

1 Architektur einer vernetzten, adaptiven Produktion

R. Schmitt, N. König, S. Jung, M. Peterek

Gliederung

1	Einleitung	6
2	Anforderungen der Produktion an Vernetzung und Adaptivität	7
2.1	Universelle Konnektivität – „Connect Everything“	7
2.2	Datenintegrität	10
2.3	Souveränität	12
3	Architektur für die vernetzte, adaptive Produktion	13
3.1	Standortübergreifende Vernetzung	14
3.2	Dynamische Vernetzung	15
3.3	Plattformen für die unternehmensübergreifende Vernetzung	17
4	Ausblick	18

Kurzfassung

Architektur einer vernetzten, adaptiven Produktion

Die Vision einer vernetzten adaptiven Produktion gelingt nur über eine leistungsfähige Infrastruktur. Was sind die Leistungsmerkmale einer solchen Infrastruktur und wie sieht eine skalierbare Umsetzung im Produktionsumfeld aus? Welche Bausteine ermöglichen die echtzeitfähige Bereitstellung von Information entlang der gesamte Prozesskette und können auch ohne bedeutende Mehrkosten in die Produktion integriert werden? Das Internet of Production ist der Rahmen für eine solche durchgängige, sichere und leistungsfähige Architektur. Die Integrität, Souveränität und Echtzeitfähigkeit der erhobenen Daten ist dabei notwendige Bedingung für die Nutzbarmachung in der Produktion.

Abstract

Architecture of a Networked Adaptive Production

The vision of a networked adaptive production can only succeed with a high-performance infrastructure. What are the performance characteristics of such an infrastructure and what does a scalable implementation in the production environment look like? Which building blocks enable the real-time provision of information along the entire process chain and can be integrated into production without significant additional costs? The Internet of Production is the framework for such an integrated, secure and powerful architecture. The integrity, sovereignty and real-time capability of the collected data is a necessary condition for the utilization in production.

1 Einleitung

Die wirtschaftliche Situation in Deutschland ist maßgeblich auf die Stärke der produzierenden Industrie zurückzuführen. Sie schafft wertschöpfende Arbeitsplätze und Produkte, die höchsten Qualitätsanforderungen genügen. Dabei sehen Unternehmen die Digitalisierung zunehmend als Chance [1] – durch die Sammlung und Verwertung von Produktions- und Produktdaten über den gesamten Produktlebenszyklus lassen sich Produktivitätssprünge erzielen oder gleich gänzlich neue datenbasierte Geschäftsmodelle anbieten. Diese Datenmenge wird bis 2025 auf 79,4 Billionen Gigabyte anwachsen [2], birgt bei Datenverlust jedoch ein Risiko des Know-how-Abflusses oder bei Manipulation gar die Nichterfüllung von Kunden-, Qualitäts- oder Gesetzesanforderungen. Die große Datenmenge dem Wertschöpfungsnetzwerk sicher bereitzustellen, um auf deren Basis die Produktivität zu erhöhen, ist ein kritischer Faktor für die Zukunftsfähigkeit von Unternehmen.

Dies macht deutlich, dass die größtmögliche Realisierung von Potenzialen der Digitalisierung unabdingbar ist, um im Wettbewerb produzierender Unternehmen auf globalen Märkten dauerhaft eine Vorreiterrolle einnehmen zu können. Aufgrund steigender Komplexität in den Produktionsabläufen steigt die Anzahl der immanenten Wechselwirkungen einzelner Prozesse immer stärker an. Darüber hinaus führt die steigende Individualisierung der Produkte zu einer deutlichen Erhöhung der Prozessvarianz. Die konsequente Nutzung des Wissens, welches in den exponentiell ansteigenden Datenmengen steckt, verfügt dabei über eine starke Hebelwirkung zur kontinuierlichen *Verbesserung der produkt- und prozessbezogenen Qualität*. Anstatt einer reinen Beurteilung anhand der Prozessdaten können auch vorhandene Informationen über Zwischenerzeugnisse und individuelle Baugruppen berücksichtigt werden. Gleichzeitig kann so durch eine qualitätsgetriebene Optimierung des Ressourceneinsatzes den stetig zunehmenden Nachhaltigkeitsforderungen aus Bevölkerung und Politik begegnet werden. Der rasante *Anstieg an Datenverfügbarkeit* liegt zum einen an einer immer stärkeren Vernetzung von Lieferanten, Produzenten und Kunden, zum anderen an der Nutzung einer steigenden Anzahl unterschiedlicher Informationskanäle von integrierter Sensorik bis zu online Produktreviews.

Ziel ist dabei immer einen sehr konzentrierten und bewussten Umgang mit den Themen der Vernetzung und Digitalisierung zu ermöglichen. Jedoch ist die Vernetzung kein Selbstzweck, sondern soll im Sinne des Internet of Production (IoP) einen direkten Mehrwert für die Produktion bedeuten. Letzterer entsteht durch eine durchgängige Nutzung der verfügbaren Daten – *Turning Data into Value*.

In diesem Beitrag liegt der Fokus an der notwendigen Infrastruktur, die eine solche Nutzung erst ermöglicht. Es sollen Möglichkeiten aufgezeigt werden, die bereits jetzt einsetzbar und integrierbar sind. Die Kommunikation erfolgt dabei in der Regel in verteilten Kommunikationsnetzwerken. Eine Infrastruktur im Sinne des IoP berücksichtigt dabei funktionale, physikalische und konzeptionelle Perspektiven des Digitalen Schattens [3] in der Produktion. Die physische Infrastruktur unterstützt die verteilten Multi-Agent-Modellausführungen und Datenflüsse mit hoher Leistung, Zuverlässigkeit und Sicherheit in verteilten Kommunikationsnetzen. Darüber hinaus muss die Infrastruktur den Digitalen Schatten als Wissensdiagramm heterogener Datenspeicher und Agenten konsistent verwalten, formale Zuordnungen zwischen ihnen ermöglichen und Code für eine effiziente Datenintegration und einen effizienten Datenaustausch generieren. Die angestrebte Infrastruktur schafft eine neuartige Kombination von datengesteuerten Lernalgorithmen und physikalischen oder Simulationsmodellen, um über den Digitalen Schatten große Datenmengen in Instanzen und formale Modelle zu verwandeln, die

zusammen mit Kontextänderungen wiederum neue Daten erzeugen. Aber auch die dabei entstehenden Herausforderungen, wie Datenintegrität und Datensouveränität, sollen beleuchtet werden.

2 Anforderungen der Produktion an Vernetzung und Adaptivität

Grundlage der vernetzten, adaptiven Produktion bildet die vollständige Vernetzung von Maschinen, Produkten und Menschen mittels Software zu einem cyber-physischen Produktionssystem [4]. Dafür sind unterschiedliche Wertschöpfungsglieder einzubinden. Für eine mögliche Skalierung des Ansatzes auf die gesamte Wertschöpfungskette, die alle Phasen des Produktlebenszyklus abbildet, d.h. von der Idee über die Entwicklung, Fertigung, Nutzung, Wartung bis zum Recycling, ist eine einfache und schnelle Einbindung vieler unterschiedlicher Teilnehmer wie Produktionsmaschinen, Datenbanken und IT-Systeme notwendig. Als Ideal werden daher Technologien angestrebt, die eine *universelle Konnektivität* bieten.

Mitunter ist ein Datenaustausch zwischen mehreren Unternehmen mit einer dezentralen Datenspeicherung erforderlich. Hierdurch wird der Produktstatus in allen Phasen transparent und rückverfolgbar. Die transparente Rückverfolgung bietet im Produktschadensfall die bestmögliche Versicherung der Wertschöpfungspartner gegen Regressforderungen und Reputationsverluste. Die Vernetzung von Wertschöpfungsketten und die dezentrale Verfügbarkeit von Daten aller Partner ist somit Treiber für die Wettbewerbsfähigkeit.

Die grundlegende Forderung nach Vernetzung muss jedoch einhergehen mit der Gewährleistung der Sicherheit von Daten, wobei deren Austausch durch Verschlüsselung gegen unbefugten Zugriff und Nutzerberechtigungen sichergestellt werden muss. Insbesondere die Manipulationssicherheit der Daten zum Qualitätsnachweis ist innerhalb der Wertschöpfungskette in Form einer Echtheitsprüfung essentiell. Zusammenfassend leiten sich verschiedene Handlungsfelder ab, die im Folgenden beschrieben werden.

2.1 Universelle Konnektivität – „Connect Everything“

Die oben genannte Forderung, die verschiedenen Glieder der Wertschöpfung vollständig zu vernetzen, stellt Unternehmen vor die Herausforderung, Daten in einem heterogenen Ressourcennetzwerk zwischen unterschiedlichen Endpunkten über verschiedene Schnittstellen und in verschiedenen Protokollen zu übertragen. Die Forderung nach einer einfachen und schnellen Einbindung ist diametral hierzu, bedeutet sie doch in Konsequenz die Komplexität in der Auswahl aus den vielzähligen Optionen stark zu reduzieren.

Eine *universelle Konnektivität* soll dagegen auf eine geringstmögliche Auswahl an Übertragungstechnologien zurückgreifen können, ohne dass die jeweilige Applikation an Leistungsfähigkeit einbüßt. Eine Auswahl kann an Hand der folgenden Kriterien getroffen werden:

- *Mobilität* – Fähigkeit, Daten von bzw. zu mobilen Gütern über weite Flächen zu übertragen, z.B. mobile und sensorgestützte Roboter, kabellose Sensoren, autonome Förderzeuge (AGV).
- *Echtzeitfähigkeit* – Möglichkeit der Synchronisation von Endgeräten sowie Übertragungsraten und Datentransferintervalle im Bereich weniger Millisekunden, um damit eine Konnektivität bis in die Feldebene zu ermöglichen.

- *Übertragungsbandbreite* – Vermögen, Daten mit Übertragungsraten bis in den einstelligen GBit/s Bereich je Endgerät zu übertragen.
- *Skalierbarkeit* – Vermögen, die oben genannten Eigenschaften für mehrere Endgeräte gleichzeitig zur Verfügung zu stellen.

Eine besondere Bedeutung kommt der echtzeitfähigen Kommunikation zu. Bislang ist diese primär auf die Feldebene beschränkt. Eine umfängliche Nutzung der Daten aus dieser Ebene, d.h. die Erfassung, Aggregation und Verarbeitung der Daten sowie die Rückkopplung in die Wertschöpfungskette bis in die Feldebene, setzt voraus, dass die Echtzeitfähigkeit der Datenübertragung in allen Ebenen gewährleistet ist.

Tabelle 1: Bewertung verschiedener Technologien für die Konnektivität

Kriterium	WLAN	Bluetooth	ZigBee	5G	Ethernet
<i>Mobilität</i>	+	o	o	+	—
<i>Echtzeitfähigkeit</i>	—	o	—	+	+
<i>Übertragungsbandbreite</i>	o	—	—	+	+
<i>Skalierbarkeit</i>	o	—	o	+	+

Tabelle 1 zeigt eine qualitative Bewertung verschiedener Konnektivitätslösungen in Bezug auf die oben angeführten Kriterien. WLAN erfüllt die Anforderungen hinsichtlich Mobilität im industriellen Kontext. Über eine entsprechende Anzahl an WLAN Access Points lässt sich prinzipiell ein WLAN-Netz für eine gesamte Produktionshalle aufspannen. Es gibt eine Vielzahl an kostengünstigen Sende-Empfangsmodulen für die Integration in die Produktionsausrüstung. Da WLAN im unlizenzieren Spektrum betrieben wird, ist es herausfordernd, eine robuste und performante Konnektivität zu erreichen. WLAN-Netze sind typischerweise bandbreitenoptimiert, das heißt, dass die zur Verfügung stehende Bandbreite auf alle Teilnehmer aufgeteilt wird. Dies und die Tatsache, dass ein Betrieb im unlizenzieren Spektrum anfällig für Störungen ist, legen den Schluss nahe, dass eine Echtzeitfähigkeit mit niedriger und reproduzierbarer Latenz mit WLAN schwer zu realisieren ist. Zwar lassen sich seit Einführung von Technologien gemäß des IEEE 802.11ac Standards Übertragungsraten von bis zu 1,3 GBit/s erreichen, jedoch werden diese auf alle Teilnehmer aufgeteilt. Auf Grund der hier genannten Eigenschaften ist insbesondere die robuste, echtzeitfähige Übertragungseigenschaft für WLAN kritisch zu sehen.

Bluetooth verfügt auf Grund der vergleichsweise geringen Reichweite von mehreren 10 m sowie der vorwiegenden Nutzung im Peer-to-Peer Verfahren mit nur wenigen Teilnehmern über eine begrenzte Mobilitätseignung. Auf Grund der geringen Anzahl an verbundenen Endgeräten lassen sich über Bluetooth vergleichsweise geringe, reproduzierbare Übertragungslatenzen von bis zu 2 ms erreichen. Auch hier gilt wie bereits für WLAN, dass die Übertragung in einem unlizenzieren Spektrum stattfindet und generell störanfällig ist. Als Übertragungsbandbreiten werden bis zu 2 Mbit/s angegeben, was für zahlreiche Anwendungen nicht ausreichend ist. Ein großer Schwachpunkt von Bluetooth ist die mangelnde Skalierbarkeit. Es lassen sich keine Netze mit einer größeren Anzahl an Teilnehmern wie z.B. Sensornetze realisieren, weshalb es als universelle Konnektivitätslösung ausscheidet.

Ähnliche Eigenschaften wie Bluetooth besitzt ZigBee, welches von der Skalierbarkeit jedoch besser ist, da es sich als Mesh verbindet und damit generell mehr Teilnehmer integrieren kann. Nachteilig ist die geringe Übertragungsbandbreite von max. 250 kBit/s sowie die höhere Latenz im zweistelligen ms-Bereich.

5G dagegen unterscheidet sich von den anderen drahtlosen Verbindungstechnologien dadurch, dass die Übertragung im lizenzierten Spektrum erfolgt und damit deutlich weniger stör anfällig ist als die vielen Verfahren, die im unlizenzierten Frequenzbereich von 2,4 GHz übertragen. 5G lässt in der sogenannten Ultra-Reliable Low Latency Communication (URLLC) Latenzen im einstelligen ms-Bereich zu. Eine weitere Ausprägung ist die sogenannte Enhanced Mobile Broadband (eMBB) Übertragung, die dafür sorgt, dass mit bis zu 10 GBit/s genügend Kapazitäten zur Verfügung stehen. Ebenso ist es möglich, die genannten Bedingungen für eine große Anzahl an Teilnehmern zu garantieren und damit die Konnektivätslösung im industriellen Umfeld für ein Unternehmen leicht zu skalieren. Die Möglichkeit in Zukunft ein Time Sensitive Network (TSN) [5] über 5G zu realisieren eröffnet mit einer synchronisierten Datenübertragung das Potenzial, Sensordaten mit einem Zeitstempel zu versehen oder Steuerungsaufgaben in eine Cloud auszulagern.

Ethernet hat sich als Standard in der drahtgebundenen Kommunikation etabliert. Über eine zeitgemäße Netzwerkinfrastruktur sind die Anforderungen hinsichtlich der Übertragungsbandbreite mit 1 GBit/s über Kupferleitungen und der Teilnehmerzahl leicht skalierbar. TSN wird auch für Ethernet umgesetzt, so dass mit Hilfe der Precision Time Protocol (PTP) die Echtzeitfähigkeit gelöst werden kann. Erste Produkte hierfür sind auf dem Markt erhältlich. Die Konnektivität für mobile Anwendungen kann wegen der Kabelverbindung selbstverständlich nicht gewährleistet werden.

Die Analyse zeigt, dass der Wunsch einer universellen Konnektivität durch eine Kombination von Ethernet für die kabelgebundene Infrastruktur (Server, stationäre Produktionsausrüstung) sowie 5G für die mobile Produktionsausrüstung erreicht werden. Wie eine solche Architektur aussehen kann, zeigt Bild 1. Verschiedene kabellose Sensoren mit 5G-Übertragung befinden sich an unterschiedlichen Messorten in der Produktion, z.B. Körperschall-, Beschleunigungs- oder Kraftsensoren auf Werkstücken zur Prozessüberwachung, Schwingungssensoren oder Mikrofone in Werkzeugmaschinen zur Zustandsüberwachung oder verteilte Sensoren für Temperatur oder Luftfeuchte zur Überwachung der Infrastruktur. Die verschiedenen Sensoren übertragen Messdaten und empfangen Konfigurationsdaten, zum Beispiel zur Bestimmung der Messfrequenz oder Ein/Aus, drahtlos mittels 5G. Die Daten werden an der 5G-Basisstation beziehungsweise dem 5G-Core per Local Breakout über Ethernet in die Produktions-IT gekoppelt. Hier können Sie beispielsweise in einer Factory Cloud, einer on-premise edge-cloud Lösung, in verschiedenen virtuellen Maschinen verarbeitet werden. Die Werkzeugmaschine kann über verschiedene hardware- oder softwarebasierte Monitoring-Möglichkeiten ihren jeweiligen Bearbeitungszustand, unter anderem Achskoordinaten oder Spindeldrehzahlen, als Datenstrom übermitteln. Die Datenströme der Sensoren und Maschinen können in der Factory Cloud zentral zusammengeführt und ausgewertet werden. Die Prozessdokumentation kann als Digitaler Zwilling in Datenbanken abgelegt werden und steht für weitere Auswertungen zur Verfügung. Prozesseingriffe und Prozessregelungen können von der Factory Cloud drahtgebunden über Machine-to-Machine (M2M) Kommunikation zur Werkzeugmaschine übertragen werden. Weitere Informationen sind im Deliverable 3.2 des EU-Projekts „5G-SMART“ zu finden [6]. Im Falle einer Regelung ist in jedem Fall eine Echtzeitfähigkeit aller Kommunikationskanäle inklusive der Factory Cloud notwendig.

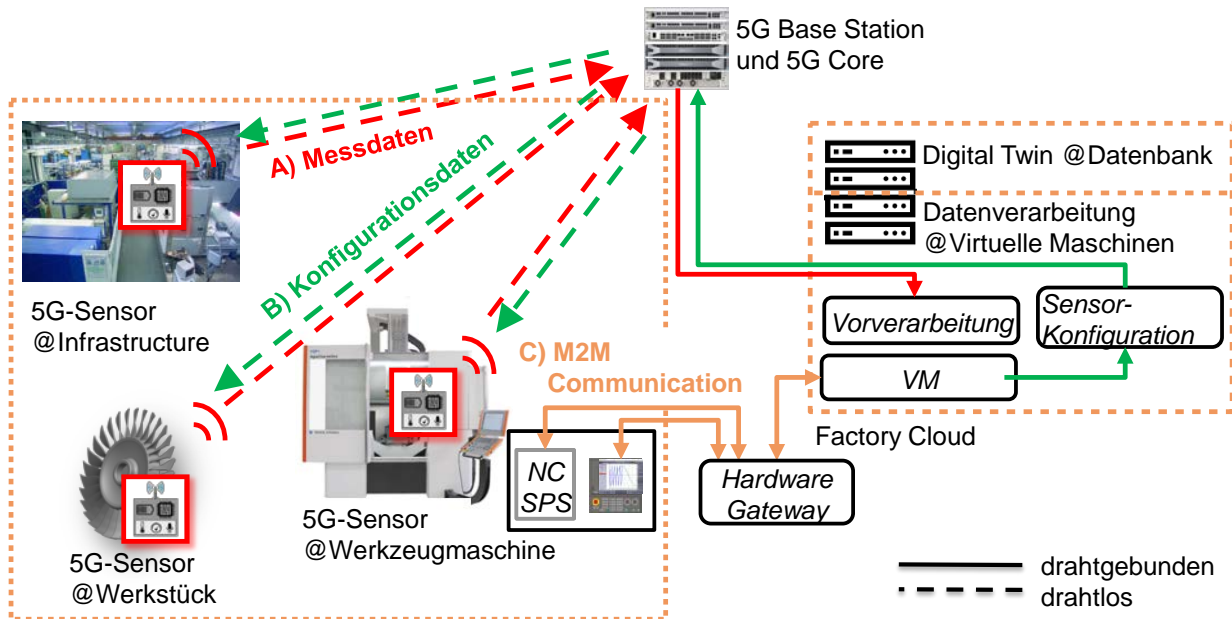


Bild 1: Architektur für ein 5G-basiertes Prozess- und Zustandsmonitoring (nach [6])

Potenziell kann die Konnektivität über 5G auch für nicht-mobile Anwendungen sinnvoll sein, etwa wenn die Datenraten über 1 GBit/s liegen oder eine Verlegung zusätzlicher Ethernet-Verbindungen wirtschaftlich nicht sinnvoll ist.

Neben der reinen Datenverfügbarkeit gilt es noch zwei weitere klassischen Ziele der Informationssicherheit zu betrachten – die Datenintegrität und die Datensouveränität.

2.2 Datenintegrität

Durch diese neu entstandene, durchgehende Konnektivität werden die Verfügbarkeit und Nutzung von Daten für Unternehmen somit immer einfacher. Vernetzte Produktionsressourcen produzieren laufend Daten und die neu entstandene IT-Infrastruktur ist in der Lage, Daten automatisiert und effizient zu speichern, zu verarbeiten und zu nutzen.

Mit dieser zunehmenden Vernetzung und Verfügbarkeit von Daten ergeben sich immer neue Herausforderungen in Bezug auf die Zuverlässigkeit und Vertrauenswürdigkeit von Daten – die sogenannte *Datenintegrität* (siehe Bild 2). Sendet zum Beispiel eine Person, in dem Fall Alice, ein Datenpaket zu ihrem Kollegen Bob, beschreibt die Datenintegrität die Korrektheit, Vollständigkeit und Konsistenz der Daten, sodass sichergestellt ist, dass Mallet die Daten nicht verändert hat. Dies wird insbesondere dann relevant, wenn sich Entscheidungen in Bezug auf das Geschäft oder die Produktion in zunehmendem Maße auf Daten stützen. So geben laut Aussage des Bundesamts für Sicherheit in der Informationstechnik 87% der Betroffenen an, dass Cyber-Angriffe erhebliche Konsequenzen für den Betriebsablauf verursachten [7]. Aus diesem Grund muss sichergestellt sein, dass die zugrundeliegenden Daten korrekt sind. Kann eine Veränderung oder Beschädigung der Daten nicht verhindert werden, so muss dies mindestens erkannt werden. Folgende Begriffe sind im Kontext der Datenintegrität wichtig:

- Richtigkeit des Inhaltes – korrekte Abbildung von realen Sachverhalten.
- Unveränderter Zustand – Daten werden bei einer Übertragung unverändert zugestellt und durch Systeme bei einer Verwendung nicht verändert.

- Erkennung von Modifikation – unerwünschte Modifikationen werden erkannt.
- Zeitliche Korrektheit – relevante Bedingungen wie Reihenfolge oder Verzögerungen werden eingehalten.
- Sicherstellung regulatorischer Vorgaben – Einhaltung der DSGVO und Datensicherheit.

Somit unterscheidet sich die Datenintegrität von der Datensicherheit in der Zielstellung – die Datensicherheit bezieht sich auf den Schutz von Daten und der Minimierung des Risikos eines Datenverlustes, wobei die Datenintegrität sich auf die Vertrauenswürdigkeit von Daten bezieht.

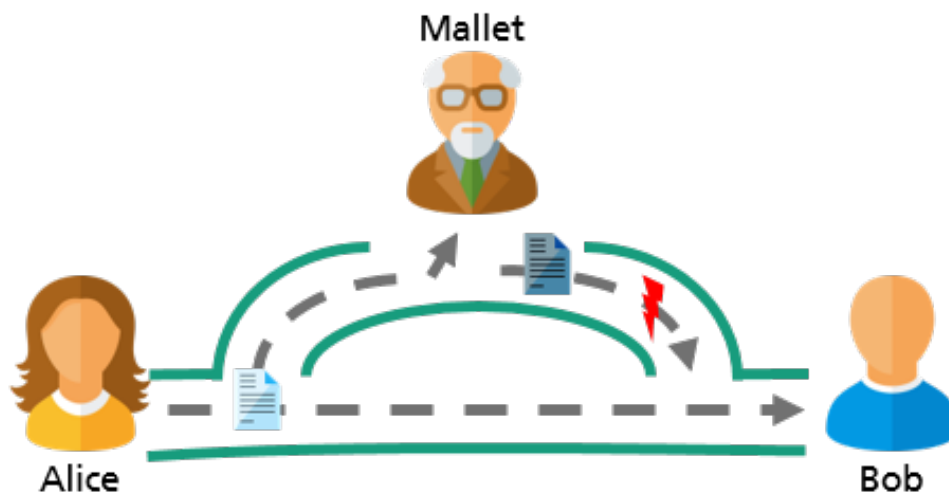


Bild 2: Schaubild der Datenintegrität

Die Datenintegrität umfasst somit Maßnahmen, Daten während deren gesamter Lebensdauer vor unautorisierter Veränderung zu schützen. Besonders im öffentlichen Fokus gewinnt das Thema häufig im Zusammenhang mit kriminellen Risiken an Aufmerksamkeit, welche z.B. unautorisierte Angriffe oder Datendiebstahl umfasst. Dabei zielen solche Angriffe darauf ab, Daten zu verändern oder zu beschädigen, um Unternehmensprozesse zu manipulieren oder stillzulegen. Dabei können Gefahren für die Datenintegrität sehr vielschichtig sein und sich neben böswilligen Handlungen ebenfalls auf menschliches Versagen und auf technische Fehler beziehen.

- Menschliche Fehler – Informationen können durch Mitarbeiter beabsichtigt oder unbeabsichtigt falsch erfasst oder gelöscht werden.
- Übertragungsfehler - werden Daten zwischen Systemen transferiert, so können Daten beabsichtigt oder unbeabsichtigt verloren oder verändert werden.
- Kriminelle Handlungen – Unautorisierte Zugriffe auf Daten mit dem Ziel diese bewusst zu manipulieren oder zu entwenden.
- Technische Fehler – sind essentielle Infrastrukturkomponenten defekt, wie z.B. Netzwerkkomponenten, Serverhardware oder Softwaresysteme, können Daten falsch oder unvollständig sein.

Die Hauptaspekte der Datenintegrität sind somit hauptsächlich die Nachvollziehbarkeit und Transparenz. Im Sinne der Datenintegrität gilt es demnach, geeignete Maßnahmen mit Hilfe von geeigneten Systemen, Prozessen und Standards zu entwickeln, um das Risiko von Gefahrenquellen zu minimieren oder komplett auszuschließen. Die besondere

Herausforderung hierbei ist die flächendeckende Auswirkung auf globaler Ebene auf Grund der allgegenwärtigen Vernetzung. Unternehmen und Systemhersteller werden in Zukunft noch enger zusammenarbeiten und vorliegende Abhängigkeiten identifizieren und auflösen müssen. Eine technisch gelungene aber dafür mit heterogenen Systemen, wie sie in der Industrie häufig historisch gewachsen sind, inkompatible Lösung, liefert an der Stelle keinen Mehrwert. Die Herausforderung hierbei ist, den Aspekt der Datenintegrität ausreichend zu beleuchten, den Fortschritt jedoch nicht zu hemmen oder zu verlangsamen.

2.3 Souveränität

Gemäß einer Studie von PwC [8] äußern 59% von 200 befragten Führungskräften deutscher Unternehmen, dass sie Angst haben, die Kontrolle über die eigenen Daten zu verlieren. Dies ist verbunden mit Bedenken, wertvolle Daten und Geschäftsgeheimnisse zu verlieren, bei 57% der Befragten. Fehlende Möglichkeiten, diesen Bedenken organisatorisch, technisch und regulatorisch zu begegnen, können somit als Hindernis für die Digitalisierung in Unternehmen gesehen werden. Neben den Aspekten Sicherheit und Vertrauen ist auch die *Datensouveränität* zu adressieren, auf welche im Folgenden näher eingegangen wird.

Die Datensouveränität ist zu verstehen als die Hoheit eines Dateneigners über die Nutzung der eigenen Daten souverän und exklusiv zu entscheiden. Exklusivität bedeutet in diesem Zusammenhang, dass die Zuständigkeit dieser Entscheidung eindeutig ist (siehe Bild 3). Eine Datensouveränität versetzt Unternehmen somit in die Lage, die Verarbeitung und Nutzung der Daten proaktiv steuern zu können. Dies ist genau genommen unabhängig von den Fragen des Datenschutzes und der Integrität, jedoch profitiert die Souveränität von der Gewissheit, dass die Daten korrekt und vor unbefugtem Zugriff geschützt sind. Als Beispiel ist die Monetarisierung von Daten genannt, welche ein Unternehmen souverän umsetzen kann, wenn es sicherstellen kann, dass die Daten beim Kunden korrekt und unversehrt ankommen, insbesondere, wenn daran Haftungsfragen geknüpft sind. Damit ist ebenfalls verbunden, dass der Ort der Speicherung und der Verarbeitung der Daten zu allen Zeiten bekannt ist, genauso wie die Möglichkeit, die Löschung der Daten zu kontrollieren.

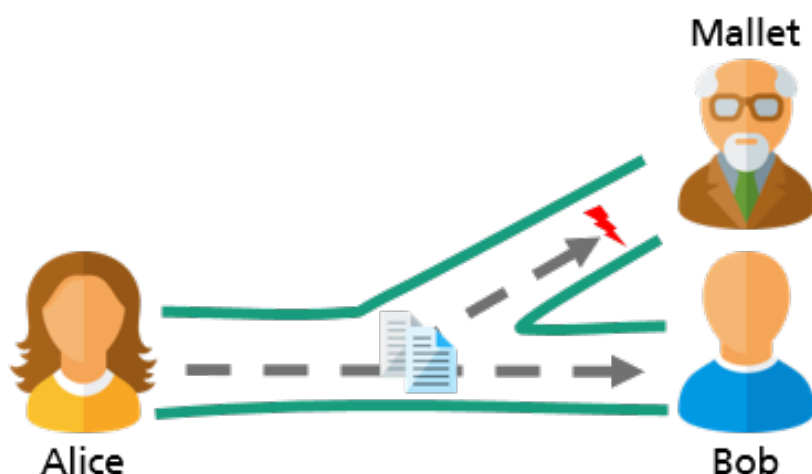


Bild 3: Schaubild der Datensouveränität

Die DSGVO liefert die rechtliche Grundlage für eine Datensouveränität, wenngleich sie primär auf die Verarbeitung persönlicher Daten abzielt. Während eine Verordnung einen Standard auf der rechtlichen Seite setzt, braucht es auch auf der technischen Seite einen

Standard für den Austausch von Unternehmensdaten. Hier setzt die International Data Spaces (IDS) Association mit seinen mehr als 100 Mitgliedern an. Im Rahmen mehrere Projekte wurde ein Referenzarchitekturmodell geschaffen, welches den Datenaustausch zwischen Datengeber und Datennutzer und die dafür nötigen Konnektoren sowie Zertifizierung, Verschlüsselung, Datenstruktur bis hin zur Übermittlung des Nutzungsvertrags für die Daten spezifiziert [9].

Neben der Spezifizierung ist auch das Schaffen eines Datenraums sehr wichtig, um das Konzept der Souveränität auch als digitale Souveränität zu begreifen, welche die dafür notwendige Infrastruktur mit einbezieht. Das Projekt GAIA-X schafft die Randbedingungen für einen solchen Datenraum auf europäischer Ebene und bringt Datengeber und -nutzer mit Anbietern für Cloud- und Edge-Cloud-Lösungen zusammen. Über die Vernetzung dezentraler Infrastrukturdienste hin zu einem homogenen, nutzerfreundlichen System haben auch Unternehmen die Chance, sich mit der GAIA-X Infrastruktur zu verbinden und ihre Daten abzulegen und zu teilen.

Beide Initiativen, International Data Spaces und GAIA-X, tragen zur Sicherheit und Souveränität einer europäischen Plattformökonomie und Wettbewerbsposition bei.

3 Architektur für die vernetzte, adaptive Produktion

Auf Grund der zunehmenden Spezialisierung von Unternehmen und der damit einhergehenden Fragmentierung von Prozessketten hat die Konnektivität dabei längst die Grenzen der Produktion überwunden und eine standortübergreifende Vernetzung gewinnt zunehmend an Bedeutung (siehe Bild 4). Dies stellt insbesondere neue Anforderungen an *einheitliche Kommunikations- und Datenkonzepte* als auch eine *leistungsfähige Ende-zu-Ende Infrastruktur*. So ergeben sich im Zuge der Digitalisierung unter anderem Problemstellungen wie Echtzeitfähigkeit zwischen den Netzwerkknoten verschiedener Standorte, eine effiziente und skalierbare Handhabung und Verarbeitung der erzeugten Datenmenge für Big Data Anwendungen und vor allem ein sicherer Zugriff und Austausch bei transparenten Mehrparteiennetzwerken.

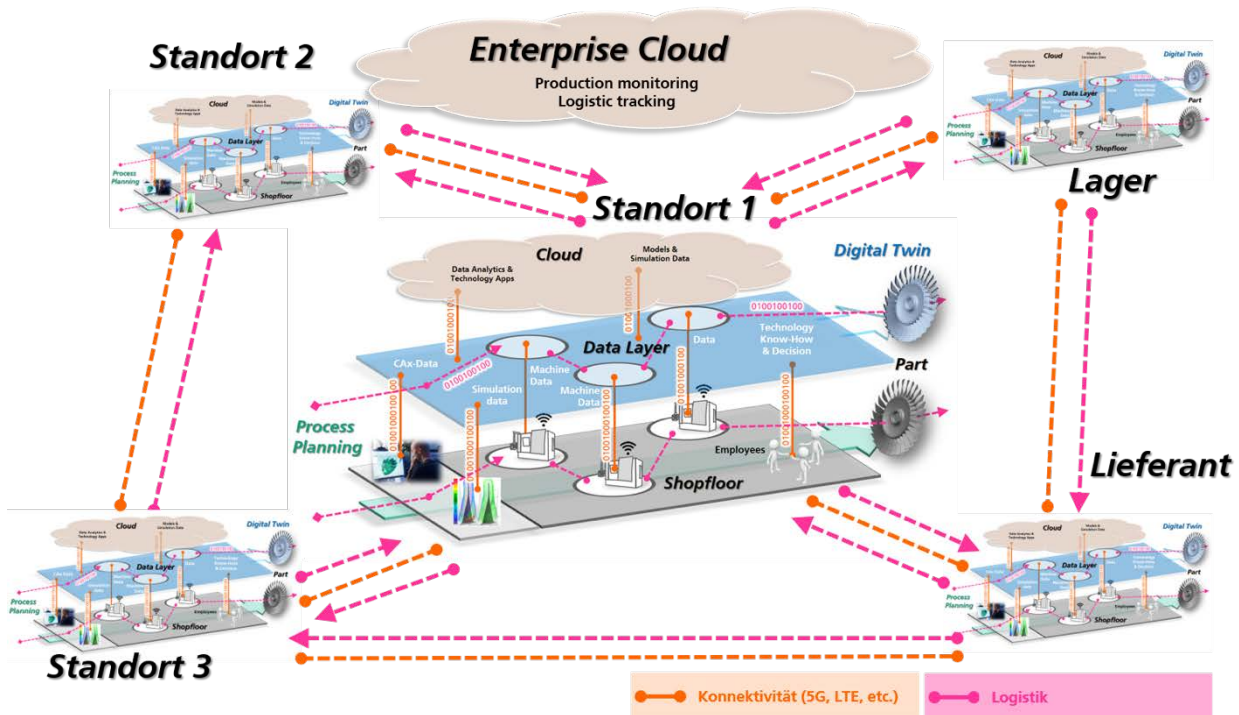


Bild 4: Architektur einer durchgängigen, standortübergreifenden Vernetzung

3.1 Standortübergreifende Vernetzung

Oberstes Ziel der Produktion ist stets die Herstellung eines Bauteils unter Einhaltung aller vorgegebenen Toleranzen. Daher ist es wichtig, alle Daten aufzuzeichnen, die Hinweise auf die Entwicklung des Bauteilzustands entlang der Prozesskette geben können. Durch Sensoren in der Fertigungsmaschine lassen sich zum Beispiel wertvolle Informationen über Vibrationen, Bearbeitungskräfte und Prozesstemperaturen gewinnen, an denen der Anwender sehen kann, ob eine Toleranzverletzung droht oder nicht. Die Voraussetzung dafür ist die vollständige Vernetzung der Maschinen, Sensoren, Simulationstools und Datenbanken mit der Historie der gefertigten Bauteile. Daher müssen produzierende Unternehmen in der heutigen Zeit praktisch in zwei Welten agieren – in einer realen, in der mit Bauteilen, Werkzeugen und Maschinen umgegangen werden muss und getrennt davon in einer virtuellen Welt, in der Prozess- und Bauteildaten zu verwalten sind.

Disruptive Technologien versprechen hier eine Lösung für eine *durchgängige Ende-zu-Ende Konnektivität*. Auf lokaler Ebene hat sich zunehmend der Bedarf nach drahtloser Kommunikation aufgetan, um eine leichte Nachrüstbarkeit ohne Umbau der vorhandenen Infrastruktur zu erreichen oder um prozessintegrierte oder mobile Sensorik mit in das Produktionsnetzwerk integrieren zu können. Dabei lässt sich unterscheiden zwischen sehr lokalen Verbindungsmöglichkeiten, wie zum Beispiel Bluetooth oder ZigBee, und flächendeckenden Lösungen, wie zum Beispiel 5G und WLAN. Der Vorteil ist jeweils zugleich auch Nachteil – lokale Ansätze brauchen keine aufwändige Infrastruktur und lassen sich unabhängig temporär oder lokal einsetzen, flächendeckende Lösungen lassen dafür einheitlich und zentral verwalten, wodurch eine Fehleranfälligkeit und gegenseitige Störungen vermieden werden. Auch zwischen den Technologien gibt es deutliche Leistungsunterschiede, sodass pro Anwendungsfall individuell zu untersuchen ist, welche Lösung in dem Fall technisch als auch wirtschaftlich am besten geeignet ist. Insbesondere 5G hat sich dabei, wie bereits in Kap. 2.1 beschrieben, als Allround-Lösung herauskristallisiert, da es mit den geringen Latenzen und hohen Datenraten allen industriellen Anwendungen gerecht wird und die einzige Technologie ist, bei der das

Frequenzspektrum reguliert und damit kontrollierbar ist. Somit ist es gerade für die Summe an verschiedensten Anwendungsfälle geeignet und lohnenswert. Im Zusammenspiel mit verschiedenen Netzwerken und verteilten Datenquellen sorgen dann Ansätze wie Time Sensitive Networking (TSN) für die Einhaltung von harten Anforderungen an eine Maschinenkommunikation wie Echtzeitfähigkeit und erlauben das weitere Aufbrechen von lokalen Anwendungen hin zu globalen und verteilten Netzwerken. Aufbauend auf der reinen Konnektivität gibt es eine Reihe verschiedener *Schnittstellen und Kommunikationsprotokolle*, wie zum Beispiel Modbus, MQTT, MT-Connect, Umati oder OPC-UA. Entwickelt für verschiedene Einsatzzwecke ist stets die Intention, Daten möglichst einheitlich zu verpacken und zu versenden. Für eine gegenseitige Kommunikation müssen dafür beide Seiten das selbe Protokoll sprechen. Ähnlich wie die verschiedenen Konnektivitätstechnologien haben auch die Kommunikationsprotokolle individuelle Leistungseigenschaften und müssen für jeden Anwendungsfall untersucht werden.

Generell zeichnet sich jedoch der Trend ab, für eine standardisierte und autonome Kommunikation zwischen Maschinen und Software Protokolle einzusetzen, die neben den reinen Daten ebenfalls die semantische Struktur übertragen, um die Daten global und maschinenlesbar verständlich zu machen. Auch hier basiert dies jedoch darauf, dass alle Teilnehmer sich über die verwendete Semantik einig sind, wie z.B. bei der Sensor Markup Language (SenML) [10]. Gerade im Hinblick auf branchenübergreifende Prozessketten ist diesbezüglich noch akuter Entwicklungsbedarf. Dazu kommt, dass im Zweifel solche Protokolle den Nachteil haben, auf Grund des übertragenen Overheads deutliche Performanceeinbußen vorzuweisen, weswegen häufig für Anwendungen mit hohen Leistungsanforderungen, wie zum Beispiel bei der Prozessüberwachung oder der Maschinenregelung, noch deutlich primitivere Protokolle zur Anwendung kommen, was eine Plug & Play Fähigkeit verhindert oder erschwert. Auch hier ist noch Nachholbedarf für echtzeitfähige und leistungsstarke Kommunikationsprotokolle oder Implementierungen.

3.2 Dynamische Vernetzung

Dynamische Prozesse und eine schwankende Nachfrage verlangen heutzutage sich schnell ändernde und erweiterbare Produktionssysteme. Gerade für die IT-Infrastruktur bedeutet dies ein Höchstmaß an *Flexibilität und Skalierbarkeit* – Software, Hardware oder ganz neue Technologien müssen in immer häufigeren Abständen eingebunden oder ausgetauscht werden und Anwendungen müssen heutzutage nach Bedarf gestartet oder erweitert werden. Cloudsysteme boten hier schon frühzeitig einen Ansatz, um nicht nur schnell und *dynamisch Speicher- und Rechenkapazität* auszulagern, sondern ebenfalls um besonders kleinen und mittelständischen Unternehmen eine wirtschaftliche Lösung zu bieten. Ermöglicht wurde dies vor allem durch den enormen Ausbau der Netzwerkbandbreite in den 90er Jahren. Eine Cloud ist in der Regel ein zentral verwaltetes Rechenzentrum, bei dem virtuelle Ressourcen an verschiedene Kunden vermietet werden und von diesen in die lokale IT-Infrastruktur eingebunden werden können. Somit wird die reine Verwaltung der Hardware ausgelagert und es müssen lokal keine großen Kapazitäten für Spannungsspitzen vorgehalten werden. Bei Bedarf lassen sich einfach weitere Ressourcen hinzubuchen oder pausieren. Hier lassen sich zwei grundlegende Ansätze unterscheiden: beim Scale-Up wird eine Skalierbarkeit über eine Vergrößerung der genutzten Ressourcen erreicht, beispielweise über die Verwendung einer größeren virtuellen Maschine, beim Scale-Out werden weitere, gleiche Instanzen der Anwendung auf zusätzliche Ressourcen verteilt, um die Last zu verteilen. In diesem Zusammenhang haben sich verschiedene Dienstleistungskonzepte etabliert: stellt eine

Cloud lediglich Hardwareinfrastruktur für den Betrieb eigener Softwaresysteme bereit, so spricht man von IaaS (Infrastructure as a Service), umfasst die Dienstleistung zusätzlich Betriebssysteme und Laufzeitumgebungen, so spricht man von PaaS (Platform as a Service) und werden darüber hinaus ganze Softwareumgebungen bereitgestellt, so spricht man von SaaS (Software as a Service). Bei allen drei Konzepten wird der Verbrauch nutzungsbezogen berechnet und ermöglicht so die hohe Flexibilität.

Auf Grund von Latenzzeiten und besondere Anforderungen an die Datenhoheit kann es für ein Unternehmen sinnvoll sein, die Rechenzentren lokal zu betreiben – dann spricht man von einer sogenannten Private Cloud. Eine solche Lösung bietet alle Vorteile einer dynamischen Allokation von Rechen- und Speicherressourcen, liegt jedoch in der vollen Kontrolle der unternehmenseigenen IT. Mischt ein Unternehmen dann Elemente einer Private Cloud und einer Public Cloud, so ergibt sich eine Hybrid Cloud. Hybride Cloud-Architekturen vereinen hier die Vorteile beider Ansätze und ermöglichen einen flexiblen Ansatz für verteilte Systeme. Daher wird es für die nächsten Jahre als dominierendes Betriebsmodell gehandelt [11].

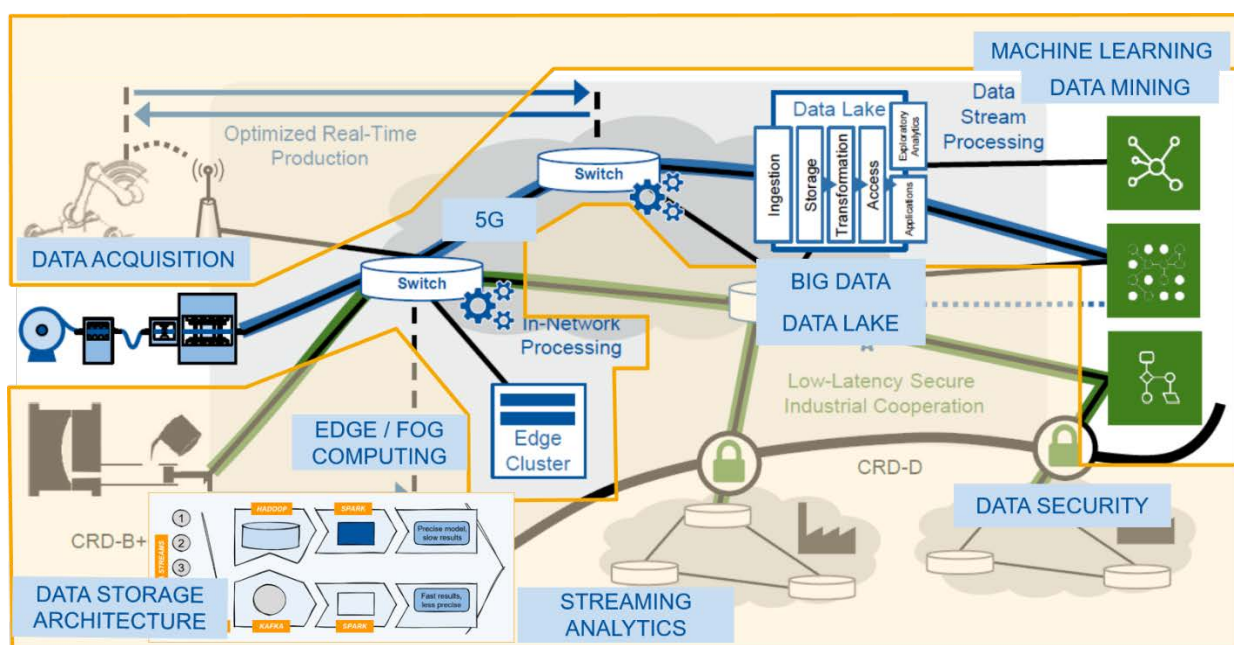


Bild 5: Referenzarchitektur des Internet of Production

In diesem Rahmen haben sich sogenannte Microservice-Architekturen etabliert, bei denen komplexe Softwaresysteme durch das Zusammenspiel von einzelnen, unabhängigen Anwendungen entstehen, die untereinander kommunizieren (siehe Bild 5). Dabei übernimmt jede Komponente eine spezifische kleine Aufgabe und ermöglicht auf diese Weise einen beliebigen modularen Aufbau, der leicht ergänzt oder erweitert werden kann. So werden beispielsweise keine komplexen, ganzheitlichen Softwaresysteme für Datenspeicherung, -aufbereitung, und -auswertung geschaffen, sondern einzelne, spezialisierte Softwaremodule, die jeweils eine dieser Aufgaben übernehmen und miteinander zum Wohle des gemeinsamen Ziels zusammenarbeiten. Ermöglicht wird dies durch immer neue technologische Ansätze der Virtualisierung, bei der Ressourcen, wie zum Beispiel ein Server, über eine Abstraktionsschicht logisch und unabhängig von der darunterliegenden Hardware in verschiedene Bereiche aufgeteilt werden kann. Softwaresysteme werden dann nicht mehr manuell auf verschiedenen Systemen

installiert, sondern werden in sogenannte virtuelle Maschinen (VMs) oder seit neuestem auch Containern betrieben. Diese lassen sich dann nicht nur standardmäßig von verschiedenen Anwendern nutzen, sondern auch per Software automatisiert verlagern und verwalten. Hauptunterschied zwischen den beiden genannten Lösungen ist, dass Container im Gegensatz zu VMs ebenfalls das Betriebssystem virtualisieren, wodurch mehrere Instanzen von Containern parallel auf dem selben Betriebssystem laufen können. Bei VMs ist lediglich die Hardware virtualisiert, wodurch mehrere VM Instanzen parallel auf der selben Hardware laufen können. Man könnte also sagen, dass Container leichtgewichtiger sind, je nach Anwendung haben beide Ansätze jedoch Vor- und Nachteile, was die Leistungsfähigkeit und Kompatibilität zu Softwarebibliotheken angeht.

Um diese modularen Microservice-Systeme effizient verwalten zu können, ergab sich schnell der Bedarf nach IT-Infrastrukturen, dessen Abläufe vollständig durch Software definiert und automatisiert sind, sogenannte SDDC (Software Defined Data Center). In Rechenzentren werden daher neben den reinen Virtualisierungs- und Containerlösungen zur parallelen Nutzung der Serverhardware auch sogenannte Cloud-Integrations-Stacks verwendet, wie zum Beispiel OpenStack oder Kubernetes. Ihre Aufgabe ist es, große Cluster an Ressourcen und Applikationen zu orchestrieren und vor allem zu automatisieren. Mit Ihrer Hilfe ist es möglich, ganze Netzwerklandschaften und verteilte virtuelle Rechencluster per Software zu definieren und automatisiert zu verwalten. Insgesamt entsteht so ein sehr flexibles System, das je nach Bedarf erweitert oder angepasst werden kann oder sich sogar selbständig anpasst. Schon jetzt ist dies kein lokales Phänomen mehr – betrachtet man heutige Anwendungen in der Produktion, so beziehen sich viele Dienste auf standort- oder sogar unternehmensübergreifende IT-Ressourcen, oft sogar dynamisch zwischen diesen wechselnd. So werden zum Beispiel Algorithmen zur adaptiven Prozessüberwachung und -steuerung heutzutage als Dienstleistung von Maschinenherstellern angeboten, müssen jedoch möglichst nah am Rande des Netzwerks beim Kunden vor Ort bereitgestellt werden. Andere Anwendungen erwarten sogar, dass digitale Dienste dem realen Produkt bei seinem Weg durch die einzelnen Netzwerkknoten einer komplexen IT-Infrastruktur folgen, um zum Beispiel Latenzanforderungen bei Lokalisierungsanwendungen einzuhalten. Bereits jetzt zeichnen sich erste Lösungen ab, um Software dynamisch und unabhängig vom Standort und Betreiber zu verwalten

Durch das Aufbrechen der standortbezogenen IT-Infrastruktur ergeben sich ganz neue Möglichkeiten für eine vernetzte, adaptive Produktion. Eines ist jedoch sicher: in Zukunft werden nahtlose Ressourcen- und Anwendungsverwaltungen über Unternehmens- und sogar Betreiber Grenzen hinweg die Industrie beschäftigen und dominieren.

3.3 Plattformen für die unternehmensübergreifende Vernetzung

Über die reine Virtualisierung und Flexibilisierung von IT-Infrastrukturen hinaus resultiert auch immer mehr der Bedarf, Daten aber auch Anwendungen standardisiert unternehmensübergreifend zur Verfügung zu stellen. Hierfür bieten die in Kap 3.2 beschriebenen XaaS (Anything as a Service) Ansätze eine Möglichkeit, in dem die Infrastrukturen unterschiedlicher Unternehmen über Marketplace-Applikationen miteinander verbunden werden. Neben der Datenmonetarisierung (siehe Kap. 2.3) ergeben sich durch den Vertrieb von Applikationen beziehungsweise Microservices neue Geschäftsmodelle. Ein Prototyp eines solchen Marketplace ist Teil des Virtual Fort Knox (VFK), einer Cloud-Lösung der Fraunhofer-Gesellschaft. Einzelne Rechenknoten werden

lokal betrieben, sind aber gleichzeitig untereinander vernetzt. Über ein Software Development Kit (SKD) können produzierende Unternehmen, aber auch Drittanbieter, ihre Softwareanwendungen für den Marketplace vorbereiten. Das VFK verfügt über spezielle Automatisierungslösungen, mit dem diese Anwendungen ähnlich wie in einem App-Store vertrieben beziehungsweise verteilt werden können. Applikationen, die auf diesem Wege ausgetauscht werden, können dem Anwender sogar als virtuelle Maschine in der lokalen Instanz zur Verfügung gestellt werden (vgl. SaaS). Neben einfachen Softwareprogrammen sind aufwändigere Simulations- und Berechnungstools, beispielsweise spezielle CAM-Programme, denkbar und – eine echtzeitfähige Kommunikation zwischen den lokalen Knoten und der Feldebene vorausgesetzt – sogar das Zuweisen von Steuerungen beziehungsweise Steuerparameter für Roboter und Maschinen gelangt in Reichweite. Forscher der Fraunhofer-Gesellschaft arbeiten an einem Transfer dieser Funktionalität in eine OpenStack-Plattform, einer OpenSource Virtualisierungsumgebung, welche aktuell einen erhöhten Verbreitungsgrad erfährt und durch die Nutzung der TSN-fähigen Version StarlingX die erwähnte Echtzeitfähigkeit ermöglichen soll.

Entscheidend für den Erfolg unternehmensübergreifender XaaS-Anwendungen und damit die Erschließung neuer Geschäftsmodelle wird es sein, einheitliche Schnittstellen für die technische Integration zu schaffen. Für den Austausch von Daten bietet die International Data Spaces Association [9] eine sehr gute Grundlage. Um dabei innerhalb des Teilnehmernetzwerkes die Authentizität zu gewährleisten, bieten sich zum Beispiel Blockchain-Mechanismen an. Daten und Dienste sollen demnach in einer sogenannten Blockchain-basierten Datenökonomie zum wichtigsten Treiber moderner Geschäftsmodelle werden. Dezentrale, standardisierte Buchführungsmechanismen gewährleisten dabei eine lückenlose Dokumentation von Transaktionen durch kryptografische Verkettungen. Damit wird es unmöglich gemacht, frühere Transaktionen zu manipulieren und garantiert eine Rückverfolgbarkeit innerhalb des Netzwerks.

Die Verteilung von Applikationen ist schwieriger, weil hier die Fragen der Funktion und Haftung hinzukommen. Zu lösen ist in jedem Fall die Aufgabe der Softwareprüfung, die im Bereich von Smart Device von den Betreibern der jeweiligen App-Store Google und Apple übernommen werden. Sofern diese Hürden überwunden werden können, bieten sich neue Geschäftsmodelle für produzierende Unternehmen, Softwareanbieter sowie für Anbieter und Betreiber von Cloud-Lösungen. Für Nutzer aus der produzierenden Industrie kann es die Aufwände für eigene Entwicklungen drastisch verkürzen.

4 Ausblick

Die Vision einer vernetzten, adaptiven Produktion gelingt nur über eine geeignete und maßgeschneiderte Infrastruktur. Dabei sind viele Bausteine bereits aktuell verfügbar und können an die Bedürfnisse des Anwenders angepasst werden.

Das Internet of Production bildet den Rahmen für eine solche durchgängige, sichere und leistungsfähige Architektur. Die Integrität, Souveränität und Echtzeitfähigkeit in der Produktion erhobener Daten sind dabei notwendige Bedingung für eine leistungsfähige Infrastruktur zur verteilten Kommunikation. Insbesondere die standortübergreifende Vernetzung wird zum entscheidenden Faktor einer erfolgreichen Nutzbarmachung von Daten. Gelingt der Aufbau einer maßgeschneiderten Infrastruktur, kann zum Beispiel Ressourceneffizienz durch datengetriebene Unterstützungssysteme die Produktion nachhaltiger gestaltet werden.

Reallabore ermöglichen die konzentrierte Entwicklung leistungsfähiger Architekturen. Dabei wird das Zusammenspiel der einzelnen Komponenten unter realen Bedingungen erprobt und weiterentwickelt. Ein solches Beispiel ist das Blockchain Reallabor Rheinisches Revier. Solche Labore erleichtern durch die Kooperation der Wissenschaft und des praktischen Einsatzes die Standardisierung besonders leistungsfähiger Komponenten. Die Standardisierung ist wie in diesem Beitrag ausführlich beschrieben insbesondere in Hinblick auf die Kommunikation ein kritischer Baustein für eine belastbare Kommunikations-Infrastruktur. Im Bereich 5G beispielsweise erarbeitet die 5G Alliance for Connected Industries and Automation (5G-ACIA), die ein Zusammenschluss aus IT-Unternehmen, Produktionsausrüstern sowie akademischen Partnern ist, Handlungsanweisungen und Vorgaben für Standards für das 5G-Ökosystem.

Viele der hier beschriebenen Elemente der vernetzten, adaptiven Produktion basieren auf einer leistungsfähigen Infrastruktur. Ein weiteres Reallabor, welches eine solche Infrastruktur schafft, ist der 5G-Industry Campus Europe [12], ein Zusammenschluss des Fraunhofer-Instituts für Produktionstechnologie IPT, des Werkzeugmaschinenlabors WZL der RWTH Aachen sowie des FIR e.V. an der RWTH Aachen. Im 5G-Industry Campus Europe werden zahlreiche Anwendungen aus dem gesamten Spektrum der Produktion mit 5G umgesetzt, von drahtloser Sensorik über mobile Robotik und Logistik bis hin zu standortübergreifenden Ende-zu-Ende Vernetzungslösungen für die Fertigungssteuerung und -diagnostik. Hierfür wird das größte private 5G-Netz für die Produktion in Europa geschaffen, welches unter anderem die Abdeckung von vier Maschinenhallen sowie des Campus Melaten der RWTH Aachen beinhaltet. Alle Teilnetze in den einzelnen Hallen sind so konfiguriert, dass die einzelnen Institute die Souveränität über ihre eigenen Daten behalten. Das zentrale Core-Netzwerk am Fraunhofer IPT regelt die Zugriffsrechte sowie Roaming-Agreements für jeden einzelnen Netzwerkteilnehmer. Als Teil des Ökosystems verfügt der 5G-Industry Campus Europe über ein Edge-Cloud System der Firma German Edge Cloud, welches für die beteiligten Institute als XaaS-Plattform für latenzkritische Anwendungen genutzt werden kann. Die so geschaffene Infrastruktur ist damit optimal für konkrete Umsetzungen im Sinne der vernetzten, adaptiven Produktion ausgestattet.

Literatur

- [1] Dirks, T.: Digitalisierung der Wirtschaft. URL: <https://www.bitkom.org/sites/default/files/file/import/Bitkom-Charts-PK-Digitalisierung-der-Wirtschaft-20-03-2017-final.pdf> [Stand: 25.06.2020].
- [2] MacGillivray, C.; Reinsel, D.: Worldwide Global DataSphere IoT Device and Data Forecast, 2019–2023. Framingham: IDC Corporate USA, 2019.
- [3] Bauernhansl, T.; Krüger, J.; Reinhart, G.; Schuh, G.: WGP-Standpunkt Industrie 4.0. URL: https://www.ipa.fraunhofer.de/content/dam/ipa/de/documents/Presse/Presseinformationen/2016/Juni/WGP_Standpunkt_Industrie_40.pdf [Stand: 25.06.2020].
- [4] Klocke, F.; Bergs, T.; Bobek, T.; Huwer, T.; Liu, G.; Pothen, M.; Staasmeyer, J.-H.; Winands, K.: Vernetzte, adaptive Produktion. In: Brecher, C.; Klocke, F.; Schmitt, R.; Schuh, G. (Hrsg.): Internet of Production für agile Unternehmen. AWK Aachener

- Werkzeugmaschinen-Kolloquium 2017, 18. bis 19. Mai. Aachen: Apprimus, 2017, S. 263-286.
- [5] IEEE: IEEE Draft Standard for Local and Metropolitan Area Networks - Timing and Synchronization for Time-Sensitive Applications 35.110 (2019) P802.1AS. New York.
- [6] Ansari, J.; Németh, G.; König, N.; Mohanram, P.; Kehl, P.; Padovani, R.; Torreggiani, A.; Lange, D.; Overbeck, D.: D3.2. Report on System Design Options for Monitoring of Workpieces and Machines. URL: <https://5gsmart.eu/wp-content/uploads/5G-SMART-D3.2.pdf> [Stand: 25.06.2020].
- [7] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Die Lage der IT-Sicherheit in Deutschland 2019. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2019.pdf?__blob=publicationFile&v=7 [Stand: 25.06.2020].
- [8] Pauer, A.; Nagel, L.; Fedkenhauser, T.; Fritzsche-Sterr, Y.; Resetko, A.: Data exchange as a first step towards data economy. URL: <https://www.pwc.de/en/digitale-transformation/data-exchange-as-a-first-step-towards-data-economy.pdf> [Stand: 25.06.2020].
- [9] Otto, B.; Steinbuß, S.; Teuscher, A.; Lohmann, S.: Reference Architecture Model. Version 3.0 | April 2019. URL: <https://www.internationaldataspaces.org/wp-content/uploads/2019/03/IDS-Reference-Architecture-Model-3.0.pdf> [Stand: 25.06.2020].
- [10] Jennings, C.; Shelby, Z.; Arkko, J.; Keranen, A.; Bormann, C.: Sensor Measurement Lists (SenML). URL: <https://tools.ietf.org/html/rfc8428> [Stand: 25.06.2020].
- [11] IDC: Mit Consumption-based Services die Hybrid Cloud optimal nutzen. URL: <https://whitepaper.silicon.de/resource/idc-studie-mit-consumption-based-services-die-hybrid-cloud-optimal-nutzen/> [Stand: 25.06.2020].
- [12] Willrett, M.: In Echtzeit auf eine neue Stufe. Forschungs-Campus zeigt den Nutzen von 5G für die vernetzte Produktion. In: *Industrieanzeiger*. 142. Jg., 2020, Nr. 14, S. 38–41.

Mitarbeiter der Arbeitsgruppe für den Beitrag 1:

Prof. Dr.-Ing. Robert H. Schmitt, WZL der RWTH Aachen

Sven Jung M.Sc., Fraunhofer IPT, Aachen

Dipl.-Phys. Niels König, Fraunhofer IPT, Aachen

Dr.-Ing. Dipl.-Wirt.-Ing. Martin Peterek, WZL der RWTH Aachen