Fraunhofer SIT

FRAUNHOFER-INSTITUT FÜR SICHERE INFORMATIONSTECHNOLOGIE

EBERBACHER GESPRÄCH ZU »SICHERHEIT IN DER INDUSTRIE 4.0«

10/2013

INHALT

1 Vorwort

2 Zusammenfassung

3 IT-Sicherheit in der Industrie

4

Herausforderungen und Lösungsansätze

4.1 Bauanleitungen

4.2 »Security by Design« für Einzel- und Gesamtsysteme

4.3 Vertrauenswürdige Infrastrukturen und sichere Identitäten

4.4 Wissensschutz, Piraterieschutz und Nachweisbarkeit

4.5 Benutzbarkeit – Faktor Mensch

4.6 Rechtssicherheit und Datenschutz

5

Schlussbetrachtung

1. VORWORT

Angewandte Forschung zur IT-Sicherheit braucht den Dialog zwischen Wissenschaft und Wirtschaft, um anwendungsrelevante Antworten auf die grundsätzlichen Fragestellungen zu erhalten: Was sind die aktuellen Herausforderungen für IT-Sicherheit und Privatsphärenschutz? Was ist für die Zukunft zu erwarten? Was kann und soll Technik leisten? Wo sind die Grenzen des Machbaren? Wo braucht es neue Ideen?
Die »Eberbacher Gespräche« des Fraunhofer SIT bieten ein Forum für diesen Dialog. Experten aus Wissenschaft, Wirtschaft und Verwaltung treffen sich für jeweils einen Tag im Kloster Eberbach im Rheingau und erarbeiten für ein Thema gemeinsam Antworten auf diese Fragen. Im Oktober 2013 ging es um »Sicherheit in der Industrie 4.0«.Teilnehmer waren:

Prof. Dr.-Ing Reiner Anderl	Technische Universität Darmstadt
Klaus Bauer	TRUMPF Werkzeugmaschinen GmbH + Co. KG
Dr. Thomas Bornkessel	Rolls Royce Aeroengines Deutschland
Dr.-Ing. Thorsten Henkel	Fraunhofer SIT
Stefan Hoppe	OPC Europe
Holger Junker	Bundesamt für Sicherheit in der Informationstechnik (BSI)
Michael Kasper	Fraunhofer SIT
Dr. Sven Kleiner	:em engineering methods AG
Dr. Ulf Lange	Bundesministerium für Bildung und Forschung (BMBF)
Dr. Thomas Rollmann	Miele & Cie. KG
Dr. Carsten Rudolph	Fraunhofer SIT
Dr. Harald Schöning	Software AG
Michael Voeth	Robert Bosch GmbH
Friedrich Vollmar	IBM Deutschland
Prof. Dr. Michael Waidner	Fraunhofer SIT / Technische Universität Darmstadt

Die in diesem Papier dargestellten Ergebnisse werden von den Teilnehmern unterstützt, stellen aber nicht notwendigerweise die Sichtweise des jeweiligen Arbeitgebers dar.

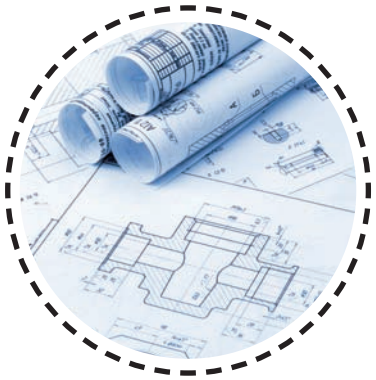
2. ZUSAMMENFASSUNG

Die Informationstechnologie (IT) ist einer der wichtigsten Innovationsmotoren für die Produktion und Automatisierung. In Deutschland werden die entsprechenden Entwicklungen unter dem Schlagwort Industrie 4.0 lebhaft diskutiert. Stets haben Politik, Industrie und IT-Wirtschaft dabei die wichtige Rolle der IT-Sicherheit herausgestellt. Sie gilt deshalb als grundlegende Voraussetzung für die neue Produktionswelt. Viele Struktur- und Detailfragen im Hinblick auf die konkreten Zielsetzungen der Anwendungsforschung sind jedoch noch unbeantwortet.

Um Leitlinien und konkrete Vorschläge für eine sichere Industrie 4.0 zu formulieren, veranstaltete das Fraunhofer-Institut für Sichere Informationstechnologie am 1. Oktober das Eberbacher Gespräch IT-Sicherheit in der Industrie 4.0.[1] Im Rahmen dieses Workshops identifizierten Teilnehmer aus Industrie, Forschung und Verwaltung die wichtigsten praktischen Herausforderungen zum Thema. Hierzu zählen insbesondere die folgenden Punkte:

- Etablierung ausreichender Sicherheit über den gesamten Lebenszyklus von Maschinen und Anlagen.
- Eindeutige Beschreibung von IT-Sicherheit im industriellen Umfeld und aussagekräftige Bewertung von industrieller IT-Sicherheit.
- Verbindung von informationstechnischer Angriffssicherheit (Security) und Gewährleistung funktionaler Betriebssicherheit (Safety).
- Schutz industrieller Infrastrukturen und Kommunikation angesichts Echtzeitanforderungen und wachsender Dynamik und Komplexität.
- Datenschutz, Datensicherheit und Rechtsicherheit für unternehmensübergreifende Dienste sowie Klärung von Haftungsfragen.

1 Der Begriff IT-Sicherheit ist hier insbesondere abzugrenzen vom Begriff der Betriebssicherheit (Safety), der vor allem den Schutz von Leib und Leben sowie vor zufälligen Ausfällen und Störungen meint. IT-Sicherheit hingegen bezeichnet im Kern »Angriffssicherheit«, den Schutz vor IT-basierten Angriffen und Manipulationen.

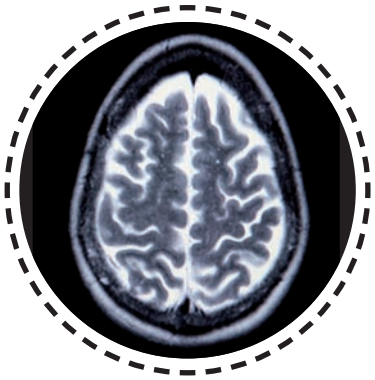


Bauanleitungen

»Security by Design« für Einzel- und Gesamtsysteme

Vertrauenswürdige Identitäten und Infrastrukturen

Wissensschutz, Piraterieschutz und Nachweisbarkeit



Benutzbarkeit – Faktor Mensch

Rechtssicherheit und Datenschutz

Aus diesen Problemlagen entwickelten die Teilnehmer anschließend konkrete Lösungsansätze in den folgenden sechs Handlungsfeldern:

1. Bauanleitungen
Anlagenplaner, Integratoren und Betreiber benötigen konkrete Handlungsempfehlungen für die Planung und den Betrieb von Systemen. Für die Modernisierung bestehender Anlagen braucht es neben Mindeststandards auch ein Reifegradmodell, mit dem sich Übergangsstrategien entwickeln und die dafür notwendigen Investitionen verlässlich planen lassen. Grundlegend für jede Definition ist eine hersteller- und betreiberübergreifende Begrifflichkeit und Systematik für industrielle IT-Sicherheit.

2. »Security by Design« für Einzel- und Gesamtsysteme
Um IT-Sicherheit bereits in Planung und Entwurf berücksichtigen zu können, gilt es Methoden und Werkzeuge zu entwickeln, die den technischen und organisatorischen Anforderungen der industriellen Welt gerecht werden. Zur Sicherheitsbewertung von Systemen und Komponenten braucht es zudem aussagekräftige Kennzahlen.

3. Vertrauenswürdige Identitäten und Infrastrukturen
Um ausreichende Verlässlichkeit in der Industrie 4.0 zu gewährleisten, braucht es eine Vertrauensinfrastruktur, die verlässliche Identitäten und Systemintegrität entlang von Wertschöpfungsketten gewährleistet. Basis hierfür ist die kryptografisch basierte Ende-zu-Ende-Sicherheit, die in Referenzarchitekturen praktisch zu erproben ist. Notwendiger Bestandteil dieser Implementierung sind Systeme, welche Identität und Integrität von Cyber-physischen Systemen (CPS) prüfen, Anomalien automatisch erkennen und Angriffe erfolgreich abwehren.

4. Wissensschutz, Pirateriesschutz und Nachweisbarkeit
Unternehmen werden nur dann neue Geschäftsmodelle entwickeln, wenn ihre wirtschaftlichen Interessen dabei gewahrt bleiben. Flexible Datenflüsse verlangen deshalb nach Möglichkeiten, Entwürfe, Fabrikations- und Produktionsdaten wirksam zu schützen. In vielen Branchen müssen Unternehmen zudem Systemzustände verlässlich dokumentieren. Dazu braucht es hersteller- und betreiberübergreifende Sicherheitslösungen zum Schutz von Wissen und von Urheberrechten sowie zur Erfüllung von Nachweispflichten.

5. Benutzbarkeit – Faktor Mensch
Auch in der Industrie 4.0 gilt der Schutz von Leib und Leben als wichtigstes Ziel. Dementsprechend muss die Funktionalität von Sicherheitsmaßnahmen und Notfallszenarien gewährleistet sein. Darüber hinaus gilt es, IT-Sicherheitsbewusstsein und Kompetenz des Personals zu erhöhen und gleichzeitig Schnittstellen möglichst benutzerfreundlich zu gestalten.

6. Rechtsicherheit und Datenschutz
Die dezentrale Organisation der Industrie 4.0 schafft neue Fragen hinsichtlich Haftungs- und Gewährleistungsfragen, die es zu beantworten gilt, um die industrielle Innovation nicht zu verzögern.

3. IT-SICHERHEIT IN DER INDUSTRIE

Seit den 1970er-Jahren können wir ein Zusammenwachsen der klassischen Produktions- und Automatisierungstechnik mit der Informationstechnologie beobachten. Maschinen, Fertigungsstraßen und Fabriken werden »digitalisiert«, also durch IT-Elemente wie Speicher, Prozessoren, Software, Kommunikationstechnik angereichert. Aus den speicherprogrammierbaren Maschinensteuerungen des 20. Jahrhunderts wurden nach dem Jahr 2000 die Cyber-physischen Systeme (CPS). Solche Systeme sind physische Dinge mit eingebetteten IT-Elementen, die frei programmierbar sind und die Fähigkeit haben, mit anderen CPS digital zu kommunizieren.

Die CPS einer Produktionsstätte kommunizieren untereinander meist über geschlossene Industrienetze. Zunehmend sind CPS aber auch über das Internet ansprechbar. Dadurch lassen sich etwa Produktions- und Geschäftsprozesse besser integrieren und gemeinsam optimieren und auch Produktionsfunktionen wie Entwurf und Qualitätskontrolle an andere Standorte, andere Firmen oder an freie Mitarbeiter auslagern.

Durch diese internetbasierte Integration von Produktions-IT und klassischer IT kann die Industrie unmittelbar teilhaben an der Weiterentwicklung der Informationstechnologie.[2] Die IT-Megatrends Mobile Computing, Cloud Computing und Big Data sind so auch zu wichtigen Innovationsmotoren in der Industrie geworden. Beispielsweise werden durch Cloud-Dienste Warenströme und komplexe Zulieferketten optimiert. Durch Big Data-Algorithmen werden Maschinenausfälle besser vorhersagbar, wodurch Ausfallzeiten und Wartungskosten gesenkt werden.

2 Der Begriff »Unternehmens-IT« bezeichnet hier alle Informations- und Kommunikationstechnologien, die man üblicherweise im geschäftlichen und privaten Bereich verwendet. Die entsprechenden Technologien im Produktionsumfeld, also in Fabriken, Produktionsstätten, Maschinen und den sie verbindenden speziellen Infrastrukturen, werden hier als »Produktions-IT« bezeichnet.

DIE BREMSKLÖTZE BEI DER REALISIERUNG VON INDUSTRIE 4.0 AUS UNTERNEHMENSSICHT

Quelle: VDE-Trendreport 2013, http://www.vde.com/de/verband/pressecenter/pressemeldungen/fach-und-wirtschaftspresse/2013/seiten/34-2013.aspx

43%

Fehlende Normen & Standards

43%

Hoher Qualifizierungsbedarf

66%

Unzureichende IT-Sicherheit

31%

Hohe Investitionen

3. IT-SICHERHEIT IN DER INDUSTRIE

Weitere Auswirkungen dieser Integration sind absehbar: Über Cloud-Dienste können Kundenwünsche enger in den Produktentwurf und die Produktionsplanung einbezogen werden, was völlig neue Maßstäbe für die Personalisierung von Produkten zur Folge haben kann – bis hin zu Losgröße 1. Ebenso lassen sich über Cloud-Dienste Arbeitsabläufe dynamisieren, was zu neuen, virtuellen Organisationsformen und neuen Formen von Arbeit führen kann. Diese IT-getriebene Entwicklung der Industrie bezeichnet man in Deutschland als die »Vierte industrielle Revolution« oder kurz als Industrie 4.0. [3]

Der industrielle Sektor, z.B. der Maschinen- und Anlagenbau und der Automobilbau, ist für die deutsche Volkswirtschaft von überragender Bedeutung. Industrie 4.0 ist in Deutschland deshalb ein industrieübergreifendes Thema, gleichberechtigt getrieben vom Verband Deutscher Maschinen und Anlagenbauer (VDMA), vom Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (BITKOM) und vom Zentralverband Elektrotechnik- und Elektronikindustrie (ZVEI).[4] Dieser industrieübergreifende Ansatz ist dem Problem angemessen und kann zu einem entscheidenden Vorteil im weltweiten Wettbewerb werden. Andernorts, insbesondere in den USA, wird das Thema vorrangig von der IT-Industrie und oftmals losgelöst vom industriellen Kontext betrachtet. Dementsprechend spricht man nicht nur vom »Industrial Internet«, sondern viel stärker auch vom »Internet of Things«.

IT-Sicherheit in der Industrie 4.0:
Alte und neue Herausforderungen

Bis heute ist in der Industrie »Sicherheit« nahezu gleichbedeutend mit »Betriebssicherheit« (Safety), also dem Schutz von Mensch, Umwelt und Anlage vor den Auswirkungen von mehr oder weniger zufälligen Fehlern. Erst durch die Vision der Industrie 4.0 und erste IT-gestützte Angriffe rückte »Angriffssicherheit«, also der Schutz vor Angriffen durch Saboteure, Spione und das organisierte Verbrechen, in den Fokus.

Die systematische Absicherung gegen Angriffe folgt meist mit einigem zeitlichen Abstand der Einführung der IT selbst – es entstehen Schutzlücken. Das Risiko, dass solche Lücken ausgenutzt werden, muss gerade in der Industrie als sehr hoch eingeschätzt werden. Industrieanlagen sind prinzipiell lohnende Ziele für wirtschaftlich und politisch motivierte Saboteure und Spione. Die mit Industrie 4.0 einhergehende Zunahme in der Vernetzung in und zwischen Unternehmen und die steigende Komplexität von Prozessen vergrößern die Angriffsfläche und sorgen so für eine weitere Erhöhung des Risikos.

Die Teilnehmer des Eberbacher Gesprächs gehen davon aus, dass die heutige Produktionslandschaft den gleichen IT-Bedrohungen ausgesetzt ist wie die klassische IT. Beispiele für die prinzipielle Angreifbarkeit jedweder IT-Systeme sind hinlänglich bekannt. Im Juni 2010 demonstrierte »Stuxnet«, dass eine Industrieanlage durch einen IT-gestützten Angriff zerstört werden kann. Bis dahin galten solche Angriffe als eine rein hypothetische Gefahr. Seit Juli 2013 enthüllte Edward Snowden, über welche nahezu unbegrenzten Möglichkeiten der US-amerikanische Geheimdienst NSA und der britische Geheimdienst GCHQ verfügen, um IT-Systeme auszuspionieren und zu manipulieren.

3 Forschungsunion und Deutsche Akademie der Technikwissenschaften (acatech): Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0; Berlin, April 2013; Online: http://www.bmbf.de/pubRD/Umsetzungsempfehlungen_Industrie4_0.pdf.

4 Webseiten der Initiative »Plattform Industrie 4.0«: http://www.plattform-i40.de

1. Infektion mit Schadsoftware über Internet und Intranet
2. Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware
3. Social Engineering
4. Menschliches Fehlverhalten und Sabotage
5. Einbruch über Fernwartungszugänge
6. Internetverbundene Steuerungskomponenten
7. Technisches Fehlverhalten und höhere Gewalt
8. Kompromittierung von Smartphones im Produktionsumfeld
9. Kompromittierung von Extranet und Cloud-Componenten
10. (D)DoS Angriffe

DIE TOP 10-BEDROHUNGEN DER INDUSTRIAL CONTROL SYSTEM SECURITY 2014

Quelle: BSI-CS 029 | Version 1.10 , 03.2014, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/techniker/hardware/BSI-CS_005.pdf?__blob=publicationFile

3. IT-SICHERHEIT IN DER INDUSTRIE

Es muss davon ausgegangen werden, dass andere Staaten über ähnliche Spionageprogramme verfügen. Auch die von Snowden beschriebenen Angriffe galten bis dahin als unrealistisch und rein hypothetische Gefahren.

Die Forschung und Entwicklung in der IT-Sicherheit hat sich bislang vorwiegend mit der Absicherung der klassischen IT und insbesondere der Unternehmens-IT beschäftigt. Die bekannten Konzepte übertragen sich prinzipiell auch auf die Produktions-IT. Im Detail zeigen sich aber deutliche Unterschiede zwischen den beiden Welten. Beispielsweise sind Integrität und Vertraulichkeit die primären Schutzziele in der Unternehmens-IT, und dementsprechend wird hier Angriffen oftmals auf Kosten der Verfügbarkeit begegnet: Unkritische Systeme schaltet man bei Angriffen etwa mitunter einfach ab. In der Produktions-IT ist ein schneller Neustart des Systems aber meist schwerer zu realisieren. Das primäre Schutzziel in der Produktion ist, materiellen Schaden von Mensch, Umwelt und Anlage abzuwenden. Dementsprechend gilt Vertraulichkeit als nachrangig, die primären Ziele sind Integrität und Verfügbarkeit.

Weitere Unterschiede ergeben sich beispielsweise durch die strengeren Echtzeitanforderungen in der Produktion, die oft geringen Speicher- und Rechenfähigkeiten von CPS und durch die aus IT-Sicht ungewöhnlich langen Lebenszeiten von Industrieanlagen. Besonderheiten bestehen auch im Bereich des Schutzes von Entwurfs- und Konfigurationsdaten (Wissensschutz) und der Erkennung von gefälschten physischen und Cyber-physischen Systemen (Pirateriesschutz). In vielen Industriesektoren gibt es zudem gesetzliche Vorgaben zur Protokollierung von Experimenten und Vorgängen (Accountability, Provenance). Hinzu kommt mit dem Übergang zur Industrie 4.0 die Verhinderung von Big Data-Analysen. Die Analyse von Protokolldaten könnte beispielsweise den Arbeitnehmerdatenschutz gefährden oder dem Maschinenhersteller geheime Produktionsdaten seiner Kunden verraten.

Um den skizzierten Anforderungen gerecht zu werden, bedarf es einer ganzheitlichen Betrachtung von IT-Sicherheit in der Industrie 4.0. Die Sicherheitsanforderungen müssen insbesondere über den kompletten Lebenszyklus von Produktionssystemen und Produkten hinweg betrachtet und garantiert werden.

4. HERAUSFORDERUNGEN UND LÖSUNGSANSÄTZE

» INDUSTRIE 4.0 BRAUCHT STANDARDISIERTE BAUANLEITUNGEN FÜR DIE IT-SICHERHEIT.«

Die Teilnehmer des Eberbacher Gesprächs identifizierten sechs Herausforderungen für die IT-Sicherheit in der Industrie 4.0 und diskutierten mögliche Herangehensweisen.

4.1 BAUANLEITUNG

Mittelständische Maschinen- und Anlagenbauer und ihre Kunden spielen in Deutschland eine herausragende Rolle. Gerade im Mittelstand fehlt es jedoch oft an der Bereitschaft und den Ressourcen, sich intensiv mit dem Thema IT-Sicherheit auseinanderzusetzen. IT-Sicherheit ist für Maschinenbauer und ihre Kunden kein Kernthema, sondern eine Eigenschaft, die auf möglichst einfache und modulare Weise garantiert werden soll.

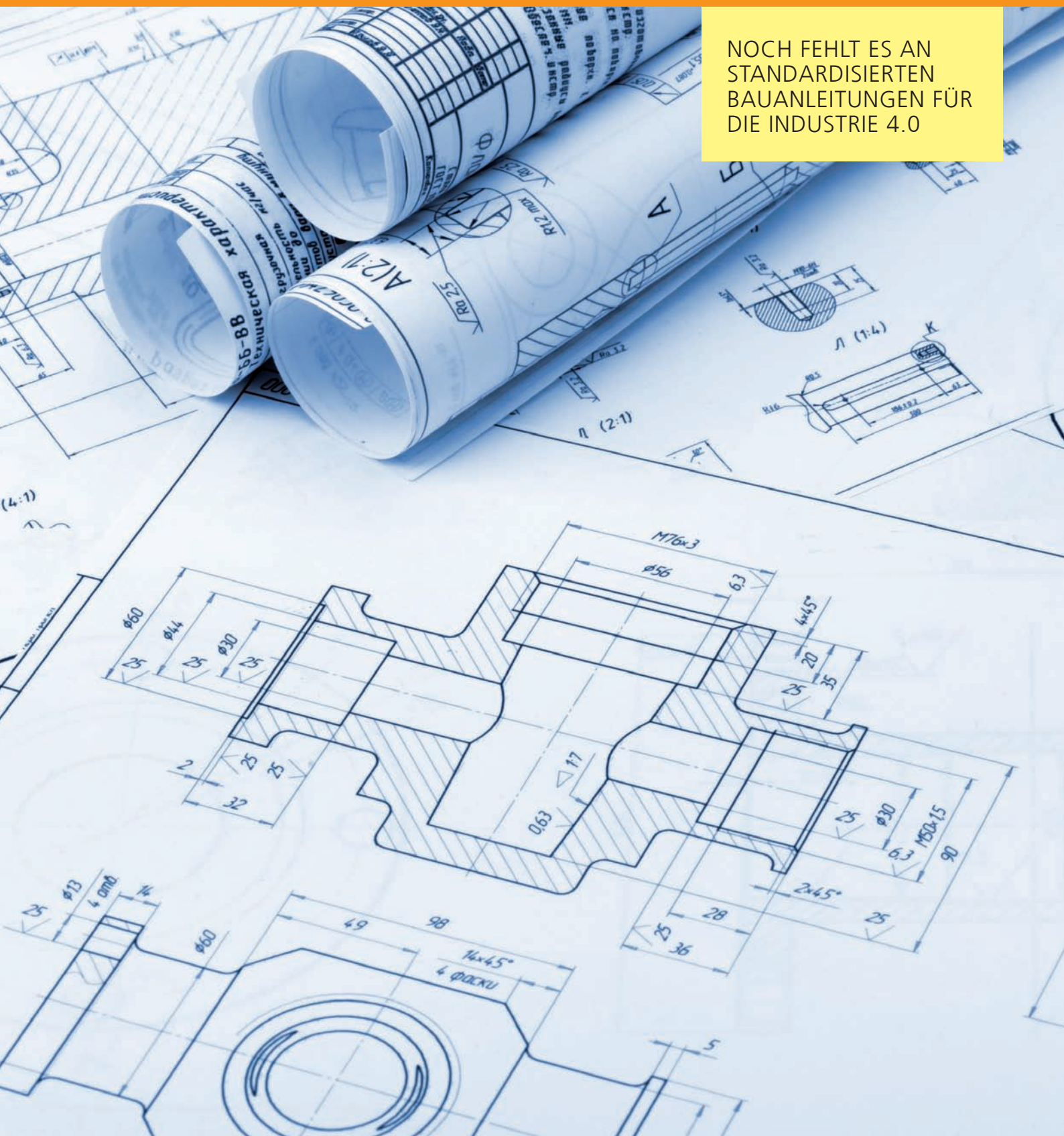
Die Branche wünscht sich deshalb einen standardisierten Ansatz, mit dem sich die Produktion absichern lässt, und zwar innerhalb einer Produktionsstätte, innerhalb eines Unternehmens und auch entlang firmenübergreifender Wertschöpfungsketten. Der Ansatz soll auf einem Katalog von standardisierten Maßnahmen aufbauen und letztlich umgesetzt werden durch mit diesem Katalog konformen Technologien, IT-Produkten und IT-Dienstleistungen. Referenzmodelle liefern Standards und Best Practices dazu, welche Maßnahmenkombinationen und welche Sicherheitsarchitekturen sinnvoll sind und wie diese über Firmengrenzen hinweg unter Wahrung der IT-Sicherheit kombiniert werden können. Ziel ist ein ausreichendes IT-Sicherheitsniveau, das mit Metriken und Messmethoden von unabhängiger Stelle geprüft/nachgewiesen werden kann. Bei Anwendung dieses Ansatzes erhält ein Unternehmen eine konkrete Bauanleitung, mit der sich vorhersagbar und ohne eigene IT-Sicherheitsexpertise das angestrebte IT-Sicherheitsniveau erreichen lässt.

Die Realität ist von diesem Ideal sehr weit entfernt. Die heutige IT-Sicherheit ist geprägt von herstellerspezifischen Insellösungen und punktuellen Schutzvorkehrungen. Ende-zu-Ende-Sicherheit in einer heterogenen Umgebung und über Unternehmensgrenzen hinweg ist eine offene Herausforderung für Forschung und Entwicklung. Es existieren zwar diverse Standards – z.B. zu Verschlüsselung, sicherer Kommunikation, Schlüsselmanagement, Authentisierung und Autorisierung, Sicherheits-Monitoring. Oft sind diese aber zu aufwendig für den Einsatz in der Produktions-IT und für die vertikale Integration zwischen Unternehmens- und Produktions-IT. Es existieren auch diverse Rahmenwerke, mit denen sich herstellerunabhängig unternehmensübergreifende Sicherheit realisieren ließe – z.B. Web Services Security. Diese sind allerdings ebenfalls sehr aufwendig und aufgrund ihrer hohen Flexibilität und Erweiterbarkeit zu unspezifisch für den hier angestrebten industriellen Einsatz.

Herstellern und Integratoren von Anlagen fehlt es also an konkreten Vorgaben, wie sich angemessene IT-Sicherheit in Planung und Betrieb umsetzen lässt. Nach Kenntnis der Teilnehmer des Eberbacher Gesprächs wurde dieses Problem von den bekannten Pilotprojekten zu Industrie 4.0 bislang nicht ausreichend aufgegriffen.

Eine umfassende Lösung dieses Problems erfordert eine signifikante und längerfristige Investition in Forschung und Entwicklung. Es gibt allerdings auch eine ganze Reihe von kurzfristig realisierbaren Maßnahmen, die dringend angegangen werden sollten.

Leitfäden, Mindeststandards und Reifegradmodelle
Eine erste Annäherung an die oben skizzierte Vision stellen branchenspezifische, informelle Leitfäden (Best Practices) und verpflichtende Mindeststandards für die IT-Sicherheit dar.



NOCH FEHLT ES AN STANDARDISIERTEN BAUANLEITUNGEN FÜR DIE INDUSTRIE 4.0

4. HERAUSFORDERUNGEN UND LÖSUNGSANSÄTZE

Zur Erarbeitung von Leitfäden und Mindeststandards gilt es, die Besonderheiten und spezifischen Schutzbedarfe einer Wertschöpfungskette innerhalb einer Branche zu erfassen und mit Hilfe dieser Informationen eine Bedrohungs- und Risikoanalyse durchzuführen. Aus den Ergebnissen lassen sich dann branchenspezifische Szenarien, Beispiele, Verhaltensmaßregeln und Richtlinien entwickeln. Im Rahmen von eher kurzfristigen Forschungsprojekten sollten die vorgeschlagenen Leitfäden und Mindeststandards exemplarisch umgesetzt und hinsichtlich Kosten und Nutzen bewertet werden.

Aufbauend auf den so gesammelten Erkenntnissen lassen sich mit Hilfe von Metriken und Messmethoden mehrstufige Reifegradmodelle erzeugen, mit denen Unternehmen den Übergang vom niedrigen zum höheren Sicherheitsniveau zielgerichtet verfolgen und zeitlich gestaffelt planen können. Mittelfristig kann dieser Ansatz zu einer formalen IT-Sicherheitszertifizierung von Industrieanlagen und Anlagenkomponenten beitragen.

Best Practices für Entwickler, Hersteller und Betreiber
Während es in der IT-Industrie für viele Themen der Entwicklung bereits ausgiebiges öffentliches Schulungsmaterial und Best Practice-Sammlungen gibt, existieren kaum spezialisierte Best Practices für den industriellen Kontext bzw. für die Softwareentwicklung für Industrieanlagen. Weil im Industrieumfeld viele verschiedene Parteien beteiligt sind, sind neben Informations- und Schulungsmaterial für Softwareentwickler von Industrieanlagen auch Best Practices für Anlagenbauer zur Konzeption von Industrieanlagen nötig.

Herstellerunabhängige Sicherheitsmodelle und Semantik
Bereits heute stellt die Erfassung einer bestehenden Produktionslandschaft und ihrer IT-Sicherheitseigenschaften nicht nur aufgrund ihrer Komplexität eine Herausforderung dar. Grundsätzlich fehlt es an einer branchenunabhängigen Semantik und entsprechenden IT-Sicherheitsmodellen. Deshalb sind Anlagenhersteller und -betreiber derzeit nicht in der Lage, Sicherheitseigenschaften von Maschinen, Anlagen und Prozessen einheitlich – also unabhängig von Hersteller oder Betreiber – darzustellen.

Im Maschinenbau sind diverse Ansätze bekannt, eine Automatisierungs- und Produktionslandschaft zu modellieren und formal zu beschreiben. Diese Ansätze sind mit den entsprechenden Methoden der IT-Sicherheit zu kombinieren. Auf diese Weise kann relativ schnell ein branchenübergreifender Ansatz zur Modellierung von Industrieanlagen unter Einbeziehung der IT-Sicherheit entwickelt werden. Mit diesem Ansatz wird es möglich sein, Geräte und Dienste im industriellen Kontext zu erfassen und zu beschreiben. Die Notation muss maschineninterpretierbar sein, sodass aufbauend auf den semantischen Modellen weitere Auswertungen möglich sind.

DIE AUTOMATISIERUNGS-PYRAMIDE

4. HERAUSFORDERUNGEN UND LÖSUNGSANSÄTZE

4.2 »SECURITY BY DESIGN« FÜR EINZEL- UND GESAMTSYSTEME

Aktuell existiert keine einheitliche Methodik, mit der Softwareentwickler die Sicherheitsanforderungen und den Schutzbedarf industrieller Systeme frühzeitig berücksichtigen können. Dadurch werden IT-Systeme oftmals erst nach dem funktionalen Entwurf evaluiert und um Sicherheitsmaßnahmen ergänzt. Diese nachträgliche Integration von Sicherheitslösungen verursacht oft große Aufwände für Nachbesserungen und damit erfahrungsgemäß unnötig hohe Kosten für Hersteller und Betreiber.[5]

Besondere Herausforderungen bestehen auch hinsichtlich der Erprobung von IT-Sicherheitslösungen im industriellen Umfeld. Zum einen sollen diese Lösungen komplexe Systeme vor Angriffen schützen, zum anderen müssen sie hohe Anforderungen hinsichtlich Echtzeit und funktionaler Sicherheit erfüllen. Gerade Letzteres lässt sich nicht ohne weiteres testen: Um die Praxistauglichkeit dieser Lösungen zu prüfen, muss man sie unter möglichst realen Bedingungen testen. Dies ist aber bislang nicht möglich, ohne Risiken hinsichtlich Zuverlässigkeit und Echtzeit-Anspruch einzugehen.

Wer die Industrie 4.0 vor Ausfällen und Angriffen schützen will, der muss IT-Sicherheit und Privatsphärenschutz bereits beim Entwurf intelligenter Produktionsanlagen, Prozesse und Dienste berücksichtigen – und dies über den kompletten Lebenszyklus von Systemen hinweg. Um Angriffssicherheit realitätsnah zu erproben, Ausfallrisiken zu minimieren und Unternehmen zu Investitionen in IT-Sicherheit zu bewegen, erscheint die Etablierung von Testmöglichkeiten und aussagekräftigen Kennzahlen (Metriken) ein vielversprechender Weg.

Secure Engineering

In der IT-Welt gibt es für die Entwicklung sicherer Software bereits entsprechende Methoden und Werkzeuge, die helfen, Schwachstellen frühzeitig zu identifizieren oder ganz zu vermeiden. Dieses Wissen gilt es, von der IT-Welt auf Produktion und Automation zu übertragen. Dazu braucht es unter anderem entsprechende Entwicklungsstandards und Testwerkzeuge, die den besonderen Anforderungen der Produktionswelt gerecht werden. Existierende Standards zur sicheren Entwicklung von IT-Anwendungen (z.B. ISO 27034 / 27036) sollten in die Industriewelt übertragen und mit den Standards zur funktionalen Sicherheit (Safety) verbunden werden.

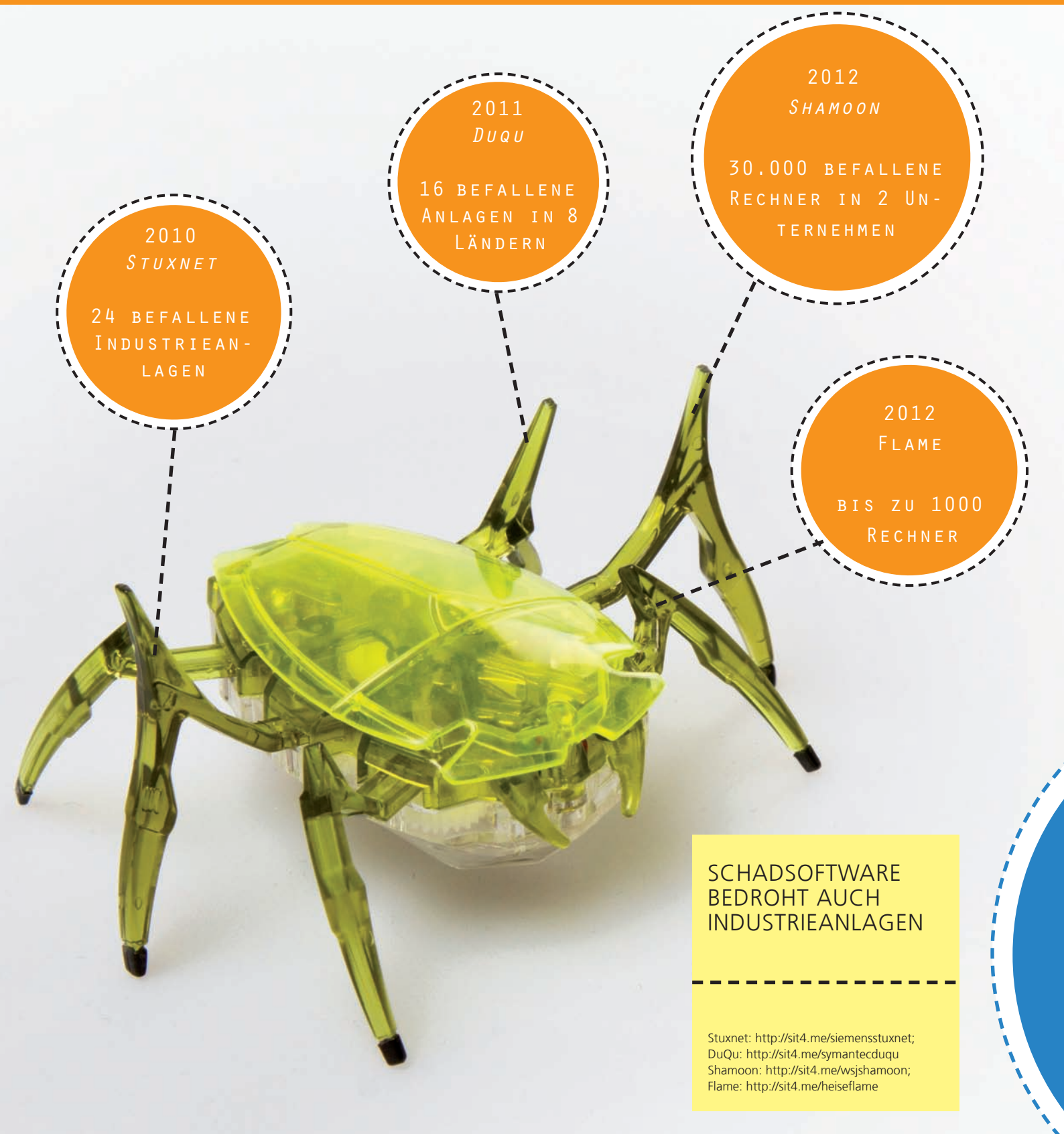
Weiterhin ist auch eine Adaption von Testwerkzeugen für den industriellen Kontext seitens der Industrie wünschenswert, um »Security by Design« durch effiziente Prüfangebote unterstützen zu können. Techniken wie Bedrohungs- und Risikoanalyse müssen dabei so angepasst werden, dass die Verantwortlichen in der Industrie, welche oft einen IT-fernen Hintergrund haben, die Ergebnisse einschätzen und die Techniken effizient anwenden können. Zudem müssen Werkzeuge entwickelt werden, die eine möglichst automatische Analyse von Quellcode und Industrieprozessen hinsichtlich der Verwundbarkeiten gestatten. So existieren derzeit kaum Werkzeuge zur statischen Codeanalyse für die in der Industrie üblichen Programmiersprachen und -werkzeuge (z.B. Assembler, Scout, HIMA ELOP II SPS, CoDeSys, Step-7 oder Sprachen nach EN 61131-3).

Metriken

Damit es sich für Unternehmen lohnt, IT-Sicherheit

»SICHERHEIT MUSS FESTER BESTANDTEIL DER INTEGRATIONSARCHITEKTUR SEIN – OHNE SICHERHEIT KEINE INDUSTRIE 4.0«

5 Michael Waidner, Michael Backes, Jörn Müller-Quade (Hrsg.): Entwicklung sicherer Software durch Security by Design; SIT Technical Report, Fraunhofer Verlag, München, 2013; https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Trendbericht_Security_by_Design.pdf.



SCHADSOFTWARE BEDROHT AUCH INDUSTRIEANLAGEN

Stuxnet: http://sit4.me/siemensstuxnet;
DuQu: http://sit4.me/symantecduqu
Shamoon: http://sit4.me/wsjshamoon;
Flame: http://sit4.me/heiseflame

4. HERAUSFORDERUNGEN UND LÖSUNGSANSÄTZE

in ihre Angebote zu integrieren, müssen sie die Möglichkeit besitzen, die Sicherheitseigenschaften im Markt zu kommunizieren. Kurzfristig wünschen sich Unternehmen deshalb Metriken zur Bewertung von IT-Sicherheitseigenschaften in Anlagen und Komponenten. Mit aussagekräftigen Informationen lassen sich Produkte vergleichen, und Hersteller sicherer Angebote können sich von weniger sicheren Wettbewerbern abgrenzen. Betreiber und Integratoren wiederum können IT-Sicherheitseigenschaften bei der Auswahl von Maschinen besser berücksichtigen.

Hersteller- und branchenübergreifende Testzentren
Gerade bei vernetzten Produktions- und Automationsanlagen existieren begründete Ängste, dass Angreifer unerkannt Maschinen manipulieren oder Produktionsdaten ausspähen können. In diesem Zusammenhang zeigen Erfahrungen aus anderen Branchen, dass oft Lösungen angeboten werden, die noch nicht über das notwendige Maß an IT-Sicherheit verfügen oder deren Angriffssicherheit noch keiner aussagekräftigen Prüfung unterzogen wurde. Dies wäre für die Industrie 4.0 rufschädigend und könnte enorme wirtschaftliche Schäden verursachen.

Aktuell existieren keine offenen Testzentren, die eine systematische Identifikation von Sicherheitslücken im Gesamtkomplex von realistischen Industrieumgebungen vorantreiben und potenzielle Risiken (z.B. unabsichtliche Schwachstellen, gezielte Spionagesoftware) evaluieren. Unternehmen wünschen sich deshalb eine Testumgebung, bei der Hersteller und Dienstleister ihre Lösungen modular auf einer branchen- und herstellerübergreifenden IT-Sicherheitsplattform testen können. Damit ließen sich auch neue Wertschöpfungsprozesse, softwarebasierte Dienste, CPS und die damit verbundenen IT-Sicherheitslösungen auf standardisierten Betriebsplattformen und Referenzarchitekturen zuverlässig validieren.

> »INDUSTRIE 4.0 LÄSST SICH NUR ENTLANG VON WERTSCHÖPFUNGSKETTEN REALISIEREN UND DAS SETZT VERLÄSSLICHES, DYNAMISCH ÜBERPRÜFBARES VERTRAUEN VORAUS.«

4.3 VERTRAUENSWÜRDIGE INFRASTRUKTUREN UND SICHERE IDENTITÄTEN

Bereits jetzt stellt es Unternehmen vor große Herausforderungen, klassische IT und Produktionssysteme hinreichend gegen Eindringlinge zu schützen. Patch-Management und komplizierte Update-Prozeduren erschweren die tägliche Praxis in industriellen Netzwerken. In der Idealvorstellung einer Industrie 4.0 bilden verschiedene Firmen für eine bestimmte Zeit gemeinsam ein virtuelles Unternehmen mit flexiblen Wertschöpfungsketten, die sich schnell an Marktveränderungen anpassen. Um dies zu erreichen, müssen die Partner diverse horizontale und vertikale Prozesse eng und vertrauensvoll verzahnen.

Technisch ist dies nur über eine durchgehende Vernetzung auf unterschiedlichen Ebenen machbar, was jedoch diverse Risiken mit sich bringt: Auf Anlagen-/Maschinen-Ebene verschafft die wachsende Vernetzung Angreifern mannigfaltige Zugriffsmöglichkeiten – z.B. durch mobile Endgeräte in Funknetzwerken. Besonders problematisch ist in diesem Zusammenhang, dass Produktionssysteme in hochgradig vernetzten Umgebungen für Angreifer leichte Ziele darstellen.

Die Vernetzung vollzieht sich auch auf Prozessebene entlang von Wertschöpfungsketten, etwa durch Cloud-Anbindung. Damit sich etwa Dienstleistungsmarktplätze für Fertigungsleistungen etablieren können, müssen Unternehmen Vertrauen in die virtuellen Partner und deren Dienstqualität haben. Diese


4.0
13406
ERP

4. HERAUSFORDERUNGEN UND LÖSUNGSANSÄTZE

Kombination aus extremer Flexibilität und großer Zuverlässigkeit in dienstorientierten industriellen Netzen stellt hohe Anforderungen an eine Sicherheits- und Vertrauensarchitektur.

Angesichts wachsender Komplexität und Bedrohungen brauchen Anlagenbetreiber darüber hinaus die Möglichkeit, ihre IT-Infrastrukturen effizient zu überwachen, Angriffe zu erkennen und abzuwehren. Damit verbunden ist die Integritätsprüfung von Maschinen und Anlagen. Effiziente Kryptografie und leichtgewichtige Primitive bilden die Basis, mit der Unternehmen die Integrität prüfen und sensible Informationen schützen können. Die Teilnehmer des Eberbacher Gesprächs plädieren für eine konsequente Verschlüsselung sämtlicher sensibler Daten. Die Verwendung von zuverlässigen und effizienten kryptografischen Mechanismen zum Schutz der Daten muss Standard sein und nicht die Ausnahme. Ziel ist eine echtzeitfähige und verlässliche Verschlüsselung.

Modulare Sicherheitsarchitektur

Für die Zusammenarbeit verschiedener Partner ist ein starkes gegenseitiges Vertrauen erforderlich. Verlässliche Konzepte, HW/SW-Architekturen und Standards im Bereich der IT-Sicherheit können diese Vertrauensbasis schaffen, müssen aber kostengünstige Anpassungen zulassen, um flexible Geschäftsprozesse und spezifische Ausprägungen zu unterstützen. Maschinen- und Anlagenbauer werden in Zukunft nicht mehr ausschließlich Produktionsanlagen vertreiben. Sie sehen einen Großteil ihres zukünftigen Gewinnwachstums in einer Industrie 4.0 zum Beispiel bei produktbegleitenden Dienstleistungen. Um neue Funktionen zu schaffen, werden Unternehmen etwa Softwarekomponenten oder Hardware-Funktionalität (z.B. optimierte IP-Cores in FPGA-gestützten Steuerungen) dynamisch nachladen und aktivieren. Durch die Veredelung der Maschine mittels Softwarekomponenten, Maschinen-Apps oder innovative Software-Diensten entsteht eine neue Art von Funktionsmodulen. Diese modularen und selbstkonfigurierenden Einheiten benötigen eine proaktive Sicherheitsarchitektur, die Vertraulichkeit und Integrität gewährleistet und automatisierte (Re-)Konfigurationen und Updates ermöglicht. Wichtig dabei ist die Schaffung von sicheren, besonders vertrauenswürdigen Elementen (»Vertrauensankern«), mit denen sich Identitäten von Maschinen, Anlagen und Diensten wirksam und schnell prüfen lassen. Entsprechende Konzepte etwa aus dem Kontext von »Trusted Computing« sind anzupassen. Damit lässt sich die notwendige echtzeitfähige Ende-zu-Ende-Sicherheit sicherstellen.

Monitoring und Angriffserkennung

Für den erfolgreichen Betrieb industrieller Netze in der Industrie 4.0 sind intelligente Monitoring- und autonome Entscheidungsprozesse notwendig, denn einzelne Unternehmen und ganze Wertschöpfungsnetzwerke müssen ihre Prozesse nahezu in Echtzeit optimieren und steuern. Die hohen Echtzeiterfordernisse stellen besondere Anforderungen an effiziente und wirksame Schutzmechanismen. Es wäre beispielsweise fatal, wenn Angreifer qualitätsbestimmende Prozessparameter in selbstregulierenden Anlagen unerkannt modifizieren und damit immense Schäden anrichten könnten. Damit Unternehmen Produktionsanlagen effizient überwachen, Angriffe erkennen und abwehren können, muss die Wehrhaftigkeit von Produktionsanlagen gesteigert werden – etwa durch Systeme für herstellerübergreifende Angriffserkennung (»Intrusion Detection«) und auf die Industrie ausgerichtete »Honeypots«.

Nach Meinung führender IT-Sicherheitsexperten genügen zur Realisierung der skizzierten Maßnahmen mitunter Anpassungen bestehender Verfahren und Technologien. Deren Praxistauglichkeit muss jedoch im Rahmen von Referenz-Architekturen und Pilotprojekten praktisch nachgewiesen werden. Erst wenn die kryptografiebasierte Ende-zu-Ende-Sicherheit diesen Belastungstest bestanden hat, werden produzierende Unternehmen bereit sein, in sie zu investieren.

SCHÜTZENSWERTES WISSEN FÄLLT IN ALLEN BEREICHEN DER INDUSTRIE 4.0 AN

Produktionsprozess

- Fabrikationsdaten
- Fertigungsschritte
- Protokolldaten

Produktions-schnittstelle

- Produktbezogene Daten
- Softwarekonfiguration

Produktstruktur

- Konstruktionsdaten
- Bauteile
- Entwürfe

Unternehmensumfeld

- Konstruktionsdaten
- Produktionsparameter

Unternehmensstruktur

- Personenbezogene Daten

Unternehmens-prozesse

- Unternehmensdaten
- Produktionsprozesse

4. HERAUSFORDERUNGEN UND LÖSUNGSANSÄTZE

4.4 WISSENSSCHUTZ, PIRATERIESCHUTZ UND NACHWEISBARKEIT

In der Industrie 4.0 ist der schnelle Fluss von Informationen, auch über Unternehmensgrenzen hinweg, von zentraler Bedeutung. Wertvolles Wissen in Produkten und Dokumenten sowie Prozesswissen über Produktionsverfahren und Produktionssysteme dürfen nicht fahrlässig übertragen und verbreitet werden. Im Rahmen eines föderierten Datenmanagements werden Unternehmen ihr geistiges Eigentum in Zukunft deshalb grundlegend anders organisieren und verwalten müssen als bislang. Das Interesse der legitimen Rechteinhaber ist dabei, Nachahmung zu vereiteln oder zumindest erkennbar zu machen.

Durch Sensoren und Aktoren und die zunehmend flexible Produktionsorganisation entstehen in der Industrie 4.0 neue Wissensformate. Neben den altbekannten und schützenswerten Entwürfen und Konstruktionsdaten treten Fabrikationsdaten, etwa als Produktionsparameter auf speicherprogrammierbaren Systemen (SPS) oder als Software/Hardware-Konfigurationen auf dynamischen Produktionsplattformen (»Platform as a Service«). Auch während der Produktion entstehen schützenswerte Informationen, meist in Form von Protokolldaten. Protokolldaten lassen einerseits Rückschlüsse auf Entwürfe und Konstruktionsdaten zu und sind damit ebenso schutzbedürftig wie diese. Andererseits können Protokolldaten im Sinne eines Produktgedächtnisses der Erfüllung gesetzlicher Nachweispflichten dienen, etwa in der Pharmaindustrie, müssen dann aber auch besonders gegen Manipulation geschützt werden.

Um angemessenen Wissensschutz, Datensicherheit und -integrität zu erreichen, müssen Industrie und Wissenschaft gemeinsam verlässliche Methoden und Werkzeuge zur Absicherung des digitalen Produktgedächtnisses entwickeln sowie Plattformen, mit denen sich Informationen über die gesamte Wertschöpfungskette und den Produktlebenszyklus hinweg schützen lassen.

Einbettung von Urheberschutz

Zur Produkterstellung werden sensible Daten auf unternehmensfremde Produktionssysteme transferiert und dort oft von fremden Systemen verwendet. Dies erfordert die Einbettung von Methoden und Techniken zum Urheberschutz von Konstruktionsdaten und Produktionsparametern. Als Vorbild können etwa Verfahren dienen, wie man sie aus der digitalen Fotografie kennt, wo Meta-Informationen in Bilddateien eingebettet werden. Um die Urheberschaft von digitalen Daten eindeutig und gerichtsverwertbar nachweisbar zu machen, eignen sich Werkzeuge aus der klassischen Kryptografie. Diese verlässlichen Mechanismen müssen an dienstorientierte, vernetzte Produktions- und Steuerungssysteme angepasst werden. Die Anwendungsforschung muss insbesondere Verfahren entwickeln, die Informationen über Urheber, Rechteinhaber, Version und Wissen über Herstellungsprozesse untrennbar mit den Daten verbinden. Sicherheitssensitive Daten und Informationen sollten nach Möglichkeit von den Maschinen und Produktionssystemen entkoppelt werden und deren Kenntnis nur bei Bedarf gewährleistet sein.

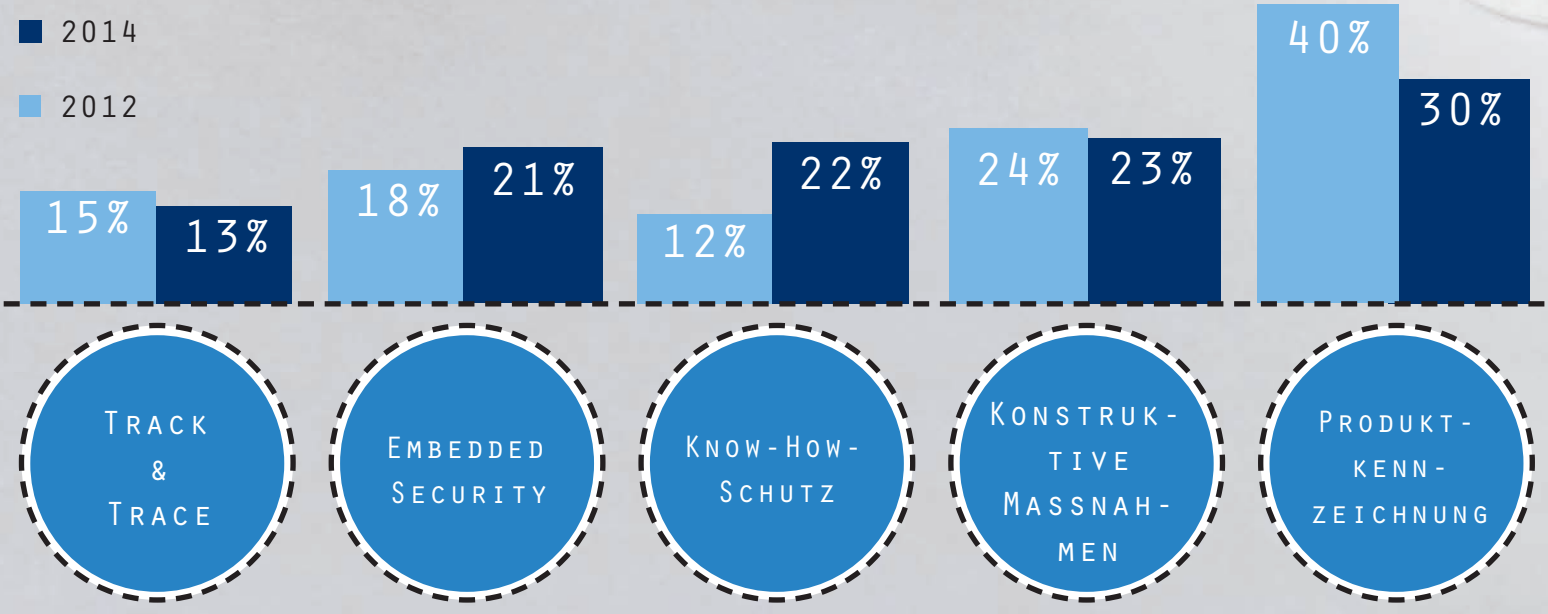
Industrielles Rechtemanagement

Grundsätzlich lassen sich Informationen durch Absicherung von Kommunikation, die Verschlüsselung von Daten sowie gezielte Informationsverarmung schützen. Die Industrie 4.0 braucht darüber hinaus ein industrielles Rechtemanagement sowie sichere und vertrauenswürdige

» INDUSTRIE 4.0 GENERIERT NEUE ARTEN VON WISSEN, DAS ES TECHNISCH UND RECHTLICH ZU SCHÜTZEN GILT«

ORIGINAL ODER FÄLSCHUNG? MIT WELCHEN MITTELN SCHÜTZEN DEUTSCHE ANLAGENBAUER IHRE PRODUKTE?

VDMA, VDMA-Studie Produktpiraterie 2014, S.22



4. HERAUSFORDERUNGEN UND LÖSUNGSANSÄTZE

Ausführungsplattformen, mit denen sich Ausführungsanforderungen der Rechteinhaber durchsetzen lassen. Auf welchem Produktionssystem und unter welchen Produktionsbedingungen (Parametern) darf ein spezielles Produkt hergestellt werden? Mit welcher Güte und Qualität und innerhalb welcher Fertigungstoleranzen? Bekannte Methoden des Enterprise bzw. Digital Rights Managements sind an die Industrie 4.0 anzupassen.

4.5 BENUTZBARKEIT – FAKTOR MENSCH

Vielerorts gibt es bereits Ansätze für eine Industrie 4.0, etwa in Form von »Lean Production«, »Collaborative Engineering« oder durch eine horizontale Integration über die Wertschöpfungskette hinweg. Besonders kleine und mittelständische Unternehmen hoffen von solchen neuen Formen der Produktionsorganisation zu profitieren. Allerdings existiert gerade dort wenig Wissen über potenzielle Gefahren, Risiken und existierende Sicherheitslösungen. Fehlendes Wissen und mangelndes Sicherheitsbewusstsein sowie falsche Sicherheitsannahmen können neue Sicherheitsvorfälle im produzierenden Sektor verursachen und damit eine breite Akzeptanz und eine zügige Umsetzung von Industrie 4.0-Konzepten gefährden.

Gleichzeitig muss die zuverlässige Kontrolle und echtzeitfähige Ausführung von systemkritischen Funktionen auch in vernetzten und IT-kontrollierten Fertigungslinien grundsätzlich gewährleistet sein. Softwaregestützte Schutz- und Steuerungsfunktionen müssen verlässlich und in Echtzeit erfolgen, etwa für die Übermittlung von Notfallkommandos zum Schutz menschlichen Lebens. Solche Not-Aus-Szenarien müssen auch in der Industrie 4.0 und im Rahmen einer nahezu echtzeitfähigen Vernetzung über das Internet/Intranet funktionieren, auch wenn die Signale drahtlos übermittelt oder von mobilen Geräten wie Tablets ausgelöst werden.

Industrie 4.0 ermöglicht dem Fabrikpersonal der Zukunft interessantere, flexiblere und selbstbestimmtere Arbeitsformen, stellt jedoch auch höhere Anforderungen an die Menschen, denn die wachsenden Risiken lassen sich nur mit Hilfe von sicherheitsbewusstem und geschultem Personal bewältigen. Neben entsprechenden Basisschulungen zur IT-Sicherheit braucht es deshalb konkrete Leitfäden zu Installation und Betrieb von Industrieanlagen und Geräten, die eine sichere Installation/Konfiguration und regelmäßige Kontrolle

Der Mensch ist in Zukunft für die Produktion...

Unwichtig
0,5%

Teils/Teils
2,7%

Wichtig
36,6%

Sehr wichtig
60,2%

WIE WICHTIG WIRD MENSCHLICHE ARBEIT IN DER ZUKUNFT FÜR DIE PRODUKTION SEIN?

Quelle: Produktionsarbeit der Zukunft, Fraunhofer Verlag 2013, S.50

4. HERAUSFORDERUNGEN UND LÖSUNGSANSÄTZE

von Industrieanlagen und Geräten beschreiben. Darüber hinaus kann es sinnvoll sein, besondere Fachkarrieren zu etablieren, die Kenntnisse aus Maschinenbau, IT-Sicherheit und Informatik kombinieren.

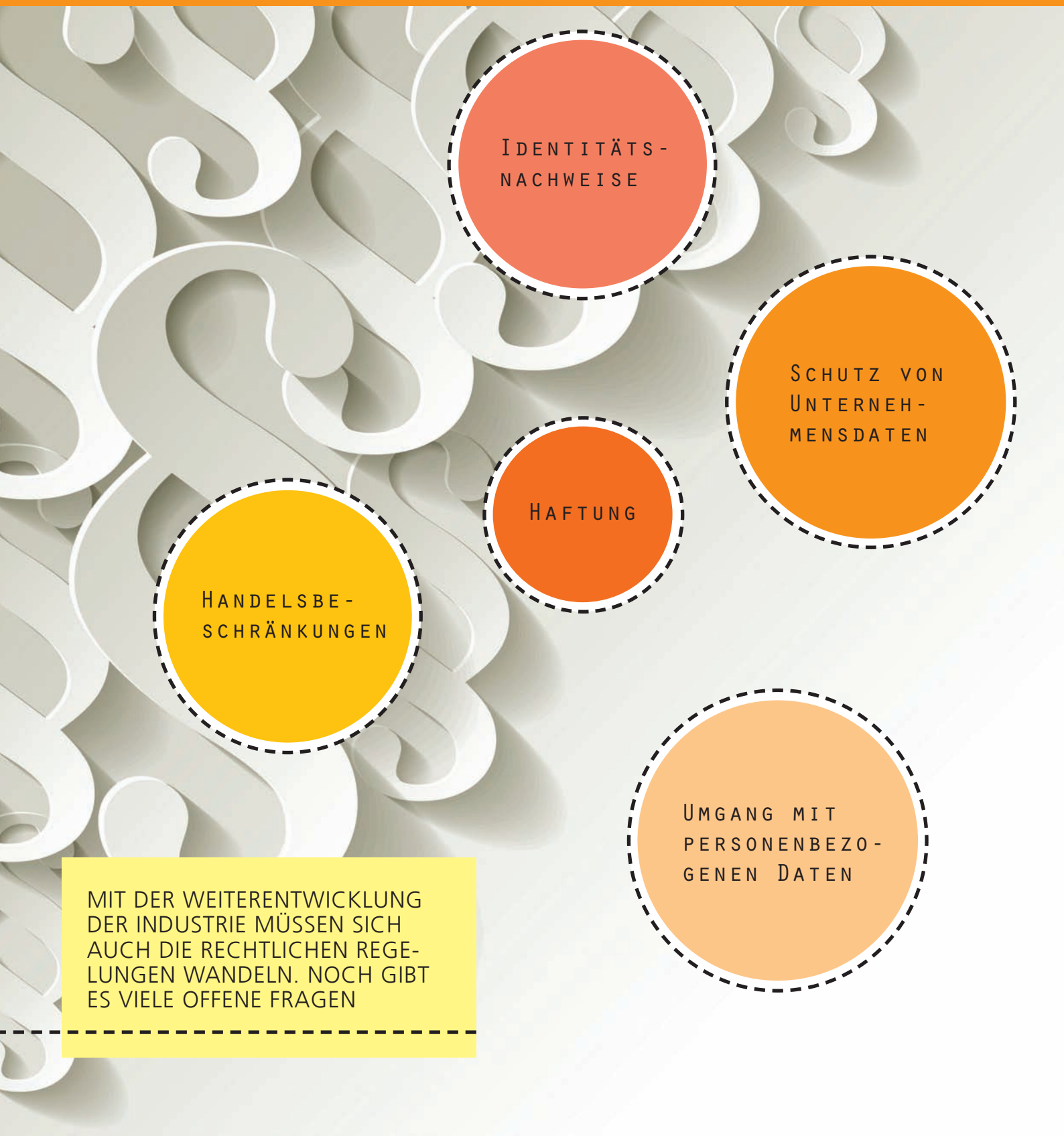
Grundsätzlich sind die Teilnehmer der Meinung, dass die Unternehmen den industriellen Transformationsprozess menschengerecht gestalten müssen. Der Sicherheit von Leib und Leben kommt dabei die höchste Priorität zu. Um dies zu gewährleisten, müssen die Benutzerschnittstellen sowie Zugangs- und Zugriffssicherungssysteme entsprechend einfach und verständlich gestaltet werden. Darüber hinaus sind aber auch für Notfälle alternative Prozeduren zu entwickeln. Bei der Gestaltung der betrieblichen Abläufe sollte die Belegschaft aktiv miteinbezogen werden, um den Erfahrungsschatz des Personals mit einzubringen und eine hohe Akzeptanz der neuen Organisationsregeln sicherzustellen.

4.6 RECHTSSICHERHEIT UND DATENSCHUTZ

Die Industrie 4.0 ist im starken Maß auf verteilte Dienstleistungen im Zusammenschluss unterschiedlicher Anbieter ausgelegt. Neben den technischen Herausforderungen einer solchen verteilten Produktionsplattform müssen ebenfalls rechtliche und juristische Anforderungen von Beginn an beachtet werden. Andernfalls können Rechtsunsicherheiten und unüberschaubare Haftungsrisiken die industrielle Entwicklung und damit die praktische Umsetzung von Industrie 4.0-Konzepten massiv behindern.

Zusätzliche Anforderungen ergeben sich in der Industrie 4.0 beispielsweise durch unklare rechtliche Rahmenbedingungen bei selbstorganisierenden, dienstorientierten Produktionsplattformen. Bei solchen Plattformen ist die Rechtssicherheit für Kunden und Produzenten deutlich unklarer und aufwendiger als bei herkömmlichen, starr organisierten Industrien. Gerade in einem internationalen Markt muss sichergestellt sein, dass die beteiligten Partner wirklich existieren und die angebotenen Leistungen auch in der gewünschten Qualität erbringen bzw. dass sie in Haftung genommen werden können. Dementsprechend ergeben sich für dezentral organisierte Produktionssysteme besondere Anforderungen an die Identität von Vertragspartnern, die Nachweisbarkeit und Gültigkeit angebotener Dienstleistungen und Absicherung der Vertragsleistungen.

Besonders problematisch sind zudem Fragen des Datenschutzes. Das hohe Datenvolumen sowie die starke Interaktion und Auswertung (Big Data) zwischen den Beteiligten führt zu neuen Herausforderungen. Dies gilt für den Schutz von Unternehmens- und Produktionsdaten ebenso wie für personenbezogene Daten von Mitarbeitern und Kunden. Um Haftungsrisiken zu minimieren, brauchen Unternehmen nicht nur entsprechende Sicherheitstechnik, sondern müssen auch orga-



MIT DER WEITERENTWICKLUNG DER INDUSTRIE MÜSSEN SICH AUCH DIE RECHTLICHEN REGELUNGEN WANDELN. NOCH GIBT ES VIELE OFFENE FRAGEN

4. HERAUSFORDERUNGEN UND LÖSUNGSANSÄTZE

nisatorische Maßnahmen ergreifen, die sich allerdings nur im Rahmen von Rechtssicherheit entwickeln lassen. Um das Zusammenwirken neuer Technologien zu befördern und gleichzeitig die informationelle Selbstbestimmung des Einzelnen zu ermöglichen, braucht es die rechtliche Analyse und juristische Gestaltung des industriellen Kontextes. Besonders wichtig ist Rechtssicherheit auch, um ein gesichertes und verbindliches unternehmensübergreifendes Qualitätsmanagement von Dienstleistungen in der Industrie 4.0 zu ermöglichen.

Existiert der Partner wirklich und ist er der, der er vorgibt zu sein? Wer garantiert die Zuverlässigkeit und Qualität dieser neuen, äußerst dynamischen Dienste? Sind die übermittelten Daten korrekt? Wer haftet bei Ausfall oder Fehlern? Wer hat das Recht an Daten, die erst im Laufe des Produktionsprozesses entstehen? Welche Daten sind personenbezogen und unterliegen damit dem Datenschutz? Diese Fragen gilt es zu beantworten, sodass Unternehmen in ihren jeweiligen Branchen verlässlich agieren können, national und international.

5. SCHLUSSBETRACHTUNG

IT-Sicherheit ist bereits heute ein wichtiges Thema in der Industrie und ein entscheidendes Thema für den Erfolg von Industrie 4.0. Mit den hier skizzierten Maßnahmen sollte es möglich sein, die Herausforderungen der industriellen IT-Sicherheit zielgerichtet anzugehen und den aktuellen und kommenden Gefahren wirkungsvoll zu begegnen.

Dazu müssen klassische IT und Industrieproduktion noch stärker zusammenwachsen. Die entsprechenden Anstrengungen, die hierzulande bereits unternommen wurden, gilt es zu verstärken, denn Innovationen sind notwendiger denn je: Laut einer KPMG-Studie sind viele Industrieunternehmen in Sorge, im internationalen Wettbewerb ins Hintertreffen zu geraten. Nicht zuletzt fehlt es ihnen auch an Arbeitskräften, welche die Digitalisierung der Produktionsprozesse verstehen und gestalten können.

Die Unternehmen haben ihre Strategie entsprechend ausgerichtet: Auffällig, so die Studie, sei die große Bereitschaft zu bahnbrechenden Innovationen in Deutschland, die mit 77 Prozent doppelt so hoch sei wie der internationale Wettbewerb. Wenn die hier skizzierten Lösungsansätze ausgearbeitet und angegangen werden, kann »Industrial Security made in Germany« ein wichtiges Qualitätsmerkmal dieser Innovationen werden und dazu beitragen, den technischen Vorsprung der deutschen Industrie nachhaltig zu sichern

Redaktion
Michael Waidner
Michael Kasper
Thorsten Henkel
Carsten Rudolph
Oliver Küch

Layout
Sonja Karl

Anschrift der Redaktion
Fraunhofer SIT
Presse- und Öffentlichkeitsarbeit
Rheinstraße 75
64295 Darmstadt
Telefon +49 6151 869-282
Fax +49 6151 869-224
redaktion@sit.fraunhofer,de

Bildquellen

Cover:	© buchachon - Fotolia.com
S.3:	© GettyImages
S.5:	© nicolas hansen - iStockPhoto
S.7: o.l.n.r:	© Freepik.com
	© Freepik.com
	© xyno - iStockphoto.com
S.7: u.l.n.r:	© v.poth - Fotolia.com
	© tobkatrina - iStockphoto
	© Getty Images
S. 9:	© Fraunhofer IGD
S. 12, o.l.n.r:	© Rido - Fotolia.com
	© Zerbor - Fotolia.com
S. 12, u.l.n.r:	© fox17 - Fotolia.com
	© alphaspirit - Fotolia.com
S. 13:	© rangizzz - Fotolia.com
S. 15:	© JZhuk - Fotolia.com
S. 17:	© Olga Gwalushko - Fotolia.com
S. 19:	© stockWERK - Fotolia.com
S. 23:	© Mimi Potter - Fotolia.com
S. 25.:	© alphaspirit - Fotolia.com
S. 27:	© Daniel Coulman - Fotolia.com
S. 39:	© Sergey Nivens - Fotolia.com
S. 31:	© AllebaziB - Fotolia.com
S. 33:	© apops - Fotolia.com
Andere:	@ Fraunhofer SIT