



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. 15 Seiten.

Minges, Philipp:

TODO - Title EN / Philipp Minges. –

Bachelor Thesis, Mannheim: University of Applied Sciences Mannheim, 2018. 15 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

1	Einleitung	1
2	Grundlagen	3
2.1	Die 4. industrielle Revolution	3
2.1.1	Historie	3
2.1.2	Aktueller Stand der Technik	6
2.1.3	Referenzarchitekturmodell Industrie 4.0 (RAMI4.0)	6
2.1.4	Automatisierungspyramide	6
2.2	Grundprinzipien der sicheren Kommunikation	8
2.2.1	Vertraulichkeit/Zugriffsschutz	8
2.2.2	(Daten-)Integrität/Änderungsschutz	8
2.2.3	Authentizität/Fälschungsschutz	8
2.2.4	Verbindlichkeit/Nichtabstreitbarkeit	8
2.2.5	Anonymität	8
2.3	sichere Kommunikation in Industrie 4.0	8
2.3.1	Anforderungen	9
2.3.2	Komponenten einer I4.0 Architektur	9
2.3.3	Kommunikationsstrukturen	9
3	Analyse	11
3.1	Protokollstandards	12
3.1.1	OPC UA	12
3.1.2	MConnect	12
3.1.3	TODO	12
3.2	Sicherheitsanforderungen des Kommunikationsstacks	12
3.2.1	Physical Layer	12
3.2.2	Data Link Layer	12
3.2.3	Network Layer	12
3.2.4	Transport Layer und End2End Security	12
3.2.5	Prozess- und Businesslogik - Application Layer	12
3.3	Probleme bei Migration alter Systeme	12
3.3.1	Inkompatibilität	12
3.3.2	spezielle bzw. proprietäre Protokolle	12
3.3.3	besondere Anforderungen der Shop-Floor-Ebene	12

3.4	Angriffsvektoren	12
3.4.1	Verschlüsselung	12
3.4.2	Paketversand	12
3.4.3	TODO	12
3.5	Auswertung der Ergebnisse	12
3.6	Maßnahmenkatalog	12
4	Implementierung	15
	Abkürzungsverzeichnis	vii
	Tabellenverzeichnis	ix
	Abbildungsverzeichnis	xi
	Quellcodeverzeichnis	xiii
	Literatur	xv

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 Die 4. industrielle Revolution

Der Grundgedanke von Industrie 4.0 ist die flächendeckende Vernetzung von Informations- und Kommunikationstechnik zu einem Internet der Dinge, Dienste und Daten. (Spath, 2014 - TODO ref.)

2.1.1 Historie

TODO - Industrie 3.0 -> Industrie 4.0 - Kommunikation über Unternehmensgrenzen

TODO - Beschreibung der unternehmensinternen Kommunikation der Systeme mit Hinblick auf die Automatisierung der Industrie in der dritten Revolution.

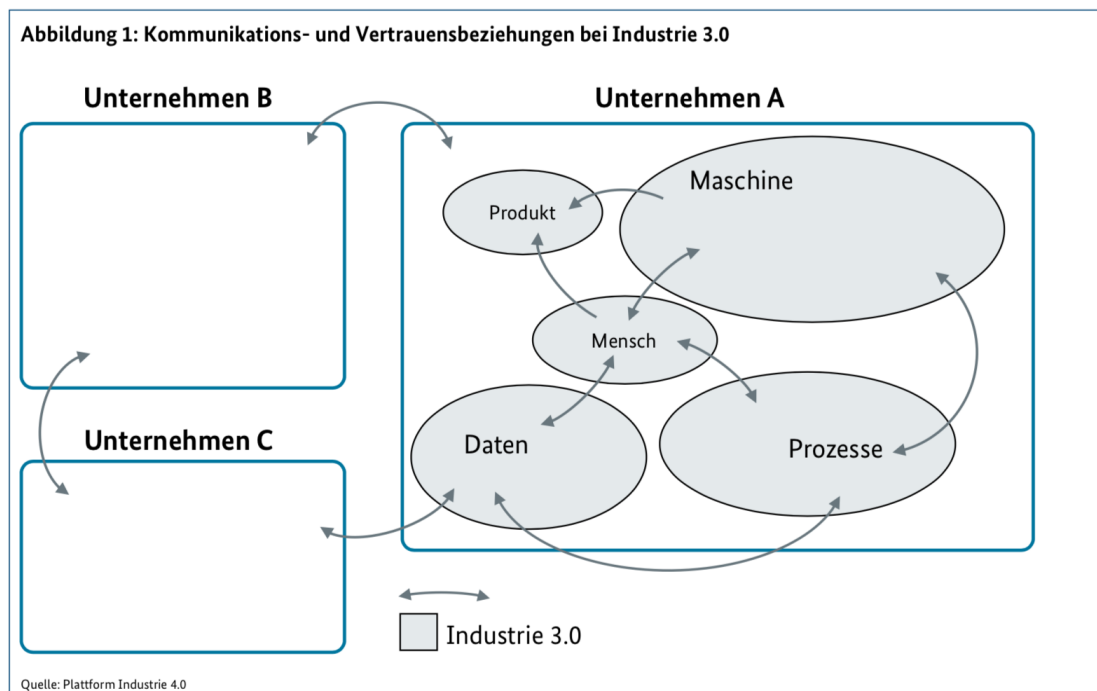


Abbildung 2.1: Kommunikationsbeziehungen in einer Industrie 3.0 Umgebung - TODO ref. sichere unternehmensübergreifende Kommunikation

TODO - Beschreibung der unternehmensübergreifenden Kommunikation in Industrie 4.0 Umgebungen.

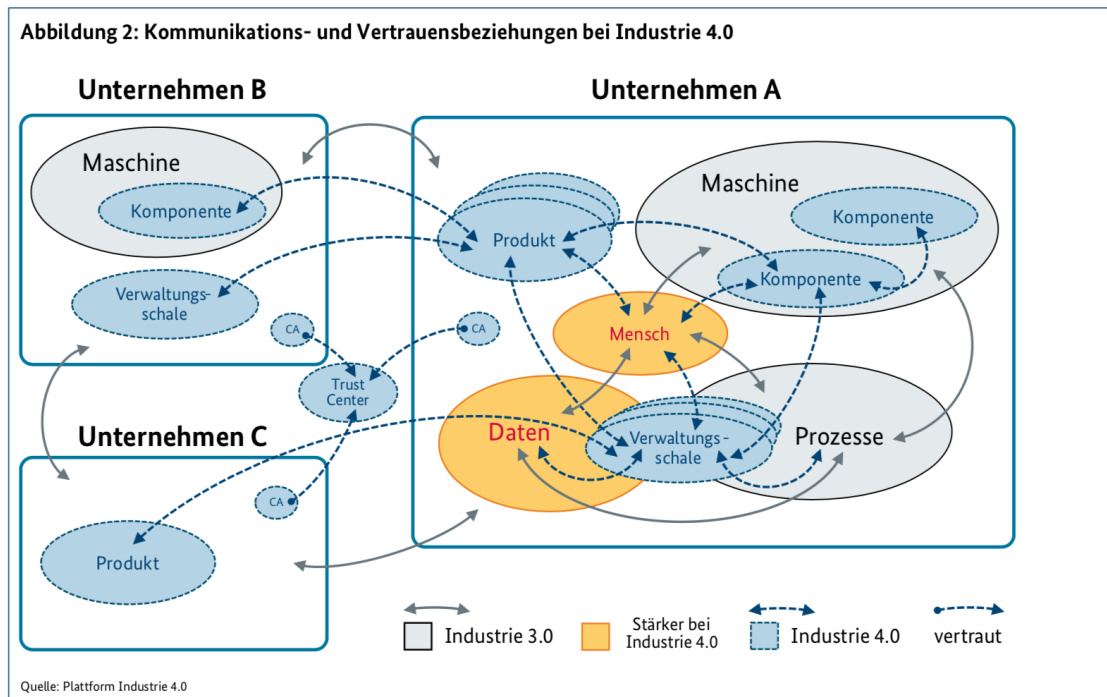


Abbildung 2.2: Kommunikationsbeziehungen in einer Industrie 4.0 Umgebung - TODO ref. sichere Unternehmenseübergreifende Kommunikation

2.1.2 Aktueller Stand der Technik

Die Entwicklung der Industrie zu ihrer vierten Revolution ist ein stetiger, nicht abgeschlossener Prozess. Aktuell werden die ersten Smart Factories der Industrie errichtet und erste smarte Einkaufsmöglichkeiten, wie Amazon Go, 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.

2.1.3 RAMI4.0

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

2.1.4 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.

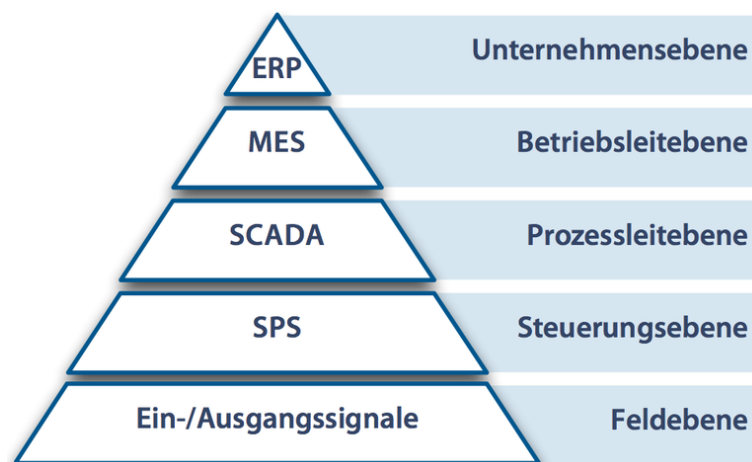


Abbildung 2.3: Automatisierungspyramide - TODO ref. Langmann,2004

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.

2.2 Grundprinzipien der sicheren Kommunikation

2.2.1 Vertraulichkeit/Zugriffsschutz

2.2.2 (Daten-)Integrität/Änderungsschutz

2.2.3 Authentizität/Fälschungsschutz

2.2.4 Verbindlichkeit/Nichtabstreitbarkeit

2.2.5 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.

2.3 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.

2.3.1 Anforderungen

2.3.2 Komponenten einer I4.0 Architektur

Assets

Smarte Sensoren

TODO

2.3.3 Kommunikationsstrukturen

End2End

Gateways

Publish-Subscribe

Kommunikation mit Netzwerk als Partner

Kapitel 3

Analyse

3.1 Protokollstandards

3.1.1 OPC UA

3.1.2 MConnect

3.1.3 TODO

3.2 Sicherheitsanforderungen des Kommunikationsstacks

3.2.1 Physical Layer

3.2.2 Data Link Layer

3.2.3 Network Layer

3.2.4 Transport Layer und End2End Security

3.2.5 Prozess- und Businesslogik - Application Layer

3.3 Probleme bei Migration alter Systeme

3.3.1 Inkompatibilität

3.3.2 spezielle bzw. proprietäre Protokolle

3.3.3 besondere Anforderungen der Shop-Floor-Ebene

3.4 Angriffsvektoren

3.4.1 Verschlüsselung

3.4.2 Paketversand

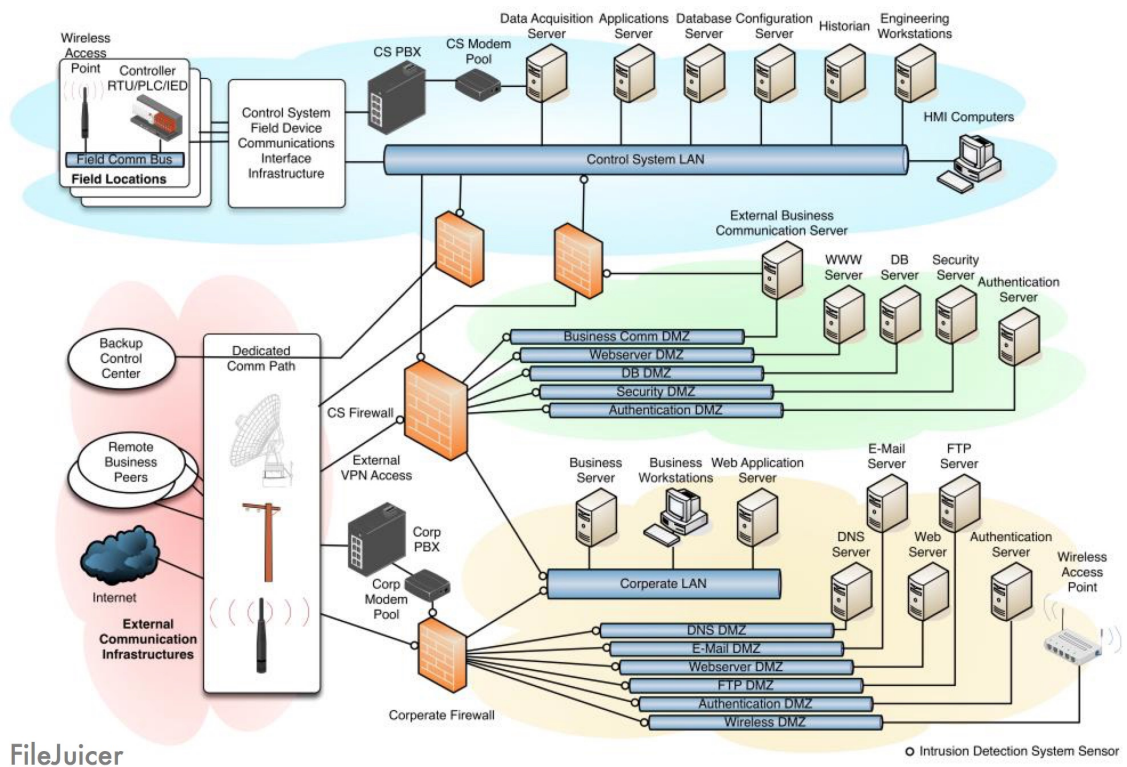
3.4.3 TODO

3.5 Auswertung der Ergebnisse

3.6 Maßnahmenkatalog

Defense in Depth Strategie - TODO (Kuipers,2006)

TODO - Beschreibung und Einordnung der Defense in Depth Strategie



FileJuicer

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

Kapitel 4

Implementierung

Abkürzungsverzeichnis

KRITIS	Kritische Infrastrukturen
IPC	Industrie PC
SPS	speicherprogrammierbare Steuerungen
SCADA	Supervisory Control and Data Acquisition
ERP	Enterprise Resource Planning
MES	Manufacturing Execution System
RAMI4.0	Referenzarchitekturmodell Industrie 4.0

Tabellenverzeichnis

Abbildungsverzeichnis

2.1	Kommunikationsbeziehungen in einer Industrie 3.0 Umgebung - TODO ref. sichere unternehmensübergreifende Kommunikation . .	4
2.2	Kommunikationsbeziehungen in einer Industrie 4.0 Umgebung - TODO ref. sichere Unternehmensübergreifende Kommunikation . .	5
2.3	Automatisierungspyramide - TODO ref. Langmann,2004	7
3.1	Defense in Depth Strategie - TODO ref. Kuipers,2006	13

Listings

Literatur

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

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.

