



hochschule mannheim

**Sicherheitsanalyse der  
Netzwerkkommunikation in Industrie 4.0  
Umgebungen und Erweiterung einer  
prototypischen Industrie 4.0 Security  
Testumgebung um Funktionalitäten im  
Bereich der Netzwerksicherheit**

Philipp Minges

Bachelor-Thesis

zur Erlangung des akademischen Grades Bachelor of Science (B.Sc.)

Studiengang Informatik

Fakultät für Informatik

Hochschule Mannheim

15.07.2018

Betreuer

Prof. Sachar Paulus, Hochschule Mannheim

TODO - Zweitkorrektor

**Minges, Philipp:**

Sicherheitsanalyse der Netzwerkkommunikation in Industrie 4.0 Umgebungen und Erweiterung einer prototypischen Industrie 4.0 Security Testumgebung um Funktionalitäten im Bereich der Netzwerksicherheit / Philipp Minges. –

Bachelor-Thesis, Mannheim: Hochschule Mannheim, 2018. 17 Seiten.

**Minges, Philipp:**

TODO - Title EN / Philipp Minges. –

Bachelor Thesis, Mannheim: University of Applied Sciences Mannheim, 2018. 17 pages.

## **Erklärung**

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe.

Ich bin damit einverstanden, dass meine Arbeit veröffentlicht wird, d. h. dass die Arbeit elektronisch gespeichert, in andere Formate konvertiert, auf den Servern der Hochschule Mannheim öffentlich zugänglich gemacht und über das Internet verbreitet werden darf.

Mannheim, 15.07.2018

Philipp Minges



# Abstract

## ***Sicherheitsanalyse der Netzwerkkommunikation in Industrie 4.0 Umgebungen und Erweiterung einer prototypischen Industrie 4.0 Security Testumgebung um Funktionalitäten im Bereich der Netzwerksicherheit***

Nach der Einführung des Begriffs „Industrie 4.0“ im Jahr 2011 und dem gleichzeitigen Start der 4. industriellen Revolution werden Kommunikationsnetze in der Industrie immer mehr zur Automatisierung der Produktion von Gütern oder zum unternehmensinternen sowie -externen Datenaustausch genutzt. Um diese Echtzeitkommunikation oder auch Möglichkeiten der Fernwartung zu gewährleisten, werden immer mehr Anlagen mit Netzwerkzugängen ausgestattet. Die Kommunikation der Industrie 4.0 Netze und Systeme findet unternehmensübergreifend über einen unsicheren Kanal statt und kann somit ohne bereitgestellte Sicherheitsmaßnahmen genauso angegriffen werden, wie herkömmliche Heim- oder Büronetzwerke. Das Ziel dieser Arbeit ist es zum einen, die Netzwerkkommunikation zwischen Industrie 4.0 Komponenten anhand aktueller Standards zu analysieren, mögliche Angriffsvektoren darzustellen und deren Eintrittswahrscheinlichkeit sowie Schaden zu bewerten. Zum anderen wird ein vorhandenes Industrie 4.0 Security Testsystem anhand der gewonnenen Erkenntnisse im Bereich der Netzwerksicherheit zu Lehr- und Testzwecken prototypisch erweitert.

***TODO - Title EN***

TODO - Abstract EN



# Inhaltsverzeichnis

<b>1</b>	<b>Einleitung</b>	<b>1</b>
<b>2</b>	<b>Grundlagen</b>	<b>3</b>
2.1	Historie . . . . .	3
2.1.1	1. industrielle Revolution . . . . .	3
2.1.2	2. industrielle Revolution . . . . .	3
2.1.3	3. industrielle Revolution . . . . .	4
2.1.4	4. industrielle Revolution . . . . .	6
2.2	aktueller Stand der Technik . . . . .	7
2.3	Industrie 4.0 . . . . .	8
2.3.1	Automatisierungspyramide . . . . .	10
2.3.2	Referenzarchitekturmodell Industrie 4.0 (RAMI4.0) . . . . .	11
2.4	Grundprinzipien der sicheren Kommunikation . . . . .	11
2.4.1	Vertraulichkeit/Zugriffsschutz . . . . .	11
2.4.2	(Daten-)Integrität/Änderungsschutz . . . . .	11
2.4.3	Authentizität/Fälschungsschutz . . . . .	11
2.4.4	Verbindlichkeit/Nichtabstreitbarkeit . . . . .	11
2.4.5	Anonymität . . . . .	11
2.5	sichere Kommunikation in Industrie 4.0 . . . . .	11
2.5.1	M2M-Kommunikation . . . . .	12
2.5.2	Anforderungen . . . . .	12
2.5.3	Komponenten einer I4.0 Architektur . . . . .	12
2.5.4	Kommunikationsstrukturen . . . . .	12
<b>3</b>	<b>Analyse</b>	<b>13</b>
3.1	Integrationsansätze - Industrie 4.0 . . . . .	13
3.1.1	Konsolidierung der Netzwerkkommunikation . . . . .	13
3.1.2	TODO - Gateways zum Übersetzen der Kommunikation . . . . .	13
3.2	Protokollstandards . . . . .	15
3.2.1	OPC UA . . . . .	15
3.2.2	MConnect . . . . .	15
3.2.3	TODO . . . . .	15
3.3	Sicherheitsanforderungen des Kommunikationsstacks . . . . .	15
3.3.1	Physical Layer . . . . .	15

3.3.2	Data Link Layer . . . . .	15
3.3.3	Network Layer . . . . .	15
3.3.4	Transport Layer und End2End Security . . . . .	15
3.3.5	Prozess- und Businesslogik - Application Layer . . . . .	15
3.4	Probleme bei Migration alter Systeme . . . . .	15
3.4.1	Inkompatibilität . . . . .	15
3.4.2	spezielle bzw. proprietäre Protokolle . . . . .	15
3.4.3	besondere Anforderungen der Shop-Floor-Ebene . . . . .	15
3.5	Angriffsvektoren . . . . .	15
3.5.1	Verschlüsselung . . . . .	15
3.5.2	Paketversand . . . . .	15
3.5.3	TODO . . . . .	15
3.6	Auswertung der Ergebnisse . . . . .	15
3.7	Maßnahmenkatalog . . . . .	15
<b>4</b>	<b>Implementierung</b>	<b>17</b>
	<b>Abkürzungsverzeichnis</b>	<b>vii</b>
	<b>Tabellenverzeichnis</b>	<b>ix</b>
	<b>Abbildungsverzeichnis</b>	<b>xi</b>
	<b>Quellcodeverzeichnis</b>	<b>xiii</b>
	<b>Literatur</b>	<b>xv</b>



# Kapitel 1

## Einleitung

Mit der heutigen, immer weiter fortschreitenden Vernetzung von Geräten aus Unternehmensinfrastrukturen und Heimnetzen über das Internet, erfährt die Industrie und deren Wertschöpfung einen strukturellen Wandel. Im Gegensatz zur Industrie 3.0, in der die Kommunikation der Geräte nur innerhalb einer Produktionsstätte oder eines Unternehmens stattgefunden hat, erstreckt sich die Kommunikation in Industrie 4.0 Umgebungen über die Unternehmensgrenzen hinweg. Es werden Konzepte zur Einbindung aller Komponenten eines Firmenprozesses, welcher z. B. Produktion, Service- Instandhaltungsaufgaben beinhaltet, realisiert. Diese Systeme kommunizieren miteinander und nutzen dafür immer häufiger eine Ethernet Netzwerkwerkstruktur. Dies setzt die Produktionsanlagen sowie die genutzten Softwaresysteme den gleichen potentiellen Gefahren durch Viren, Würmer oder Trojaner aus, wie reguläre Büro- oder Heim-PC.

Viele Kritische Infrastrukturen (KRITIS), wie Produktionsanlagen zur Energie- und Wasserversorgung nutzen automatisierte Prozesssteuerungssysteme, Industrie PC (IPC), speicherprogrammierbare Steuerungen (SPS) und Supervisory Control and Data Acquisition (SCADA) Systeme zur Steuerung der Abläufe in den Produktionsanlagen zwischen verteilten Systemen. Die ständige Verfügbarkeit und Überwachung dieser Dienste ist für eine funktionierende Infrastruktur essentiell. Systeme der KRITIS können nicht angehalten werden, um Sicherheitsupdates und einen anschließenden Systemneustart durchzuführen. Bei vielen dieser Prozesssteuerungssystemen wurde der Aspekt der IT-Sicherheit nicht berücksichtigt, da eine Vernetzung der Systeme im heutigen Ausmaß nicht vorgesehen war. Die Systeme bieten keine Möglichkeit der Verschlüsselung des Datenverkehrs oder der Authentifizierung der Benutzer.

Die Sicherheit der Produktionsanlagen und deren Netzwerkkommunikation spielt für ein Unternehmen im Industrie 4.0 Umfeld mit Hinblick auf Verfügbarkeit, Zuverlässigkeit und Authentizität eine essentielle Rolle. Sollte es durch Angriffe möglich sein, die Produktion zu sabotieren oder Anlagen und Systeme zu manipulieren, so können die Folgen schwerwiegend sein. Es kann zu Produktionsausfällen kommen und es können Vertragsstrafen drohen. Ein bekannter Angriff wurde im Jahr 2016 auf das Netz des deutschen Bundestages durchgeführt. Dort wurde ein Zusammenbruch der getroffenen Sicherheitsmaßnahmen erreicht. Es wurden über mehrere Monate unbemerkt sensible Daten entwendet. [TODO - Quelle]

TODO - Stuxnet, Duqu -> auf Produktionsanlagen zugegriffen

Die beschriebenen Probleme bei der Umsetzung einer sicheren Kommunikation im Industrie 4.0 Umfeld sowie die dargestellten, erfolgreich durchgeführten Angriffe auf bestehende Infrastrukturen bieten mir einen Anlass, den aktuellen Stand der IT-Sicherheit beim Datenaustausch in einer heterogenen Industrie 4.0 Umgebung zu analysieren und mögliche Risiken aufzuzeigen.

Um das erwünschte Ergebnis zu erhalten, muss im ersten Schritt eine Literaturanalyse durchgeführt werden. Mit Hilfe dieser werden die Grundlagen zur Analyse der Kommunikation geschaffen.

Anschließend wird die Sicherheitsanalyse der Netzwerkkommunikation in Industrie 4.0 Umgebungen durchgeführt. Diese beinhaltet die Analyse des Kommunikationsstacks der Netzwerkebene und der verwendeten Protokolle sowie Standards.

Zuletzt werden die Ergebnisse der Analyse durch eine prototypische Implementierung und Erweiterung eines vorhandenen Industrie 4.0 Security Testsystems dargestellt und validiert.

TODO ref. W.A. Halang 2016 und Bundesministerium für Wirtschaft und Energie 2016 und Schleupner 2016 und Lass Sander 2014

## **Kapitel 2**

# **Grundlagen**

### **2.1 Historie**

Seit dem Beginn des Industriezeitalters um 1800, welches mit der Mechanisierung (Industrie 1.0) startete, befindet sich die Industrie in einem stetigen Wandel. Sie entwickelte sich um 1900 durch die Massenproduktion zur Industrie 2.0 und in den 1970er Jahren durch die Automatisierung zur Industrie 3.0. Die Einteilung der Industriezeitalter ist durch tiefgreifende Veränderungen im technologischen Fortschritt möglich, welche auch als industrielle Revolution bezeichnet werden. Aktuell befinden wir uns in der Phase der 4. industriellen Revolution.

#### **2.1.1 1. industrielle Revolution**

Die 1. industrielle Revolution fand mit der Erfindung der Dampfmaschine statt. Sie ermöglichte es Eisenbahnen und Dampfschiffe sowie verschiedene Maschinen im Kohleabbau oder in Textilfabriken anzutreiben und trug massiv zur Industrialisierung und der Entstehung der Industrie 1.0 bei. Nach und nach wurden immer mehr Produktionsanlagen errichtet und somit Arbeitsplätze in Infrastruktur, Textilfabriken, Häuserbau, Kohleabbau und anderen Bereichen geschaffen.

#### **2.1.2 2. industrielle Revolution**

Die Erforschung der Elektrizität im 19. Jahrhundert war der Auslöser der 2. industriellen Revolution. Nachdem ab 1830 die Gesetze der Elektrotechnik bekannt

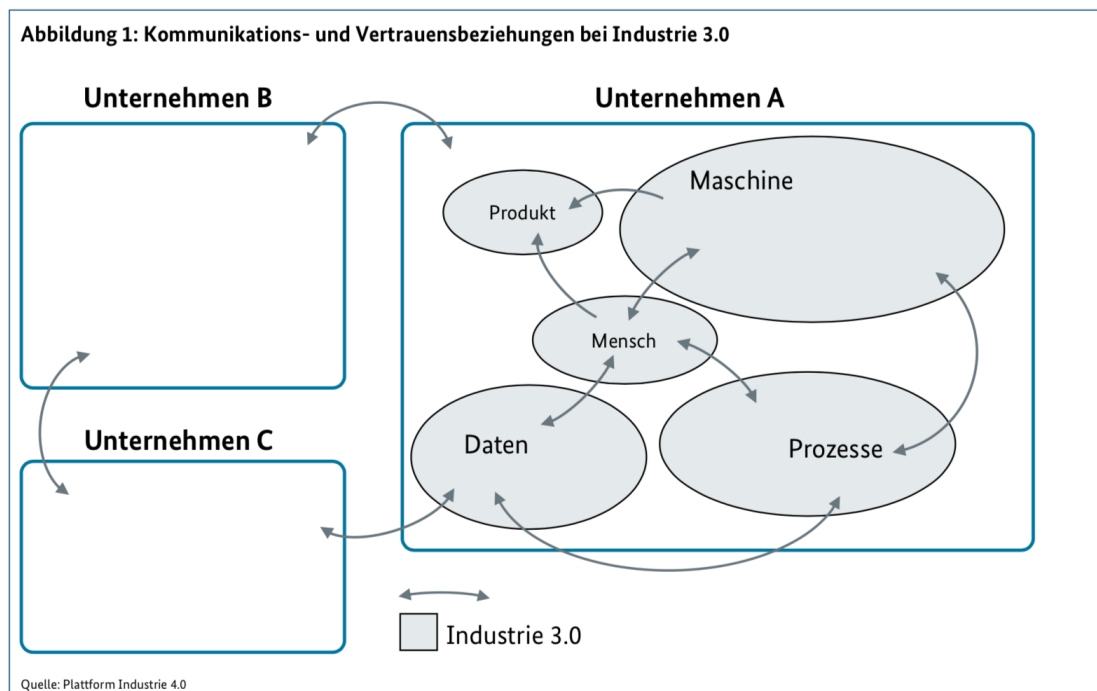
waren, fand die Elektrizität eine breite Anwendung in der Industrie und im Alltag. Im Jahr 1913 führte Henry Ford das Fließband in der Automobilbranche ein. Im Zuge dessen musste jeder Arbeiter nur noch einen Arbeitsschritt erledigen, welches einerseits die Produktion wesentlich beschleunigte und eine Massenproduktion ermöglichte und andererseits eine hohe Spezialisierung der einzelnen Arbeitskräfte für ihre bestimmte Aufgabe erforderte.

Außerdem wurde es durch die Luftfahrt möglich Produkte wie Autos, Kleidung und Lebensmittel über Kontinente hinweg immer schneller zu transportieren und zu handeln.

### **2.1.3 3. industrielle Revolution**

Die 3. industrielle Revolution fand in den 1970er Jahren statt. Sie ist durch eine sukzessive (Teil-) Automatisierung der Prozesse und durch den Einzug der IT in die Industrie- und Verbraucherwelt geprägt. In den 1940er Jahren wurden die ersten Rechenmaschinen und programmierbare Steuerungen in Unternehmen eingesetzt. In den 1970er Jahren zog der Computer auch in den Privatbereich ein, wurde zunehmend beliebter und schaffte einen neuen Industriezweig. Der Fertigungsprozess in Fabriken wurde mehr und mehr von Maschinen übernommen.

Durch den zunehmenden Einsatz von IT in Unternehmen entstand immer mehr Kommunikation zwischen Menschen und Maschinenn. Diese Kommunikation und die anfallenden Daten wurden jedoch nur unternehmensintern verarbeitet. Es gab nur wenige Schnittstellen nach außen.

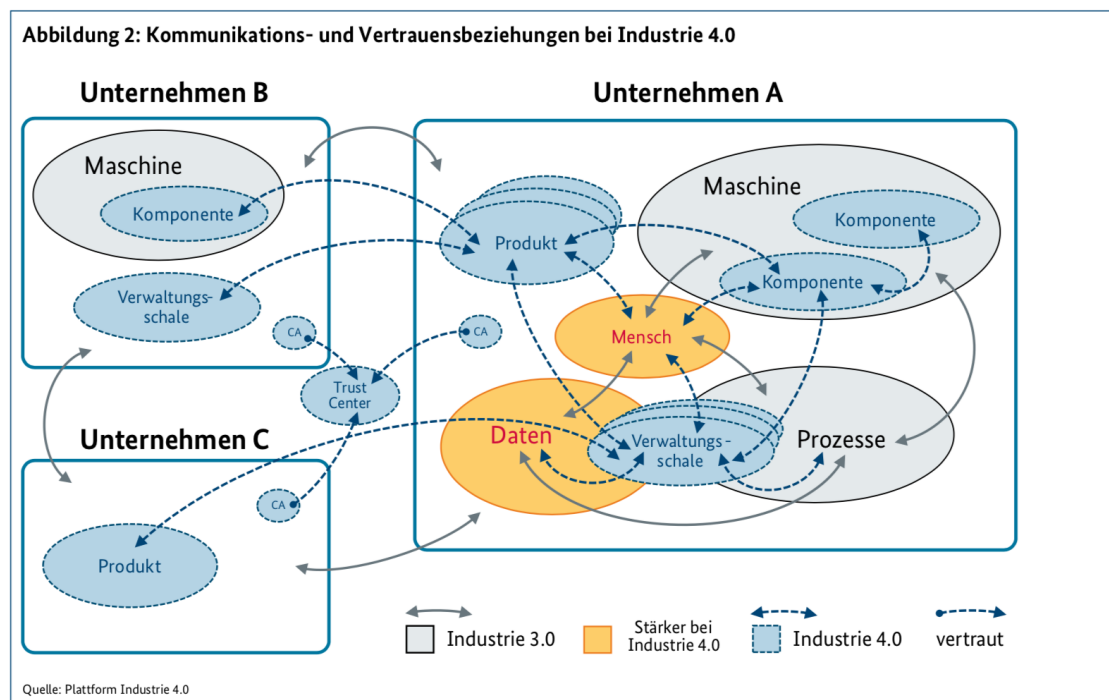


**Abbildung 2.1:** Kommunikationsbeziehungen in einer Industrie 3.0 Umgebung - TODO ref. sichere unternehmensübergreifende Kommunikation

### 2.1.4 4. industrielle Revolution

Das Ende des 20. Jahrhunderts gilt als der Beginn der 4. industriellen Revolution. Das Kennzeichen dieser Phase ist die zunehmende Digitalisierung. Mit ihr geht die technische Vernetzung physischer Gegenstände, dem Internet of Things (IOT), einher. Mehr und mehr Geräte oder Gegenstände besitzen die Möglichkeit aktiv durch Datenaustausch oder passiv z. B. mit Hilfe eines Bar- oder QR-Codes mit der digitalen Welt zu kommunizieren und somit eine fortschreitende Automatisierung sowie Individualisierung zu ermöglichen.

Im Gegensatz zur Industrie 3.0 sollen Maschinen autonom, auch über Unternehmensgrenzen hinweg, miteinander kommunizieren können um gesamte Geschäftsprozesse zu übernehmen. Dies setzt eine Öffnung der Unternehmen nach außen voraus.



**Abbildung 2.2:** Kommunikationsbeziehungen in einer Industrie 4.0 Umgebung - TODO ref. sichere Unternehmensübergreifende Kommunikation

Diese Entwicklung erzeugt durch die ständige Kommunikation eine enorme Menge an Daten, welche den Anforderungen der IT-Sicherheit gerecht werden müssen, um Verbraucher und Unternehmen zu schützen.

### **2.2 aktueller Stand der Technik**

Der Prozess der vierten industriellen Revolution ist ein stetiger, nicht abgeschlossener Prozess. Aktuell werden die ersten Smart Factories der Industrie errichtet und erste smarte Einkaufsmöglichkeiten, wie Amazon Go und TODO - siehe Trumpf, für den Endverbraucher geschaffen. Diese Fabriken und Filialen stellen die ersten ihrer Art dar und dienen als Prototypen. Das Ziel des Wandels in der Strukturierung und Organisation der Produktion in Unternehmen ist eine immer weitere Automatisierung der Prozessabwicklung bis hin zu autonom arbeitenden Fabriken.

TODO - Trumpf

Die Umsetzung dieser Innovationen basiert hauptsächlich auf dem Fortschritt der Informationstechnik (IT) und dem Einzug der Internet-Technologien in die Industrie. Diese Entwicklung macht es möglich immer schneller Informationen auszutauschen, größere Datenmengen zu analysieren und diese zu verarbeiten. In der Industrie entstehen dadurch u. a. die folgenden Chancen:

- Die Kommunikationsinfrastruktur wird in Zukunft in Produktionssystemen so preiswert sein, dass sie sinnvoll für Konfiguration, Service, Diagnose, Bedienung und Wartung genutzt werden kann.
- Die Produktionssysteme werden mehr und mehr mit einem Netz verbunden, erhalten dort eine digitale Identität, werden somit such- und analysierbar und besitzen die Möglichkeit Daten über sich selbst zu veröffentlichen.
- Maschinen und Anlagen speichern ihre Zustände in ihrer digitalen Identität im Netz. Diese Zustände sind aktuell, aktualisierbar und zunehmend vollständig. Sind im Netzwerk viele solcher Identitäten vorhanden, können die Daten effizient abgerufen und ausgetauscht werden.
- Softwaredienste werden über das Netz verknüpft werden und können somit automatisiert individuelle Aufgaben durch die direkte Kommunikation der Systeme erledigen. Eine solche individuelle Wertschöpfung war bisher nur unwirtschaftlich oder gar nicht möglich.

Diese Veränderungen im Wertschöpfungsprozess und die ständige Kommunikation der Systeme bereiten jedoch auch Probleme. Es entstehen große Mengen an Daten, welche u. a. über einen unsicheren Kanal verbreitet werden sollen. Des weiteren sind viele vorhandene Produktionsanlagen nicht für diese Form von vermaschter Kommunikation entwickelt worden. Diesen Problemen wird aktuell durch die Entwicklung von Industriestandards und Machine to Machine (M2M)-Protokollen, wie z. B. die Open Platform Communications Unified Architecture (OPC UA) entgegengewirkt. Um vorhandene Anlagen weiterhin nutzen zu können, werden Gateways genutzt. (TODO Trumpf ref.)

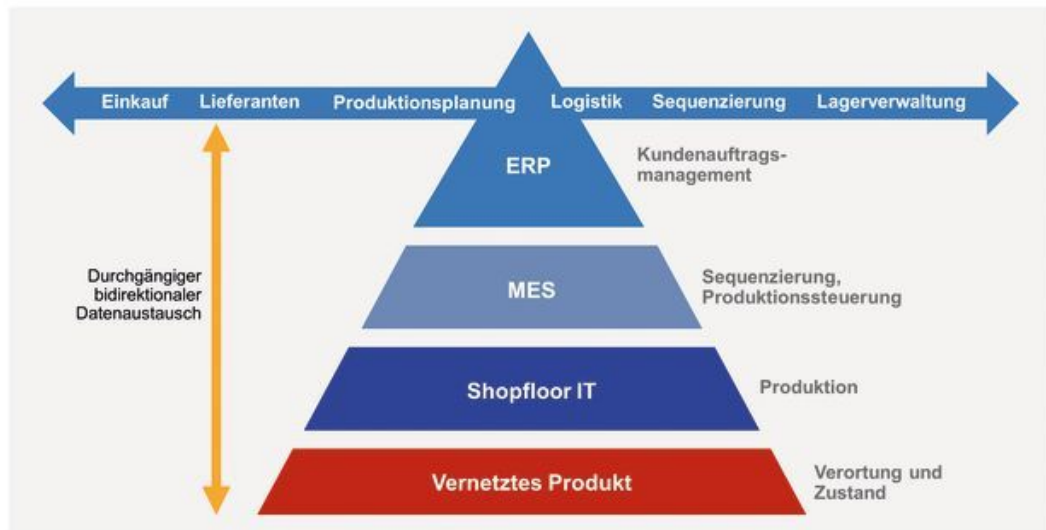
### 2.3 Industrie 4.0

Der Begriff Industrie 4.0 wurde erstmals auf der Hannover Messe 2011 verwendet (Drath 2014) und soll das Ergebnis der 4. industriellen Revolution darstellen. Der Grundgedanke hinter Industrie 4.0 ist die flächendeckende Vernetzung von Informations- und Kommunikationstechnik zu einem Internet der Dinge, Dienste und Daten (**Spath2013**). Diese Vernetzung soll einen ständigen Informationsaustausch zwischen den Komponenten ermöglichen. Jede Komponente des IOT soll als Cyber-physisches System (CPS) arbeiten. Ein CPS besitzt neben seiner realen Identität eine digitale Identität, über welche es ständig mit anderen IOT-Geräten kommunizieren kann.

Für Unternehmen bedeutet dies einen Wechsel von einer linearen Prozesskette hin zu einem vermaschten Netzwerk, in dem jede Komponente mit dem gesamten Netzwerk kommunizieren kann. Dies beinhaltet die Vernetzung der Komponenten auf horizontaler und vertikaler Ebene. Die vertikale Ebene stellt die technischen Komponenten dar und wird durch die Automatisierungspyramide beschrieben. Die horizontale Ebene beschreibt die wirtschaftlichen Geschäfts- bzw. Produktionsprozesse und besteht u. a. aus: Einkauf, Lieferanten, Produktionsplanung, Logistik, Sequenzierung und Lagerverwaltung. Das Ziel ist die Vernetzung aller Beteiligten.



### Horizontale und vertikale Integration

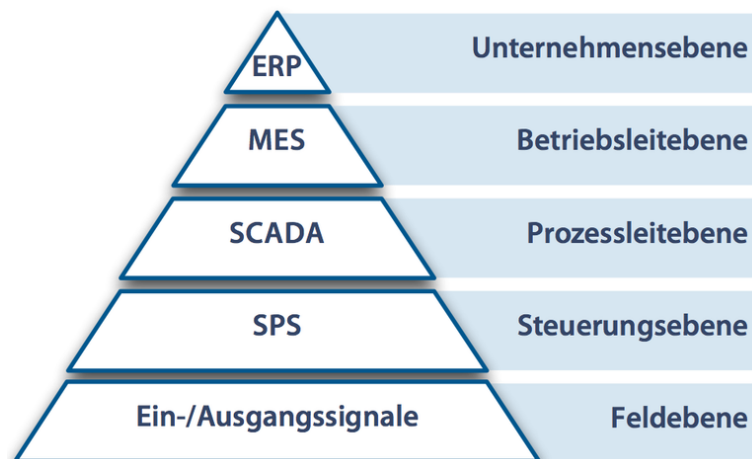


**Abbildung 2.3:** horizontale und vertikale Integration - TODO ref. HP industry-of-things siehe bookmark

Aus zeitlichen Gründen wird im Rahmen der Bachelorthesis hauptsächlich die Kommunikation der vertikalen Achse auf technischer Ebene untersucht.

### 2.3.1 Automatisierungspyramide

Die Automatisierungspyramide stellt die beteiligten Systeme und Softwarekomponenten eines automatisierten Prozesses systematisch dar. Diese beginnen, ausgehend vom Kundenauftrag und der betriebswirtschaftlichen Planung der Produktion auf der Unternehmensebene im Enterprise Resource Planning (ERP) System. Die Ergebnisse der Planung werden an das Manufacturing Execution System (MES) übergeben, welches die verschiedenen Fertigungs- oder Logistikaufträge generiert. Die Aufträge werden anschließend auf der Prozessleit- (SCADA), Steuerungs- (SPS) und Feldebene (Ein-/Ausgangssignale) bearbeitet.



**Abbildung 2.4:** Automatisierungspyramide - TODO ref. Langmann,2004

Während die oberen Schichten der Pyramide (ERP und MES) durch Standardkomponenten bzw. -software der IT realisiert werden, zählen die unteren Schichten (Prozessleit- bis Feldebene) zur Automatisierung, welche die Steuerung und Kontrolle der technischen Anlagen übernimmt. Diese werden auch als Shop-Floor-Ebene bezeichnet. Sie sind durch spezielle Hard- und Softwarelösungen umgesetzt. Die Kommunikation dieser Systeme ist u. a. für spezielle Anwendungsfälle wie harte Echtzeitreaktionszeiten mit Verzögerungen  $< 1\text{ms}$  ausgelegt. Die Integration von Sicherheitsmaßnahmen bei der Kommunikation dieser Systeme stellt oft eine große Herausforderung dar.

### **2.3.2 RAMI4.0**

TODO - notwendig? Schichtenmodell, Darstellung eines Assets. nur kurze Beschreibung? wenig Bezug zur Netzwerkkommunikation. Smart Sensors, Kommunikationsfähigkeit eines Assets (aktiv,passiv)

## **2.4 Grundprinzipien der sicheren Kommunikation**

### **2.4.1 Vertraulichkeit/Zugriffsschutz**

### **2.4.2 (Daten-)Integrität/Änderungsschutz**

### **2.4.3 Authentizität/Fälschungsschutz**

### **2.4.4 Verbindlichkeit/Nichtabstreitbarkeit**

### **2.4.5 Anonymität**

TODO - Industrie 4.0 beinhaltet durch die Unternehmensübergreifende Kommunikation außerdem den rechtlichen Rahmen, welcher bei Nichteinhaltung von Verträgen bzgl. Verfügbarkeit, Integrität und Vertraulichkeit gelten kann.

## **2.5 sichere Kommunikation in Industrie 4.0**

Im Gegensatz zur I3.0, in welcher Daten auf lokaler Ebene oder zwischen einzelnen internen Unternehmensebenen ausgetauscht wurden, stellt in der I4.0 der Austausch

von Daten und Informationen über Unternehmensgrenzen hinweg eine wesentliche Herausforderung dar. Dabei findet die Kommunikation nicht mehr über ein Enterprise-Resource-Planning-System (ERP) statt, sondern auch direkt von einer darunterliegenden Ebene, wie z. B. einer Maschine mit ihrem Lieferanten. Durch diese enge Vernetzung können sowohl Menschen, als auch Maschinen die Kommunikationspartner sein.

### **2.5.1 M2M-Kommunikation**

TODO - Maschine 2 Mensch und Maschine 2 Maschine -> M2M Protokolle

### **2.5.2 Anforderungen**

### **2.5.3 Komponenten einer I4.0 Architektur**

*Assets*

*Smarte Sensoren*

*TODO*

### **2.5.4 Kommunikationsstrukturen**

*End2End*

*Gateways*

*Publish-Subscribe*

*Kommunikation mit Netzwerk als Partner*

## **Kapitel 3**

# **Analyse**

### **3.1 Integrationsansätze - Industrie 4.0**

#### **3.1.1 Konsolidierung der Netzwerkkommunikation**

TODO - siehe Testsystem Martin - alles spricht OPC UA

#### **3.1.2 TODO - Gateways zum Übersetzen der Kommunikation**

TODO - siehe Trumpf, axoom -> Gateways übersetzen von heterogener Netzwerkkommunikation in Protokollstandard für unternehmensübergreifende bzw. externe Kommunikation. Ansatz: Softwareschwachstellen, Softwarefehler, müssen viele Herstellerprotokolle unterstützen - Probleme?



### *Security-Komponenten*

#### *Router*

#### *Gateways*

## **3.2 Protokollstandards**

### **3.2.1 OPC UA**

### **3.2.2 MConnect**

### **3.2.3 TODO**

## **3.3 Sicherheitsanforderungen des Kommunikationsstacks**

### **3.3.1 Physical Layer**

### **3.3.2 Data Link Layer**

### **3.3.3 Network Layer**

### **3.3.4 Transport Layer und End2End Security**

### **3.3.5 Prozess- und Businesslogik - Application Layer**

## **3.4 Probleme bei Migration alter Systeme**

### **3.4.1 Inkompatibilität**

### **3.4.2 spezielle bzw. proprietäre Protokolle**

### **3.4.3 besondere Anforderungen der Shop-Floor-Ebene**

## **3.5 Angriffsvektoren**

### **3.5.1 Verschlüsselung**

### **3.5.2 Paketversand**

### **3.5.3 TODO**

## **3.6 Auswertung der Ergebnisse**

## **3.7 Maßnahmenkatalog**

### *Defense in Depth Strategie - TODO (Kuipers,2006)*

TODO - Beschreibung und Einordnung der Defense in Depth Strategie

### 3 Analyse

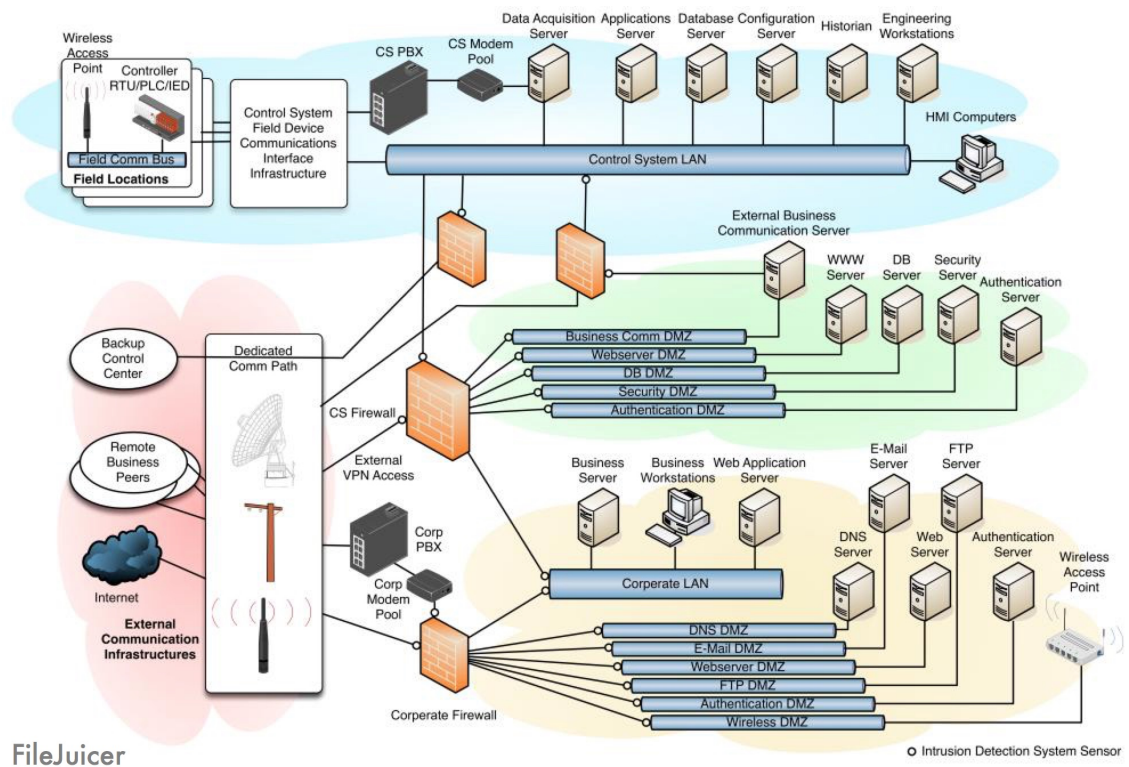


Abbildung 3.1: Defense in Depth Strategie - TODO ref. Kuipers,2006



## **Kapitel 4**

# **Implementierung**



# Abkürzungsverzeichnis

<b>KRITIS</b>	Kritische Infrastrukturen
<b>IPC</b>	Industrie PC
<b>SPS</b>	speicherprogrammierbare Steuerungen
<b>SCADA</b>	Supervisory Control and Data Acquisition
<b>ERP</b>	Enterprise Resource Planning
<b>MES</b>	Manufacturing Execution System
<b>RAMI4.0</b>	Referenzarchitekturmodell Industrie 4.0
<b>IOT</b>	Internet of Things
<b>IT</b>	Informationstechnik
<b>CPS</b>	Cyber-physisches System
<b>OPC UA</b>	Open Platform Communications Unified Architecture
<b>M2M</b>	Machine to Machine



# **Tabellenverzeichnis**



# Abbildungsverzeichnis

2.1	Kommunikationsbeziehungen in einer Industrie 3.0 Umgebung - TODO ref. sichere unternehmensübergreifende Kommunikation . .	5
2.2	Kommunikationsbeziehungen in einer Industrie 4.0 Umgebung - TODO ref. sichere Unternehmensübergreifende Kommunikation . .	6
2.3	horizontale und vertikale Integration - TODO ref. HP industry-of- things siehe bookmark . . . . .	9
2.4	Automatisierungspyramide - TODO ref. Langmann,2004 . . . . .	10
3.1	Defense in Depth Strategie - TODO ref. Kuipers,2006 . . . . .	16





# Listings



# Literatur

Bundesministerium für Wirtschaft und Energie, BMWi (2016). „Technischer Überblick: Sichere unternehmensübergreifende Kommunikation“. In:

Drath, Rainer (2014). „Industrie 4.0 - eine Einführung“. In: *openautomation.de*.

URL:

[https://www.openautomation.de/fileadmin/user\\_upload/Stories/Bilder/oa\\_2014/oa\\_3/oa\\_3\\_14\\_ABB.pdf](https://www.openautomation.de/fileadmin/user_upload/Stories/Bilder/oa_2014/oa_3/oa_3_14_ABB.pdf).

Lass Sander, Kotarski David (2014). „IT-Sicherheit als besondere Herausforderung von Industrie 4.0“. In: *Kersten W, Koller H, Lödding, H (ed) Industrie 4.0: Wie intelligente Vernetzung und kognitive Systeme unsere Arbeit verändern*.

Schleupner, Linus (2016). *Sichere Kommunikation im Umfeld von Industrie 4.0*. Springer.

W.A. Halang, H. Unger (Hrsg.) (2016). *Internet der Dinge*. Springer.

