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. 37 Seiten.

Minges, Philipp:
TODO - Title EN / Philipp Minges. –
Bachelor Thesis, Mannheim: University of Applied Sciences Mannheim, 2018. 37 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

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 - mehr -> leitfaden-it-security-i40.pdf - Einleitung 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 2016c 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.

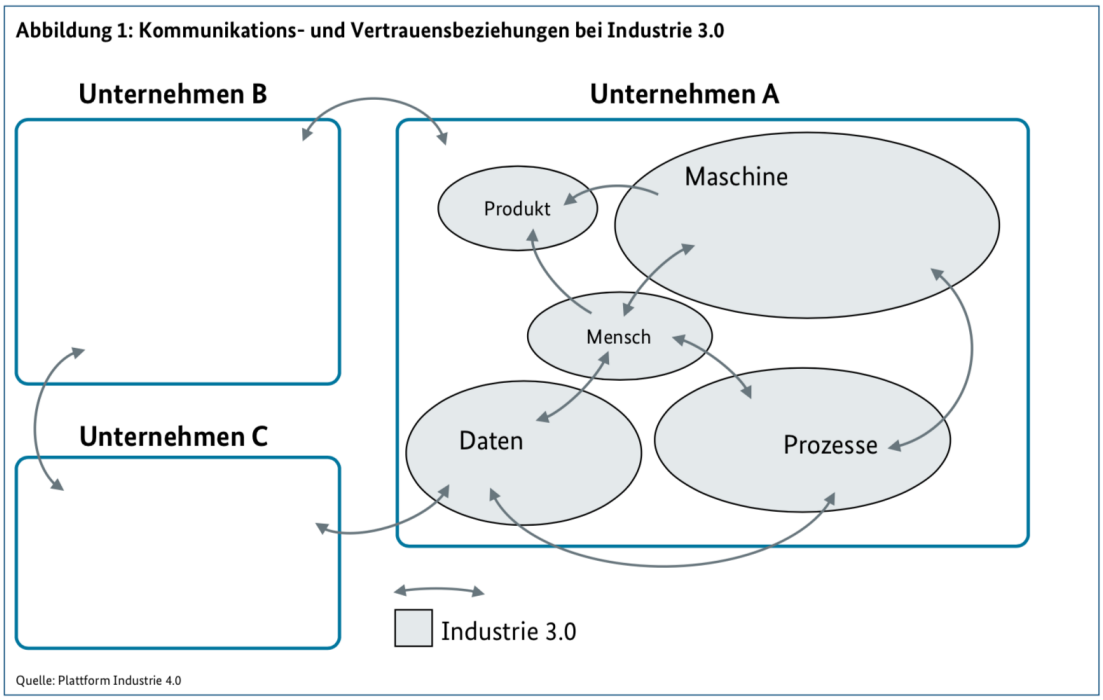

Abbildung 2.1: Kommunikationsbeziehungen in einer Industrie 3.0 Umgebung - TODO ref. sichere unternehmensübergreifende Kommunikation

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 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.

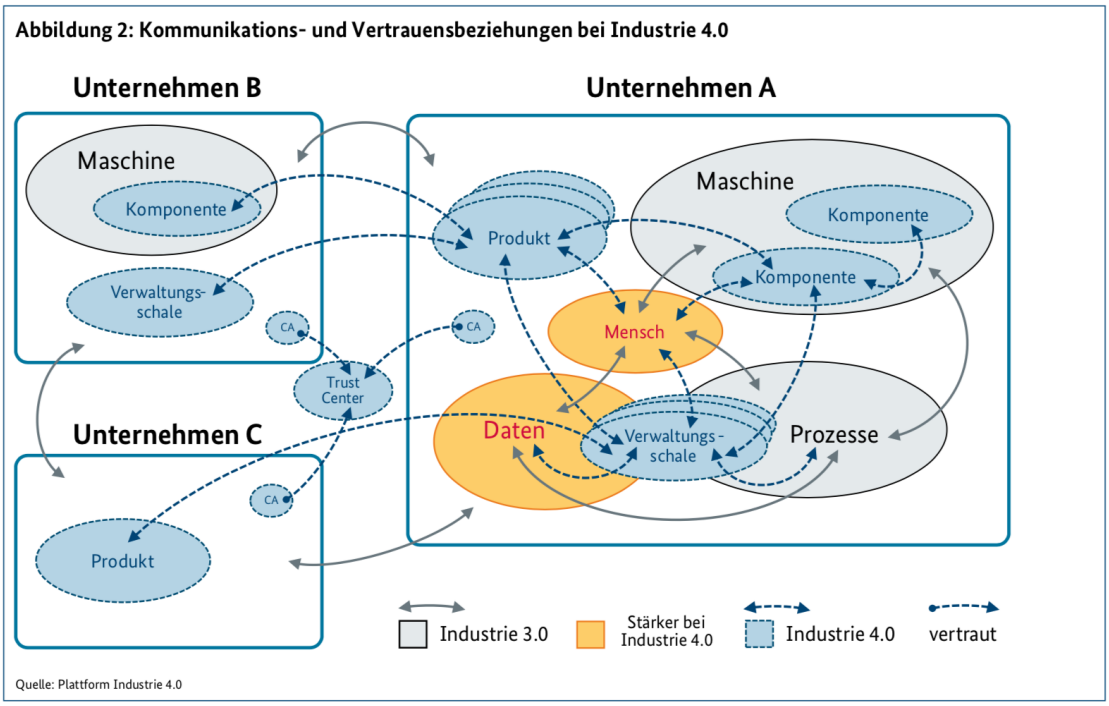

Abbildung 2.2: Kommunikationsbeziehungen in einer Industrie 4.0 Umgebung - TODO ref. sichere Unternehmensübergreifende Kommunikation

Diese Entwicklung erzeugt durch die ständige Kommunikation eine ernome 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. Für kritische Infrastrukturen, wie z. B. im Energie-, Wasser-, Transport- und Gesundheitssektor existiert diese Verbindung bereits.

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. Kunden- und Maschinendaten werden miteinander vernetzt 4.0 2016.

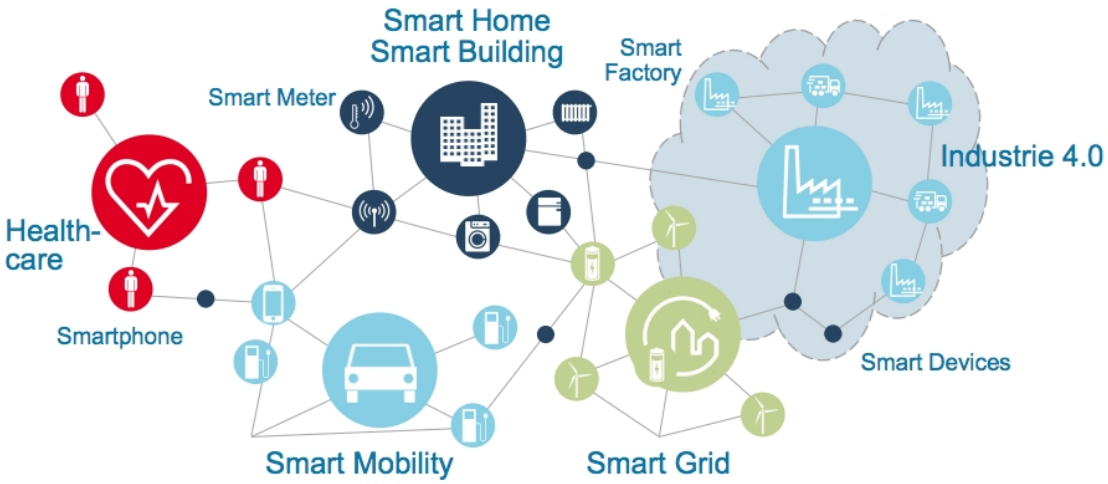

Abbildung 2.3: Das Internet der Dinge - 4.0 2016

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.

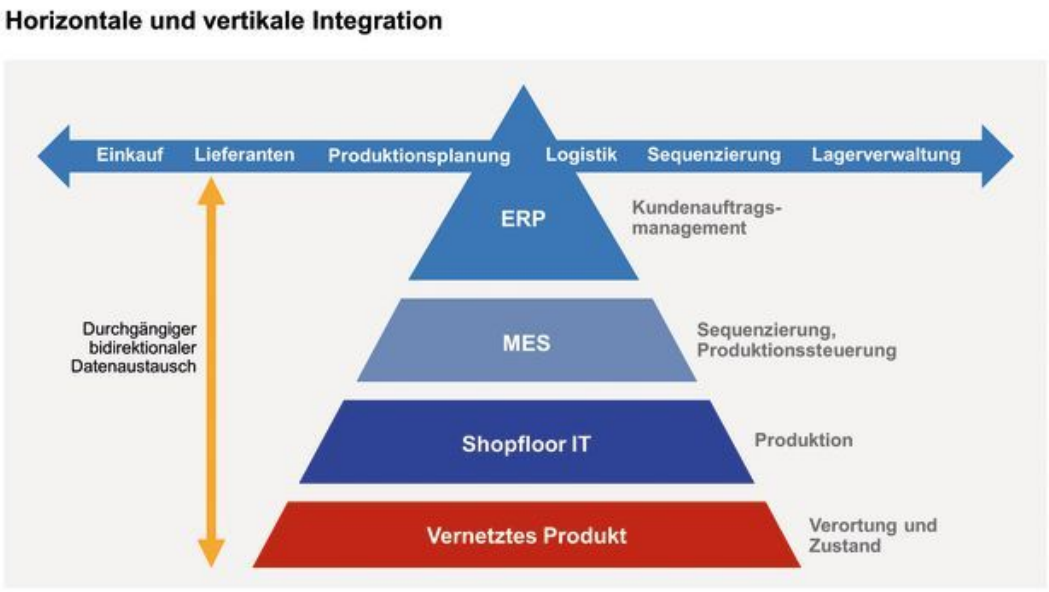

Abbildung 2.4: horizontale und vertikale Integration - TODO ref. HP Industry-of-things siehe bookmark

2.3.1 IoT/IIoT

IoT beschreibt ein verbraucherorientiertes Konzept für die Nutzung von digitalisierten und vernetzten Systemen. Hierbei werden die physischen Systeme virtuell abgebildet. Dies wird genutzt, um die Effektivität der Systeme zu verbessern und intelligente Services zu nutzen. Das IIoT beschreibt den Gebrauch von IoT-Technologien im industriellen Raum.

Das IoT ist ein wesentlicher Bestandteil der Industrie 4.0, welche Netzwerke aus Systemen, Daten und Dienstleistungen herstellt, in denen diese Komponenten miteinander kommunizieren. Für die Kommunikation haben sich, je nach Anforderungen, verschiedene Protokolle, wie z.B. Hypertext Transfer Protocol (HTTP), Constrained Application Protocol (CoAP), Extensible Messaging and Presence Protocol (XMPP) und Message Queue Telemetry Transport (MQTT), etabliert. Jedes dieser Protokolle besitzt für spezifische Anforderungen wie Skalierbarkeit, vorhandene Ressourcen, Echtzeitkommunikation oder Sicherheit Vor- und Nachteile.

2.3.2 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.

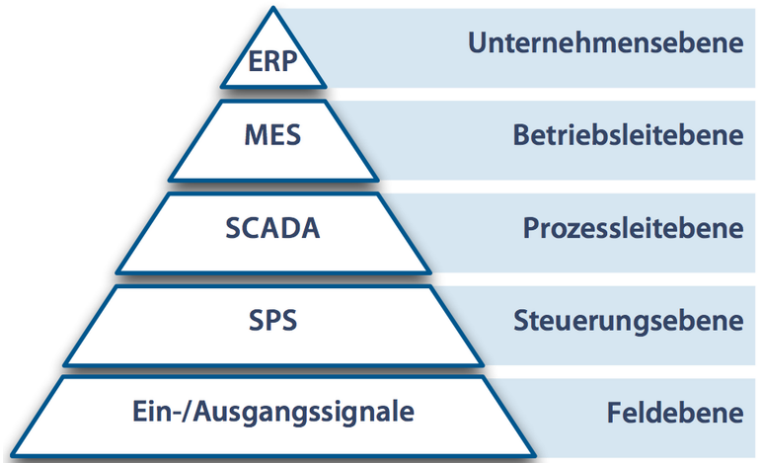

Abbildung 2.5: Automatisierungspyramide - TODO ref. Langmann,2004

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 Echtzeitkommunikation mit Verzögerungen <1ms ausgelegt. Die Integration von Sicherheitsmaßnahmen bei der Kommunikation dieser Systeme stellt oft eine große Herausforderung dar.

2.4 Grundprinzipien der sicheren Kommunikation

Die Grundprinzipien der sicheren Kommunikation beschreiben die Schutzziele im Bereich der Informationssicherheit. Diese verdeutlichen den Anspruch an die Sicherheit an ein zu implementierendes System oder ein Netzwerk. Sie stellen einen vereinbarten Umfang gegen Bedrohungen dar, welcher von den Kommunikationspartnern gewährleistet wird und nachgewiesen werden kann. Diese klassischen Schutzziele sind auch für Industrie 4.0 Umgebungen zutreffend. Die weitreichende Vernetzung der Systeme in der Industrie 4.0 erfordert jedoch weitere Schutzziele, um einen rechtskonformen Umgang oder besondere Anforderungen sicherzustellen.

2.4.1 klassische Schutzziele

- Vertraulichkeit/Zugriffsschutz
- (Daten)-Integrität/Änderungsschutz
- Authentizität/Fälschungsschutz
- Verfügbarkeit

2.4.2 weitere Schutzziele

- Verbindlichkeit/Nichtabstreitbarkeit
- Anonymität

TODO - gefällt mir nicht. Muss man die Begriffe erklären? TODO - ref. Bundesministerium für Wirtschaft und Energie 2016a

2.5 Kommunikationsstrukturen in Industrie 4.0 Umgebungen

Um die Kommunikation zwischen verschiedenen Teilnehmern zu ermöglichen, ergeben sich in der Praxis unterschiedliche Strukturen. Jede dieser Strukturen bietet, je nach Anwendungsfall und zu erfüllenden Anforderungen, Vor- und Nachteile.

TODO - mehr -> siehe sichere Kommunikation-i4.0

2.5.1 End2End

Die Komponenten der Industrie 4.0 Umgebung kommunizieren über einen direkten Kanal miteinander. Dies setzt voraus, dass sich beide Teilnehmer in einem Netzwerk befinden, welches die benötigten Dienste wie z. B. Internet Protocol (IP) und Domain Name System (DNS) zur Kommunikation bereitstellt. Des weiteren müssen beide Systeme diese Dienste und Protokolle unterstützen.

2.5.2 Gateways

Um existierende Systeme, welche selbst nicht Industrie 4.0 konform kommunizieren oder zu wenig Rechenleistung besitzen, in die Industrie 4.0 Welt zu integrieren, werden Industrie 4.0 Gateways genutzt. Dabei ist jedoch zu beachten, dass die Systeme hinter den Gateways nicht als Industrie 4.0 Komponenten entwickelt wurden und somit auch keine oder nur wenige dieser Eigenschaften besitzen. Des Weiteren ist es möglich, dass die Kommunikation aus Leistungsgründen oder besonderer Anforderungen über optimierte, proprietäre Protokolle stattfindet. Die Gateways müssen auf die Systeme und deren Protokolle individuell konfiguriert werden, um die Funktionalitäten im Industrie 4.0 Netz bereitstellen zu können, und die Kommunikation zu schützen.

2.5.3 Publish-Subscribe

Das Publish-Subscribe Modell bietet die Möglichkeit Informationen an mehrere Teilnehmer zu verteilen. Hierbei melden sich die Empfänger beim Verteiler an und wählen aus, über welche Nachrichtentypen sie informiert werden möchten. Diese Verteildienste nutzen zur besseren Skalierung und Reduzierung der Netzlast häufig Datagramme wie User Datagram Protocol (UDP). Durch die Nutzung von Datagrammen geht jedoch die Fehlertoleranz verloren. Somit muss entweder dafür gesorgt werden, dass eine sehr zuverlässige Netzwerkinfrastruktur vorhanden ist und hohe Bandbreitenreserven geschaffen werden, um die Dienstgüte (Quality of Service (QoS)) sicherzustellen oder dieses Modell nur für fehlertolerante Kommunikation wie z. B. Audio- und Video-Anwendungen oder Businessprozesse zu nutzen.

2.5.4 Kommunikation mit Netzwerk als Partner

Zeitkritische Automatisierungsanwendungen verlangen besondere Netzwerkeigenschaften. Sie können auf Latenz oder Jitter angewiesen sein. Um diese Eigenschaften sicherzustellen, ist es sinnvoll in diese Netze eine Industrie 4.0 Schnittstelle zu integrieren. Somit ist es den Teilnehmern möglich, über die Verwaltungsschale sicherzustellen, dass das Netzwerk die erforderlichen Anforderungen bereitstellt. 4.0 2017

TODO - Bilder -> sichere-kommunikation-i40

2.6 Normen und Standards

Im Gegensatz zur Industrie 3.0, in welcher Daten auf lokaler Ebene oder zwischen einzelnen internen Unternehmensebenen ausgetauscht wurden, stellt der Datenaustausch und Informationsfluss im vermaschten Industrie 4.0 Netzwerk einen wesentlichen Bestandteil dar. Aktuell gibt es zwei Architekturmodelle zur Umsetzung von Industrie 4.0 Umgebungen. Diese setzen sich aus dem von der Platform Industrie 4.0 entwickelten Referenzarchitekturmodell Industrie 4.0 (RAMI4.0) und der Industrial Internet Reference Architetecture (IIRA) der Industrial Internet Consortium (IIC) zusammen. Beide Modelle verfolgen verschiedene Integrationsansätze.

Des Weiteren findet die Kommunikation in der Industrie 4.0 nicht mehr über einzelne, vorgegebene Schnittstellen statt, sondern direkt von den Produktionssystemen, also den unteren Ebenen der Automatisierungspyramide. Um dies zu ermöglichen, ist es notwendig, eine einheitliche Kommunikation durch Normen und Standards herzustellen, um eine unternehmensübergreifende Kommunikation dieser Shop-Floor IT zu ermöglichen.

2.6.1 Referenzarchitekturen

RAMI4.0

Um eine flächendeckende Vernetzung zu ermöglichen, muss eine einheitliche Kommunikation geschaffen werden. Die RAMI4.0 ist eine dreidimensionale Darstellung aller Teilnehmer einer Industrie 4.0 Umgebung und stellt ein Modell einer Service Oriented Architecture (SOA) dar. Sie soll eine Verwaltungsschale für Teilnehmer bilden, um eine standardisierte Kommunikation und einfache Inbetriebnahme neuer Komponenten ermöglichen. 4.0 2016 Die Achsen des RAMI4.0 bestehen aus:

- Achse 1 - Die Hierarchie zeigt die Anlagen, Maschinen sowie das Endprodukt, welche miteinander Vernetzt sind. In diesem Netzwerk werden Funktionen bereitgestellt und Daten ausgetauscht.
- Achse 2 - Die Architektur beschreibt - TODO
- Achse 3 - Der Produktlebenszyklus wird im Gegensatz zur Industrie 3.0 in das Netzwerk mit eingebunden. Der gesamte Prozess der Produktion, Wartung bis hin zur Verschrottung soll digital erfasst werden.

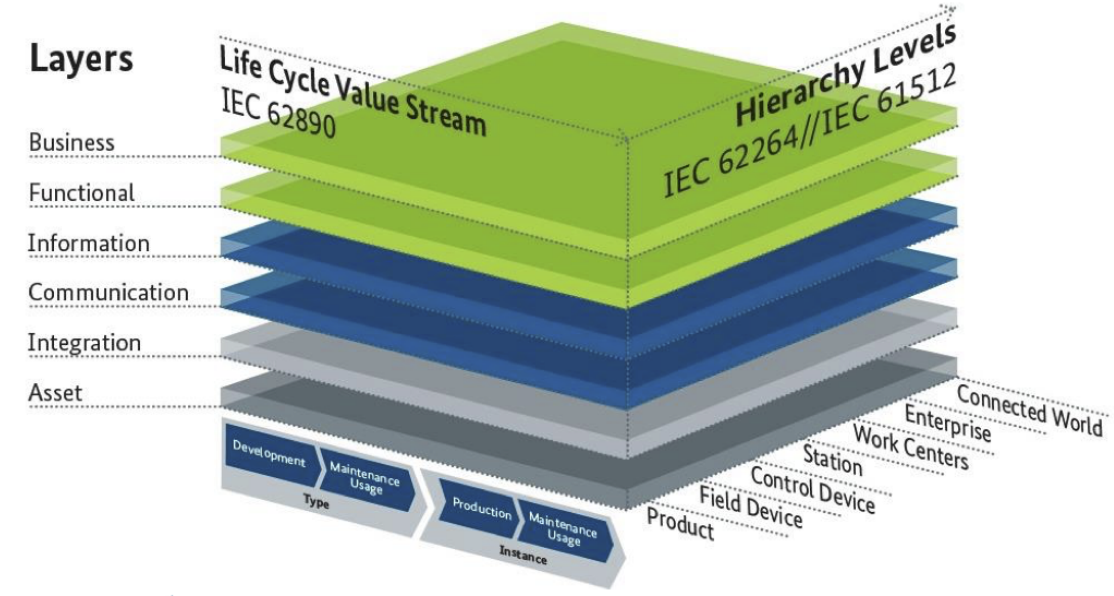

Abbildung 2.6: RAMI 4.0 - 4.0 2016

Nach dem RAMI4.0 stellt der Communication Layer das Bindeglied zwischen dem Integration Layer, welcher Eigenschaften der physischen Welt für Computersysteme erreichbar macht, und dem Information Layer, welcher die Funktionsbezogenen Daten beinhaltet, dar. Bundesministerium für Wirtschaft und Energie 2016b

TODO - Kommunikation beschreiben

Jeder Teilnehmer der Architektur wird als Asset bezeichnet und besitzt seine eigene Verwaltungsschale, welche als Schnittstelle zum Austausch von Informationen dient. Die Verwaltungsschale ist der Übergang zwischen der physischen zur digitalen Welt.

TODO - genauer auf die einzelnen Komponenten eingehen! - Assets, Architektur, Komponenten, Verwaltungsschale TODO - Architektur wichtig SOA beschreiben -> Angriffsvektoren TODO - siehe DIN 91345 TODO - Anforderungen an diese Komponenten unterschiedlich

IIRA

TODO

2.6.2 Protokollstandards

TODO - Durch die vorausgesetzte M2M-Kommunikation wurde die Entwicklung neuer Protokolle zum effizienten Informationsaustausch vorangetrieben, welche es ermöglichen sollen, eine Standardisierung bereitzustellen und somit eine herstellerübergreifende und plattformunabhängige Kommunikation zu ermöglichen.

OPC UA

TODO

DDS

TODO

2.7 Testsystem

Die aus der Analyse hervorgehenden möglichen Schwachstellen im Bereich der Netzwerksicherheit und deren Auswirkungen werden anhand eines vorhandenen, prototypischen Industrie 4.0 Testsystems Weber 2018 veranschaulicht. Das vorhandene System setzt die drei Schichten der Software-Architektur (Verteilungs-, Baustein- und Laufzeitschicht) nach Starke / Hruschka um. Die Netzwekkommunikation wird über das Protokoll OPC UA realisiert, welches die Anforderungen der Industrie 4.0 und RAMI4.0 umsetzt.

2.7.1 Architektur

Das vorhandene System ist, aufgrund der vorgesehenen Einsatzgebiete Lehre, Integrations- und Sicherheitstests, als virtuelle Maschine (VM) umgesetzt worden. Dies ermöglicht es die Testinfrastruktur vom restlichen Netz zu kapseln. Das Betriebssystem der VM stellt eine Firewall bereit, welche unerwünschten Netzwerktraffic von oder zu dem System verhindert. Um eine gute Erweiterbarkeit der Testumgebung und Modularisierung der Komponenten zu erreichen, werden die einzelnen Industrie 4.0 Komponenten mit Hilfe der Containerlösung Docker isoliert ausgeführt, verwaltet und deren Netzwerkkommunikation sichergestellt. Durch den zusätzlichen Einsatz des Deploymentsystems Kubernetes wird ein verteiltes Ausführen des Systems ermöglicht und somit eine gute Skalierbarkeit erreicht.

2.7.2 Komponenten

Repository

Discovery Server

Public-Key Infrastructure (PKI)

Identity Provider

Verwaltungsinterface

Scheduler

Kapitel 3

Konzept

Um die in den Grundlagen beschriebenen Sicherheitsstandards, Protokolle und Integrationslösungen auf ihre Standhaftigkeit in Bezug auf die IT-Schutzziele zu analysieren, werden die Protokolle und Systeme in ihrem Aufbau untersucht und mögliche Schwachstellen herausgearbeitet, daraus hervorgehende Risiken beschrieben und erforderliche Maßnahmen empfohlen. Die RAMI4.0 beschreibt ein Referenzmodell für Industrie 4.0 Umgebungen. Bereits etablierte Lösungen bestehen aus heterogenen, individuellen Netzwerklandschaften. Um eine Untersuchung der vorhandenen Systeme im neuen Umfeld durchzuführen, müssen verschiedene Faktoren, wie Infrastruktur oder besondere Anforderungen an die Systeme mit einbezogen werden. Das folgende Kapitel dient der Beschreibung der Vorgehensweise bei der Analyse der Netzwerkkommunikation und deren Komponenten.

3.1 Anforderungen

Die Kommunikation in Industrie 4.0 Umgebungen findet über diverse Übertragungsmedien, Protokolle und Software statt. Um die beteiligten Komponenten auf Schwachstellen zu untersuchen, werden zuerst die Anforderungen für eine sichere Kommunikation herausgearbeitet, um eine Grundlage der Analyse zu schaffen.

3.1.1 Grundlegende Anforderungen

Aufgrund der sehr unterschiedlichen Einsatzbereiche von Industrie 4.0 Systemen, unterscheiden sich auch dementsprechend deren Anforderungen. Aus den Referenz-

modellen RAMI4.0 und IIRA lassen sich grundsätzlich drei grundlegende Anforderungen an den Übertragungskanal ableiten Bundesministerium für Wirtschaft und Energie 2016b.

Sicherheit

TODO - Hierunter fallen die Bereiche a) Netzsicherheit und Datensicherheit, b) Sichere Identitäten und c) funktionale Sicherheit. Die Punkte a) und b) werden in der AG3 der Plattform Industrie 4.0 adressiert [6], [7]. Die UAG Netzkommunikation arbeitet bzgl. dieser Punkte mit der AG3 zusammen. Zum Thema „Security und funktionale Sicherheit“ arbeitet die AG3 mit dem DKE-TBINK AK IT Security und Security by Design zusammen. Hinsichtlich funktionaler Sicherheit gibt es Anforderungen von Seiten IEC 61784-3. Diese müssen bei der Definition neuer Systeme berücksichtigt werden.

- Netzsicherheit und Datensicherheit
- Sichere Identitäten
- funktionale Sicherheit

Verfügbarkeit

Die ständige Verfügbarkeit von Daten und Diensten spielst in der Industrie 4.0 eine bedeutende Rolle, um den Datenaustausch zwischen zwei Kommunikationspartnern im Netz jederzeit zu ermöglichen. Als Verfügbarkeit wird die Wahrscheinlichkeit bezeichnet, dass ein System innerhalb eines bestimmten Zeitraumes erreichbar ist. Ein System gilt als verfügbar, wenn es erreichbar ist und die für es vorgesehenen Aufgaben erledigen kann.

Die Verfügbarkeit eines Systems wird in Verfügbarkeitsklassen gegliedert. Diese beschreiben Verfügbarkeitswahrscheinlichkeiten von 99% (Verfügbarkeitsklasse 2) bis 99,9999% (Verfügbarkeitsklasse 6). Eine exakte Definition, wann ein System hochverfügbar ist, gibt es nicht - TODO ref. Im Allgemeinen wird ab Verfügbarkeitsklasse 3 (99,99%) von Hochverfügbarkeit gesprochen. Industrie 4.0 Systeme sind meist Hochverfügbar.

QoS

TODO - Es ist die originäre Aufgabe der Datenkommunikation, Distanzen zu überwinden - egal wie weit die Kommunikationspartner voneinander entfernt sind: Effizienz- und produktivitätssteigernd ist sowohl die Überwindung von wenigen Zentimetern per Near Field Communication (NFC) als auch die Datenübertragung rund um den Globus durch verschiedene Netze; nicht zu vergessen: Teleservices zur Unterstützung bei Inbetriebnahmen, zum Remote Debugging und zum Fernwirken. Die Qualitätsanforderungen an Kommunikationsnetze (wired und wireless) sind: hochverfügbare, homogene Netze; garantierte Bandbreiten für die sehr unterschiedlichen Anwendungen (Bild 1); verbindliche Dienstgüte (Quality of Service, QoS) [1]; standardisierte Dienste (z.B. mobilfunkproviderübergreifende SMS-Bestätigung).

TODO - ref. Torscht 2014 und IEEE 802.1p

Industrie 4.0 Dienste basieren auf IP-Netzen. Sie bilden nach dem OSI-Modell eine höhere Schicht im Netz. Somit setzt sich die Güte eines Dienstes aus der Übertragungsgüte der unteren Schichten des OSI-Modells sowie der QoS-Parameter des Network Layer (IP-Ebene) zusammen. In IP-Netzen wird der Einfluss auf die QoS in folgenden Parametern beschrieben:

- Latenzzeit: Dauer der Paketübertragung
- Jitter: Abweichung der Latenzzeit von ihrem Mittelwert
- Paketverlustrate: Wahrscheinlichkeit des Verlusts von IP-Paketen während der Übertragung
- Durchsatz: gemittelte Datenmenge pro Zeiteinheit

3.1.2 Besondere Anforderungen

zeitkritische Prozesse

Migration vorhandener Systeme

3.1.3 Rechtliche Anforderungen

TODO - DSGVO

3.2 Komponenten

Die beschriebenen Anforderungen müssen, um eine sichere Netzwerkkommunikation zu gewährleisten, von allen beteiligen Komponenten der Umgebung integriert und umgesetzt werden. Industrie 4.0 Umgebungen können in unterschiedlichster Form ausgeprägt sein. Die Umsetzung der Hard- und Softwarekomponenten hängt von den zu übertragenden Daten, dem Übertragungsmedium, der Übertragungsdistanz und vorausgesetzten Dienstgüte ab. Somit werden die zu analysierenden Komponenten in Hard- und Softwarekomponenten gegliedert.

3.2.1 Hardware

Übertragungskanal

Der Übertragungskanal ist Bestandteil der ersten Schicht des OSI-Schichtenmodells (Physical Layer). In Industrie 4.0 Umgebungen ist es notwendig, Daten zu übertragen, um eine räumliche oder zeitliche Distanz zu überbrücken. Je nach Anwendungsfall findet diese Kommunikation über Kupfer- bzw. Glasfaserkabel, Funkübertragung oder ein Speichermedium statt. Je nach Beschaffenheit des Übertragungskanals, ist es notwendig, weitere Maßnahmen zur Sicherheit der Kommunikation zu treffen.

Infrastruktur

TODO - DMZ, Defense in Depth usw.?

3.2.2 Software

Jede Komponente einer Industrial Control System (ICS)-Umgebung kann Softwareschwachstellen und Sicherheitslücken enthalten. Dabei spielt es keine Rolle, ob es sich um ein komplexes ICS handelt oder um einen einfachen Anwendungsserver. Software-Aktualisierungen sowie ein Patch-Management sind für einen sicheren Betrieb notwendig, um Angriffe über Exploits zu verhindern.

Netzwerkstack

Die Kommunikation zwischen Industrieanlagen findet mehr und mehr auf der Basis von TCP-basierten Netzwerken statt. Das RAMI4.0 beschreibt Industrie 4.0 Umgebungen als SOA. SOA beschreibt ein Netzwerk, in welchem von den Teilnehmern Dienste bereitgestellt und genutzt werden können. Die Dienste im Netzwerk werden i. d. R. über eine Representational State Transfer (REST)-Application Programming Interface (API) bereitgestellt. Diese Schnittstellen nutzen bereits etablierte Protokolle der IoT oder IIoT Welt. Im Rahmen der Thesis werden ausgewählte Protokolle auf ihre Standhaftigkeit in Industrie 4.0 Umgebungen geprüft.

Protokolle

IoT-Geräte nutzen das Internet als Übertragungsmedium. Somit müssen sie zur Übertragung ihrer Daten Protokolle nutzen, welche die Internet Protocol Suite der Internet Engineering Task Force (IETF) einhalten. Etablierte Internet-Protokolle wie HTTP und XMPP wurden zur Kommunikation ressourcenreicher Geräte mit hoher Leistung entwickelt und sind für viele Netzwerke mit IoT- oder IIoT-Endknoten zu komplex, bzw. nicht geeignet. Im Rahmen der 4. industriellen Revolution wurden daher, vor allem für IIoT Umgebungen, neue Protokolle entwickelt, welche ressourcensparende, sichere Kommunikation zwischen Maschinen sicherstellen sollen. Im Rahlen der Thesis werden die IoT-Protokolle HTTP und XMPP sowie die IIoT-Protokolle OPC UA, MQTT, CoAP und DDS mit Bezug auf ihre Netzwerksicherheit analysiert.

3.3 Umsetzung

Bei der Analyse auftretende, mögliche Sicherheitslücken werden in einer vorhandenen, prototypischen Industrie 4.0 Testumgebung implementiert und nachgewiesen. Sicherheitslücken, welche durch Fehlkonfiguration von Software auftreten und keine konzeptionellen Schwachstellen der Software oder deren Protokolle darstellen, sollen in der Testumgebung aktiviert und deaktiviert werden können, um die Auswirkung eines Angriffs auf ein Industrie 4.0 System zu Lehr- und Testzwecken darstellen zu können.

Kapitel 4

Analyse

4.1 Übertragungsmedien

Somit können als Übertragungsmedien neben der klassischen Kabelverbindung auch andere (instabile) Kanäle wie Mobilfunk oder Satelliten in Frage kommen. Um die Kommunikation über alle Medien sicher und zuverlässig zu gestalten, müssen auf technischer Ebene Protokolle genutzt werden, welche es ermöglichen die gegebenen Schutzziele zu realisieren.

Des Weiteren müssen die Daten über große Entfernungen hinweg übertragen werden.

4.1.1 Kabelgebunden

4.1.2 Funk/instabile Übertragungskanäle

Global System for Mobile Communications (GSM)

High Speed Downlink Packet Access (HSDPA)

Long Term Evolution (LTE)

Low-Power Wide Area (LPWA)

4.2 Integrationsansätze

4.2.1 Konsolidierung der Netzwerkkommunikation

TODO - alles spricht OPC UA

4.2.2 Gatewaykommunikation

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

4.3 Kommunikationsstack

4.3.1 Physical Layer

4.3.2 Data Link Layer

4.3.3 Network Layer

4.3.4 Transport Layer und End2End Security

4.3.5 Prozess- und Businesslogik - Application Layer

4.4 Protokolle

4.4.1 etablierte Kommunikationsprotokolle

HTTP

XMPP

MQTT

CoAP

4.4.2 M2M-Kommunikationsprotokolle

OPC UA

MTConnect

4.4.3 weitere? PLCOpen, AutomationML

4.5 Probleme bei Migration alter Systeme

4.5.1 Inkompatibilität

4.5.2 spezielle bzw. proprietäre Protokolle

4.5.3 besondere Anforderungen der Shop-Floor-Ebene

4.5.4 Industrial Ethernet

4.6 Angriffsvektoren

4.6.1 Verschlüsselung

4.6.2 Paketversand

4.6.3 TODO

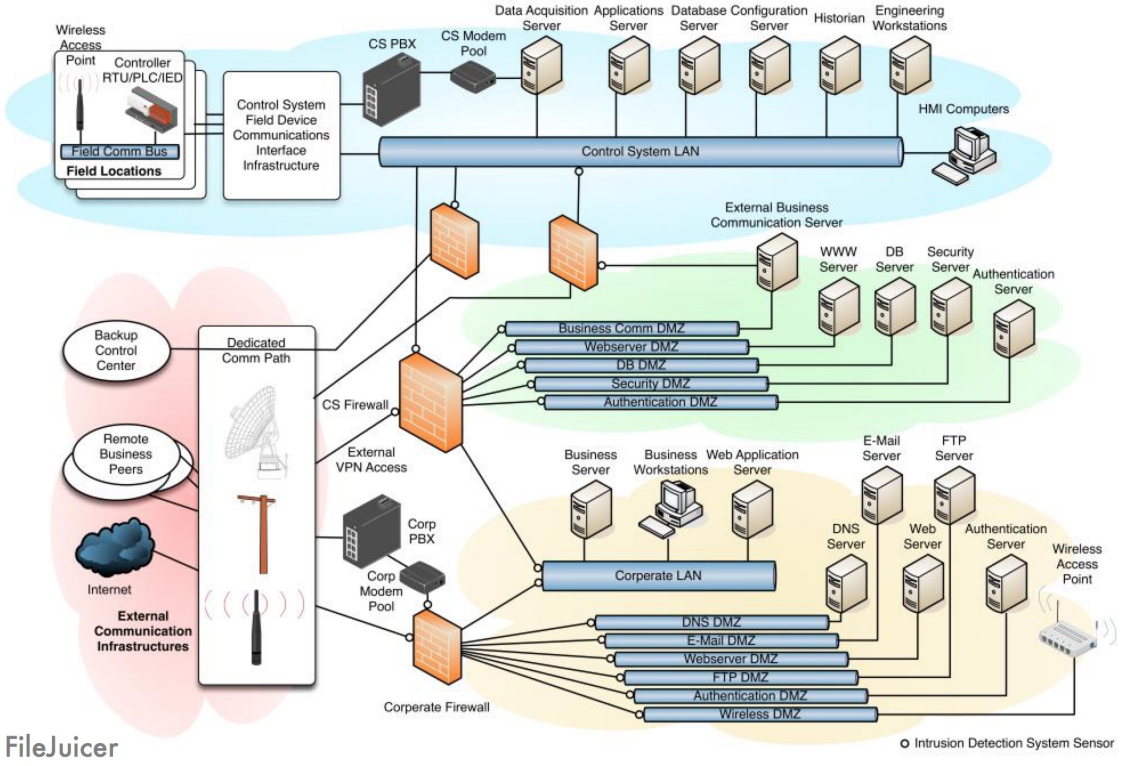

Abbildung 4.1: Defense in Depth Strategie - TODO ref. Kuipers,2006

Kapitel 5

Implementierung

Kapitel 6

Validierung

Kapitel 7

Fazit

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
IIRA	Industrial Internet Reference Architetecture
IIC	Industrial Internet Consortium
IoT	Internet of Things
IIoT	Industrial Internet of Things
IT	Informationstechnik
CPS	Cyber-physisches System
OPC UA	Open Platform Communications Unified Architecture
M2M	Machine to Machine
QoS	Quality of Service
ICS	Industrial Control System
REST	Representational State Transfer
API	Application Programming Interface
IETF	Internet Engineering Task Force
IP	Internet Protocol
DNS	Domain Name System
UDP	User Datagram Protocol
SOA	Service Oriented Architecture
GSM	Global System for Mobile Communications

HSDPA High Speed Downlink Packet Access

LTE Long Term Evolution

LPWA Low-Power Wide Area

HTTP Hypertext Transfer Protocol

CoAP Constrained Application Protocol

XMPP Extensible Messaging and Presence Protocol

MQTT Message Queue Telemetry Transport

VM virtuelle Maschine

PKI Public-Key Infrastructure

Tabellenverzeichnis

Abbildungsverzeichnis

Listings

Literatur

4.0, Plattform Industrie (2016). „Reference Architectural Model Industrie 4.0 (RAMI 4.0): An Introduction“. In: *Publikationen der Plattform Industrie 4.0*. URL: https://www.plattform-i40.de/I40 /Redaktion/DE/Downloads/Publikation/rami40 -eine-einfuehrung.pdf?__blob=publicationFile&v=9.

— (2017). „Sichere Kommunikation für Industrie 4.0“. In: *Publikationen der Plattform Industrie 4.0*. URL: https://www.plattform-i40.de/I40 /Redaktion/DE/Downloads/Publikation/sichere-kommunikation-i40 .pdf?__blob=publicationFile&v=6.

Bundesministerium für Wirtschaft und Energie, BMWi (2016a). „IT-Security in der Industrie 4.0“. In:

— (2016b). „Netzkommunikation für Industrie 4.0“. In: *Platform Industrie 4.0*.

— (2016c). „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.

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.

Torscht, Dipl.-Ing. Robert (2014). „Kommunikation bei Industrie 4.0“. In: *SPS-Magazin, Fachzeitschrift für Automatisierungstechnik*.

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

Weber, Martin (2018). „Ein Konzept für ein virtuelles Security Testbed für eine Industrie 4.0 Umgebung mit prototypischer Implementierung“. In: