# IT-Sicherheit als besondere Herausforderung von Industrie 4.0

*Sander Lass, David Kotarski*

## 1 Problemstellung

Die Vision von Industrie 4.0 – die vollständige Vernetzung aller eingesetzten Systeme zur erweiterten Kommunikation inklusive der Shop-Floor-IT – ergeben sich auch neue Bedrohungsszenarien. Zahlreiche Beispiele aus dem aktuellen Geschehen (Stuxnet, Duqu, etc.) zeigen, dass Cyber-Kriminalität nicht mehr nur auf die Standard-IT und -anwendungen beschränkt ist, sondern auch in die bisher vermeintlich sichere Shop-Floor-Ebene und deren IT-Lösungen (SPS, SCADA, etc.) vordringt. Vor allem Stuxnet hat bewiesen, dass auch auf der Ebene der Steuerung von Maschinen operiert wird. Hier ist es Angreifern möglich, direkt in den Produktionsprozess einzugreifen und diesen zu manipulieren.

Bisherige Ansätze und Vorgehensmodelle gehen entweder sehr generell vor, d.h. sie geben allgemeine Empfehlungen für die IT-Infrastruktur, oder sind im Wesentlichen auf Office- bzw. Standard-IT ausgerichtet und nur mit Aufwand und mit Abstrichen auf die Bedarfe der Automatisierungstechnik zu übertragen. Da für die Steuerung und Überwachung der IT im Produktionsbereich von Fabriken besondere Anforderungen an die eingesetzten Informationssysteme und Anwendungen gestellt werden. Der Beitrag befasst sich mit den typischen Komponenten der Automation und den spezifischen Bedingungen innerhalb von Produktionsanlagen, die die Übertragbarkeit bisheriger Modelle einschränken. Zur Illustration dienen die Grundschutz-Methodik des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und die Defense in Depth-Strategie als Adaption eines Militärkonzeptes für die IT-Sicherheit.

Die anstehende vierte industrielle Revolution mit ihrer starken Vernetzung bis in die Automatisierungstechnik in der Fabrikhalle hat Auswirkungen auf die Implementierung von IT-Sicherheit. Gerade durch die verstärkte

Kommunikation der Elemente, auch überbetrieblich, gewinnen die Umsetzung der Schutzziele Verfügbarkeit, Vertraulichkeit und Authentizität sowie Integrität besondere Bedeutung. Auch hier stellt sich die Frage nach einer geeigneten Adaptierung bestehender Konzepte und Methoden, welche die Anforderungen der Automatisierungsebene berücksichtigen als auch die sich neu ergebenden Problemstellungen (z. B. Wegfall des Air Gaps) adäquat adressieren.

Eine Fallstudie die mit Hilfe des Labors des Anwendungszentrums Industrie 4.0, welches eine hybride Simulationsumgebung als Forschungsplattform und Werkzeug zur Analyse von Produktionsanlagen zur Verfügung stellt, zeigt an Hand von verschiedenen Szenarios den Handlungsbedarf.

## 2 Die Fabrik als Anwendungsdomäne

Die eingesetzte IT-Infrastruktur produzierender Unternehmen – von den Bürosystemen der klassischen IT bis hin zu den Komponenten der Automatisierung auf der Feldebene – ergibt inzwischen ein komplexes und vielschichtiges Bild. Effektiver Betrieb, Wartung und Erweiterung bedürfen zwangsweise profundes Wissen und systematisches Vorgehen.

### *2.1 Anwendungs- und IT-Systeme in der Fabrik*

Mit dem Ziel einer effizienten Fertigung setzen produzierende Unternehmen typischerweise etliche IT-basierte Lösungen ein. Die Anwendungslandschaft und die konstituierende IT-Infrastruktur bestehen aus unterschiedlichen Systemen und Softwarekomponenten zur Durchführung unterschiedlicher Aufgaben: betriebswirtschaftliche und produktionstechnische Planung von Ressourcen und Aufträgen, die Steuerung der Produktionsanlagen und die Verwaltung von Betriebsmitteln und Lagern sowie für die Logistik von Rohmaterial, Betriebs- und Hilfsstoffen, etc. Abbildung 1 zeigt eine Systematisierung der beteiligten Systeme und deren Wirkungsbereiche. Je nach Ausgestaltung im konkreten Unternehmen sind diese mehr oder wenige stark ausgeprägt.

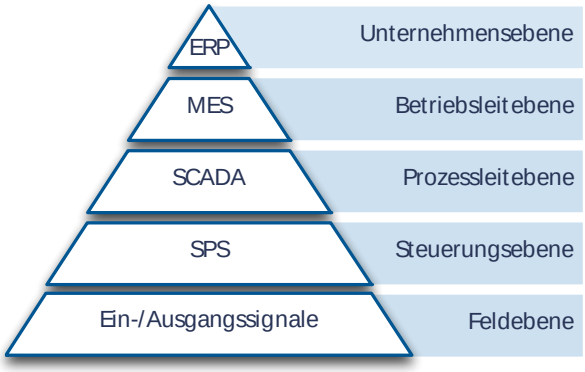


Abbildung 1: Automatisierungspyramide (Langmann,2004, S. 335)

Ausgehend vom Kundenauftrag beginnt an der Spitze der Pyramide mit dessen Erstellung im Enterprise Ressource Planning System (ERP) die betriebswirtschaftliche Planung der Produktion. Die Feinplanung erfolgt anschließend mit Hilfe des Manufacturing Execution System (MES). Als Ergebnis liegen Fertigungsaufträge vor, die mit Hilfe unterschiedlicher Medien – vom Laufzettel an der Gitterbox oder vollständig elektronisch mit geeigneten Terminals, z. B. als Teil der Betriebsdatenerfassung (BDE) – den Werkern oder direkt den Maschinensteuerungen zur Ausführung bereitgestellt werden.

Während der obere Teil der Pyramide (ERP und MES) im Wesentlichen aus Komponenten der Standard-IT aufgebaut ist und von der IT-Abteilung betrieben wird, sind die Systeme des unteren Teils (Prozessleit- bis Feldebene – auch als Shop-Floor bezeichnet) dem Bereich Automatisierung zugeordnet, der die Steuerung, technische Kontrolle und Koordination der Industrieanlagen übernimmt.

Als Bedien- und Beobachtungssystem ermöglicht Supervisory Control and Data Acquisition (SCADA) die erweiterte Überwachung durch die Aggregation und Visualisierung von Daten aus der Steuerungsebene als auch die Fernwartung der Anlagen.

Speicherprogrammierbare Steuerungen (SPS) sind für die Verarbeitung von Signalen der Sensorik und das Ansprechen der Aktorik der Anlagen zuständig. Sie sind wesentliche Elemente der Steuer- und Regelkreise der Automatisierung. Weitere Komponenten der Shop-Floor-IT sind neben den SPS die diskrete Verkabelung von Sensorik und Aktorik und Feldbussysteme (z. B. Modbus, PROFIBUS, SERCOS, AS-Interface, etc.) zur Signalkommunikation.

### *2.2 Besondere Anforderungen der Shop-Floor-Ebene*

Aus der Betrachtung der Aufgaben einer SPS als typischen Vertreter eines IT-Systems der Shop-Floor-Ebene, Steuer- oder Regelkreise für physisch agierende Komponenten zu implementieren, ergeben sich erhöhte Anforderungen an das Echtzeitverhalten, sowie an die funktionale und technische Robustheit. Auch auf Grund der rauen Einsatzumgebungen bestehen hinsichtlich Schutzart und -klasse besondere Ansprüche (IEC 60529).

Deshalb werden auf der Shop-Floor-Ebene dedizierte Informationssysteme und Anwendungen mit besonderen Merkmalen eingesetzt. Im Vergleich zu der betrieblichen Standard-IT ergeben sich u.a. folgende zusätzliche Anforderungen und Faktoren (BSI, 2013, S. 27f.):

- Echtzeitfähigkeit der Steuer- und Regelkreise
- Ausführung als Embedded Device
- fehlende Testmöglichkeiten
- lange Betriebs- und Innovationszyklen (> 7 Jahre)
- Sicherstellung von Gefahrlosigkeit für Mensch und Technik

Die dargestellten Punkte haben starken Einfluss auf die Gestaltung der IT-Sicherheit in der Werkhalle. Typische Lösungen aus der Standard-IT sind nur schwer oder mit größerem Aufwand bzw. spezifischen Anpassungen sinnvoll umsetzbar.

Wegen der unumgänglichen Aufrechterhaltung der Echtzeitfähigkeit, d. h. zum großen Teil harte Echtzeit mit Reaktionszeiten < 1ms, sind Aufbau und Segmentierung von Shop-Floor-Netzwerken nach sicherheitstechnisch relevanten Kriterien eine besondere Herausforderung. Komponenten, die Sicherheitsmaßnahmen technisch umsetzen, dürfen den Datenaustausch im System nicht verzögern. Mit diesen zusätzliche Leistungsanforderung gehen erhöhte Kosten einher, so dass in der Praxis auch schon mal das angestrebte Sicherheitsniveau nach untern korrigiert wird.

Unter eingebetteten Systemen (Embedded-Systems) sind spezialisierte Geräte subsummiert, die in Baurat und Hardwareausstattung auf einen bestimmten Aufgabenbereich abgestimmt sind. Embedded-Systems besitzen häufig längere Wartungszyklen. Dies liegt u. a. darin begründet, dass die Ausrollung von Patches mit hohem Aufwand verbunden ist. Updates stellen den Komplettaustausch der auf dem Gerät befindlichen Software (Firmware) dar, spezifische Konfigurationen (Einstellungen und Programme) müssen anschließend neu eingespielt und angepasst werden. Ergänzend gestalten sich die Update-Prozesse häufig sehr komplex, weshalb die Ausführung nicht intern, sondern oftmals durch den Hersteller selbst erfolgt und damit zusätzliche Kosten verursacht (BSI, 2013, S. 27).

Ein effektives Testsystem mit realistischer Umgebung ist aus Kostengründen selten vorhanden. Somit sind zum Beispiel Penetrationstests (Eindringen in die IT-Systeme einer Anlage zur Aufdeckung von Sicherheitslücken) ohne den Produktionsbetrieb zu gefährden bzw. zu beeinflussen nur begrenzt möglich. Dies bezieht sich auch auf die Durchführung von Vorabtests, wie z. B. beim Patch- und Updatemanagement üblich.

Im Vergleich zur Standard-IT ist der Lebenszyklus von Industrieanlagen und deren Komponenten beträchtlich länger. Dies bedeutet, dass in der Werkhalle Geräte unterschiedlichster Generationen zu finden sind und neue Informationstechnologien sich vergleichsweise langsam durchsetzen. In der Praxis existieren dahingehend interessante „Integrationslösungen“, bei deren Implementierung IT-Security, im Gegensatz zur Sicherstellung von Safety, nur unwesentlich oder gar keine Rolle spielten.

Im Kontext von Sicherheit bei Produktionsanlagen müssen die Begriffe Security und Safety differenziert werden. Neben der reinen Sicherheit als Schutz einer Anlage vor dem Menschen, ist die Sicherstellung des Schutzes von Menschen und Umwelt in der Werkhalle unbedingt in die Betrachtungen mit einzubeziehen. Während des Betriebs einer Produktionsanlage müssen die interagierenden Personen vor Schaden an Leib und Leben geschützt werden. Das hieraus entstehende Ziel wird typischerweise unter den Begriffen Safety oder funktionale Sicherheit (vgl. BSI, 2013, S. 12) subsummiert. Safety bezieht sich im Wesentlichen auf den Schutz von Menschen und ihrer Umwelt. Die funktionale Sicherheit bezüglich des gefahren- und störungsfreien Betriebes muss sichergestellt sein.

Im Gegensatz hierzu hat Security in Bezug auf IT einen anderen Fokus. Das zu schützende Objekt sind Informationen. Es gilt, das System vor schädlichen Eingriffen seitens des Menschen oder der Umwelt zu schützen. Schwachstellen sind mögliche Fehlbedienung, vorsätzliche Handlungen oder organisatorische Defizite. Die zu schützenden Hauptziele sind die Integrität, Vertraulichkeit und Verfügbarkeit der Daten sicherzustellen.

Gesetzlich vorgeschrieben (Arbeitsschutz, etc.) oder durch die bisherige Abschottung der produktionsnahen IT bzw. Automatisierungstechnik, welches ein Gefühl der Sicherheit vermittelt, beschränken sich die Sicherheitsaktivitäten häufig auf den Safety-Bereich.

Es bleibt festzuhalten, dass IT-Sicherheit für Industrieanlagen der Generation „Industrie 3.0“ ein relevantes Thema darstellt. Auf der einen Seite besteht durch die speziellen Gegebenheiten der Shop-Floor-Ebene eine nicht ausreichend effektive Anwendbarkeit klassischer IT-Sicherheitskonzepte. Andererseits können eben jene speziellen Gegebenheiten den Sicherheitsbeauftragten helfen, ein gewisses Maß an Sicherheit zu gewährleisten.

Beispielsweise sind zwei Systeme physikalisch getrennt, die jedoch Daten vom jeweilig anderen System benötigen, erfolgt der Datenaustausch unter

Verwendung eines Datenträgers. Es ergibt sich eine erhöhte Zugangssicherheit durch die notwendige physische Interaktion vor Ort. Dieses Prinzip wird als „Air Gap“ bezeichnet.

Werden proprietäre Systeme mit herstellerspezifischen bzw. nicht standardisierten Protokollen eingesetzt, kann sich dies durchaus positiv auf die Security auswirken. Gemäß dem Prinzip „security by obscurity“ sind Informationen zur jeweiligen Implementierung nicht oder kaum öffentlich zugänglich und erschweren das Aufdecken von Schwachstellen und deren Ausnutzung. Da es profundes Spezialwissen und spezielle Entwicklerwerkzeuge auf Seiten des Angreifers bedarf, ist einerseits der Aufwand einer Attacke sehr hoch und anderseits dessen Wirkungskreis beschränkt. Die Zahl potenzieller Angreifer ist demnach gering.

### *2.3 Der Grundschutz des BSI*

Über die letzten zwei Jahrzehnte sind für die Standard-IT verschiedene Familien von Normen und Richtlinien zur Behandlung von IT-spezifischen Risiken entstanden. Sie beinhalten Vorgehensweisen und Konzepte zur systematischen Bearbeitung sowie Möglichkeit entsprechender Zertifizierungen. Beispiele sind die internationale ISO 27000er-Familie (ISO, 2005), die nationale Variante des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) mit dem „IT-Grundschutz“ (BSI, 2008), aus den USA die NIST Special Publications der 800er-Reihe (NIST, 2010) oder für die Zertifizierung von Produkten die internationalen Common Criteria (CoCri 2012).

Der vom Bundesamt für Sicherheit in der Informationstechnik definierte Grundschutz wird in Form von Katalogen umgesetzt und definiert das folgende Begriffsmodell. Eine Bedrohung ist ein Umstand oder Ereignis, durch das ein Schaden entstehen kann (BSI, 2014, Abschnitt: Bedrohung). Der Schaden bezieht sich im Falle der Informationstechnik auf Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen. Damit eine Bedrohung zur Gefährdung wird, muss für ein konkretes Objekt eine bekannte Schwachstelle vorliegen. Welcher Schutz für die wertschöpfenden

Prozesse angemessen ist, definiert den Schutzbedarf (BSI, 2014, Abschnitt: Schutzbedarf).

Die in den Katalogen enthaltenen Maßnahmen lassen sich im Wesentlichen im Bereich der Standard-IT applizieren. Eine Projektstudie am Lehrstuhl für Wirtschaftsinformatik der Universität Potsdam in Zusammenarbeit mit der HiSolutions AG als Spezialist für IT-Risk und Compliance zeigte, dass die besonderen Anforderungen und Gegebenheiten der Shop-Floor-IT nur wenig berücksichtigt werden (Lass & Fuhr, 2014, S. 13ff.] Auch das BSI hat das Potenzial erkannt und arbeitet an einer Erweiterung ihre Grundschutz-methodik auf Anwendbarkeit in der industriellen Fertigung.

### *2.4 Defense in Depth als Lösungsansatz*

Um seine Infrastruktur zu schützen, wird oft die „Defense in Depth"-Strategie eingesetzt. Es werden mehrere Verteidigungsmaßnahmen, auch als Abwehrlinien bezeichnet, kombiniert und so Risiken eingegrenzt. Sämtliche Kommunikation erfolgt, wie Abbildung 2 verdeutlicht, in separierten Netzsegmenten, welche zusätzlich mit Intrusion Detection Systemen ausgestattet sind, um eventuelle Angriffe schnell aufzuzeigen und rechtzeitig Gegenmaßnahmen zu ergreifen. Das Einteilen in verschiedene Zonen ist in den Standards ANSI/ISA-99 (IEC62443) geregelt.

Der Aufwand um eine Shop-Floor-Infrastruktur zu kompromittieren wird durch den Einsatz mehrerer Einzelmaßnahmen (DMZ, Paket Filter, IDS, Timed Access Control, Deaktivierte USB-Ports) erhöht. Damit reduziert sich das Risiko und es bleibt mehr Zeit um entsprechende Gegenmaßnahmen einzuleiten. Abbildung 2 erläutert den schematischen Aufbau. Systeme werden in verschiedene Zonen segmentiert und können nur mittels speziellen „Leitungen" sogenannte Conduits kommunizieren. Dabei ist die Kommunikation so reglementiert, dass sämtliche irrelevanten Informationen, welche nicht direkt zwischen zwei Zonen benötigt werden, blockiert werden. Dieses auch als „Zone and Conduit" definierte Modell ist eines der zentralen Elemente der Defense in Depth-Strategie.

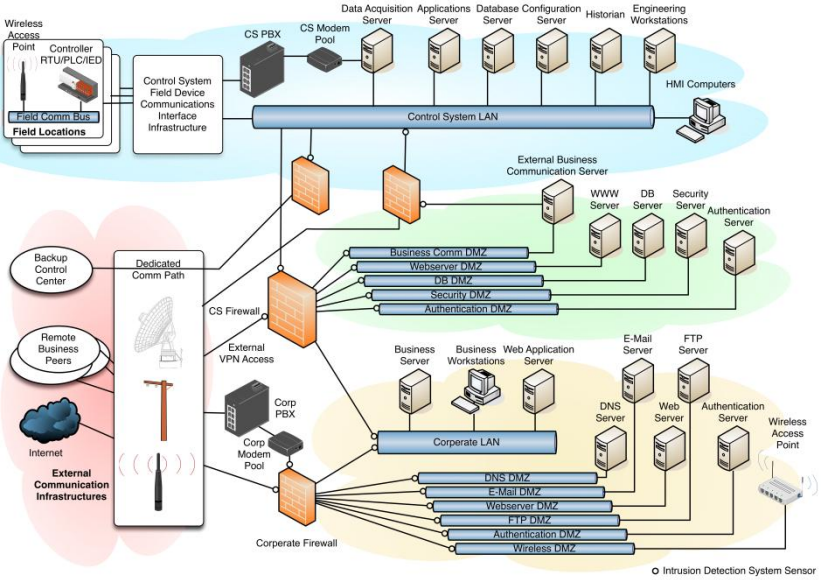


Abbildung 2: Beispiel einer Defense in Depth-Strategie (Kuipers, 2006, S. 23)

Defense in Depth bietet jedoch keinen vollständigen Schutz, härtet aber das System als solches vor Angriffen. Bei Standardangriffen (z. B. Portscans, Bruteforce, Skript-Kiddies) wirken diese Maßnahmen sehr gut, sodass schnell das Interesse verloren wird. Allerdings ist die abschreckende Wirkung im Falle von gezielten Angriffen, welche keine zufällige Bedrohung darstellen, sondern eine klare Absicht erkennen lassen und mit dem Einsatz von Geld für das Eindringen in die Anlage einhergehen, eher gering.

Defense in Depth kann in beliebiger Granularität umgesetzt werden, jedoch ist mit zunehmender Detailtiefe auch mit erheblichen Kosten zu rechnen. Da einzelne Zonen nur kontrolliert und reglementiert kommunizieren, sollten diese wohl überlegt strukturiert werden. Jeder Conduit muss gepflegt/gewartet und auch an die sich ändernden Anforderungen angepasst werden. Dementsprechend ergeben sich aus der zunehmenden Anzahl von Conduits auch steigende Kosten für Wartung und Anpassung.

Auch werden mit dem zunehmenden Einsatz von Sicherheitstechnik die Grenzen der Echtzeitanforderungen erreicht. Eine generelle Lösung kann

hier nicht aufgezeigt werden, da die jeweiligen Spezifika jeder Anlage genau berücksichtigt werden müssen. Defense in Depth dient daher als Leitfaden um zum Beispiel das „Zone and Conduit"-Modell einzusetzen. Nachdem ein Modell für die IT-Sicherheit einer Anlage aufgestellt wurde, muss es validiert, verifiziert und oftmals nachträglich angepasst werden. Nachträgliche Änderungen sind im laufenden Betrieb jedoch nur mit Aufwand zu realisieren, da es keine ausgiebigen Tests an Produktionsanlagen geben kann.

### *2.5 Der Faktor Mensch*

Auch in der Werkhalle spielt der Faktor Mensch im Zusammenhang mit sicherheitstechnischen Belangen eine Rolle. Der sorglose Umgang mit Wechseldatenträgern in Verbindung mit Bring-your-own-Device stellt die Sicherheitsexperten vor neue Herausforderungen (Deutschland sicher im Netz, 2014, S. 24). Ähnlich wie bei Stuxnet werden USB-Sticks mit ihrer gefährlichen Payload immer häufiger. Speziell präparierte Datenträger werden an Orten, die das Personal aufsucht ausgelegt und auf die Neugier der Angestellten gesetzt. Steckt ein Angestellter einen solch präparierten Stick in sein Dienstgerät, so beginnt der eigentliche Angriff auf das System. Unauffällig werden Daten transferiert und ein Einfallstor für weitere Angriffe geschaffen. Hier reichen technische Maßnahmen (z.B. Deaktivieren der USB-Ports) nicht aus, da sie den Arbeitsablauf behindern. Es müssen organisatorische Regelungen gefunden werden, die zum einen einfach zum anderen aber auch weitreichend sind. Beispielsweise könnten nur firmeneigene Datenträger erlaubt sein und alle privaten Datenträger sind per Dienstanweisung nicht zu benutzen. Auch hier müssen eventuelle Situationen von Vorhinein betrachtet werden: Was passiert wenn die Größe des Datenträgers nicht ausreicht? Wer inventarisiert und wartet die Firmendatenträger? Wie wird unterbunden, dass Datenträger die Firma verlassen?

Auch hier rüsten Betreiber und Angreifer kontinuierlich auf, weshalb das Sicherheitskonzept stetig angepasst werden muss. Ist die technische Seite

sehr gut abgedeckt, so versuchen die Angreifer die Lücken auf organisatorischer Seite auszunutzen. Oft geben nicht sensibilisierte Mitarbeiter unbeabsichtigt unternehmensrelevante Daten weiter. (Mitnick & Simon, 2003, S. 16f.) Für sie harmlose Informationen ergeben in ihrer Gesamtheit jedoch wertvolle Fakten für die potentiellen Angreifer. Beispielsweise empfinden Angestellte Informationen über interne Abläufe oder die eingesetzte Standardsoftware als harmlos. Die daraus ableitbaren Schlussfolgerungen hingegen (Wissen welche Person zugriffsberechtigt bzw. weisungsberechtigt ist oder bekannte Schwachstellen bei der eingesetzten Software) sind durchaus für die Planung eines Angriffs von Nutzen. Mittels einfacher Prinzipien ist es möglich das Handeln von Angestellten zu manipulieren. Ähnlich wie beim Marketing werden dabei die sechs Prinzipien von Cialdini (Autorität, Zuneigung, Revanchieren, Konsequenz, soziale Bestätigung und Mangel) erläutert, die die Grundlage für eine Manipulation einer Person schaffen, angewendet. (Cialdini, 2001, S. 76ff.) Social Engineering ist und bleibt eine eigesetzte Angriffstechnik, der mit organisatorischen und technischen Maßnahmen begegnet werden muss.

## 3 Die 4. industrielle Revolution

Industrie 4.0 als vierte industrielle Revolution propagiert eine Abkehr von der klassischen automatisierten Fabrik, die große Mengen gleichartiger Produkte auf der Basis zentraler Produktionspläne herstellt. Die Vision beschreibt die selbstorganisierte Fabrik, in der intelligente und teilautonome Objekte sich selbst die passenden Ressourcen suchen und viele Probleme der heutigen Fabrikorganisation durch direkte lokale Interaktion vermieden werden. Dieses Cyber Physical Production System (CPPS) realisiert eine neue Art von Fabrik – die „Smart Factory“.

### *3.1 Die vernetzte Fabrik*

Vernetzung und Kommunikation kommen in der Smart Factory besondere Bedeutung zu. Der Arbeitskreis Industrie 4.0 nennt als wesentliche Elemente autonome eingebettete Systeme, die drahtlos untereinander und mit dem Internet vernetzt sind (Kagermann, Wahlster & Helbig, 2012, S. 17).

Die flächendeckende Vernetzung von Informations- und Kommunikationstechnik zu einem Internet der Dinge, Dienste und Daten ist der Grundgedanke von Industrie 4.0 (Spath, 2014, S. 2)

Bezogen auf die Automatisierungspyramide erfolgt die Integration der Systeme in vertikaler Richtung – auch unter dem Begriff Konvergenz der IT aggregiert – als auch horizontal über ganze Wertschöpfungsnetzwerke. Die klare Trennung der Ebenen der klassischen Pyramide (Abbildung 1) ist in der Smart Factory nicht mehr gegeben (Günthner, Chisu & Kuzmany, 2010, S. 44). Ergänzend soll der gesamte Lebenszyklus des Produktes einbezogen werden. Informationen aus der Nutzung und Verwendung eines Produktes fließen in den Produktionsprozess ein und decken Potenziale auf (Barthelmey, 2014, S. 209).

### *3.2 Dezentrale Steuerung mit autonomen intelligenten Elementen*

Industrie 4.0 stellt innerhalb der Produktionsorganisation und -steuerung moderne Technologien, um dezentral gesteuerte Produktionsanlagen mit intelligenten und selbststeuernden Elementen in der Werkhalle zu gestalten. AutoID-Technologien und smarte Sensoren statten Systeme und Produktionsobjekte mit erweiterten Fähigkeiten zur Umgebungserfassung und Entscheidungsfindung aus.

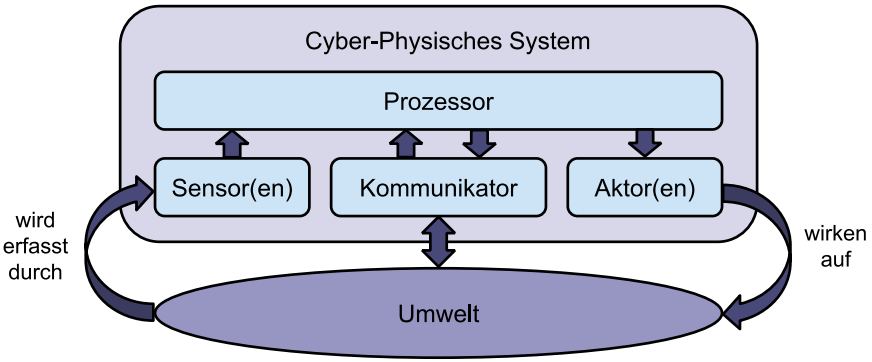


Abbildung 3: Schematischer Aufbau eines Cyber-Physischen Systems (Veigt, 2013)

Mit diesen, auch als Cyber Physical Systems (CPS) bezeichneten Elementen, und deren Zusammenspiel werden neue Paradigmen der dezentralen Steuerung und Prozessgestaltung in Fabrikanlagen implementiert. CPS realisieren die eindeutige Identifizierung und Lokalisierbarkeit von Produktionsobjekten, besitzen Informationen zu ihrem aktuellen Zustand und zu ihrer Historie, sowie zu alternativen Wegen zum gewünschten Zielzustand. Sie können autonom Entscheidungen treffen, d. h., Umgebungsinformationen aus der Sensorik oder der Kommunikation mit anderen CPS werden selbsttätig verarbeitet und entsprechende Aktionen ausgelöst. Abbildung 3 zeigt die vorhandenen Kommunikationswege sowie die möglichen Interaktionen zwischen System und Umgebung.

### *3.3 Standardisierung des Informationsaustauschs*

Bedingt durch das dezentrale Steuerungskonzept findet in der Smart Factory ein hohes Maß an Kommunikation statt. Etliche Informationen unterschiedlicher Aggregationsstufen werden zwischen den einzelnen Systemen ausgetauscht. Von einfachen An-Aus-Signalen bis hin zu vielschichtigen Datenstrukturen, welche die von CPS aufbereiteten Statusinformation als auch Konfigurations- und Fertigungsdaten transportieren, Anfragen beinhalten oder komplexe Interaktionen beschreiben. Durch die übergreifende Integration der Systeme über Domänen- und Hierarchiegrenzen, sowie über den gesamten Lebenszyklusphasen eines Produktes hinweg, entstehen hohe Ansprüche an die Interoperabilität der Systeme.

Durch geeignete Standards werden sowohl die technische als auch die semantische Dimension abgebildet, um eine ungehinderte Kommunikation aller beteiligten Elemente zu ermöglichen. Beispielsweise bietet OPC-UA einen flexiblen Container, der auch die Kommunikationsinfrastruktur vereinfacht (im Gegensatz zum klassischen OPC-DA). In Kombination mit einer semantischen Beschreibung entfallen umständliche und fehleranfällige Konvertierungen und hoher Anpassungs- und Konfigurationsaufwand. Universal Machine to MES (UMCM) ist dahingehend ein viel-

versprechende Ansatz. Feldbusssysteme lösen zunehmend durch Einsatz smarter Sensoren die diskrete Verkabelung ab (Lass & Hennig, 2012, S. 16ff.). Sie lassen sich einfach in Standardinfrastrukturen integrieren bzw. können dann deren Medien (Kommunikationsstack und Protokolle) nutzen. Bereits jetzt gibt es dahingehend durchaus markreife Systeme z.B. EtherCAT, Modbus TCP. In der Realität werden stets autonome Objekte unterschiedlicher Hersteller mit unterschiedlichen Fähigkeiten zur Autonomie in Fertigung, Montage und Logistik interagieren. Bisherige Insellösungen einzelner Bereiche, die eine aggregierte und zeitnahe Auswertung (wie Manufacturing Analytics) nur mit großem Aufwand und inhaltlichen Verlusten zuließen, werden durch eine einheitliche und standardisierte Kommunikationsinfrastruktur ersetzt.

### *3.4 Die psychosoziale Komponente*

Der Arbeitsablauf kann sich durch Industrie 4.0 stark verändern. Human Maschine Interaction (HMI) gewinnt an Bedeutung (Scheer, 2013). Durch die Steigerung der Komplexität von Maschinen und Steuerungssystemen steigen auch die Anforderung an das technische Personal. Der Mensch ist in der Smart Factory ein wesentlicher Akteur. Durch technische Unterstützung in seinen Fähigkeiten erweitert, wird er vom klassischen Bediener zum Steuernden und Regulierenden. Stark ausgeprägt sind selbstverantwortliche Autonomie und dezentrale Führungs- und Steuerungsformen sowie erweiterte kollaborative Arbeitsorganisation (Kagermann, Wahlster & Helbig, 2013, S. 27). Langjährige Erfahrung qualifizierter Mitarbeiter zur Beurteilung und Lösung von Ausnahmesituationen, kombiniert mit den informationstechnischen Werkzeugen des Industrie 4.0 Konzepts, ergeben neben hoher Effizienz auch bisher nicht denkbare Entfaltungsmöglichkeiten für Mitarbeiter. (Spath, 2014, S. 2)

## 4 Mit Industrie 4.0 wird alles anders?

Durch den zuvor schon erwähnten stetig steigenden Grad an Komplexität und Vernetzung, steigen auch die Risiken und der Bedarf an adäquaten Konzepten zur deren Minderung.

### *4.1 Anpassung bisheriger Konzepte*

Durch die verstärkte Kommunikation der Komponenten von Industrie 4.0 sind nun auch externe Quellen (Kundenwünsche, Zuliefererdaten) in den Produktionsprozess integriert. Da der Grad der Vernetzung stetig steigt und auch der Bedarf an Informationen unternehmensübergreifend ist, sind vermeintlich sichere Konzepte wie Air Gap nicht mehr zeitgemäß (Byres, 2013, S. 29ff.). Eine Anpassung bisheriger Konzepte ist erforderlich:

- Entwicklung einheitlicher Protokolle
- Erhöhung des Wirkungsgrad klassischer Technologien
- ergänzende Sensibilisierung der Mitarbeiter
- Sicherstellung der Integrität, Vertraulichkeit und Authentizität

Durch die Entwicklung einheitlicher Protokolle zwecks Interoperabilität und dem zunehmenden Einsatz vom Standard-IT ist die potentielle Wirkung eines Exploits größer, da eine größere Anzahl von Benutzer betroffen sind. Ein Exploit ist ein Softwarecode, welcher eine Schwachstelle gezielt ausnutzt um die Verwundbarkeit aufzuzeigen. Mittels Exploits kann festgestellt werden, ob die vorhandene Schwachstelle auch tatsächlich genutzt werden kann. Auch ist der Exploit mit weniger Aufwand zur erstellen, da die benötigten Informationen vorhanden oder einfach zu erlangen sind bzw. Erkenntnisse ohne Probleme von einem System auf das andere übertragen lassen. Damit fällt auch das ebenfalls als sicher geglaubte Prinzip „security by obscurity“. [Byres & Lowe, 2004, S. 213ff.]

Da die Kommunikation auf semantisch höherer Ebene bzw. durch einen höheren Aggregationsgrad gekennzeichnet ist, wird die Erweiterung klassischer Verfahren notwendig: beispielsweise semantische Plausibiltätschecks von Steuerungsinformationen in Firewalls der Gateways zwischen Netzwerksegmenten anstelle einfacher headerorientierter Packetfilterung und dies alles unter Berücksichtigung der Echtzeitanforderungen. Komponenten die Sicherheitsmaßnahmen technisch umsetzen (Firewall, Verschlüsselung, etc.) implementieren algorithmisch aufwendigere Verfahren und

stellen im Vergleich zur herkömmlichen Technik einen höheren Kostenfaktor dar. Lösungsanbieter müssen unter Ausnutzung der Fähigkeiten von CPS die Markttauglichkeit solcher Produkte sicherstellen.

Auch in Zukunft wird der Mensch in einem Produktionssystem als Akteur eine zentrale Rolle spielen. Im Hinblick auf IT-Security bleibt damit Social Engineering ein wesentliches Thema und entsprechende Maßnahmen ein wichtiges Instrument zur Realisierung von sicheren Systemen. Die Sensibilisierungsmaßnahmen müssen auch vermitteln, dass der Mitarbeiter sich nicht ausschließlich auf die Intelligenz des Systems hinsichtlich Security verlässt, sondern sich selbst weiterhin als sicherheitsverantwortlichen Akteur begreift.

Dieses allgemeine Ziel gilt nicht nur weiterhin, sondern gewinnt im Industrie 4.0 Kontext besondere Bedeutung. Da die Komponenten der Anlage intern Daten austauschen als auch die unternehmensübergreifende Kommunikation stattfindet ist die effektive Implementierung entsprechender Maßnahmen und damit die Schaffung von Vertrauen in die Informationen eines der wichtigsten Zielstellungen für die Zukunft von Industrie 4.0. (Kagermann, Wahlster & Hebig, 2013, S. 45 , 50).

### *4.2 Neue Konzepte*

Als Teil der Lösungsstrategie, IT-Sicherheit in Industrie 4.0 adäquat zu integrieren, bedarf es auch neuer Konzepte. Systematisch betrachtet ergeben sich unterschiedliche Aufgabenfelder:

- Integration von Sicherheitsmaßnahmen bereits bei der Standardisierung von Industrie 4.0 Komponenten
- Berücksichtigung bei der Planung und Entwurf der Produktionsanlage (Security per Design)
- Bereitstellung Vorgehensmodellen zum Übergang bestehender Anlagen vom Ist zu Industrie 4.0

- Angepasste Tools für die Wartung und Pflege der komplexen Software- und Steuerungssysteme der Smart Factory

Entsprechende Mechanismen zur Realisierung von Sicherheit sind vorzusehen und praxistauglich zu gestalten. Gerade hier sind die Standardisierungsgremien gefragt, IT-Sicherheit nicht als lästiges Begleitthema im Sinne eines zusätzlichen und vermeidbaren Add-Ons zu behandeln, sondern als von Grund auf als wichtiges Thema zu etablieren.

Sicherheit im Nachhinein zu implementieren bedeutet häufig erhöhten Aufwand und kann auf Grund der technischen Komplexität zu schwer beherrschbaren Seiteneffekten führen. Allerdings ist dieser Punkt kritisch zu betrachten. Gerade kleine und mittelständische Unternehmen (KMU) werden in den seltensten Fällen komplette Anlagen und Prozesse umstellen. Umso wichtiger sind Werkzeuge, welche die prozessspezifische Adaption von Industrie 4.0 Lösungen aufwandsarm gestalten und deren ganzheitliche Analyse hinsichtlich Wirtschaftlichkeit gestatten. Mit resultierenden Nutzenargumentationen können zielgerichtet Inventionen vorbereitet und Fehlschläge vermieden werden.

Im Hinblick auf die langen Innovationszyklen von Industrieanlagen und den hohen Investitionsbedarfs einer ganzheitlichen Umstellung wird die vollständige Adaption von Industrie 4.0 Konzepten einen längeren Prozess darstellen. Zur erfolgreichen Gestaltung dieser Übergangsphase der Heterogenität (klassische Komponenten neben Industrie 4.0 Elementen) sind langfristige Lösungen und Migrationskonzepte gefragt, welche die Transformation systematisch und zielführend gestalten.

Die Wartungs- und Pflegetools müssen entsprechende Richtlinien einhalten und während des gesamten Einsatzes beherrschbar bleiben. Sie müssen in ihrer Methodik und ihren Funktionen unterschiedlichen Nutzergruppen (IT-Abteilung, Automatisierungstechniker) im operativen Betrieb in Fragen der Sicherheit assistieren und eine ganzheitliche Perspektive hinsichtlich vertikaler und horizontaler Integration der Systeme bieten.

### *4.3 Fallstudie*

Untersuchungen im Labor des Lehrstuhls für Wirtschaftsinformatik der Universität Potsdam zeigen den konkreten Handlungsbedarf. Als Anwendungszentrum Industrie 4.0 Potsdam (AZI 4.0) stellt das Labor reale Komponenten (z. B. SPS, Robotersteuerungen, CPS mit unterschiedlichen Graden an Intelligenz, etc.) und eine Softwareumgebung zur Verfügung. Es erlaubt die prozessspezifische Adaption von Industrie 4.0 Lösungen und die Simulation von Fabrikanlagen. (vgl. www.industrie40-live.de). Mit Hilfe von Szenarien können mit der Simulationsumgebung des AZI 4.0 Bedrohungen und mögliche Gegenmaßnahmen praxisnah ermittelt und überprüft werden.

Die Abbildung einer typische Fabrikanlage bzw. Fertigungsprozesses, basierend auf bereits umgesetzten Szenarios diverser Projekte in der Simulationsumgebung, stellt die Grundlage für die Simulation und Untersuchung verschiedener Testcases dar. Angriffe auf die vorhandenen Industriekomponenten der Anlage im Rahmen von Penetration Tests bilden die Testcases. Durch systematisches Vorgehen und Zugriff auf das Fabrik-LAN war die Manipulation der Anlage innerhalb kurzer Zeit möglich. Gemäß der Simulationsmethodik (vgl. Lass & Gronau, 2012; Gronau, Theuer & Lass 2012) wurden folgende Testcases aufgestellt:

- Ausspähung der Infrastruktur
- bekannte Schwachstellen nutzen
- reguläre Operation von Systemelementen verhindern
- Manipulation des Cyber Physical Production System

Mit Hilfe des Werkzeugs Nessus erfolgte eine erste Untersuchung des Netzwerkes. Nessus ist ein Netzwerk- und Vulnerability Scanner. Zahlreiche Netzwerkkomponenten antworten beim Netzwerkscan mittels einen für sie typischen Fingerprint. Dieser kann genutzt werden um das eingesetzte Betriebssystem, sowie auch die Art des Gerätes zu bestimmen. So war es möglich die anzugreifenden Komponenten BDE-Terminal, Robotersteuerung

und SPS schnell ausfindig zu machen und anlagenspezifische Informationen zu beschaffen.

Nach Kenntnis der konkreten Netzwerkinfrastuktur sowie Art und Typ der eingesetzten Geräte, konnten spezifische Schwachstellen mit Hilfe von Metasploit identifiziert werden. Metasploit ist ein komfortables webbasiertes Tool mit Zugriff auf eine Datenbank möglicher Schwachstellen. Vor einigen Jahren war noch ein hohes Maß an Fachwissen notwendig um solche Untersuchungen durchzuführen. Durch eine immer einfacher werdende Bedienung von Analyse- und Angriffswerkzeuge, wächst auch der Kreis der Anwender, die es missbräuchlich einsetzen. Metasploit ermöglicht unter anderen das einfache Entwickeln und Ausführen von Exploits.

Eine Lücke im IP-Stack des BDE-Terminals ermöglichte den Neustart des Gerätes ohne Vorwarnung. Da dieser Angriff beliebig oft funktionierte, war es möglich, das Terminal durch ständigen Neustart zu blockieren. Danach wurde die Steuerung des Roboters attackiert. Diese ist zur Konfigurationszwecken in das Produktionsnetzwerk eingebunden. Über einen offenen Port, welcher sich bei der Verbindung mittels Telnet als Debugschnittstelle herausstellte, konnte nach kurzer Zeit der Roboter in einen undefinierten Zustand versetzt werden. So schalteten die Safety-Maßnahmen den Roboter in den Störungsmodus. Das Gerät war nicht mehr verfügbar, die Funktionsfähigkeit musste durch manuellen Eingriff wiederhergestellt werden. Mit entsprechenden Information (z. B. durch intensives Studium von Handbüchern, Datenblättern, etc.; verfügbar im Internet) ist das zielgerichtete und unbemerkte Manipulieren des Roboterprogramms ohne weiteres möglich, wenn auch mit hohem Aufwand verbunden. Eine besondere Bedrohung liegt in der subtile Veränderungen von Parametern, die durch langfristiges Wirken nur schwer nachvollziehbare Störungen oder Qualitätsprobleme hervorrufen (Falliere, Murchu, Chien, 2011, S. 3f).

Nach den Angriffen auf die klassischen Komponenten standen die eingesetzten CPS im Mittelpunkt der Betrachtung. Nach Analyse des

aufgezeichneten Datenverkehrs und mittels Replay-Attacke konnten die übertragen Daten beeinflusst werden. Bei einer Replay-Attacke werden valide Datenpakete modifiziert und in das Netzwerk eingeschleust. Das Empfängersystem geht von einer normalen Kommunikation aus und interpretiert die Daten regulär. Im konkreten Fall ist es gelungen, Mengenmeldungen eines CPS-Werkstückträgers zu modifizieren. Resultat war die Erhöhung der Schlechtmenge eines Arbeitsganges, deren Ursache in den Kontrollsystemen nicht nachvollziehbar war und die effizienten Planungsaktivitäten verhinderte.

Es folgte der systematische Versuch, die Autonomie des CPS für Manipulationen auszunutzen und die möglicherweise implementierten Plausibilitätschecks zu umgehen. Nach Auswertung der Kommunikation mit der koordinierenden SPS des Transportsystems, konnten Antworten von Seiten der Steuerung imitiert werden. Als Szenario wurden Teile des Transportsystems als belegt markiert und die autonome Wegplanung erzeugte einen Mehraufwand durch Umwege zu den Bearbeitungsstation.

Die Testfälle zeigen, dass die Kommunikation nicht ausreichend hinsichtlich der Schutzziele Integrität, Authentizität und Verfügbarkeit abgesichert sind und klassische Angriffsmethoden auch im Industrie 4.0 Kontext effektiv anwendbar sind. Da ein CPS Informationen über sich für andere Systeme bereitstellt, müssen diese Daten valide sein. Im Labor konnte gezeigt werden, dass wenn Daten zum Zustand des Werkstücks verändert werden, erhebliche Folgen daraus resultieren.

## 5 Zusammenfassung und Ausblick

Die Implementierung der unter Industrie 4.0 subsumierten Konzepte und Technologien bedeutet beträchtliche Veränderungen in der Anwendungslandschaft produzierender Unternehmen. Durch diese vierte industrielle Revolution ergeben sich neue Herausforderungen hinsichtlich IT-Sicherheit und deren systematischen Umsetzung.

Weder die Maßnahmen und Best-Practice-Methoden aus der klassischen IT-Welt noch die besonderen Gegebenheiten aus der Automatiserungsdomäne

bieten ausreichend Effektivität für die Anlagen der neuen Generation Industrie 4.0. IT-Sicherheit umzusetzen. Bewährte Konzepte (wie BSI-Grundschutz sind nicht ohne weiteres auf den Anwendungsbereich Fabrik anzuwenden. Spezifika des Automatisierungsbereichs, die bisher durchaus als Sicherheitsmechanismen wirkten, verlieren durch Umsetzung des Industrie 4.0 Paradigmas ihre Effektivität.

Die Untersuchungen im Labor des Anwendungszentrum Industrie 4.0 zeigen den dringlichen Handlungsbedarf bzgl. des Thema IT-Sicherheit und dessen Relevanz für Industrie 4.0. Adäquate Sicherheitskonzepte müssen die Komponenten von Produktionsanlagen und Automationssystemen stärker einzubeziehen, um Schaden zu vermeiden.

Die angesprochen Themenfelder liefern eine grundsätzliche Richtung für des Vorgehen und setzen die Schwerpunkte, die für weitere Arbeiten des Anwendungszentrum Industrie 4.0 die aktuelle Arbeitspakete definieren.

## Literatur

*Barthelmey, A. et al. (2014). Cyber Physical Systems for Life Cycle Continuous Technical Documentation of Manufacturing Facilities. Procedia CIRP, 17, 207-211.*

*Brettelet, M. al. (2014). How Virtualization, Decentralization and Network Building Change the Manufacturing Landscape: An Industry 4.0 Perspective. In: International Journal of Science, Engineering and Technology 8 (1), 37-44.*

*Bundesamt für Informationssicherheit (2014) IT-Grundschutzkataloge: Glossar und Begriffsdefinitionen, Stand: 13. EL Stand 2009*

*Bundesamt für Sicherheit in der Informationstechnik (2008). IT-Grundschutz-Vorgehensweise, BSI-Standard 100-2, Version 2.0.*

*Bundesamt für Sicherheit in der Informationstechnik (2013). ICS-Security-Kompendium.*

*Bundesamt für Sicherheit in der Informationstechnik (2014). Industrial Control System Security -Top 10 Bedrohungen und Gegenmaßnahmen.*

*Byres, E. (2013). The air gap: SCADA's enduring security myth. In: Communications of the ACM, 56(8), 29-31.*

*Byres, E. / Lowe, J. (2004). The myths and facts behind cyber security risks for industrial control systems. In Proceedings of the VDE Kongress (Vol. 116). Berlin, 213-218.*

*Cialdini, R. B. (2001). The Science of Persuasion. Scientific American, 284(2), 76-81.*

*Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, 2012. Parts 1-3, http://www.commoncriteriaportal.org/cc/.*

*DsiN-Sicherheitsmonitor Mittelstand - IT-Sicherheitslage 2014 in Deutschland, Deutschland sicher im Netz e.V ,2014.*

*Falliere, N. / Murchu, L. O. / Chien, E. (2011). W32. stuxnet dossier. White paper, Symantec Corp., Security Response.*

*Gronau, N. / Theuer, H. / Lass, S. (2012). Evaluation of Production Processes using Hybrid Simulation. In: Proceeding of the 1st International Conference Robust Manufacturing Control (RoMaC 2012).*

*Günthner, W. A. / Chisu, R. / Kuzmany, F. (2010). Die Vision vom Internet der Dinge (pp. 43-46). Springer Berlin Heidelberg.*

*Helmus, F. P. (2003). Anlagenplanung: Von Der Anfrage Bis Zur Abnahme, Wiley-VCH Verlag, 19.*

*ISO copyright office (Hrsg.) (2005). ISO/IEC 27001:2005. Information technology – Security techniques – Information security management systems – Requirements.*

*Kagermann, H. / Wahlster, W. / Helbig, J. (2013). Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0 – Abschlussbericht des Arbeitskreises Industrie 4.0. Forschungsunion im Stifterverband für die Deutsche Wissenschaft.*

*Kuipers, D. / Fabro, M. (2006). Control Systems Cyber Security: Defense in Depth Strategies. Idaho: Idaho National Laboratory.*

*Langmann, R. (2004). Taschenbuch der Automatisierung. Leipzig: Hanser Verlag.*

*Lass, S. / Fuhr, D. (2014). IT-Sicherheit in der Fabrik. In: Productivity Management 19 (3), 13-16.*

*Lass, S. / Gronau, N. (2012) Efficient Analysis of Production Processes with a Hybrid Simulation Environment. In: Proceeding of the 22nd International Conference of Flexible Automation and Intelligent Manufacturing (FAIM 2012), Helsinki, Finnland.*

*Lass, S. / Hennig, G. (2012). Smarte Sensoren in der Produktion: Mit intelligenten Systemen einen hohen Automatisierungsgrad realisieren, In: Productivity Management 17 (2), 16-19.*

*Mitnick, K. D. / Simon, W. L. (2006). Die Kunst der Täuschung: Risikofaktor Mensch. Hüthig Jehle Rehm.*

*National Institute of Standards and Technology (2010). Special Publication 800-53, Recommended Security Controls for Federal Information Systems and Organizations, Revision 3, August 2009, mit Updates von 2010.*

*Scheer, A. W. (2013). Industrie 4.0: Wie sehen Produktionsprozesse im Jahr 2020 aus?. IMC AG.*

*Spath, D. et al. (2013). Produktionsarbeit der Zukunft - Industrie 4.0. Fraunhofer Verlag.*

*Veigt, M. et al. (2013) Entwicklung eines Cyber-Physischen Logistiksystems. In: Industrie Management 29(1), 15-18.*