Arno Fiedler, Christoph Thiel

Nutzenpotenziale europäischer Vertrauensdienste für verlässliche Produktionsprozesse

In dem Maße, wie eine durchgängige Digitalisierung sowohl horizontal über Zulieferer und Lieferanten bis zum Kunden als auch vertikal vom Entwickler bis zum Produkt unsere Produktionswelt und unsere Umwelt zweckbestimmend beeinflusst, ist für ihre wirtschaftliche und gesellschaftliche Akzeptanz das begründbare Vertrauen in die Beherrschung möglicher Risiken eine notwendige Voraussetzung. Eine wichtige Grundlage für dieses Vertrauen kann der Einsatz europäischer Vertrauensdienste zur Schaffung eines digitalen Vertrauensraums über alle Glieder der Wertschöpfungsketten und über alle Wertschöpfungsnetzwerke hinweg sein.

1 Einleitung

Die industrielle Produktion steht im 21. Jahrhundert vor einem tiefgreifenden Wandel, ermöglicht und zugleich getrieben durch den technischen Fortschritt. Unter dem Schlagwort „Industrie 4.0“ steht nichts weniger zur Diskussion als die Ablösung der traditionellen Produktionsstrukturen durch eine neue Stufe der Organisation und Steuerung der gesamten Wertschöpfungskette über den gesamten Lebenszyklus von Produkten. Grundlage dafür soll in Zukunft die Verfügbarkeit aller relevanten Informationen in Echtzeit durch Vernetzung aller an der Wertschöpfung beteiligten Instanzen sein sowie die Fähigkeit aus den Daten den zu jedem Zeitpunkt optimalen Wertschöpfungsfluss abzuleiten. Durch die Verbindung von Menschen, Objekten und Systemen sollen dadurch dynamische, echtzeitoptimierte und selbst organisierende, unternehmensübergreifende Wertschöpfungsnetzwerke entstehen, die sich nach unterschiedlichen Kriterien wie beispielsweise Kosten, Verfügbarkeit und Ressourcenverbrauch optimieren lassen [8].

Das steigende Interesse der Öffentlichkeit an der Gestaltung dieses Wandels führt zu einem Erwartungsdruck gegenüber der technischen Entwicklung, aber auch zur Besinnung auf mögliche Risiken. Nur wenn ein ausreichendes Vertrauen in die Beherrschung dieser Risiken gegeben ist, kann davon ausgegangen werden, dass der erwartete Wandel Realität wird (vgl. [3]).

Die vorliegende Arbeit konzentriert sich auf Risiken, die sich hinsichtlich der IT-Sicherheit bei Industrie 4.0 ergeben, und hierbei speziell aufgrund von Bedrohungen der Authentizität, Integrität und Vertraulichkeit. Ausgehend von einem Überblick über die Entwicklungsgeschichte der industriellen Produktion und die dabei wachsende Bedeutung der Digitalisierung und Informationsverarbeitung in Abschnitt 2 werden in Abschnitt 3 die Bedeutung der Aspekte Identität und Vertrauen bei Industrie 4.0 vorgestellt und zueinander in Beziehung gesetzt. In Abschnitt 4 werden erste Lösungswege für die Herstellung eines begründeten Vertrauens insbesondere auf Basis europäischer Vertrauensdienste skizziert werden. Abschnitt 5 schließt diese Arbeit mit einer kurzen Zusammenfassung.

Dipl. Wirtsch.-Ing. Arno Fiedler

Geschäftsführer Nimbus Technologieberatung GmbH

E-Mail: arno.fiedler@nimbus-berlin.com

Prof. Dr. Christoph Thiel

Professor für sichere und zuverlässige Softwaresysteme an der Fachhochschule Bielefeld, Standort Minden

E-Mail: thiel.chr@gmxpro.de

2 Entwicklungsgeschichte

Die fortlaufende Weiterentwicklung der industriellen Produktionssysteme ermöglichte in den letzten Jahrhunderten in den sich entwickelnden Industriestaaten Europas eine Wertschöp-

fung, die über alle Bevölkerungsschichten einen deutlichen Wohlstandszuwachs erbrachte. Günter Spur weist 1997 darauf hin, dass dieser „komplexe wirtschaftliche und technologische Wandlungsprozess unter dem zeitlichen Aspekt einer über mehrere Generationen reichenden Ausdehnung eher als eine Evolution bewertet werden muss" [2]. Andererseits hat der technische Fortschritt Phasensprünge in der Entwicklungsgeschichte der Industrialisierung ausgelöst, die dem heutigen Zeitgeist folgend retrospektiv gerne als Industrielle Revolutionen beschrieben werden.

Technologisch begann die Industrialisierung oder erste Industrielle Revolution in der zweiten Hälfte des 18. Jahrhunderts mit der Verbesserung von Kraftmaschinen zum Antrieb von Arbeitsmaschinen, wie z.B. der Verbesserung der Newcomenschen Dampfmaschine durch James Watt. Handarbeit wurde durch Maschinenarbeit ergänzt. Aus der Handwerkstechnik entstand die Fabriktechnik [7]. Maschinenarbeitsplätze bestimmten die Gestaltung der Werkstätten, wobei Energiefluss und Arbeitsfluss die Struktur der Produktionswelt prägten. Energie, Material, Wissen und Information waren lokal gebunden.

Der Begriff der zweiten Industriellen Revolution ist bereits nicht mehr klar umrissen. Einerseits kann von einer organisationsgetriebenen Revolution gesprochen werden, die durch den Durchbruch zur Massenproduktion mit Hilfe der Fließfertigung und die wissenschaftliche Betriebsführung des Taylorismus/Fordismus charakterisiert wird. Andererseits kann aus technologischer Sicht die zweite Industrielle Revolution mit der Nutzung der Elektrizität, der Entwicklung elektrischer Antriebe und von Verbrennungsmotoren begründet werden. Der dezentrale Antrieb von Arbeitsmaschinen (elektrischer Antrieb und der Antrieb auf Basis von Verbrennungsmotoren), die Flexibilisierung und Optimierung des Energie-, Material- und Personentransports (Eisenbahn und Automobil) und die Entwicklung von einfachen Sprachübertragungssystemen (Telegraf, Telefon) führten zur schärferen Trennung des Produktionsbetriebes von der Produktionsvorbereitung und zur steigenden Unabhängigkeit von lokalen Material- und Energiequellen.

In industriellen Produktionssystemen findet neben der Energie- und Materialumsetzung permanent die Umsetzung von Wissen und Information statt. Es ist nur folgerichtig, dass die Entwicklung der Elektronik und später der Informations- und Kommunikationstechnologie eine dritte Industrielle Revolution auslöste, in der eine weitergehende Automatisierung der Produktionsprozesse und die Übernahme von administrativen und technologischen Informationsflüssen durch miteinander vernetzte Informations- und Kommunikationssysteme stattfand. Damit wurde einerseits eine fortschreitende Rationalisierung und Optimierung auf Basis von Wissen und Informationen, anderseits in der Folge auch die variantenreiche Serienproduktion ermöglicht. Durch den Einsatz moderner Informations- und Kommunikationstechnologien wurden Möglichkeiten für einen umfassenden Austausch von Wissen und Information geschaffen, wodurch diese beiden zentralen Produktionsfaktoren im Grundsatz nun ebenfalls nicht mehr lokal gebunden sind.

Günter Spur hebt 1997 in dem Forschungsbericht „Optionen zukünftiger industrieller Produktionssysteme" die Bedeutung eines durchgängigen Informationsflusses hervor, bei dem die Informations- und Kommunikationstechnik alle Bereiche des industriellen Produktionssystems miteinander verbindet. Ferner beschreibt er das vernetzte Virtuelle Unternehmen, das er als ein zeitlich befristetes Netzwerk unabhängiger Regionen versteht, die durch eine leistungsfähige Informations- und Kommunikationsstruktur miteinander verknüpft sind. Ein solches Virtuelles Unternehmen kann innerbetrieblich zur Lösung einer Projektaufgabe, andererseits aber auch auf der zwischenbetrieblichen Ebene durch die Einbeziehung von Kunden, Lieferanten und Geschäftspartnern in den Wertschöpfungsprozess als ein Netzwerk miteinander kooperierender Unternehmen entstehen. Die letztgenannte Form Virtueller Unternehmen zeichnet sich durch die unternehmensübergreifende Verknüpfung von Kernkompetenzen entlang der gesamten Wertschöpfungskette aus. Mit seiner Arbeit beschreibt Günter Spur wesentliche Teile der voraussichtlichen evolutionären technischen Weiterentwicklung der industriellen Produktion: Der Grad der Vernetzung und Informationsverarbeitung mit dem Ziel eines durchgängigen horizontalen und vertikalen Informationsflusses innerhalb von Produktionssystemen wird weiter zunehmen. Die industrielle Produktion wird sich aus den engen Strukturen einzelner Produktionssysteme lösen, und eine unternehmensübergreifende Wertschöpfung wird entstehen, welche nicht durch einzelne zentrale Akteure geführt wird, die auf Basis eines Informations- und Wissensdefizits Entscheidungen in einer komplexen Umwelt treffen [2].

Das perspektivische Weiterverfolgen von Günter Spurs Ideen und ihre Verknüpfung mit der Beobachtung einer evolutionären Weiterentwicklung intelligenter Sensor- und Aktor-Technologie führen direkt zur Vision Industrie 4.0. Diese zeichnet sich insbesondere durch

- den Aufbau von Wertschöpfungsketten und -netzwerken über Firmengrenzen hinweg auf Basis einer horizontalen Integration,
- ein digital durchgängiges Engineering über die gesamte Wertschöpfungskette des Produkts und des zugehörigen Produktionssystems und
- den Aufbau und die Realisierung flexibler und re-konfigurierbarer Produktionssysteme innerhalb eines Unternehmens und deren vertikale Integration

aus. Entscheidend ist dabei aus technischer Sicht, dass einerseits IT-Systeme, die für unterschiedliche Prozessschritte der Unternehmenssteuerung (Material-, Energie- und Informationsfluss) zuständig sind, sowohl innerhalb eines Unternehmens als auch unternehmensübergreifend miteinander verbunden sind und gleichzeitig auf unterschiedlichen Hierarchieebenen (ERP, MES, Automatisierungstechnik (SPS, Sensoren, Aktoren)) lösungsorientiert miteinander kommunizieren. Andererseits kommt der Vernetzung aller physischen und logischen Objekte durch das Internet der Dienste und das Internet der Dinge und auf Basis von Cloud Computing eine wesentliche Rolle zu. Die Verbindung zwischen physischer und virtueller Welt gelingt mittels cyber-physischer Systeme (CPS), d.h. Objekte, Geräte, Gebäude, Verkehrsmittel, aber auch Produktionsanlagen, Logistikkomponenten etc., die eingebettete, kommunikationsfähige Systeme enthalten. Diese Systeme können über das Internet kommunizieren und Internetdienste nutzen. Cyber-physische Systeme können ihre Umwelt unmittelbar mit ihrer entsprechenden Sensorik erfassen, sie mit Hilfe weltweit verfügbarer Daten und Dienste auswerten, Daten speichern und mit Hilfe von Aktoren auf die physikalische Welt einwirken. Der Mensch ist über multimodale Mensch-Maschine-Schnittstellen mit diesen CPS verbunden und kann sie zum Beispiel über Sprache, Touch Displays oder Gesten steuern. CPS können autonom und dezentral Netz-

werke aufbauen und sich eigenständig optimieren. Es ist ein zentrales Merkmal der CPS, Daten in Echtzeit zu verarbeiten und zur Verfügung zu stellen. Und über diese echtzeitfähigen Daten ist es möglich, die reale Welt mit der virtuellen Welt zu verschmelzen; ein virtuelles Abbild der Realität permanent mit Hilfe der Echtzeitdaten zu aktualisieren. CPS bilden somit die Basis, um die verschiedenen „Internets" miteinander zu verbinden: das Internet der Menschen mit dem Internet der Dinge und dem Internet der Dienste. Sie ermöglichen einerseits die Realisierung intelligenter Produkte, die Informationen über ihren kompletten Herstellungsprozess sowie ihren künftigen Einsatz enthalten, und andererseits die Realisierung intelligenter Fabriken, die als intelligente, hochvernetzte Produktionssysteme die Produktion dynamisch und standortübergreifend steuern und den unterschiedlichen Anforderungen der intelligenten Produkte entsprechend ihre Produktionsprozesse flexibel anpassen, um maximal effizient zu arbeiten.

3 Identität und Vertrauen in Industrie 4.0

Die industrielle Produktion ist (seit Beginn der ersten Industriellen Revolution) ständigen Bedrohungen ausgesetzt, aus denen sich Risiken für den einzelnen Menschen, die Umwelt, die Produktionssysteme selbst und schließlich für den wirtschaftlichen Erfolg des einzelnen Unternehmens oder gar ganzer Wirtschaftsstandorte ergeben können. Mit Einsetzen der dritten Industriellen Revolution und dem damit verbundenen zunehmenden IT-Einsatz müssen Bedrohungen für die Informationstechnik und Informationsverarbeitung betrachtet werden. Nun treibt die Vision Industrie 4.0 mit horizontalen und vertikalen Wertschöpfungsketten die Vernetzung von Maschinen und Anlagen, die engere Verknüpfung mit der Unternehmens-IT und der Anbindung an das Internet massiv voran und führt damit zu weiteren, neuen Angriffsmöglichkeiten und entsprechend neuen Bedrohungen. Die Wandlung linearer Wertschöpfungsketten zu Wertschöpfungsnetzwerken und die vollständige Vernetzung und IT-Durchdringung aller Wertschöpfungspartner erfordern, dass unterschiedliche Objekte und Akteure ad hoc und tief in Produktionsprozesse integriert werden und z.T. sensible Produktions- sowie Prozessdaten miteinander austauschen müssen. Dabei werden klare Abgrenzungen zwischen Einflusssphären und Verantwortungsbereichen sowohl im physischen als auch im informationstechnischen Sinne zunehmend schwieriger werden. Die daraus resultierenden Bedrohungen werden beispielsweise im Ergebnisbericht „Umsetzungsstrategie Industrie 4.0" der Plattform Industrie 4.0 ausgeführt [8].

Die in der Vision Industrie 4.0 angestrebte Kooperation und Kommunikation zur Steigerung der Effizienz und Produktivität führt zwangsläufig zur verteilten Speicherung und einem Austausch produktions- oder produktspezifischen Wissen. Die im Umfeld der Office-IT bekannten Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit erfahren daher naturgemäß den gleichen hohen Stellenwert bei Industrie 4.0. Zusätzliche Bedeutung kommt den Schutzzielen Authentizität, Integrität der Zeit (vor allem bei Wertschöpfungsnetzwerken über Firmengrenzen), Nachvollziehbarkeit und Rechtssicherheit zu. Speziell die Authentizität ist essentielles Merkmal in einem Wertschöpfungsnetzwerk, in dem die Komponenten und Partner dynamisch wechseln können und Kommunikation auch über Firmengrenzen hinweg erfolgt. Die Forderung nach Nachvollziehbarkeit ergibt sich auch aus Datenschutzanforderungen.

Alle genannten Schutzziele gelten in gleicher Weise für die Betriebsfunktionen, Überwachungsfunktionen und Schutzfunktionen (z. B. Funktionaler Sicherheit). In der Regel werden funktionale Sicherheit (Safety) und IT-Sicherheit in getrennten Fachwelten betrachtet. In den einschlägigen Standards und Normen (z.B. [9], [10]) wird zwar darauf hingewiesen, dass der jeweils andere Sicherheitsaspekt zu beachten ist. Es fehlt allerdings eine ganzheitliche oder auch integrierte Betrachtung. Dabei haben funktionale Sicherheit und IT-Sicherheit ein gemeinsames Ziel: den sicheren und zuverlässigen Betrieb von Anlagen, Maschinen, Prozessen und technischen Infrastrukturen. Während man darunter aus dem Blickwinkel der funktionalen Sicherheit die Aufgabe versteht, (insbesondere auch) durch Automatisierungstechnik sicherzustellen, dass von einem System (z.B. Anlage, Maschine) keine Gefahr für seine Umgebung (Menschen, andere Anlagen und Geräte, die Umwelt) ausgeht, steht bei der IT-Sicherheit die Abwehr von Bedrohungen (z.B. unautorisierte Zugriffe, Ausspähen oder Manipulationen von Konfigurationsdaten, Verlust von Knowhow), die von der Umgebung auf ein System einwirken, im Vordergrund (s.a. [11], [12]).

Bisher werden Safety Systeme (SIS)[1] in Produktionssystemen getrennt und zum Teil redundant eingerichtet, um höchste Verfügbarkeit und Verlässlichkeit zu gewährleisten Durch den steigenden Vernetzungsgrad im Industrie 4.0-Umfeld ist es zunehmend denkbar, dass durch technische Schnittstellen und Anknüpfungspunkte unberechtigte Eingriffe bis hinein in die eigentliche Funktionssteuerung der Maschinen und Anlagen erfolgen können. Safety-Systeme können daher den gleichen Angriffen über das Netzwerk ausgesetzt sein wie andere Komponenten auch. Dabei sind Angriffe auf die sicherheitsgerichtete Funktion wie auch indirekte Angriffe auf die Verfügbarkeit denkbar. Die Folge ist, dass die funktionale Sicherheit nicht mehr gewährleistet ist. Schäden an Mensch und Umwelt können in diesem Fällen nicht ausgeschlossen werden.

Nur die durchgängige Umsetzung aller genannten Schutzziele für die alle Betriebsfunktionen, Überwachungsfunktionen und Schutzfunktionen ermöglicht letztlich ein begründetes Vertrauen in die Sicherheit der Produktionssysteme und Wertschöpfungsketten. Dabei spielen umgekehrt für viele Sicherheitsmaßnahmen zur Gewährleistung dieser Schutzziele Vertrauensverhältnisse eine wesentliche Rolle. Notwendige Grundlagen für die Schaffung solcher Vertrauensverhältnisse in einem Industrie 4.0-Wertschöpfungsnetzwerk sind eindeutige, fälschungssichere Identitäten aller Teilnehmer (Maschine, Prozess, Material, Benutzer, Produkt, Software im Sinne von Code, Daten, etc.), repräsentiert durch digitale Zertifikate (im Sinne von [14]), und darauf aufbauende Authentisierungs- und Autorisierungsverfahren. Die digitalen Zertifikate enthalten neben den Schlüsseln zur Authentifikation ggf. auch die notwendigen Informationen und Schlüssel zur Ver- und Entschlüsselung. Gerade weil im Rahmen von Industrie 4.0 die Virtualisierung von Systemen und Prozessen stark an Bedeutung gewinnt, sind zur Ablage und kryptographischen Nutzung der sicherheitsrelevanten Informationen und Schlüsseldaten vertrauenswürdige, sichere Hardwarekomponenten als Si-

1 Während SIS in IEC 61511 [13] definiert wird und IEC 61508 [9] den Begriff E/E/PE-sicherheitsbezogenes System verwendet, ist SIS der bevorzugte Ausdruck in unserem Beitrag.

cherheitsanker erforderlich. 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).

Ebenfalls erforderlich sind eine oder mehrere Identitätsinfrastrukturen, die die eindeutige und konsistente Identifizierung und Zuordnung der Identität eines Teilnehmers gewährleisten und die Authentifikation und Rechtevergabe auf der Basis der Identitäten unterstützen. Gefordert sind damit letztlich auch vertrauenswürdige Zertifizierungsstellen (Certification Authorities) als Verwaltungsinstanzen der digitalen Identitäten und 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.

Der Aufbau und die Pflege von Identitätsinfrastrukturen für sämtliche Identitäten bzw. von Zertifizierungsstellen für alle digitalen Zertifikate von Maschinen, Prozessen, Materialien, Benutzern, Produkten etc. eines Wertschöpfungsnetzwerks sowie die Modellierung von differenzierten Rollen und Rechten, die deren Aktivitäten abbilden können, stellen eine große Herausforderung dar. Dies gilt alleine schon aufgrund der erwartbar großen Anzahl an Identitäten. Neben Fragen zur Erfassung oder Festlegung dieser Identitäten müssen Fragen der Dezentralisierung und Hochverfügbarkeit geeigneter Verzeichnisse gelöst werden, damit diese jederzeit und den Anforderungen von Industrie 4.0 entsprechend überwiegend in Echtzeit (z.B. im Rahmen einer Maschine-zu-Maschine-Identifikation) verfügbar und abfragbar sind. 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 oder bei Umkonfiguration eines CPS. Zusätzlich stellen sich Fragen der Interoperabilität und Standardisierung verschiedener Identitätsinfrastrukturen bzw. Zertifizierungsstellen. Antworten auf diese Fragen sind unabdingbar, um überhaupt das Zusammenspiel aller Teilnehmer im Wertschöpfungsnetz zu ermöglichen.

Unabhängig von solchen grundsätzlichen technischen Herausforderungen stellt sich jedoch einerseits pragmatisch und andererseits wiederum aus dem Blickwinkel des notwendigen Vertrauens heraus die Frage, wer für den Aufbau und die Pflege der entsprechenden Identitätsinfrastrukturen bzw. Zertifizierungsstellen zuständig sein kann, und welchen organisatorischen, rechtlichen und sicherheitstechnischen Vorgaben und Regelungen dieser Jemand unterworfen ist. Da sich die Konstellationen beteiligter Unternehmen, Produktionssysteme, Personen, Dienste, Sensoren, etc. in den Industrie 4-0-Wertschöpfungsnetzwerken dynamisch und ad hoc ändern und über Ländergrenzen hinausreichen können, ist noch viel stärker als heute die aus Sicherheitssicht schwächste Zertifizierungsstelle für digitale Identitäten, die zu einem bestimmten Zeitpunkt von Teilnehmern der Wertschöpfungskette genutzt wird, für die Sicherheit des gesamten Wertschöpfungsnetzes entscheidend.

4 Lösungsansätze

Für alle in Frage kommenden Betreiber von Identitätsinfrastrukturen bzw. Zertifizierungsstellen ist ein verbindlicher und von allen denkbaren Teilnehmern des Wertschöpfungsnetzwerkes akzeptierter Rahmen erforderlich, der sowohl Vertrauen bzgl. rechtlicher Fragen als auch hinsichtlich des anwendungsorientierten Nutzens der technischen Vorgaben und Standards rechtfertigen kann. Dieser Rahmen muss international anerkannt und bei größtmöglicher Freiheit für die Betreiber gleichzeitig ein definiertes und akzeptiertes Sicherheitsniveau der Identifizierung und des Zertifikatsmanagements über den gesamten Lebenszyklus der digitalen Zertifikate festlegen.

Als Ausgangspunkt für einen solchen Rahmen kann die Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt der Europäischen Union (eIDAS) [14] dienen, mit deren Veröffentlichung die Basis für eine europaweite, rechtsgültige elektronische Kommunikation und sichere elektronische Identifizierung geschaffen wurde. Kernstück dieser Verordnung ist der Begriff des Vertrauensdienstes, der

- die Erstellung, Überprüfung und Validierung von elektronischen Signaturen, elektronischen Siegeln oder elektronischen Zeitstempeln, und elektronischen Einschreib-Zustelldiensten sowie von diese Dienste betreffenden Zertifikaten oder
- die Erstellung, Überprüfung und Validierung von Zertifikaten für die Website-Authentifizierung oder
- die Bewahrung von diese Dienste betreffenden elektronischen Signaturen, Siegeln oder Zertifikaten

umfasst und in der Form eines sogenannten qualifizierten Vertrauensdienstes die Basis für eine europaweite, rechtsgültige elektronische Kommunikation und sichere elektronische Identifizierung schafft. Idealerweise können europäische Vertrauensdienste den Betrieb der oben genannten Identitätsinfrastrukturen bzw. Zertifizierungsstellen leisten. Die genannte Verordnung alleine löst jedoch noch nicht das grundsätzliche Problem der Interoperabilität und der Standardisierung in den Wertschöpfungsketten. Dies könnte jedoch u.a. durch die Umsetzung derjenigen europäischen Standards geleistet werden, welche im Rahmen der Harmonisierungsbemühungen der Europäischen Kommission im Mandate 460 von CEN/CENELEC und ETSI entwickelt wurden und werden [15].

Während diese Verordnung zunächst den Europäischen Digitalen Binnenmarkt abdeckt und ebenso die erarbeiteten Standards überwiegend europäischen Charakter zeigen, kann gehofft werden, dass diese sich aufgrund ihrer Qualität, die aus einer langjährigen internationalen (wenn auch innereuropäischen) Diskussion erwachsen ist, auch über Europa hinaus zum weltweit anerkannten Rahmenwerk für sichere Kommunikation und sichere elektronische Identifizierung entwickeln, zumindest aber als Vorlage für internationale Standards dienen werden

5 Zusammenfassung

Die Fragen, ob die vierte Industrielle Revolution wie vorgedacht stattfinden wird oder ob man den aktuellen Paradigmenwechsel überhaupt als Revolution und nicht besser als evolutionäre Weiterentwicklung des im letzten Jahrhunderts begonnenen Einsatzes der Informations- und Kommunikationstechnik

begreifen sollte, wird erst rückblickend zu beantworten sein. Unstrittig ist, dass durch dynamische Wertschöpfungsnetze und eine weiter zunehmende IT-Durchdringung der Bedarf an sicheren digitalen Identitäten sowohl für Unternehmen, Personen, Anlagen, Maschinen, Prozesse, Software, Daten etc. massiv zunehmen wird. Nur durch internationale Vorgaben und Standards können Dienstleister in die Lage versetzt werden, diesen Bedarf zu decken. Qualifizierte Vertrauensdienste auf Basis europäischer Standards können dazu ein über Europa hinausreichendes Vorbild sein.

Literatur

[1] Schuh, G.: Referenzstrategien in einer vernetzten Welt. In: Milberg, J.; Schuh, G. (Hrsg.): Erfolg in Netzwerken. Springer-Verlag, Berlin, Heidelberg, New York 2002, S. 20

[2] Spur, G. (Hrsg.): Optionen zukünftiger industrieller Produktionssysteme. Forschungsberichte der interdisziplinären Arbeitsgruppen der Berlin-Brandenburgischen Akademie der Wissenschaften, Band 4, Berlin: Akademie Verlag, 1997.

[3] Akademie der Wissenschaften zu Berlin (Hrsg.): Erfolgsbedingungen technischer Innovationen in Industrieländern. Forschungsbericht der Arbeitsgruppe (Leitung: H. Albach/W. Fischer). Berlin/Heidelberg/New York: 1993

[4] Kagermann H., Wahlster W., Helbig J. (Hrsg.) (2013) Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0 : Abschlussbericht des Arbeitskreises Industrie 4.0. www.bmbf.de/pubRD/Umsetzungsempfehlungen_Industrie4_0.pdf. Zugegriffen: .24.07.2015

[5] Vogel-Heuser B., Diedrich C., Broy M. (2013) Anforderungen an CPS aus Sicht der Automatisierungstechnik, at – Automatisierungstechnik 10:669-676.

[6] Spur, G. : Vom Wandel der industriellen Welt durch Werkzeugmaschinen . München : Hanser 1 99 1

[7] Spur, G. : Produktionstechnik im Wandel. München: Hanser 1979

[8] Umsetzungsstrategie Industrie 4.0, Ergebnisbericht der Plattform Industrie 4.0, April 2015. http://www.plattform-i40.de/sites/default/files/150410_Umsetzungsstrategie.pdf. Zugegriffen: .24.07.2015

[9] IEC 61508: Functional safety of electrical/ electronic/programmable electronic safety related systems, Part 1 to 7, ed. 2.0, 2010

[10] IEC 62443: Industrial communication networks – Network and system security. Part 1-1: 2009; part 2-1: 2010; part 3-1: 2009; part 3-3: 2013

[11] Line, M.B., Nordland, O., Røstad, L., Tøndel, I.A.: Safety vs Security?. In: Proceedings of PSAM 8, New Orleans, 2006

[12] Neugebauer, R., Jarke, M., Thoma, K. Strategie- und Positionspapier: Herausforderungen für die Cyber-Sicherheit 2020. Fraunhofer-Verbund IuK-Technlogie Fraunhofer-Gesellschaft Zur Förderung der angewandten Forschung e.V, München, 2014

[13] IEC 61511: Functional safety: Safety instrumented systems for the process industry. Part 1 to 3. ed. 1.0: 2003 (ed. 2.0 voraussichtlich August 2015)

[14] REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

[15] Mandate M460: "Standardisation Mandate to the European Standardisation Organisations CEN, CENELEC and ETSI in the Field of Information and Communication Technologies Applied to Electronic Signatures".