hochschule mannheim

Analyse der Netzwerkkommunikation in Industrie 4.0 Umgebungen und Erweiterung einer protoypischen Security Testumgebung zur Darstellung von Bedrohungsfaktoren

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:
Analyse der Netzwerkkommunikation in Industrie 4.0 Umgebungen und Erweiterung einer protoypischen Security Testumgebung zur Darstellung von Bedrohungsfaktoren / Philipp Minges. –
Bachelor-Thesis, Mannheim: Hochschule Mannheim, 2018. 75 Seiten.

Minges, Philipp:
TODO - Title EN / Philipp Minges. –
Bachelor Thesis, Mannheim: University of Applied Sciences Mannheim, 2018. 75 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

Analyse der Netzwerkkommunikation in Industrie 4.0 Umgebungen und Erweiterung einer protoypischen Security Testumgebung zur Darstellung von Bedrohungsfaktoren

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

TODO - Um die Komplexität zu reduzieren, wird eine umfassende Modularisierung, eine breite Standardisierung und eine durchgängige Digitalisierung benötigt. Diese Anforderungen sind nicht neu, sie sind auch nicht revolutionär sondern die Folge einer permanenten Weiterentwicklung. Diese Evolution ist ein langjähriger Prozess, der schon lange begonnen hat und es existieren bereits Lösungen für viele der nachfolgend skizzierten Anforderungen, die unter anderem auch die zentralen

Grundbausteine für Industrie 4.0 sind. (ref. OPC UA - Wegbereiter der Industrie 4.0)

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.

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.

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.

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.

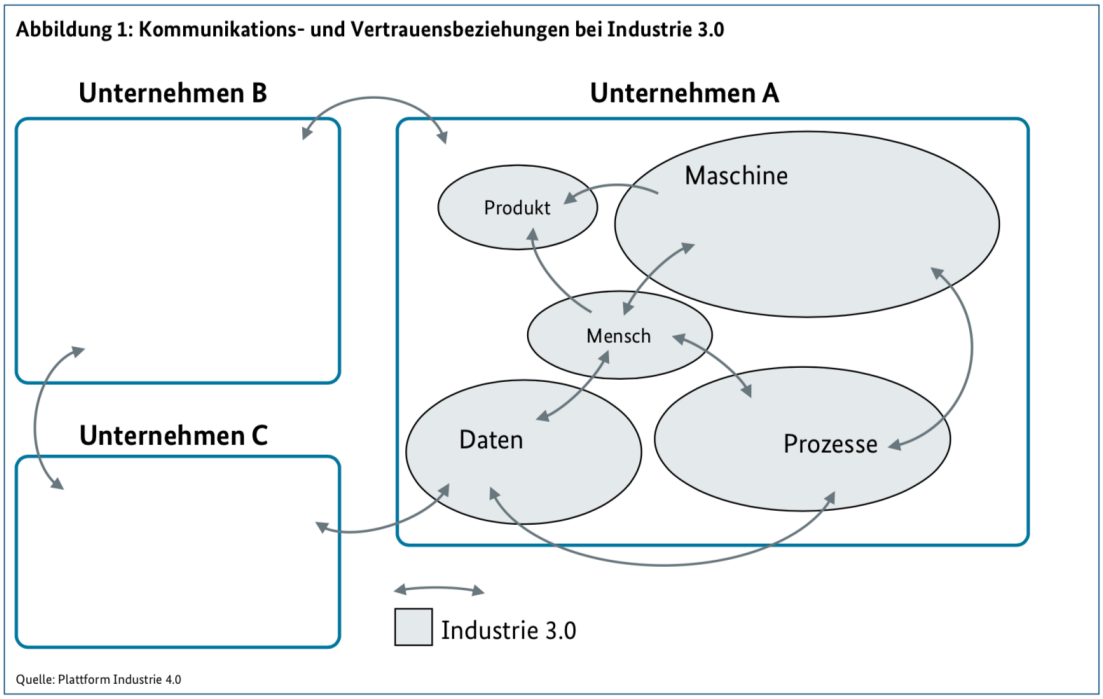
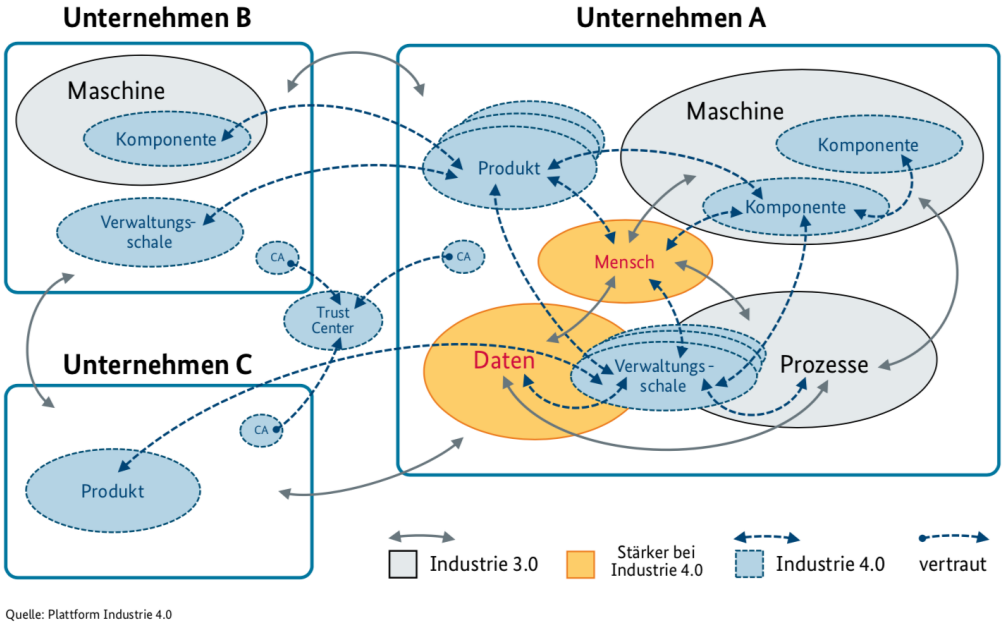


Abbildung 2.1: Kommunikationsbeziehungen in einer Industrie 3.0 Umgebung - TODO ref. sichere unternehmensübergreifende Kommunikation

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: Kommunikations- und Vertrauensbeziehungen bei Industrie 4.0



Quelle: Plattform Industrie 4.0

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.

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 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.

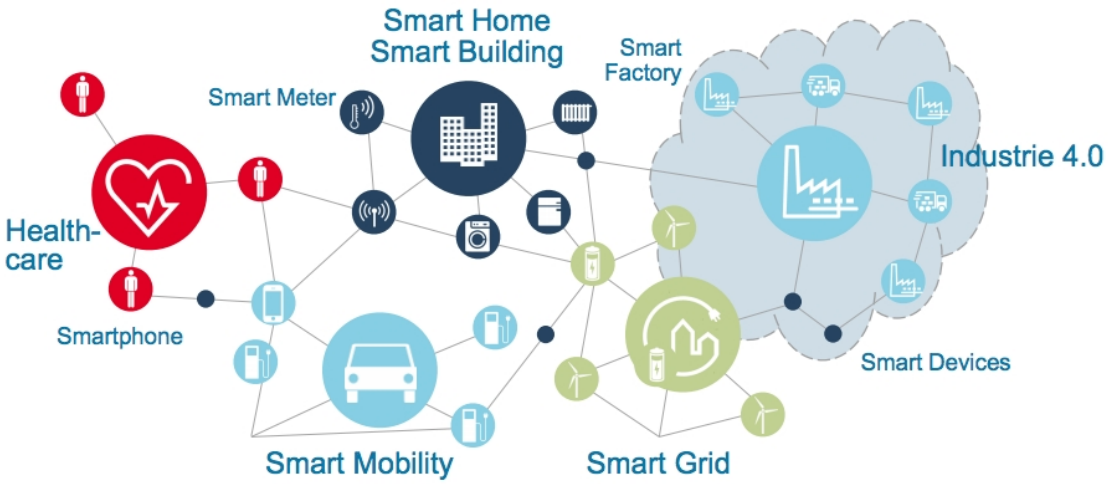


Abbildung 2.3: Das Internet der Dinge - Plattform Industrie 4.0 2016

2.3.1 Automatisierungspyramide

TODO - Zusammenfassen mit Industrie 4.0 -> Automatisierungspyramide ist Bestandteil. Fertig. Die Automatisierungspyramide stellt die beteiligten Systeme und Softwarekomponenten eines automatisierten Prozesses systematisch dar. Diese beginnen, ausgehend vom Kundenauftrag und der betriebswirtschaftlichen Planung der Produktion auf der Unternehmensebene im Enterprise Resource Planning (ERP) System. Die Ergebnisse der Planung werden an das Manufacturing Execution System (MES) übergeben, welches die verschiedenen Fertigungs- oder Logistikaufträge generiert. Die Aufträge werden anschließend auf der Prozessleit- (SCADA), Steuerungs- (SPS) und Feldebene (Ein-/Ausgangssignale) bearbeitet.

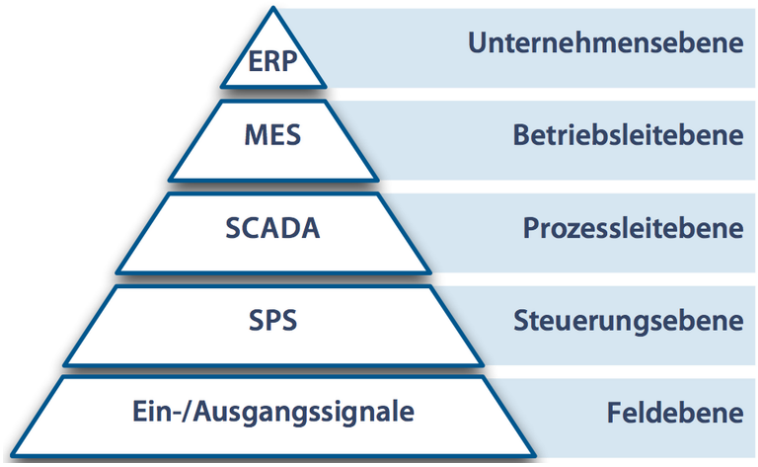


Abbildung 2.4: Automatisierungspyramide - TODO ref. Langmann,2004

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

2.3.2 Kommunikation in der Industrie 4.0

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.

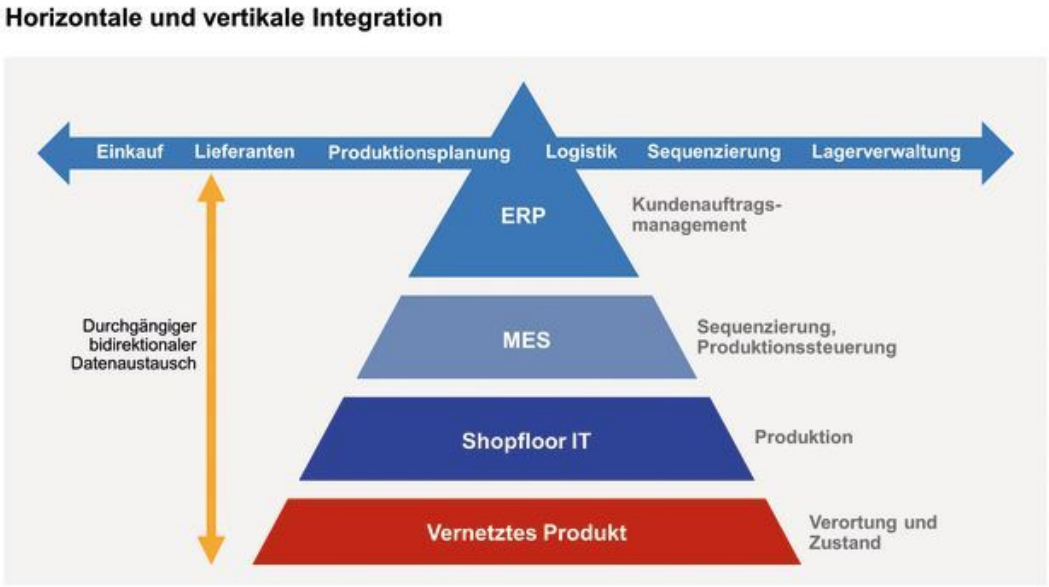


Abbildung 2.5: horizontale und vertikale Integration - TODO ref. HP Industry-of-things siehe bookmark

Kommunikationsstrukturen

TODO

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 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.

TODO - Netzlast bei

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.

2.3.3 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), CoAP, Extensible Messaging and Presence Protocol (XMPP) und MQTT, etabliert. Jedes dieser Protokolle besitzt für spezifische Anforderungen wie Skalierbarkeit, vorhandene Ressourcen, Echtzeitkommunikation oder Sicherheit Vor- und Nachteile.

2.3.4 Industrial Ethernet

TODO - Ethernet für Industrieanlagen

2.4 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.

2.4.1 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.

2.4.2 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.

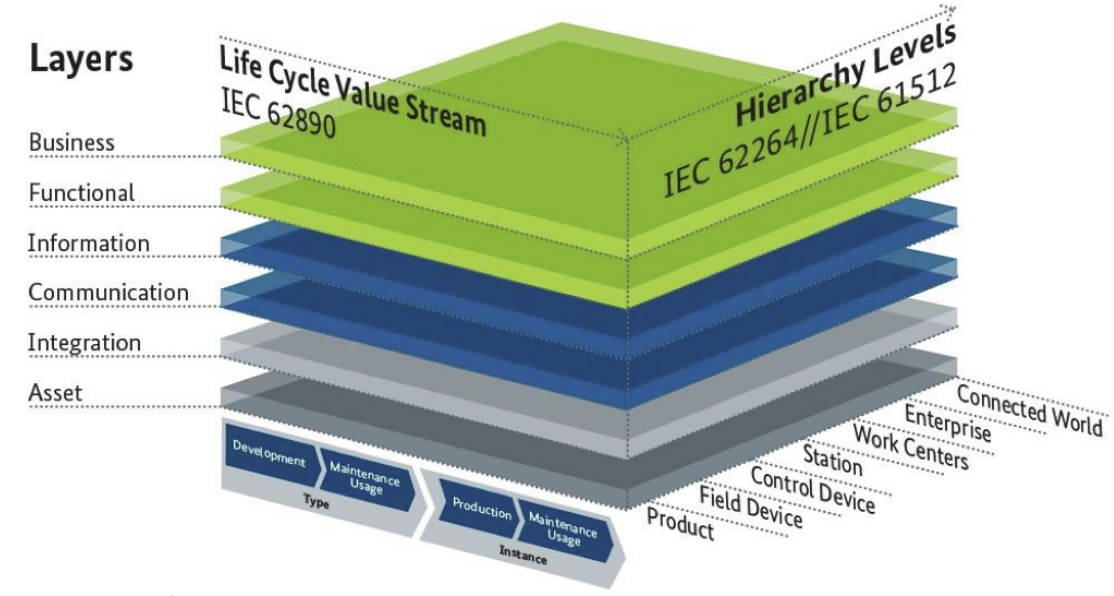


Abbildung 2.6: RAMI 4.0 - Plattform Industrie 4.0 2016

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). 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 - Kommunikation beschreiben - Assets, Verwaltungsschale 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 zu ermöglichen. Das IIAF folgt der Vorgehensweise des ISO/IEC/IEEE Standard 42010:2011[1]. Die Anforderungen beinhalten niedrige Latenzen und Schwankungen, einen hohen Durchsatz, Skalierbarkeit, Ausfallsicherheit, Datensicherheit und QoS.

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

[1] ISO/IEC/IEEE Standard 42010:2011 - Systems and Software Engineering–Architecture Description

Viewpoints. Abbildung 2.7 beschreibt die grundlegende Idee und den Aufbau der IIRA.

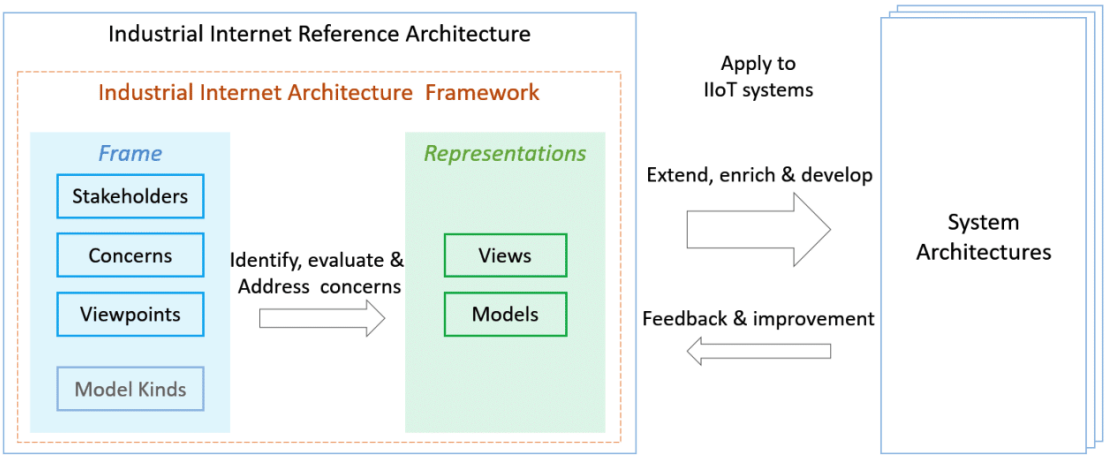


Abbildung 2.7: IIAF/IIRA - Übersicht

2.4.3 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

TODO - OPC UA ist in der International Electrotechnical Commission (IEC) 62541 als offener Standard definiert und erstreckt sich über Communication- und Information Layer des RAMI4.0. Es vereint Daten- und Informationsdienste und stellt einen sicheren, zuverlässigen und plattformübergreifenden Informationsaustausch zwischen unterschiedlichen Geräten und Systemen der Industrie bereit. Es wird die Kommunikation über die verschiedenen Schichten der Anwendungspyramide von der Feldebene bis zur Unternehmensebene ermöglicht (OPC Foundation 2014). OPC UA stellt ein Informationsmodell mit Hilfe einer SOA bereit, erfüllt die Anforderungen des RAMI4.0 und etabliert sich zunehmend im Maschinen- und Anlagenbau.

OPC UA 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 Architekturmodells dar. Sie beschreiben die Struktur des OPC Addressraums und der Dienste, die darauf operieren. Die Spezifikationen 8-11 wenden diese Kernfunktionalitäten auf spezifische Open Platform Communications (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.

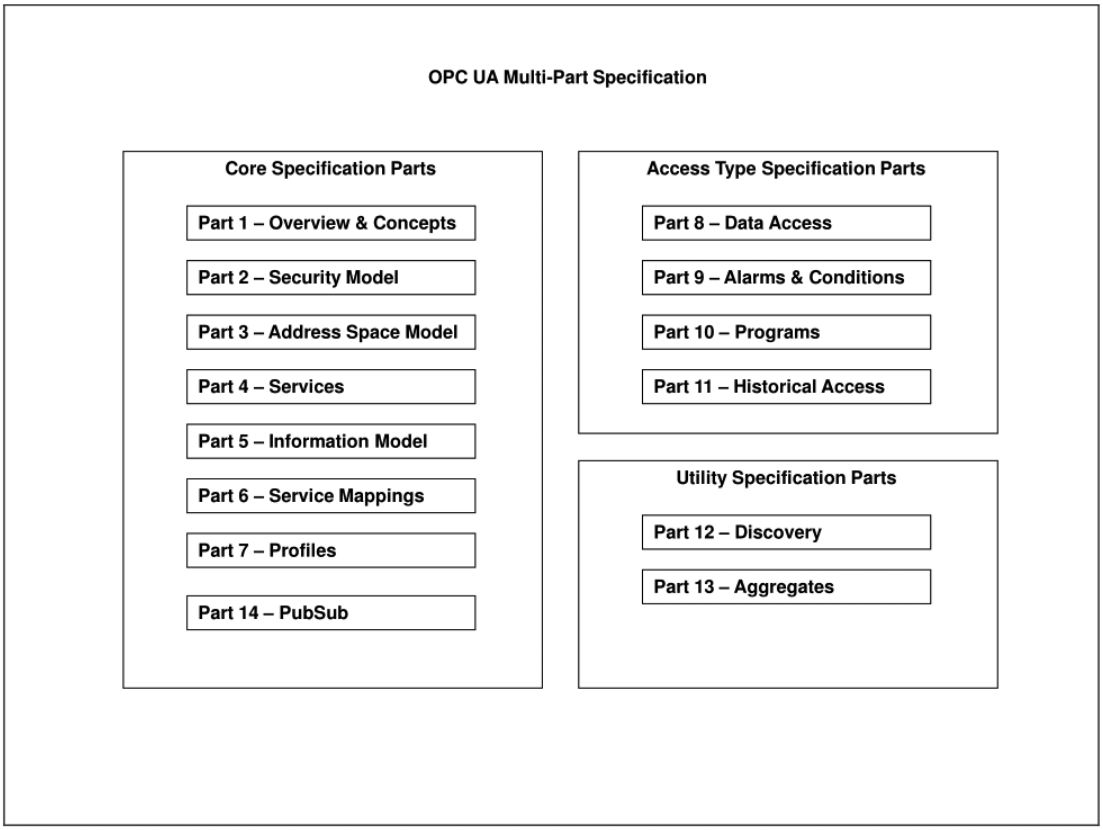


Abbildung 2.8: OPC UA Multi-Part Specification - OPC Foundation 2018a

Das Lesen- und Schreiben von Daten und die Kommunikation in Industrie 4.0 Umgebungen findet nach RAMI4.0 durch die Verwaltungsschale der Komponenten statt. Diese wird im OPC UA Stack durch den Adressraum 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 Spezifikationen 3 **opcpc3** und 5 OPC Foundation 2018c definiert.

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, wird ein OPC UA Client in einen OPC UA Server integriert. In der Grafik Abbildung 2.9 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.

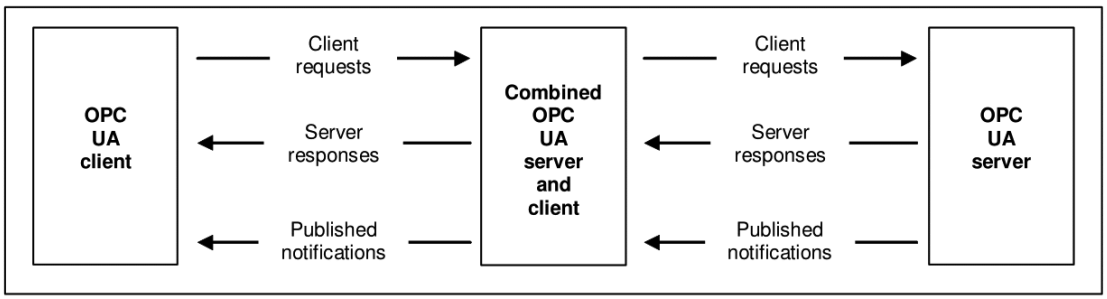


Abbildung 2.9: OPC UA Client-Server Architektur - OPC Foundation 2018a

Im Jahr 2018 wurde der Standard zusätzlich um eine Spezifikation für das Publish-Subscribe Modell erweitert (Hoppe 2018). Das Publish-Subscribe Modell ermöglicht die Nutzung von OPC UA in Wide Area Network (WAN) Umgebungen und die Verwendung von Protokollen wie MQTT und Advanced Message Queuing Protocol (AMQP), während die Ende zu Ende Sicherheit und die standardisierte Datenmodellierung erhalten bleiben. Im Publish-Subscribe Modell wird das fehlertolerante Datagramm UDP als Transportprotokoll verwendet, wodurch geringe Latenzen bei der Kommunikation ermöglicht werden.

DDS

DDS ist ein weiterer offener Standard der Open Management Group (OMG) und stellt eine Message oriented Middleware (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 Broad- und 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.

2.5 Anforderungen an Industrie 4.0 Umgebungen

Aufgrund der unterschiedlichen Einsatzbereiche von Industrie 4.0 Systemen, unterscheiden sich auch dementsprechend deren Anforderungen. Um eine sichere Kommunikation in diesen Umgebungen bereitzustellen dienen die Grundprinzipien der sicheren Kommunikation. Die Referenzmodelle RAMI4.0 und IIRA beschreiben ebenfalls drei Anforderungen an den Übertragungskanal: Sicherheit, Verfügbarkeit und QoS (Bundesministerium für Wirtschaft und Energie 2016a).

2.5.1 Grundprinzipien der sicheren Kommunikation

TODO - in Bezug auf Industrie 4.0 ... oder Anforderungen an Industrie 4.0 Umgebungen basieren auf 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 vereinbar-

ten 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.

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

weitere Schutzziele

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

2.5.2 Anforderungen der Referenzmodelle

Sicherheit

- Netzsicherheit und Datensicherheit
- Sichere Identitäten

- funktionale Sicherheit

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...

QoS

TODO - QoS

2.5.3 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 Unterabschnitt 2.5.1 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 Sicherheitsimplementierung 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 (Platform Industrie 4.0 2015). Die Referenzarchitekturen RAMI4.0 und IIRA sowie die in den Architekturmodellen genutzten Techniken OPC UA und DDS haben das Konzept des *Security by Design* in ihre Kernbestandteile mit aufgenommen.

2.6 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.

2.6.1 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.

2.6.2 Komponenten

Repository

Discovery Server

Public-Key Infrastructure (PKI)

Identity Provider

Verwaltungsinterface

Scheduler

Kapitel 3

Konzept

TODO - Konzept komplett überarbeiten. Siehe 1. Absatz Analyse z.B.

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 2.6 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 Anpassungen

TODO GEHT NIX DOCKER

3.4 Vorgehensweise

Die Analyse der Netzwerkkommunikation der unteren Schichten (Internet- und Link Layer) des im Unterabschnitt 2.4.1 beschriebenen TCP/IP Referenzmodells

wird auf Basis der in Unterabschnitt 2.5.1 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. Diese 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. Zuerst wird eine Beschreibung und Einordnung der Bedrohungen von Industrie 4.0 Systemen anhand der in Unterabschnitt 2.5.1 genannten Schutzziele und der aktuellen Industriestandards Abschnitt 2.4 durchgeführt. Anschließend werden, aufgrund der bestehenden Infrastruktur und der Heterogenität der Netzwerklandschaft der Industrie, verschiedene Integrationsansätze für einen standardisierten Datenaustausch beschrieben. Die dabei etablierten Techniken und Protokolle des IoT und IIoT sowie neue M2M Kommunikationswege der Industrie 4.0 werden dann nach den Schichten des TCP/IP Referenzmodells untersucht, 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 unterschiedliche 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 Indus-

trie 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

TODO - Einordnung - Bezug auf Analyse

Um die in Unterabschnitt 2.5.1 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 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.

4.2.1 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

4.2.2 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. eher nicht!

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 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."TODO - offene Schnittstellen für Low Level TODO - REST usw. für High Level Applications TODO - Softwareschwachstellen, Softwarefehler TODO - Herstellerabhängigkeit TODO - Kosten der Interfaceentwicklung, usw. TODO - AXOOM Absatz unnötig

4.3 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.

4.3.1 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)

4.3.2 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). 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

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

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

4.3.3 VLAN

TODO - Taggen von Frames, da keine Kommunikation im Schichtenmodell zwischen den Schichten stattfindet. Somit QoS schwierig, da es von allen Hardwarekomponenten unterstützt werden muss und nicht nur auf Anwendungsebene funktionieren kann.

4.3.4 ARP

TODO - praktisch nur wenn Tool vorhanden ist.

4.3.5 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.

4.4 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 durch-

[4] Link zu IEEE Ethernet

gesetzt (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 (Unterabschnitt 4.6.1) und DHCP (Unterabschnitt 4.6.2) genutzt. Das IP Adress Management (IPAM) und die Zuordnung der physikalischen Hardware zur logischen IP-Adresse erfolgt mit Hilfe des ARP. Da die Kommunikation in einem IP-Netz ohne diese Dienste und Protokolle nicht möglich ist, stellen sie einen wichtigen Bestandteil im Netzwerk dar und müssen vor Sabotage geschützt werden.

4.4.1 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 Unterabschnitt 2.3.1 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 Gegebenheiten wie Latenz und Jitter betroffen. Diese Erscheinungen müssen berücksichtigt werden, um eine fehler- und verlustfreie, sichere Kommunikation zu gewährleisten Torscht 2014.

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

All diese Faktoren haben in einem paketorientierten Netzwerk, in welchem die Datenpakete nach dem *Best-Effort-Prinzip* versendet werden, auf die fehlerfreie Kommunikation aufgrund der durch *Ethernet* und IP bereitgestellten Fehler- und Flusskontrolle wenig Einfluss. Sie spielen jedoch bei zeitkritischen Anwendungen der Industrie 4.0 eine wichtige Rolle. Auf den niedrigeren Schichten des TCP/IP Referenzmodells ist es nicht möglich zwischen verschiedenen Datenpaketen der höheren Schichten zu unterscheiden. Um dieses Problem zu lösen werden auf Dienste mit besonderer Güte in VLANs aufgenommen und somit deren Pakete bereits auf der Netzzugangsschicht kenntlich gemacht (Unterabschnitt 4.3.3), um die Dienstqualität sicherzustellen. Des Weiteren müssen, um QoS in einem Netzwerk anzuwenden, diese Mechanismen auf der gesamten Übertragungsstrecke implementiert werden. Der Transport von Daten unterschiedlicher Priorität in Netzwerken wird in IEEE 802.1p und IEEE 802.1Q[5] beschrieben.

4.4.2 IPsec

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

4.5 Transportschicht

Während auf der Netzwerkschicht allein das Protokoll IP die Basis für die Vernetzung und Adressierung von Industrie 4.0 Systemen darstellt, wird das Protokoll der Transportschicht durch die Anforderungen an das Netzwerk bestimmt. Der wesentliche Teil der Kommunikation in der Industrie 4.0 erfolgt über ein IP Netzwerk, welches zum Datentransport das Protokoll TCP für *End2End* (Abschnitt 2.3.2) Kommunikation nutzt (Plattform Industrie 4.0 2017). Wie in Abschnitt 2.3.2 beschrieben, bieten sich in der Praxis bei besonderen Anforderungen wie der Verteilung von Informationen im Netzwerk oder zeitkritischen Automatisierungsanwendungen jedoch auch andere Strukturen für die Kommunikation wie *Publish-Subscribe* (Abschnitt 2.3.2) in Verbindung mit dem Datagramm UDP an.

[5] IEEE Std 802.1Q - IEEE Standard for Local and metropolitan area networks–Bridges and Bridged Networks

Das Protokoll TCP sowie das Datagramm UDP sind für die Übertragung der Segmente im Netzwerk sowie das Multi-/Demultiplexing verantwortlich. Dabei spielt der Inhalt der zu übertragenden *payload* keine Rolle. Die Analyse der Sicherheit im Netzwerk auf dieser Schicht des TCP/IP Referenzmodells beschränkt sich somit ausschließlich auf die Form der Datenübertragung sowie der dafür genutzten Netzlast.

4.5.1 TCP

Das Protokoll TCP[6] verfolgt das Prinzip eines *guaranteed delivery* und stellt eine zuverlässige Datenübertragung zwischen zwei *Hosts* (Unicast) bereit. Hierzu werden verschiedene Mechanismen zur Segmentierung der Daten, dem Verbindungsmanagement sowie der Fehler- und Flusskontrolle bereitgestellt. Diese Mechanismen, welche durch den Aufbau des des TCP Headers und die Nutzung von Timeouts und Algorithmen realisiert werden, sind für den Erfolg des Protokolls für zuverlässige, paketorientierte *End2End* Kommunikation verantwortlich.

Ein wichtiger Bestandteil des TCP Verbindungsmanagements und der Fehlerkontrolle stellt der 3-Wege-Handshake beim Verbindungsaufbau sowie -abbau dar. Er wird mittels der *Sequence*- und *Acknowledgementnumber* sowie den zugehörigen *Flags* des TCP Headers (synchronise (SYN), synchronise-acknowledge (SYN-ACK), acknowledge (ACK), final (FIN)) realisiert. Während des Verbindungsaufbaus werden die Adresse des Clients sowie der Status der Verbindung im Speicher gehalten. Die folgende Abbildung zeigt schematisch den Ablauf eines TCP Verbindungsaufbaus zwischen Client und Server. Der Client sendet zuerst eine Paket mit SYN-Flag zum Server. Dieser bestätigt das eingetroffene Paket des Clients mit dem SYN-ACK Flag, inkrementiert die Sequenznummer x in seinem *acknowledgment number* Segment[7] und erzeugt eine neue Sequenznummer für das Antwortpaket. Der Verbindungsaufbau wird durch die Bestätigung des SYN-ACK Pakets durch den Client und den Empfang des ACK Pakets vom Server abgeschlossen. Die initiale Sequenznummer x des SYN Pakets sowie die initiale Sequenznummer y des SYN-ACK Pakets können von den Beteiligten frei bestimmt werden.

[6] Network Working Group 1981
[7] text

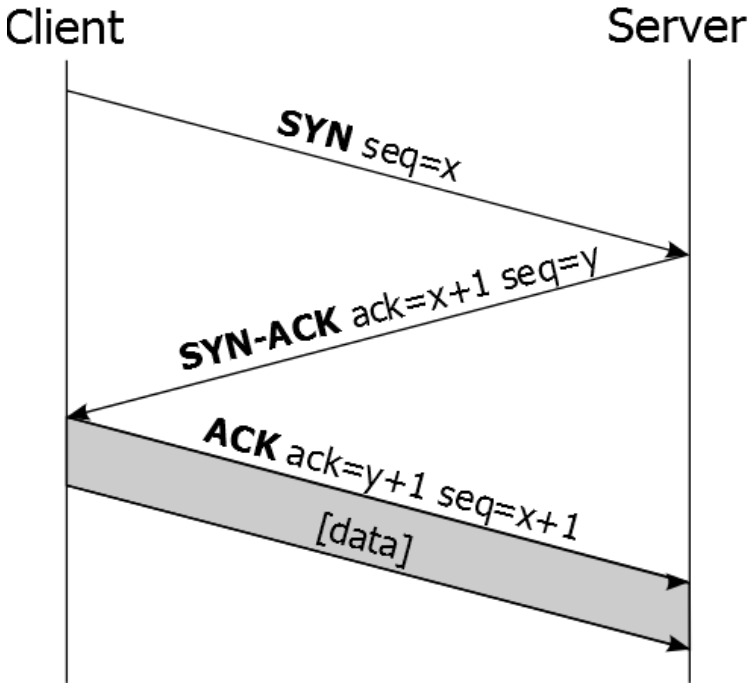


Abbildung 4.1: TCP Verbindungsaufbau

SYN-Flood

Der Mechanismus des 3-Wege-Handshakes kann durch einen SYN-Flood Angriff ausgenutzt werden und somit die Netz- und Systemlast manipuliert werden. Der SYN-Flood stellt eine Form des DoS bzw. DDoS Angriffs dar. Dabei werden zu einem gezielten TCP Dienst viele Pakete mit gesetztem SYN *Flag* gesendet, um einen Verbindungsaufbau zum Server vorzutäuschen. Nach Erhalt des Pakets sendet der Server dem Client ein SYN-ACK Paket um den Verbindungsaufbau zu initiieren und wartet auf Bestätigung. Diese Bestätigung wird vom Angreifer unterschlagen. Somit bleiben auf dem angegriffenen System Ressourcen dieser halb offenen Verbindung bis zum erreichen eines Timouts belegt. Ein verteilter Angriff auf ein System kann dessen Ressourcen schnell komplett beanspruchen und somit zur Ablehnung jeglicher weiterer Verbindungen führen.

Die Kritikalität dieses Angriffs liegt in der Unausgewogenheit der benötigten Ressourcen zwischen Angreifer und Opfer. Es benötigt nur wenig Rechenaufwand und Bandbreite um ein 20 Byte großen TCP-SYN Header mit entsprechender *payload* zu erzeugen und zu versenden, jedoch viele Ressourcen um sich durch eine Echtzeitanalyse der Pakete durch eine Firewall oder SYN-Cookies vor diesen Angriffen zu schützen. Diese werden aufgrund ihrer Ressourcenbelastung aus wirtschaftlichen Gründen meist nur minimal oder gar nicht umgesetzt.

Der Mechanismus der SYN-Cookies wird auf dem Server implementiert. Hierbei werden in die initiale Sequenznummer des vom Server gesendeten SYN-ACK Pakets die Informationen Zeitstempel, IP Adresse und Port von Client und Server kodiert, welche normalerweise in einer Tabelle im Speicher gehalten werden müssten. Somit ist ein überlaufen der Tabelle unmöglich, da sie nicht vorhanden ist. Jedoch benötigt jede Kodierung und Dekodierung Systemressourcen. Ein ausreichend großer Angriff auf das System kann somit trotzdem die gesamten Systemressourcen beanspruchen und somit das Ziel eines DDoS Angriffs, die Negierung eines Dienstes, erfüllen.

Dedizierte Firewalls können mit Hilfe von Instrusion Detection System (IDS) die Pakete beim Eintreffen im Netzwerk analysieren, Angriffe erkennen und Verbindungen dieser Quelladressen blockieren.

Sockstress

Die Angriffsform Sockstress wurde im Jahr 2008 von den Sicherheitsforschern Jack C. Louis und Robert E. Lee von Outpost24[8] entdeckt. Sie beinhaltet eine einfache Form eines DoS Angriffs, welche den 3-Wege-Handshake des TCP für unterschiedliche Angriffsszenarien manipuliert. Das Ziel dieses Angriffs ist, ähnlich wie beim SYN-Flood, eine Negierung eines Dienstes oder des gesamten Systems mit Hilfe asymmetrischer Ressourcenauslastung bei Angreifer und Opfer.

Im Gegensatz zu SYN-Flood stellt Sockstress eine Verbindung zum Server über den 3-Wege-Handshake her. In der einfachsten Form des Angriffs wird beim letzten TCP Segment, welches vom Client zum Server während des 3-Wege-Handshakes übertragen wird, das *Receive Window* Flag des Headers auf 0 gesetzt. Dies bedeutet, dass der Client dem Server mitteilt, dass er im Moment keine weiteren Daten empfangen kann. Der Server wird, durch den abgeschlossen Verbindungsaufbau, gezwungen die Verbindung im Speicher zu halten, offen zu lassen und den Client periodisch zu prüfen, ob dieser wieder Daten empfangen kann. Dies belegt Systemressourcen und kann genutzt werden, um einen Dienst oder ein System zum Ablehnen aller Verbindungen oder zum Absturz zu bewegen.

Da die Verbindungen zum Client zum Server vollständig aufgebaut werden, hat die Nutzung von SYN Cookies keine Auswirkungen auf den Erfolg dieses Angriffs. Industrieanlagen müssen mit Hilfe externer DDoS Serviceanbieter wie Akamai[9] oder Cloudflare[10], Firewalls und IDS Systeme oder spezieller Appliances, welche den Netzwerkverkehr Netzwerk-, Transport- und Anwendungsschicht überwachen, geschützt werden.

Diese Form des DoS Angriffs wurde am vorhandenen Industrie 4.0 Testsystem (Weber 2018) durchgeführt, um den Angriffsaufwand sowie die Auswirkungen auf die Systeme und Netzwerkkommunikation in Industrieumgebungen an einem Beispiel darzustellen (siehe **??**).

TODO - In Abbildung XY ist zu erkennen - asymmetrischer Angriff - Monitoring Ressourcenauslastung - RAM bleibt nach dem Angriff weiterhin belegt -> nur Systemneustart gibt Speicher wieder frei TODO - Diagramm als Zusammenfassung der Implementierung TODO - Ergebnisse beschreiben

[8] http://www.outpost24.com
[9] https://www.akamai.com
[10] https://www.cloudflare.com

4.5.2 UDP

UDP[11] ist ein verbindungsloses[12], nicht-zuverlässiges[13] Übertragungsprotokoll. Der UDP Header ist im Gegensatz zum TCP Header (20 Bytes) nur 8 Byte lang und bietet somit einen sehr geringen *Overhead*[14] beim Versenden von IP Paketen. UDP wurde als Alternative zu TCP entwickelt, um die Kommunikation mit niedrigeren Latenzen für Dienste wie Simple Network Management Protocol (SNMP) oder DNSoder Voice over IP (VoIP) zu ermöglichen (Olsen 2003). Es wird auf den für die Latenz kritischen 3-Wege-Handshake verzichtet und das *Fire-and-Forget*[15] Prinzip angewandt, wobei keine Verbindung zwischen zwei Kommunikationspartnern hergestellt wird, sondern die Pakete ohne Flusskontrolle vom Sender zum Empfänger gesendet werden.

UDP findet in vielen Industrienetzen Einsatz als Transportprotokoll. Es bietet sich, vor allem durch seine Simplizität und den geringen Overhead im Netzwerk für die Informationsverteilung mit niedrigen Latenzzeiten an. Durch die Broad- und Multicast Funktionalitäten des UDP ist es möglich über das Publish-Subscribe Pattern zu kommunizieren und somit die Netzlast bei eine großen Anzahl von Empfängern gering zu halten. Diese Form der Informationsverteilung über UDP wird in Unterabschnitt 4.6.3 mit Bezug auf das Protokoll OPC UA analysiert.

UDP führt keine Validierung der Absenderadresse im Paketheader durch (Olsen 2003). Dies ermöglicht die Anwendung von IP Spoofing. IP Spoofing kann genutzt werden, um DoS bzw. DDoS Angriffe auf ein System durchzuführen. Eine Analyse des Netzwerkdienstes DNS, welcher auf der Nutzung des Transportprotokolls UDP basiert, wird in Kapitel Unterabschnitt 4.6.1 beschrieben und durchgeführt.

4.6 Anwendungsschicht

Die Netzwerkkommunikation der Anwendungsschicht in Industrie 4.0 Umgebungen basiert auf dem IP der Internetschicht. Um die Integration und Verwaltung der Netzwerkteilnehmer zu erleichtern, werden IP basierende Dienste wie DNS für die Namensauflösung sowie DHCP für die Adressvergabe und das Routing genutzt.

[11] Link - https://tools.ietf.org/html/rfc768
[12] verbindungslos - TODO
[13] nicht zuverlässig - TODO
[14] Overhead - TODO
[15] Fire-and-Forget - TODO

Des Weiteren wird sie in Industrieumgebungen durch eine Vielzahl von Protokollen beschrieben. Bestehende Lösungen des IoT nutzen Protokolle wie HTTP, XMPP oder Simple Mail Transfer Protocol (SMTP) zur Kommunikation über das Netzwerk. In der M2M Kommunikation des IIoT haben sich die Protokolle und Standards OPC UA, DDS, MQTT und CoAP für unterschiedliche Anforderungen an die Netze und deren Teilnehmer hervorgetan.

4.6.1 DNS

DNS wird von der IETF in den Request for Comments (RFC) 1034[16], 1035[17], 2181[18] und 2782[19] 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*[20], 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*[21] so manipuliert, dass sie vorgeblich vom *authorativen* Nameserver stammen.

[16] Domain Names – Concepts and Facilities
[17] Domain Names – Implementation and Specification
[18] Clarifications to the DNS Specification
[19] A DNS RR for specifying the location of services (DNS SRV)
[20] Cache Poisoning - iwas
[21] IP Spoofing bezeichnet das Versenden von IP Paketen mit gefälschter Absender-IP

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 gehalten werden. Ist dies nicht möglich, kann mit Hilfe eines DoS bzw. DDoS Angriffs 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[22] nachgewiesen werden.

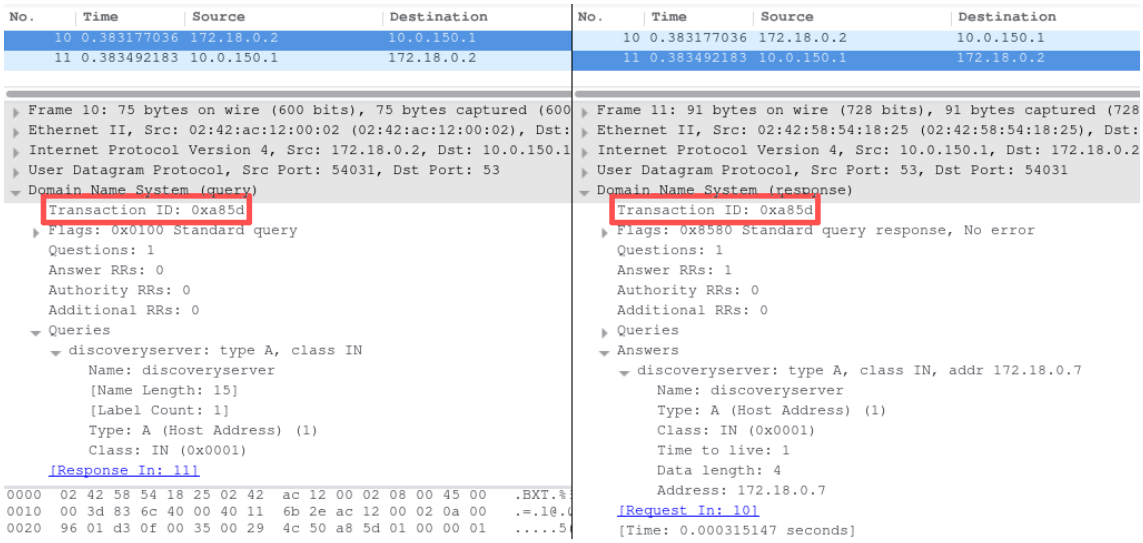


Abbildung 4.2: Wireshark - ID im DNS Header

[22] 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 DNS Nameservers zu sehen.

DNS Amplification

Eine Form eines DDoS Angriffs (**??**) ist über DNS möglich und wird DNS Amplification genannt. Bei der DNS Amplification werden DNS Anfragen an offene Nameserver gesendet und mit Hilfe von IP Spoofing als Quell-IP die Adresse des Angreifers genutzt. Somit treffen die DNS Antworten beim anzugreifenden System ein und belasten dieses durch erhöhten Rechenaufwand sowie dessen Netzwerk durch Traffic. Ein weiterer Seiteneffekt dieses Angriffs ist eine hohe Last der Nameserver, welches durch das rekursive Verhalten der DNS Namensauflösung hervorgerufen wird. DNS Amplification bezeichnet eine Form des Destributed-Reflected-Denial-of-Service (DRDoS).

Mit der Erweiterung des DNS in der IETF RFC 2617[23] wurde es notwendig, die Größe der DNS Antworten von 512 Byte auf einen dynamischen Puffer bis über 4000 Bytes zu erhöhen, um zusätzliche Informationen und Flags wie Abbildung 4.6.1 über das DNS übertragen zu können. Dies wird sich vom Angreifer zunutze gemacht, da an den Nameserver Requests mit einer Paketgröße von 60 Bytes gesendet werden können, welche eine Antwort mit 4000 Bytes und mehr provozieren und somit einen Base Amplification Factor (BAF) von ca. 66 im Netz haben. Ledermüller 2009. Der BAF beschreibt das Verhältnis von Eingang- zum Ausgangssignal. Dies wird bei DNS Amplifikation durch die Paketgröße der Anfrage sowie der Antwort dargestellt.

Die folgende Abbildung stellt einen DDoS Angriff durchgeführt durch DNS Amplification schematisch dar. Der Angreifer (links) sendet zu zwei offenen Nameservern gefälschte DNS Anfragen mit Quelladresse des Opfers (rechts). Die offenen Nameserver erfragen beim authorativen Nameserver die Zone, dieser stellt die erfragten RR bereit und die offenen Nameserver senden dem Opfer Antworten zu.

[23] Link - https://www.ietf.org/rfc/rfc2671.txt

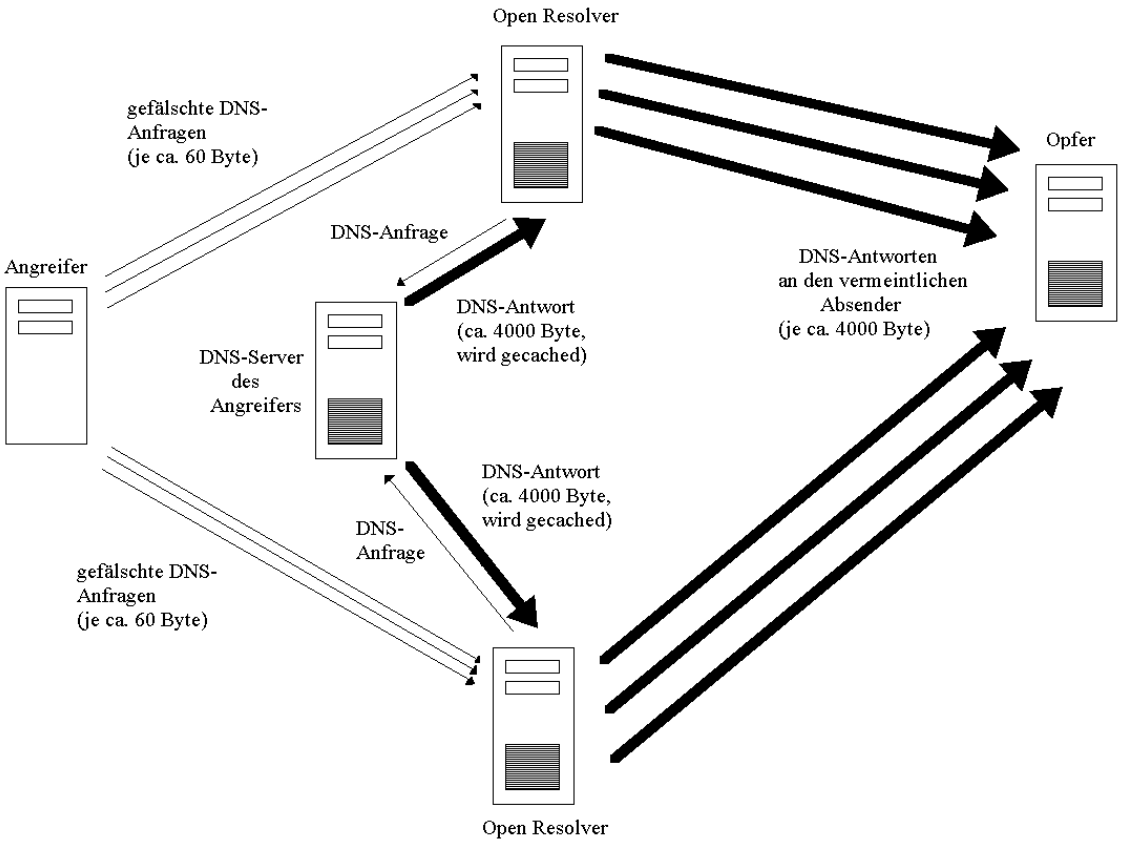


Abbildung 4.3: Schematisches Beispiel: DNS Amplification

Diese Form des Angriffs kann aus dem internen Netz sowie von extern auf öffentlich zugängliche Systeme durchgeführt werden. DoS Attacken stellen besonders für Industrie 4.0 Netzwerke, deren komplexe Kommunikation und Anforderungen eine hohe Bedrohung dar. Durch den erheblichen BAF können diese Angriffe mit wenig Bandbreite beim Angreifer durchgeführt werden und gleichzeitig das Netzwerk des Opfers voll auslasten. Wie in Abbildung Abbildung 4.4 dargestellt, kann durch die Abfrage der Zone *isc.org* eine 3385 Byte große Antwort vom Nameserver provoziert werden.

```
; <<>> DiG 9.13.0 <<>> -t any isc.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45468
;; flags: qr rd ra; QUERY: 1, ANSWER: 32, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;isc.org.                       IN      ANY

;; ANSWER SECTION:
isc.org.                7200    IN      SPF     "v=spf1 a mx ip4:204.1
isc.org.                7200    IN      CAA     0 issue "letsencrypt.o
isc.org.                60      IN      A       149.20.64.69
isc.org.                7200    IN      MX      20 mx.ams1.isc.org.
isc.org.                7200    IN      TXT     "google-site-verificat
isc.org.                7200    IN      CAA     0 iodef "mailto:hostma
isc.org.                7200    IN      NS      ams.sns-pb.isc.org.
isc.org.                7200    IN      NS      ord.sns-pb.isc.org.
isc.org.                7200    IN      CAA     0 issue "comodoca.com"
isc.org.                7200    IN      MX      10 mx.pao1.isc.org.
isc.org.                7200    IN      SOA     ns-int.isc.org. hostma
isc.org.                7200    IN      DNSKEY  257 3 5 BEAAAAOhHQDBrh
isc.org.                7200    IN      CAA     0 issue "Digicert.com"
isc.org.                7200    IN      DNSKEY  256 3 5 AwEAAcdkaRUlsR
isc.org.                7200    IN      NS      ns.isc.afilias-nst.inf
isc.org.                7200    IN      TXT     "v=spf1 a mx ip4:204.1
isc.org.                3600    IN      NSEC    _adsp._domainkey.isc.o
isc.org.                7200    IN      NAPTR   20 0 "S" "SIP+D2U" ""
isc.org.                7200    IN      NS      sfba.sns-pb.isc.org.
isc.org.                60      IN      AAAA    2001:4f8:0:2::69
isc.org.                7200    IN      RRSIG   SOA 5 2 7200 201807112
isc.org.                7200    IN      RRSIG   NS 5 2 7200 2018071123
isc.org.                60      IN      RRSIG   A 5 2 60 2018071123340
isc.org.                7200    IN      RRSIG   MX 5 2 7200 2018071123
isc.org.                7200    IN      RRSIG   TXT 5 2 7200 201807112
isc.org.                60      IN      RRSIG   AAAA 5 2 60 2018071123
isc.org.                7200    IN      RRSIG   NAPTR 5 2 7200 2018071
isc.org.                3600    IN      RRSIG   NSEC 5 2 3600 20180711
isc.org.                7200    IN      RRSIG   DNSKEY 5 2 7200 201807
isc.org.                7200    IN      RRSIG   DNSKEY 5 2 7200 201807
isc.org.                7200    IN      RRSIG   SPF 5 2 7200 201807112
isc.org.                7200    IN      RRSIG   CAA 5 2 7200 201807112

;; Query time: 596 msec
;; SERVER: 10.0.150.1#53(10.0.150.1)
;; WHEN: Mo Jun 18 18:04:45 CEST 2018
;; MSG SIZE  rcvd: 3385
```

Abbildung 4.4: DNS Amplification am Beispiel von isc.org

Dies führt zu einem BAF von ca. 56. Die folgende Grafik stellt einen Angriff mit diesem BAF dar. Auf der X-Achse ist die Anzahl der gesendeten Pakete dargestellt, die Y-Achse zeigt die Last des Netzwerkes in Gigabit auf. Die Kurven beschreiben das Netz des Angreifers sowie des Opfers.

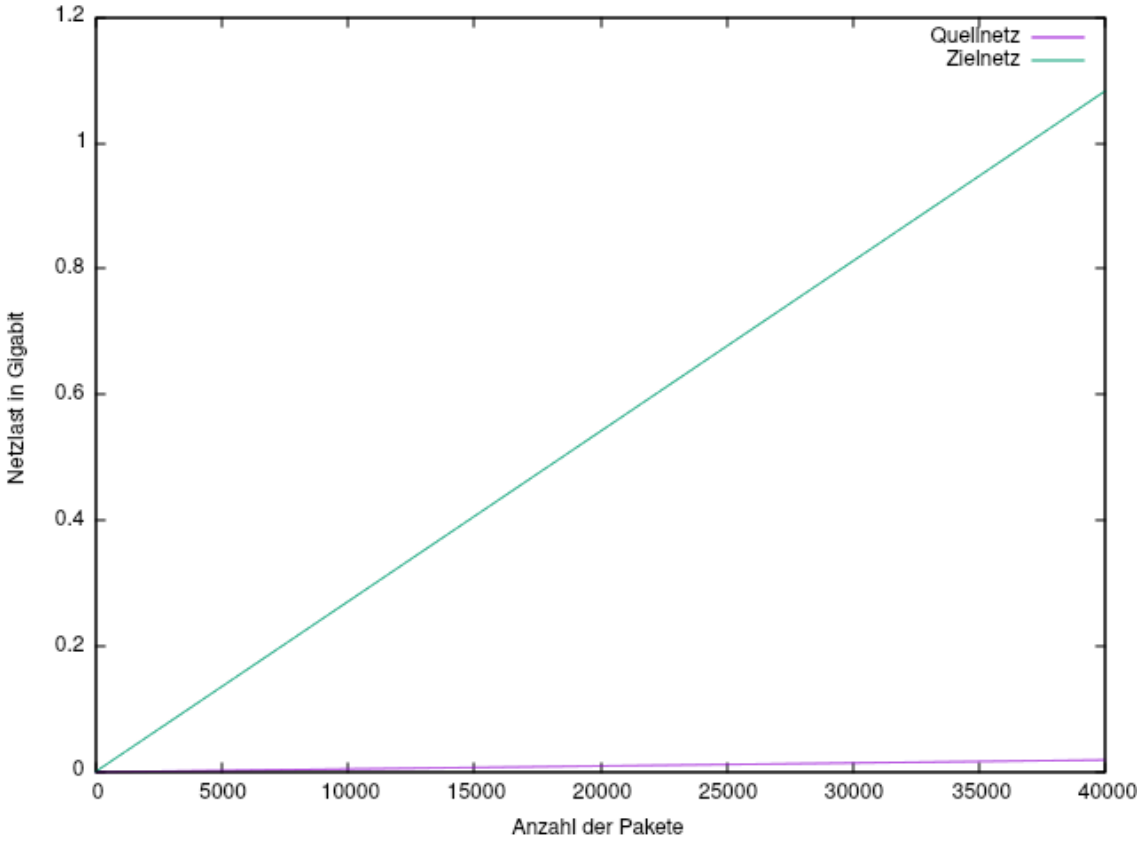


Abbildung 4.5: Netzlast bei DNS Amplification

Auf der Darstellung ist zu erkennen, dass bei diesem Angriff eine lineare Steigerung der Netzlast in beiden Netzen vorliegt. Entscheidend ist jedoch der BAF, welcher das Verhältnis zwischen der Lastzunahme im Angreifer- und Opfernetz beschreibt. Es ist zu erkennen, dass beim Versandt von 35000 Paketen im Quellnetzwerk nur ca. 0.016 Gigabit Daten transferiert werden müssen, dafür aber knapp 1 Gigabit an Daten in das Zielnetzwerk übertragen werden und dort für eine erhebliche Last sorgen.

Der DNS bietet weitere Angriffsmöglichkeiten wie DNS Fast Fluxing oder DNS Information Leakage. Diese Angriffe dienen zum *Phishing* von Daten oder der Spionage der Netzwerkstruktur. Sie nehmen initial keinen Einfluss auf den Netzwerkverkehr und dienen der Vorbereitung von Folgeangriffen und dem Sammeln von Informationen. Die Angriffsformen werden in Ledermüller 2009 näher beschrieben. Die Analyse der Sicherheit der Netzwerkkommunikation beschränkt sich auf Angriffe, welche direkten Einfluss in die Kommunikation im Netzwerk haben. Weitere Formen der DoS/DDoS Angriffe finden auf Transportschicht Abschnitt 4.5 durch *SYN-Flooding* oder auf Anwendungsschicht Abschnitt 4.6 zur Negierung eines Speziellen Dienstes statt.

TODO - Schutzmaßnahmen sind DNSSEC und zufällige Informationen TODO - Die Auswirkungen eines solchen Angriffs ... TODO - Sicherheitsmaßnahmen siehe Ledermüller 2009

4.6.2 DHCP

DHCP ist von der IETF im RFC 2131[24] definiert. Es stellt ein Framework zur Bereitstellung von *Host* Konfigurationsparamertern in einem TCP/IP Netzwerk dar. Dazu gehören die IP Adresse, Netzmaske, Gateway sowie zuständiger DNS des Clients. Da ein neuer Client im Netzwerk keine Informationen über die vorhandenen Clients und dessen Topologie besitzt, muss er, um die Konfigurationsparameter für das Netzwerk zu erhalten (DHCP Discover), über einen Broadcast im Netz nach Adress-Angeboten fragen. Dieser findet über das Transportprotokoll UDP statt über die Ports 67 (Server) und 68 (Client) statt.

Der Mangel an Informationen bei der initialen Verbindung eines Clients im Netzwerk, kann von einem Angreifer genutzt werden, um die Netzwerkkonfiguration

[24] Link - https://www.ietf.org/rfc/rfc2131.txt

zu manipulieren. Da der Broadcast des Clients an das gesamte Netzwerk versandt wird, ist es dem Angreifer möglich selbst auf diese Anfrage zu antworten. Hierzu wird die Technik des Spoofing in Verbindung mit ARP Poisoning oder einem zusätzlichen DHCP Server (Rogue DHCP), welcher vom Angreifer kontrolliert wird, im Netzwerk genutzt. In diesem Fall muss es dem Angreifer nur gelingen schneller auf den DHCP Discover bzw. DHCP Request des Clients zu antworten als der zuständige DHCP Server. Somit ist es möglich die Netzwerkkonfiguration des Clients zu manipulieren.

In Kapitel **??** wird die Erweiterung des Testsystems (Weber 2018) um einen zusätzlichen DHCP Server im Netzwerk durchgeführt, um mögliche Auswirkungen auf den Netzwerkverkehr an einem praktischen Beispiel darzustellen. Durch die Implementierung eines weiteren DHCP Servers im Netzwerk wird ein Eingriff auf das Netzwerk in der Netzzugangsschicht und die gleichzeitige Manipulation des DHCP der Anwendungsschicht des TCP/IP Referenzmodells beschrieben.

Ein Angriff auf das DHCP in Netzwerken kann weitreichende folgen für die Netzwerksicherheit mit sich bringen. Durch die Änderung der Client-Adressen und Subnetze kann es zu IP Adresskonflikten im Netzwerk kommen oder die Kommunikation beschränkt bzw. stillgelegt werden. Weitreichendere Auswirkungen auf die Netzwerksicherheit stellt das Umlenken des Datenverkehrs durch Manipulation der DNS- bzw. Gateway-Parameter dar. Hierbei kann der gesamte Netzwerkverkehr eines Clients umgelenkt werden, um einen Man in the Middle (MitM) Angriff durchzuführen und den Netzwerkverkehr auszulesen.

Da das IP Hilfsprotokoll DHCP keine Sicherheitsmaßnahmen zur Verhinderung dieser Angriffe mit sich bringt, ist es notwendig sich vor diesen Bedrohungen schon auf den unteren Schichten des TCP/IP Referenzmodells zu schützen. Eine in der Industrie weit verbreitete Technik zum verhindern von Angriffen auf das DHCP wird bereits in der Netzzugangsschicht umgesetzt. Netzwerkkomponenten wie Router und Swichtes werden mit Hilfe von DHCP Snooping konfiguriert, welches es ermöglicht DHCP Nachrichten zu überwachen und diese nur von vertrauenswürdigen Ports in das Netzwerk weiterzuleiten. Somit werden DHCP Pakete, welche von einem im Netzwerk eingeschleusten Rogue-DHCP im Netzwerk verteilt werden sollen direkt verworfen und nehmen keinen Einfluss auf das bestehende Netzwerk.

4.6.3 OPC UA

Die Kommunikation zwischen OPC UA Komponenten findet auf der Anwendungsschicht des TCP/IP Referenzmodells statt. OPC UA stellt eine vertikale Verbindung der Kommunikationspartner auf allen Ebenen der Automatisierungspyramide her. Aufgrund der Öffnung von Unternehmen nach außen, den immer höheren Informationsbedarf und die direkte Kommunikation mit Händler und Kunden ist OPC UA ein attraktives Ziel für Industriespionage und Sabotage des Netzwerks (OPC Foundation 2018b).

OPC UA wurde als Client-Server Architektur entwickelt. Um OPC UA auch in Systemen der unteren Ebenen der Automatisierungspyramide, wie Kleinsteuerungen, Sensoren und Low-End-Embedded-Systeme, einsetzen zu können, werden meist geringe Latenzen in den Netzwerken und ein geringer Overhead aufgrund von Ressourcenmangel sowie die Kommunikation mit mehreren Partnern benötigt. Diese Anforderungen werden von dem im Jahr 2018 veröffentlichten 14 Teil der OPC UA Spezifikation *Publish Subscribe* adressiert. Das *Publish Subscribe* Modell wird mit Hilfe des Transportprotokolls UDP umgesetzt und ermöglicht den Multi- und Broadcast sowie die Möglichekit der häufigen Übertragung von kleinen Datenmengen um *Logging* oder *Monitoring* durchzuführen, ohne das Netzwerk durch einen 3-Wege-Handshake bei jedem Verbindungsaufbau zusätzlich zu belasten (OPC Foundation 2018a).

Aus zeitlichen Gründen wird sich im weiteren Verlauf der Thesis auf die Sicherheit der Netzwerkkommunikation im etablierten OPC UA *Client Server* Modell beschränkt.

Die OPC UA beschreibt ein mehrschichtiges Sicherheitskonzept, welches *Transport Layer-* und *Application Layer Security* umfasst. Die *Transport Layer Security* stellt die Sicherheit auf Nachritenebene her und beinhaltet *Application Authentication*, *Integrity* und *Confidentiality*. Um dies zu ermöglichen, werden verschiedene Transport- sowie Anwendungsprotokolle im Verbund genutzt. Die Sicherheit auf Anwendungsebene stellt weitere Sicherheitsmechanismen zur *Availability*, *Auditing*, *User Authorization* und *User Authentication* bereit.

Transport Layer Security

Die OPC UA beschreibt mit dem OPC UA Connection Protocol (UACP) ein abstraktes Protokoll zur Herstellung einer Vollduplexverbindung in einer Client-Server Architektur. Implementierungen dieses Protokolls können über jede Middleware, welche den Austausch von Nachrichten im Vollduplexverfahren über TCP/IP und *Websockets* unterstützt, durchgeführt werden. Somit ist das von OPC UA spezifizierte Protokoll für die Zukunft flexibel. Die Spezifikation des abstrakten Protokolls UACP wird im 5. Teil der OPC UA Spezifikation[25] beschrieben und beinhaltet die Form der Nachricht, den Verbindungsaufbau, die Kommunikation und die Fehlerbehandlung.

In Abbildung 4.6 ist dargestellt, dass OPC UA verschiedene Protokollestacks für unterschiedliche Anforderungen zur Kommunikation zwischen den Komponenten bereitstellt. Diese bestehen aus einer Verbindung von TCP auf Transportebene und dem Unified Architecture (UA) Binary Protokoll zur Kodierung der Nachrichten, einem Webservice über HTTP/Hypertext Transfer Protocol Secure (HTTPS) und Simple Object Access Protocol (SOAP) mit Extensible Markup Language (XML) Encoding oder einer hybriden Form aus beiden. Alle Kommunikationsformen beinhalten ein Sicherheitsmodell auf Transport- oder Nachrichtebene.

[25] OPC Unified Architecture Specification Part 6: Mappings (OPC Foundation 2018c)

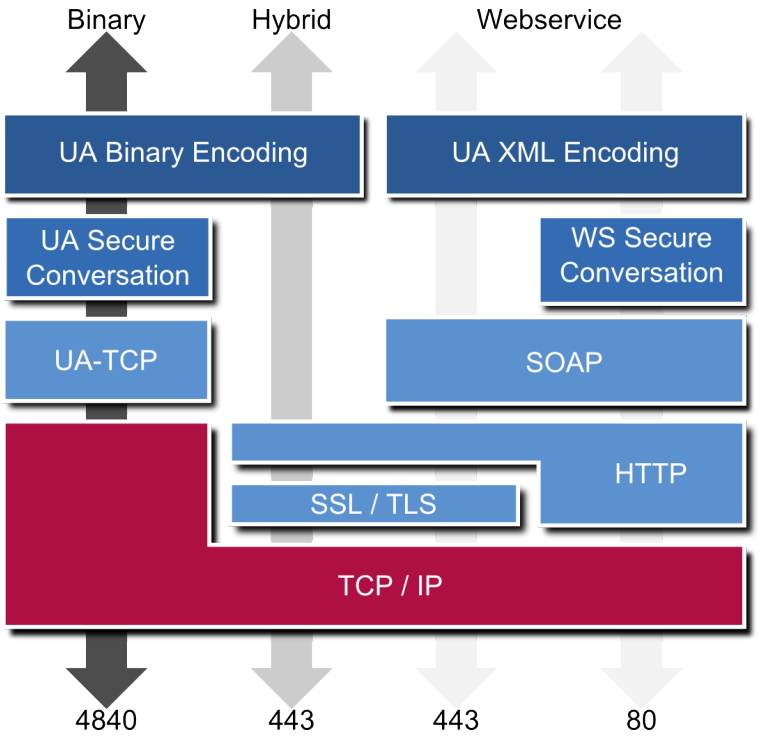


Abbildung 4.6: OPC UA Kommunikationswege

Die beschriebenen Protokollstacks bilden mit ihren Sicherheitsmechanismen die Grundlage für eine sichere Datenübertragung. Die Form der Datenübertragung über SOAP/HTTP wurde ab Version 1.03 der Spezifikation als veraltet angesehen, da es in der Industrie nicht umgesetzt wurde (OPC Foundation 2018c). Die Protokolle UA Binary über TCP und die Hybridform aus den Protokollen UA Binary und HTTPS Webservice werden im folgenden auf ihre Standhaftigkeit bzgl. der Sicherheitsanforderungen in Industrie 4.0 Umgebungen analysiert.

UA Binary über TCP

Das UA Binary Protokoll über TCP wird für Kommunikation mit optimierter Geschwindigkeit und Durchsatz genutzt. Es besitzt den geringsten Overhead sowie Ressourcenverbrauch, da kein zusätzlicher Parser für HTTP oder XML genutzt werden muss und somit die Systemlast gering gehalten werden kann. Zur Kommunikation wird standardmäßig der Port 4840 genutzt. Die sichere Kommunikation wird erst auf Nachrichtenebene durch die UA Secure Conversation hergestellt (siehe Abschnitt 4.6.3). Für die Transportebene gelten durch das genutzte Protkoll TCP weiterhin die Bedrohungen von Unterabschnitt 4.5.1.

UA Binary über HTTPS

Die Hybridform der Kommunikation über einen HTTPS Webservice mit Hilfe der UA Binary Protokolls vereint die Vorteile des Ressourcenschonenden UA Binary Protokolls über TCP und die weitreichende Kompatibilität eines Webservice. Die Sicherheit der Netzwerkkommunikation wird bereits auf der Transportebene mit Hilfe von Transport Layer Security (TLS) hergestellt.

Die Transportsicherheit wird mit TLS 1.2 und der Cipher Suite *TLS RSA WITH AES 256 CBC SHA256* bereitgestellt (OPC Foundation 2018d). Hierbei ist zu beachten, dass die Rechenleistung der Systeme wächst und somit Verschlüsselungsalgorithmen mit der Zeit unsicher werden. Eine TLS Verbindung mit schwacher Cipher Suite stellt keine sichere Verbindung bereit. Des Weiteren wurden in den Implementierungen von TLS Fehler verursacht, welche die Transportsicherheit wie z. B. im Falle von *Heartbleed*[26] verhinderten.

[26] Link zu Heartbleed

Eine weitere Bedrohung stellt das genrelle Verfahren der Ausstellung von Zertifikaten bereit. Diese Zertifikate werden von Dienstleistern ausgestellt, welche als vertrauenswürdig eingestuft und als Root-Certificate Authority (CA) bezeichnet werden. Die Herstellung der Vertrauenswürdigkeit eines Ausstellers liegt im Ermessen des Softwareherstellers und dessen Aufnahme in die Liste vertrauenswürdiger CA.

TODO - zu dünn

Die Kommunikation des Protokolls OPC UA über Webservices und HTTP bzw. HTTPS wird im Rahmen dieser Thesis nicht weiter bearbeitet, da die Implementierung des im Testsystem genutzten NodeJS Moduls node-opcua unvollständig ist.

Application Layer Security

OPC UA stellt aufgrund der verschiedenen Anforderungen der Industrie an ihre Systeme mehrere Sicherheitskonfigurationen zur Informationsübertragung zur Verfügung. Dies ist notwendig, da die Verwendung von Verschlüsselungsalgorithmen und Kodierungsverfahren Ressourcen benötigt und Latenzen verursacht, welche unter Umständen nicht vorhanden sind oder nicht geleistet werden können. Eine Fehlkonfiguration des Protokolls kann jedoch auch Auswirkungen auf den Betrieb des Netzwerks und der Komponenten haben sowie die Integrität der Daten gefährden.

OPC UA verifiziert vor dem Austausch von Nachrichten zwischen zwei Komponenten, ob ein SecureChannel vorhanden ist, über welchen die Daten übertragen werden. Dieser wird vom bestehenden Netzwerkstack und den genutzten niedrigeren Protokollen bereitgestellt (OPC Foundation 2018a). Die UA Secure Conversation besteht aus dem *Secure Channel* und der Session und desssen gesetzten *SecurityMode* (OPC Foundation 2018b). Die Form der Nachrichten im *Secure Channel* wird durch den in der gewählen *Security Mode* bestimmt. Bei der Verwendung der *Security Policy* None wird ein *Secure Channel* hergestellt, welcher jedoch keine Sicherheitsprofile bereitstellt (OPC Foundation 2018d). Dies wird in Abbildung 4.7 dargestellt.

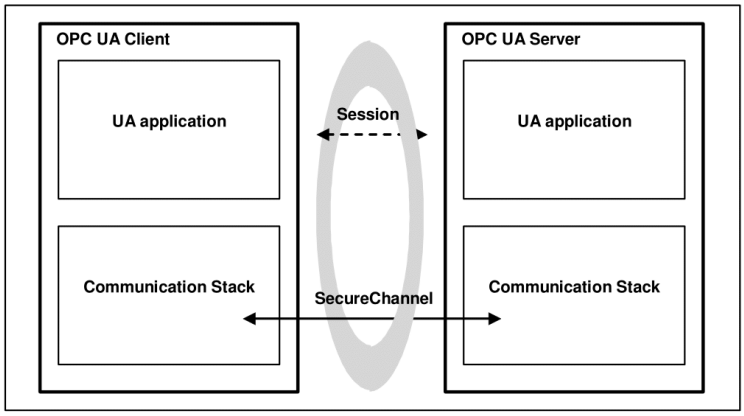


Abbildung 4.7: OPC UA Secure Channel

Mit Hilfe des vorhandenen Testsystems (Weber 2018) kann dieses Verhalten nachgewiesen werden. Hierfür wurde das Netzwerkanalysetool Wireshark[27] genutzt, um an der Netzwerkbrücke der Docker Container den Netzwerkverkehr zwischen den Komponenten abzuhören. In Verbindung mit dem OPC UA *Secure Channel* wurde das System erweitert, um verschiedene Sicherheitsprofile für die Kommunikation bereitzustellen. Die Erweiterung des Systems wird in **??** beschrieben.

Die folgenden Abbildungen zeigen die Ergebnisse der Paketanalyse mit der vorhandenen Security Policies "none". Der OPC UA Client des Control Containers, welcher die Liste der im Netzwerk vorhandenen OPC UA Server abfrägt besitzt die IP-Adresse 172.18.0.6, der Container des Discoveryservers die IP-Adresse 172.18.0.2. In Abbildung 4.8 ist der Request des Control Containers zum Aufbau eines *Secure Channel* dargestellt. Die verwendete *Security Policy* ist im Bereich SecurityPolicyUri des OPC UA Protokolls beschrieben. In Abbildung 4.9 ist die Antwort des OPC UA Discoveryservers im *Secure Channel* dargestellt.

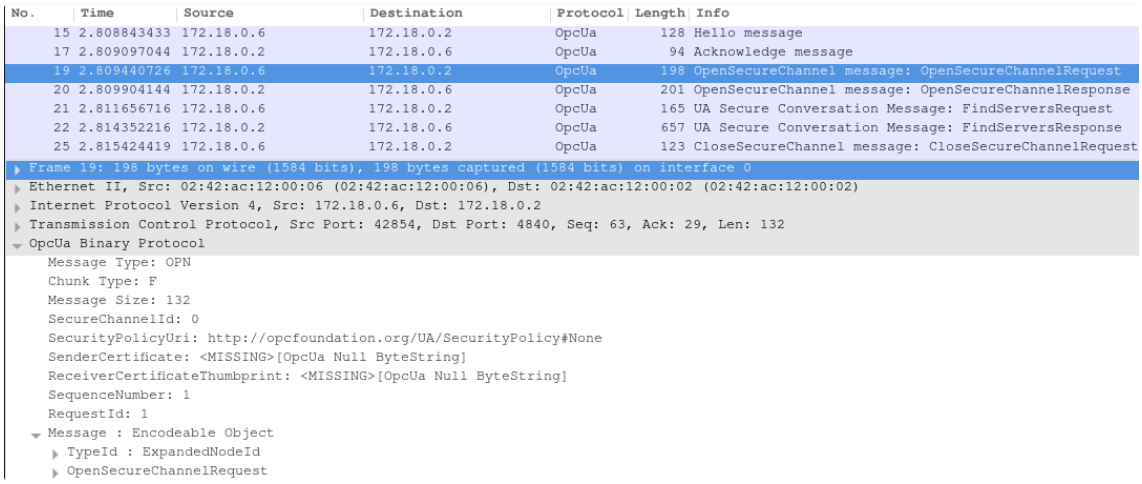


Abbildung 4.8: Paketanalyse OPC UA - Client Request bei Sicherheitsprofil "none"

[27] TODO - WIRESHARK

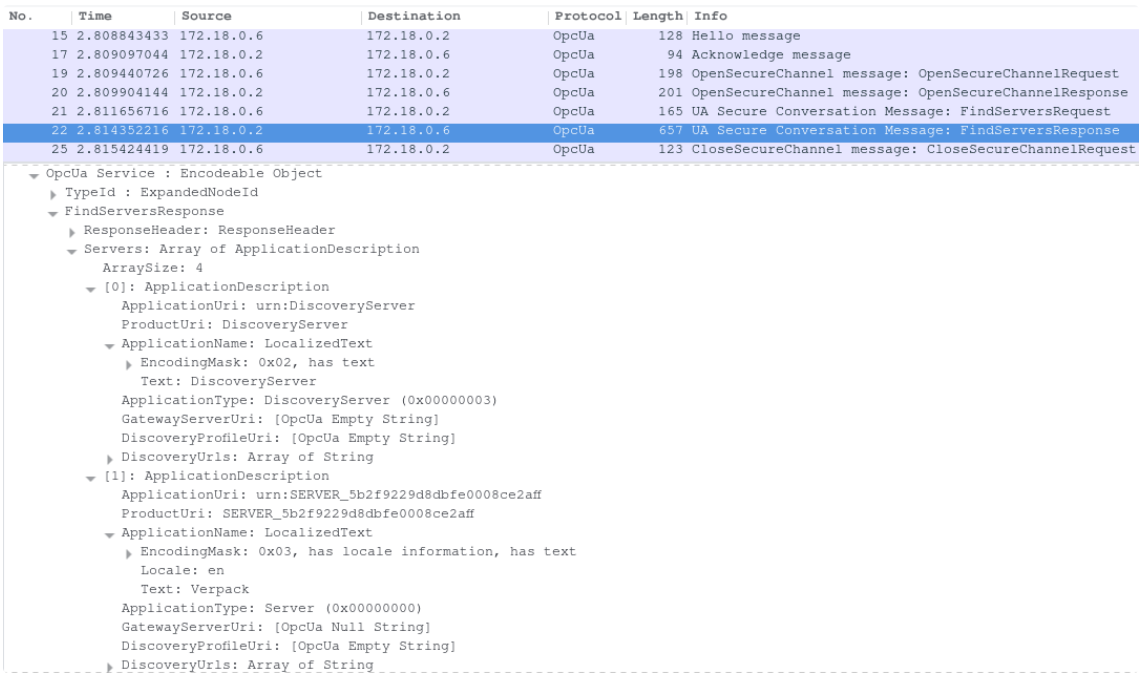


Abbildung 4.9: Paketanalyse OPC UA - Server Response bei Sicherheitsprofil "none"

Es ist zu erkennen, dass die Kommunikation, obwohl der *Secure Channel* genutzt wird, nicht verschlüsselt ist. Die Endpunkte sowie deren Adressen und bereitgestellte Methoden können aus den Paketen ausgelesen werden.

Im Folgenden wird erneut das Abfragen des Control Containers aller im Netzwerk vorhandenen Endpunkte beim Discoveryserver beschrieben, jedoch wird das Sicherheitsprofil "Basic256Sha256"mit dem *MessageSecurityMode* SSIGNANDENCRYPT"genutzt. Der OPC UA Client besitzt die IP-Adresse 172.18.0.7. Der Discoveryserver weiterhin die Adresse 172.18.0.2. Abbildung 4.10 zeigt den Request, Abbildung 4.11 die verschlüsselte Response im *Secure Channel*.

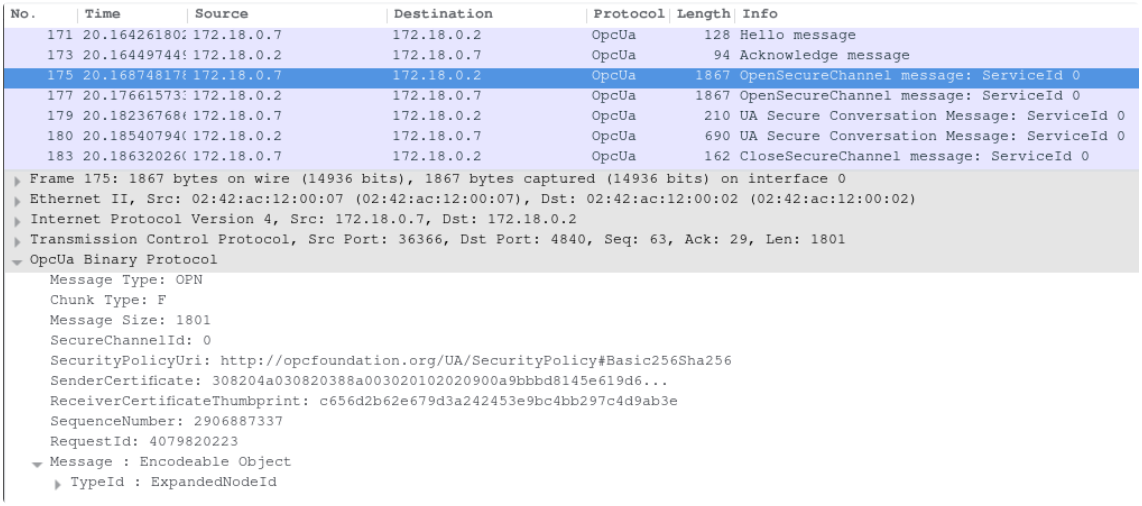


Abbildung 4.10: Paketanalyse OPC UA - Client Request bei Sicherheitsprofil "Basic256Sha256ünd MessageSecurityMode SSIGNANDENCRYPT"

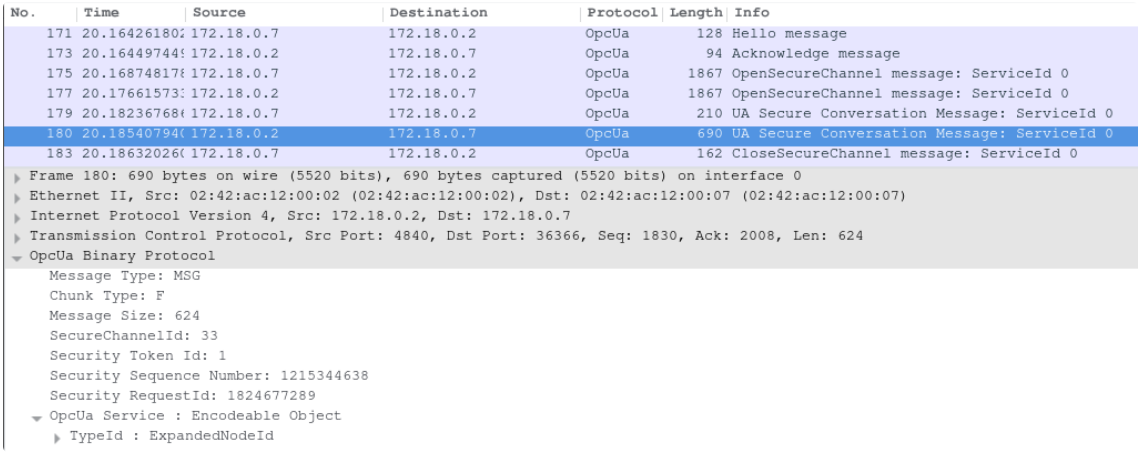


Abbildung 4.11: Paketanalyse OPCUA - Server Response bei Sicherheitsprofil "Basic256Sha256ünd MessageSecurityMode SSIGNANDENCRYPT"

Es ist zu erkennen, dass der gesamte Netzwerkverkehr im *Secure Channel* durch ein Zertifikat signiert sowie durch den Algorithmus SHA256 verschlüsselt wurde. Die Integrität und Vertraulichkeit während der Kommunikation im Netzwerk ist gewährleistet.

Es ist zu Beachten, dass - TODO Rechenleistung erhöht sich -> Verschlüsselungsalgorithmen werden unsicher -> OPC ist flexibel für zukunft und anforderungen

weitere Sicherheitsbestandteile

TODO - PKI TODO - Zertifikatsmanagement TODO - Zeitsynchronisation TODO - Kerberos OAuth2 TODO - siehe BSI UPC UA Analyse

4.6.4 MQTT/CoAP

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

4.7 Schutzmaßnahmen

TODO - Applikationssicherheit != Netzwerksicherheit != Betriebssystemsicherheit

4.7.1 allgemeine Schutzmaßnahmen

TODO - Schutz auf allen Ebenen -> z.B. OPC UA basiert auf IP-Netz -> Angriffsvektoren von IP und genutzten Diensten immer noch zutreffend

4.7.2 TODO

4.7.3 TODO

4.7.4 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[28] 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 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.

[28] ref. IEC 62443

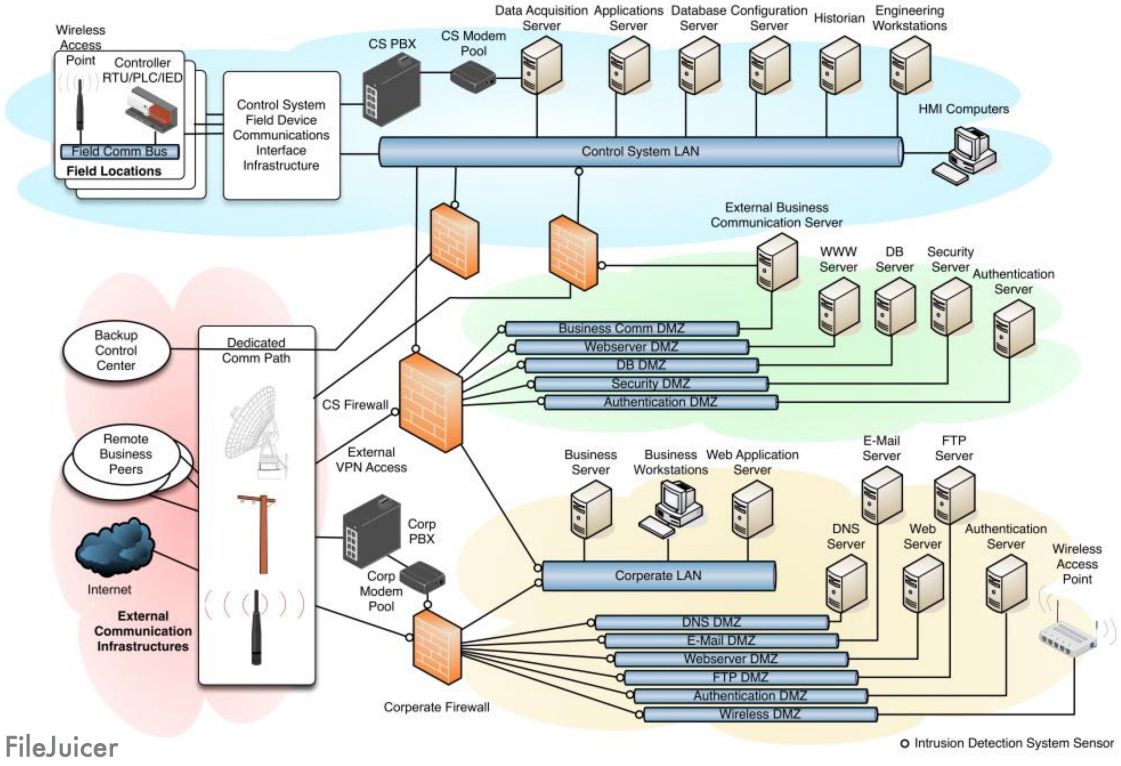


Abbildung 4.12: Defense in Depth Strategie - David Kuipers 2006

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.

Kapitel 5

Implementierung

Die prototypische Implementierung von verschiedenen Angriffsformen im Industrie 4.0 Testsystem wird genutzt, um die Analyse der in Kapitel 4 beschriebenen Bedrohungsszenarien und deren Auswirkungen an einem vorhandenen System zu testen und deren Einfluss auf die Netzwerkkommunikation zu bewerten. Mit der Implementierung der Angriffe wird die im Konzept (Kapitel 3) beschriebene Vorgehensweise validiert. Die Auswahl der implementierten Angriffsformen wird vom Testsystem und dessen Infrastruktur bzw. Umsetzung bestimmt. Aus zeitlichen Gründen und aufgrund von Beschränkungen durch das Testsystem (siehe Abschnitt 3.3) werden nicht alle analysierten Angriffe in der Praxis implementiert.

Die Implementierung umfasst die Erweiterung und Anpassung des vorhandenen Systems. Die vorhandene Implementierung über das Protokoll OPC UA wird angepasst, um die Kommunikation über den *Secure Channel* mit Hilfe verschiedener Sicherheitsprofile zu analysieren. Hierbei wird eine unverschlüsselte sowie verschlüsselte Kommunikation zwischen OPC UA Client und Server bereitgestellt.

Das Testsystem wurde um einen zusätzlichen OPC UA Produktionsserver erweitert. Dieser dient als Gateway zur Kommunikation mit einer Komponente, welche das Protokoll MQTT zur Nachrichtenübermittlung nutzt. Das Szenario dient der Analyse eines weiteren IIoT Protokolls in Verbindung mit einer OPC UA Umgebung.

Des Weiteren wurde ein zusätzliches System bereitgestellt, welches verschiedene Angriffsmöglichkeiten auf das vorhandene Netzwerk bereitstellt. Hierbei handelt es sich um bekannte Angriffsformen, welche Bezug auf die in Abschnitt 4.1 genannten Bedrohungen auf Industrie 4.0 Umgebungen nehmen.

Ausgeschlossen von der Implementierung sind die Angriffsformen des DHCP und ARP Spoofing. Diese wären, wie in Abschnitt 3.3 beschrieben nur mit erheblichem Mehraufwand möglich, da ein gesamtes Netzwerk mit eigenem DHCP und DNS bereitgestellt werden müsste, welchen Zonen und automatische DNS Updates konfiguriert werden müssten. Außerdem stellt die vorhandene Netzwerk-Infrastruktur des Testsystems mit der genutzten Docker Bridge[1] die Funktionalitäten eines MitM Angriffs und somit die Möglichkeit der Paketanalyse im Netzwerk bereits bereit.

Eine PKI sowie **IdM!** (**IdM!**) wird im vorhandenen Testsystem nicht umgesetzt, da das genutzte NodeJS Modul *node-opcua*[2] das Zertifikatsmanagement zum aktuellen Stand nicht implementiert[3].

5.1 Software

Beim verwendeten Softwarestack wurde sich weitestgehend am Testsystem (Weber 2018) orientiert, um die Kompatibilität zu bestehenden Komponenten zu gewährleisten und weiterhin ein durch Container flexibles System bereitzustellen. Für die Analyse der Netzwerkkommunikation benötigte Änderungen der Software wurden am Quellcode vorgenommen. Weitere Komponenten wurden in zusätzlichen Docker Containern implementiert.

5.2 Erweiterung des Testsystems

5.2.1 OPC UA Secure Channel

Um die Verwendung verschiedener Sicherheitsrichtlinien im OPC UA Secure Channel bereitzustellen muss die Form des Verbindungsaufbaus der vorhandenen OPC UA Clients im Quellcode geändert werden. Die OPC UA Server des Testsystems stellen die verschiedenen Sicherheitsprofile *None*, *Basic128Rsa15*, *Basic256* und *Basic256Sha256* bereit. Diese beinhalten den für die Nachrichtenübermittlung genutzten Verschlüsselungsalgorithmus. Bei der Übertragung der Daten im Secure Channel wird der OPC UA MessageSecurityMode auf das Sicherheitsprofil angewandt. Hierbei stehen die Optionen NONE, SIGN und SIGNANDENCRYPT zur

[1] text
[2] LINK
[3] TODO - Link - Github

Verfügung. Im Vorhandenen Testsystem werden keine Zertifikate verwaltet. Das Signieren der Nachrichten mit dem privaten Schlüssel des Absenders ermöglicht einen Zuwachs der Sicherheit der Netzwerkkommunikation, da dies die Integrität der Nachrichten sicherstellt. Im gegebenen System wurde eine Verschlüsselung der Nachricht auf Anwendungsebene durch den Algorithmus *Basic256Sha256* implementiert.

Der Quellcode der OPC UA Clients in den Containern *scheduler* und *control* wurde so angepasst, dass eine Aktivierung und Deaktivierung der Verschlüsselung in der Konfigurationsdatei *config.json* der jeweiligen Server vorgenommen werden kann. Zur Anwendung einer Konfigurationsänderung ist ein erneutes Bauen sowie der Neustart des Containers notwendig[4].

5.2.2 externe Komponente

TODO

5.3 Angriffsszenarien

Die verschiedenen Angriffsszenarien wurden wie auch die Erweiterung des Systems um eine externe Komponente in einem zusätzlichen Docker Container realisiert. Der Container stellt im interaktiven Homeverzeichniss Scripte bereit, um verschiedene Angriffe auf den Netzwerkstack des Testsystems durchzuführen.

TODO - vielleicht Interface

[4] TODO - siehe Repo Readme

5.3.1 SYN-Flood

5.3.2 Sockstress

5.3.3 DNS Amplification

5.4 Quellcode

Der erstellte Quellcode ist im öffentlichen GitHub Repository[5] unter der Massachusetts Institute of Technology (MIT) Lizenz verfügbar. Das Lizenzierungsmodell erlaubt die freie Nutzung und Änderung der Software durch Dritte.

Die in (Weber 2018) beschriebene Verzeichnisstruktur des genutzten Testsystems wurde beim erstellten Fork beibehalten. Das Wurzelverzeichnis des Testsystems befindet sich im im Ordner "testbed"des GitHub Repository https://github.com/fjnalta/thesis. Im Ordner "dockers"befindet sich für jede Komponente der Umgebung ein weiteres Verzeichnis. In diesen liegen die Container, der Quellcode, deren Dockerfile sowie eine Beschreibung der Funktionsweise der jeweiligen Komponente.

Es wurden Scripte zur Installation, Konfiguration sowie Verwaltung der zusätzlichen Docker Container geschrieben. Diese wurden im Ordner ßcriptsäbgelegt.

5.5 Dokumentation

Die Dokumentation der implementierten Komponenten, deren Inbetriebnahme und Funktionsweise findet neben der schriftlichen Ausarbeitung in den jeweiligen *Readme* Dateien des Repositories https://github.com/fjnalta/thesis im Verzeichnis "testbedünd dessen Unterverzeichnissen statt. Des Weiteren wurde der Quellcode der Software mit Kommentaren versehen, um eine Nutzung des Testsystems auch ohne die schriftliche Ausarbeitung zu ermöglichen.

[5] https://github.com/fjnalta/i40-testbed

Kapitel 6

Validierung

Kapitel 7

Ausblick

TODO

7.1 Analysegegenstände

PKI weitere Protokolle untersuchen -> LDAP nicht gemacht

7.2 Erweiterungen am Testsystem

Kapitel 8

Fazit

Da die grundlegende Netzwerkstruktur der TCP/IP Netzwerke für Industrie 4.0 Kommunikation übernommen wird, sind auch die damit zusammenhängenden Voraussetzungen und Sicherheitsgedanken zu beachten. Plattform Industrie 4.0 2017

Vielzahl von Angriffen auf die verschiedenen Schichten des TCP/IP Referenzmodells, welches in Industrie 4.0 Umgebungen genutzt wird. In der Thesis wurden nur wenige Beispielhafte Angriffe dargestellt und durchgeführt.

TODO - TITEL: Sicherheitsanalyse der Netzwerkkommunikation in Industrie 4.0 Umgebungen und Erweiterung einer prototypischen Industrie 4.0 Security Testumgebung um Funktionalitäten im Bereich der Netzwerksicherheit

Analyse der Netzwerkkommunikation in Industrie 4.0 Umgebungen und Erweiterung einer protoypischen Security Testumgebung zur Darstellung verschiedener Berohungsfaktoren

Security Mechanismen sind nicht umsonst und beeinträchtigen die Performance. Security sollte daher nur dort zur Anwendung kommen, wo sie auch benötigt wird. Diese Entscheidung soll aber nicht der Entwickler / Produktmanager treffen, sondern der Anlagenbetreiber (Systemadministration).

Die Nutzung von OPC UA bietet keinen automatischen Schutz der IT-Infrastruktur - Konfiguration ist notwendig. Obwohl Securiy by Design. Basiert auf Unteren Schichten.

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

OPC COM Open Platform Communications
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
HTTPS Hypertext Transfer Protocol Secure
SOAP Simple Object Access 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
ARP Address Resolution Protocol
DHCP Dynamic Host Configuration Protocol
RFC Request for Comments
IETF Internet Engineering Task Force
RR Resource Record
BAF Base Amplification Factor

DRDoS Destributed-Reflected-Denial-of-Service

VLAN Virtual Local Area Network

IPAM IP Adress Management

SYN synchronise

ACK acknowledge

SYN-ACK synchronise-acknowledge

FIN final

VoIP Voice over IP

SNMP Simple Network Management Protocol

TLS Transport Layer Security

SMTP Simple Mail Transfer Protocol

MOM Message oriented Middleware

UA Unified Architecture

XML Extensible Markup Language

CA Certificate Authority

UACP OPC UA Connection Protocol

MitM Man in the Middle

MIT Massachusetts Institute of Technology

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:

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*.

Ledermüller, Thomas (2009). „DNS-Sicherheit im Rahmen eines IT-Grundschutz-Bausteins“. In:

Network Working Group (1981). *Transmission Control Protocol*. URL: https://tools.ietf.org/html/rfc793.

Olsen, Camilla (2003). „Security issues relating to the use of UDP“. In: *Global Information Assurance Certification Paper*.

OPC Foundation (2014). „OPC Unified Architecture - Wegbereiter der 4. industriellen (R)Evolution“. In:

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

— (2018b). „OPC Unified Architecture Specification Part 2: Security Model“. In: URL: https://opcfoundation.org/UA/Part2/.

— (2018c). „OPC Unified Architecture Specification Part 5: Information Model“. In: URL: https://opcfoundation.org/UA/Part5/.

— (2018d). „OPC Unified Architecture Specification Part 7: Profiles“. In: URL: https://opcfoundation.org/UA/Part7/.

Platform Industrie 4.0 (2015). „Umsetzungsstrategrie Industrie 4.0“. In:

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: