



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 Netzwirkommunikation 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. 13 Seiten.

**Minges, Philipp:**

TODO - Title EN / Philipp Minges. –

Bachelor Thesis, Mannheim: University of Applied Sciences Mannheim, 2018. 13 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 erweitert.

***TODO - Title EN***

TODO - Abstract EN



# Inhaltsverzeichnis

<b>1</b>	<b>HOWTO</b>	<b>1</b>
1.1	Hervorhebungen . . . . .	1
1.2	Anführungszeichen . . . . .	1
1.3	Abkürzungen . . . . .	1
1.4	Querverweise . . . . .	2
1.5	Fußnoten . . . . .	2
1.6	Fremdsprachige Begriffe . . . . .	2
1.7	Tabellen . . . . .	2
1.8	Harveyballs . . . . .	3
1.9	Aufzählungen . . . . .	3
1.10	Zitate . . . . .	4
1.10.1	Zitate im Text . . . . .	4
1.10.2	Zitierstile . . . . .	4
1.10.3	Zitieren von Internetquellen . . . . .	5
<b>2</b>	<b>Einleitung</b>	<b>7</b>
<b>3</b>	<b>Grundlagen</b>	<b>9</b>
3.1	Historie . . . . .	9
3.2	Kommunikation in Industrie 4.0 . . . . .	9
3.2.1	Anforderungen . . . . .	10
3.2.2	Komponenten einer I4.0 Architektur . . . . .	10
3.2.3	Kommunikationsstrukturen . . . . .	10
3.2.4	Schutzziele . . . . .	10
<b>4</b>	<b>Analyse</b>	<b>11</b>
4.1	Sicherheitsanforderungen des Kommunikationsstacks . . . . .	12
4.1.1	Physical Layer . . . . .	12
4.1.2	Data Link Layer . . . . .	12
4.1.3	Network Layer . . . . .	12
4.1.4	Transport Layer und End2End Security . . . . .	12
4.1.5	Prozess- und Businesslogik - Application Layer . . . . .	12
4.2	Protokollstandards . . . . .	12
4.2.1	OPC UA . . . . .	12

4.2.2	MConnect . . . . .	12
4.2.3	... . . . .	12
4.3	Angriffsvektoren . . . . .	12
4.3.1	Verschlüsselung . . . . .	12
4.3.2	Paketversand . . . . .	12
4.4	Auswertung der Ergebnisse . . . . .	12
4.5	Maßnahmenkatalog . . . . .	12
<b>5</b>	<b>Implementierung</b>	<b>13</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>
	<b>Index</b>	<b>xvii</b>



# Kapitel 1

## HOWTO

### 1.1 Hervorhebungen

Achten Sie bitte auf die grundlegenden Regeln der Typographie<sup>1</sup>, wenn Sie Ihren Text schreiben. Hierzu gehören z. B. die Verwendung der richtigen „Anführungszeichen“ und der Unterschied zwischen Binde- (-), Gedankenstrich (–) und langem Strich (—). Wenn Sie Text hervorheben wollen, dann setzen Sie ihn *kursiv* (Italic) und nicht **fett** (Bold). Fettdruck ist Überschriften vorbehalten; im Fließtext stört er den Lesefluss. Das Unterstreichen von Fließtext ist im gesamten Dokument tabu und kann maximal bei Pseudo-Code vorkommen.

### 1.2 Anführungszeichen

Deutsche Anführungszeichen gehen so: „dieser Text steht in ‚Anführungszeichen‘; alles klar?“. Englische Anführungszeichen werden anders benutzt: “this is an ‘English’ quotation.”

### 1.3 Abkürzungen

Eine Abkürzung (ABK) wird bei der ersten Verwendung ausgeschrieben. Danach nicht mehr: ABK. Man kann allerdings die Langform explizit anfordern: Abkürzung oder die Kurzform ABK oder auch noch einmal die Definition: Abkürzung (ABK).

---

<sup>1</sup>Ein Ratgeber in allen Detailfragen ist **Forssman2002**

Beachten Sie, dass bei Abkürzungen, die für zwei Wörter stehen, ein kleines Leerzeichen nach dem Punkt kommt: z. B. bzw. z. B. , d. h. bzw. d. h. .

### 1.4 Querverweise

Querverweise auf eine Kapitelnummer macht man im Text mit `\ref` (Kapitel 1.1) und auf eine bestimmte Seite mit `\pageref` (Seite 1). Man kann auch den Befehl `\autoref` benutzen, der automatisch die Art des referenzierten Elements bestimmt (z. B. Abschnitt 1.1 oder Tabelle 1.1).

### 1.5 Fußnoten

Fußnoten werden einfach mit in den Text geschrieben und zwar genau an die Stelle<sup>2</sup>

### 1.6 Fremdsprachige Begriffe

Wenn Sie Ihre Arbeit auf Deutsch verfassen, gehen Sie sparsam mit englischen Ausdrücken um. Natürlich brauchen Sie etablierte englische Fachbegriffe, wie z. B. *Interrupt*, nicht zu übersetzen. Sie sollten aber immer dann, wenn es einen gleichwertigen deutschen Begriff gibt, diesem den Vorrang geben. Den englischen Begriff (*term*) können Sie dann in Klammern oder in einer Fußnote<sup>3</sup> erwähnen. Absolut unakzeptabel sind deutsch gebeugte englische Wörter oder Kompositionen aus deutschen und englischen Wörtern wie z. B. downgeloadet, upgedated, Keydruck oder Beautyzentrum.

### 1.7 Tabellen

Tabellen werden normalerweise ohne vertikale Striche gesetzt, sondern die Spalten werden durch einen entsprechenden Abstand voneinander getrennt.<sup>4</sup> Zum Einsatz kommen ausschließlich horizontale Linien (siehe Tabelle 1.1).

---

<sup>2</sup> An der die Fußnote auftauchen soll.

<sup>3</sup> Englisch: *footnote*.

<sup>4</sup> Siehe **Willberg1999**

**Tabelle 1.1:** Ebenen der Kopplung und Beispiele für enge und lose Kopplung










Form der Kopplung	enge Kopplung	lose Kopplung
Physikalische Verbindung	Punkt-zu-Punkt	über Vermittler
Kommunikationsstil	synchron	asynchron
Datenmodell	komplexe gemeinsame Typen	nur einfache gemeinsame Typen
Bindung	statisch	dynamisch

Eine Tabelle fließt genauso, wie auch Bilder durch den Text. Siehe Tabelle 1.1.

## 1.8 Harveyballs

Harvey Balls sind kreisförmige Ideogramme, die dazu dienen, qualitative Daten anschaulich zu machen. Sie werden in Vergleichstabellen verwendet, um anzuzeigen, inwieweit ein Untersuchungsobjekt sich mit definierten Vergleichskriterien deckt. ([Wikipedia\\_HarveyBalls](#))

**Tabelle 1.2:** Beispiel für Harvey Balls

	Ansatz 1	Ansatz 2	Ansatz 3
Eigenschaft 1			
Eigenschaft 2			
Eigenschaft 3			

## 1.9 Aufzählungen

Aufzählungen sind toll.

- Ein wichtiger Punkt
- Noch ein wichtiger Punkt
- Ein Punkt mit Unterpunkten
  - Unterpunkt 1
  - Unterpunkt 2
- Ein abschließender Punkt ohne Unterpunkte

Aufzählungen mit laufenden Nummern sind auch toll.

1. Ein wichtiger Punkt
2. Noch ein wichtiger Punkt
3. Ein Punkt mit Unterpunkten
  - a) Unterpunkt 1
  - b) Unterpunkt 2
4. Ein abschließender Punkt ohne Unterpunkte

### 1.10 Zitate

#### 1.10.1 Zitate im Text

Wichtig ist das korrekte Zitieren von Quellen, wie es auch von **Kornmeier2011** dargestellt wird. Interessant ist in diesem Zusammenhang auch der Artikel von **Kramer2009**. Häufig werden die Zitate auch in Klammern gesetzt, wie bei (**Kornmeier2011**) und mit Seitenzahlen versehen (**Kornmeier2011**).

Bei Webseiten wird auch die URL und das Abrufdatum mit angegeben (**Gao2017**). Wenn die URL nicht korrekt umgebrochen wird, lohnt es sich, an den Parametern *biburl\*penalty* in der `preamble.tex` zu drehen. Kleinere Werte erhöhen die Wahrscheinlichkeit, dass getrennt wird.

#### 1.10.2 Zitierstile

Verwenden Sie eine einheitliche und im gesamten Dokument konsequent durchgehaltene Zitierweise. Es gibt eine ganze Reihe von unterschiedlichen Standards für das Zitieren und den Aufbau eines Literaturverzeichnisses. Sie können entweder mit Fußnoten oder Kurzbelegen im Text arbeiten. Welches Verfahren Sie einsetzen ist Ihnen überlassen, nur müssen Sie es konsequent durchhalten.

In der Informatik ist das Zitieren mit Kurzbelegen im Text (Harvard-Zitierweise) weit verbreitet, wobei für das Literaturverzeichnis häufig die Regeln der ACM oder IEEE angewandt werden.<sup>5</sup>

---

<sup>5</sup>Einen Überblick über viele verschiedene Zitierweisen finden Sie in der <http://amath.colorado.edu/documentation/LaTeX/reference/faq/bibstyles.pdf>

Denken Sie daran, dass das Übernehmen einer fremden Textstelle ohne entsprechenden Hinweis auf die Herkunft in wissenschaftlichen Arbeiten nicht akzeptabel ist und dazu führen kann, dass die Arbeit nicht anerkannt wird. Plagiate werden mit mangelhaft (5,0) bewertet und können weitere rechtliche Schritte nach sich ziehen.

### 1.10.3 Zitieren von Internetquellen

Internetquellen sind normalerweise *nicht* zitierfähig. Zum einen, weil sie nicht dauerhaft zur Verfügung stehen und damit für den Leser möglicherweise nicht beschaffbar sind und zum anderen, weil häufig der wissenschaftliche Anspruch fehlt.<sup>6</sup>

Wenn ausnahmsweise doch eine Internetquelle zitiert werden muss, z. B. weil für eine Arbeit dort Informationen zu einem beschriebenen Unternehmen abgerufen wurden, sind folgende Punkte zu beachten:

- Die Webseite ist auszudrucken und im Anhang der Arbeit beizufügen,
- das Datum des Abrufs und die URL sind anzugeben,
- verwenden Sie Internet-Seiten ausschließlich zu illustrativen Zwecken (z. B. um einen Sachverhalt noch etwas genauer zu erläutern), aber nicht zur Faktenvermittlung (z. B. um eine Ihrer Thesen zu belegen).

Wenn Sie aufgrund der Natur Ihrer Arbeit sehr viele Internetquellen benötigen, dann können Sie diese statt sie auszudrucken auch in elektronischer Form abgeben (CD/DVD). Als Abgabeformat der elektronischen Quellen ist PDF/A<sup>7</sup> vorteilhaft, weil es von allen Formaten die größte Stabilität besitzt. Auf der CD/DVD geben Sie bitte auch eine HTML-Version des Literaturverzeichnisses ab, in der die Online-Quellen sowie die gespeicherten PDF-Dateien verlinkt sind.

Wikipedia stellt einen immensen Wissensfundus dar und enthält zu vielen Themen hervorragende Artikel. Sie müssen sich aber darüber im Klaren sein, dass die Artikel in Wikipedia einem ständigen Wandel unterworfen sind und nicht als Quelle für wissenschaftliche Fakten genutzt werden sollten. Es gelten die allgemeinen Regeln für das Zitieren von Internetquellen. Sollten Sie doch Wikipedia nutzen müssen,

---

<sup>6</sup>Eine lesenswerte Abhandlung zu diesem Thema findet sich (im Internet) bei **Weber2006**

<sup>7</sup>Bei PDF/A handelt es sich um ein besonders stabile Variante des Portable Document Format (PDF), die von der International Organization for Standardization (ISO) standardisiert wurde.

verwenden Sie bitte ausschließlich den Perma-Link<sup>8</sup> zu der Version der Seite, die Sie aufgerufen haben.

---

<sup>8</sup>Sie erhalten den Permalink über die Historie der Seite und einen Klick auf das Datum.

## **Kapitel 2**

# **Einleitung**

TODO

W.A. Halang 2016 und Bundesministerium für Wirtschaft und Energie 2016





## **Kapitel 3**

# **Grundlagen**

### **3.1 Historie**

Industrie 3.0 -> Industrie 4.0 - Kommunikation über Unternehmensgrenzen, Kommunikation nicht mehr über ERP und MES sondern direkt von unteren Schichten, wie z.B. Maschinen oder Komponenten

### **3.2 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.

### 3.2.1 Anforderungen

### 3.2.2 Komponenten einer I4.0 Architektur

### 3.2.3 Kommunikationsstrukturen

*End2End*

*Gateways*

*Publish-Subscribe*

*Kommunikation mit Netzwerk als Partner*

### 3.2.4 Schutzziele

Für diese neuen Szenarien gelten weiterhin die klassischen Schutzziele der Vertraulichkeit, Integrität und Verfügbarkeit.

Des Weiteren werden Bestellungen oder Logistikprozesse durch I4.0 Kommunikation abgewickelt. Diese stellen einen rechtlichen Rahmen dar, welcher weitere Schutzziele beinhaltet:

- Authentizität
- Nichtabstreitbarkeit
- Verbindlichkeit
- Zurechenbarkeit

TODO – Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Nichtabstreitbarkeit, Verbindlichkeit, Zurechenbarkeit

## **Kapitel 4**

# **Analyse**

## **4.1 Sicherheitsanforderungen des Kommunikationsstacks**

### **4.1.1 Physical Layer**

### **4.1.2 Data Link Layer**

### **4.1.3 Network Layer**

### **4.1.4 Transport Layer und End2End Security**

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

## **4.2 Protokollstandards**

### **4.2.1 OPC UA**

### **4.2.2 MConnect**

### **4.2.3 ...**

## **4.3 Angriffsvektoren**

### **4.3.1 Verschlüsselung**

### **4.3.2 Paketversand**

### **4.3.3**

## **4.4 Auswertung der Ergebnisse**

## **4.5 Maßnahmenkatalog**

## **Kapitel 5**

# **Implementierung**



# Abkürzungsverzeichnis

**ABK** Abkürzung

**ACM** Association of Computing Machinery

**PDF** Portable Document Format

**IEEE** Institute of Electrical and Electronics Engineers

**ISO** International Organization for Standardization





# Tabellenverzeichnis

1.1	Ebenen der Kopplung und Beispiele für enge und lose Kopplung . .	3
1.2	Beispiel für Harvey Balls . . . . .	3



# **Abbildungsverzeichnis**



# Listings



# Literatur

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

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





# Index

Abbreviation, *siehe* Abkürzungen

Abkürzungen, 1

Hervorhebungen, 1

Permalink, 6

Plagiat

    Bewertung, 5

Typographie, 1

Zitat

    Internetquellen, 5

    Kurzbeleg, 4

    Wikipedia, 5

Zitierweise, 4