenzarchitekturmodell bietet auch die Möglichkeit, Industrie 4.0-Use Cases zu verorten, um z. B. die für den jeweiligen Use Case notwendigen Normen und Standards zu identifizieren.

Verortung von Beziehungen

Verschiedene Themen können als Unterräume des Referenzarchitekturmodells dargestellt werden. Industrie 4.0 lebt wesentlich davon, dass Beziehungen z. B. zwischen diesen Unterräumen elektronisch erfasst und bearbeitet werden können.

Definition übergeordneter Regeln

Das Referenzarchitekturmodell erlaubt die Ableitung von Regeln für die Umsetzung von Industrie 4.0-Implementierungen auf einer übergeordneten Ebene.

Die Ziele im Überblick:

- Anschauliches und einfaches Architekturmodell als die Referenz
- Verortung von vorhandenen Normen und Standards
- Identifikation und Schließen von Lücken in Normen und Standards
- Identifikation von Überschneidungen und Festlegung von Vorzugslösungen
- Minimierung der Zahl der eingesetzten Normen und Standards
- Identifikation von Untermengen einer Norm bzw. eines Standards zur schnellen Umsetzung von Teilinhalten für Industrie 4.0 („I4.0-Ready“)
- Verortung von Use Case-Inhalten
- Verortung von Beziehungen
- Definition übergeordneter Regeln

6.2.2 Kurzbeschreibung des Referenzarchitekturmodells

Ein dreidimensionales Modell kann den Industrie 4.0-Raum am besten darstellen. Dabei orientiert sich das Modell in seinen Grundzügen am Smart Grid Architecture Model (SGAM[3]), das von der europäischen Smart Grid Coordination Group (SG-CG) definiert wurde und weltweit akzeptiert ist. Es wurde anhand der Industrie 4.0-Erfordernisse angepasst und erweitert.

In der senkrechten Achse werden Layer/Schichten für die Darstellung der unterschiedlichen Sichtweisen, wie z. B. Datenabbild, funktionale Beschreibung, Kommunikationsverhalten, Hardware/Assets oder auch Geschäftsprozesse verwendet. Dies entspricht der Denkweise der IT bei der Clusterung komplexer Projekte in überschaubare Teileinheiten.

Ein weiteres wichtiges Kriterium ist der Produktlebenszyklus mit seinen darin enthaltenen Wertschöpfungsketten. Dieser Sachverhalt wird auf der waagrechten Achse dargestellt. Damit können in dem Referenzarchitekturmodell auch Abhängigkeiten gut dargestellt werden, z. B. die durchgängige Datenerfassung über den gesamten Lebenszyklus.

Das dritte wichtige Kriterium, in der dritten Achse dargestellt, ist die Verortung von Funktionalitäten und Verantwortlichkeiten innerhalb der Fabriken/Anlagen. Es geht um eine funktionale Hierarchie und nicht um Geräteklassen oder Hierarchieebenen der klassischen Automatisierungspyramide.

3 CEN/CENELEC/ETSI SG-CG, Overview of SG-CG Methodologies, Version 3.0, Annex SGAM User Manual, 2014

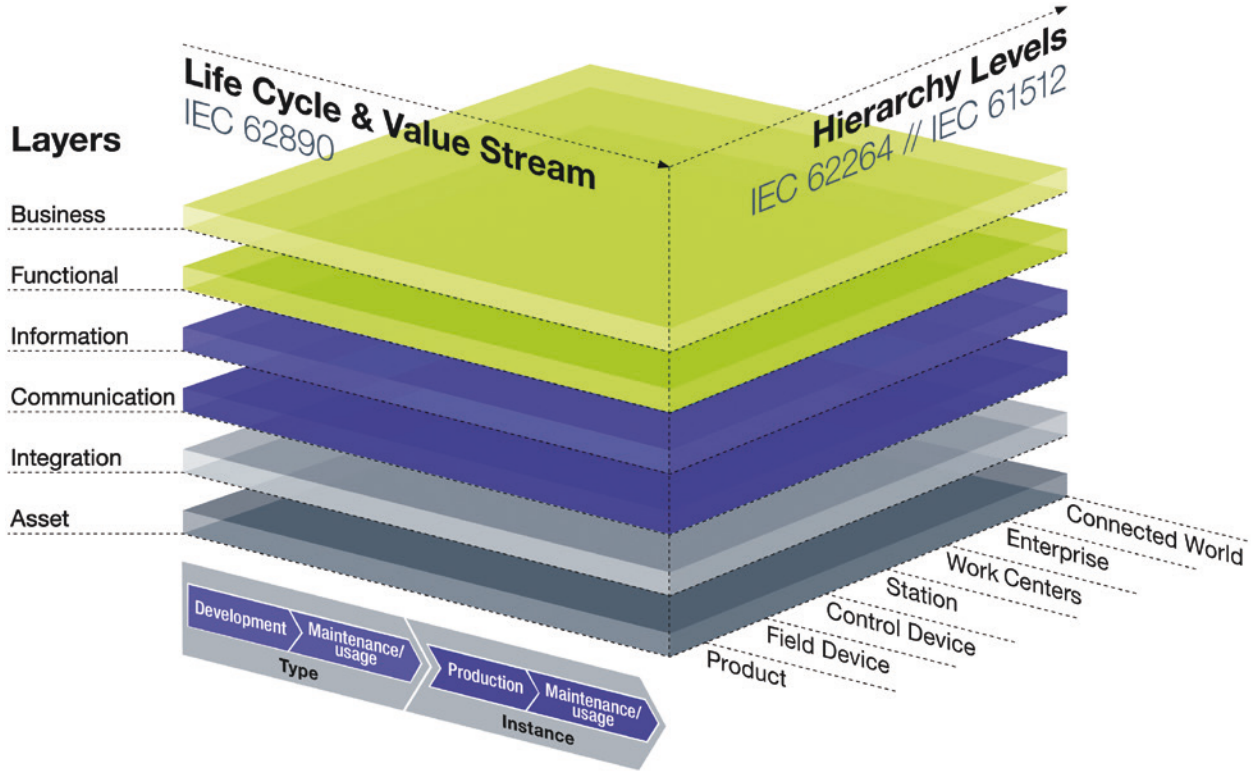


Abbildung 15: Referenzarchitekturmodell / Reference Architecture Model Industrie 4.0 (RAMI 4.0)

6.2.3 Die Schichten des Referenzarchitekturmodells (Layers)

Das Smart Grid Modell (SGAM) stellt einen guten ersten Ansatz zur Darstellung der zu beschreibenden Sachlage dar. Es behandelt das Stromnetz von der Erzeugung über die Übertragung und Verteilung bis zum Verbraucher. Bei Industrie 4.0 stehen Produktentwicklungs- und Produktionsszenarien im Mittelpunkt. D.h., es muss beschrieben werden, wie Entwicklungsprozesse, Produktionslinien, Fertigungsmaschinen, Feldgeräte und die Produkte selbst beschaffen sind bzw. funktionieren.

Für alle Komponenten, ob Maschine oder Produkt, ist nicht nur die informations- und kommunikationstechnische Funktionalität von Interesse. Für die Simulation eines Systems z. B. einer kompletten Maschine werden auch deren Kabel, der Linearantrieb oder auch die mechanische Konstruktion mit betrachtet. Sie sind Teil der Realität ohne aktiv kommunizieren zu können. Ihre Informationen müssen als virtuelle Repräsentation vorhanden sein. Dafür werden sie z. B. passiv über einen 2D-Code mit einem Datenbankeintrag verbunden.

Um sowohl Maschinen, Komponenten und Fabriken besser beschreiben zu können wurde gegenüber SGAM dessen Component Layer durch einen Asset Layer ersetzt, als untere Schicht in das Modell eingefügt und darüber der Integration Layer neu hinzugefügt. Dieser ermöglicht die digitale Umsetzung der Assets für die virtuelle Repräsentation. Der Communication Layer behandelt Protokolle und Übertragung von Daten und Dateien, der Information Layer beinhaltet die relevanten Daten, der Functional Layer alle notwendigen (formal beschriebenen) Funktionen und im Business Layer ist der relevante Geschäftsprozess abgebildet.

Hinweis: *Innerhalb der Schichten soll eine hohe Kohäsion und zwischen den Schichten eine lose Kopplung herrschen. Der Ereignisaustausch darf nur zwischen zwei benachbarten Schichten und innerhalb einer Schicht erfolgen.*

Mehrere Systeme werden zu größeren Gesamtsystemen zusammengefasst. Dabei müssen die Einzelsysteme und das Gesamtsystem dem Referenzarchitekturmodell folgen. Die Inhalte der Schichten müssen zueinander kompatibel sein.

Nachfolgend werden die einzelnen Schichten und ihre Beziehung untereinander beschrieben:

6.2.3.1 Geschäftssicht (Business Layer)

- Sicherstellung der Integrität der Funktionen in der Wertschöpfungskette
- Abbildung der Geschäftsmodelle und dem sich daraus ergebenden Gesamtprozess
- Rechtliche und regulatorische Rahmenbedingungen
- Modellierung der Regeln, denen das System folgen muss
- Orchestrierung von Diensten des Functional Layers
- Verbindungselement zwischen verschiedenen Geschäftsprozessen
- Empfang von Ereignissen für die Weiterschaltung des Geschäftsprozesses

Der Business Layer bezieht sich nicht auf konkrete Systeme wie beispielsweise ein ERP. ERP-Funktionen, die im Prozesskontext arbeiten, finden sich typischerweise im Functional Layer wieder.

6.2.3.2 Funktionsschicht (Functional Layer)

- Formale Beschreibung von Funktionen
- Plattform für die horizontale Integration der verschiedenen Funktionen
- Laufzeit- und Modellierungsumgebung für Dienste, die Geschäftsprozesse unterstützen
- Laufzeitumgebung für Anwendungen und fachliche Funktionalität

Innerhalb des Functional Layer werden Regeln/Entscheidungslogiken erzeugt. Diese können auch abhängig vom Anwendungsfall in den unteren Schichten (Information- oder Integration Layer) ausgeführt werden.

Fernzugriffe und horizontale Integration finden nur innerhalb des Functional Layer statt. Damit werden die Integrität der Informationen und Zustände im Prozess und die Integration der technischen Ebene sichergestellt. Zu Wartungszwecken können auch temporäre Zugriffe auf Asset Layer und Integration Layer stattfinden.

Solche Zugriffe werden insbesondere verwendet, um auf Informationen und Prozesse, welche nur für untergeordnete Schichten relevant sind, zuzugreifen. Beispiele hierfür sind das Flashen von Sensoren/Aktoren oder das Auslesen von Diagnosedaten. Die wartungsbezogenen temporären Fernzugriffe sind für eine permanente funktionale oder horizontale Integration nicht relevant.

6.2.3.3 Informationsschicht (Information Layer)

- Laufzeitumgebung für die Ereignis(vor-)verarbeitung
- Ausführung von ereignisbezogenen Regeln
- Formale Beschreibung von Regeln
- Kontext: Ereignisvorverarbeitung

Dabei werden aus einem oder mehreren Ereignissen über Regeln ein oder mehrere weitere Ereignisse erzeugt, die dann im Functional Layer die Verarbeitung anstoßen.

- Persistieren der Daten, welche die Modelle repräsentieren
- Sicherstellung der Datenintegrität
- Konsistente Integration verschiedener Daten
- Gewinnung von neuen, höherwertigen Daten (Daten, Informationen, Wissen)
- Bereitstellung strukturierter Daten über Dienstschnittstellen
- Entgegennahme von Ereignissen und deren Transformation passend zu den Daten, die für den Functional Layer verfügbar sind

6.2.3.4 Kommunikationsschicht (Communication Layer)

- Vereinheitlichung der Kommunikation unter Verwendung eines einheitlichen Datenformats in Richtung des Information Layer
- Bereitstellung von Diensten zur Steuerung des Integration Layer

6.2.3.5 Integrationsschicht (Integration Layer)

- Bereitstellung der rechnerverarbeitbaren Informationen der Assets Physik/ Hardware/ Dokumente/ Software etc.
- Rechnergestützte Steuerung des technischen Prozesses
- Generierung von Ereignissen aus den Assets
- Enthält die mit der IT verbundenen Elemente, wie z. B. RFID Reader, Sensoren, HMI, etc.

Die Interaktion mit dem Menschen erfolgt ebenfalls in dieser Ebene, z. B. mittels der Mensch-Maschine Schnittstelle (HMI).

Hinweis: Jedes wichtige Ereignis in der Realität weist auf ein Ereignis in der Virtualität, d.h. im Integration Layer, hin. Ändert sich die Realität, wird das Ereignis mit geeigneten Mechanismen an den Integration Layer gemeldet. Relevante Ereignisse können Ereignisse über den Communication Layer an den Information Layer auslösen.

6.2.3.6 Gegenstandsschicht (Asset Layer)

- Repräsentiert die Realität, z. B. physikalische Elemente wie Linearachsen, Blechteile, Dokumente, Schaltpläne, Ideen, Archive etc.
- Der Mensch ist ebenfalls Bestandteil des Asset Layers und ist über den Integration Layer an die virtuelle Welt angebunden.
- Passive Verbindung der Assets mit der Integrationsschicht über z. B. QR-Codes

6.2.4 Lebenszyklus und Wertschöpfungskette (Life Cycle & Value Stream)

Lebenszyklus (Life Cycle):

Industrie 4.0 bietet über den gesamten Lebenszyklus von Produkten, Maschinen, Fabriken, etc. großes Verbesserungspotenzial. Um Zusammenhänge und Verknüpfungen zu visualisieren und zu standardisieren, repräsentiert die zweite Achse des Referenzarchitekturmodells den Lebenszyklus und die damit verbundenen Wertschöpfungsketten.

Für die Betrachtung des Lebenszyklus bietet der Entwurf zur IEC 62890 eine gute Orientierung. Dabei ist die grundsätzliche Unterscheidung von Typ und Instanz ein zentraler Teil für die Betrachtungen.

Typ (Type):

Ein Typ entsteht immer mit der ersten Idee, also der Entstehung des Produkts in der Phase „Development“. Damit sind die Beauftragung, die Entwicklung, die Tests bis hin zum ersten Muster und der Prototypenfertigung gemeint. In dieser Phase entsteht also der Typ des Produktes, der Maschine, etc. Nach Abschluss aller Tests und Validierung wird der Typ für die Serienproduktion freigegeben.

Instanz (Instance):

Auf Basis des allgemeinen Typs werden in der Produktion Produkte hergestellt. Jedes gefertigte Produkt stellt dann eine Instanz dieses Typs dar und erhält z. B. eine eindeutige Seriennummer. Die Instanzen gelangen in den Verkauf und werden an Kunden ausgeliefert. Für den Kunden sind die Produkte zunächst wieder nur Typen. Zur Instanz werden sie, wenn sie in eine konkrete Anlage eingebaut werden. Der Wechsel vom Typ zur Instanz kann sich mehrmals wiederholen.

Aus der Verkaufsphase zurückgemeldete Verbesserungen können beim Hersteller eines Produkts zur Anpassung der Typunterlagen führen. Mit dem neu entstandenen Typ können wieder neue Instanzen hergestellt werden. Der Typ unterliegt damit einer Nutzung und Pflege genauso wie jede einzelne Instanz.

Beispiel:
Die Entwicklung eines neuen Hydraulikventils stellt einen neuen Typ dar. Das Ventil wird entwickelt, erste Muster werden aufgebaut und getestet und zum Abschluss wird eine erste Prototypen-Serie in der Produktion aufgelegt und anschließend validiert. Nach erfolgreichem Abschluss der Validierung erfolgt die Freigabe dieses Hydraulikventiltyps für den Verkauf (Materialnummer und/oder Produktbezeichnung im Verkaufskatalog). Damit startet auch die Serienproduktion.
In der Serienproduktion erhält nun jedes hergestellte Hydraulikventil z. B. seine eineindeutige Kennzeichnung (Seriennummer) und ist eine Instanz zu dem einmal entwickelten Hydraulikventil.
Rückmeldungen zu den verkauften Hydraulikventilen (Instanzen) im Feld führen z. B. zu einer kleinen Anpassung der mechanischen Konstruktion und Zeichnungsunterlage sowie zu einer Softwarekorrektur in der Firmware des Ventils. Diese Anpassungen sind Anpassungen am Typ, d.h. sie fließen in die Typunterlagen ein, werden wieder frei gegeben und somit entstehen neue Instanzen des geänderten Typs in der Produktion.

Wertschöpfungsketten:

Die Digitalisierung und Verknüpfung der Wertschöpfungsketten bieten ein hohes Verbesserungspotential durch Industrie 4.0. Dabei ist eine funktional übergreifende Verknüpfung von entscheidender Bedeutung.

Logistikdaten können in der Montage verwendet werden, die Intralogistik organisiert sich selbst anhand der Auftragsbestände. Der Einkauf sieht in Realtime Bestände und wo sich Zulieferteile zu einem bestimmten Zeitpunkt befinden. Der Kunde sieht den Fertigstellungsgrad seines bestellten Produkts in der Fertigung usw. Mit der Verknüpfung von Einkauf, Auftragsplanung, Montage, Logistik, Maintenance, Kunde, Zulieferer etc. bestehen große Verbesserungspotenziale. Daher muss der Lebenszyklus mit den enthaltenen Wertschöpfungsprozessen zusammen betrachtet werden; dies nicht isoliert mit Blick auf eine Fabrik, sondern im Verbund aller Fabriken und aller Partner vom Engineering über Zulieferer bis hin zum Kunden.

Zu den Wertschöpfungsketten sei auch auf die Veröffentlichung des VDI/VDE GMA FA7.21 „Wertschöpfungsketten“ [1] verwiesen.

6.2.5 Hierarchieebenen (Hierarchy Levels)

Die dritte Achse des Referenzarchitekturmodells beschreibt die funktionale Einordnung einer Sachlage innerhalb Industrie 4.0. Dabei geht es nicht um eine Implementierung, es geht allein um funktionale Zuordnungen.

Für die Einordnung innerhalb einer Fabrik orientiert sich das Referenzarchitekturmodell für diese Achse an den Normen IEC 62264 und IEC 61512 (siehe Abbildung). Für eine einheitliche Betrachtung über möglichst viele Branchen von Prozessindustrie bis Fabrikautomation wurden aus den dort aufgeführten Optionen die Begriffe „Enterprise“, „Work Center“, „Station“ und „Control Device“ verwendet.

Für Industrie 4.0 ist neben dem Control Device (z. B. einer Kopfsteuerung) auch die Betrachtung innerhalb einer Maschine oder Anlage entscheidend. Daher wurde unterhalb des Control Device das „Field Device“ hinzugefügt. Dies stellt die funktionale Ebene eines intelligenten Feldgeräts z. B. eines intelligenten Sensors dar.

Ausserdem ist neben der Anlage zur Herstellung von Produkten in Industrie 4.0 auch das herzustellende Produkt selbst für die Betrachtungen wichtig. Daher ist es als untere Ebene zusätzlich als „Product“ eingeführt. Damit wird im Referenzarchitekturmodell eine homogene Betrachtung von herzustellendem Produkt und Produktionsanlage mit deren Abhängigkeiten untereinander möglich.

Am oberen Ende der Hierarchy Levels wurde ebenfalls eine Ergänzung vorgenommen. Die beiden erwähnten IEC Normen stellen nämlich nur die Ebenen innerhalb einer Fabrik dar. Industrie 4.0 geht aber einen Schritt weiter und beschreibt auch den Fabrikverbund, die Zusammenarbeit mit externen Engineeringbüros, Zulieferern und Kunden usw. Daher wurde für die Betrachtungen über den Enterprise Level hinaus noch zusätzlich die Ebene „Connected World“ eingeführt.

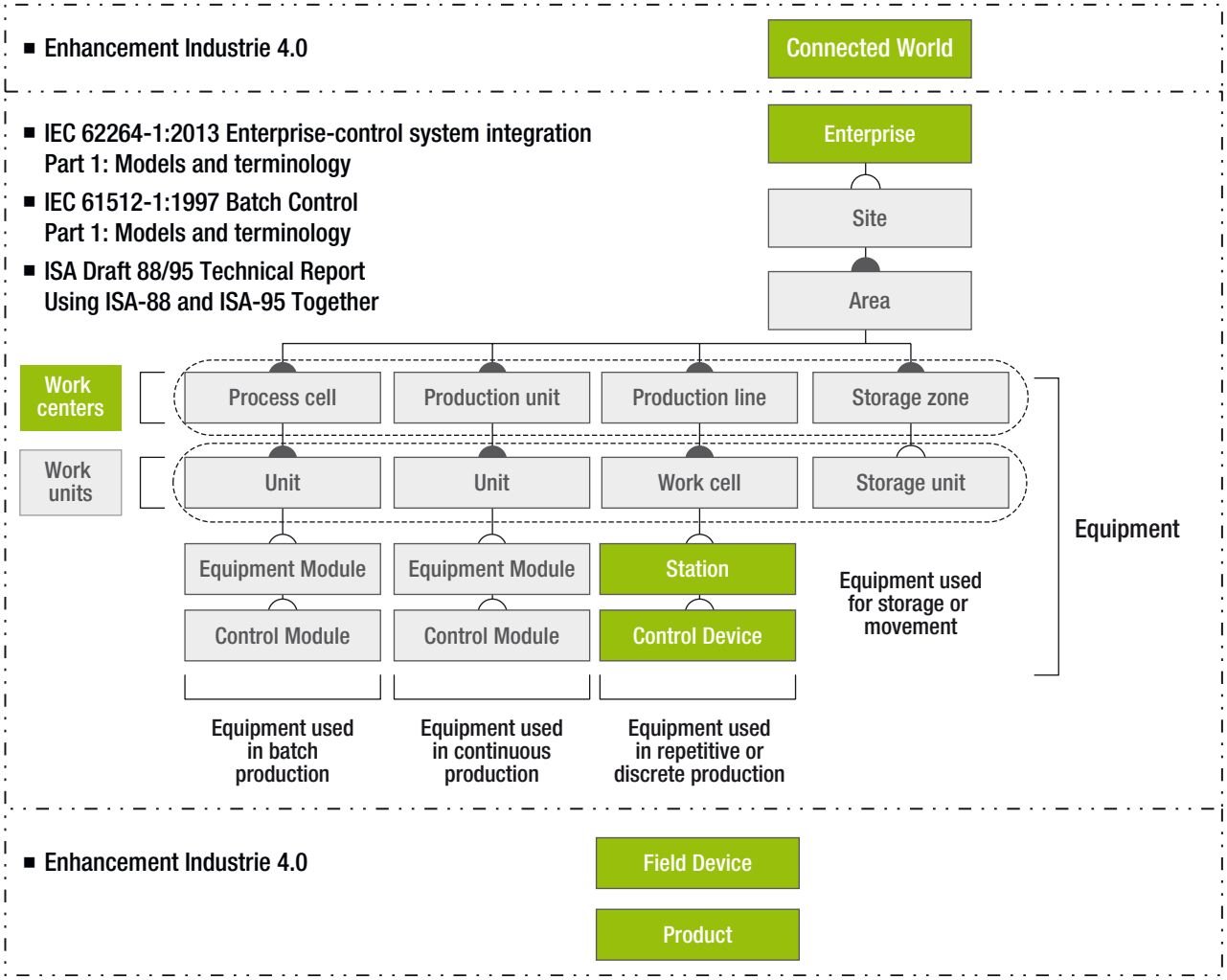


Abbildung 16: Ableitung der Hierachieebenen des Referenzarchitekturmodells RAMI 4.0

6.3 Referenzmodell für die Industrie 4.0-Komponente

Die nachfolgend beschriebene Version 1.0 des Referenzmodell Industrie 4.0-Komponente soll die erste von mehreren Verfeinerungen sein, die in unterjährigen Zeitabständen veröffentlich werden sollen. In einem weiteren Schritt sollen daher Kapitel mit genaueren Definitionen folgen, eine Formalisierung mit UML ist vorgesehen.

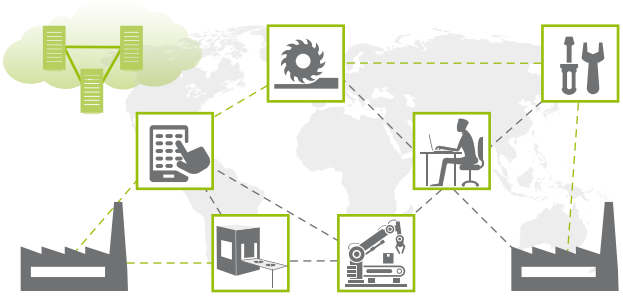
Der Text bemüht sich, genau auszuweisen, wenn Texte/Zitate aus anderen Quellen im Industrie 4.0-Umfeld übernommen werden (z. B. VDI/VDE GMA 7.21). Im Endstand sollen die Begriffsverwendungen identisch mit denen der GMA 7.21 sein. Beispiele werden ebenfalls explizit gekennzeichnet, um Ausschlüsse, die im Beispiel nicht explizit genannt werden, zu vermeiden.

6.3.1 Einordnung in die Diskussion zu Industrie 4.0

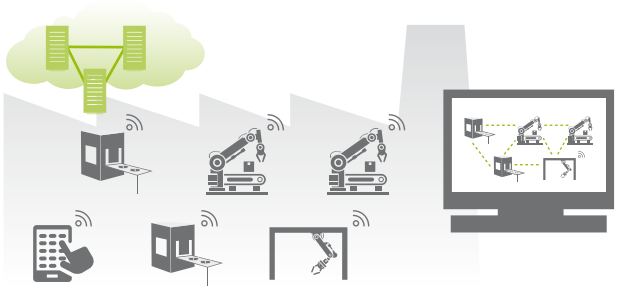
Die Diskussion Industrie 4.0 lässt sich grob als Zusammenspiel von vier Aspekten auffassen, wie die folgende Abbildung aus [3] illustriert:

4 Quelle: IEC 61512, IEC 62264, ISA Draft 88/95 Technical Report, Plattform Industrie 4.0

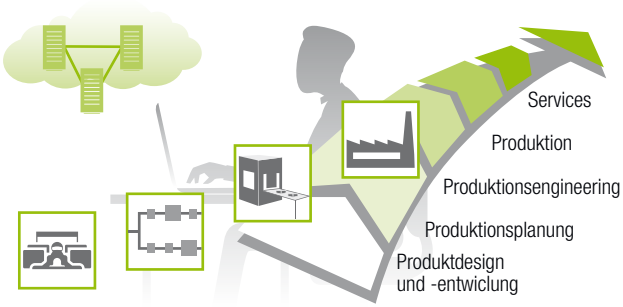
Horizontale Integration über Wertschöpfungsnetzwerke



Vertikale (Integration und vernetzte Produktionssysteme)



Digitale Durchgängigkeit des Engineerings über die gesamte Wertschöpfungskette



Mensch als Dirigent der Wertschöpfung

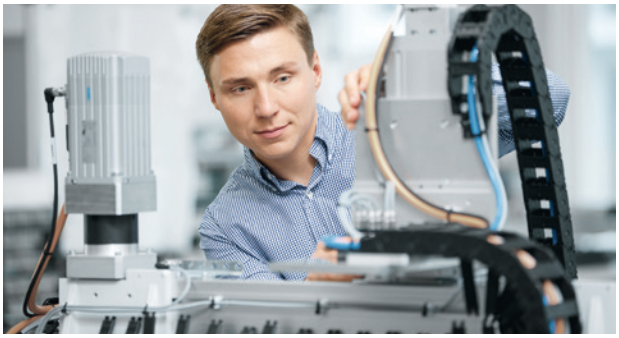


Abbildung 17: Vier wichtige Aspekte von Industrie 4.0[5]

Nach obigen Bildern sind diese vier Aspekte:

- Industrie 4.0-Aspekt (1)
  Horizontale Integration über Wertschöpfungsnetzwerke
- Industrie 4.0-Aspekt (2)
  Vertikale Integration, z. B. innerhalb einer Fabrik/ Fertigung
- Industrie 4.0-Aspekt (3)
  Lebenszyklus-Management, Durchgängigkeit des Engineering
- Industrie 4.0-Aspekt (4)
  Der Mensch als Dirigent im Wertschöpfungsnetzwerk[6]

Die in diesem Text beschriebene Industrie 4.0-Komponente gibt einen flexiblen Rahmen vor, mit welchem Daten und Funktionen beschrieben und bereitgestellt werden können, welche die oben angeführten Industrie 4.0-Aspekte fördern und möglich machen. Die in diesem Text beschriebenen Konzepte bedienen zum jetzigen Zeitpunkt vor allem Aspekt (2) und berücksichtigen Anforderungen aus Aspekt (3).

6.3.2 Relevante Materialien aus anderen Arbeitskreisen

VDI/VDE GMA 7.21: Industrie 4.0: Gegenstände, Entitäten, Komponenten

Für die Definitionen aus dem VDI/ VDA GMA 7.21 sei auf die vorausgegangenen Kapitel verwiesen.

Typen und Instanzen

Es wird kurz auf den Stand der Technik bezüglich der Typ/ Instanz-Unterscheidung in Industrie 4.0 eingegangen.

5 angelehnt an [3], Bild unten rechts Quelle: Festo

6 nach Prof. Bauernhansl

Lebenszyklen

Nach Fraunhofer IPA, Prof. Constantinescu und Prof. Bauernhansl sind für den Betrieb einer Fabrik Lebenszyklen mehrerer Dimensionen von Relevanz für Industrie 4.0.

- **Produkt:** Eine Fabrik produziert mehrere Produkte. Jedes Produkt hat einen eigenen Lebenszyklus.
- **Auftrag:** Jeder Auftrag, der gefertigt werden soll, durchläuft einen Lebenszyklus und muss seine Spezifitäten während der Auftragsausführung in den Produktionsbetrieb abprägen können.
- **Fabrik:** Auch eine Fabrik hat einen Lebenszyklus: Sie wird finanziert, geplant, aufgebaut und wiederverwertet.
  Eine Fabrik integriert Produktionssysteme und Maschinen verschiedener Hersteller
- **Maschine:** Eine Maschine wird in Auftrag gegeben, konstruiert, in Betrieb genommen, betrieben, gewartet, umgebaut und verwertet.
  Der Maschinenhersteller bezieht dazu einzelne Zulieferteile, die in diesem Text als Gegenstände bezeichnet werden. Der Zulieferer (in der Regel ein Komponentenhersteller) realisiert einen Lebenszyklus auch für diese Zulieferteile.
- **Komponente:** Planung und Entwicklung, Rapid Prototyping, Konstruktion, Produktion, Nutzung bis hin zum Service

Die Abbildung 18 verdeutlicht dies.

Verbindung von Lebenszyklen

Ursächlich für die notwendige Unterscheidung von Typen und Instanzen sind das Zusammenwirken verschiedener Geschäftspartner und deren jeweiliger Lebenszyklen mit den Planungsprozessen. Während einer Planung werden verschiedene Hypothesen und Alternativen erwogen. Die Planung geht von potenziellen Gegenständen aus und nennt diese „Typen“:

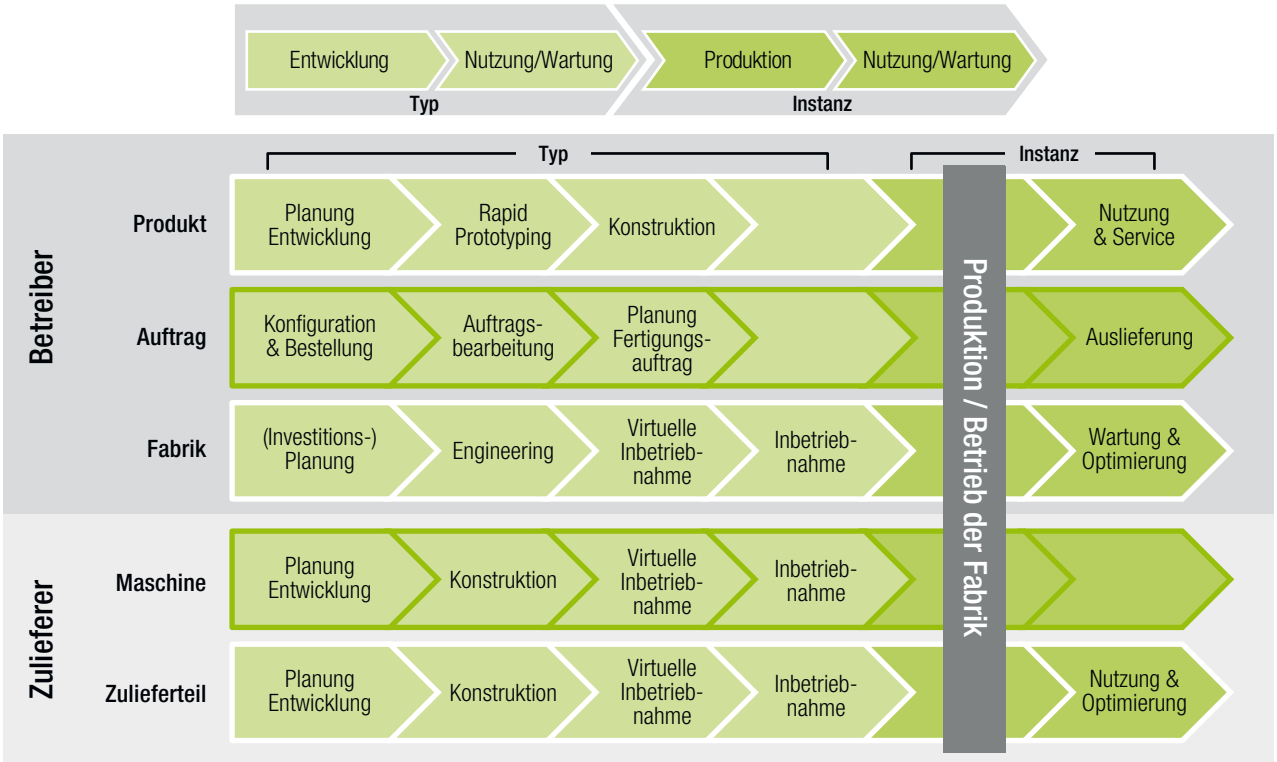


Abbildung 18: Relevante Lebenszylen für Industrie 4.0-Komponenten[7]

7 Quelle: Martin Hankel, Bosch Rexroth; Prof. Thomas Bauernhansl, Fraunhofer IPA; Johannes Diemer, Hewlett-Packard

- **Der Zulieferer** nennt diese „Teiletypen“: Erst die Fertigung und die anschließende Auslieferung an den Kunden (Maschinenhersteller) „erschafft“ eine Instanz, die dieser als Zulieferteil weiterverwendet.
- **Der Maschinenhersteller** bespricht mit seinen Kunden und plant „Maschinentypen“: Die Konstruktion einer speziellen Maschine und deren Realisierung erschafft eine Instanz, welche der Fabrikbetreiber weiterverwendet.
- **Der Fabrikbetreiber** entwickelt ein Produkt, ebenfalls zunächst als Produkttyp. Erst der Auftrag stößt die Fertigung an und realisiert die Fertigung konkreter Produkt-Instanzen, welche ausgeliefert werden.

Bemerkenswert ist nun, dass während der Konzeption und Planung eines jeweiligen Typs viele Informationen und Daten generiert werden, welche bei der Verwendung der jeweiligen Instanz durch den nachfolgenden Geschäftspartner im Wertschöpfungsnetzwerk genutzt werden können. Weitere Informationen kommen während der Produktion einer bestimmten Instanz hinzu (z. B. Tracking-Daten und Qualitätsdaten). Das Referenzmodell für Industrie 4.0-Komponenten behandelt daher Typen und Instanzen gleichwertig und gleichartig.

Referenzarchitekturmodell Industrie 4.0 (RAMI4.0)

Für die Definitionen des „Referenzarchitekturmodell Industrie 4.0 (RAMI4.0)“ sei auf die vorausgegangenen Kapitel verwiesen. Die hier vorgestellte „Industrie 4.0-Komponente“ ordnet sich in die Schichten des RAMI4.0 ein. Sie kann verschiedene Positionen des Life-Cycle und Value-Streams genauso wie verschiedene Hierarchieebenen abbilden; hier bedarf es der konkreten Instantiierung zur eindeutigen Festlegung.

6.3.3 Die “Industrie 4.0-Komponente“

6.3.3.1 In diesem Kapitel wird eine erste allgemein anerkannte Definition einer Industrie 4.0-Komponente hergeleitet. Abgrenzung der Industrie 4.0-Komponente zwischen „Office floor“ und „Shop floor“

Um eine Abgrenzung der Verantwortlichkeiten vornehmen zu können, wird in Unternehmen gewöhnlich zwischen „Office Floor“ und „Shop Floor“ unterschieden. In modernen Unternehmen sind allerdings diese Bereiche zunehmend miteinander verzahnt. Wird ein Augenmerk auf die Automatisierungstechnik gelegt, so nimmt die Relevanz des „Office-Floor“ ab, während immer mehr Anforderungen

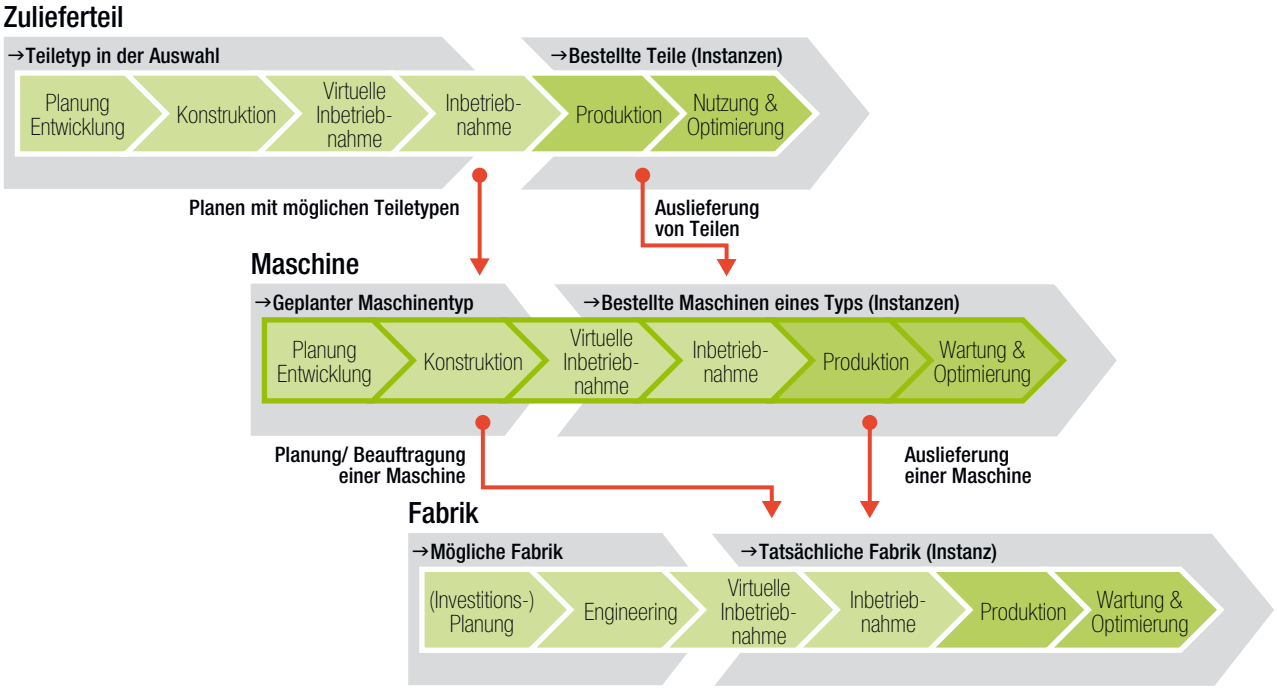


Abbildung 19: Typen und Instanzen im Lebenszyklus

des „Shop-Floor“ relevant werden. Gleiches gilt auch in anderer Richtung. Aufgrund der Forderung in der folgenden Abbildung nach Konnektivität zu beliebigen Endpunkten und einem gemeinsamen semantischen Modell, müssen Komponenten bestimmte gemeinsame Eigenschaften unabhängig von den Ebenen aufweisen. Sie sind in Form der Industrie 4.0-Komponente spezifiziert.

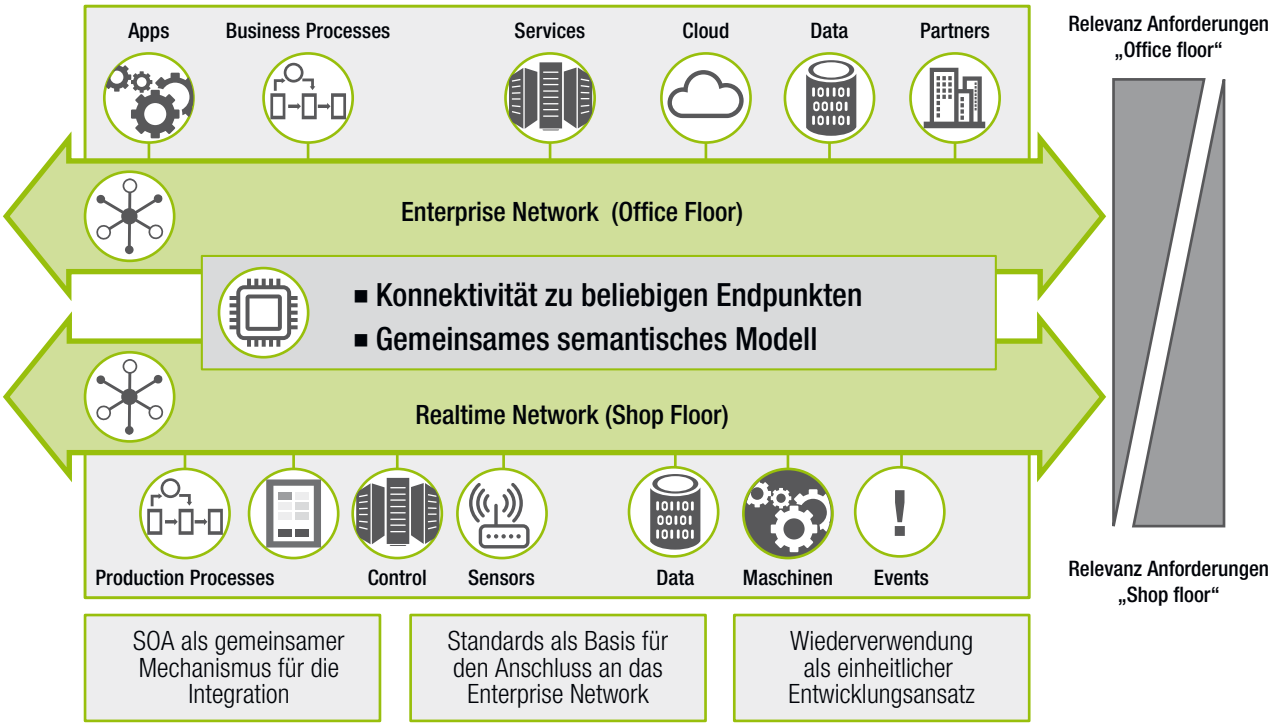


Abbildung 20: Abgrenzung „Office Floor“ und „Shop Floor“

Eine Industrie 4.0-Komponente kann ein Produktionssystem, eine einzelne Maschine oder Station oder auch eine Baugruppe innerhalb einer Maschine repräsentieren. Damit bewegt sich jede Industrie 4.0-Komponente, so verschieden sie sein mag, im Spannungsfeld der Relevanzen „Office-floor“ und „Shop-floor“, entlang des Lebenszyklus der Fabrik und in Kontakt mit so zentralen und signifikanten Fabrik-Systemen wie dem PLM (Product Lifecycle Management), ERP (Enterprise Ressource Planning), Industrial Control und Logistik-Systemen.

Anforderung:
Ein Netzwerk von Industrie 4.0-Komponente muss so aufgebaut sein, dass Verbindungen zwischen beliebigen Endpunkten (Industrie 4.0-Komponenten) möglich sind. Die Industrie 4.0-Komponenten und deren Inhalte sollen einem gemeinsamen semantischen Modell folgen.

Anforderung:
Das Konzept einer Industrie 4.0-Komponente muss so ausdifferenziert werden können, dass es verschiedenen Anforderungsschwerpunkten, also „Office-floor“ oder „Shop-floor“, gerecht werden kann.

6.3.3.2 Vom Gegenstand zur Industrie 4.0-Komponente

Im folgenden Abschnitt sollen die einzelnen Festlegungen der GMA miteinander in Bezug gesetzt werden, um zu einer Definition einer Industrie 4.0-Komponente zu gelangen:

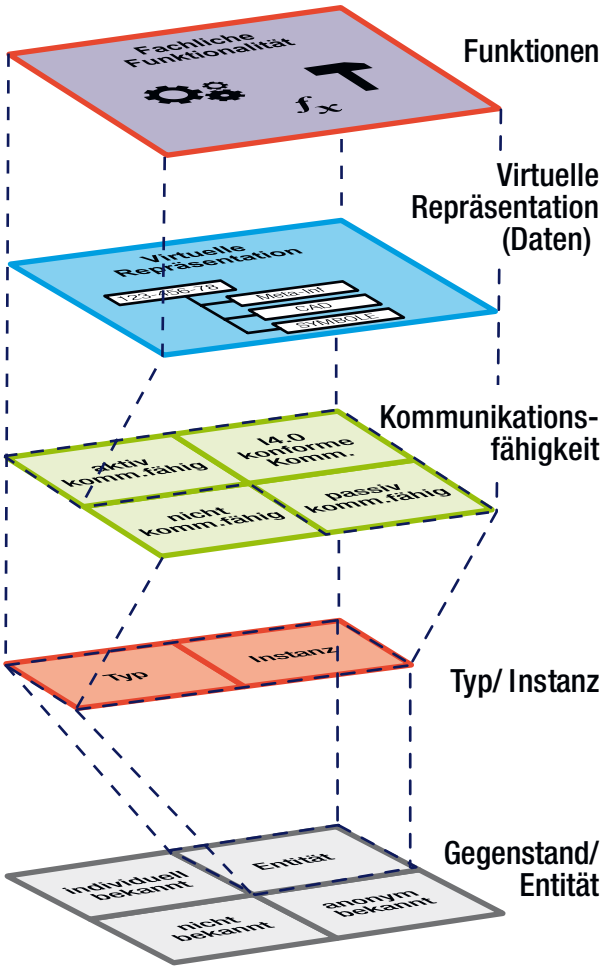


Abbildung 21: Ebenen einer Industrie 4.0-Komponente nach GMA 7.21

Gegenstandsklassen:

- GMA benennt vier Gegenstandsklassen:
- nicht bekannt
- anonym bekannt
- individuell bekannt und
- Entitäten

Um Daten und Funktionen an einen Gegenstand binden zu können, muss dieser als Entität vorliegen. Software, welche im herkömmlichen Sinne auch physisch oder nicht-physisch ausgeliefert wird, ist ebenfalls ein Gegenstand. Auch Ideen, Archive und Konzepte sind Gegenstände in diesem Sinn.

Bemerkung 1:
Da ein Ziel einer Industrie 4.0-Komponente ist, Daten und Funktionen in einem Informationssystem bereitzustellen, ergibt sich für individuell bekannte Gegenstände im Sinne der GMA per se ein Übergang zu einer Entität.

Bemerkung 2:
Im Folgenden wird immer von Gegenstand gesprochen, wenn ein Gegenstand/Entität bezeichnet wird.

Typ/Instanz

Gegenstände können als Typ oder als Instanz bekannt sein. Als Typ ist ein Gegenstand zum Beispiel in der Planungsphase bekannt; sind die Bestellinformationen eines geplanten Gegenstands bekannt, kann dieser als individuell bekannter Typ aufgefasst werden. Als Instanzen sind zum Beispiel alle Gegenstände einer real existierenden Maschine aufzufassen. Scheinbare Instanzen, die durch mehrfache Instantiierung eines Types im Sinne einer Abzählbarkeit entstehen (Chargen), sind zurzeit nicht gesondert berücksichtigt. Hier sollte die Instantiierung konkret ausgeführt werden und ein Rückbezug auf den Typ vorgesehen werden.

Kommunikationsfähigkeit

Um Eigenschaften einer Industrie 4.0-Komponente bereitstellen zu können, muss mindestens ein Informationssystem eine Verbindung zum Gegenstand halten. Daher wird mindestens passive Kommunikationsfähigkeit für den Gegenstand vorausgesetzt, was bedeutet, dass ein Gegenstand nicht unbedingt die Fähigkeit einer Industrie 4.0-konformen Kommunikation entsprechend GMA FA 7.21 aufweisen muss. Damit können bereits bestehende Gegenstände zu Industrie 4.0-Komponenten „erweitert“ werden. In diesem Fall übernimmt ein übergeordnetes IT-System einen Teil der Industrie 4.0-konformen Kommunikation im Sinne einer SOA-Architektur und eines Stellvertreterprinzips.

Beispielsweise kann so eine identifizierbare Klemmleiste zu eienr Industrie 4.0-Komponente werden oder auch ein ProfiNet-Gerät (identifizierbar über seine I&M-Daten).

Virtuelle Repräsentation

Die virtuelle Repräsentation hält Daten zu dem Gegenstand. Diese Daten können entweder „auf/in“ der Industrie 4.0-Komponente selbst gehalten und durch eine Industrie 4.0-konforme Kommunikation der Außenwelt zur Verfügung gestellt werden. Oder sie werden auf einem (übergeordneten) IT-System gehalten, welches sie durch Industrie 4.0-konforme Kommunikation der Außenwelt zur Verfügung stellt.

Im Referenzarchitekturmodell RAMI4.0 findet die Virtuelle Repräsentation auf der Informationsschicht statt. Damit kommt der Industrie 4.0-konformen Kommunikation eine hohe Bedeutung zu.

Anforderung:
Die Industrie 4.0-konforme Kommunikation muss so ausgeführt sein, dass die Daten einer Virtuellen Repräsentation einer Industrie 4.0-Komponente entweder im Gegenstand selbst oder aber in einem (übergeordneten) IT-System gehalten werden können.

Ein wichtiger Teil der Virtuellen Repräsentation ist das „Manifest“[8], welches als Verzeichnis der einzelnen Dateninhalte der Virtuellen Repräsentation angesehen werden kann. Damit enthält es sogenannte Meta-Informationen. Es enthält außerdem verpflichtende Angaben zu der Industrie 4.0-Komponente, unter anderem zur Verbindung mit dem Gegenstand durch die entsprechende Identifikationsmöglichkeit.

Mögliche weitere Daten in der Virtuellen Repräsentation sind Daten, die einzelne Lebenszyklus-Phasen umfassen, wie zum Beispiel CAD-Daten, Anschlussbilder, Handbücher usw.

Fachliche Funktionalität

Neben Daten kann eine Industrie 4.0-Komponente auch eine fachliche Funktionalität besitzen. Diese Funktionalität kann beispielsweise umfassen:

- Software zur „lokalen Planung“ in Verbindung mit dem Gegenstand. Beispiele: Schweißplanung, Software zum Beschriften der Klemmleisten usw.
- Software zur Projektierung, Konfiguration, Bedienung, Wartung
- Mehrwerte zum Gegenstand
- weitere fachliche Funktionalitäten, die für die Ausführung der Geschäftslogik relevant sind

Im Referenzarchitekturmodell RAMI4.0 findet die Fachliche Funktionalität auf der Funktionsschicht statt.

6.3.3.3 Eine „Verwaltungs-Schale“ macht einen Gegenstand zu einer Industrie 4.0-Komponente

Wie der obige Abschnitt beschreibt, können verschiedenartige Gegenstände mit verschiedenartigen Kommunikationsfähigkeiten zu einer Industrie 4.0-Komponente ausgeführt werden. Dieser Abschnitt soll diese verschiedenen Ausführungsformen anhand von Beispielen näher beleuchten. Im Sinne des Konzeptes Industrie 4.0-Komponente sind diese Ausführungsformen gleichwertig.

Die Abbildung 22 zeigt, dass ein Gegenstand, gleich welcher Art, zunächst keine Industrie 4.0-Komponente ist. Erst wenn dieser Gegenstand, der eine Entität und mindestens passiv kommunikationsfähig sein muss, mit einer „Verwaltungs-Schale“ umgeben wird, kann er als Industrie 4.0-Komponente bezeichnet werden.

Im Sinne des obigen Abschnitts umfasst dabei die Verwaltungs-Schale die Virtuelle Repräsentation und die Fachliche Funktionalität des Gegenstandes.

8 Gewählt wegen .JAR-Datei, siehe Manifest [11]

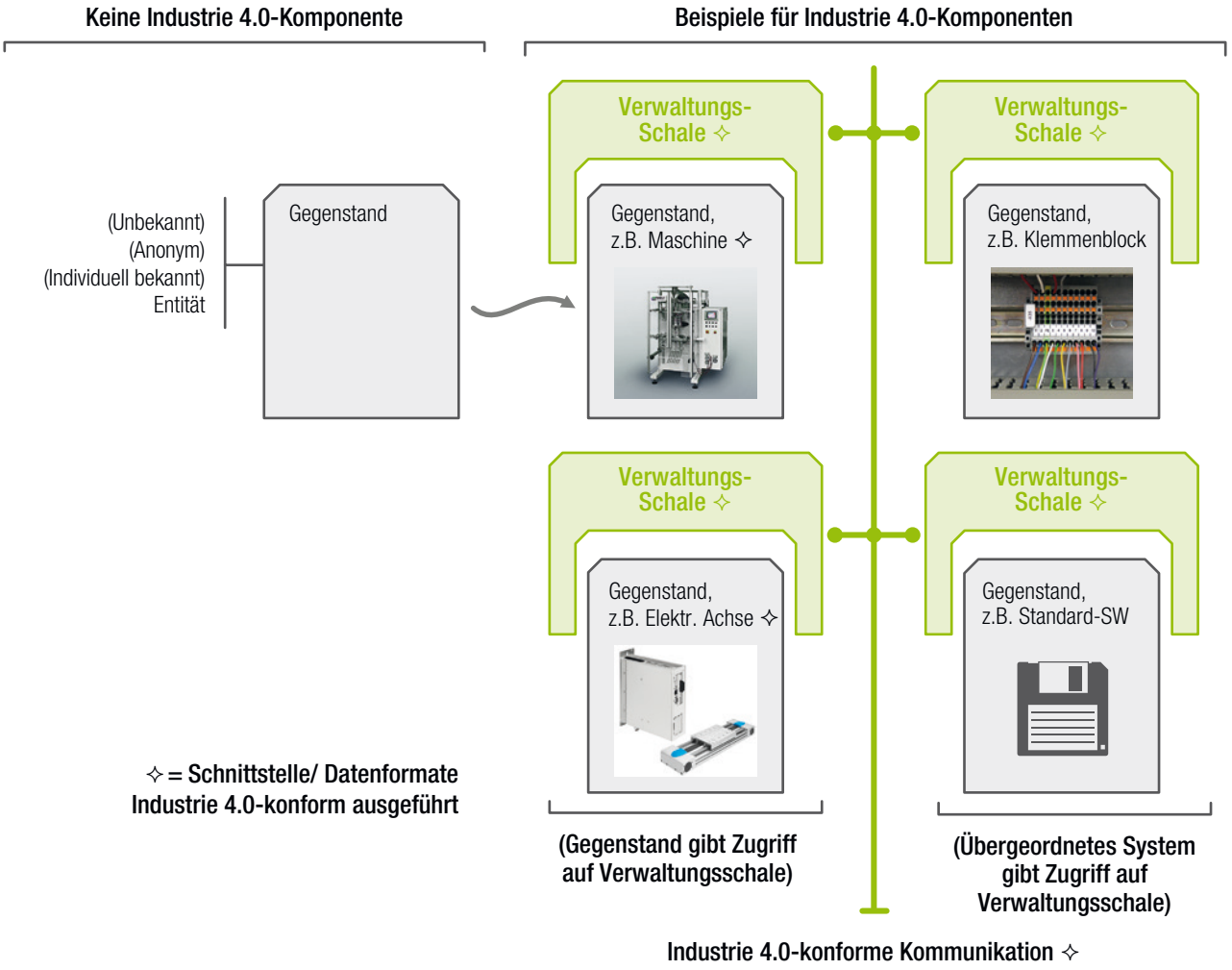


Abbildung 22: Ein Gegenstand wird zur Industrie 4.0-Komponente

Für einen möglichen Gegenstand gibt die obige Abbildung vier Beispiele:

1. Eine ganze Maschine kann vor allem aufgrund ihrer Steuerung als Industrie 4.0-Komponente ausgeführt werden. Diese Ausführung der Industrie 4.0-Komponente übernimmt dann beispielsweise der Maschinenhersteller.
2. Auch eine strategisch wichtige Baugruppe[9] von einem Zulieferer kann als eigenständige Industrie 4.0-Komponente aufgefasst werden, um sie beispielsweise von Asset-Management- und Wartungs-Systemen eigenständig zu erfassen. Die Ausführung der Industrie 4.0-Komponente übernimmt dann beispielsweise der Komponentenhersteller.
3. Ebenso ist es möglich, einzelne konstruierte Baugruppen der Maschinen als Industrie 4.0-Komponente aufzufassen. Beispielsweise ist es für einen Klemmenblock wichtig, die Beschaltung mit einzelnen Signalen festzuhalten und über den Lebenszyklus der Maschine aktuell zu halten. Diese Ausführung der Industrie 4.0-Komponente übernimmt dann beispielsweise der Elektro-Planer und Elektriker.
4. Letztlich kann eine bereitgestellte Software ein wichtiges Asset eines Produktionssystems und somit eine Industrie 4.0-Komponente darstellen. Eine solche Standard-Software könnte zum Beispiel ein eigen-

9 um den Begriff Komponente zu vermeiden

ständiges Planungs- oder Engineering-Werkzeug sein, welches heute oder in Zukunft für den Betrieb der Fertigung wichtig ist. Auch ist es denkbar, dass ein Zulieferer eine Bibliothek, welche erweiterte Funktionen zu seinen Produkten bereitstellt, als reine Software verkaufen möchte. Diese Ausführung der Industrie 4.0-Komponente übernähme dann beispielsweise der Bereitsteller der Software; eine Verteilung auf einzelne IEC61131-Steuerungen würde dann von den verschiedenen Industrie 4.0-Systemen geleistet.

Die Abbildung 22 stellt in einer logischen Sicht dar, dass zu einem Gegenstand eine „Verwaltungs-Schale" gehört. Im Hinblick auf eine Verteilungs-Sicht können Gegenstand und Verwaltungs-Schale durchaus entkoppelt existieren. So kann bei passiv kommunikationsfähigen Gegenständen die Verwaltungs-Schale in einem übergeordneten IT-System abgebildet[10] werden. Mithilfe der passiven Kommunikationsfähigkeit des Gegenstandes und einer Industrie 4.0-konformen Kommunikation des übergeordneten IT-Systems wird die Verbindung zwischen Gegenstand und Verwaltungs-Schale gewahrt. Gleiches gilt, wenn der Gegenstand aktiv, aber nicht Industrie 4.0-konform kommunikationsfähig ist. Erst bei einer Industrie 4.0-konformen Kommunikationsfähigkeit kann die Verwaltungs-Schale „im" Gegenstand abgebildet werden (sie wird beispielsweise in der Steuerung einer Maschine gespeichert und durch die Netzwerkschnittstelle ausgeliefert). Im Sinne des Konzeptes Industrie 4.0-Komponente sind alle Alternativen als gleichwertig anzusehen.

Ein Gegenstand kann mehrere Verwaltungsschalen für unterschiedliche Zwecke besitzen.

Anforderung:

Durch ein geeignetes Referenzmodell muss beschrieben werden, wie ein übergeordnetes IT-System die Verwaltungs-Schale Industrie 4.0-konform zur Verfügung stellen kann (SOA-Ansatz, Stellvertreter-Prinzip).

10 „gehostet"

Anforderung:

Es muss beschrieben werden, wie die Verwaltungs-Schale vom Erzeuger (z. B.. Komponenten-Hersteller, Elektro-Planer) zum übergeordneten IT-System „transportiert" werden kann (z. B. als Attachment zu einer eMail..).

6.3.3.4 Weitere Begriffs-Abgrenzung

Die folgende Abbildung grenzt die Begriffe nochmals voneinander ab:

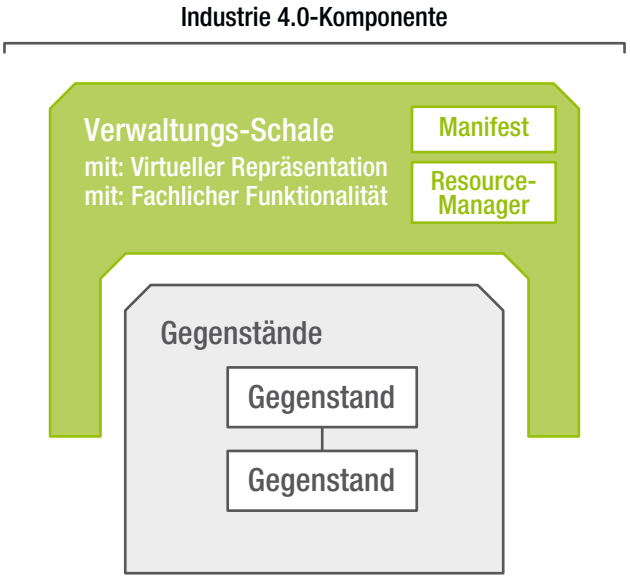


Abbildung 23: Industrie 4.0-Komponente

Eine Industrie 4.0-Komponente umfasst aus logischer Sicht ein oder mehrere Gegenstände und eine Verwaltungsschale, welche Daten der Virtuellen Repräsentation und Funktionen der Fachlichen Funktionalität enthält. Das Manifest als Teil der Virtuellen Repräsentation detailliert die notwendigen verwaltungs-technischen Angaben zu der Industrie 4.0-Komponente. Der „Resource-Manager", wie von der GMA FA 7.21 definiert, ist ebenfalls Teil der Verwaltungsschale. Damit haben die IT-technischen Dienste Zugriff auf die Daten und Funktionen der Verwaltungsschale und machen sie nach außen verfügbar.

Die Verwaltungsschale und ihre Objekte können innerhalb eines „embedded Systems" eines der Gegenstände „gehostet" sein (aktive, Industrie 4.0-konforme Kommunikationsfähigkeit) oder aber in ein oder mehrere übergeordnete IT-Systeme verteilt werden (Verteilungs-Sicht).

Anforderung:
Je nach Art der übergeordneten Systeme müssen die Verwaltungsobjekte in mehr als ein übergeordnetes IT-Systems verteilt werden können.

Cyber-Physisches System

Die Industrie 4.0-Komponente stellt eine Spezialisierung eines Cyber-Physischen Systems dar.

6.3.3.5 Industrie 4.0-Komponenten aus Verteilungs-Sicht

Der obere Abschnitt stellt dar, dass aus einer logischen Sicht heraus für jede Industrie 4.0-Komponente zu jedem Gegenstand eine „Verwaltungs-Schale“ gehört. Er betont aber auch, dass situativ aus Verteilungs-Sicht die Verwaltungs-Schale in ein übergeordnetes System ausgelagert werden kann.

Industrie 4.0-Komponente in Repository abgebildet

Zum besseren Verständnis kann eine zu einem Repository der „Digitalen Fabrik“ konforme Darstellung gezeigt werden, die im Einklang mit den dargelegten Konzepten ist:

Industrie 4.0-Komponente durch Gegenstand abgebildet

Ist einer der Gegenstände der Industrie 4.0-Komponente Industrie 4.0-konform kommunikationsfähig (CP34- oder CP44 nach [2]), so bietet sich an, die Industrie 4.0-Komponente durch den Gegenstand abzubilden:

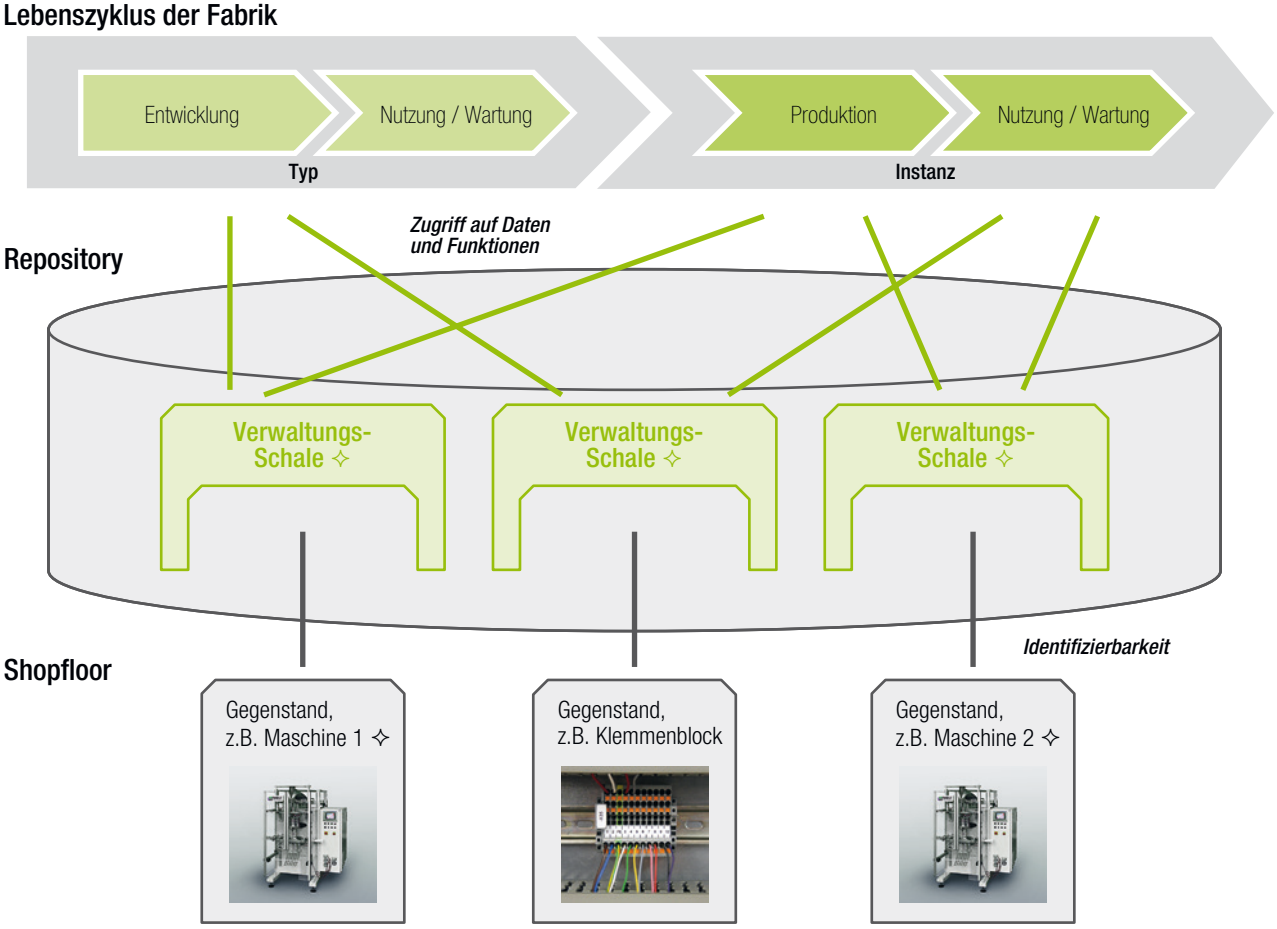


Abbildung 24: Repository

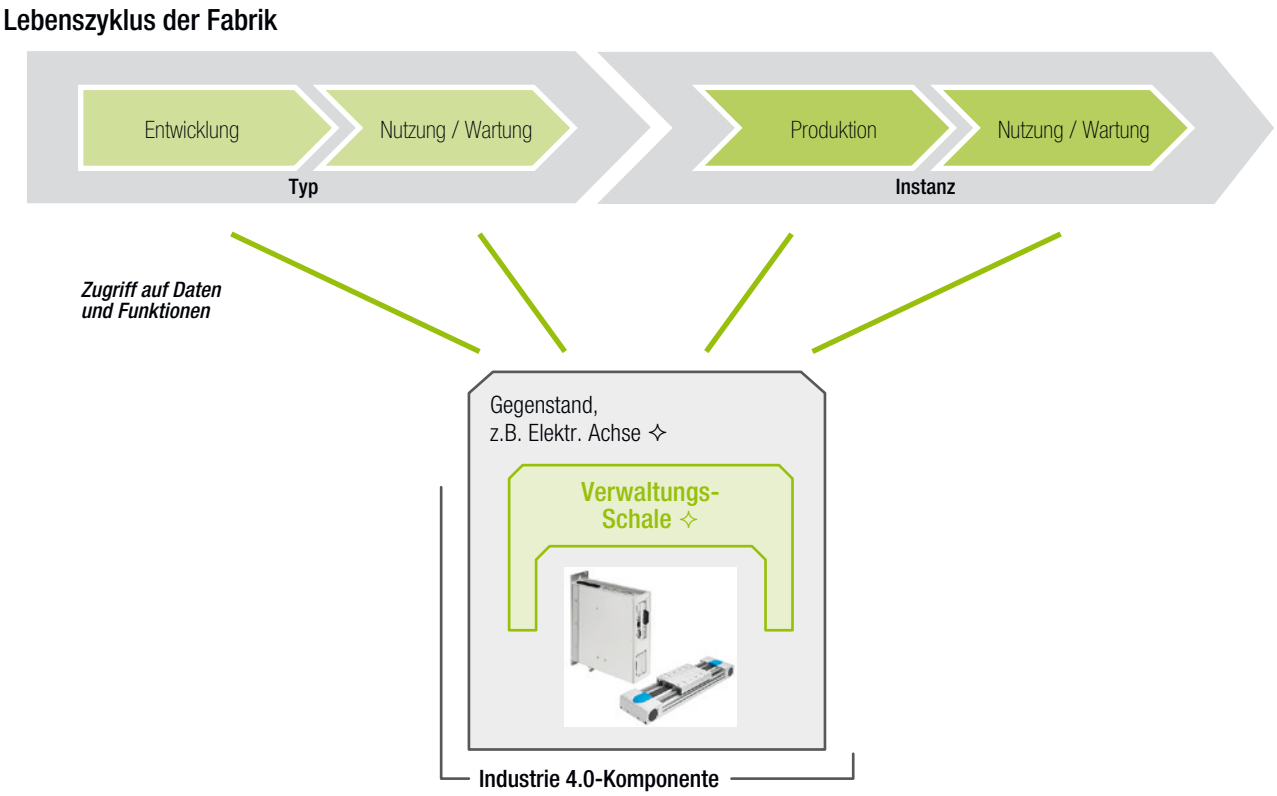


Abbildung 25: Lebenszyklus der Fabrik

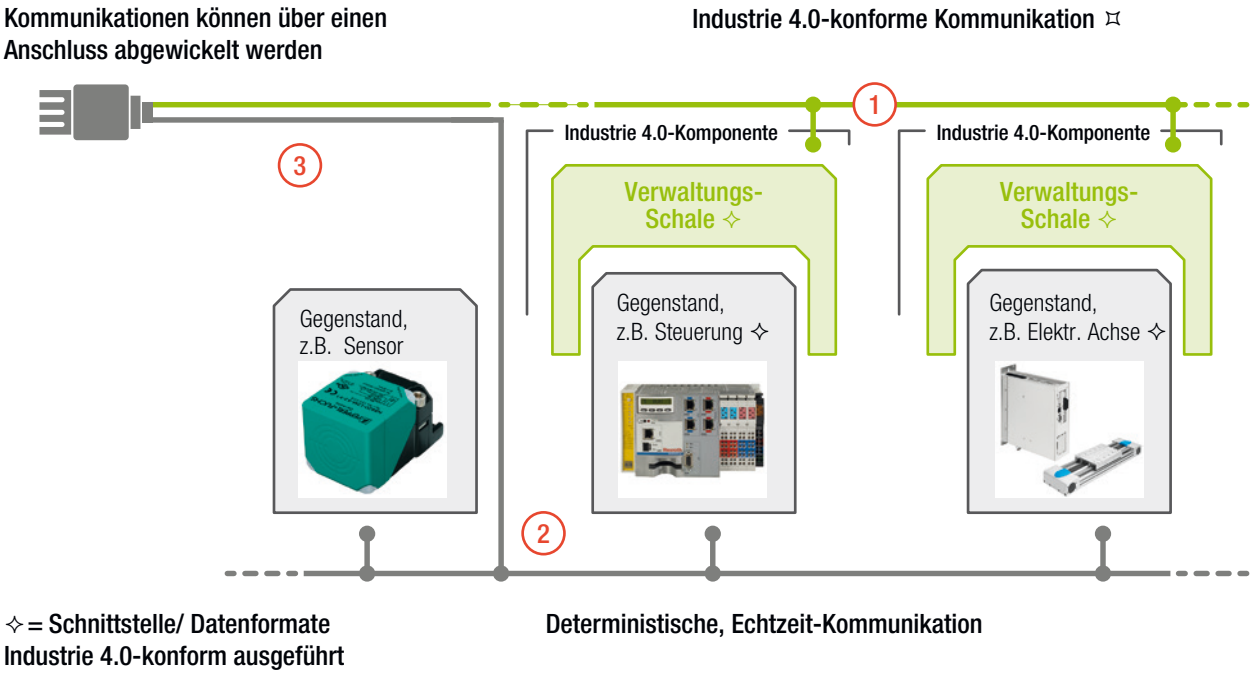


Abbildung 26: Kapselfähigkeit und Vernetzung einer Industrie 4.0 Komponente

Die Industrie 4.0-Komponente ist kapselfähig

Die Industrie 4.0-Komponente soll bewusst alle möglichen Querverbindungen innerhalb der Industrie 4.0-Fabrik eingehen bzw. aufbauen können (Abbildung). Doch diese Vernetzung darf nicht zur Einschränkung der Kernfunktionalität führen (Abbildung). Die Fähigkeit, diesen Kernbereich störungsfrei zu erhalten, selbst wenn die „äußere“ Vernetzung Störungen unterliegt, wird durch SG2 (ZVEI Spiegelgremium Referenzarchitektur) und SG4 (ZVEI Spiegelgremium Security) als „kapselfähig“ bezeichnet.

Anforderung:

Die Industrie 4.0-Komponente, insbesondere die Verwaltungsschale, ihre enthaltene Funktionalität und die damit befassten Protokolle sollen „kapselfähig“ sein.

Das vorliegende Konzept verwirklicht diese Anforderung dadurch, dass die Verwaltungsschale als unabhängiges Daten-/Funktionsobjekt ausgeführt wird. Der Zugriff auf die darin enthaltenen Daten und Funktionen soll nach dem Prinzip von „Separation of Concerns (SoC)“[11] gestaltet werden, sodass eine Beeinflussung von für die Fertigung kritischen Abläufen nach dem Stand der Technik ausgeschlossen werden kann.

Aus der Anwendung dieses Prinzips folgt, dass die Industrie 4.0-konforme Kommunikation nach heutigem Stand in der Fertigung verwendete Ethernet-basierte Feldbusse nicht vollständig ersetzen muss (Migrationsszenario).

Allerdings sollen Industrie 4.0-konforme Kommunikation und eine mögliche deterministische oder Echtzeit-Kommunikation aufeinander abgestimmt sein und zum Beispiel nach Möglichkeit die gleichen (physikalischen) Schnittstellen und Infrastrukturen verwenden. Die Widerspruchsfreiheit zwischen beiden Kommunikations-Kanälen muss gewährleistet sein.

Für das in diesem Text beschriebene Referenzmodell bedeutet diese Argumentation, dass Industrie 4.0-konforme Kommunikation nicht sämtliche Eigenschaften einer deterministischen oder Echtzeit-Kommunikation selbst realisieren muss, sondern sie an bestehende Technologien delegieren kann.

Anforderung:

Anspruch der Industrie 4.0-Komponente ist, nicht-Industrie 4.0-konforme Kommunikationsbeziehungen, die in die Gegenstandsschale führen oder diese verlassen, zu erfassen und einem durchgängigen Engineering zu öffnen.

Die heute üblichen Echtzeit-Ethernet-Protokolle lassen es möglich erscheinen, beide Kommunikationen über die gleiche Kommunikations-Infrastruktur (Anschlüsse, Stecker, Zwischenstationen) abzuwickeln (Abbildung). Nach dem Prinzip „Separation of Concern“ sind aber beide Kommunikationsarten logisch weiterhin getrennt.

Eine Industrie 4.0-Komponente kann mehrere Gegenstände enthalten

Dieser Abschnitt zeigt an einem Beispiel, dass eine Industrie 4.0-Komponente nicht nur ein, sondern mehrere Gegenstände enthalten kann.

Abbildung 27: Industrie 4.0-Komponente bestehend aus mehreren Gegenständen

11 http://en.wikipedia.org/wiki/Separation_of_concerns

Die in der Abbildung 27 gezeigten Gegenstände formen zusammen ein beispielhaftes elektrisches Achssystem. Von einem Hersteller gibt es eine Auslegungs-Software, welche während der Engineering-Phase dazu geführt hat, dass die einzelnen Teilsysteme zu einem System kombiniert wurden. Außerdem gibt es eine Konfigurations-Software, mit welcher das System als Ganzes in Betrieb gesetzt werden kann. Verfahrsätze, aufgezeichnete Verschleißdaten und das Condition Monitoring müssen die einzelnen Systembestandteile miteinander in Bezug setzen (z. B. bezüglich maximaler Verfahrlänge).

Daher macht es aus Industrie 4.0-Sicht Sinn, diese einzelnen Gegenstände als ein System zu verwalten und als eine Industrie 4.0-Komponente abzubilden. Eine Zerlegung in einzelne Industrie4.0-Komponenten würde die Abbildung vieler verschiedener Sinnzusammenhänge durch ein oder sogar mehrere übergeordnete Industrie 4.0-Systeme erfordern und unnötig verkomplizieren.

6.3.3.8 Eine Industrie 4.0-Komponente kann logisch schachtelbar sein

Industrie 4.0 fordert die Modularisierung von Produktionssystemen für auftragsgerechte Rekonfiguration und Wiederverwendung von (Unternehmens-) Assets[12] im Rahmen vom Industrie 4.0-Aspekt (2) „Vertikale Integration“. Daher sieht das Konzept vor, dass eine Industrie 4.0-Komponente andere Komponenten logisch umfassen, als Einheit agieren und für ein übergeordnetes System logisch abstrahieren kann.

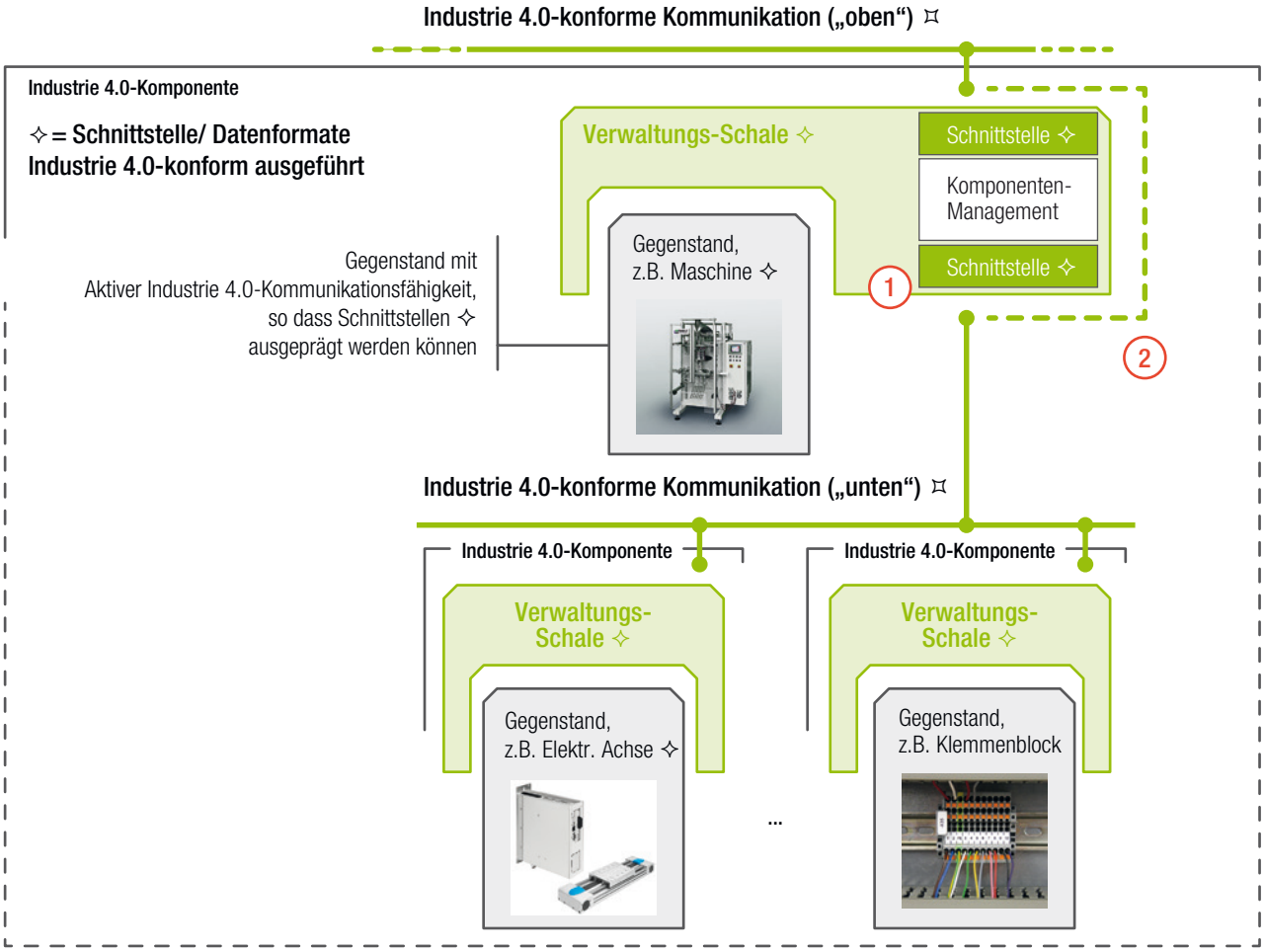


Abbildung 28: Schachtelbarkeit von Industrie 4.0-Komponenten

12 siehe [3]: „Zudem sind Modularisierungs- und Wiederverwendungskonzepte als Voraussetzung für Ad-hoc-Vernetzung und Rekonfigurierbarkeit von Produktionssystemen in Kombination mit geeigneten intelligenten Anlagen-Fähigkeitsbeschreibungen zu entwickeln.“

Zudem fordert Industrie 4.0-Aspekt (3) „Durchgängigkeit im Engineering“, dass für möglichst viele Gegenstände eines Produktionssystems weiterführende Daten und Engineering-Planungen online verfügbar sind. Die Verwaltungs-Schale sieht vor, dass Daten, die den Gegenständen der Industrie 4.0-Komponente eindeutig zugeordnet werden können, auch derart verteilt verfügbar sind. Derart verteilte Daten sind für ein verteiltes Engineering und für eine schnelle Rekonfiguration von Vorteil.

Daher soll das Konzept für eine Industrie 4.0-Komponente vorsehen, dass einer Industrie 4.0-Komponente (z. B. einer ganzen Maschine) andere Industrie 4.0-Komponenten logisch zugeordnet werden, sodass sich eine (temporäre) Schachtelung ergibt.

Technisch gesehen kann dieses so ausgeführt werden, dass der übergeordnete Gegenstand (z. B. eine Maschine) zwei Industrie 4.0-konforme Kommunikationsschnittstellen ausprägt, sodass sich eine klare logische und physikalische Trennung von übergeordneten und untergeordneten Industrie 4.0-Komponenten ergibt (in Abbildung). Eine weitere Möglichkeit besteht darin, dass die Industrie 4.0-konforme Kommunikation „oben“ und „unten“ physisch eins sind, aber logisch voneinander getrennt werden (in Abbildung).

Um eine solche logische Zuordnung von „untergeordneten“ Industrie 4.0-Komponenten zu managen, kann die Verwaltungs-Schale ein geeignetes „Komponenten-Management“ vorsehen. Dieses kann zum Beispiel die Rekonfiguration einer Maschine unterstützen oder aber den Status der Maschine „nach oben“ geeignet abbilden.

Anforderung:
Einer Industrie 4.0-Komponente (z. B. einer ganzen Maschine) sollen andere Industrie 4.0-Komponenten logisch zugeordnet werden können, so dass sich eine (temporäre) Schachtelung ergibt.

Anforderung:
Übergeordnete Systeme sollen zweckgebunden und einschränkbar auf alle Industrie 4.0-Komponenten zugreifen können, auch wenn diese (temporär) logisch zugeordnet sind.

6.3.3.9 Zustandsmodell

Der Zustand einer Industrie 4.0-Komponente ist von anderen Teilnehmern einer Industrie 4.0-konformen Kommunikation immer abrufbar. Er folgt dabei einem definierten Zustandsmodell.

Da Industrie 4.0-Komponenten hierarchisch organisiert sein können, sollte eine geeignete Abbildung von Unter-Zuständen in einen Zustand definiert werden (Was bedeutet es für die Maschine, wenn ein Teil nicht betriebsbereit ist?).

Zusätzlich soll das Zustandsmodell auch mit einer größeren Menge von Zustandsvariablen komplementiert werden, die eine detaillierte Sicht auf die Zustände der Virtuellen Repräsentation und der Fachlichen Funktionalität erlauben. Dies erlaubt zu einem Zeitpunkt ‚t‘ eine konsistente Sicht auf den Zustand einer Industrie 4.0-Komponente, etwa zum Zweck der statistisch korrekten Datenanalyse.

6.3.3.10 Allgemeine Merkmale der Industrie 4.0-Komponente

GMA 7.21 [2] definiert den Begriff Komponente im Kontext zu Industrie 4.0 wie folgt:

Der Begriff Komponente ist allgemein. Er bezeichnet einen Gegenstand der physischen Welt oder der Informationswelt, der in seinem Systemumfeld eine bestimmte Rolle spielt oder für eine solche vorgesehen ist. Eine Komponente kann z. B. ein Rohr, ein SPS-Funktionsbaustein, eine Lampe, ein Ventil, eine intelligente Antriebseinheit usw. sein. Wichtig ist die Betrachtung als Einheit und der Bezug zu der Rolle (Funktion), die sie in einem System wahrnehmen soll oder bereits wahrnimmt. Als Industrie 4.0-Komponente bezeichnen wir eine spezielle Art von Komponente. Industrie 4.0-Komponenten zeichnen sich dadurch aus, dass sie bezüglich der oben dargestellten Klassifikationsmerkmale bestimmte Anforderungen erfüllen. Auch in einem Industrie 4.0-System gibt es viele Komponenten, die diese Anforderungen nicht erfüllen und die damit keine Industrie 4.0-Komponenten sind.

Das hier vorliegende Konzept lässt auch Gegenstände zu, welche passiv oder aktiv, aber nicht Industrie 4.0-konform kommunikationsfähig sind. Daher gilt für die Industrie 4.0-Komponente im Sinn dieses Dokumentes:

- Sie ist bezüglich der CP-Klassifikation entweder eine CP24, CP34, oder eine CP44-Komponente.
- Sie besitzt eine Verwaltungsschale, welche so kommuniziert werden kann, dass sie zu einem vollwertigen Dienstsystemteilnehmer im Industrie 4.0-Netzwerk wird.

Der folgende Abschnitt wurde auf Basis der GMA-Definition [2] verfeinert und stellt daher eine Detaillierung der Konzepte dar. In voller Übereinstimmung mit [2] werden als Dienstsystemteilnehmer im Industrie 4.0-Netzwerk von einer Industrie 4.0-Komponente zunächst folgende Merkmale verlangt (Anforderungen):

Identifizierbarkeit

Sie ist im Netzwerk eindeutig identifizierbar und ihre physischen Gegenstände werden mittels eines eineindeutigen Identifiers (ID) identifiziert. Ist sie eine CP34- oder CP44-Komponente, so ist sie über eine Kommunikationsadresse (z. B. IP-Adresse) erreichbar.

Industrie 4.0-konforme Kommunikation

Die Industrie 4.0-Komponenten kommunizieren untereinander mindestens nach dem SOA Prinzip (inkl. gemeinsamer Industrie 4.0-konformer Semantik).

Industrie 4.0-konforme Dienste und Zustände

Sie unterstützt die für ein Industrie 4.0-System allgemein standardisierten (auch nachladbaren) Dienstfunktionen und Zustände.

Virtuelle Beschreibung

Sie liefert ihre virtuelle Beschreibung einschließlich ihres dynamischen Verhaltens. Diese Beschreibung wird durch die Virtuelle Repräsentation und das Manifest erreicht.

Industrie 4.0-konforme Semantik

Sie unterstützt die für ein Industrie 4.0-System standardisierte Industrie 4.0-konforme Semantik.

Security und Safety

Sie bietet für Ihre Funktionalität und Daten einen der Aufgabe entsprechenden ausreichenden Schutz (Security). Zusätzlich können in Anwendungen auch Maßnahmen zur funktionalen Sicherheit, Maschinensicherheit notwendig sein (Safety).

Quality of Services

Sie besitzt die für ihre Aufgabe erforderlichen Eigenschaften als Quality of Services (QoS). Bzgl. der Anwendung in der Automatisierungstechnik sind dies Eigenschaften wie Echtzeitfähigkeit, Ausfallsicherheit, Uhrensynchronisation, u.a. Diese Eigenschaften richten sich möglicherweise nach einem Profil aus.

Zustand

Sie liefert jederzeit ihren Zustand.

Schachtelbarkeit

Jede Industrie 4.0-Komponente kann aus weiteren Industrie 4.0-Komponenten bestehen.

Industrie 4.0-Komponenten im Kontext dieses Dokuments stehen für Produktionssysteme, Maschinen, Stationen und konzeptuell wichtige Teile bzw. Baugruppen von Maschinen.

Zu Merkmal (1): Identifizierbarkeit

Ziel des „Industrie 4.0“-Ansatzes ist es, auf alle relevanten Daten in Echtzeit zugreifen zu können. Die Industrie 4.0-Komponenten stellen einen wichtigen Teil einer gegenüber heute erweiterten Infrastruktur dar. Dies gilt während der gesamten Lebenszeit des Produktionssystems. Industrie 4.0-Komponenten spielen also auch in allen Industrie 4.0-Wertschöpfungsketten [1] und allen ihren Wertschöpfungsprozessen eine zentrale Rolle für den durchgängigen und einheitlichen Informationsaustausch.

Eine aktive Industrie 4.0-Komponente kann Industrie 4.0-konforme Kommunikation selbst abwickeln; für eine passive Industrie 4.0-Komponente erledigt dies die notwendige Infrastruktur.

Es besteht die Notwendigkeit für eine den industriellen Anforderungen gerecht werdende Kommunikation. Da Produktionssysteme immer mehr im Verbund arbeiten und dabei auch größere Entfernungen überbrückt werden müssen, wird die Verbindung lokaler Netze mittels der Weitverkehrstechnik immer wichtiger.

Anforderung:
Bei der Vernetzung von Industrie 4.0-Komponenten sollte sich die Weitverkehrstechnik so verhalten, dass lokale Netze weitgehend ohne Einschränkungen über die Weitverkehrsanbindung miteinander kommunizieren können.

Dies betrifft die Verfügbarkeit solcher Verbindungen, die Sicherheit (Security), aber auch das zeitgerechte Verhalten. Wenngleich Streaming-Technologien und andere Mechanismen eine Basis für passende Lösungen darstellen könnten, sind hierzu noch grundlegende Arbeiten erforderlich.

Eine Ebene höher müssen Verbindungen dafür sorgen, dass die Kommunikation zuverlässig und stabil über einen langen Zeitraum garantiert ist. Hier sind bestehende Protokolle auf ihre Tauglichkeit in Industrie 4.0-Anwendungen zu prüfen. Zu unterscheiden ist die Adressierung der Industrie 4.0-Komponente und die Adressierung ihrer (Anwendungs-)Objekte. Diese werden mittels einer weltweit und herstellerübergreifenden eineindeutigen ID angesprochen. Zum Umgang mit IDs sei auf [4] und [5] und andere Standards verwiesen.

Anforderung:
Zu unterscheiden ist die Adressierung der Industrie 4.0-Komponente und die Adressierung ihrer (Anwendungs-) Objekte.

Zu Merkmal (2): Industrie 4.0-konforme Kommunikation

Die Selbstauskunft einer Industrie 4.0-Komponente wird auf Basis einer serviceorientierten Architektur (SOA) mit Diensten entsprechend einem Dienste-Modell realisiert (Resource-Manager). Ein entsprechendes Profil der Industrie 4.0-Komponente kann regeln, wie diese Dienste technologisch realisiert werden können (zum Beispiel über OPC-UA-Basisdienste).

Zu Merkmal (3): Industrie 4.0-konforme Dienste und Zustände

Da im Shopfloor und im Officefloor unterschiedliche Anwendungen bedient werden müssen, muss die Option bestehen, dass Industrie 4.0-Komponenten die verschiedenen Anwendungsebenen mit unterschiedlichen Protokollen bedienen können.

Anforderung:
Protokolle und Anwendungsfunktionen sollen daher optional nachladbar sein.

Zu Merkmal (4): Virtuelle Beschreibung

Die Informationen zur Beschreibung der Eigenschaften einschließlich des relevanten dynamischen Verhaltens einer Industrie 4.0-Komponente werden aus dem virtuellen Abbild der realen Komponente in einem Industrie 4.0-Datenformat erzeugt. Dieses Abbild wird als Virtuelle Repräsentation bezeichnet; Teil der Virtuellen Repräsentation ist das Manifest, welches mit einer eindeutigen Semantik belegt sein muss. Dabei spielt die Spezifikation von Merkmalen eine wichtige Rolle.

Teil des Manifests sind zum Beispiel:

- Charakteristische Merkmale der realen Komponente
- Informationen über Beziehungen der Merkmale untereinander
- produktions- und produktionsprozessrelevante Beziehungen zwischen Industrie 4.0-Komponenten
- Formale Beschreibung relevanter Funktionen der Maschine und ihrer Abläufe

Teil der Virtuellen Repräsentation sind zum Beispiel:

- Kaufmännische Daten
- Historische Daten, zum Beispiel Servicehistorie
- und weitere…

Abgrenzung zwischen Manifest im Besonderen und Verwaltungsobjekten im Allgemeinen ist, dass das Manifest Informationen enthält, die für die Verwirklichung eines Industrie 4.0-konformen Netzwerkes entsprechend den Industrie 4.0-Aspekten nach einer eindeutigen Semantik öffentlich bekannt sein müssen. Verwaltungsobjekte können auch solche Informationen tragen, bei denen der Hersteller selbst entscheiden kann, was in welcher Form er offenlegen möchte.

Zu Merkmal (5): Industrie 4.0-konforme Semantik

Der Informationsaustausch zwischen zwei oder mehreren Industrie 4.0-Komponenten erfordert eine eineindeutige Semantik. Diese muss mittels der unter 4. aufgeführten Charakteristika Industrie 4.0-weit festgelegt werden. Hilfreich erscheint nach [4] die Klassifikation der Merkmale nach folgenden Feldern:

- Mechanik
- Funktionalität
- Örtlichkeit
- Leistungsfähigkeit und
- Geschäftliche Rahmenbedingungen

Zum Umgang mit Merkmalen sei auf [4], [5] und [6] verwiesen.

Zu Merkmal (6): Security und Safety

Jede Industrie 4.0-Komponente weist eine Mindestinfrastruktur zur Sicherstellung der Security-Funktionen auf. Da Security nur sichergestellt ist, wenn die jeweiligen Produktionsprozesse in die Security-Betrachtungen unmittelbar einbezogen sind, stellt die Security-Infrastruktur einer Industrie 4.0-Komponente zwar notwendige aber bei Weitem nicht hinreichende Funktionalität zur Verfügung. Muss die funktionale Sicherheit, Maschinensicherheit (Safety) sichergestellt werden, so hat dies Einfluss auf die Eigenschaften der einzelnen Industrie 4.0-Komponenten. Zusätzliche Merkmale müssen hier erfasst, bewertet und an übergeordnete Systeme weiter gegeben werden.

Anforderung:
Die Mindestinfrastruktur muss den Prinzipien von „Security-by-Design“ (SbD) gerecht werden.

Zu Merkmal (7): Quality of Services

Die Anwendung einer Industrie 4.0-Komponente in einer bestimmten Umgebung bestimmt deren Anforderungen. Die in der jeweiligen Umgebung geforderten Eigenschaften (QoS) müssen daher schon bei der Auswahl der Komponenten für eine Maschine oder Anlage berücksichtigt werden. Speziell für Automatisierungsumgebungen sind das Eigenschaften wie:

- Zeitspanne der Echtzeit für die Produktivkommunikation, z. B. Deterministik mit Echtzeitfähigkeit von D1ms.
- Höchste Ausfallsicherheit bzgl. der umgebenden Netzinfrastruktur (Robustheit)
- Uhrensynchronisation
- Interoperabilität
- Diagnose und Engineering auf Basis einheitlicher Regeln
- Aufbau von Adhoc-Verbindungen

Zu Merkmal (8): Zustand

Da jede Industrie 4.0-Komponente Teil eines Verbundes mit bestimmten Aufgaben darstellt und diese Aufgaben in Prozessen koordiniert erledigt werden, muss der Zustand jeder Industrie 4.0-Komponente zu jedem Zeitpunkt von anderen Teilnehmern eines Industrie 4.0-konformen Kommunikationsnetzwerks abrufbar sein. Diese Informationen dienen der lokalen Verwaltung anderer Industrie 4.0-Komponenten und der globalen Verwaltung zur Koordination der Abläufe.

Zu Merkmal (9): Schachtelbarkeit

Industrie 4.0-Komponenten können zu einer Industrie 4.0-Komponente zusammengefasst werden. So kann sich bspw. eine Maschine als Industrie 4.0-Komponente darstellen. Sie kann selbst aus Komponenten aus mehreren eigenständigen Industrie 4.0-Komponenten bestehen, z. B. eine modulare Maschine. Und auch die einzelnen Maschinenmodule können wieder in einzelne Industrie 4.0-Komponente gegliedert werden.

6.4 Standardisierung und Normung

6.4.1 Hintergrund

Gemäß der deutschen Normungsstrategie wird unter Normung (engl. de jure „standard“) die vollkonsensbasierte Erarbeitung von Regeln, Leitlinien und Merkmalen für Tätigkeiten zur allgemeinen oder wiederkehrenden Anwendung durch eine anerkannte Organisation verstanden. Unter Standardisierung wird in der deutschen Normungsstrate-

gie der Erarbeitungsprozess von Spezifikationen bezeichnet. Dazu gibt es beispielsweise unterschiedliche Dokumentenformen wie etwa die VDE-Anwendungsregel oder die DIN-Spezifikation (DIN SPEC), PAS (Publicly Available Specifications), Technische Spezifikation (TS), ITA (Industry Technical Agreement) oder TR (Technical Report).

Die im vorigen Jahr von DKE in einer ersten Version herausgegebene und gerade in Überarbeitung befindliche „DKE-Roadmap Industrie 4.0“ ist hierbei sehr hilfreich. Zweck des Dokuments ist die Unterstützung des Entwurfs einer strategischen, technisch orientierten Roadmap, welche die Anforderungen an Normen und Spezifikationen für Industrie 4.0 unter besonderer Berücksichtigung der Handlungsempfehlungen der Forschungsunion Wirtschaft – Wissenschaft sowie der entsprechenden BMWi- und BMBF-Fördermaßnahmen darstellt, dabei notwendige Handlungsfelder aufzeigt und entsprechende Empfehlungen abgibt. Zudem bietet sie eine Übersicht über Normen und Spezifikationen in diesem Umfeld.

Die Normungsroadmap dient in der Plattform einerseits der Bestandsaufnahme, andererseits als Mittel der Kommunikation zwischen den beteiligten Akteuren aus verschiedenen technologischen Sektoren wie der Automatisierungstechnik, Informations- und Kommunikationstechnik und der Produktionstechnik.

6.4.2 Standardisierung und Normung als Innovationstreiber

Normen und Standards schaffen eine sichere Grundlage für die technische Beschaffung, stellen die Interoperabilität im Anwendungsfall sicher, schützen Umwelt, Anlagen und Verbraucher durch einheitliche Sicherheitsnormen, sind eine zukunftssichere Grundlage für die Produktentwicklung und unterstützen die Kommunikation unter allen Beteiligten durch einheitliche Begriffe und Konzepte.

Für das Gelingen des Zukunftsprojekts Industrie 4.0 ist die Standardisierung und Normung von zentraler Bedeutung. Industrie 4.0 erfordert eine nie dagewesene Integration der Systeme über Domänengrenzen, Hierarchiegrenzen und Lebenszyklusphasen hinweg. Dies ist nur auf der Grundlage konsensbasierter Spezifikationen und Normen möglich. In der Plattform Industrie 4.0 findet daher eine enge Zusammenarbeit zwischen Forschung, Industrie und der Standardisierung und Normung statt, um die notwendigen Voraussetzungen für eine durchgreifende Innovation zu schaffen: methodische Fundierung und Funktionalität, Stabilität und Investitionssicherheit, Praxistauglichkeit und Marktrelevanz (siehe Abb. 29). Denn für eine schnelle Umsetzung in die industrielle Praxis ist eine zeitnahe Stabilisierung der Konzepte durch einen konsensbasierten, forschungsbegleitenden Standardisierungs- und Normungsprozess unerlässlich.

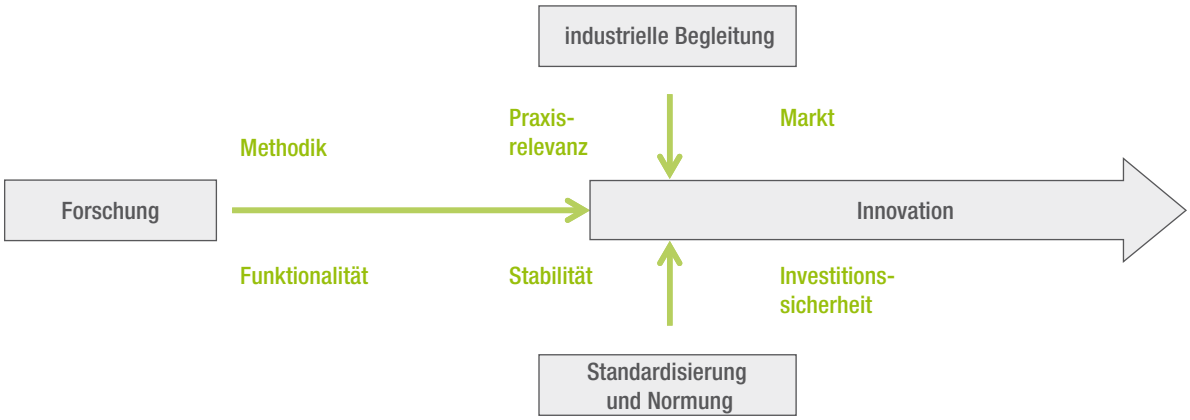


Abbildung 29: Innovation durch Standardisierung (angelehnt an [10])

6.4.3 Zusammenarbeit Standardisierungs- und Normungsgremien

Für die global agierende und exportorientierte deutsche Industrie ist die Festlegung von technischen Anforderungen in global gültigen Normungssystemen von besonderer Bedeutung. Ziel ist es, Schritt für Schritt alle für die einheitliche technische Funktion und Anwendbarkeit wesentlichen Festlegungen in internationalen Normen zu verankern. Die relevanten Ziel-Normungsorganisationen sind hier insbesondere IEC und ISO.

Für die Informationstechnik spielen u.a. die weltweit akzeptierten Standards von IETF und des W3C-Konsortiums eine zentrale Rolle. Ziel der Normung für Industrie 4.0 ist die Verbesserung der Interoperablilität auf der Anwendungsebene einerseits und die Verbesserung der Netzqualität andererseits.

Die Erstellung konsensbasierter Normen kann auf unterschiedlichen Wegen erfolgen. Abb. 30 zeigt schematisch die typischen Vorgehensweisen. Ausgangspunkt ist die Feststellung eines bestimmten Normungsbedarfs. Dieser ergibt sich durch Rückmeldungen aus der praktischen Anwendung, durch das Entstehen neuer Technologien, aus Forschungsergebnissen oder aus regulatorischen Vorgaben.

Betrachtet man den Weg zu einer internationalen Norm (ISO3, IEC4), dann kann man drei typische Routen unterscheiden:

- Die direkte Festlegung innerhalb der zuständigen Normungsgremien. In diesem Fall werden die zu normenden Festlegungen innerhalb des zuständigen internationalen und der nationalen Spiegelgremien erarbeitet. Ein Beispiel ist die Entwicklung der IEC 61131-3 „Speicherprogrammierbare Steuerungen“ in IEC/SC 65B/WG 7 und in Deutschland in DKE/AK 962.0.3 „SPS Sprachen“.
- Die direkte Übernahme von Konsortialspezifikationen. In diesem Fall wird die Spezifikation innerhalb eines Konsortiums erarbeitet und dann weitgehend unverändert in eine Norm übernommen. Beispiele sind z. B. die Übernahmen der Batch-Control-Spezifikation ISA S 88 (ISA) in IEC 61512, der OPC-UA-Spezifikation in IEC 62541 oder der PROLIST- Spezifikation in IEC 61987.
- Die konsensbasierte Entwicklung in nationalen Gremien mit anschließender Weiterentwicklung in den zuständigen Normungsgremien. In diesem Fall werden die grundlegenden Festlegungen in den Fachverbänden vorbereitet und als Richtlinien oder nationale Spezifikationen veröffentlicht und dann in einem zweiten Schritt von den zuständigen Normungsgremien zu internationalen Normen weiterentwickelt.

Die alternativen Wege sind in Bild 5.4.2 dargestellt. Nationale Normung im Bereich der elektrotechnischen Normung basiert heute zu 90 Prozent auf internationale Normen der IEC. IEC-Normen werden während der Erarbeitung parallel europäisch (CENELEC5) und international abgestimmt und anschließend national als DIN-Normen übernommen (Dresden -Vereinbarung). Bei ISO und CEN gibt es mit der Wiener Vereinbarung eine vergleichbare Vorgehensweise.

In den letzten Jahren hat sich gezeigt, dass die Entwicklung und Ausarbeitung von Normvorschlägen und Norminhalten durch die zuständigen Normungsgremien selbst zunehmend an ihre Grenzen stößt. In vielen Fällen reicht dazu das zeitliche Kontingent der ehrenamtlich mitarbeitenden Gremienmitglieder nicht aus. Aus diesem Grund hat sich der Weg einer weitreichenden Normvorbereitung durch Konsortien und Fachverbände als Alternative in vielen Bereichen etabliert. Diesen Weg wird die Plattform Industrie 4.0 bezüglich inhaltlich relevanter Teilergebnisse beschreiten.

Die für die Normung zuständigen Gremien übernehmen dabei die Aufgabe der Prüfung, Moderation, Begleitung, Beratung und Integration. Sie stellen sicher, dass die interessierten Kreise über die Inhalte und die geplanten Vorgehensweisen informiert werden und der Normungsprozess konsensbasiert erfolgt. Neben diesen Aufgaben und dem verwaltungstechnischen und redaktionellen Tagesgeschäft übernehmen Normungsgremien zunehmend die wichtige Rolle bei der Analyse der bestehenden Normlandschaft und der Initiierung und Koordination von Normungsvorhaben in strategisch wichtigen Bereichen. Hier waren sie von Beginn der Arbeiten im Plattformprojekt Industrie 4.0 sehr hilfreich. Auch bei den nun anstehenden Fragen zur Verwertung von Ergebnissen sind sie unverzichtbar.

Vergleicht man die Zielsetzung von Konsortien und Fachverbänden in der Standardisierung, dann lässt sich ein prinzipieller Unterschied feststellen: Konsortien versuchen in

einer Festlegung eine vollständige Lösung zu beschreiben, Fachverbände zielen auf die Erstellung von Richtlinien oder die Standardisierung von einzelnen Lösungsaspekten. Im Umfeld von Industrie 4.0 benötigt man beide Richtungen. Im nationalen Umfeld gibt es eine Reihe relevanter Fachverbände. In vielen Fällen sind sie so breit aufgestellt und intern konsensbasiert organisiert, dass ihre Veröffentlichungen als gemeinsame Meinung der entsprechenden Fachgemeinde verstanden werden kann und damit eine besonders sichere und stabile Grundlage sowohl für den weiteren Normungsprozess als auch für die sofortige industrielle Nutzung darstellen. Dies macht sich die Plattform zunutze. Von einer konsensbasierten Vorgehensweise soll hier gesprochen werden, wenn folgende Voraussetzungen erfüllt sind:

- Die Ausarbeitung der Spezifikationen erfolgt in Gremien, in denen jeder Fachmann mitarbeiten kann. Die Mitgliedschaft in einer Organisation ist nicht Voraussetzung. Muss die Anzahl der Mitarbeiter begrenzt werden, erfolgt die Auswahl nach einem transparenten und nicht diskriminierenden Verfahren.
- Die Ergebnisse des Gremiums werden frühzeitig als Entwürfe (Draft for comment) veröffentlicht. Sie können von jedermann unabhängig von der Mitgliedschaft in einer Organisation bezogen und kommentiert werden.
- Vor einer Veröffentlichung als Spezifikation gibt es ein Einspruchsverfahren, bei dem jedermann einen Einspruch formulieren kann. Über die Berücksichtigung des Einspruchs entscheidet das Gremium in offener Diskussion.

Die beschlossene Spezifikation wird veröffentlicht und kann von allen Interessierten unabhängig von der Mitgliedschaft in einer Organisation bezogen werden.

Mit konsensbasierten Spezifikationen lässt sich also zunächst auf nationaler Basis zeitnah eine solide Standardisierungsgrundlage für die Entwicklungsprozesse in den Unternehmen bereitstellen. Diese Spezifikationen sind dann ein guter Ausgangspunkt für die internationale Normung. Insofern ist die Entwicklung des Konzepts zu Industrie 4.0 u.a. in Form eines Referenzmodells innerhalb der Plattform Industrie 4.0 und dessen Überführung in die internationale Normung konsequent.

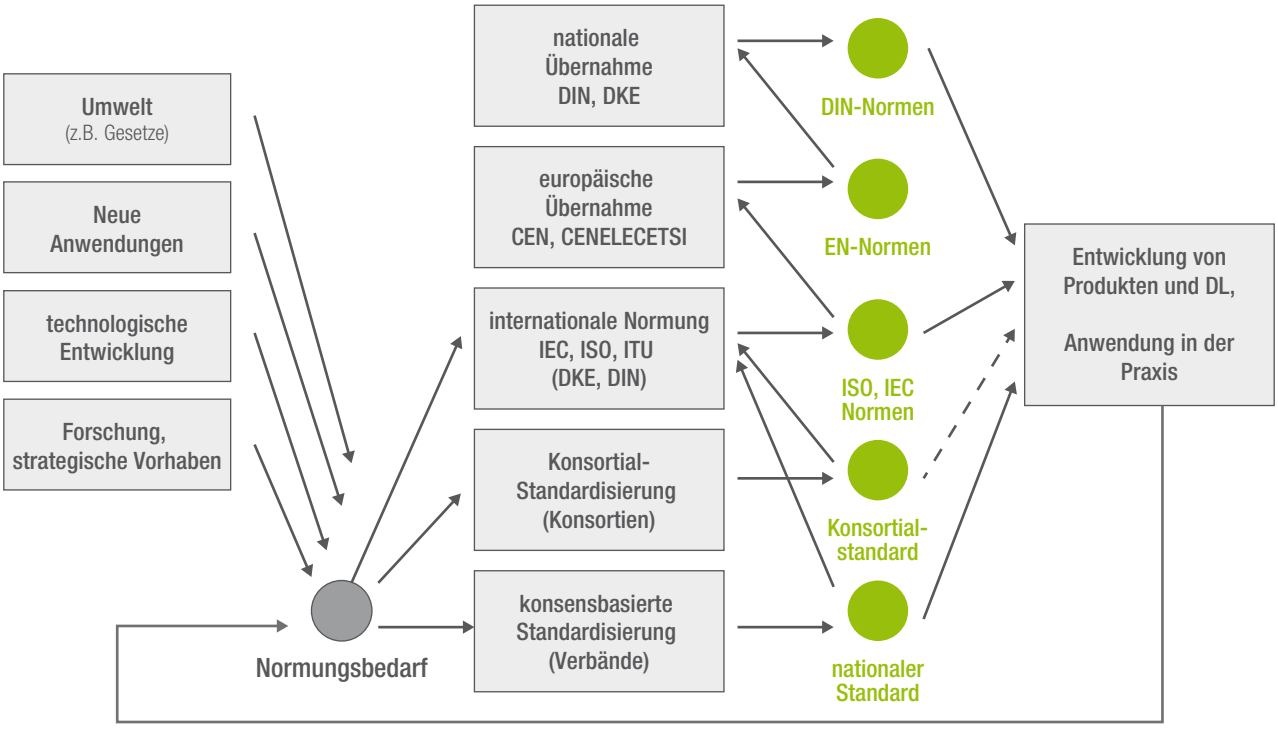


Abbildung 30: Vom Normungsbedarf zur Norm (entspricht [10])

Document Number	Title	Committee
ISO/IEC 62264	Enterprise-control system integration	IEC TC65
IEC TR62794	Industrial-process measurement, control and automation – Reference model for representation of production facilities (Digital Factory)	IEC TC65
IEC 62832	Industrial-process measurement, control and automation – Reference model for representation of production facilities (Digital Factory)	IEC TC65
IEC 62541	OPC Unified Architecture	IEC TC65
IEC 61360-1 IEC 61360-2	Standard data element types with associated classification scheme for electric items	IEC SC3D
ISO 13584-42	Industrial automation systems and integration – Parts library – Part 42: Description methodology: Methodology for structuring parts families	ISO TC184
IEC 61987	Industrial-process measurement and control – Data structures and elements in process equipment catalogues	IEC TC65
IEC 62683	Low-voltage switchgear and controlgear – Product data and properties for information exchange	IEC TC17B
IEC 61804-1 IEC 61804-3	Function blocks (FB) for process control – General requirements Function blocks (FB) for process control – Part 3: Electronic Device Description Language (EDDL)	IEC TC65 IEC TC65
IEC 62453	Field device tool (FDT) interface specification	IEC TC65
IEC 62769	Devices and integration in enterprise systems; Field Device Integration	IEC TC65
IEC 62714	Automation ML	IEC TC65
ISO/IEC 2700x	Information technology – Security techniques – Information security management systems – Requirements	ISO/IEC JTC1
ISO 15926	Industrial automation systems and integration – Integration of life-cycle data for process plants including oil and gas production facilities	ISO TC184
ISO 8000	Data Quality	ISO TC184
IEC 62439	Industrial communication networks – High availability automation networks	IEC TC65
IEC 62443	Industrial communication networks – Network and system security	IEC TC65
ISO 15926	Industrial automation systems and integration – Integration of life-cycle data for process plants including oil and gas production facilities	ISO TC184
IEC 61158	Industrial communication networks – Fieldbus specifications	IEC TC65
IEC 61784	Industrial communication networks – Profiles	IEC TC65
IEC 62591 IEC 62601 EN 300328	Industrial communication networks – Wireless communication network and communication profiles – WirelessHART™ Industrial communication networks – Fieldbus specifications – WIA-PA communication network and communication profile Elektromagnetische Verträglichkeit und Funkspektrumangelegenheiten (ERM) - Breitband-Übertragungssysteme - Datenübertragungsgeräte, die im 2,4-GHz-ISM-Band arbeiten und Breitband-Modulationstechniken verwenden	IEC TC 65 IEC TC65 ETSI

Document Number	Title	Committee
IEC 62591 IEC 62601	Industrial communication networks – Wireless communication network and communication profiles – WirelessHART™ Industrial communication networks – Fieldbus specifications – WIA-PA communication network and communication profile	IEC TC 65 IEC TC65
IEC 61984	Connectors – Safety requirements and tests	IEC TC65
IEC 61508	Functional safety of electrical/electronic/programmable electronic safety-related systems	IEC TC65
IEC 61511	Functional safety – Safety instrumented systems for the process industry sector	IEC TC65
IEC 62061	Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems / This document and its separate amendments continue to be valid together with the consolidated version	IEC TC44
VDMA 24582	Fieldbus neutral reference architecture for Condition Monitoring in production automation	VDMA
ecl@ss V9.0	Database with product classes and product properties	ecl@ss
IEC CDD	IEC Common Data Dictionary	IEC SC3D
PROFIBUS International Profile 3.02	Profile for Process Control devices	Profibus International
Sercos	Function Specific Profiles	Sercos International
Recommendation 5th Edition 2008	XML	W3C
Recommendation 5th edition 2014	HTML5	W3C
VDI 5600	Fertigungsmanagementsysteme	VDI
…..	…..	…..

Tabelle 1: Offene Liste von als relevant eingestuften Normen für Industrie 4.0

6.4.4 Schlussfolgerungen

Die Entwicklung konsensbasierter Normen wird von den zuständigen Gremien weltweit langfristig und nachhaltig unterstützt. In Deutschland sind dies insbesondere DKE und DIN, in Europa ETSI, CENELEC und CEN und international IEC und ISO. Neben diesen mit Mandat versehenen Normungsgremien treiben insbesondere die konsensbasierten Standardisierungsgremien im Verbund mit den in der Plattform Industrie 4.0 organisierten Industrieverbänden durch Ausarbeitung von Spezifikationen und Normvorlagen die Normung voran. Dies ist national z. B. VDI/GMA. Die bewährte Zusammenarbeit der unterschiedlichen Gremien unterstützt die Überführung der Ergebnisse des Plattformprojekts Industrie 4.0 in gewohnter Weise.

Mit Industrie 4.0 kommen jedoch auch neue Themenfelder und insbesondere ein system-orientiertes Vorgehen in den Fokus. Ebenen- und domänenübergreifende Konzepte werden entwickelt und dann auch genormt. Als Ergebnis der bisherigen Arbeiten lässt sich feststellen, dass Industrie 4.0 auf einer ganzen Reihe von Konzepten aus existierenden Normen aufbauen kann. Sicherlich sind einige davon zu modifizieren, andere zu erweitern und auch neue Normen zu schaffen. Das existierende Normenumfeld wird den Migrationsweg von Industrie 3.0 zu Industrie 4.0 aber nachhaltig unterstützen. Eine offene Liste potenziell relevanter Normen zeigt die Tabelle. Diese Liste mit u.a. wesentlichen Normen der Automatisierungstechnik wird schrittweise z. B. um ICT-Normen erweitert und in der Neuausgabe der Normungs-Roadmap „Industrie 4.0“ von DKE und DIN in überarbeiteter Form veröffentlicht.

6.5 Themenroadmap

Mit der Erarbeitung und Diskussion des Referenzarchitekturmodells Industrie 4.0 (RAMI4.0) und der Industrie 4.0-Komponente sind nun erste Grundlagen für die weitere Arbeit geschaffen. Wichtige anstehende Themen sind im Folgenden beschrieben. Ein wichtiges Ziel dabei ist die Verbesserung der Interoperablilität auf der Anwendungsebene einerseits und die Verbesserung der Netzqualität entsprechend der Anforderungen aus Industrie 4.0 andererseits.

Identifikation

Die Identifikation ist eine notwendige Voraussetzung, damit sich Dinge selbstständig finden können. Die ersten Diskussionen haben bereits gezeigt, dass eine Identifikation im Warenverkehr, eine Identifikation des Ortes und eine Identifikation innerhalb des Netzwerkes benötigt wird. Hier existieren unterschiedliche Standards und Normen, teilweise werden aber auch Ergänzungen mit neuen technischen Möglichkeiten diskutiert werden.

Semantik

Ein wichtiger Layer im RAMI4.0 stellt der Information Layer da. Hier sind u.a. die Daten abgelegt. Für einen herstellerübergreifenden Datenaustausch wird eine einheitliche Sematik inkl. Syntax für die Daten benötigt. Erste Überlegungen existieren, ein Konzept für die gesamte Ausgestaltung einschl. Normung gilt es nun zu erstellen. Als Basis für eine umfassende Merkmalsdefinition „Industrie 4.0“ bietet sich z. B. die Merkmalsspezifikation von eCl@ss an.

Quality of Services (QoS) / Dienstqualitäten der Industrie 4.0-Komponente

Damit werden wichtige Eigenschaften der Industrie 4.0-Komponente festgelegt. Sie sind einstellbar bzw. abrufbar. Zwischen den Komponenten sollen auch Vereinbarungen von Dienstqualitäten möglich sein. Bzgl. der Anwendungen in der Automatisierungstechnik sind dies Eigenschaften wie Echtzeitfähigkeit, Ausfallsicherheit, Uhrensynchronisation, u.a. Solche Eigenschaften können in Profilen beschrieben werden.

Industrie 4.0-Kommunikation

Kommunikationsverbindungen und Protokolle gibt es in der Automatisierungstechnik und der Informationstechnik bereits sehr viele. Dazu kommen neue Verfahren aus der Telekommunikations- und Informationstechnik. Alle müssen entsprechend den Anforderungen an eine Industrie 4.0-Kommunikation auf ihre Eignung geprüft und ggf. angepasst werden. Hier bietet sich zur Strukturierung der Communication Layer aus RAMI4.0 an. Anhand der Kommunikation läßt sich das Vorgehen zur Identifikation geeigneter Normen gut erklären. Zur Normenfindung werden z. B. alle geeigneten Kandidaten in den Layer eingetragen. Überschneidungen werden diskutiert und Vorzugsprotokolle definiert. Eventuelle Lücken werden geschlossen.

Standardfunktionen:

Eine größere Herausforderung ist die Ausbildung von herstellerübergreifenden Standardfunktionen, die auf dem Functional Layer von RAMI4.0 abgebildet sind.

Für einen einfachen Austausch von Informationen und für die Interoperabilität zwischen Herstellern ist die Festlegung einheitlicher Basisfunktionen notwendig. Einfache und für den Austausch von Informationen wichtige Funktionen müssen daher offen spezifiziert sein. Dies senkt für den Anwender die Schnittstellenanpassungskosten in seinen Maschinen/ Anlagen/ Fabriken deutlich. Als Beispiel kann hier das Einheitsblatt vom VDMA bzgl. der Festlegung von Condition Monitoring dienen. Dort sind hersteller-übergreifende Standardfunktionen festgelegt, aber auch ein Modell, in das jeder Hersteller seine eigenen Funktionen einbringen (kapseln) kann. Dabei bleiben der Datenaustausch und eine Verknüpfung von Condition Monitoring Funktionen leicht möglich.

Sicherheit vernetzter Systeme

7 Sicherheit vernetzter Systeme

7.1 Einleitung

Security ist der „Enabler“ für Industrie 4.0-Wertschöpfungsnetzwerke. Maßgeblich für den Entwicklungsprozess hin zur Industrie 4.0 ist es, dass sich lineare Wertschöpfungsketten zu Wertschöpfungsnetzwerken wandeln. Die so vollständige Vernetzung aller Wertschöpfungspartner führt dazu, dass in einem bisher unbekannten Maße mehr Akteure tiefer und zum Teil auf ad hoc Basis in die Unternehmens- und Fertigungsprozesse einzubinden sind. Um die angestrebten Effizienz- und Produktivitätsgewinne zu erzielen, müssen die Partner sensible Produktions- sowie Prozessdaten mit einander austauschen können. Dies kann nur auf der Basis von Vertrauen zwischen den Partnern geschehen, da zentrales Know-how – d.h. das Kern-Asset jedes Unternehmens – wenigstens anteilig zu teilen ist. Vertrauen entsteht, wenn die Informationen und Daten sicher und korrekt nachweislich zwischen den tatsächlich berechtigten Partnern ausgetauscht werden können. Das zu gewährleisten ist Aufgabe der Security in der Industrie 4.0. Ohne eine sichergestellte Security in den Office- und Produktionssystemen ist Industrie 4.0 nicht umzusetzen, da kein Vertrauen für die sensiblen Kommunikationsprozesse entstehen kann.

Zusätzliche Herausforderung an die Security ist es, die Implementierungen nicht nur sicher, sondern auch benutzer- sowie anwendungsfreundlich zu gestalten, um die Akzeptanz der Kunden zu gewinnen. Diese wünschen am Ende eine Plug&Operate Vorgehensweise. Zudem steigt im Zuge der individuellen Kundenabstimmung mit Industrie 4.0 der unmittelbare Einfluss der Kundenwünsche auf den Produktionsverlauf (siehe z. B. Losgröße 1 in der Automobilherstellung). Kann die notwendige enge B2B und B2C Kommunikation nicht sicher, korrekt und rechtssicher verlaufen, sind die angestrebten Geschäftsmodelle schwer realisierbar. Security-Maßnahmen werden die Basis legen, die Anforderung erfüllen zu können.

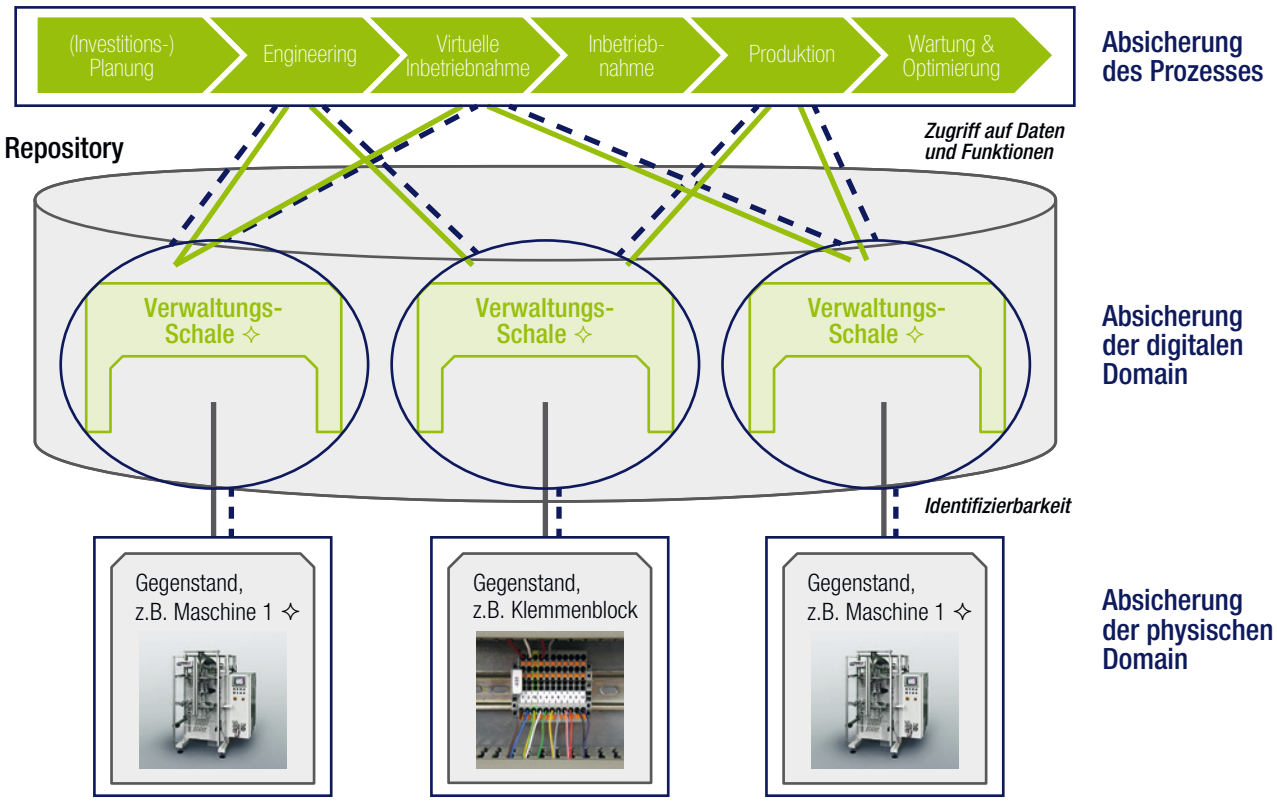


Abbildung 31: Sicherheitsanforderungen

Übertragen auf die technische Ebene der aktuellen Industrie 4.0-Entwicklung gilt daher folgender Grundsatz:

Die übergreifende Absicherung der physischen und digitalen Domain, der jeweiligen Prozesse sowie der Kommunikation zwischen diesen Bereichen ist Voraussetzung für das Gelingen der Industrie 4.0. Denn eine isolierte Umsetzung der Security ist leicht zu umgehen und wäre wirkungslos.

Sicherheit geht alle an

Unternehmen sind herausgefordert, eine unternehmensinterne und externe Mehrdimensionalität zu managen. Intern wird es mit Industrie 4.0 ein „Silo-Denken" im Sinne eines statischen linearen Organigramms nicht mehr geben können. Denkbar ist, dass beispielsweise Produktionsprozesse integraler Bestandteil der ERP-Ebene werden (siehe Produktionsnetze werden zunehmend integraler Bestandteil des Enterprise Networks). Langfristig bedingt diese Entwicklung eine Verschmelzung von Office-IT und Produktion-IT und damit zur notwendigen Aufgabe der statisch-linearen Unternehmensorganisation. Entsprechend wird es mehr Aufgaben geben, die als Querschnittsthema durch alle Bereiche zu führen und in diese zu integrieren sind. Ein durchgängiges und fortlaufendes Risiko- und Sicherheitsmanagement im Unternehmen wird mit Industrie 4.0 unerlässlich sein. Die Mehrdimensionalität entsteht, da diese Managementaufgaben nicht mehr in „intern" und „extern" aufzuteilen sind. Das Risiko- und Sicherheitsmanagement muss die Veränderungen bei Industrie 4.0 abbilden, durch die externe Akteure verstärkt unmittelbaren Einfluss auf traditionell interne Prozesse nehmen können. Der klassisch „eingezäunte" und dadurch bestimmbare Unternehmensbereich löst sich auf. In einem Wertschöpfungsnetzwerk sind die Übergänge von internen und externen Unternehmensbereich fließend und über die Zeit variabel.

Vor diesem Hintergrund kann ein Unternehmen nicht mehr allein für die eigene Sicherheit sorgen. Selbst wenn es alle denkbaren Vorkehrungen trifft, kann es nicht als sicher gelten. Durch die enge Verzahnung mit Kunden und Zulieferern, wo die entsprechenden Schnittstellen als Angriffsmöglichkeit dienen können, beeinflusst das Security-Management der Kunden und Zulieferer auch den eigenen Schutzlevel. Noch viel stärker als heute beeinflusst das schwächste Glied die Sicherheit des gesamten Wertschöpfungsnetzwerks. Folglich muss als Grundsatz gelten, dass mit Industrie 4.0 Sicherheit alle angeht. Security ist eine gemeinschaftliche Verantwortung, die von keinem Akteur allein mehr zu leisten ist – unabhängig davon wie groß das jeweilige Unternehmen ist.

Security ist ein Moving Target

Die Notwendigkeit einer mehrdimensionalen Betrachtung der Security in der Industrie 4.0 basiert zusätzlich auf einem technischen Prinzip, das bereits heute gilt, aufgrund der noch zahlreicheren Schnittstellen an Relevanz aber zunehmen wird. Security muss als „Moving Target" verstanden werden. Die Kernfragen „Worauf muss ich mich einstellen?" und „Welche Maßnahmen sind zu ergreifen?" sind immer wieder neu zu evaluieren. Denn jede Sicherungsstrategie verursacht, dass eine entsprechende Gegenstrategie entworfen wird, die wiederum die Sicherungsstrategie beeinflusst. Zudem verändert der technische Fortschritt die Angriffsmethoden und -möglichkeiten permanent. Jede technische und personelle Maßnahme kann mit entsprechendem Aufwand durch technische und personelle Maßnahmen umgangen werden. Für die Security ergibt sich somit eine stets wandelbare, dynamische Bedrohungslage, die eine stetige Adaptionen verlangt. Eine wirksame Security-Implementierung im Sinne eines „Einrichten und vergessen" kann es nicht geben. Dies ist unter anderem auch ein elementarer Unterschied zu den Prinzipien der Safety/Betriebssicherheit (= Schutz des Menschen vor der Maschine). Die Safety-Bestimmungen basieren auf festen und zum Teil gesetzlich vorgeschriebenen Regelungen und statistisch bewertbaren Annahmen.

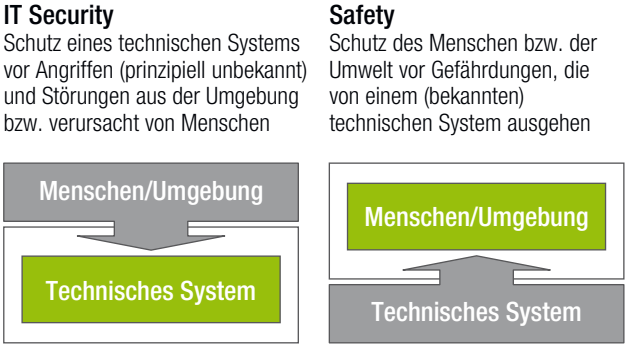


Abbildung 32: IT-Security vs. Safety

Die hohe Dynamik des Security-Umfelds in Industrie 4.0-Wertschöpfungsnetzwerken verlangt einen effizienten und anpassungsfähigen Security-Ressourceneinsatz. Basis hierfür ist das Wissen um die eigenen Werte im Unternehmen sowie deren Schutzbedarf. Allein aus Gründen der Wirtschaftlichkeit müssen Security-Maßnahmen nicht nur wandelbar, sondern auch passgenau sein. Nicht alle Assets müssen beispielsweise „hochsicher" geschützt werden. Den erforderlichen Maßnahmen-Mix kann eine Unternehmensführung nur durch ein fortlaufendes Risikomanagement umsetzen. Zu klären ist: Was sollte mit welchen Aufwand und Schutzbedarf abgesichert werden? Die Bewertungsergebnisse dienen als Orientierung für alle weiteren Maßnahmen und sollten in größeren Abständen regelmäßig evaluiert werden.

Eine 100-Prozent-Security für Industrie 4.0 wird es nicht geben

Die Dynamik des „Moving Target" sowie des technischen Fortschritt bedeuten, dass Security 1) als Einheit aus Technik, Menschen und Prozess sowie 2) als spezifische Einzelfallbetrachtung vor Ort verstanden werden muss. Security lässt sich nicht als Produkt fertig kaufen. Die notwendigen Ausprägungen der Sicherheitsmaßnahmen sind stark unternehmensspezifisch. Für das Thema Security ist daher grundsätzlich festzuhalten, dass es keine allgemeingültige Lösung geben kann.

7.2 Annahmen, Hypothesen und Voraussetzungen

Auch wenn die einzelnen Architekturen, Modelle und Anlagen der Industrie 4.0 noch nicht feststehen, lässt sich ein technischer Trend verlässlich annehmen: Die automatisierte und unternehmensübergreifende Kommunikation zwischen einzelnen Industriekomponenten wird zunehmen. Dies bringt insbesondere aus Security-Sicht mehrere Konsequenzen mit sich. Die Bestimmbarkeit der Einheit „abgeschlossene Fabrik" verschwimmt. Eine klare Abgrenzung zwischen internen und externen Verantwortungsbereichen wird immer schwieriger. Dies gilt sowohl im physischen wie im digitalen/informationstechnischen Sinne. Bestehen in einem Industrie 4.0-Wertschöpfungsnetzwerk sehr enge Kommunikationsprozesse zwischen Zulieferer und Hersteller, wo ggf. unter Echtzeitbedingungen produktionsrelevante Entscheidungen getroffen werden, kann ein Zulieferer unter Umständen unmittelbaren Einfluss auf die Abläufe beim Hersteller nehmen. Prozessstörungen können sich so gegenseitig bewirken. Die Kontrollierbarkeit und Beherrschbarkeit der internen Abläufe nimmt ab und es steigt die gegenseitige Abhängigkeit. Die ausschlaggebende Einflusssphäre, die konkrete Auswirkungen auf die eigenen Unternehmensbereiche hat, geht über die eigene Handlungskompetenz hinaus.

Das Fabrikgelände geht nun über den Werkszaun hinaus. Bisher konnte man Zu- und Ausgänge sowohl für die physische Domäne (Zaun + Pförtner/Wachdienst) und informationstechnische Domäne (Trennung von Intra- und Internet, Einführung von DMZs) kontrollieren. Das klassische Zonenkonzept wird sich mit Industrie 4.0 jedoch dahingehend verändern müssen, dass es dynamisch und gegebenenfalls ad hoc definierbar ist.

Security-Hypothesen

Diese Entwicklungen führen zusammen mit den in Kapitel 7.1 dargestellten Kernaussagen zu fünf Security-Hypothesen. Die Hypothesen sollten bei der Konzeption künftiger Architekturen und Modelle für Industrie 4.0 von Beginn an mitgedacht werden:

1. Das Wertschöpfungsnetzwerk an sich wird zum möglichen Angriffsvektor

   Das eigene Unternehmen mag mit umfangreichen Mitteln auf der Kommunikations- und Fertigungsebene geschützt sein. All dies kann schnell zur Makulatur werden, wenn die Systeme der Zulieferer und Kunden nicht ebenfalls auf einem verlässlichen Niveau abgesichert sind. In einer Industrie 4.0-Umgebung muss man damit rechnen, dass Angriffe und Störfälle durch die Systeme externer Partner erfolgen können. Eine reine „Innenbetrachtung" des selbst kontrollierten Bereichs reicht nicht mehr aus. Insbesondere in den Fällen, in denen beispielsweise die Zulieferpartner wechseln, sollten von Beginn an Vorkehrungen, Security-Abstimmungen und Prüfungen in angemessener Weise Bestandteil der Geschäftsvereinbarung und -beziehung sein. Gegenseitige (vertragliche) Vereinbarungen über Sicherheitsvorkehrungen sind dafür erforderlich.

2. Die Verletzlichkeit von Safety-Funktionen nimmt zu

   Durch den steigenden Vernetzungsgrad auf allen Ebenen industrieller Produktion wachsen korrespondierend die potentiellen Möglichkeiten der Manipulation und Sabotage in ihrer Anzahl und Wirkungstiefe. Es ist zunehmend denkbar, dass unberechtigte Eingriffe bis hinein in die eigentliche Funktionssteuerung der Maschinen und Anlagen erfolgen. Im extremen Fall gibt es keinen Bereich mehr, der nicht manipulierbar ist.

   Steigt mit Industrie 4.0 die Durchdringung der Digitalisierung bis in die tiefsten Funktionssteuerungen der Maschinen und Anlagen, die eventuell auch Safety-Funktionen (z. B. Notfall-Abschaltung, Klemmschutz, elektrische Abschirmung, Verbrennungsschutz etc.) umfassen, werden letztere ebenfalls angreifbar. Bisher werden Safety-Funktionen getrennt und zum Teil redundant eingerichtet, um höchste Verfügbarkeit und Verlässlichkeit zu gewährleisten. Die Vernetzung im Industrie 4.0-Umfeld kann nun dazu führen, dass mehr technische Schnittstellen und „Berührungspunkte" zwischen Safety- und sonstigen Vorrichtungen existieren. Die Systeme werden auf diese Art theoretisch zugänglicher. Dies bedeutet, dass durch einen Security-Vorfall (z. B. externer Hacker-Angriff) ein Safety-Vorfall verursacht werden kann (z. B. Manipulation der Lichtschrankensteuerung eines Klemm- und Quetschschutzsystems bei einer Metallpresse). Die bisher absichtliche Trennung oder Kapselung von Safety- und sonstigen Systemen hebt sich auf. Das bisherige Gebot der Störungsfreiheit wird zugunsten der Flexibilität immer schwerer zu gewährleisten sein.

   Hohe Brisanz hat dieses Verhältnis in Gebieten, wo Menschen mit Maschinen eng zusammenarbeiten, wie zum Beispiel in der robotergestützten Fertigung. Folglich müssen die bisher eher getrennt voneinander betrachteten – heute nur für Safety genormten – Bereiche verstärkt als interdependent verstanden und darauf die Schutzkonzepte angepasst werden.

3. Detektions- und Reaktionsfähigkeiten gehören zur Grundausstattung

Die Auswertung verschiedener Security-Vorfälle zeigt deutlich, dass jede Schutzmaßnahme mit einem entsprechenden Aufwand zu umgehen ist. Die Kernaussage „es gibt keine 100-Prozent-Security" bedeutet, dass jedes Produkt und jede Maßnahme keine abschließende Sicherheit gewährleisten kann. Die durchschnittliche Zeit zur Erkennung eines Angriffs beträgt heute mehrere hundert Tage, dabei wird eine zunehmende Anzahl von Angriffen nicht vom betroffenen Unternehmen erkannt.

Selbst die Kombination von unterschiedlichen technischen und organisatorischen Maßnahmen stößt an Grenzen, wenn potentielle Angreifer über viel Zeit, Recherche- und Security-Kompetenz verfügen (sogenannte APT-Angriffe). Derartige zielgerichtete und langwierige Attacken sind darauf ausgerichtet, von den gängigen Sicherungsmaßnahmen unentdeckt zu bleiben.

Staatlich unterstützte Organisationen gehen auf eine ähnliche Weise vor, ihre Angriffsmöglichkeiten – etwa auf Prozesse wie Vertrauensbeziehungen, Personen und Technologien sind jedoch noch einmal deutlich weitreichender. Die Verhinderung eines solchen Angriffs kann je nach dessen Professionalität wirtschaftlich nicht vertretbar sein.

Im Spektrum der gewöhnlichen Angriffe und Cyber-Kriminalität steigt das Niveau der Fähigkeiten ebenfalls. Früher oder später wird sich ein Vorfall ereignen. Die alles abschirmende Firewall wird es nicht geben. Dies bedeutet, dass im Bedarfsfall auch Fähigkeiten existieren müssen, um Vorfälle zu erkennen, darauf zu reagieren und diese schnellstmöglich beheben zu können. Die Robustheit von Sicherheitsmaßnahmen als dem Zusammenwirken von präventiven und reaktiven Maßnahmen (Detektionsfähigkeiten sind implizit eingeschlossen) werden unter der eingangs erwähnten Annahme entscheidend für die Security der Industrie 4.0 sein. Auch künftig werden professionelle Angriffe voraussichtlich nicht schnell oder gar in Echtzeit feststellbar sein. Vor allem im mittelständischen Bereich kann es verstärkt die Situation geben, dass Unternehmen auch erst nachträg-

lich durch Externe von einem Sicherheitseinbruch und neuen Angriffsmöglichkeiten erfahren. Eine notwendige Stärkung der Detektions- und Reaktionsfähigkeiten erlaubt es jedoch, APT-Angriffe während oder nachdem sie geschehen sind, zu erkennen oder wenigstens im Nachhinein deren Umfang und Wirkungstiefe zutreffend zu bewerten und die Reaktionsmaßnahmen zu verbessern. Damit werden Unternehmen in die Lage versetzt sowohl mehr zu erkennen, was die Sensibilität erhöhen dürfte, als auch effizienter und damit kostengünstiger zu reagieren.

4. Die aus dem Office-Bereich bekannten Detektionsfähigkeiten müssen für den Produktionsbereich entwickelt und bereitgestellt werden

   Derzeit besteht ein Fokus auf der Absicherung von Office-Kommunikationssystemen. Dies ist der Situation geschuldet, dass die bisher gängigen Angriffsvektoren und Schwachstellen sich auf Office-Systeme beziehen (z. B. Betriebssysteme, Browser, internetbasierte Kommunikation, Datenträger usw.). Folgerichtig fokussieren die gängigen Schutzmaßnahmen genau diese Bereiche (z. B. Virenscanner, Email- und Festplattenverschlüsselung, Kontrolle von Datenverkehr und Datenzugriffen etc.). Für die industrielle Kommunikation im Produktionsbereich existieren derartige Umsetzungen wie „Intrusion-Detection-Systeme“ in der Fläche nicht. Industrieangriffe wie Stuxnet zeigen, dass derartige Programme Monate oder Jahre lang aktiv sein können, bevor sie entdeckt werden.

   Unternehmen haben aus Know-how-Schutz-Gründen ein starkes Interesse, informiert und handlungsfähig sein. Entsprechend sind derartige „Blinde Flecken“ auf der Security-Karte zu identifizieren und systematisch abzubauen. Das heißt auch, dass organisatorische, personelle und technische Security-Investitionen in bisher nicht beachteten Feldern zu leisten sind.

5. Mit Industrie 4.0 wird die verteilte Datenhaltung zur zentralen Security-Herausforderung

   Viele Dienste und Services können durch die Anwendung von Big Data, Predictive Analytics und intelligenter Sensorik neu in der Industrie 4.0 entstehen. Die Einbeziehung von Datenexperten und Auswertungsprogrammen soll Effizienzpotenziale ermöglichen (z. B. Verminderung des Materialausschusses bei Metallpressen durch datengestützte Anpassung des Stanzprozesses). Für die Analysen wird sehr spezifisches Prozess-, Maschinen- und Anlagen-Know-how notwendig sein. Das bedeutet, dass Betreiber gegebenenfalls ihre Daten externen Dienstleistern und/oder den Herstellern zur Analyse überlassen bzw. diese sich über Schnittstellen in den Datenverkehr integrieren. Darüber hinaus ermöglichen Cloud- und sonstige Datenplattformen eine ortsunabhängige Industriesteuerung und Produktion.

   Die Datenerzeugung, -übertragung und -verarbeitung in der Produktion findet unter Umständen digital und über externe Plattformen statt. Das stellt die Betreiber verstärkt vor technische, security-betreffende und rechtliche Herausforderungen. Das Unternehmen verwendet ggf. eine zusätzliche kritische Infrastruktur, bezieht einen zusätzlichen externen Akteur mit ein und kann dessen Einfluss auf die Daten nur bedingt kontrollieren. Ist der Anbieter der Datenplattform außerhalb des eigenen Rechtsraums, sind zudem vertragliche Bestimmungen und Sanktionen schwerer zu implementieren. Aufgrund der notwendigen, permanenten technischen Zugänglichkeit derartiger Plattformen, entsprechend der Anforderungen eines Wertschöpfungsnetzwerks mit vertikaler und horizontaler Vernetzung, ergibt sich eine Vielzahl an möglichen Angriffsvektoren. Ohne eine umfassende Gewährleistung des Datenschutzes sowie der Informationssicherheit wird eine verteilte Datenhaltung in der Industrie 4.0 kaum zu realisieren sein.

Grundsatz der Security-Entwicklung: Security wird als Migration und in Abhängigkeit von der Ausgangslage in den Unternehmen umgesetzt.

Die formulierten Hypothesen werden sich kontextbezogen und nicht losgelöst von der existierenden Ausganglage entwickeln. Alle Security-Konzepte werden auf bestehenden Systemen und Anlagen aufbauen. Der grundlegende Wandel vom Security als untergeordnetes, nachträgliches Thema hin zum „Security-by-Design“-Ansatz wird sich graduell und über die verschiedenen Anlagen- und Komponen-

tengenerationen vollziehen. Gleiches gilt für die Weiterentwicklung der Security-Standards und Normen. Vielerorts ist eine Anpassung bestehender Regularien anstatt der Erstellung völlig neuer Standards von Nöten. Security-Features werden auch weiterhin als reiner Kostenfaktor in Unternehmensentscheidungen einfließen. Entsprechend wird es größeren Unternehmen aufgrund der Skaleneffekte leichter fallen, derartige Investitionen zu tätigen und Anlagen auszutauschen, um neue Security-Level zu implementieren. Vor allem kleinere und mittlere Unternehmen können keine umfassenden Investitionen in Security leisten.

Zusätzlich ergeben sich durch Entwicklungen wie intelligente Sensorik kombiniert mit Big Security Data auch neue Möglichkeiten Sicherheitsmaßnahmen in Bereiche zu bringen die heute noch isoliert und proprietär sind, wodurch Manipulationen oft unerkannt bleiben.

7.3 Bedrohungswelt Industrie 4.0

Dass Bedrohungen für die IT in Office- und Produktionsbereich in der heutigen Welt bestehen, kann nicht mehr bestritten werden. Gerade im letzten Jahr wurden eine Vielzahl von Schwachstellen in Anwendungen und Systemen offengelegt. Damit einhergehend kam es zu diversen erfolgreichen Angriffen auf Unternehmen, die öffentlich geworden sind. Ein Beispiel für Angriffe ist das 2014 bekannt gewordene Schadprogramm „Havex“. Dieses sammelt gezielt Informationen zu industriellen Kontroll- und Steuerungssystemen. Dabei kann es sich um Produktionsanweisungen handeln oder Daten zur Infrastruktur, die für weitere Angriffe verwendet werden können. Es besteht die Möglichkeit, weitere Module nachzuladen, die ggf. zu Schäden an einer Anlage führen können.

Im Rahmen dieses Angriffs wurden die Webseiten verschiedener Anlagenhersteller manipuliert. Verbindet sich nun eine Anlage zwecks Software-Update mit der Herstellerseite, wird diese Kommunikation angegriffen. Aus Kundensicht schaut der Angriff also wie eine plausible und legitime Kommunikation zwischen Anlage und Hersteller aus und fällt vermutlich zunächst nicht auf. Da sich auch andere moderne Angriff durch legitime Zugriffe verstecken, stellt die Erkennung von Sicherheitsvorfällen die Unternehmen vor neue Herausforderungen. Oft ist eine Erkennung – wenn überhaupt – nur noch rückwirkend möglich Das kann immer noch deutlich kostengünstiger sein, als die gesamte Infrastruktur komplett neu aufzusetzen. Es ist von einer erheblichen Dunkelziffer weiterer Angriffe auf Unternehmen auszugehen. Die Schäden reichen dabei von Datendiebstählen über Erpressung bis hin zu Schäden an Betriebs- und Produktionsprozessen.

Dies soll verdeutlichen, dass bereits heute Gefahren für Produktionsanlagen bestehen, auf die sich Unternehmen einstellen müssen. Industrie 4.0 bietet mit den einleitend beschriebenen Trends neue Möglichkeiten um die Produktivität und Möglichkeiten von Prozessen und Anlagen zu verbessern. Dazu gehören auch die Verwaltungsschalen der Industrie 4.0-Komponenten. Durch zunehmend dynamische Kommunikation und beteiligte Dienstleister entstehen leider auch neue Angriffsmöglichkeiten und entsprechend neue Bedrohungen. Diese Bedrohungen gelten gleichermaßen für beide Netzwerke: dem der Verwaltung und dem der Automatisierung.

In vielen Fällen sind die Systeme, die besonders schützenswert sind, vom Internet aus nicht zu erreichen, dies gilt häufig auch für den Produktionsbereich. An dieser Stelle verwenden Angreifer gerne eine Zwei-Sprung-Technik: Zuerst wird ein Rechner in einem weniger geschützten Bereich angegriffen, auf dem eine Schadsoftware installiert wird. Von diesem Rechner aus werden dann weitere Angriffe in die Tiefe des Unternehmens ausgeführt. Diese Art der Infiltration ist häufig langfristig angelegt und erfolgt daher minimal invasiv und wird daher erst spät oder nachträglich erkannt. Entsprechende gezielte Angriffe, z. B. Stuxnet, werden als Advanced Persistant Threat „APT“ bezeichnet. Das sogenannte „Air Gap“ stellt keine hinreichende Sicherheit mehr dar.

Bei den Angreifern wird oft zwischen drei Typen unterschieden: Nachrichtendiensten, Cyber-Kriminellen und Cyber-Aktivisten. Cyber-Kriminelle wollen mit ihren Tätigkeiten illegal Geld verdienen. Dies geschieht durch Erpressung von Unternehmen oder Privatpersonen, indem gedroht wird, bestimmte Daten zu löschen oder Systeme zu deaktivieren. Cyber-Aktivisten verfolgen politische oder ideologische Ziele. Dies kann vom Diebstahl und Veröffentlichung von unternehmensinternen Informationen bis hin zu DDoS-Angriffen oder der Deaktivierung von Systemen gehen. Vor diesen beiden Gruppen gilt es, das eige-

ne Unternehmen zu schützen. Bei nachrichtendienstlichen Angreifern ist es aufgrund der fast unbegrenzt vorhandenen Ressourcen für ein Unternehmen wirtschaftlich kaum vertretbar, sämtliche Angriffswege auszuschließen.

Neben diesen gezielten Angriffen sollten sich Unternehmen auch gegen unabsichtlich herbeigeführte Probleme, etwa menschliches Fehlverhalten, oder nicht zielgerichtete Angriffe – etwa „Drive-By Angriffe[13]“ – zu wappnen. Dies kann die Verbreitung von Schadprogrammen zwischen dem Verwaltungs- und Automatisierungsnetz sein oder auch die ungewollte Fehlkonfiguration von Systemen sein.

Die Entwicklung von Angriffs-Software wird immer professioneller und zielt bemerkenswerter Weise zunehmend auf den Bereich der Automatisierung ab. Das Ziel dabei ist zunächst die Spionage. Ein Beispiel dafür ist der Schadcode „BlackEnergy“: Er zielt auf HMI-Systeme bestimmter Hersteller ab, wobei die betroffenen Systeme nach der Veränderung unbemerkt für weitere Analysen missbraucht werden. Der aktuelle Schadcode ist seit etwa dem Jahr 2008 mehrfach überarbeitet und verbessert worden und kann heute modular um zusätzliche Funktionen ergänzt werden. Er wird einer Spionage-Gruppe[14] zugeordnet, die bereits in der jüngsten Vergangenheit auf Schwachstellen in der Programmiersoftware für HMI- und SCADA-Systeme abzielte.

Es kann davon ausgegangen werden, dass auch vor dem erfolgreichen Angriff auf den Hochofen eines deutschen Stahlwerks [8] eine Spionage-Phase vorgeschaltet war – jedenfalls deuten die bisher fehlenden Erkenntnisse zum Angriffsablauf darauf hin.

7.3.1 Werte in den Unternehmen

Um weiter auf die Bedrohungen einzugehen, muss betrachtet werden, was für ein Unternehmen von Wert ist. Im Kontext der Security kann der zentrale Unternehmensnutzen in einer Anlage, einem Anlagenteil, aber auch etwa in Legierungs- und Rezeptdaten oder einem Dienst liegen.

Man konzentrierte sich bisher bei der Produktionsanlage im Wesentlichen auf die Verfügbarkeit. Bei Rezepturen liegt der Fokus auf der Vertraulichkeit. Dies sind nur zwei Beispiele für Assets, die von existenzieller Bedeutung für ein Unternehmen sind, da hier ggf. substanzieller Forschungs- und Entwicklungsaufwand betrieben wurden. Durch die entstehenden Trends und neuen Techniken, die in die Produktion eingeführt bzw. integriert werden, kommen weitere Assets in Form von Diensten hinzu. Dies können IT-Systeme (zur Auftragsannahme oder Produktionskoordination) sein, die vorher noch keine zentrale Rolle gespielt haben, noch gar nicht vorhanden waren oder bisher in abgeschotteten Bereichen betrieben wurden. Beispiele sind digitale Identitäten von Produkten oder Bauteilen oder die rechtssichere Erteilung und Verwaltung von maschinell ausgehandelten Verträgen.

Auf die mit den Trends und Entwicklung in Verbindung stehenden neuen Bedrohungen soll hier im Folgenden etwas genauer eingegangen werden.

7.3.2 Verfügbarkeit und Zuverlässigkeit

Unternehmensprozesse werden durch Systeme unterstützt. Ein System kann beispielsweise eine Maschine, ein Anlagenteil oder auch ein IT-System sein. Eine Verwaltungsschale einer Industrie 4.0-Komponente zählt ebenfalls zu diesem Bereich. Bei Industrie 4.0 ist von einer weiteren Zunahme betriebsnotwendiger Systeme und Schnittstellen unternehmensübergreifender Kommunikation und einer zunehmenden Dynamik der Betriebsprozesse auszugehen.

Sind diese Systeme oder deren Schnittstellen nicht verfügbar, wirkt sich das mehr oder weniger direkt auf Unternehmensprozesse, die Wertschöpfung und damit monetäre Aspekte aus. Kritische Störungen der Produktion oder anderer Dienste stellen ein direktes Unternehmensrisiko dar. Es sind auch Gefahren denkbar, die die Notwendigkeit einer koordinierten Abschaltung von Anlagen erforderlich machen – etwa um physische Schäden zu verhindern.

Ein schwer abzusicherndes Risiko für jede extern erreichbare Schnittstellen stellen Distributed-Denial-of-Service (DDoS) Angriffe dar. Dabei werden so viele Anfragen gestellt, dass beispielsweise der Empfänger mit Anfragen überlastet wird oder die gesamte zur Verfügung stehende Netzwerkbandbreite besetzt wird, so dass legitime

13 Angriffe, bei denen ein Benutzer auf eine präparierte Webseite geleitet wird von der aus eine Schwachstelle im Webbrowser ausgenutzt um die Systeme des Benutzers zu kompromitieren.

14 “Sandworm”

Anfragen nicht mehr verarbeitet werden können. Es gibt bereits Beispiele für Unternehmen, die durch einen lang anhaltenden DDoS-Angriff in Verbindung mit Zugang zu den Systemen in den Bankrott getrieben wurden [8].

Mit Industrie 4.0 gibt es mehr zeitkritische Prozesse und Dienste, damit entstehen zusätzliche Angriffspunkte für DDoS.

Wird in industriellen Umgebungen mit hochdynamischen Daten nahezu in Echtzeit gearbeitet, besteht wenig Raum für die sonst in der Office IT Security üblichen Korrekturmaßnahmen. Die zu verarbeitenden Daten müssen dabei nicht nur genau sein, sie müssen unter Umständen auch zeitlich synchron von verschiedenen Systemen gleichzeitig erhalten und verarbeitet werden. SCADA-Systeme berechnen verschiedene Prozessdaten, die sie von unterschiedlichen Systemen erhalten, automatisiert und leiten ihrerseits Steuerbefehle anhand der Berechnung weiter. Eine Kommunikationsstörung in den für die Berechnung von Steuerbefehlen benötigten Daten kann bei dynamischen Industrie 4.0-Umgebungen (Beispiel aus dem Energiebereich) zu einer Herausforderung werden.

7.3.3 Safety als Zielscheibe

Die angesprochene zunehmende Vernetzung und gemeinsame Nutzung von Ressourcen innerhalb eines Unternehmens erfolgt in begrenztem Umfang auch bei Safety-Komponenten. So werden diese zunehmend an einem gemeinsamen Netzwerk mit anderen Systemen betrieben. Dies hat zur Folge, dass Safety-Komponenten den gleichen Angriffen über das Netzwerk ausgesetzt sind wie andere Komponenten auch. Dabei sind Angriffe auf die sicherheitsgerichtete Funktion wie auch indirekte Angriffe auf die Verfügbarkeit denkbar.

Indirekte Angriffe auf die Verfügbarkeit

Beim Angriff auf Safety-Funktionen droht etwa eine Not-Abschaltung einer Anlage oder Maschine. Dies kann beispielsweise durch eine Überlastung der Komponente durch sehr viele Anfragen, durch die Überlastung des genutzten Netzwerks oder durch einen Softwarefehler in der Komponente geschehen, die eine vorgesehene Safety-Funktion zum Ausfall bringt. Die eigentliche Funktion der Safety-Komponente bleibt in diesen Fällen erhalten, so dass für Mensch und Umwelt keine Gefahr droht, trotzdem führt dies zu einer Einschränkungen des Produktionsprozesses.

Angriffe auf die sicherheitsgerichtete Funktion

Im schlimmsten Fall führt die Ausnutzung von Schwachstellen in einer Safety-Komponente zu einer Manipulation der Funktion – etwa wenn Schwellwerte verändert werden. Die Folge ist, dass die funktionale Sicherheit (inkl. Safety und Security) nicht mehr gewährleistet ist. Schäden an Mensch und Umwelt können in diesem Fällen nur durch weitere Schutzmaßnahmen, beispielsweise eine mechanische Vorrichtung, gewährleistet werden. Da die entsprechenden Schutzfunktionen durch gesetzliche Vorgaben (z. B. die Maschinenrichtlinie) zwingend vorgeschrieben sind, wird bereits in Standardisierungsgremien die Integration von Security-Anforderungen für die Erfüllung der Safety-Anforderungen erarbeitet.

7.3.4 Integrität

Die Integrität sowohl der zur Produktion verwendeten wie auch der aufgezeichneten Daten ist von größter Bedeutung.

Durch Angriffe auf die zur Produktion verwendeten Daten ist es möglich, die Qualität der erzeugten Produkte negativ zu beeinflussen. In einem extremen Fall könnten zum Beispiel sicherheitsrelevante Eigenschaften des Produkts verändert werden, die zu einem späteren Zeitpunkt zu Personen- oder Sachschäden führen.

Die Integrität von Aufzeichnungen zur Nachverfolgung des Produktionsvorgangs sind ebenso relevant, da je nach Branche oder Produkt Haftungsfragen vorliegen können oder sogar regulatorische Vorgaben wie etwa in der Pharmaindustrie.

Aus den genannten Gründen wird in fast allen Branchen der Integrität die höchste Bedeutung eingeräumt, auch wenn dies häufig nur implizit geschieht und in der Wahrnehmung der Beteiligten die Zuverlässigkeit als wichtigster Aspekt gesehen wird.

In den unternehmensübergreifenden Wertschöpfungsnetzen der Industrie 4.0 wird dann die Integrität durch die zusätzliche Frage der Authentizität[15] ergänzt.

Da für die Abstimmung der Abläufe in Industrie 4.0 eine gute Synchronisation notwendig ist, wird auch die Integrität der Zeit relevant.

7.3.5 Vertraulichkeit

Bereits heute gilt es für Unternehmen bestimmte Informationen – häufig zeitlich beschränkt – vertraulich zu behandeln. Dazu gehören beispielsweise Rezepturen, Konstruktionsdaten oder Steuerprogramme. Diese Daten können einen erheblichen Wert für ein Unternehmen darstellen, weil viel Aufwand und Wissen zur Erstellung aufgewendet wurde.

Für den unerwünschten Informationsabfluss wird üblicherweise der Begriff „Datendiebstahl“ verwendet. Leider ist der Begriff insofern unpassend, als die Daten nicht wirklich gestohlen sondern kopiert werden und somit im Original noch vorhanden sind. Eine wesentliche Herausforderung beim „Datendiebstahl“ ist daher, dass er leicht unbemerkt bleiben kann.

Beim Diebstahl oder dem unberechtigtem Zugriff auf Daten besteht insbesondere das Problem, dass es in diesem Fall keine Möglichkeiten gibt, diesen Prozess rückgängig zu machen oder alternative Schutzmaßnahmen zu ergreifen. Ein Unternehmen verliert ab dem ersten Datenverlust die vollständige Kontrolle über weitere unberechtigte Zugriffe. Hier gibt es keine Rückfallposition wie bei der Safety. Es ist daher zu empfehlen, entsprechende Maßnahmen bereits bei der Planung zu berücksichtigen und vor allem sicher zu stellen, dass unternehmenskritische Daten auch als solche gekennzeichnet sind und ein entsprechender Umgang definiert ist.

Bisher ist das Unternehmen allein dafür verantwortlich, dass Informationen nicht gestohlen oder veröffentlicht werden. Bei Industrie 4.0 geht diese Verantwortung auch auf die verbundenen Unternehmen über. Es ist daher wichtig, entsprechende vertragliche Regelungen zur Kennzeichnung und zum Umgang sowie den Verantwortlichkeiten zu treffen, um einen vertrauenswürdigen Umgang mit kritischen Daten sicherzustellen. Berücksichtigt werden sollten bei der Einstufung, dass beispielsweise einige Daten durch ein Endprodukt oder eine Maschine selbst bereits aus der eigenen Kontrolle gegeben werden. Bei einem Endprodukt können die Abmessungen durch einen Mitbewerber selbst ermittelt werden, hier ist die Vertraulichkeit vor der Veröffentlichung besonders wichtig, danach ist eine Rekonstruktion durchaus anhand des Produktes selbst möglich.

Ein Beispiel für eine solche Verarbeitung sensibler Daten ist die Übertragung von Konstruktionsdaten an einen Auftragsfertiger. Dieser soll eine bestimmte Anzahl an Produkten fertigen. Hier muss sichergestellt sein, dass er nur die gewünschte Anzahl an Produkten fertigt und die Informationen danach nicht weiter verwenden kann.

Ein weiteres Beispiel betrifft den Fernzugriff für Wartungsaufgaben. Hierbei steht dem Maschinenbauer möglicherweise ein weitreichender Zugriff auf eine Maschine oder Produktionsnetzwerk zur Verfügung. Auf diese Weise können Daten aus dem System zur Auslastung und zu Produktionszahlen sowie weitere Daten aus dem Produktionsnetzwerk abgezogen werden, wenn kein ausreichender Schutz vorhanden ist.

Unabhängig von sensiblen Unternehmensdaten sind personenbezogene Informationen zu betrachten. Besonders bei der in Industrie 4.0 angestrebten Losgröße 1 ist damit zu rechnen, dass auch personenbezogene Informationen zu den Produktionsaufträgen verarbeitet werden. Hier müssen die gesetzlichen Auflagen beachtet werden und der Schutz gewährleistet werden.

7.3.6 Manipulation (beabsichtigt und unbeabsichtigt)

Ein bereits bekanntes Problem stellen Sabotage und menschliches Fehlverhalten dar. Diese kommen üblicherweise bereits heute vor. Aufgrund der zunehmenden Vernetzung innerhalb von Unternehmen und die entstehenden unternehmensübergreifenden Wertschöpfungsketten können die Folgen weitreichender und wenig kontrollierbarer sein. Dies gilt insbesondere dann, wenn durch die dynamischeren Anforderungen (prozessual) keine ausreichenden Verantwortlichkeiten und Kommunikationswege sowie (technisch) keine ausreichende Netzsegmentierung oder Zugriffkontrolle stattfindet.

15 Siehe Bedrohung „Identitätsdiebstahl“

Durch eine größere Anzahl möglicher Zugangspunkte wird das Risiko eines unautorisierten Zugangs durch Angreifer weiter erhöht. Zu den gefährdeten Zugangspunkten zählen unter anderem unbemannte Stationen, offene oder ungesicherte Netzwerkzugänge sowie Verbindungspunkte zu anderen Unternehmen (etwa zur Wartung oder Auftragsverarbeitung). Eine neue Qualität entsteht bei Industrie 4.0 durch die zunehmend dynamische und unternehmensübergreifende Vernetzung. Angriffe dürften zunehmend aus verbundenen Unternehmen auf Vertragspartner abzielen. Bei der Angriffsanalyse ist man damit zunehmend auf das Sicherheitsmanagement bei Vertragspartner angewiesen.

Als Risiken drohen insbesondere der Abfluss von Informationen, denkbar ist jedoch auch, dass manipulierte Auftrags- oder Produktionsdaten eingespielt werden. Die Konsequenzen wären ein unberechtigter Zugriff auf sensible Informationen oder die Manipulationen an Maschinen und Anlagenteilen bis hin zur Abschaltung oder Zerstörung.

7.3.7 Identitätsdiebstahl

Vertrauensverhältnisse spielen bei Sicherheitsmaßnahmen eine herausragende Rolle: Wird etwa eine Webseite besucht, vertraut der Benutzer darauf, dass ihn die übermittelte Adresse nicht auf eine völlig andere, schädliche – möglicherweise genau für diesen Zweck präparierte – Webseite umleitet. Der Webdienst wiederum vertraut darauf, dass der angemeldete Benutzer auch derjenige ist, für den er sich ausgibt. Dieses Vertrauensverhältnis gilt sowohl privat wie geschäftlich und wird in der Regel durch verschiedene Sicherheitsmaßnahmen unterstützt (vertrauliche Anmeldedaten, Token-Schlüssel und eindeutige Biometrie-Daten).

Das Risiko eines Identitätsdiebstahls besteht nun einerseits darin, dass sich ein Angreifer für eine ganz andere Person ausgibt und deren legitime Zugriffsrechte erhält. Andererseits unterscheidet sich die Authentifizierung etwa im Zugriffsprotokoll nicht von der des echten, legitimen Benutzers. Es gibt hier verschieden Ansätze das Risiko einzudämmen. So können heute öffentlich erreichbare Dienste (z. B. Gmail) anhand der Geo-IP erkennen wo sich ein Benutzer physisch befindet – und alarmieren den Anwender, wenn mehrere Zugriffe aus verschiedenen Ländern erfolgen. Meldet sich der echte Benutzer am System an, wird er über den potentiellen Sicherheitsbruch informiert und kann diesen bestätigen oder verneinen. Häufig ist hier eine Interaktion zur Überprüfung mit der betroffenen Person erforderlich. Mit der Rückmeldung wird der Prüfprozess dann weiter verbessert und irgendwann komplett maschinell automatisiert.

Für Industrie 4.0 stellt der Identitätsdiebstahl aus zweierlei Gründen ein ernstzunehmendes Risiko für die Verfügbarkeit von Systemen und Vertraulichkeit von Informationen dar:

Die Konstellation beteiligter Personen, Dienste, Anlagen und Sensoren kann sich dynamisch verändern. Das bedeutet viele Identitäten und viele mögliche Angriffsvektoren. Ferner verfügen Maschinen nicht über die Möglichkeit, flexible Entscheidungen zu treffen. Das erschwert die Erkennung, Verbesserung und Automatisierung von Sicherheitsmaßnahmen. Das Problem hier besteht weniger in der Maschine-zu-Maschine-Identifikation, sondern eher darin, das sich ein Angreifer für eine Maschine ausgibt. Es ist zu erwarten, dass hier eine zentrale Überwachungsinstanz benötigt wird, die verschiedene Identitätsaspekte wie Anmeldedaten, Kommunikationsverhalten oder auch ausgetauschte Datenmengen erfasst, überwacht und einen potentiellen Identitätsdiebstahl zur Überprüfung weiterleitet.

7.4 Schutzziele für Industrie 4.0 und Security-Anforderungen

Industrie 4.0 mit horizontalen und vertikalen Wertschöpfungsketten treibt die Vernetzung von Maschinen und Anlagen und die engere Verknüpfung mit der Unternehmens-IT und der Anbindung an das Internet massiv voran. Der Schutz gegen Angriffe von außen und der Schutz gegen Manipulationen durch sogenannte Innentäter muss den erhöhten Anforderungen von Industrie 4.0 Rechnung tragen.

Für Industrie 4.0. ist die reibungslose Zusammenarbeit zwischen Industrial Security (Security in der Produktion) und IT-Security (Office) grundlegende Voraussetzung. Dieses Zusammenwirken ist zu organisieren mit dem Ziel einer gemeinsamen standardisierten sicheren IT-Infrastruktur.

7.4.1 Generelle Schutzziele

Die heute aus dem Fertigungsumfeld bekannten Schutzziele genießen den gleichen hohen Stellenwert bei Industrie 4.0:

- Verfügbarkeit
- Integrität
- Know-how-Schutz/Vertraulichkeit

Dazu kommen noch

- Authentizität
- Integrität der Zeit, vor allem bei Wertschöpfungsnetzwerken über Firmengrenzen
- Nachvollziehbarkeit
- Rechtssicherheit

Die Authentizität ist essentielles Merkmal in einem Wertschöpfungsnetzwerk, vor allem, wenn die Kommunikation über Firmengrenzen hinweg erfolgt. Die Forderung nach Nachvollziehbarkeit resultiert auch aus Datenschutzanforderungen, sobald personenbeziehbare Daten verarbeitet werden, betroffen sind z. B. Mitarbeiter und Kunden. Insgesamt wird die technische Unterstützung von Privacy/Datenschutz durch Security-Mechanismen eine wichtige Rolle einnehmen.

Diese Schutzziele gelten in gleicher Weise für die Betriebsfunktionen, Überwachungsfunktionen und Schutzfunktionen (z. B. Safety). Bei Safety („Funktionale Sicherheit“, engl.: „functional safety“) für Systeme geht es darum, durch geeignete Maßnahmen sicherzustellen, dass von der Funktion einer Maschine oder Anlage keine Gefahr für Menschen oder Umwelt ausgeht. Dabei ist auch auf die Rückwirkungsfreiheit von Security in jeder speziellen Ausprägung („Profil“) zu achten.

7.4.2 Security-by-Design für Industrie 4.0.

Für die Realisierung von Industrie 4.0 Szenarien ist die frühzeitige Berücksichtigung von Maßnahmen zum Schutz der Informationssicherheit unerlässlich. Es kann dabei nicht um die nachträgliche Integration von technischen Mechanismen zur Security gehen, vielmehr ist ein integrierter Ansatz bei Produktentwicklung und Prozessen zum Schutz der Anlagen und der Infrastruktur erforderlich.

Ziel ist es, die erforderlichen Security-Funktionen als integrierten Teil eines Produktes bzw. einer Lösung zu realisieren. Neben einer klaren Verankerung von Security in den betroffenen Standards, und zwar von Anfang an, ergeben sich Konsequenzen für Hersteller und Betreiber von Anlagen.

Umfassende Ergänzungen zu den bestehenden Prozessen werden erforderlich.

Die bestehenden Entwicklungsprozesse müssen angepasst werden. Um Security-Requirements dort zielgerichtet einzubringen, sind Bedrohungs- und Risikoanalysen erforderlich, die insbesondere die entsprechenden Anwendungsfälle des späteren Produktes in Betracht ziehen. Schutzziele von Sicherheitsmaßnamen für ein Produkt orientieren sich an den schützenwerten Assets der betroffenen Hersteller, Integratoren und Betreiber und gegebenenfalls an (oft länderspezifischen) regulatorischen Vorgaben von Behördenseite, zum Beispiel, wenn Einsatzszenarien im Rahmen kritischer Infrastrukturen zu erwarten sind.

Das Securitydesign muss die Lebensdauer von Fertigungsanlagen – vielfach mehr als zehn bis 15 Jahre – mit berücksichtigen.

Nach der Identifikation der zu schützenden Assets wird eine Bedrohungs- und Risikoanalyse durchgeführt. Anhand der identifizierten Risiken werden mögliche Sicherheitsmaßnahmen ausgewählt. Hier spielen auch wirtschaftliche Aspekte eine wichtige Rolle. Security-Maßnahmen werden nur dann im Markt akzeptiert, wenn sie zum Geschäftsmodell der Zielarchitektur passen und die damit verbundenen finanziellen Aufwände tragbar sind.

Bei der Auswahl kryptographischer Komponenten müssen Exportrichtlinien und die damit verbundenen Prozesse beachtet werden. Betroffen sind hier insbesondere Funktionen zur Verschlüsselung von Daten, weniger kritisch sind reine Authentifizierungs- oder Integritätsmechanismen.

Wenn Produkte mit integrierter Sicherheit in verschiedenen Bereichen eingesetzt werden sollen, führt dies ggf. zu einer Bandbreite von zu implementierenden Maßnahmen (Profilen), die auch verschiedene Sicherheitsniveaus unterstützen müssen.

Der Fokus von Sicherheitsbetrachtungen liegt heute oft auf Funktionen im Rahmen der Netzsicherheit wie z. B.

Firewalls, VPNs, Remote Zugang zum Netz, etc. Dies wird sich mit Industrie 4.0 ändern: Komplexe und verteilte Anwendungen müssen mittels Security by Design a priori Sicherheitsmaßnahmen enthalten. Sicherheitsprofile müssen „agil" sein, d.h. man muss sie dynamisch anpassen und aushandeln können. Schnelles (Um-)Konfigurieren muss inklusiver Sicherheit möglich sein.

Gewohnte Qualitätsmaßnahmen sind zu ergänzen um Security-typische Maßnahmen. Dazu zählen u.a.:

- Vulnerabilitäts-Tests, Penetration Testing
- Integritätssicherung der Produktionsprozesse, insbesondere bei Security-Protokollen und Kryptofunktionen
- Erforderliche Zertifizierungen (z. B. nach IEC 62443) erzeugen im Einzelfall hohen zeitlichen Aufwand und beträchtliche Zusatzkosten, abhängig von dem beabsichtigten Sicherheitsniveaus.

Neben der prozessualen Bewältigung von expliziten Sicherheitsfunktionen an sich ist insbesondere auch die sichere Implementierung von Software-basierten Anwendungen im Sinne der Softwarequalität zu gewährleisten. Für die konsequente Umsetzung sind Schulungen der beteiligten SW-Ingenieure und zielgerichtete Qualitätstests der Ergebnisse bzgl. Schwachstellen erforderlich. Erfahrungen aus den Qualitätstests müssen ausgewertet und in den Designprozess einfließen.

7.4.3 Identitätsmanagement

Ein erforderliches und essentielles Merkmal eines Teilnehmers (Maschine, Benutzer, Produkt) in einem Industrie 4.0-Wertschöpfungsnetzwerk ist eine eindeutige, fälschungssichere Identität, repräsentiert durch ein digitales Zertifikat. Die digitalen Zertifikate enthalten neben den Schlüsseln zur Authentifikation die notwendigen Informationen zur Ver- und Entschlüsselung.

Zur Ablage der sicherheitsrelevanten Informationen sind vertrauenswürdige, sichere Speicher erforderlich. Sicherheitsprotokolle und Anwendungen mit integrierter Security müssen entsprechend sicher mit den erforderlichen Anmeldedaten versorgt werden. Voraussetzung dafür ist eine Identitätsinfrastruktur (je nach Komplexität eine oder mehrere Instanzen) entlang des Wertschöpfungsnetzwerkes, die die eindeutige und konsistente Identifizierung und Zuordnung der Identität eines Teilnehmers gewährleistet und die Authentifikation und Rechtevergabe auf der Basis der Identitäten unterstützt.

Gefordert werden vertrauenswürdige Zertifizierungsstellen (Certification Authorities, CA) als Verwaltungsinstanzen der digitalen Identitäten (Zertifikate) aller Teilnehmer in einem Industrie 4.0-Wertschöpfungsnetzwerk.

Zur Gewährleistung eines effizienten Identitätsmanagements müssen die Sicherheits-Anmeldedaten/Schlüssel der Teilnehmer mit sicheren Identitäten personalisiert bzw. an das Gerät gekoppelt werden.

Das Identitätsmanagement muss durchgängig den Schutz des geistigen Eigentums (IP-Schutz) unterstützen. Dazu gehören u.a. Produkt- und Produktionsmodelle. Ein vom Benutzer akzeptiertes und anwendbares digitales Rechtemanagement ist eine wichtige Voraussetzung dafür.

7.4.4 Dynamische Konfigurierbarkeit der Wertschöpfungsnetzwerke

Effiziente Wertschöpfungsnetzwerke erfordern dynamisches Konfigurieren/Umkonfigurieren der Industrie 4.0-Anlage. Das Security-Management muss die Dynamik der Industrie 4.0-Anlage unterstützen. Dazu ist eine Beschreibung der Security-Eigenschaften einer Industrie 4.0-Komponente (Security-Profile) mit einer standardisierten Sprache (Security-Semantik) notwendig, die auch eine klare Beschreibung der Kommunikationsschnittstellen/-protokolle und deren Security-Eigenschaften beinhaltet.

Die Security-Eigenschaften müssen als Bestandteil der Semantik der Referenzarchitektur vorhanden sein.

Aus der Beschreibung muss hervorgehen, welche Security-Fähigkeiten die Industrie 4.0-Komponente hat und mit welchen Verfahren das erforderliche Security-Niveau im Wertschöpfungsnetzwerk erreicht werden kann.

Die Security-Funktionen in Komponenten müssen prinzipiell verschiedene Security-Niveaus unterstützen können, um den jeweils aktuellen Anforderungen hinsichtlich des Wertschöpfungsnetzwerkes gerecht werden zu können. Mit diesen Voraussetzungen muss eine einfache Bewertung des resultierenden Security-Niveaus einer Industrie 4.0-

Anlage durch die Aggregation von Security-Profilen der Industrie 4.0-Komponenten möglich sein.

Die Security-Profile müssen die erforderliche Flexibilität der sich dynamisch ändernden Wertschöpfungsnetzwerke durch adäquate Schutzfunktionen unterstützen können. Dies wird für die heterogene Systemlandschaft bei Industrie 4.0 einen erheblichen Standardisierungsbedarf bewirken (vgl. KITS Roadmap – Normungs-Roadmap IT-Sicherheit, DIN/DKE, 17.02.2015).

Insgesamt wird sich die klassische Betrachtung (Kommunikations- und Netzzentrierte Security) in eine komplexe Sicherheits-Architektur für die Anwendungs-Ebene verschieben.

7.4.5 Sicherheit für die virtuelle Instanz

Bei Industrie 4.0 spielt die „virtuelle Instanz“ einer Produktion eine wichtige Rolle. Neben der physikalischen Umsetzung von Sicherheitsanforderungen ist gleichzeitig die entsprechende Security für diese virtuelle Repräsentation erforderlich.

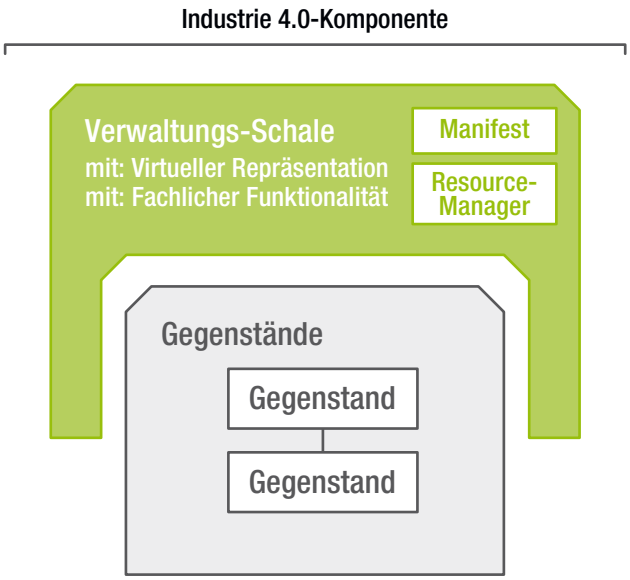


Abbildung 33: Industrie 4.0-Komponente

Eine Industrie 4.0-Komponente umfasst aus logischer Sicht ein oder mehrere Gegenstände und eine Verwaltungsschale, welche Daten der Virtuellen Repräsentation und Funktionen der Fachlichen Funktionalität enthält.

Anforderung:
Je nach Art der übergeordneten Systeme müssen die Verwaltungsobjekte in mehr als ein übergeordnetes IT-Systems verteilt werden können.

Abhängig von der Verteilung der „virtuellen Instanz“ (Office-Plattform bzw. in der Cloud) ergeben sich andere Security-Randbedingungen als bei dessen physikalischer Umsetzung. Natürlich muss auch die Interaktion mit der physikalischen Ebene sicher und nachvollziehbar gestaltet sein. Damit werden komplexe Sicherheits-Architekturen für die Anwendungsebene erforderlich. Know-how-Schutz und Integrität sind hier besonders wichtige Anforderungen. Klassische Domänengrenzen für Security werden nicht einfach im „virtuellen Modell“ abgebildet werden können. End-to-End-Security wird ein wichtiger Aspekt. Einen sehr positiven Beitrag zur Umsetzung einer Sicherheitsarchitektur kann eine „virtuelle Instanz“ im Rahmen von Recovery-Funktionen leisten, da es auch alle notwendigen Informationen für ein Wiederaufsetzen der physikalischen Umgebung nach einem Sicherheitsvorfall enthalten sollte.

7.4.6 Prävention und Reaktion

Prävention und Reaktion sind gleichermaßen notwendig: es werden keine fertigen Industrie 4.0 Security-Lösungen ohne weiteren Handlungsbedarf existieren.

Angreifer-Know-how und -Ausrüstungen nehmen kontinuierlich zu. Damit verändern sich Angriffsvektoren kontinuierlich und erfordern eine wirkungsvolle Weiterentwicklung effektiver Gegenmaßnahmen.

Neben vorbeugenden Schutzmaßnahmen sind auch Response Mechanismen absolut notwendig (Monitoring und Event Handling, Incident Management). Eine standardisierte Semantik für die Security-Meldungen mit einer regelbasierten Auswertung kann die Voraussetzungen schaffen für ein aktives Response Management. Die Bündelung der Aktivitäten in einem Security Operation Center (SOC) mit einer Verfügbarkeit von 24h an 365 Tagen schafft die operative Voraussetzung für eine zielgerichtete Erfassung, Analyse und Bewertung aller Aspekte der Security.

Sicherheit ist kein „Einmal-Thema“: Sicherheit kann nicht durch eine einmalige Aktion erreicht werden, die Bedrohungslage verändert sich kontinuierlich mit neuen technischen Möglichkeiten für potenzielle Angreifer oder mit der Entdeckung und Veröffentlichung von Schwachstellen in Standardprodukten und -komponenten. Hersteller und Betreiber müssen darauf mit Patches und Updates reagieren können, Möglichkeiten für das Einbringen von neuen Security-Versionen müssen identifiziert und prozessual eingeplant werden. Die Kosten für Security sind sowohl auf Hersteller- wie auch auf Betreiberseite nicht unerheblich, daher muss in allen beteiligten Prozessen ein Over-Engineering konsequent vermieden werden.

Betrachtungsgegenstand ist stets die Realisierung einer übergreifenden Security-Architektur. Dabei sind die Gesamtarchitektur der Anwendungsumgebung und alle Prozesse im Rahmen von Standardisierung, Entwicklung, Produktion und dem Management zu betrachten.

Sicherheit ist und bleibt in der Hauptsache ein Prozessthema und wird nicht durch einen einzelnen Security-Chip gewährleistet.

Eine Anpassung der IT-Strukturen unter Berücksichtigung der besonderen Rahmenbedingungen des Produktionsumfelds ist anzustreben.

7.4.7 Awareness, Ausbildung, Weiterbildung

Eine Schlüsselrolle spielen organisatorische Maßnahmen. Awareness-Schulungen des beteiligten Personals zur Stärkung des Bewusstseins für Security-Maßnahmen und deren Notwendigkeit müssen in jeder beteiligten Organisation (Hersteller, Anlagenbauer und Betreiber) geschaffen werden. Das erleichtert das Verständnis für die Maßnahmen und fördert die Qualität der Umsetzung.

Für Security Management Funktionen und Prozesse (Key Management, Audit-Funktionen, Event Handling) müssen Infrastrukturen und Personal mit entsprechender Ausbildung bereitgestellt werden. User-Guidelines, die von Seiten der Hersteller von Produkten und Lösungen zur Verfügung gestellt werden, müssen in die Prozesse integriert werden. Dazu gehören z. B. Passwort-Handhabung, Umgang mit Daten und Datenträgern, regelmäßige Datensicherung etc.

7.4.8 Handhabung

Die Bedienung der Industrial-Security-Funktion muss ohne umfangreiche Vorkenntnisse möglich sein. Dies gilt insbesondere im Hinblick auf die Behebung von Störfällen bei Wartungen und anderen Services. Ein Plug&Operate ist insbesondere für Security-Lösungen anzustreben.

7.4.9 Standards und Vorgaben

Industrial Security, gerade auch im Hinblick auf Industrie 4.0, ist deshalb aktuell Gegenstand von Diskussionen in Verbänden und Normungsausschüssen.

Mit der internationalen Norm IEC 62443 „IT-Sicherheit für industrielle Leitsysteme – Netz- und Systemschutz“ entsteht ein Rahmen mit Bewertungsmaßstäben für Industrial Security auf der Basis von vier Security Levels. Sieben grundlegende Anforderungen zur IT-Sicherheit von industriellen Automatisierungssystemen (Foundational Requirements, FR) werden detailliert in System Requirements (SR) und Requirement Enhancements (RE). Einem Security Level (SL 1.4) liegt ein Set von SR und RE zu Grunde.

Die Security-Fähigkeiten der Komponenten sind bei der Integration in ein System entsprechend dem geforderten Security-Level zu berücksichtigen. Gleichzeitig müssen die Prozesse so gestaltet sein, dass der geforderte Security-Level erreicht werden kann.

Erwartet wird, dass die IEC 62443 zukünftig für Zertifizierung verwendet wird.

Das aus der VDI-Richtlinie 2182 bekannte Vorgehensmodell für Informationssicherheit in der industriellen Automatisierung verzahnt die Aktivitäten der Komponentenhersteller, der Maschinenbauer und der Betreiber. Der Betreiber identifiziert und bewertet im Rahmen einer Risikoanalyse die potenziellen Schwachstellen. Der Hersteller muss die notwendigen Informationen (u.a. relevante Netzwerkeigenschaften) für den Integrator/Maschinenbauer bzw. Betreiber zur Erarbeitung von Security-Konzepten und Lösungen standardmäßig zur Verfügung stellen. Diese Richtlinie ist in die IEC 62443 eingeflossen.

Die Fähigkeit der Organisation zur Etablierung und Umsetzung von Security-Prozessen ist mit geeigneten Maßstäben zu ermitteln.

Der Anspruch in Industrie 4.0-Wertschöpfungsnetzwerken nach dynamischer Konfiguration steht orthogonal zu gültigen regulatorischen und normativen Vorgaben, die einen Verlust der Zertifizierung/Betriebszulassung bei Änderung zur Folge haben. Erforderlich wird daher ein Regelwerk, dass der Dynamik Rechnung trägt. Konsequente Eigensicherung aller Teilnehmer mit rückwirkungsfreien Sicherheitsmechanismen ist eine Voraussetzung.

7.5 Exemplarische IT Sicherheitsmaßnahmen

Die in diesem Kapitel vorgestellten exemplarischen Maßnahmen sind als generischer Werkzeugkasten zu verstehen, der ausgewählte Lösungsansätze vorstellen soll, in welche Richtung IT, Fachabteilungen bzw. Zentralabteilungen wie ein Security-Kompetenzzentrum wirkungsvolle Maßnahmen zur Verbesserung der IT-Sicherheit eines Unternehmens entwickeln und umsetzen können. Dabei werden insbesondere solche Ansätze beschrieben, deren Relevanz für morgen schon heute als hochwahrscheinlich angenommen wird, während ihre Verbreitung und Umsetzung heute noch schwach ausgeprägt ist. Die Beschreibungen stellen damit einen Auszug aus der aktuellen Diskussion hinsichtlich der zu leistenden Transformation von industrieller Security für Industrie 4.0 dar, liefern aber keine abgeschlossenen Maßnahmenkataloge. Die Weiterentwicklung auf Konzeptebene zur Serienreife benötigt insbesondere noch wesentlich detailliertere Anforderungen.

7.5.1 Security-Architektur

Auf Architekturebene gibt es mehrere Maßnahmen, die bei der Konzeption von Security für Industrie 4.0 zu berücksichtigen sind (Security by Design).

Eine Funktionstrennung („segregation of duties“ / „separation of duties“) findet in der Produktion heutzutage üblicherweise meist nur zwischen administrativen und Benutzer-Berechtigungen statt. Die Komponenten werden gewöhnlich durch einen mit vollen Rechten ausgestatteten, administrativen Zugang (Super-User) betrieben, der nicht selten auch über die Grenze der Produktions-Domäne hinweg Berechtigungen besitzt. Das ist der Tatsache geschuldet, dass der Fokus in der Produktion aus nachvollziehbaren Gründen bislang auf den Schutzzielen Verfügbarkeit und Integrität der Daten lag und nicht so sehr auf Vertraulichkeit und Authentizität. Dies wird sich mit Industrie 4.0 ändern (müssen), da die Wahrscheinlichkeit für einen erfolgreichen Cyber-Angriff auf eine ungeschützte, mit dem Internet verbundene Komponente sehr hoch ist. Die Auswirkungen sind umso höher, wenn diese Komponente darüber hinaus mit vollen administrativen Berechtigungen über die Grenzen der eigenen Domäne hinweg betrieben wird. Sofern die Schutzziele Vertraulichkeit und Authentizität vernachlässigt werden, kann dies kurz-, mittel- oder langfristig – beispielsweise durch einen Cyber-Angriff über das Internet – auch Auswirkungen auf die Verfügbarkeit und die Integrität der Daten haben. An diesem Beispiel ist erkennbar, dass die Aufteilung des Systemdesigns, also von Modulen, Maschinen und ganzen Produktionsanlagen bis hin zu Wertschöpfungsnetzen, in mehrere voneinander abgetrennte Bereiche eine notwendige Architekturmaßnahme ist. Dabei kann die Trennung logischer und/oder physischer Natur sein, sie kann sich auf die Existenz von Informations-Assets in gespeicherter oder transferierter Form beziehen oder auf getrennte Domänen bzgl. Zugriffe, was in Domänengrenzen für Authentisierung resultiert. Diese können wiederum vertikal sein – Administrator- versus Bediener-Login am selben Modul oder horizontal – getrennte Administrator- und Bediener-Accounts für verschiedene Module. Gemeint ist hier als Maßnahme nach Analyse die Isolationsgrenzen an den richtigen Stellen ins Design einzufügen, insbesondere in Kombination mit Unterscheidung bekannter kritischer Aspekte, z. B. Safety-relevanter Anteile. In einer – wahrscheinlich unpraktikablen – Maximalausprägung würde jede Funktion eine eigene Security-Domäne darstellen und über eigene Zugriffskontrollen, Rechte und andere Security-Funktionen verfügen.

Eng verbunden damit und in der Security schon oft und regelmäßig thematisiert ist die Netzwerksegmentierung: die klar definierten Unterschiede zwischen „Innen“ und „Außen“, bzw. zwischen unterschiedlich vertrauenswürdigen Netzwerkbereichen oder Zonen mit unterschiedlich starkem Schutzbedarf weichen jedoch in Industrie 4.0 Szenarien zunehmend zugunsten einer feiner granularen Unterscheidung auf (Sub-)Baustein-Ebene auf. Firewalls sind durch die Vielzahl an Systemen, die mit dem Internet kommunizieren müssen, entweder durchlöchert oder so

komplex, dass kaum noch ein Mensch in der Lage ist, einen Überblick über die Vielzahl an Regeln zu behalten, was die Gefahr beinhaltet, dass sich einige Regeln gegenseitig aufheben. Auch bei korrekten Regeln nimmt deren Anzahl so stark zu, dass eine rechtzeitige Prüfung der laufenden Kommunikation immer schwieriger wird. Dieser Trend wird mit Industrie 4.0 noch weiter verstärkt, da die verstärkte Automatisierung die zeitlichen Abläufe insgesamt verdichtet. Daraus folgt. dass der bisherige Perimeter-Schutz in Form von Firewalls und baulichen Sicherheits-Maßnahmen zunehmend an Wirkung und somit auch Bedeutung verliert. Daher ist es wichtig, die sich mit Industrie 4.0 verändernden Voraussetzungen in Zukunft bereits beim Design der einzelnen Komponenten und Workflows zu berücksichtigen. Als Maßnahme wird es wichtiger werden, die Trennung auf Kommunikationsebene wesentlich feingranularer zu organisieren, und dabei typischerweise von einer formal arbeitenden Trennung durch Firewalls mit recht statischen Regeln zu einem System überzugehen, welches die folgenden Ansätze kombiniert: Firewalls mit großzügigeren Regeln, welche unverhandelbare Leitplanken für die Kommunikation festlegen – hier wird alles unterbunden, was in der Industrie 4.0-Produktion in keinem Fall erlaubt ist, z. B. potentiell ein steuernder Durchgriff von einer externen übergeordneten Leitstelle zu einem internen dezentralen Aktuator. Eine weitere Maßnahme ist ergänzend, verschiedene Modi von Produktionseinheiten voneinander abzugrenzen, indem Regeln für die Kommunikation in Abhängigkeit vom Modus erlaubt oder unterbunden werden. Als Beispiel kann eine klassische Fernwartungssituation dienen, bei der während der laufenden Fernwartung eine Kommunikation mit anderen Produktionseinheiten unterbunden wird. Diese Art der Verfeinerung der Kommunikationssteuerung kann auf weitere Dimensionen ausgedehnt werden, die Details hängen von den Anforderungen an zukünftige Produktionskommunikationsnetze ab.

„Defense-in-Depth“ als Architekturmaßnahme bricht einerseits mit der Gewohnheit, die Produktionsstätte als isolierte Insel zu begreifen, die es vor feindlichem Zutritt oder Zugriff zu schützen gilt, und andererseits mit der Annahme, durch eine einzelne Gegenmaßnahme das notwendige Schutzniveau erreichen zu können. Vielmehr wird jedes Bauteil, letztlich jedes Informations-Asset, als eigenständige, zu schützende Komponente betrachtet, die es beispielsweise durch eine Authentifizierung oder Verschlüsselung zu schützen gilt. Gleichzeitig wird berücksichtigt, dass es unterschiedliche Angreifer und Angriffsfähigkeiten gibt und per Defense-in-Depth im besten Fall jeder Angreifertyp so früh wie möglich an seiner individuellen Maßnahmenhürde scheitert. Es werden also Kombinationen von geeigneten Gegenmaßnahmen auf unterschiedlichen Ebenen verwendet, um Kosten- und Performance-effizient den geeignetsten Schutz zu organisieren. Dazu gehören neben der Infrastruktur auch Übertragungswege und die für die Datenübertragung verwendeten Protokolle. „Defense-in-Depth“ kann beginnen mit der Verschlüsselung der Daten, die innerhalb der Komponente verarbeitet und (zwischen) gespeichert wird, kann über spezielle Daten-Übertragungsprotokolle zur Authentifizierung und Autorisierung von Zugriffen auf Daten bis hin zur Ende-zu-Ende-Verschlüsselung reichen. Dabei ist es unerheblich, ob der Zugriff durch einen Mensch oder eine Maschine erfolgt. Welche Kombination von Maßnahmen den besten Gesamtschutz ergeben muss in individuellen Analysen, begleitet von einer vereinheitlichenden Gesamt-Strategie, festgestellt werden.

Strikte Regeldurchsetzung bei gleichzeitiger Flexibilität wird voraussichtlich ein notwendiges Architektur-Paradigma sein. Damit ist gemeint, dass es nicht-verhandelbare „Leitplanken“ geben wird, die als Security-Policy in der Produktion strikt durchzusetzen sind. Als Beispiel kann die flächendeckende Verschlüsselung für Personen (Bediener-) beziehbare Informationen dienen, die aus Gründen des Datenschutzes unabhängig von Unternehmensgröße, Region etc. als Mindestmaßnahme immer notwendig sein wird. Innerhalb des durch diese Leitplanken definierten Spielfeldes wird jedoch eine hohe Flexibilität (vgl. „Dynamische Konfigurierbarkeit“ in Schutzzielen oben) benötigt hinsichtlich unterschiedlicher Kriterien. Im obigen Beispiel bedeutet dies z. B., regional unterschiedliche (gesetzliche) Regelungen abzubilden, welche Daten mit Personenbezug überhaupt erhoben, gespeichert, (wohin) übertragen und (wie lange) aufbewahrt werden dürfen. Es ist auch zu erwarten, dass sowohl das Schutzniveau von Maßnahmen (also Erhöhung des Widerstandes gegen Angriffe, z. B. durch Mehrfaktor-Authentisierung gegenüber einfachem Passwort, aber auch durch erhöhte Implementierungsqualität) als auch zeitliche Anforderungen an Security-Maßnahmen sowie viele weitere Ausprägungen der Security in

großen Bereichen je nach Anwendungsfall schwanken werden. Es wird zusätzlich durch die Autonomik und späten (erwünschten Auftrags-) Änderungen nicht vorhersagbare Fluktuationen von Events und Kommunikation geben. Diese Art der Dynamik ist heute im Produktionsumfeld unüblich und stellt insbesondere die Security-Maßnahmen vor neue Herausforderungen. Ein denkbarer Weg, flexible Security sicher umzusetzen, ist ein von der eigentlichen Produktionskommunikation unabhängiges Security-Administrationsnetzwerk, über welches die Security-relevante Umkonfiguration zur Laufzeit erfolgt. Für die kommerzielle Bewertung solcher Ansätze wird eine entsprechende Risikoanalyse benötigt, um die Aufwände einem bewerteten Risiko gegenüberstellen zu können.

Ebenso kann strikte Regeldurchsetzung durch statische Konfiguration bzw. Hardware im Gegensatz zu dynamischer Konfiguration durch (umkonfigurierbare) Regeln in Softwarealgorithmen implementiert werden.

7.5.2 Identitätsmanagement

Nur wenn bekannt ist, welcher Benutzer zu welchem Zeitpunkt auf welche Maschine Zugriff hat und haben darf, können unbefugte Zugriffe wirkungsvoll identifiziert und verhindert werden. Dies führt zum Identitätsmanagement.

Die flächendeckende Einführung von elektronischen Identitäten für Personen und technische Entitäten verbunden mit darauf aufbauenden Authentisierungs- und Autorisierungsverfahren implementiert die oben geforderte Separierung von Funktionen bzw. den Zugriff darauf sowie die Security-Prinzipien Mandatory Access Control und Least Privilege: Jeder Zugriff muss authentisiert und autorisiert werden und erfolgt mit den geringstmöglichen Rechten, die der Anwendungsfall erfordert.

Im Rahmen der zunehmenden Industrie 4.0-Automatisierung und Autonomik müssen die geschilderten Maßnahmen ebenso für Systeme, Maschinen und Anlagen eingeführt werden, insbesondere sofern sie auf andere Einheiten steuernd einwirken.

Voraussetzung für eine solche durchgehende Authentisierung von Zugriffen ist sowohl die Existenz eines produktionsnetzweiten Verzeichnisses sämtlicher Identitäten von Menschen und Maschinen, die im betrachteten Prozess genehmigte Zugriffe auf Ressourcen haben, als auch die Modellierung von differenzierten Rollen und Rechten, die die benötigten Aktivitäten abbilden. Schließlich muss eine Policy systemweit verfügbar und integer sein, welche die aktuell gültigen Zugriffsregeln festlegt. Dies stellt gerade international aufgestellte Großkonzerne vor echte Herausforderungen, da die schiere Masse der Prozesse, Rollen, Rechte und Identitäten häufig zu groß ist, um an einer einzigen Stelle abgelegt und verwaltet werden zu können. Weltweit verteilte Standorte und Zugriffe auf dieses Verzeichnis lassen eine zentrale Lösung als Unmöglichkeit erscheinen. Um unternehmensweit eindeutige Identitäten vergeben zu können, muss ein Prüfmechanismus existieren, der in der Lage ist auf sämtliche im Unternehmen verwendeten Identitäten zuzugreifen, um beispielsweise abprüfen zu können, ob eine neu anzulegende Identität bereits im Unternehmen existiert, um anschließend einen neuen, eindeutigen Bezeichner vergeben zu können. Dabei ist es durchaus denkbar, dass mehrere dezentrale Datenbanken existieren, in denen Identitäten verwaltet werden. Bei dieser dezentralen Variante muss sichergestellt werden, dass bei der Vergabe neuer Identitäten und der Verwaltung existierender Identitäten gegen sämtliche vorhandenen Datenbanken abgeprüft werden kann, ob die betreffende Identität bereits existiert bzw. an welcher Stelle die Verwaltung erfolgen muss. Die dezentrale Variante setzt eine Hochverfügbarkeits-Architektur mit integriertem Load-Balancing und Failover-Mechanismen voraus, damit sichergestellt ist, dass sämtliche verwendeten Datenbanken zu jeder Zeit verfügbar sind. Dabei sollten auch Zeitfenster für Wartungsarbeiten berücksichtigt werden, damit der Zugriff auf die Identitäten im eigenen Unternehmen sichergestellt ist, um beispielsweise Betriebs-Ausweise und Zertifikate ausstellen, prüfen und zurückziehen zu können. Die beschriebenen Herausforderungen gelten in vergleichbarer Weise auch für die anderen genannten Daten, so ist z. B. ein Verfahren zu implementieren, um regional unterschiedlich notwendige Rollen und Rechte zu organisieren und trotzdem zentral zu überwachen und zu dokumentieren. Es ist zu erwarten, dass die Anzahl von Identitäten für Systeme und deren Bestandteile jene für Personen schnell stark übertreffen wird.

Betriebsausweise z. B. dokumentieren die Identität einer Person im Unternehmen und können je nach

Beschaffenheit des Ausweises Zutritt zu Räumen und Gebäuden sowie Zugriffe auf Software steuern. Bei der Erstellung eines Betriebsausweises wird die Identität der Person anhand von hoheitlichen Dokumenten (Personalausweis, Reisepass, etc.) authentifiziert und die Ausweisnummer mit der unternehmensweit eindeutig vergebenen Identität der Person verknüpft. Über einen separaten Autorisierungsprozess können Zutritts- und Zugriffsberechtigungen vergeben werden und je nach Beschaffenheit des Betriebsausweises auf dessen Chip entsprechende Berechtigungszertifikate gespeichert werden. Zertifikate haben grundsätzlich nur eine befristete Gültigkeit, um unter anderem auch eine regelmäßige Überprüfung (Rezertifizierung) zu erzwingen. Anhand der mit der Identität verknüpften Berechtigungen können jeder Identität die vergebenen Berechtigungen entzogen werden, beispielsweise bei Beendigung des Arbeitsverhältnisses. Es ist ebenfalls möglich, bei Verlust des Betriebs-Ausweises dem jeweiligen Betriebsausweis Berechtigungen zu entziehen oder ihn vollständig zu sperren. Dies sollte in jedem Unternehmen über eine zentrale Plattform durchgeführt werden, die für die Ausgabe, die Prüfung und das Zurückziehen von Ausweisen verwendet wird.

Die Trennung und Aufteilung der Berechtigungen im Systemdesign auf mehrere Benutzer, die jeweils nur die für ihre Tätigkeit relevanten Rechte besitzen (Least Privilege, segregation of duties) sorgt für eine weitere Erschwernis bei dem Versuch eines außenstehenden Angreifers, an (verschlüsselte) Informationen zu gelangen.

7.5.3 Kryptografie – Vertraulichkeitsschutz

Es muss davon ausgegangen werden, dass die allermeisten klassifizierten Information, die elektronisch auf einem Datenträger abgelegt werden, gezielten Interessen gegenüberstehen, unautorisiert Kenntnis von ihnen zu erlangen. Man kann die Auswertung dieser Informationen selbst bei Zugriff für einen unbefugten Dritten allerdings deutlich erschweren, indem man beispielsweise auf eine durchgängige und hinreichend starke Verschlüsselung achtet. Gute Verschlüsselungsalgorithmen erhöhen den Schutz der Vertraulichkeit von Informationen, indem sie den notwendigen Aufwand zur unbefugten Entschlüsselung (ohne Schlüssel) extrem in die Höhe treiben. Datenübertragung erfolgt oft über mehrere Stellen. Selbst wenn die einzelnen Übertragungen verschlüsselt erfolgen, die Zwischenspeicherung allerdings im Klartext erfolgt, besteht die Gefahr des Datendiebstahls oder der Datenmanipulation durch unbefugte Dritte. Eine Ende-zu-Ende-Verschlüsselung erschwert die Möglichkeit der Datenmanipulation und die Auswertung von Daten im Falle eines unautorisierten Zugriffs bzw. eines Datendiebstahls („secure-the-weakest-link"), verhindert letzteren jedoch nicht. Die Daten werden z. B. bei asymmetrischer Kryptographie vom Absender mit dem öffentlichen Schlüssel des Empfängers verschlüsselt und zusätzlich verschlüsselt übertragen und verschlüsselt abgelegt. Die Art der Verwendung von asymmetrischer wie symmetrischer Kryptografie wird durch Konzepte festgelegt, die Spezifika der Anwendung berücksichtigen. Als Beispiel dient der Anwendungsfall austauschbarer Hersteller-Rezepturen in Produktionsmaschinen. Hierbei ist verschlüsselte Übertragung vom Hersteller zum Anwender und weiter in die Maschine vorzusehen, um die Offenlegung der in Industrie 4.0 zunehmend wertstiftenden bzw. kostenpflichtigen Rezepturen dem Anwender gegenüber zu unterbinden. Da der Anwender typischerweise Administratorrechte an der Maschine hat, ist die Speicherung der Rezeptur in der Maschine ebenfalls verschlüsselt anzulegen (oder ein nur vom Hersteller und Hersteller-signierten Code lesbarer Speicherbereich zu nutzen). Hinsichtlich der Frage ob und wie auch der Programmablauf auf Basis der Rezeptur zu verschlüsseln ist, müssen Risiken wie Laufzeit-Analysen durch den Anwender oder externe Angreifer dahingehend bewertet werden, ob sie die aufwendigere Absicherung hiergegen rechtfertigen. Im Falle der Verwendung von symmetrischer Kryptographie wird ein angemessen sicherer Speicher für den lokalen privaten Schlüssel und entsprechende Infrastruktur benötigt, was schnell ein spezielles Hardware-Sicherheits-Element erfordert. Zusätzlich oder alternativ kann die Auswirkung eines Angriffes durch die Verwendung von Maschinen-individuellen Schlüsseln eingegrenzt werden. Letzteres erlaubt zudem die Einschränkung des Einsatzes von Rezepturen auf individuelle Maschinen im Sinne eines Lizenzmanagements.

7.5.4 Kryptografie – Integritätsschutz

Kryptographie kann hervorragend zum Schutz von Integrität eingesetzt werden, indem geeignete Formen von Prüfwerten in Kombination mit Signaturen eingesetzt wer-

den. Als Maßnahme in Industrie 4.0 schützt das wirkungsvoll Integrität und Authentizität. Als Beispiel sei der Schutz von Basissystemsoftware (eingebettete Betriebssysteme) von eingebetteten Systemen genannt. Es ist flächendeckend erstrebenswert, eingebettete Systeme ausschließlich mit sicherem Startvorgang zu entwerfen. Hierfür wird von einem ersten, im Feld unveränderbaren (nicht beschreibbarer Speicher, TPM, o.ä.) Software-Anteil zuerst die Integrität des nächsten darüberliegenden Software-Codes mittels Hash und Signatur geprüft, bevor er gestartet wird. Dies kann nach Bedarf mehrstufig erfolgen und führt zu einer vertrauenswürdigen Code-Basis im Betrieb. Ein Hardware-Schutzmodul ist für ein hohes Vertrauen in die Angriffsresillienz sinnvoll. Für Industrie 4.0 gilt es zu klären, wie diese Maßnahme flächendeckend umsetzbar ist insbesondere dort, wo sie einen verhältnismäßig hohen Aufwand darstellt (z. B. bei einfachen Sensoren).

Im Rezeptur-Beispiel von oben kann z. B. asymmetrische Kryptografie eingesetzt werden, wenn die Anforderungen an die Berechnungszeit geringer sind (die üblichen symmetrischen Verfahren sind bei vergleichbarer Stärke schneller berechnet als die Asymmetrischen) bzw. wenn kein geeignet sicherer Speicherort lokal verfügbar ist (für den bei symmetrischen Verfahren notwendig geheimen Schlüssel) und die Authentizität der Rezeptur gegenüber der Vertraulichkeit im Vordergrund steht. Für die Authentizitätskontrolle genügt der öffentliche Schlüssel des Herstellers, der – weil öffentlich – keinen sicheren Speicherbereich zu Ablage erfordert.

Die im Einzelfall verwendeten Kryptoverfahren und Verschlüsselungsalgorithmen hängen von verschiedenen Kriterien ab, u.a. von der geforderten Schutzdauer, verfügbaren Ressourcen (Berechnungsperformance), Verfügbarkeit und Einführbarkeit von lokalem Geheimnisspeicher für die Ablage von Schlüsseln versus zentraler Infrastruktur (Public-Key-Infrastruktur), Verfügbarkeit von Online-Verbindungen (zentrales Management, Revocation), bekannt gewordenen Angriffen etc.

Kryptografie erleichtert zwar die Schutzaufgabe als Ganzes, erfordert aber dafür einen sorgsamen Umgang mit dem Schlüsselmaterial. Bei Verlust von Schlüsseln droht Datenverlust und falls der Schlüssel in die falschen Hände gelangt, wäre ein unbemerkter Zugriff auf die verschlüsselten Daten denkbar. Es ist jedoch einfacher, anstatt eines flächendeckenden Schutzes ohne Kryptografie die Schlüssel an wenigen Stellen fokussiert zu schützen. Etablierte Verfahren wie PKI stehen dafür zur Verfügung. Dedizierte Hardware-Bausteine – Security-Chips mit umfangreichen Security-Funktionen und starkem Schutz gegen unterschiedliche Angriffsmethoden – stehen ebenfalls zur Verfügung. Nur im auf die Anwendung und Risikosituation angepassten Konzept entfaltet die Kryptografie jedoch ihre ganze Wirkung.

7.5.5 Sicherer Fernzugriff und häufige Aktualisierungen

Es ist gängige Praxis in Fertigungsbetrieben, dass Hersteller die Fernwartung von Maschinen und Robotern über das Internet durchführen. Dabei greift der Techniker des Herstellers über das Internet direkt auf die zu wartende Maschine im Unternehmen zu, um Firmware-Updates durchzuführen oder Einstellungen zur Leistungsverbesserung vorzunehmen. Die Kooperation von unterschiedlichen Unternehmen – ggf. über gemeinsam genutzte Plattformen – birgt die große Herausforderung, die verschiedenen Benutzer korrekt zu authentifizieren, da in der Regel die Mitarbeiter des eigenen Unternehmens über Personalsysteme eindeutig zu identifizieren sind, die Mitarbeiter von Kooperationspartnern, Kunden, Herstellern allerdings nicht. Jedes der beteiligten Unternehmen hat zwar sein eigenes Identitäts-Management, es besteht üblicherweise allerdings keine auf technischer Ebene etablierte Vertrauensbeziehung zwischen den kooperierenden Unternehmen.

Diese Vertrauensstellung kann über ein sogenanntes Federated Identity Management (FIM) geschaffen werden. Ein externer Identity-Broker dem sämtliche beteiligten Unternehmen vertrauen (müssen), führt dabei die Überprüfung durch, ob die anfragende Identität (unerheblich ob es sich hierbei um einen Menschen oder eine Maschine handelt) diejenige ist, die sie vorgibt zu sein. Diese Überprüfung kann über Multi-Faktor-Authentifizierung unter Verwendung einer Kombination aus zwei oder mehr der folgenden Faktoren stattfinden: Besitz (Dongle, Smart-Card, Tokens), Wissen (Passwörter, Schlüsselphrasen) und/oder Biometrie (Fingerabdruck, Iris-Scan). Nach erfolgter Authentifizierung kann dann in einem zweiten Schritt im Unternehmen überprüft werden, ob und wenn ja welche autorisierten Zugriffe für diese Identität vorliegen und ob ein Zugriff auf das gewünschte System erfolgen darf. Spätestens hier

werden übergreifende Standards zwingend notwendig. Die gleiche Frage nach dem Vertrauen ist hinsichtlich der eingesetzten Computersysteme relevant. Um sicherzustellen, dass z. B. keine Malware-/Viren- oder sogar Backdoor-Risiken über ein vom Anwender nicht kontrolliertes, für die Fernwartung eingesetztes System des Herstellers verursacht wird, können z. B. (de-facto) standardisierte Virtualisierungstechnologien eingesetzt werden. Dabei können Anwender und Hersteller das zum Einsatz freigegebene Image gemeinsam festlegen und prüfen, da im Betrieb für den Hersteller vor allem die VM Schnittstelle und die Verfügbarkeit der notwendigen Wartungstools in der VM-Ablaufumgebung relevant ist, während der Anwender vor allem an der Vermeidung von Risiken für seine Produktion interessiert ist. Mit der Industrie 4.0-Evolution hin zu kontinuierlichen Diensten zur Beobachtung, Pflege und Analyse von Produktionssystemen wird diese Maßnahme kontinuierlich weiterentwickelt werden müssen. Als Beispiel sei hier die Kontrolle des Abflusses von operativen Daten aus der Produktion genannt.

Häufige Aktualisierung bzw. die Möglichkeit zur anlassbezogenen Schließung von Software-Lücken sind eine Anforderung an zunehmend softwarelastige vernetzte Systeme, die im Produktionsumfeld im Widerspruch mit Zertifizierungen z. B. für Betriebssicherheit steht. Als mögliche Gegenmaßnahmen steht die Kapselung von zertifizierten Systemen gegenüber Netzwerken durch Security-Gateways zur Verfügung, deren Funktionsumfang sehr unterschiedlich sein kann, im Kern jedoch die Sichtbarkeit und damit Angreifbarkeit des gekapselten Systems adressiert. Hinsichtlich immer weitergehender Modularisierung bedeutet dies eine notwendige Verkleinerung der Gateways bei gleichzeitig verbreiterter Unterstützung von Industrie-relevanten Protokollen und Schutzmechanismen. Die Grenze der Machbarkeit von Echtzeitkommunikationsprüfung auf immer mehr Protokollen und ISO/OSI-Schichten bei gleichzeitiger Vermeidung von Fehlanschlägen wird sich verschieben müssen. Als weitere zu kombinierende Maßnahme sind Verfahren gefordert, die trotz Zertifizierung eine Aktualisierung im Feld erlauben, was z. B. gemeinsam mit geeigneter Modularisierung ermöglichen kann, dass zumindest sicht- und damit angreifbare Anteile vom Zertifizierungskern entkoppelt und aktualisiert werden können.

Authentifizierungsmechanismen stellen sicher, dass ausschließlich berechtigte Benutzerkennungen Zugriff auf die geschützten Daten haben, jedoch prüft die herkömmliche Ein-Faktor-Authentifizierung mittels Passwort oder Besitz ausschließlich darauf ab, ob die Benutzerkennung autorisiert ist, nicht aber ob auch der korrekte Benutzer diese Benutzerkennung verwendet.

Solange sichergestellt ist, dass der private Schlüssel des Empfängers nicht kompromittiert wurde, kann ausschließlich der gewünschte Empfänger die Nachricht entschlüsseln und lesen. Ein Knacken des Schlüssels ist zwar grundsätzlich nicht unmöglich, erfordert aber einen verhältnismäßig hohen Aufwand und kann nach heutigem Stand der Technik nur gezielt, nicht flächendeckend durchgeführt werden.

Der Einsatz einer durchgehenden Verschlüsselung setzt voraus, dass sowohl Sender als auch Empfänger jeweils gültige Schlüssel einer Zertifizierungsstelle besitzen und verwenden, und dass eine verschlüsselte Übertragung sowie eine verschlüsselte Datenablage mit der verwendeten Infrastruktur technisch möglich sind. Dazu gehört der Einsatz geeigneter Protokolle, Hardware und Software, um die durch die Verschlüsselung bedingte erhöhte Rechenleistung und drohende Performance-Einbußen auf ein erträgliches Minimum zu beschränken.

Dies gilt nicht nur für Prozesse im Unternehmen, sondern auch für Prozesse und Datenflüsse innerhalb der hergestellten Produkte.

7.5.6 Prozesse und organisatorische Maßnahmen

Im Unternehmen wird das Management von Informationssicherheitsrisiken im Idealfall durch ein geeignetes, umfassendes Security Management inklusive Risiko-Management–System und Incident-Management-System unterstützt. Aufgabe des Risiko-Managements ist die Identifikation und Behandlung bestehender Risiken, um diese transparent zu machen und zu ermöglichen, dass der Umgang mit diesen Risiken in Kooperation mit den Fachabteilungen und unter der Berücksichtigung der Compliance organisatorisch abgebildet werden kann. Es gibt grundsätzlich 4 Möglichkeiten um mit identifizierten IT-Sicherheits-Risiken umzugehen: Akzeptanz, Mitigation, Eli-

minierung oder Transfer. IT-Sicherheits-Risiken müssen bekannt sein, um ihnen adäquat begegnen zu können. Nur ein bekanntes Risiko kann wirkungsvoll adressiert werden. Um zu vermeiden, dass die beteiligten Abteilungen und Bereiche im Unternehmen ihre Zuständigkeiten unkoordiniert selbst definieren und somit die Gefahr besteht, dass einzelne Themen unbehandelt bleiben oder sich niemand für übergreifende Themen zuständig fühlt, gilt es organisatorisch für Querschnittsfunktionen zu sorgen und unternehmensweit existierende Zuständigkeiten und Rollen klar zu definieren. Sofern noch nicht vorhanden, empfiehlt es sich hierfür dedizierte Stellen („Chief Information Security Officer", „Production Information Security Officer") zu schaffen, deren Aufgabe darin besteht, in engster Abstimmung und Kooperation IT-Sicherheit als ganzheitlichen Prozess im gesamten Unternehmen zu betrachten.

In der Regel gehört es zu den ersten Aktionen einer solchen Zentralstelle, ein umfassendes Monitoringkonzept zu entwickeln und umzusetzen. Hierzu können bestehende Monitoringmaßnahmen gegebenenfalls weiterverwendet bzw. aggregiert werden. Viele für Security relevante Bereiche die zuvor oft nicht beachtet wurden wie Dokumentation und Auswertung von Zugangskontrollen zu sicherheitsrelevanten Zentralsystemen (zentraler Schlüsselspeicher) insbesondere für Administratoren, müssen jedoch neu geschaffen werden, da sie mindestens in der Produktion nicht üblich sind.

Darüber hinaus wird es mit Industrie 4.0 zwingend erforderlich, Lösungen für die Kooperation auf Prozessebene über Unternehmens- und Ländergrenzen hinweg ggf. über eine gemeinsam genutzte Plattform zu finden, welche die unabhängige Auswertung von Vorfällen und deren Identifikation und Dokumentation erlaubt.

Erst ein eingespieltes Security-Management ermöglicht es, als Maßnahme zur Erreichung von Transparenz, Anomaliedetektion und Dokumentation, produktionsweit selbst positiv auf die Erhöhung der Sicherheit zu wirken.

7.5.7 Awareness

Es ist schließlich zwingend erforderlich, dass sowohl die Belegschaft als auch das Management sich der Bedeutung von IT-Sicherheit und der Auswirkungen beispielsweise eines potenziellen Datenverlusts oder einer Datenmanipulation bewusst sind und infolgedessen IT-Sicherheitsvorgaben verstehen, um sie einzuhalten und zu beachten. Mangelnde Einsicht kann sogar zur bewussten Umgehung von IT-Sicherheitsmaßnahmen führen, da Security-Maßnahmen oft den Ablauf nicht erleichtern und beschleunigen. Daher ist eine regelmäßige Aus- und Weiterbildung der gesamten Belegschaft eine wichtige Maßnahme.

7.5.8 Unternehmensweite Abdeckung

IT-Sicherheit beginnt allerdings nicht erst in der Fertigung, sondern bereits bei der Planung und der Beschaffung der Produktions-Komponenten. Um eine sichere IT-Umgebung für die Produktion aufbauen zu können, ist eine enge Zusammenarbeit zwischen Planung, Beschaffung und Fertigung notwendig. IT-Sicherheitsvorgaben können nur dann eingehalten werden, wenn die beschafften Produkte dies technologisch auch leisten können. Um die technologischen Anforderungen an die zu beschaffenden Komponenten zu kennen, ist ein Dialog zwischen Fertigung, Planung und Einkauf erforderlich. Ohne konkrete Vorgaben seitens der Kunden sehen Hersteller oft keine Notwendigkeit, Sicherheitsfeatures in die Produkte zu implementieren, da dies unter Umständen mit höheren Herstellungskosten und Performance-Einbußen verbunden ist. Ohne ein entsprechendes Angebot der Hersteller sehen die Kunden sich einer scheinbar alternativlosen Situation am Markt gegenübergestellt. Dieser Teufelskreis bewirkt, dass IT-Sicherheitsmaßnahmen zurzeit nur sehr langsam in den Produkten der Hersteller implementiert werden. Die in den Einkaufsrichtlinien verankerten Mindestanforderungen an die Produkte der Hersteller sollten daher regelmäßig überarbeitet und angepasst werden.

Sämtliche vorgestellten exemplarischen Maßnahmen dienen zur schrittweisen Verbesserung der IT-Sicherheit im Unternehmen. Welche dieser Maßnahmen im konkreten Fall sinnvoll eingesetzt werden, soll und muss im Einzelfall erarbeitet werden, bzw. aus Best Practices angepasst werden.

7.6 Ausblick und Forderungen

Industrie 4.0 verbindet die Informationswelten von Office bis zum Sensor über Unternehmensgrenzen hinweg. Die Sicherheit dieser Informationswelten kann nur hergestellt werden, indem die heute häufig existierende Trennung der Verantwortungen für Informationsverarbeitung und -sicherheit zwischen Office-IT und Automatisierung aufgehoben wird.

Standards und Normen existieren heute bereits für den Bereich der Office IT und regeln viele Fragestellungen von Informationssicherheit (ISO 27000-Serie) über Infrastrukturmanagement (ITIL) bis zu geschäftsrelevanten IT Maßnahmen (Cobit). In der Automatisierungstechnik besteht – obwohl es eine Vielzahl branchenspezifischer Empfehlungen[16] gibt – zum Thema „Informationssicherheit" noch großer Nachholbedarf bei der Sensibilisierung, Risikoerkennung und der Umsetzung von Security-Maßnahmen.

Kurzfristig kann mit der deutschsprachigen VDI-Richtlinie 2182 ein Vorgehensmodell für Informationssicherheit in der industriellen Automatisierung genutzt werden, das die Verzahnung von Herstellern, Integratoren und Betreibern berücksichtigt.

Aufgrund zunehmender Verschmelzung aller Unternehmensnetze und darüber hinaus ganzer Wertschöpfungsnetzwerke einerseits sowie unterschiedlicher Schutzanforderungen und -möglichkeiten andererseits, kommt der Abstimmung und Harmonisierung von Security-Maßnahmen im gesamten Unternehmen und zu Dienstleistern eine entscheidende Bedeutung zu. Mit der noch in Arbeit befindlichen IEC62443[17] wird das Ziel verbunden, Vorgehensmodell und Maßnahmen der Verwaltungs-IT (in Form der ISO 27000er Reihe) mit Besonderheiten der Automatisierung (auf Grundlage des ISA-99[18]) effizient und sicher zu verbinden. Die für Industrie 4.0 neuen Anforderungen und Maßnahmen sind entsprechend in Normen auszuarbeiten. Ob dies besser durch neue Normen oder Überarbeitung und Ergänzung existierender Normen umsetzbar ist, muss auch im Kontext anderer Normungsthemen im Rahmen von Industrie 4.0 bewertet werden.

Eine Harmonisierung bedeutet dabei auch, dass sich das Sicherheitsmanagement der Office-IT und die der Automatisierungstechnik annähern müssen. Eine Bewegung von „beiden" Seiten ist dazu erforderlich.

Dass es Richtlinien in der Automatisierung gibt, für die es in der Office-IT keine Entsprechung gibt, zeigt beispielhaft die Maschinenrichtlinie 2006/42/EG: Sie stellt auf europäischer Ebene einen regulatorischen Rahmen zum Schutz von Menschen und der Umwelt dar. Neben der Sicherstellung der Betriebssicherheit und der Zuverlässigkeit stellt die Gewährleistung der gefahrenfreien Funktion im Rahmen der dynamischen Wertschöpfungsnetzwerke in Industrie 4.0 eine besondere Herausforderung für eine aktualisierte Maschinenrichtlinie dar.

Die Sicherstellung der gefahrenfreien Funktion unter Verwendung von passenden Komponenten erfordert geeignete Integrationsmaßnahmen und -prüfungen. Übertragen auf die Informationssicherheit sind geeignete Verfahren und Mechanismen zu entwickeln, die das angestrebte Niveau der Security erreichen und es in den sich dynamischen verändernden Wertschöpfungsnetzwerken erhalten.

Der Aufbau von vertrauenswürdigen Zertifizierungsstellen und eindeutigen, fälschungssicheren Identitäten sind die Grundvoraussetzungen für eine Identitätsinfrastruktur entlang des Wertschöpfungsnetzwerkes, die die eindeutige und konsistente Identifizierung und Zuordnung der Identität eines Teilnehmers gewährleistet und die Authentifikation und Rechtevergabe auf der Basis der Identitäten unterstützt.

Security muss integraler Bestandteil des Produktentstehungsprozesses werden (Security by Design).

Auch wenn die konkreten Anforderungen und Randbedingungen in den Bereichen unterschiedlich sein mögen, können diese dennoch mit gemeinsamen Methoden und Konzepten bearbeitet werden. Durch die Zusammenführung des Know-hows aus Office-IT und Automatisierung lassen sich erhebliche Synergieeffekte erzielen.

16 etwa ISA99, NIST SP800-82, NERC CIP, CPNI Good Practice Guide (alle englischsprachig)

17 Siehe https://www.dke.de/DE/STD/INDUSTRIE40/Seiten/IEC62443.aspx

18 Siehe https://www.isa.org/isa99/

Hierzu wird eine auch inhaltliche Öffnung und Fortbildung seitens der Office-IT für die Anforderungen in der Automatisierung genauso notwendig sein wie der Ausbau des IT- und speziell Security-Know-hows in der Automatisierung.

Die Sicherheitslage wird nie statisch sein, die Bedrohungssituation wird einer ständigen Veränderung unterliegen. Security sollte daher unbedingt als kontinuierlicher Prozess und höchstens anfänglich als zeitlich begrenztes Projekt verstanden werden. Alle Beteiligten müssen einen Weg finden, mit neuen Security-Herausforderungen umgehen zu können, die u.a. bei der Produktentstehung und der Inbetriebnahme nicht bekannt waren.

Eine besondere Herausforderung wird eine Ausgestaltung sein, die die Bedürfnisse kleiner und mittelständischer Unternehmen berücksichtigt. Nur wenn Produkte und Dienste bereits unter Berücksichtigung von standardisierten Security-Eigenschaften angeboten werden, für die es eine entsprechende Infrastruktur zur einfachen Einbindung in die Unternehmensprozesse gibt, wird eine tragfähige Security-Landschaft entstehen. Schritte in diese Richtung wären ein einheitliches Kommunikations- und Security-Datasheet der Automatisierungsprodukte und standardisierte Meldungen über Security-Ereignisse mit einheitlicher Semantik, die so einfacher zentral zu erfassen und auszuwerten wären.

In den neuen Wertschöpfungsnetzwerken werden Informationen und die Vernetzung zu einem zentralen Gut. Durch das Teilen oder Bereitstellen von Informationen werden neue Möglichkeiten geschaffen. Gleichzeitig ergibt sich natürlich die Frage nach dem Eigentum an diesen Informationen und den Rollen und rechtssicheren Verantwortlichkeiten der beteiligten Parteien. Der Mehrwert durch die Auswertung von Informationen, die bei Partnern und Lieferanten erfolgt, ist abzuwägen gegen den möglichen Abfluss von Know-how.

Anhang

8 Anhang

8.1 Literaturverzeichnis

[1] VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik: Statusbericht; Industrie 4.0; Wertschöpfungsketten. Düsseldorf: VDI e.V., April 2014

[2] VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik: Statusbericht; Industrie 4.0; Gegenstände, Entitäten, Komponenten. Düsseldorf: VDI e.V., April 2014

[3] Acatech Studie, Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0, Abschlussbericht des Arbeitskreises Industrie 4.0. http://www.bmbf.de/pubRD/Umsetzungsempfehlungen_Industrie4_0.pdf

[4] IEC TR62794: Industrial-process measurement, control and automation – Reference model for representation of production facilities (Digital Factory), 2012

[5] IEC CD 62832 Digital Factory

[6] IEC 61987-10

[7] GMA Definitionen: http://www.iosb.fraunhofer.de/servlet/is/48960/

[8] Bundesamt für Sicherheit in der Informationstechnik: Die Lage der IT-Sicherheit in Deutschland 2014. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile

[9] www.iosb.fraunhofer.de/?Begriffel40

[10] https://www.dke.de/de/std/informationssicherheit/documents/nr%20industrie%204.0.pdf

[11] http://docs.oracle.com/javase/7/docs/technotes/guides/jar/jar.html#JAR_Manifest

[12] http://www.plattform-i40.de/sites/default/files/140326_Broschuere_Industrie_0.pdf

8.2 Glossar Industrie 4.0

Im Rahmen von Industrie 4.0 wachsen die Sprachen von Produktion und IKT (Informations- und Kommunikationstechnologie) zusammen. Es existieren jedoch historisch begründete Unterschiede und Unklarheiten bei wichtigen Begriffen rund um Industrie 4.0. Die Arbeitsgruppe „Begriffe“ im Fachausschuss VDI/VDE-GMA 7.21 „Industrie 4.0“ unter der Leitung von Frau Dr.-Ing. Miriam Schleipen vom Fraunhofer IOSB ist bemüht, eine gemeinsame „Basis“ (Terminologie) von Industrie 4.0 im Sinne sprachlicher und gedanklicher Konstrukte zu erarbeiten. Die Arbeiten erfolgen zudem in enger Zusammenarbeit mit den zuständigen Komitees (z. B. DKE/UK 921.1) des Fachbereichs 9 der DKE (z. B. DKE/UK 921.1). und werden mit der AG2 „Referenzarchitektur“ der Plattform Industrie 4.0 abgestimmt.

Ziel ist ein gemeinsames Verständnis der grundlegenden Begriffe! Dabei wird auf bestehenden Normen und Standards aus den Bereichen IKT und Produktion aufgesetzt.

Im Umfeld von Industrie 4.0 werden Begrifflichkeiten und Konzepte aus unterschiedlichen Domänen aufgegriffen (etwa aus dem IKT-Bereich die Orchestrierung von Diensten in einer service-orientierten Umgebung). Manche Begrifflichkeiten sind aber in den beteiligten Domänen unterschiedlich besetzt (etwa Service (Dienst) im IKT-Bereich gegenüber der Produktion). Andere Begriffe sind sogar innerhalb einer Domäne mehrdeutig oder unpräzise (etwa Komponente). Diese sprachlichen und konzeptionellen Unterschiede und Ungenauigkeiten, sowie der Bedarf nach Erklärungen zu „fachfremden Konzepten“ sind ein Hindernis in der Entwicklung übergreifender komplexer technischer Lösungen für Industrie 4.0 und in der Normung.

Mit dem Glossar wird also eine gemeinsame Basis für Begrifflichkeiten im Rahmen von Industrie 4.0 geschaffen werden, welche die unterschiedlichen Sichtweisen und Anforderungen berücksichtigt. Dies soll die Zusammenarbeit über die Grenzen von Unternehmen und Branchen hinweg erleichtern und ist Voraussetzung für die Normung.

Die aktuellen Definitionen sind unter [9] zu finden.

8.3 Autorenteam

Der fachliche Input für diese Umsetzungsstrategie wurde in den Arbeitsgruppen der Plattform Industrie 4.0 erarbeitet. Die nachfolgend genannten Autoren haben die schriftliche Zusammenfassung in Form dieses Berichts vorgenommen.

Autorenteam Kapitel 1- 4:

- Wolfgang Dorst (BITKOM e.V.)
- Carsten Glohr (Detecon International GmbH)
- Thomas Hahn (Siemens AG)
- Frank Knafla (Phoenix Contact Electronics GmbH)
- Dr. Ulrich Loewen (Siemens AG)
- Roland Rosen (Siemens AG)
- Thomas Schiemann (T-Systems International GmbH)
- Friedrich Vollmar (IBM Deutschland GmbH)
- Christoph Winterhalter (ABB AG)

Autorenteam Kapitel 5:

- Dr. Bernhard Diegner (ZVEI e.V.)
- Johannes Diemer (Hewlett Packard GmbH)
- Dr. Mathias Dümmler (Infineon Technologies AG)
- Stefan Erker (Huber + Suhner GmbH)
- Dr. Werner Herfs (RWTH Aachen, WZL – Lehrstuhl für Werkzeugmaschinen)
- Claus Hilger (HARTING IT Services GmbH & Co. KG)
- Dr. Lutz Jänicke (Innominate Security Technologies AG)
- Prof. Dr.-Ing. Jürgen Jasperneite (Institut für industrielle Informationstechnik / inIT, Hochschule OWL, Lemgo und Fraunhofer IOSB-INA)
- Johannes Kalhoff (Phoenix Contact GmbH & Co. KG)
- Prof. Dr. Uwe Kubach (SAP AG)
- Dr. Ulrich Löwen (Siemens AG)
- Georg Mattis (Huber + Suhner GmbH)
- Georg Menges (NXP Semiconductors Germany GmbH)
- Frank Mildner (Deutsche Telekom AG)
- Mathias Quetschlich (MAN Truck & Bus AG)
- Ernst-Joachim Steffens (Deutsche Telekom AG)
- Dr. Thomas Stiedl (Robert Bosch GmbH)

Autorenteam Kapitel 6:

- Dr. Peter Adolphs (Pepperl+Fuchs GmbH)
- Dr. Heinz Bedenbender (VDI e.V.)
- Martin Ehlich (Lenze SE)
- Prof. Ulrich Epple (RWTH Aachen)
- Martin Hankel (Bosch Rexroth AG)
- Roland Heidel (Siemens AG)
- Dr. Michael Hoffmeister (Festo AG & Co.KG)
- Haimo Huhle (ZVEI e.V.)
- Bernd Kärcher (Festo AG & Co.KG)
- Dr. Heiko Koziolek (ABB AG)
- Reinhold Pichler (VDE e.V. DKE)
- Stefan Pollmeier (ESR Pollmeier GmbH)
- Frank Schewe (Phoenix Contact Electronics GmbH)
- Thomas Schulz (GE Intelligent Platforms GmbH)
- Dr. Karsten Schweichhart (Deutsche Telekom AG)
- Dr. Armin Walter (Lenze SE)
- Bernd Waser (Murrelektronik GmbH)
- Prof. Dr. Martin Wollschlaeger (TU Dresden)

Autorenteam Kapitel 7:

- Dr. Lutz Jänicke (Innominate Security Technologies)
- Michael Jochem (Bosch Rexroth AG)
- Hartmut Kaiser (Secunet Security Networks AG)
- Marcel Kisch (IBM Deutschland GmbH)
- Dr. Wolfgang Klasen (Siemens AG)
- Jörn Lehmann (VDMA e.V.),
- Lukas Linke (ZVEI e.V.)
- Jens Mehrfeld (BSI)
- Michael Sandner (Volkswagen AG)