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. 55 Seiten.

Minges, Philipp:
TODO - Title EN / Philipp Minges. –
Bachelor Thesis, Mannheim: University of Applied Sciences Mannheim, 2018. 55 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 - Kleinere Losgrößen -> von Einzelmaschine zu Fabrik 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 2016b 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.

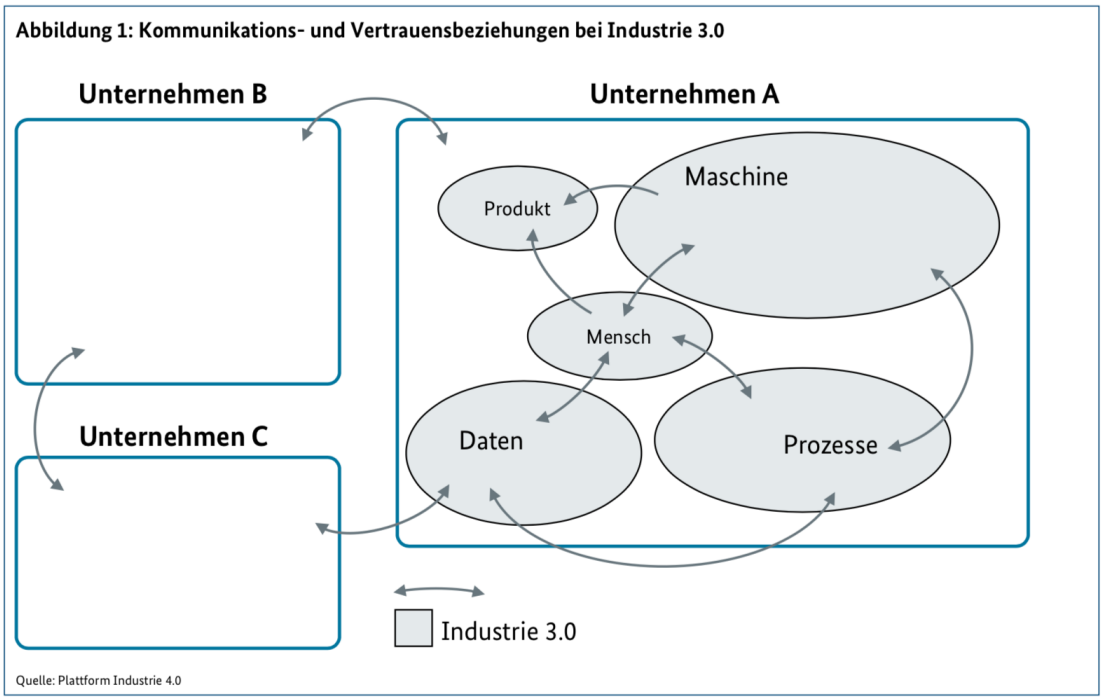

Abbildung 2.1: Kommunikationsbeziehungen in einer Industrie 3.0 Umgebung - TODO ref. sichere unternehmensübergreifende Kommunikation

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.

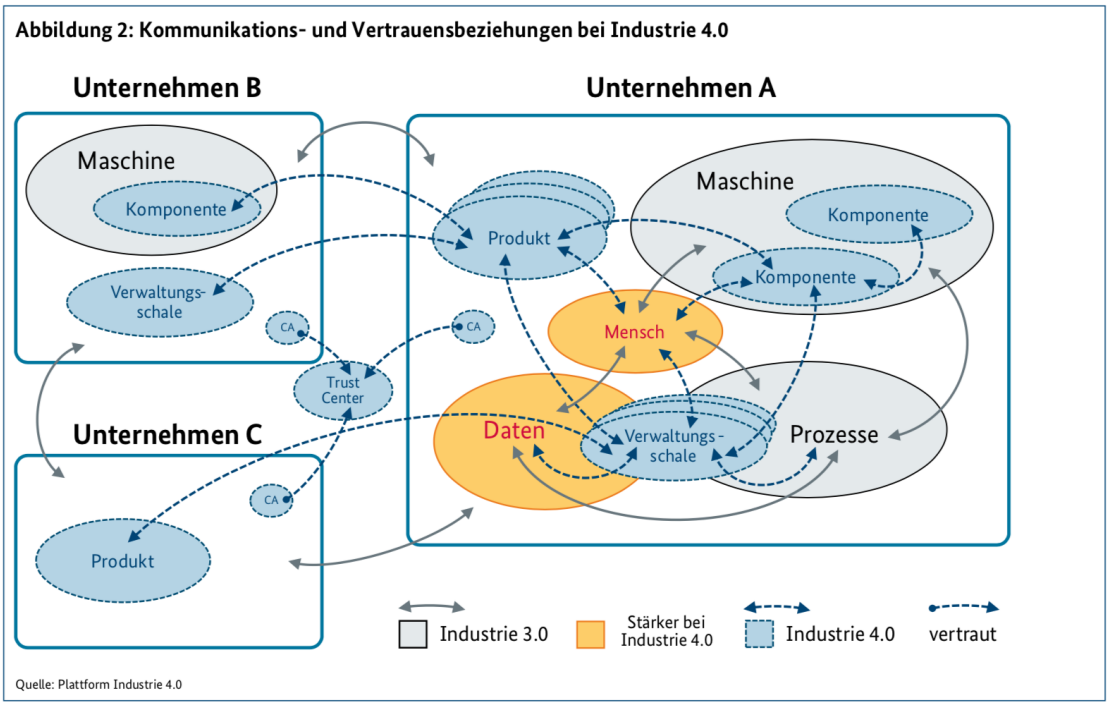

Abbildung 2.2: Kommunikationsbeziehungen in einer Industrie 4.0 Umgebung - TODO ref. sichere Unternehmensübergreifende Kommunikation

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

TODO - bis hierhin auf einen Absatz kürzen -> uninteressant!

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 OPC UA entgegengewirkt. Um vorhandene Anlagen weiterhin nutzen zu können, werden Gateways genutzt. (TODO Trumpf ref.)

2.3 Automatisierungspyramide

TODO - 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.

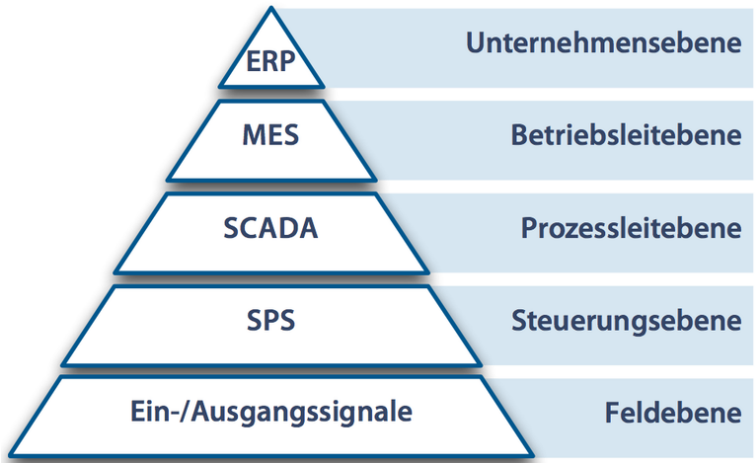

Abbildung 2.3: Automatisierungspyramide - TODO ref. Langmann,2004

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

2.4 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 Plattform Industrie 4.0 2016.

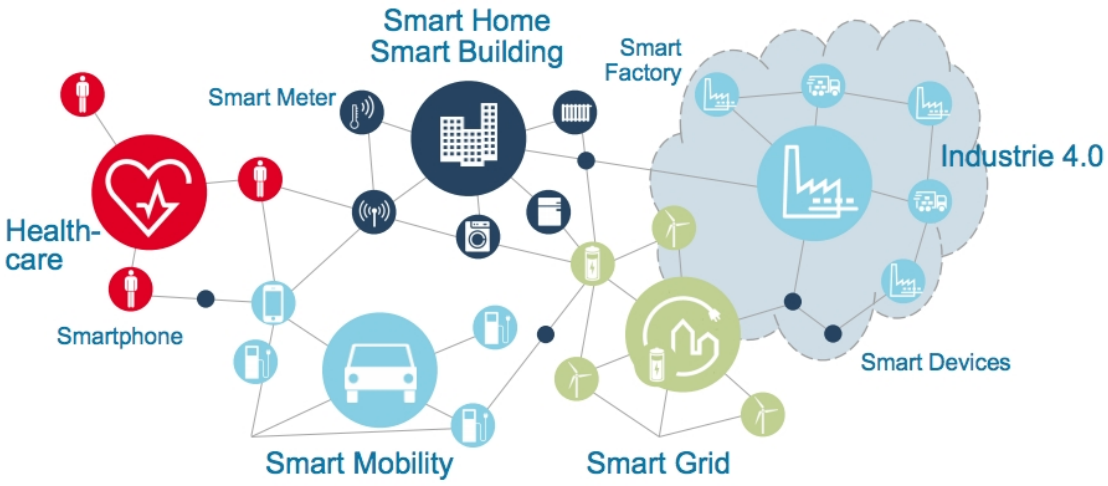

Abbildung 2.4: Das Internet der Dinge - Plattform Industrie 4.0 2016

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.

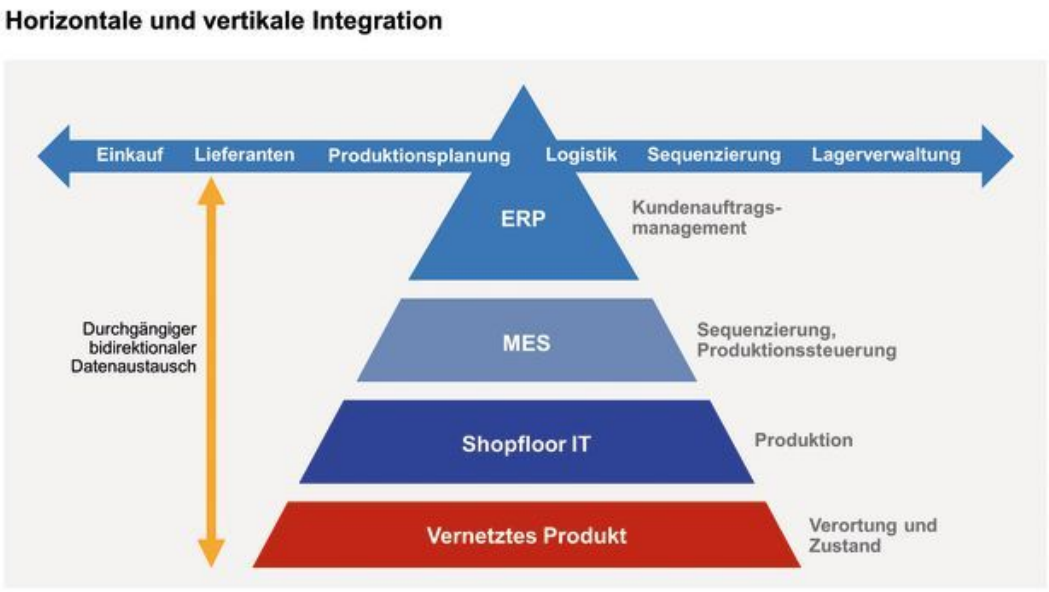

Abbildung 2.5: horizontale und vertikale Integration - TODO ref. HP Industry-of-things siehe bookmark

2.4.1 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.

2.4.2 Industrial Ethernet

TODO - Ethernet für Industrieanlagen

2.5 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.

2.5.1 klassische Schutzziele

TODO - Hierunter fallen die Bereiche Netzsicherheit und Datensicherheit, Sichere Identitäten und funktionale Sicherheit. Netzsicherheit und Datensicherheit werden in der AG3 der Plattform Industrie 4.0 adressiert. 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. - TODO

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

2.5.2 weitere Schutzziele

- Verbindlichkeit/Nichtabstreitbarkeit: TODO - z.B. rechtliche Anforderungen
- Anonymität

2.6 Anforderungen an Industrie 4.0 Umgebungen

Aufgrund der unterschiedlichen Einsatzbereiche von Industrie 4.0 Systemen, unterscheiden sich auch dementsprechend deren Anforderungen. Zusätzlich zu den in Abschnitt 2.5 Grundprinzipien der sicheren Kommunikation beschreiben die Referenzmodelle Referenzarchitekturmodell Industrie 4.0 (RAMI4.0) und Industrial Internet Reference Architetecture (IIRA) grundsätzlich drei Anforderungen an den Übertragungskanal Bundesministerium für Wirtschaft und Energie 2016a.

2.6.1 Sicherheit

- Netzsicherheit und Datensicherheit

- Sichere Identitäten
- funktionale Sicherheit

2.6.2 Verfügbarkeit

Die ständige Verfügbarkeit von Daten und Diensten spielt 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.

TODO - Verfügbarkeit gewährleisten durch...

2.7 Netzwerksicherheit

TODO - Systemsicherheit

- Physische Sicherheit
- Softwaretechnische Sicherheit

TODO - Kommunikationssicherheit

- Sicherheit der Daten während der Übertragung

TODO - Kapitel mit Abschnitt 2.5 zusammenfassen.

2.8 Security by Design

In der Vergangenheit wurden Sicherheitsmechanismen üblicherweise nachträglich und reaktiv in die Entwicklung von Komponenten mit einbezogen. Industrie 4.0

Umgebungen erfordern umfassende Maßnahmen, um die in Abschnitt 2.5 beschriebenen Schutzziele zu erfüllen und eine sichere Kommunikation zu gewährleisten. Dies gilt vor allem für Maschinenbau- und Fertigungsunternehmen, welche häufig proprietäre Individualsoftware zur Steuerung der Maschinen einsetzen DTAG 2016. Aus der Notwendigkeit, Sicherheitsaspekte bereits in die Softwareentwicklung mit einzubeziehen und einen Schutz der Kommunikation zu gewährleisten, hat sich der Begriff Security by Design entwickelt.

Die Methoden und Ziele der Angreifer stehen jedoch auch unter einem ständigen Wandel. Somit ist es nicht möglich, eine Securityimplementierung zu entwickeln und diese wiederholt einzusetzen. Vielmehr ist es notwendig, die Sicherheit durch Security by Design so weit als möglich proaktiv herzustellen und gleichzeitig im Schadensfall flexibel und rasch zu reagieren, um das Schadensausmaß zu begrenzen. Es sind Maßnahmen zur Prävention, Detektion und Reaktion erforderlich. TODO - ref. Umsetzungsstrategie Industrie 4.0

2.9 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 RAMI4.0 und der 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.

2.9.1 TCP/IP Referenzmodell

Unternehmensübergreifende Kommunikation in Industrie 4.0 Umgebungen findet im wesentlichen über IP-Netze statt. Diese basieren auf dem TCP/IP Referenzmodell, welches ein Schichtenmodell ist und die vier Schichten der Internetprotokollfamilie beschreibt. Sie setzen sich aus Application-, Transport-, Internet- und Link-Layer zusammen. Die Schichten des TCP/IP Referenzmodells überlagern sich mit den Schichten des ISO/OSI Referenzmodells.

Application Layer

Die Anwendungsschicht ist für die Übertragung der Nutzdaten zwischen verschiedenen Anwendungen zuständig. Dabei kann es sich um entfernte Anwendungen handeln. Diese sollen sich für den Benutzer verhalten, als würden sie lokal ausgeführt werden.

TODO - Prozess- und Businesslogik

Transport Layer

Die Transportschicht sorgt für die Kommunikation zwischen Prozessen. Die Transportschicht nutzt Ports um verschiedene Dienste zu adressieren. Sie beeinflusst, ob es sich um eine zuverlässige Verbindung (TCP) oder nicht (UDP) handelt.

TODO - End2End Security

Internet Layer

Die Internetschicht wird genutzt, um Daten von einem Teilnehmer im Netzwerk zum anderen zu übertragen. Die Endpunkte im Netzwerk werden durch IP Adressen beschrieben.

Link Layer

Der Bitübertragungsschicht beschreibt die Topologie des Netzwerks. Sie stellt die physikalische Verbindung der Netzwerkteilnehmer zur Verfügung.

TODO - Bild Internetprotokollfamilie TODO - Mit Bild nur kurz erklären und referenzieren, Überschriften entfernen.

2.9.2 Industrie 4.0 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. Plattform Industrie 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.

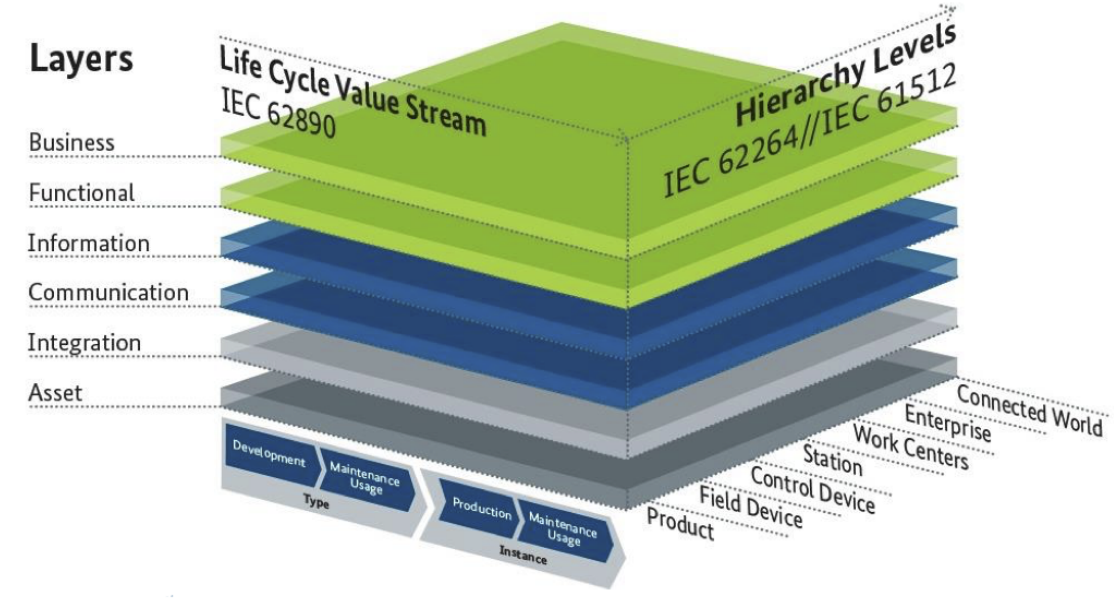

Abbildung 2.6: RAMI 4.0 - Plattform Industrie 4.0 2016

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 2016a

TODO - Kommunikation beschreiben - Assets, Verwaltungsschale

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

Das IIC veröffentlichte im Jahr 2015 die IIRA. Sie beschreibt eine standardbasierte, offene Referenzarchitektur für IIoT, welches auf dem Industrial Internet Architecture Framework (IIAF) basiert. Das IIAF unterstützt die Unternehmen bei der Entwicklung, Dokumentation, Kommunikation und Bereitstellung von Systemen im IIoT Bereich Industrial Internet Consortium 2017. Die Beschreibung der Architektur findet mit einem hohen Maß an Abstraktion statt, um das breite Feld der verschiedenen Industrielösungen abdecken zu können und standardisierte Vorgehensweisen bereitzustellen.

TODO - Diese beinhalten niedrige Latenzen und Schwankungen, einen hohen Durchsatz, Skalierbarkeit, Ausfallsicherheit, Datensicherheit und ‚Quality of Service' (QoS)

Framework

Das IIAF folgt der Vorgehensweise des ISO/IEC/IEEE Standard 42010:2011 Systems and Software Engineering–Architecture Description. Concern, Stakeholder und Viewpoint werden als Architecture Frame dargestellt. Die Views und Models als ihre Architecture Representations.

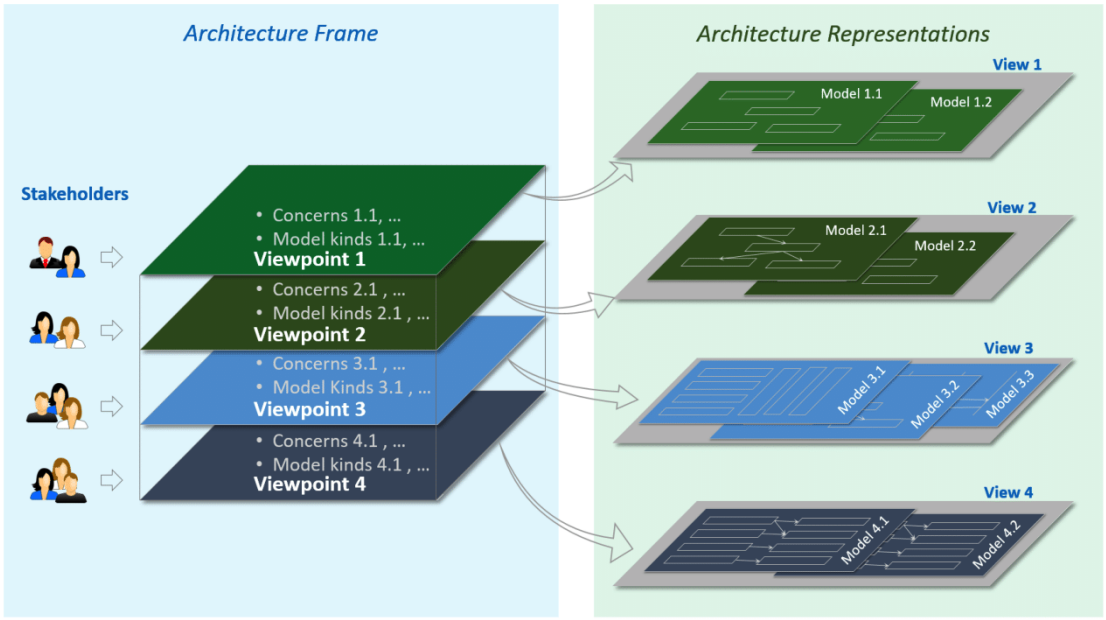

Abbildung 2.7: IIRA - Architekturframework

Referenzarchitektur

Die IIRA ist das Ergebnis der Anwendung des IIAF auf die IIoT Systeme eines Unternehmens. Sie beschreibt bekannte Risiken beim Betrieb von IIoT Systemen in verschiedensten Industriebereichen und Klassifiziert diese mit ihren zugehörigen Stakeholdern in Viewpoints. Anschließend dient die Referenzarchitektur der Beschreibung, Analyse und Behebung dieser Bedenken/Risiken in den einzelnen Viewpoints.

Abbildung Abbildung 2.8 beschreibt die grundlegende Idee und den Aufbau der IIRA.

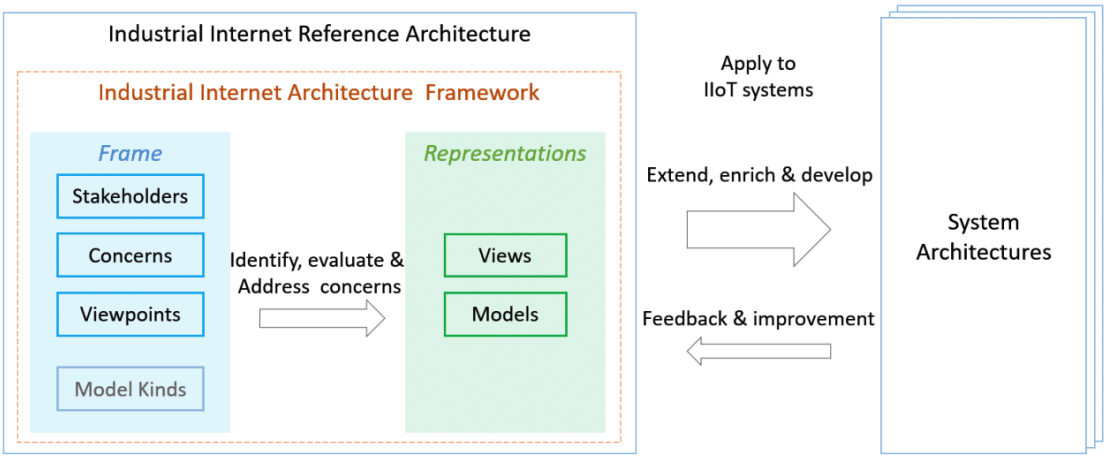

Abbildung 2.8: IIAF/IIRA - Übersicht

2.9.3 Protokollstandards

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. Hierbei haben sich bzgl. der Referenzarchitekturen RAMI4.0 und IIRA die M2M-Kommunikationsstandards OPC UA und Data Distribution Services (DDS) etabliert.

OPC UA

Die OPC UA ist ein plattformunabhängiger International Electrotechnical Commission (IEC) Standard, welcher die M2M-Kommunikation zwischen unterschiedlichen Geräten und Systemen der Industrie über verschiedene Netzwerktopologien bereitstellt. Der Standard basiert auf dem Informationsmodell, definiert eine SOA und ermöglicht eine robuste und sichere eine Ende zu Ende Kommunikation nach den Vorschriften der TODO ref. - DIN. Er erfüllt die Anforderungen des RAMI4.0 und etabliert sich zunehmend im Maschinen- und Anlagenbau.

Der Standard wird in 14 geschichteten Spezifikationen beschrieben, welche sich in die Bereiche Core, Access Type und Utility unterteilen lassen. Dabei stellen die Spezifikationen 1-7 sowie 14 die Kernfunktionalitäten des Standards dar. Sie beschreiben die Struktur des OPC Addressraums und der Dienste, die darauf operieren. Die Spezifikationen 8-11 wenden diese Kernfunktionalitäten auf spezifische OPC COM Spezifikationen, wie Data Access (DA), Alarms and Events (A&E) und Historical Data Access (HDA) an. Die Teile 12 und 13 beinhalten Mechanismen zur Discovery von Systemen und beschreiben Möglichkeiten der Datenaggregation.

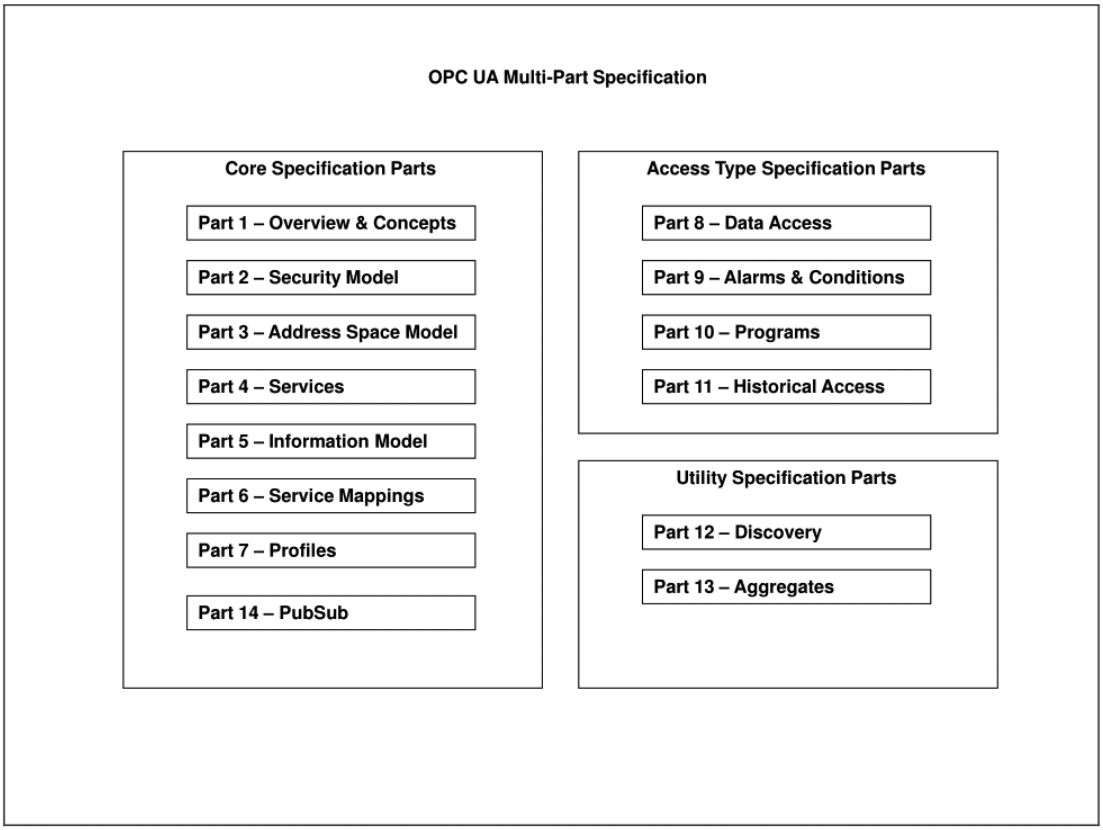

Abbildung 2.9: OPC UA Multi-Part Specification - Foundation 2018a

Die OPC UA stellt ein Informationsmodell mit Hilfe einer SOA bereit. Das Lesen- und Schreiben von Daten in Industrie 4.0 Umgebungen findet durch die Verwaltungsschale der Komponenten statt. Diese wird im OPC UA Stack durch den Addressraum beschrieben. Der Adressraum wird zur Speicherung von Knoten, deren Attribute und Referenzen zu anderen Knoten genutzt. Der Addressraum und das Informationsmodell von OPC UA werden in den Spezifikationsteilen 3 **opcpc3** und 5 Foundation 2018b beschrieben.

Im folgenden Abschnitt wird sich auf die Darstellung der Bestandteile von OPC UA, welche an der Netzwerkkommunikation beteiligt sind, beschränkt.

Kommunikationsmodell

OPC UA ermöglicht die Kommunikation der Assets über ein Client-Server Pattern. Die Architektur setzt sich dabei aus einem OPC UA Client und einem OPC UA Server zusammen. Der OPC UA Server stellt verschiedene Funktionen bereit, auf welche der OPC UA Client mit Hilfe eines Request zugreifen kann. Des Weiteren ist es möglich durch einen Request des OPC UA Clients ein Element des Servers beobachten zu lassen, um bei Änderungen vom Server benachrichtigt zu werden. Um die Kommunikation zwischen OPC UA Servern zu gewährleisten, ist es möglich einen OPC UA Client in einen OPC UA Server zu integrieren. In der Grafik Abbildung 2.10 wird das Client-Server Pattern der OPC UA Spezifikation schematisch dargestellt. Die linke Seite der Grafik beschreibt die Kommunikation zwischen einem Client und einem Server mit eingebettetem Client. In der rechten Seite der Grafik findet die Kommunikation zwischen dem eingebetteten Client und einem OPC UA Server statt.

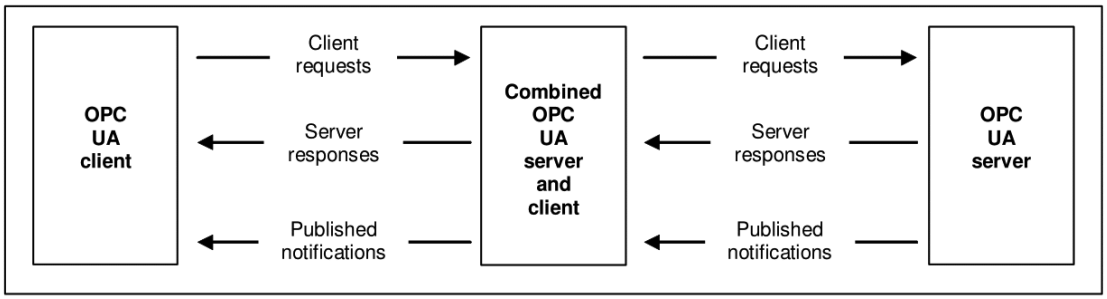

Abbildung 2.10: OPC UA Client-Server Architektur - Foundation 2018a

Im Jahr 2018 wurde der Standard zusätzlich um eine Spezifikation für das Publish-Subscribe Pattern - TODO ref. - erweitert Hoppe 2018. Das Publish-Subscribe Mo-

dell ermöglicht die Nutzung von OPC UA in Wide Area Network (WAN) Umgebungen durch die Verwendung von Protokollen wie MQTT und Advanced Message Queuing Protocol (AMQP), während die Ende zu Ende Sicherheit und die standardisierte Datenmodellierung erhalten bleiben. Das Publish-Subscribe Modell ermöglicht die Verwendung des fehlertoleranten Datagramms User Datagram Protocol (UDP), wodurch geringe Latenzen ermöglicht werden können.

Kommunikationswege

Die Kommunikation zwischen OPC UA Komponenten findet auf der Anwendungsschicht des Transmission Control Protocol (TCP)/Internet Protocol (IP) Referenzmodells statt und basiert auf dem Protokoll TCP/IP. Grundsätzlich stellt OPC UA die drei Kommunikationswege Binary, Hybrid und Webservice bereit.

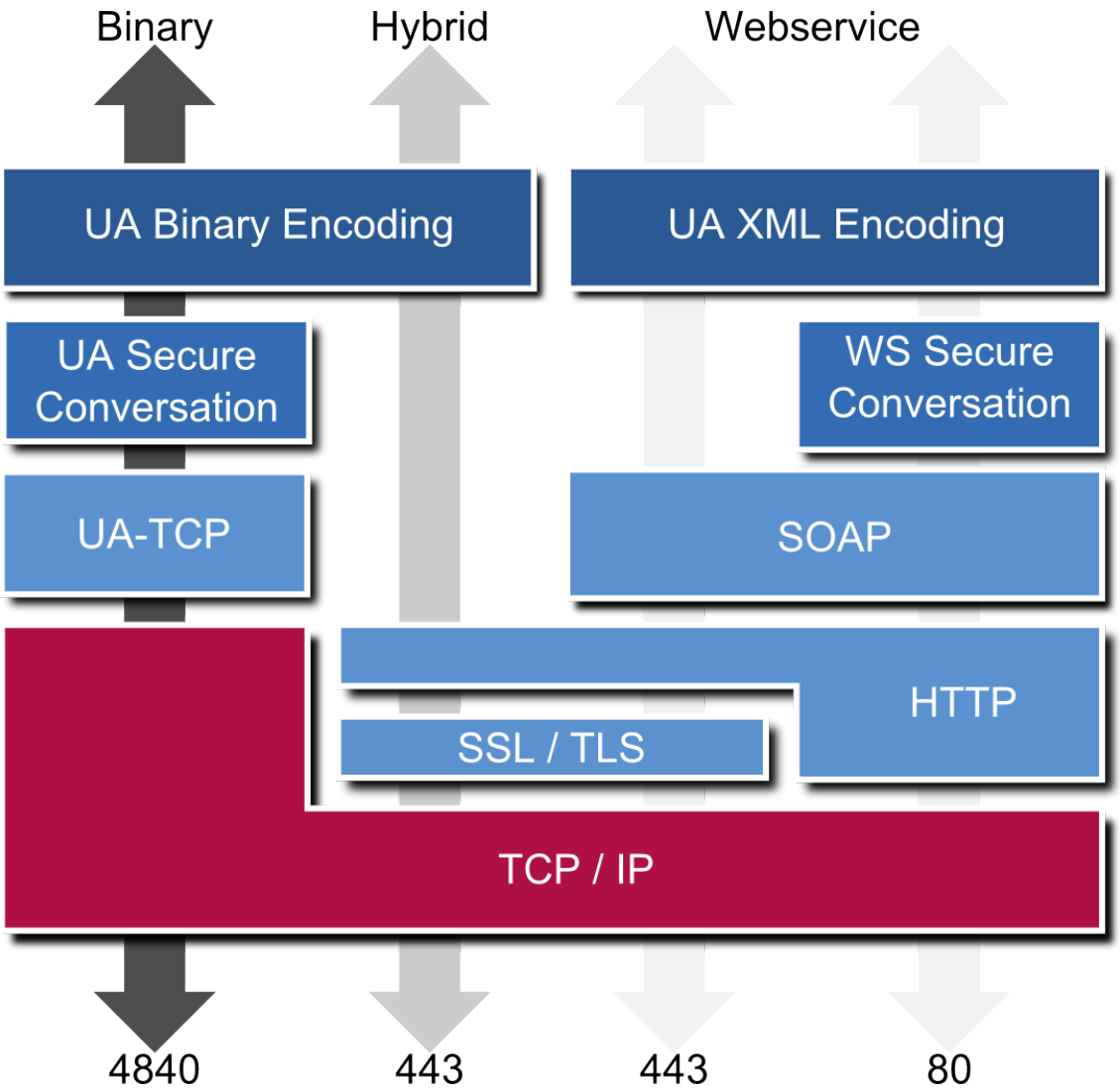

Abbildung 2.11: OPC UA Kommunikationswege

TODO - Binary TODO - Hybrid TODO - Webservice

Sicherheit TODO - siehe OPC UA Part 2

DDS

DDS ist ein offener Standard der Open Management Group (OMG) und stellt eine **MOM!** (**MOM!**) zur Kommunikation in hochdynamischen verteilten Systemen dar. Er wurde für niedrige Latenzzeiten, einen hohen Datendurchsatz und eine skalierbare, belastbase und sichere Datenverteilung entwickelt, um die Kommunikation in Steuerungs- und Kontrollaufgaben zu realisieren. Der beschriebene Standard deckt alle Anforderungen der IIRA ab und hat sich bereits in industriellen Systemen etabliert. Gegenüber OPC UA beschreibt DDS eine dezentralisierte Architektur. Es bietet ein Konnektivitäts-Framework, welches ein Kommunikationsparadigma basierend auf einem Shared Data Model, einen Standard für die Definition domain-spezifischer Informationsmodelle, ein starkes Sicherheitsmodell, Discovery und reichhaltige APIs beinhaltet. Die Kommunikation findet direkt vom Publisher zum Subscriber statt. Dabei werden Latenzzeiten reduziert und durch die Nutzung von Multicast die Netzlast beim Bereitstellen von Informationen an viele Empfänger gering gehalten. Es ist möglich die **MOM!** DDS in eine OPC UA Architektur zu integrieren und mit dem Informationsmodell nutzen.

2.10 Testsystem

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

2.10.1 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.

2.10.2 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 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. Die zu analysierenden Komponenten werden in Hard- und Softwarekomponenten gegliedert.

3.1.1 Hardware

TODO

Übertragungskanal

Der Übertragungskanal beschreibt die Bitübertragungsschicht. 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. Aufgrund der Durchführung der Analyse in einem virtuellen Testsystem, werden die Auswirkungen der Form des Übertragungskanals bei der Analyse der Kommunikation nicht beachtet.

3.1.2 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.

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 bereitstellen sollen.

TODO - CoAP, MQTT

3.2 Abgrenzung

Die IIRA ist ein anerkannter, in der Industrie verbreiteter Standard. Da die Analyse der Netzwerksicherheit am in Abschnitt 2.10 beschriebenen Testsystem durchgeführt werden soll, welches den Kommunikationsstandard OPC UA implementiert, wird sich im weiteren Verlauf der Thesis ausschließlich auf die in der IEC 62541 beschriebene Architektur RAMI4.0 als Referenzmodell zur Analyse bezogen. Es werden Bedrohungen in Industrie 4.0 Umgebungen beschrieben, eine Analyse der Übertragungsmedien und Infrastruktur durchgeführt und die im Testsystem verwendeten Protokolle mit Bezug auf ihre Anforderungen im Bereich der Netzwerksicherheit untersucht. Um verschiedene Praxisszenarien darzustellen, wird das Testsystem um für die Analyse benötigte, zusätzliche Komponenten erweitert.

3.3 Vorgehensweise

Die Analyse der Netzwerkkommunikation der unteren Schichten (Internet- und Link Layer) des im Unterabschnitt 2.9.1 beschriebenen TCP/IP Referenzmodells wird auf Basis der in Abschnitt 2.5 erläuterten Schutzziele durchgeführt. Die oberen Schichten (Transport- und Application Layer) werden in der Testumgebung durch das M2M-Protokoll OPC UA realisiert. Hierbei dient die Spezifikation des Protokolls als Grundlage der Analyse. Aus der Spezifikation ergeben sich die bei der Kommunikation für die IT-Sicherheit zuständigen Komponenten von OPC UA. Die-

se werden nach des Anforderungen des TODO - ref. BSI ICS Security Kompendium und FIRST CVSS v2.0 - auf Sicherheitslücken und Widersprüche untersucht. Bei der Analyse auftretende, mögliche Schwachstellen werden in einer vorhandenen, prototypischen Industrie 4.0 Testumgebung Weber 2018 implementiert und nachgewiesen. Sicherheitslücken, welche durch Fehlkonfiguration 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

Im folgenden Kapitel wird die Analyse der Netzwerksicherheit in Industrie 4.0 Umgebungen durchgeführt. Es wird eine Beschreibung und Einordnung der Bedrohungen von Industrie 4.0 Systemen anhand der in Abschnitt 2.5 genannten Schutzziele und der aktuellen Industriestandards Abschnitt 2.9 durchgeführt. Dabei wird nach den Schichten des TCP/IP Referenzmodells vorgegangen, um eine strukturierte Vorgehensweise zu ermöglichen und ein ganzheitliches Bild der Netzwerkkommunikation zu erhalten. Die Analyse wird mit Hilfe des Industrie 4.0 Testsystems (Weber 2018) durchgeführt. Dieses wird genutzt und erweitert, um verschiedene Szenarien darzustellen und die Sicherheit der Netzwerkkommunikation mit Hilfe verschiedener Softwaretools und Vorgehensweisen zu analysieren.

4.1 Bedrohungen

Die vierte industrielle Revolution, das IIoT und dessen Vielzahl an aktiven und passiven Elementen stellen in ihrer Komplexität eine große Herausforderung für die IT-Sicherheit dar. Einerseits muss die Sicherheit der laufenden Software, der Infrastruktur, Anwendungs- und Rechnersysteme gewährleistet werden, andererseits muss die Betriebssicherheit der Geräte und Anlagen, welche mit dem Internet verbunden sind sichergestellt werden. Das Management der IT-Sicherheit in Industrie 4.0 Netzen geht über Unternehmensgrenzen hinweg, da Netze und Systeme für Kunden, Lieferanden und Partner bereitgestellt werden (DTAG 2016). Somit hat sich auch die Bedrohungslage der Netze geändert. Das Bundesamt für Sicherheit

in der Informationstechnik (BSI) beschreibt die Top 10 Bedrohungen und deren Folgen für ICS in Bundesamt für Sicherheit in der Informationstechnik 2016.

1. Social Engineering und Phishing
2. Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware
3. Infektion mit Schadsoftware über Internet und Intranet
4. Einbruch über Fernwartungszugänge
5. Menschliches Fehlverhalten und Sabotage
6. Internet-verbundene Steuerungskomponenten
7. Technisches Fehlverhalten und höhere Gewalt
8. Kompromittierung von Extranet und Cloud Komponenten
9. Denial of Service (DoS) und Distributed Denial of Service (DDoS)
10. Kompromittierung von Smartphones im Produktionsumfeld

Um die in Abschnitt 2.5 genannten Schutzziele umzusetzen, ist es notwendig einen größtmöglichen Schutz gegen diese Bedrohungen bereitzustellen. Die Sicherheit eines Gesamtsystems kann nicht nur an einer einzigen Stelle im Kommunikationsstack hergestellt und gewährleistet werden. Es müssen alle Stellen des Kommunikationsstacks gegen Bedrohungen abgesichert werden (Plattform Industrie 4.0 2017). Dafür müssen die Netzwerkinfrastruktur und die eigentliche Kommunikation im Netzwerk gesichert werden. Dies geschieht durch die Abschottung von Systemen, die Einschränkung von Zugangsberechtigungen, die Härtung der Sicherheit der genutzten Komponenten sowie den Einsatz von geeigneten Netzwerkprotokollen und Verschlüsselungsverfahren.

4.2 Netzzugangsschicht

Die Netzzugangsschicht stellt die erste Instanz der Kommunikation in einem Netzwerk dar. Sie beinhaltet das Übertragungsmedium sowie die Topologie, in welcher die Kommunikation stattfindet. Das Übertragungsmedium bestimmt die Form der Signalübertragung. In Industrie 4.0 Netzen können 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 und die Integrität der Daten bei der Übertragung über große Entfernungen zu gewährleisten. Dominante Technologien dieser Schicht sind Institute of Electrical and Electronics Engineers (IEEE) 802.3 (Ethernet)[1], IEEE 802.11 (Wireless LAN)[2] und IEEE 802.15.4[3] (Plattform Industrie 4.0 2017).

Aus zeitlichen Gründen wird keine weitere Analyse der verschiedenen Übertragungsmedien und deren Protokolle durchgeführt und sich im Rahmen dieser Thesis auf die Analyse von kabelgebundenen Ethernet-basierten Netzen, deren Topologie und Kommunikation beschränkt.

4.2.1 physikalischer Zugang

Die Netzzugangsschicht beinhaltet als einzige Schicht des TCP/IP Referenzmodells nicht nur die verwendeten Protokolle zur Signalübertragung, sondern auch die physikalischen Gegebenheiten des Übertragungsmediums. Die Sicherheit dieser Netzwerkschicht beinhaltet somit nicht nur die verwendeten Techniken, sondern auch die physische Sicherheit der Systeme. Sie wird durch den Zugang zur Hardware dargestellt und besitzt eine große Bedeutung, um unbefugte Eingriffe in das Netzwerk zu verhindern. Die Sicherheit dieser Systeme wird durch die physikalische Abschottung mit Hilfe von abschließbaren Serverschränken, genereller Zugangskontrolle sowie der Abschaltung von Ports an Netzwerkkomponenten oder Endsystemen gewährleistet. (Plattform Industrie 4.0 2017)

4.2.2 Topologie

Die Topologie eines Netzwerks bestimmt den physikalischen Weg der Netzwerkpakete über die Leitungen. In der Industrie werden je nach Anwendungsfall verschiedene Topologien, wie Punkt-zu-Punkt-, Bus-, Stern- oder auch Hybride-, zur Kommunikation im Netzwerk genutzt. Jede dieser Netzstrukturen bietet Vor- und Nachteile bzgl. Durchsatz, Administrationsaufwand und Skalierbarkeit (Burke 2013).

[1] Link zu IEEE 802.3
[2] Link zu IEEE 802.11
[3] Link zu IEEE 802.15.4

Um die Grundidee der Industrie 4.0, die unternehmensübergreifende, intelligente Vernetzung von Produktionsressourcen umzusetzen, ist eine einheitliche Kommunikation notwendig. Industrie 4.0 Netze kommunizieren über TCP/IP Verbindungen und basieren auf dem *Ethernet*[4] Protokoll. Sie werden in über Gateways miteinander verbundenen Sterntopologien realisiert. Die Topologie eines Netzwerks bietet Schnittstellen, um Einfluss auf das Netzwerk zu nehmen. Selbst unbefugter Zugriff auf der untersten Schicht des TCP/IP Referenzmodells kann die Sicherheit der Datenübertragung oder die Funktionsweise des Netzwerks beeinträchtigen.

TODO - Beschreibung von Angriffen durch Eingriff auf Hardware; Verweis auf Anwendungsszenario in Internetschicht. TODO - Ansatz: Berechnung von Latenzzeiten, RTT, Auswirkungen aufzeigen, Congestion Window, Sliding Window

4.2.3 vertikale Integration bestehender Komponenten

TODO - Feldbus, SPS, Anlagensteuerung (SCADA) -> Bindeglied zu IP-Netzen TODO - Ansatz: OPC UA Clients sind Gateways in Testumgebung -> Verweis auf Analyse in höheren Schichten TODO - Vieles in Praxis nicht umsetzbar darum größtmöglicher Schutz durch Abschottung.

4.3 Internetschicht

Auf der Internetschicht findet die Vermittlung der Datenpakete zwischen den Teilnehmern im Netzwerk statt. Auf dieser Schicht hat sich, mit dem Siegeszug des Internets, IP zum Standard für Netzwerkübergreifende Rechnerkommunikation durchgesetzt (Christoph Meinel 2011). Dies gilt auch für die immer komplexer werdenden Industrienetzwerke und die Industrie 4.0.

Zu den Aufgaben der Internetschicht gehört das Bereitstellen von Adressen, das Routing, die Fragmentierung von Datenpaketen zur Übertragung im Netzwerk sowie die Sicherstellung der Dienstgüte. Um Routing und Adressvergabe in IP-Netzen zu realisieren, werden die Dienste DNS und Dynamic Host Configuration Protocol (DHCP) genutzt. Das **IPAM!** (**IPAM!**) und die Zuordnung der physikalischen Hardware zur logischen IP-Adresse erfolgt mit Hilfe des ARP. Da die Kommunika-

[4] Link zu IEEE Ethernet

tion in einem IP-Netz ohne diese Dienste und Protokolle nicht möglich ist, stellen sie einen wichtigen Bestandteil der Kommunikation im Netzwerk da und müssen vor Sabotage geschützt werden.

4.3.1 DNS

DNS wird von der IETF in den Request for Comments (RFC) 1034[5], 1035[6], 2181[7] und 2782[8] beschrieben und verwaltet. Es stellt einen hierarchischen Verzeichnisdienst für IP-Netze zur Verfügung.

Eine der Hauptaufgaben des DNS ist der *forward lookup*. Hierbei werden Domain- bzw. Hostnamen in IP-Adressen übersetzt. Das Zusammenspiel eines hierarchischen Verzeichnisdienstes und der Namensauflösung bietet Angriffsfläche zum Eingriff auf die Kommunikation im Netzwerk. Im folgenden werden bekannte Angriffsformen auf den DNS Dienst und deren Auswirkungen auf das Netzwerk beschrieben.

DNS Spoofing

Die Angriffsmethode des DNS Spoofing verfolgt, wie *Cache Poisoning*[9], das Ziel gefälschte Resource Record (RR) in den DNS Cache des Opfers einzuschleusen. Während das *Cache Poisoning* aus einer Softwareschwachstelle hervorging, bei der zusätzliche, gefälschte DNS Einträge zu korrekten DNS Antworten hinzugefügt wurden und somit der Cache eines Nameservers kompromittiert wird, befindet sich der Angriffsvektor beim DNS Spoofing in der Fälschung von DNS Antworten. Der Header der Netzwerkpakete werden mit Hilfe von *IP Spoofing*[10] so manipuliert, dass sie vorgeblich vom *authorativen* Nameserver stammen.

Um DNS Spoofing erfolgreich durchzuführen muss die gefälschte DNS Response des Angreifers vor der Antwort des zuständigen Nameservers beim angegriffenen DNS Resolver eintreffen. Sobald der physikalische Zugang zum Netzwerk gewährleistet ist, können die Latenzzeiten der gefälschten Pakete im Netzwerk sehr gering

[5] Domain Names – Concepts and Facilities
[6] Domain Names – Implementation and Specification
[7] Clarifications to the DNS Specification
[8] A DNS RR for specifying the location of services (DNS SRV)
[9] Cache Poisoning - iwas
[10] IP Spoofing bezeichnet das Versenden von IP Paketen mit gefälschter Absender-IP

gehalten werden. Ist dies nicht möglich, kann mit Hilfe eines DoS bzw. DDoS Angriffs (siehe Abschnitt 4.3.1) auf den zuständigen Nameserver, dessen Antwortzeit beeinflusst werden. Des weiteren muss die ID im DNS Header mit der des Request übereinstimmen. Dies kann am Testsystem am Beispiel der Namensauflösung des OPC UA Discovery Servers mit Hilfe des Netzwerkanalysetools Wireshark[11] nachgewiesen werden.

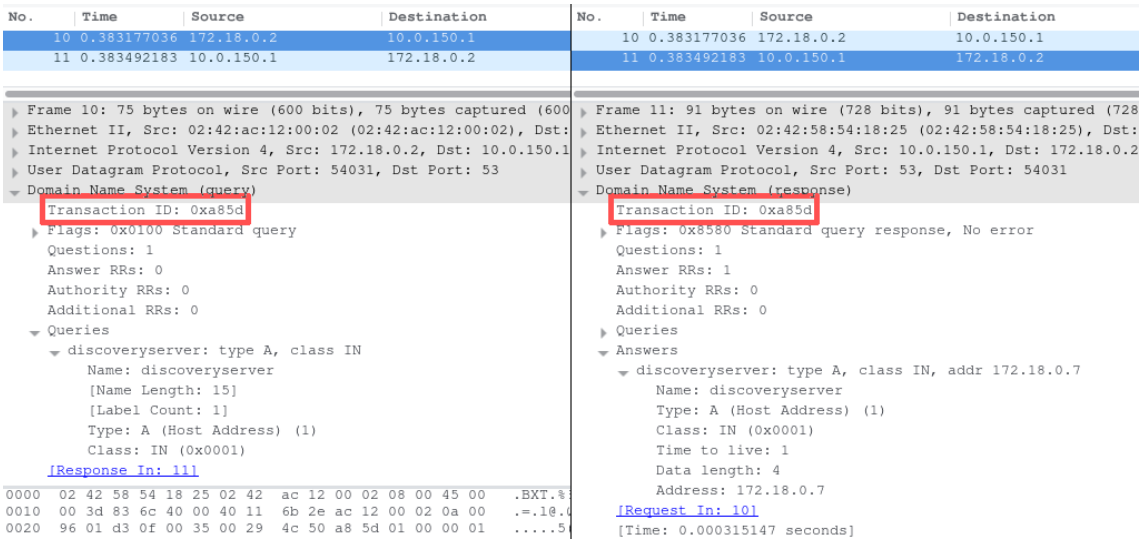

Abbildung 4.1: Wireshark - ID im DNS Header

[11] Link zu Wireshark

In der Darstellung ist auf der linken Seite ein DNS Request des OPC UA Discovery Servers und dessen DNS Header mit ID zu erkennen. Auf der rechten Seite ist die Antwort des im Netzwerk vorhandenen authorativen Nameservers zu sehen.

Schutzmaßnahmen sind DNSSEC und zufällige Informationen Die Auswirkungen eines solchen Angriffs ...

DNS Amplification

DoS/DDoS

DNS Fast Fluxing

Im Gegensatz zu den bisher beschriebenen Angriffsformen wird das Fast Fluxing zur Spionage von Daten genutzt.

4.3.2 DHCP

In Kapitel Abschnitt 5.1 wird die Erweiterung des Testsystems (Weber 2018) beschrieben und Auswirkungen eines Eingriffs auf das Netzwerk in der Netzzugangsschicht und gleichzeitige Manipulation der Internetschicht des TCP/IP Referenzmodells dargestellt.

4.3.3 ARP

4.3.4 QoS

Eine Industrie 4.0 Netzwerkinfrastruktur kann aufgrund der unterschiedlichen Anforderungen an die Systeme auf verschiedenste Weisen ausgeprägt sein. Die Heterogenität der Komponenten im Netzwerk und deren Anforderungen an die Kommunikation auf der vertikalen Ebene der Automatisierungspyramide Abschnitt 2.3 stellen eine Herausforderung für die Sicherheit der Datenübertragung dar und können die Umsetzung eines Netzwerks beeinflussen. Des Weiteren erstrecken sich Industrie 4.0 Umgebungen über weite Distanzen (Metropolitan Area Network (MAN), WAN, Global Area Network (GAN)) und sind somit auch von physikalischen Gegeben-

heiten wie Latenz und Jitter betroffen. Diese Erscheinungen müssen berücksichtigt werden, um eine fehler- und verlustfreie, sichere Kommunikation zu gewährleisten.

Für die Beurteilung und Bereitstellung der Dienstgüte in IP-Netzen müssen die Übertragungsgüte der Netzzugangsschicht sowie die übertragungstechnischen Parameter der Internetschicht (IP-Ebene) betrachtet werden. In IP-Netzen wird der Einfluss auf die QoS in den 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

TODO - ref. Torscht 2014 und IEEE 802.1p

4.3.5 IPsec

Die Internetschicht bietet mit IPsec eine Möglichkeit den Datenfluss, im Vergleich zu anderen Verschlüsselungsverfahren, die Kommunikation bereits auf der Internetschicht des TCP/IP Referenzmodells zu sichern.

4.4 Transportschicht

4.4.1 TCP

4.4.2 UDP

4.4.3 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.

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. IP und DNS zur Kommunikation bereitstellt. Des weiteren müssen beide Systeme diese Dienste und Protokolle unterstützen.

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.

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 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 (QoS) sicherzustellen oder dieses Modell nur für fehlertolerante Kommunikation wie z. B. Audio- und Video-Anwendungen oder Businessprozesse zu nutzen.

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. Plattform Industrie 4.0 2017

TODO - Bilder -> sichere-kommunikation-i40 TODO - mehr Analyse. TODO - Verweis auf **??**, da Tests mit OPC UA auch Transportschicht umfassen. -> PubSub, Client-Server = UDP/TCP

4.5 Anwendungsschicht

TODO - DDS und OPC UA TODO - Ansatz: Wireshark an Bridge der Testumgebung im Sternnetzwerk und Druckerkomponente oder andere manipulieren; andere Protokolle von Feldebene an Switch auslesen; vielleicht hier nur beschreiben und in den höheren Schichten durchführen mit CoAP oder MQTT -> OPC UA Komponenten sind Gateway

4.5.1 Integrationsansätze

Die Grundlage der Industrie 4.0 Kommunikation ist ein standardisierter Datenaustausch über alle Schichten der Automatisierungspyramide hinweg. Dabei stellt der IEC-Standard OPC UA einen vielversprechenden Ansatz für einen standardisierten Informationsaustausch über Unternehmensgrenzen hinweg dar. Jedoch müssen auch bestehende Systeme in die Industrie 4.0 Kommunikation integriert werden. Dies führt häufig zu Problemen, da diese Systeme proprietäre Protokolle nutzen, besondere Anforderungen wie Echtzeitkommunikation besitzen oder gar keine Schnittstelle bereitstellen. Es bestehen grundsätzlich zwei Ansätze zur Integration dieser Anlagen. TODO - ref.

Konsolidierung der Netzwerkkommunikation

TODO - Eine Möglichkeit der Entwicklung zu einer Smart Factory ist die Konsolidierung die Netzwerkkommunikation. Fokus auf OPC UA, da standardisiert. TODO - neue Netze/Factories können so geplant werden, dass die Maschinen die benötigten Schnittstellen bereitstellen. Ansatz: teuer, aufwendig bzw. nicht möglich, da embedded System bzw. keine Ressourcen oder keine Schnittstellen

Gatewaykommunikation

Eine Alternative zur Umstellung der bestehenden Systeme stellt die Kommunikation über Gateways dar. Hierbei gibt es mehrere Softwarelösungen, welche unterschiedliche Ziele verfolgen. Es werden Systeme zur Anlagenoptimierung (TODO - ref. SePiA.Pro), der Bereitstellung einer offenen, branchenübergreifenden Plattform mit diversen Smart Services wie Datenanalyse und Flottenmanagement (TODO - ref. Siemens Mindsphere, DeviceInsight) und dem herstellerübergreifenden Gerätemanagement (AXOOM) entwickelt **acatec2016**. Die Systeme sammeln und verwalten die Daten der Anlagen an zentraler Stelle und stellen sie im Netzwerk zur Verfügung. Der Einsatzmöglichkeiten dieser Softwarelösungen sind von den vorhandenen Schnittstellen der Anlagen abhängig und benötigen eine individuelle Konfiguration um den unterschiedlichen Anforderungen der Industrielandschaft gerecht zu werden.

TODO - Im folgenden Abschnitt wird die Umsetzung der Kommunikation über eine digitale Serviceplattform am Beispiel von AXOOM dargestellt.

4.5.2 AXOOM

TODO - Gründe der Wahl von AXOOM: TODO - 2016 Innovationspreis deutsche Indsutrie TODO - unterstützt Optimierung der Wertschöpfungskette -> ERP-, MES Kommunikation über "bekannte", offene Schnittstellen (REST usw.) TODO - unterstützt Anbindung von IoT. Analyse und Visualisierung von Daten -> Kommunikation über spezielle Schnittstellen

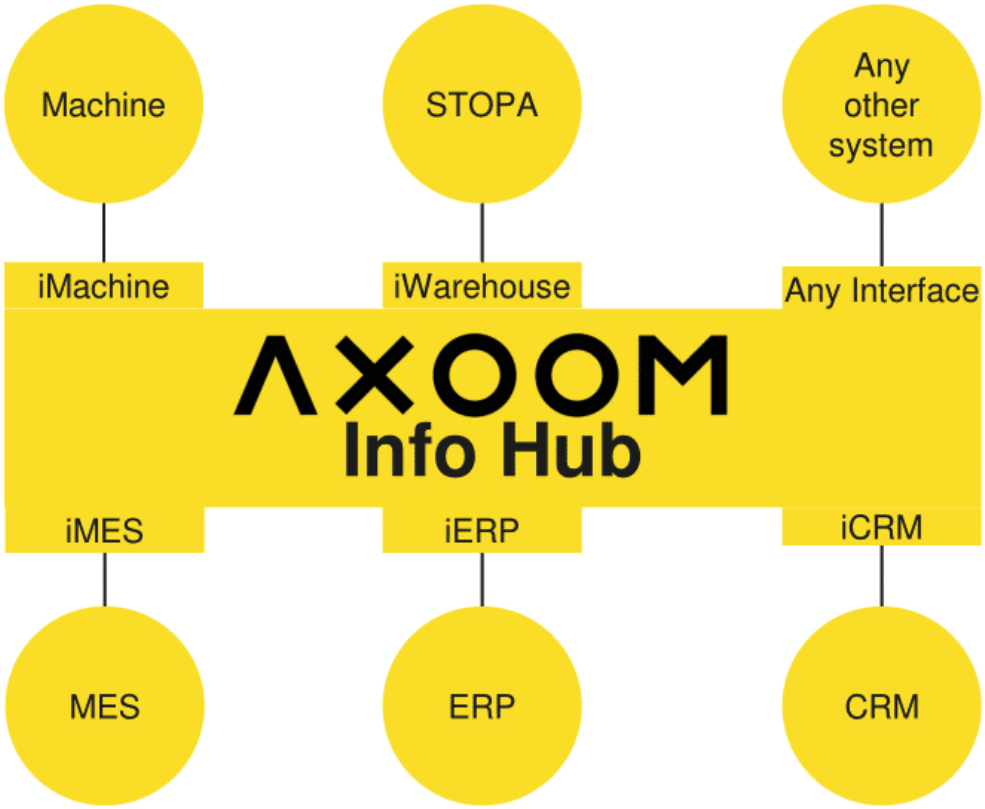

Abbildung 4.2: AXOOM Netzwerkintegration

TODO - sichere Kommunikation durch AXOOM Gate - wie? Quellen? -> "Dieses basiert teilweise auf Technologien unseres Partners C-Labs und schafft eine direkte Verbindung zwischen dem Kundennetzwerk und der Cloud. Das AXOOM Gate ist in der Lage, Daten herstellerunabhängig von allen angebundenen Geräten zu sammeln, so dass diese verschlüsselt an die AXOOM Plattform gesendet und dort visualisiert und ausgewertet werden können. Besonderen Schutz bei der Datenübertragung bietet ein mehrstufiges Sicherheits- und Verschlüsselungskonzept auf Komponenten-, Transport-, Applikations- und Anwenderebene. So wird eine genaue Zugriffskontrolle innerhalb der Fabrik sowie auf die Fabrik sichergestellt, unsichere Verbindungen von und nach Außen sind ausgeschlossen."

Schnittstellen

TODO - offene Schnittstellen für Low Level TODO - REST usw. für High Level Applications

andere Kriterien

TODO - Softwareschwachstellen, Softwarefehler TODO - Herstellerabhängigkeit TODO - Kosten der Interfaceentwicklung, usw.

4.5.3 OPC UA Protokollanalyse

TODO - siehe BSI UPC UA Analyse. TODO - The OPC UA specifications are layered to isolate the core design from the underlying computing technology and network transport. This allows OPC UA to be mapped to future technologies as necessary, without negating the basic design. Mappings and data encodings are described in Part 6. Three data encodings are defined:

- XML/Text
- UA Binary
- JSON

In addition, several protocols are defined:

- OPC UA TCP

- HTTPS
- WebSockets

TODO - ref. OPC Pt. 1 TODO - OPC UA ist in der IEC 62541 als offener Standard definiert und erstreckt sich über Communication- und Information Layer des RAMI4.0, da es eine SOA bereitstellt. TODO - vereint Daten und Informationsdienste. TODO - basiert auf IP-Netz -> Angriffsvektoren von IP und genutzten Diensten immer noch zutreffend

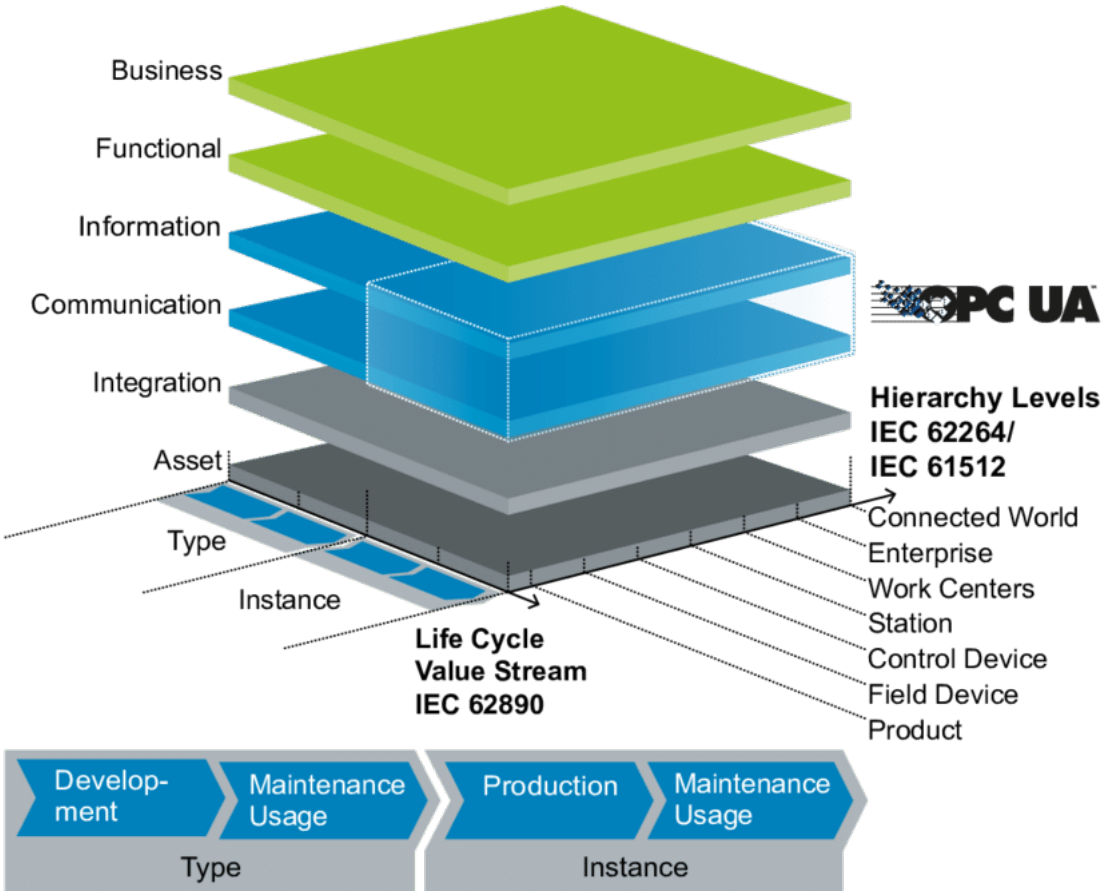

Abbildung 4.3: OPC UA im RAMI 4.0

4.6 weitere Schutzmaßnahmen

TODO - Applikationssicherheit != Netzwerksicherheit != Betriebssystemsicherheit

4.6.1 Defense in Depth

Auf der Netzzugangsschicht fallen, wie auf allen anderen Schichten, Betriebsdaten an, welche genutzt werden können, um Angriffe oder unregelmäßige Aktivitäten im Netzwerk zu erkennen. Es kann protokolliert werden, wann ein Gerät mit den Netzwerk verbunden war und welche Pakete andere Netzwerkteilnehmer von diesem Gerät erhalten haben (Plattform Industrie 4.0 2017). Die Norm IEC 62443[12] definiert die Defense in Depth Strategie. Sie stellt ein Konzept bereit, um die IT-Sicherheit der Anlagen, die Netzwerksicherheit und Systemintegrität nach dem Stand der Technik zu schützen. Sie gliedert eine Unternehmensinfrastruktur in multiple und redundante Sicherheitsschichten (Zonen), um ein höchstmögliches Sicherheitsniveau zu erreichen. Die unabhängigen Verteidigungslinien sollen Angriffe verzögern, um Zeit für Gegenmaßnahmen zu gewinnen. Die Kommunikation erfolgt in separierten Netzsegmenten, welche zusätzlich mit Instrusion Detection System (IDS) nutzen, um Angriffe schnell zu erfassen und Gegenmaßnahmen einleiten zu können. Somit wird der Aufwand, um die unteren Netzwerkebenen zu kompromittieren durch den Einsatz von Demilitarized Zone (DMZ), IDS, Paketfilter und Time Access Control wesentlich erhöht. Zusätzlich ist das „Zone and Conduit“ Modell eines der zentralen Elemente der Defense in Depth Strategie. Die verschiedenen Zonen können nur mittels spezieller Leitungen (Conduits) miteinander kommunizieren.

[12] ref. IEC 62443

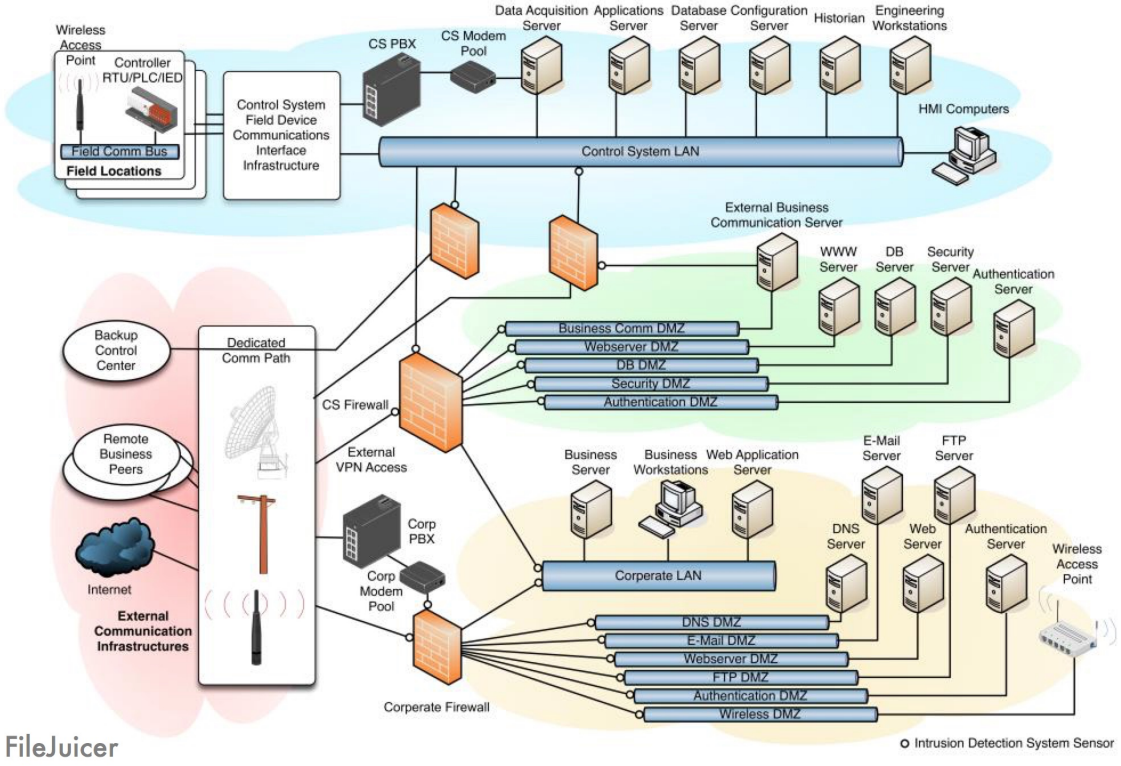

Abbildung 4.4: Defense in Depth Strategie - David Kuipers 2006

Das Defense in Depth Konzept stellt ein Konzept dar, um Industrieanlagen und Unternehmensnetzwerke vor Angriffen zu schützen. Bei der sich ständig ändernden Bedrohungslage in den komplexen Netzen wird bei dieser Strategie jedoch weniger ein vollständiger Schutz bereitgestellt, als eine Strategie zur Schadensbegrenzung im Falle eines Angriffs.

4.7 Angriffsvektoren

4.7.1 OPC UA Spezifikation

Sicherheitslücken

Widersprüche

4.7.2 Verschlüsselung

4.7.3 Paketversand

4.7.4 TODO

4.8 Auswertung der Ergebnisse

4.8.1 Probleme der Spezifikation

TODO - Widersprüche in Spezifikation, sonstiges -> Syntaxfehler, usw.

4.8.2 Erweiterung des Testsystems

TODO - gefundene Schwachstellen bzw. Fehlkonfigurationen sind Grundlage der Implementierung! TODO - Analyse dient als Basis zur Wahl der Implementierung und Darstellung der Auswirkungen am Testsystem.

Kapitel 5

Implementierung

TODO - um die Komplexität des Systems gering zu halten werden die vorhandenen Komponenten NodeJS, Angular, Docker, ... zur Implementierung der Funktionalitäten im Bereich der Netzwerksicherheit weiterhin genutzt und erweitert.

5.1 DHCP Spoofing

DHCP Spoofing -> Vortäuschen eines DHCP, schneller Leases verteilen als vorhandener DHCP -> MitM TODO - impl. 2. DHCP Server implementieren DHCP Snooping -> theor. Verteidigung gegen Spoofing, Switches erlauben nur bestimmten Ports DHCP Traffic zu versenden

5.2 Anwendungsszenario - ARP Spoofing

TODO - verfälschter Ethernetrahmen -> MAC Manipulation - MitM TODO - Schutz durch statische Tabellen, IDS

TODO - Zertifikatstests TODO - Fuzzing TODO - Logging TODO - Mustererkennung TODO - Schwachstellen in implementierten Protokollen TODO - Anschluss neuer virtueller Geräte über Gateway

Kapitel 6

Validierung

Kapitel 7

Fazit

Abkürzungsverzeichnis

IEEE	Institute of Electrical and Electronics Engineers
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
IIAF	Industrial Internet Architecture Framework
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
MAN	Metropolitan Area Network
WAN	Wide Area Network
GAN	Global Area Network

DA	Data Access
A&E	Alarms and Events
HDA	Historical Data Access
IP	Internet Protocol
TCP	Transmission Control Protocol
DNS	Domain Name System
UDP	User Datagram Protocol
SOA	Service Oriented Architecture
OMG	Open Management Group
DDS	Data Distribution Services
HTTP	Hypertext Transfer Protocol
CoAP	Constrained Application Protocol
XMPP	Extensible Messaging and Presence Protocol
MQTT	Message Queue Telemetry Transport
AMQP	Advanced Message Queuing Protocol
VM	virtuelle Maschine
PKI	Public-Key Infrastructure
BSI	Bundesamt für Sicherheit in der Informationstechnik
DoS	Denial of Service
DDoS	Distributed Denial of Service
DMZ	Demilitarized Zone
IDS	Instrusion Detection System
IEC	International Electrotechnical Commission
M2M	Machine to Machine
ARP	Address Resolution Protocol
DHCP	Dynamic Host Configuration Protocol
RFC	Request for Comments
IETF	Internet Engineering Task Force
RR	Resource Record

Tabellenverzeichnis

Abbildungsverzeichnis

Listings

Literatur

Bundesamt für Sicherheit in der Informationstechnik, BSI (2016). „Industrial Control System Security“. In:

Bundesministerium für Wirtschaft und Energie, BMWi (2016a). „Netzkommunikation für Industrie 4.0“. In: *Platform Industrie 4.0*.

— (2016b). „Technischer Überblick: Sichere unternehmensübergreifende Kommunikation“. In:

Burke, Manfred (2013). *Rechnernetze*. Springer.

Christoph Meinel, Harald Sack (2011). *Internetworking - Technische Grundlagen und Anwendung*. Springer.

David Kuipers, Mark Fabro (2006). „Control Systems Cyber Security“. 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.

DTAG, Deutsche Telekom AG (2016). „Sicherheit im Industriellen Internet der Dinge“. In:

Foundation, OPC (2018a). „OPC Unified Architecture Specification Part 1: Overview and Concepts“. In: URL: https://opcfoundation.org/UA/Part1/.

— (2018b). „OPC Unified Architecture Specification Part 5: Information Model“. In: URL: https://opcfoundation.org/UA/Part1/.

Hoppe, Stefan (2018). „OPC Foundation announces OPC UA PubSub release as important extension of OPC UA communication platform“. In: URL: https://opcfoundation.org/news/press-releases/opc-foundation-announces-opc-ua-pubsub-release-important-extension-opc-ua-communication-platform/.

Industrial Internet Consortium, IIC (2017). „The Industrial Internet of Things - Volume G1: Reference Architecture“. 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*.

Plattform Industrie 4.0 (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.

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: