Institut für Softwaretechnologie (ISTE)
Universität Stuttgart
Universitätsstraße 38
D-70569 Stuttgart

Institut für Steuerungstechnik der Werkzeugmaschinen und Fertigungseinrichtungen (ISW)
Universität Stuttgart
Seidenstraße 36
D-70174 Stuttgart

Bachelorarbeit

Technologierecherche zu Verzeichnisdiensten in der Produktion

Daniel Steinacker

Studiengang:	Softwaretechnik
Prüfer/in:	Prof. Dr. Stefan Wagner
Betreuer/in:	Wolfgang Fechner (ISTE), Dipl.-Ing. Felix Kretschmer (ISW)
Beginn am:	16. Juli 2018
Beendet am:	16. Januar 2019

Kurzfassung

Diese Arbeit dient als Literaturrecherche zu Technologien, die als Verzeichnisdienste in Produktionsnetzwerken verwendet werden können. Diese stammen dabei aus der Informationstechnologie (IT) oder der Produktion. Anschließend findet ein Vergleich einiger Technologien statt, die bei der Recherche gefunden wurden. Diese sind OpenLDAP, Active Directory, die Gelben Seiten der Industrie 4.0, OPC UA .Net-GDS, jabberd2, COM/DCOM, Bonjour und Avahi. Für den Vergleich wird ein Punktesystem eingeführt, dass die einzelnen Merkmale (Verbreitung, Aktualität, Reife der Entwicklung, Quellcodeverfügbarkeit, unterstützte Betriebssysteme, Sicherheit, Kosten, Standardisierung und Einsatzzweck) in Relation zueinander setzt. Die Ergebnisse sind in Tabelle 5.1 dargestellt. Mit 116 von 140 möglichen Punkten ergibt sich OpenLDAP als Empfehlung, weswegen diese Technologie zusammen mit OPC UA für die Machbarkeitsanalyse verwendet wird. Für diesen Proof of Concept werden mittels Python Daten zwischen den beiden Open Source Projekten transferiert.

Inhaltsverzeichnis

1. Einleitung **13**
1.1. Problemstellung . . . 13
1.2. Ziel der Arbeit . . . 14
1.3. Begriffsdefinitionen . . . 14
1.3.1. Verzeichnisdienst . . . 14
1.3.2. IT . . . 15
1.3.3. Produktion . . . 15
1.3.4. Industrie 4.0 . . . 15

2. Stand der Technik **17**
2.1. Verzeichnisdienste . . . 18
2.1.1. Verzeichnisdienste in der IT . . . 19
2.1.2. Verzeichnisdienste in der Produktion . . . 22
2.2. Nutzbare Technologien für Verzeichnisdienste . . . 24
2.2.1. IT . . . 24
2.2.2. Produktion . . . 26
2.3. Weitere nicht betrachtete Technologien . . . 26
2.3.1. MT Connect . . . 26
2.3.2. DDS . . . 27

3. Technologievergleich **29**
3.1. Vorgehen . . . 29
3.2. Verglichene Merkmale . . . 29
3.2.1. Verbreitung . . . 29
3.2.2. Aktualität . . . 30
3.2.3. Reife der Entwicklung (Reife) . . . 30
3.2.4. Quellcode Verfügbarkeit (Quellcode) . . . 31
3.2.5. Unterstützte Betriebssysteme (Betriebssysteme) . . . 31
3.2.6. Sicherheit . . . 31
3.2.7. Kosten . . . 32
3.2.8. Standardisierung . . . 32
3.2.9. Einsatzzweck . . . 32
3.3. Vergleich . . . 32
3.3.1. OpenLDAP . . . 32
3.3.2. Active Directory . . . 34
3.3.3. GESI . . . 35
3.3.4. OPC UA .Net-GDS . . . 36
3.3.5. jabberd2 . . . 38
3.3.6. COM/DCOM . . . 39

3.3.7. Bonjour 40
3.3.8. Avahi 41
3.4. Fazit 42

4. Prototypische Implementierung **45**
4.1. Systementwurf 45
4.2. Systemimplementierung 46

5. Zusammenfassung und Ausblick **49**

Literaturverzeichnis **51**

A. Technologieübersicht **57**

B. CVE-Bewertungen **59**
B.1. Active Directory 59
B.2. Distributed COM 61
B.3. Bonjour 61
B.4. Jabberd2 61

Abbildungsverzeichnis

2.1. Übersicht über alle betrachteten Technologien (Abbildung hochauflösend in Anhang A) 18
2.2. Multi-Master Replikation über mehrere Standorte 20
2.3. Master-Slave Replikation mit Fehlerfall 21

4.1. Konzept einer möglichen Kommunikation zwischen der IT und der Produktion. Auf Seiten der IT wird dazu ein OpenLDAP Server eingesetzt, der mittels des Proof of Concepts Daten der Produktion mit dem OPC Unified Architecture (OPC UA) Server austauschen kann. 46

A.1. Übersicht über alle betrachteten Technologien 57

Tabellenverzeichnis

3.1. Die Bewertung der Merkmale für OpenLDAP. 34
3.2. Die Bewertung der Merkmale für Active Directory. 35
3.3. Die Bewertung der Merkmale für die GESI. 36
3.4. Die Bewertung der Merkmale für OPC UA .Net-GDS. 37
3.5. Die Bewertung der Merkmale für jabberd2. 39
3.6. Die Bewertung der Merkmale für COM/DCOM. 40
3.7. Die Bewertung der Merkmale für Bonjour. 41
3.8. Die Bewertung der Merkmale für Avahi. 42
3.9. Ergebnis des Vergleichs. 42

5.1. Überblick über des Ergebnis des Vergleichs. 50

Abkürzungsverzeichnis

AD Active Directory. 6, 17

BSI Bundesamt für Sicherheit in der Informationstechnik. 15

COM Component Object Model. 26

CVE Common Vulnerability and Exposure. 31

CVSS Common Vulnerability Scoring System. 31

DCOM Distributed COM. 6, 26

DDS Data Distribution Service. 27

DNS Domain Name System. 19

GDS Global Discovery Server. 23

GPLv2 GNU General Public License Version 2. 36

IoT Internet der Dinge. 24

IP Internet Protocol. 18

ISO International Organization for Standardization. 18

IT Informationstechnologie. 3

ITU Internationale Fernmeldeunion. 18

LDAP Lightweight Directory Access Protocol. 18

LDS Local Discovery Server. 23

LGPL GNU Lesser General Public License v2.1. 41

mDNS DNS über Multicast. 22

OLE Object Linking & Embedding. 26

OPC Open Platform Communications. 26

OPC UA OPC Unified Architecture. 7

OSI Open Systems Interaction. 18

RADIUS Remote Authentication Dial-In User Service. 14

RCL Reciprocal Community License. 36

SASL Simple Authentication and Security Layer. 19

sha Secure Hash Algorithm. 19

SLA Service-Level-Agreement. 21

SNMP Simple Network Management Protocol. 17

SSH Secure Shell. 17

TCP Transmission Control Protocol. 18

TLS Transport Layer Security. 19

VNC Virtual Network Computing. 17

VoIP Voice over IP. 24

XML Extensible Markup Language. 24

XMPP Extensible Messaging and Presence Protocol. 24

1. Einleitung

Die Digitalisierung hält in immer mehr Bereichen unseres Lebens und Arbeitens Einzug. Dies ist an der weiten Verbreitung von Computern, Smartphones und anderen mit Recheneinheiten versehenen Geräten zu sehen. Vor nur ein paar Jahrzehnten war diese Entwicklung nicht abzusehen. So soll Thomas J. Watson, der ehemaligen Vorstandsvorsitzendem von IBM, 1943 gesagt haben: „Ich glaube, dass es auf der Welt einen Bedarf von vielleicht fünf Computern geben wird."[Wik]

Er hat mit diesem Satz allerdings alles andere als recht behalten; so zeigt eine Statistik des Statistischen Bundesamtes, dass im Jahr 2017 90 % der deutschen Haushalte mit einem PC ausgestattet waren, dies entspricht ca. 37 Millionen Haushalten. In Unternehmen sieht der Trend ähnlich aus, so werden in 90 % von diesen Computer eingesetzt.[Bun18; Sta17] Eine weitere Entwicklung der letzten Jahre ist, dass die Größe und der Energieverbrauch dieser Technik immer mehr geschrumpft sind. So passt heute ein vielfaches der Rechenleistung des Zuse Z1, des ersten Computers der Welt, in eine Hosentasche. Dieser Prozess kann natürlich auch in der Industrie von großem Nutzen sein. Folglich werden immer mehr Produktionsanlagen mit eigenen Recheneinheiten ausgestattet, um direkt vor Ort wichtige Informationen über deren Zustand und weitere Daten zu gewinnen. Dies macht die einzelnen Maschinen wesentlich unabhängiger von festen monolithischen Strukturen, wie fester Verkabelung in den Produktionsstätten. Weiterhin ist es natürlich auch möglich, wesentlich mehr Sensorik für die verschiedensten Einsatzgebiete einzusetzen. Eine der Bestrebungen ist es auch, jedes einzelne Bauteil welches innerhalb einer Fertigungslinie hergestellt wird, von Anfang bis Ende nahtlos verfolgbar zu machen. Dieser extreme Anstieg an einzelnen Recheneinheiten, die natürlich an den verschiedensten, möglicherweise auch unzugänglichen Stellen innerhalb einer Fertigungsanlage verteilt sein können, birgt aber auch Probleme in sich.[KWH13]

Im Folgenden wird zuerst die Problemstellung und das Ziel der Arbeit vorgestellt, darauf folgt eine Beschreibung des Stands der Technik, in welchem alle Technologien, auf die in dieser Arbeit eingegangen wird, beschrieben werden. Darauf folgt ein Vergleich dieser Technologien. Zuletzt wird die im Zuge dieser Arbeit durchgeführte beispielhafte Implementierung vorgestellt und beschrieben.

1.1. Problemstellung

Eines der oben genannten Probleme stellen die verschiedenen Techniken die zur Konfiguration, Rekonfiguration und Verwaltung der unterschiedlichen Plattformen innerhalb eines Unternehmens verwendet werden dar. Ein von Systemadministratoren in der IT präferierter Lösungsansatz für diese Aufgaben stellt die Verwendung von Verzeichnisdiensten dar, diese werden für die Verwaltung von Benutzern, Computern und Konfigurationen verwendet. Auf Seite der Entwickler und Verwender von Industrieanlagen, ist eine vergleichbare Technologie nicht vorhanden. Zudem ist es aus Gründen der Informationssicherheit nötig, dass an das firmeninterne Netzwerk angeschlossene Systeme, dessen verwaltenden Stellen bekannt sind.

Daher sollen die bereits von der IT bekannten Methoden auf die Produktion übertragen werden, um auch hier deren Vorteile auszuspielen und die Wandlung in Richtung Industrie 4.0 zu unterstützen. Einige mögliche Vorteile sind:

- zentrale Zugriffs- und Konfigurationsverwaltung,
- genauere Lokalisierung,
- verbesserte Organisation und Zuordnung von Maschinen,
- Erfassen von Schnittstellen und Funktionen,
- erhöhte Informationssicherheit.

1.2. Ziel der Arbeit

Ziel dieser Arbeit ist die Recherche nach Technologien, die sich für die Verwendung als Verzeichnisdienst in Produktionsnetzwerken eignen und deren Evaluation. Die Technologien dürfen sowohl aus der IT, wie auch aus der Produktion stammen. Bei der Auswahl der Technologien soll explizit darauf geachtet werden, dass deren weitere Pflege und Entwicklung garantiert ist, sodass diese länger erhalten bleiben. Dieser Umstand ist den langen Lebenszyklen von Produktionsanlagen in der Produktion von in der Regel 10 bis 20 Jahren geschuldet. Zur Evaluation entsprechender Technologien, werden diese unter definierten Gesichtspunkten gegeneinander verglichen und eine dann für die prototypische Implementierung ausgewählt. Dabei handelt es sich um einen sogenannten Proof of Concept, also eine Machbarkeitsanalyse, die zeigen soll, dass die Kommunikation zwischen einer Technologie aus der Produktion und einer aus der IT möglich ist.

1.3. Begriffsdefinitionen

1.3.1. Verzeichnisdienst

Ein Verzeichnisdienst stellt einen Dienst dar, welcher zur Verwaltung und Bereitstellung von Informationen über (technische) Ressourcen, Organisationen, deren Einheiten und Personen genutzt wird [Sch16b]. Weitere benutzerdefinierte Angaben, wie beispielsweise Terminkalender und Belegungspläne für Räume, sind allerdings auch definierbar. Ein Verzeichnis ist hier also im Sinne eines Verzeichnisdienstes, wie ein Telefonbuch definiert.

Außerdem sind sie nicht mit Diensten wie Remote Authentication Dial-In User Service (RADIUS) (RFC 2865) und Kerberos (RFC 4120) zu verwechseln, sie können allerdings miteinander gekoppelt werden. Grundsätzlich handelt es sich jedoch um verschiedene Lösungen für unterschiedliche Probleme. So ist RADIUS ein Dienst der für die Authentifizierung, Autorisierung und zum Accounting von Benutzern im Kontext von Einwahlverbindungen entwickelt wurde. Bei Kerberos wiederum handelt es sich um einen verteilten Authentifizierungsdienst für offene und unsichere Netze. Bei beiden kann ein Verzeichnisdienst verwendet werden, um die Authentifizierung durchzuführen.

1.3.2. IT

Das Gabler Wirtschaftslexikon definiert den Begriff Informationstechnologie, kurz IT (engl. information technology) wie folgt: „[. . .] Oberbegriff für alle mit der elektronischen Datenverarbeitung in Berührung stehenden Techniken. Unter IT fallen sowohl Netzwerkanwendungen, Datenbankanwendungen, Anwendungen der Bürokommunikation als auch die klassischen Tätigkeiten des Software Engineering."[Dud; LS18] Wohingegen das Bundesamt für Sicherheit in der Informationstechnik (BSI) den Begriff im Glossar des IT Grundschutz Katalogs folgendermaßen definiert: „Informationstechnik (IT) umfasst alle technischen Mittel, die der Verarbeitung oder Übertragung von Informationen dienen. Zur Verarbeitung von Informationen gehören Erhebung, Erfassung, Nutzung, Speicherung, Übermittlung, programmgesteuerte Verarbeitung, interne Darstellung und die Ausgabe von Informationen."[BSI13]

In dieser Arbeit bezeichnet IT allerdings in erster Linie die firmeninterne IT-Abteilung, also diejenigen Angestellten, die gemeinhin auch „IT-ler" genannt werden. Zu ihrem Aufgabengebiet gehört unter anderem die Verwaltung und Wartung der eingesetzten Computersysteme. Darunter fallen beispielsweise die Vergabe der Zugriffsrechte auf Daten und Computersysteme, die Installation von Softwareupdates, der Austausch von Zertifikaten und ebenso das Einpflegen von Hardware oder Benutzerprofile in Verzeichnisdienste.

1.3.3. Produktion

Produktion ist definiert als: „[. . .]Prozess der zielgerichteten Kombination von Produktionsfaktoren (Input) und deren Transformation in Produkte (Erzeugnisse, Output).[. . .]"[Voi18] Jedoch wird in dieser Arbeit der Begriff Produktion als verkürzte Version von „Produktionsstätte" verwendet, welche aus dem Englischen auch als „shop floor" bekannt ist.

1.3.4. Industrie 4.0

Nach dem Gabler Wirtschaftslexikon ist unter Industrie 4.0 folgendes zu verstehen: „‚Industrie 4.0' ist ein Marketingbegriff, der auch in der Wissenschaftskommunikation verwendet wird, und steht für ein ‚Zukunftsprojekt' der deutschen Bundesregierung. Die sog. vierte industrielle Revolution zeichnet sich durch Individualisierung bzw. Hybridisierung der Produkte und die Integration von Kunden und Geschäftspartnern in die Geschäftsprozesse aus."[Ben18] In der allgemeineren Definition umfasst der Begriff auch eingebettete und (teil-)autonome Systeme, welche sich ohne externe Eingriffe in ihrer Umgebung bewegen und selbstständige Entscheidungen treffen können. Zudem ist auch die Vernetzung der Technologien zu komplexen Systemen ein integraler Bestandteil.

2. Stand der Technik

Der Wandel, welchen die Produktion in der Industrie 4.0 durchläuft, von statischen Produktionsanlagen, welche teilweise mehrere Jahrzehnte unverändert in Betrieb sind, hin zu Fertigungslinien, die innerhalb von kürzester Zeit ohne großen Aufwand neu konfiguriert werden können um sich an gegebene Anforderungen anzupassen, erfordert Veränderungen auf vielen Ebenen der Technik. Auch soll es möglich sein, von überall auf der Welt auf Maschinen zuzugreifen, um so eine Überwachung zu ermöglichen. Dies schließt auch die Verwendung von Cloud-Technologien mit ein; nichts desto trotz soll dabei aber sichergestellt werden, dass Unbefugte keinen Zugriff auf Daten erhalten [KWH13]. In der Produktion ist dies eine relativ neue Entwicklung; in der IT werden entsprechende Konzepte seit vielen Jahren verfolgt und auch angewandt. So stehen für Fernzugriffe Technologien wie Virtual Network Computing (VNC) oder Secure Shell (SSH) zur Verfügung. Zur Überwachung von Systemen kann das Simple Network Management Protocol (SNMP) eingesetzt werden oder Skripte, welche dann die überwachten Werte an eine Software wie Icinga [1] oder Prometheus [2] melden. Eine Alarmierung der entsprechenden Mitarbeiter kann im Fehlerfall per E-Mail, SMS oder automatisiertem Anruf geschehen. Um dabei weiterhin die Datensicherheit zu gewährleisten, wird auf durchgehende Verschlüsselung und Signierung von Übertragungen und der Authentifizierung der Kommunikationspartner gesetzt. Hierbei werden Passwörter und Zertifikate in vielen Fällen von vertrauenswürdigen Stellen gespeichert, verwaltet und vergeben. Der dabei entstehende Administrationsaufwand wird durch die Verwendung von zentralen Verzeichnisdiensten minimiert. Deren Verwendbarkeit und Anwendbarkeit im Kontext der Produktion soll daher Themenschwerpunkt dieser Arbeit sein.

Die Abbildung 2.1 enthält einen Überblick über alle in dieser Arbeit betrachteten Technologien und ihren Ursprung. Dabei gibt es zwei Unterkategorien, die Technologien in der Produktion und die in der Informationstechnik. Diese können miteinander kombiniert werden. So kann unter anderem von der IT die Zertifikatsverwaltung übernommen werden, wenn OPC UA mit Active Directory (AD) gekoppelt wird.

[1] `icinga.com`
[2] `prometheus.io`

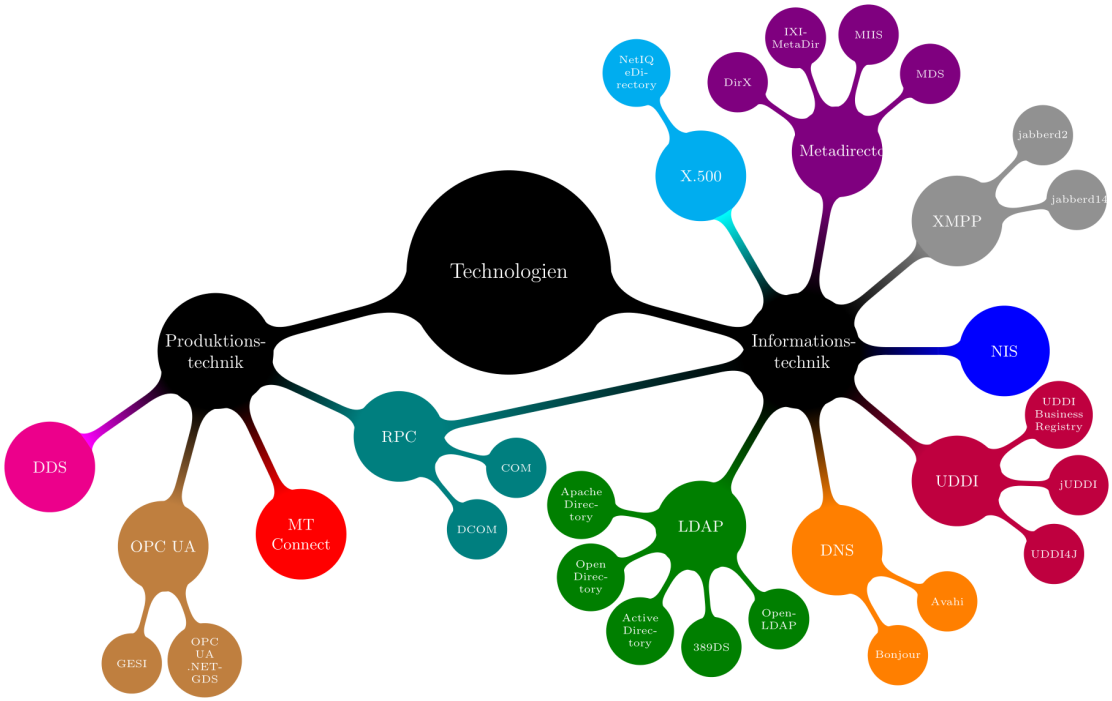

Abbildung 2.1.: Übersicht über alle betrachteten Technologien (Abbildung hochauflösend in Anhang A)

2.1. Verzeichnisdienste

Es gibt verschiedene Arten von Verzeichnisdiensten die in der Kommunikationstechnik eingesetzt werden, viele von ihnen bauen heute auf die gemeinsame Spezifikation des Lightweight Directory Access Protocol (LDAP) auf, die mittlerweile in Form von RFC 4510 bis 4519 als LDAPv3 vorliegt [Zei06]. Der erste Standard eines Verzeichnisdienstes war der von der Internationale Fernmeldeunion (ITU) verabschiedete X.500 [ITU16], jedoch wurde der spezifizierte Verzeichnisdienst nie komplett implementiert. Dies ist der strikten Verwendung des ISO-OSI Referenzmodells geschuldet. Bei diesem werden die Kommunikationsabläufe in sieben Schichten aufgeteilt und so für einen strukturierten Ablauf gesorgt. Jedoch muss sich sehr strikt an diese Schichten gehalten werden, was gerade in Betracht auf Standard-Technologien, wie Transmission Control Protocol (TCP) und Internet Protocol (IP) schwer möglich ist [Sch16b].

TCP ist zwar an sich exakt in der Transportschicht des Open Systems Interaction (OSI) Modells zu finden, der komplette Protokollstapel der Internetprotokollfamilie besitzt jedoch Protokolle, welche zwischen oder in zwei OSI-Schichten liegen. Dadurch wird eine Implementierung des X.500 erschwert und die Ausführung sehr rechenintensiv. Sehr bald führte dieser Umstand zur oben schon erwähnten Entwicklung des LDAP, welches nicht auf das OSI-Schichtenmodell setzt, sondern auf die Internetprotokollfamilie, und so wesentlich leichter zu implementieren ist. Somit stellt der X.500 Standard nur einen Vorgänger von LDAP dar. Das eigentliche Konzept bleibt allerdings erhalten [Sch16b].

Die sehr weit verbreiteten Implementierungen von LDAP liegen in Form von Microsoft AD und OpenLDAP vor und sind grundsätzlich gegeneinander austauschbar; wobei AD nicht nur einen Verzeichnisdienst beinhaltet, sondern diesen auch noch mit Kerberos, RADIUS und weiteren Technologien kombiniert. Als Produkt das einen ähnlichen Funktionsumfang aufweist ist FreeIPA bzw. der RedHat Directory Server zu nennen [Fre18; Red19].

Neben diesen klassischen Vertretern von Verzeichnisdiensten, gibt es weitere Services, die einen Verzeichnisdienst darstellen. So ist Domain Name System (DNS) auch ein Verzeichnisdienst, wobei hier IP-Adressen und Domains in Verhältnis zueinander gestellt werden, ähnlich der Zuordnung einer Telefonnummer oder einer Adresse zu einem Anschluss bzw. Haus.

Weiterhin werden zur Aggregation und Synchronisation von Daten, welche in verschiedenen Verzeichnisdiensten gespeichert sind Metaverzeichnisdienste verwendet. Diese stellen dann wie ein regulärer Verzeichnisdienst die aggregierten Daten an einer Stelle zur Verfügung.

2.1.1. Verzeichnisdienste in der IT

In diesem Kapitel sollen verschiedene Arten von Verzeichnisdiensten, welche in der IT zum Einsatz kommen vorgestellt und beleuchtet werden. Hierbei werden OpenLDAP als Standardimplementierung und Microsoft AD auf Grund der hohen Verbreitung vorgestellt. So setzen 95% der 1000 größten amerikanischen Unternehmen AD als Verzeichnisdienst ein [Blu15]. Leider sind keine weiteren Zahlen zur allgemeinen Verbreitung von Verzeichnisdiensten und der Verbreitung der einzelnen Produkte im Speziellen bekannt.

OpenLDAP

OpenLDAP ist eine Open Source Implementierung des LDAP-Standards und mit nahezu allen Betriebssystemen kompatibel. Geschrieben ist es in *C* und *Bash*. Der Code baut auf eine Protokollimplementierung auf, welche den Zugriff auf einen X.500 konformen Dienst aus einem nicht OSI-konformen Netz ermöglichte. Diese Entwicklung führte zur ersten Standardisierung von LDAP als RFC1487. Später wurde dann aus diesem Proxy eine eigenständige Implementierungen eines Verzeichnisdienstes, welche bis heute als OpenLDAP bekannt ist.[Ste10]

Standardkonform besitzt OpenLDAP unter anderem folgende Funktionen:

- starke Authentifizierung per Simple Authentication and Security Layer (SASL),
- Integritäts- und Vertraulichkeitsschutz mit Hilfe von Transport Layer Security (TLS),
- Unterstützung von Unicode und
- Unterstützung von verschiedenen Replikationsstrategien.

Die ersten beiden Funktionen sind hier besonders hervorzuheben, da in Verzeichnisdiensten zumeist sehr sensible Daten gespeichert sind. Durch beide wird sichergestellt, dass eine Übertragung der Daten nur per gesicherter und verschlüsselter Verbindung stattfindet. Weiterhin wird Hashing der gespeicherten Benutzerpasswörter in der Datenbank unterstützt, hierfür stehen neben veralteten Algorithmen, auch der modernere Secure Hash Algorithm (sha)-1 mit und ohne Salt zur Verfügung.

Aber es ist auch möglich auf dem System installierte Kryptographie-Bibliotheken für diese Aufgabe zu verwenden, dadurch ist auch ein Einsatz von sha-2 und sha-3 unter anderem in Form von sha-256 oder sha-512 bzw. sha3-256 oder sha3-512 möglich.

In der neuesten Version 2.4 sind auch verschiedene Möglichkeiten für die Konfiguration von Replikationen vorhanden. So können mit mehreren verteilten Systemen Multi-Master-Setups gebildet werden, womit sich die Möglichkeit ergibt, einen geografisch verteilten Verzeichnisdienst aufzubauen. Dies ist im Hinblick auf Informationssicherheit von Vorteil, so kann die Kommunikation zwischen dem Hauptsystemen besonders gesichert werden und die sensiblen Daten werden auf kürzestem Weg zwischen OpenLDAP-Server und Client-Systemen transportiert und verlassen nicht das interne Netz. Weiterhin können neben einem oder mehreren Hauptservern auch nur passive Systeme betrieben werden, welche als Rückfallebene dienen, sollten die Master überlastet oder wegen eines Fehlers ausgefallen sein. In Abbildung 2.2 ist eine über mehrere Standorte verteilte Multi-Master Replikation abgebildet und in Abbildung 2.3 ist der beschriebene Fehlerfall mit dem zugehörigen Normalfall zu sehen.[Ope13a; Zyt17]

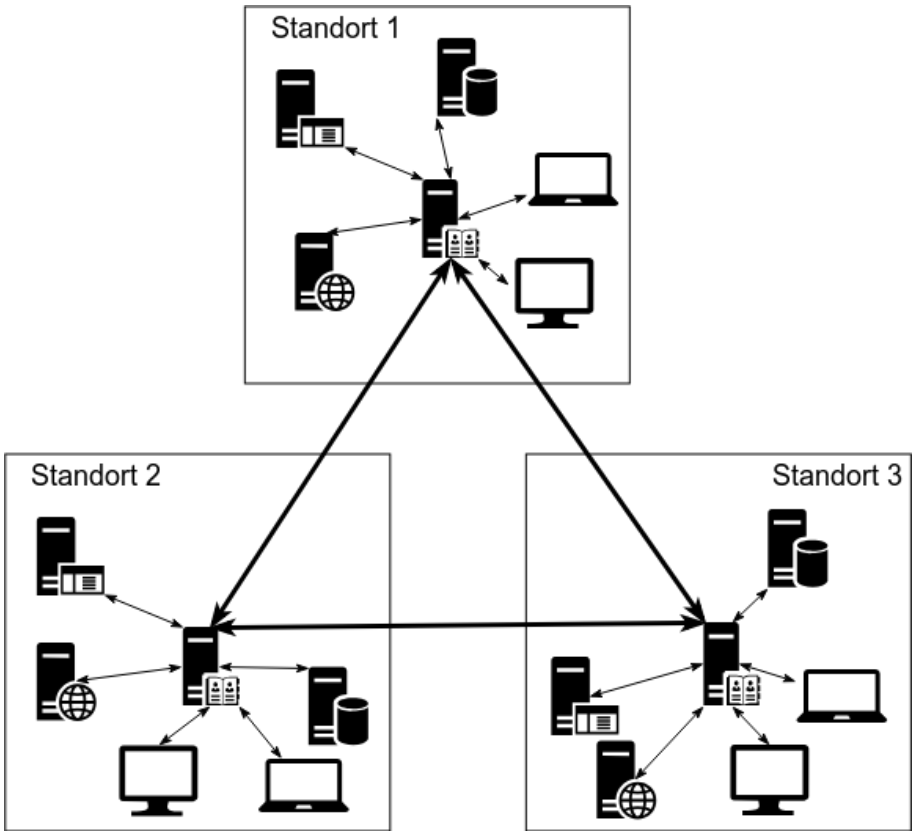

Abbildung 2.2.: Multi-Master Replikation über mehrere Standorte

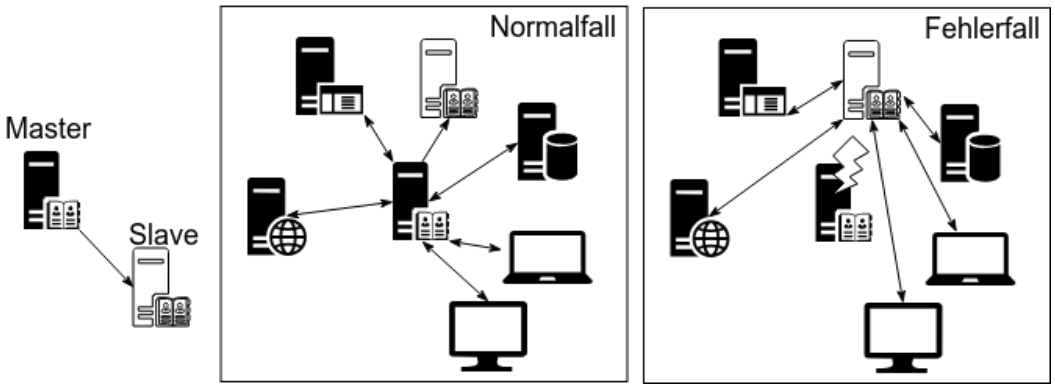

Abbildung 2.3.: Master-Slave Replikation mit Fehlerfall

Um einem Objekt neben den Standardwerten wie Name, Passwort, Adresse und Telefonnummer weitere Attribute zuzuweisen, können mit Hilfe von Schemata weitere Objektklassen nachgeladen werden. Die Auswahl an vordefinierten Objektklassen, welche verwendet werden können um Objekten weitere Attribute zuweisen zu können, ist umfangreich. Dies ermöglicht es, Zertifikate aller Art an Clients zu verteilen und mit anderen LDAP-basierten Verzeichnisdiensten zu kommunizieren. Allerdings ist es auch möglich eigene Attribute zu definieren, welche dann für Daten aller Art verwendet werden können. Diese Anpassungsfähigkeit führt zu einer Anwendbarkeit in nahezu allen Szenarien.[Ope13a; Zyt17]

Als Gegenstelle für OpenLDAP auf Seite des Endanwenders muss bei unixoiden Betriebssystemen ein OpenLDAP-Client installiert und dieser und der Autorisierungsdienst entsprechend konfiguriert werden. Um Windows als Client eines OpenLDAP-Servers zu verwenden, muss der Server die entsprechende Konfiguration aufweisen und auf dem Client der Active Directory Dienst aktiviert und konfiguriert werden. Allgemein ist eine automatische Konfiguration nicht im Standard vorgesehen, kann aber von einem Client zur Verfügung gestellt werden und ist standardisiert.[ICA18; Zyt17]

Active Directory

Bei AD handelt es sich unter anderem um die Implementierung eines Verzeichnisdienstes von Microsoft, diese baut auch auf den LDAP-Standard auf. Weiterhin werden, wie bereits angemerkt, andere Dienste angeboten. So bietet AD einen Kerberos Server für Einmalanmeldung, aber auch RADIUS und einen Zertifikatservice an. Der Betrieb eines entsprechenden Verzeichnisdienstes im eigenen Endgerät kann aber nur auf einem Server mit mindestens Windows Server 2003 oder neuer stattfinden; Windows AD ist hierbei schon enthalten. Eine Lizenz beläuft sich also auf die Kosten des Betriebssystems, hierfür fallen je nach Größe des Unternehmens, bei Verwendung von Windows Server 2019, Kosten ab 501$ pro Installation an [Mic18d]. Neben dem Betrieb eines Servers auf eigener Hardware bietet Microsoft auch eine Cloudlösung in Form von Microsoft Azure Active Directory an. Hierbei fallen bei Verwendung der kostenlosen Lizenz keine Kosten an, sollte schon ein Azure-Abonnement vorhanden sein. Dieses beinhaltet allerdings unter anderem kein Service-Level-Agreement (SLA), womit keine entsprechend niedrige Ausfallwahrscheinlichkeit gewährleistet ist, außerdem ist die Anzahl der Einträge begrenzt [Mic].

Sollte im restlichen Unternehmen auf den Benutzerendgeräten Windows als Betriebssystem installiert sein, ist auch hier ein AD Client installiert. Dieser muss lediglich aktiviert und korrekt konfiguriert werden. Auch eine Verwendung zusammen mit Clients auf Basis von unixoiden Betriebssystemen ist möglich. Hierbei müssen allerdings, ähnlich wie bei OpenLDAP mit AD-Clients, innerhalb von AD entsprechende Einstellungen vorgenommen werden und der Verzeichnisdienst muss eine definierte Struktur aufweisen.

Der Programmcode von Windows AD ist nicht öffentlich einsehbar, also Closed Source und es kann nur auf Windows Server installiert werden. Weiterhin bietet Microsoft neben einer im eigenen Netzwerk aufgesetzten Version, auch die Möglichkeit Azure AD zu verwenden, welches in der Cloud von Microsoft angesiedelt ist. Somit entfällt die Konfiguration von eigenen Servern. Beide Optionen können jedoch auch in Kombination verwendet werden. So kann ein lokaler AD Server mit einer Azure AD Instanz synchronisiert werden, um weitere Funktionen, wie die automatische Synchronisation von Benutzern und Kontakten, zu nutzen.[Mic18a; MO18]

Domain Name System

Jeder Computer, der an ein Netzwerk angeschlossen ist, besitzt eine für dieses Netzwerk einzigartige Adresse, ähnlich einer Telefonnummer. Diese Adresse nennt sich IP-Adresse (kurz: IP) und besteht im Falle von IPv4 aus vier durch Punkte getrennte 8-stellige Binärzahlen, bei IPv6 aus acht durch Doppelpunkt getrennte 16-stellige Binärzahlen. Da diese Adressen in binär lang und schwer zu merken sind, werden diese meist als Dezimalzahl (IPv4) oder Hexadezimalzahl (IPv6) notiert. Eine IP-Adresse sieht also z.B. wie folgt aus: 129.69.8.151 bzw. 2001:7c0:2041:8:0:151. Da aber auch diese Zahlenkolonnen weiterhin für Menschen weniger gut zu merken sind als beispielsweise Namen, wurde begonnen IP-Adressen Namen bzw. Domains zuzuordnen. Es geschieht also eine Zuordnung ähnlich einer Telefonnummer zu einem Anschluss. Dies macht DNS zu einem Verzeichnisdienst; die vorher genannten IP-Adressen sind der Domain „www.uni-stuttgart.de" zugeordnet. Wenn nun also ein Anwender diese Domain aufruft, wird sie in die korrespondierende IP-Adresse übersetzt und das unter dieser Adresse erreichbare System kontaktiert.[Sch16a]

Zu einem Datensatz aus Domain und IPs können auch weitere Informationen gespeichert werden. So ist ein Service (kurz SRV) Feld im Protokoll vorgesehen, in diesem können die unter der Domain erreichbaren Dienste gesammelt werden. Dieser Umstand wird sich auch bei DNS über Multicast (mDNS) zu nutze gemacht, welches fester Bestandteil von Zeroconf ist. Hierbei ist das Ziel DNS ohne zentralen Server umzusetzen. Anders als bei regulärem DNS handelt es sich bei mDNS um eine Beschreibung wie Clients mit entsprechenden Anfragen umzugehen haben und wie diese zu stellen sind. Da Multicast nicht ohne weiteres über Netzgrenzen hinweg einsetzbar ist, kann es nur in einem lokalen Netzwerk eingesetzt werden.[ITA] Ein klassisches Beispiel für die Anwendung von mDNS bzw. Zeroconf ist das automatische Auffinden von Druckern oder Netzwerkspeichern innerhalb eines Netzwerkes.

2.1.2. Verzeichnisdienste in der Produktion

In diesem Kapitel werden die zwei in dieser Arbeit betrachteten Verzeichnisdienste aus der Produktion vorgestellt. Beide sind auf Basis von OPC UA entwickelt worden und daher nur in einer Umgebung einsetzbar, die diesem Umstand Rechnung trägt.

GESI

Neben den klassischen Vertretern der Verzeichnisdienste gibt es auch speziellere Vertreter. So ist mit den Gelben Seiten der Industrie 4.0 (GESI) eine Implementierung eines Verzeichnisdienstes für die Verwendung in der Produktion geplant. Hierzu soll als Basis auf OPC UA gesetzt werden. Anders als bei OpenLDAP und AD steht hier nicht die Verwaltung von Benutzern und deren Rechten im Vordergrund, sondern die Bereitstellung von Daten für und über Maschinen in Fertigungslinien. So sollen sich Maschinen bei der GESI anmelden und ihre Funktionalitäten in dieser speichern. Anderen Produktionsteilnehmern wird darauf bekanntgegeben, dass es einen neuen Teilnehmer gibt, sollten diese dann weitere Informationen zu diesem benötigen, können sie angefragt werden. Bei weiteren Änderungen werden diese den anderen Teilnehmern mitgeteilt, sollten sie sich für den Erhalt dieser gemeldet haben. Dies ermöglicht es, dass einzelne Teilnehmer kurzfristig zu einem Produktionsablauf hinzugefügt oder von diesem entfernt werden können und die weiteren Teilnehmer von dieser Änderung automatisch erfahren und ihr Verhalten anpassen können. Auf selbe Weise kann ein Teilnehmer auch seine Funktionalität(en) ändern, woraufhin die weiteren Teilnehmer entsprechend reagieren können. Diese automatische Reaktion auf Veränderungen kann dazu genutzt werden, dass sich innerhalb weniger Handgriffe oder auch vollkommen autonom der Produktionsablauf an die äußeren Gegebenheiten anpassen kann, ohne dass aufwändige manuelle Anpassungen vorgenommen werden müssen. Dies verringert die Standzeiten, führt zu einer höheren Auslastung der Maschinen und dadurch zu einer Erhöhung des Produktionsausstoßes. Weiterhin wird so die Reaktionszeit auf externe Einflüsse und Anforderungen verringert, was zu eineren flexibleren Produktion und ermöglicht so eine kostensensitive Produktion führt, insbesondere auch in Hinblick auf Kleinserien. [KLIS18]

OPC UA .Net-GDS

Neben einer geplanten Implementierung eines Verzeichnisdienstes für Produktionsnetzwerke, hat Microsoft mit OPC UA .NET-GDS eine Implementierung eines OPC UA Global Discovery Server (GDS) veröffentlicht.

Allgemein wird die Ermittlung (Discovery) dazu benötigt um einen gewünschten Kommunikationspartner zu finden und dessen Eigenschaften, wie Konfiguration, Enkodierung oder Sicherheitseinstellungen, zu erhalten. Hierzu kommuniziert ein Endpunkt in einem einfachen Szenario mit einem bekannten OPC UA Server und erhält von diesem eine Liste von zugehörigen Endpunkten und deren Eigenschaften. Im Falle, dass mehrere OPC UA Server auf einer Maschine laufen, können diese von einem Endpunkt über den Local Discovery Server (LDS) gefunden werden. Dieser sendet dem Endpunkt eine Liste aller OPC UA Server auf einer Maschine. Somit kann der Endpunkt dann mit dem gewünschten Server kommunizieren und bei diesem eine Liste der Endpunkte erfragen, mit welchen sich dann später direkt verbunden werden kann. Bei weit über das Netzwerk verteilten Servern wird wieder ähnlich vorgegangen, jedoch wird dem LDS ein GDS vorgeschalten. Dieser liefert dem anfragenden Endpunkt eine Liste aller Maschinen, welche einen LDS oder OPC UA Server zur Verfügung stellen. Sollte sich der gesuchte OPC UA Server darunter befinden wird mit diesem wie im ersten Szenario kommuniziert. Ist dem nicht der Fall, wird mit einem LDS kommuniziert und wie im zweiten Szenario weiter verfahren.[MLD09]

Mit der Hilfe eines GDS können ähnlich der GESI Zertifikate von Maschinen verwaltet und ihre Funktionalitäten untereinander propagiert werden. Neben dem eigenständigen Betrieb eines GDS-Servers ist auch die Möglichkeit gegeben, diesen von Microsoft in Azure betreiben zu lassen und ihn mit einem bereits vorhandenen Active Directory zu koppeln. So kann auch hier die für das entsprechende Unternehmen passende Variante gewählt werden, um eine effiziente Verwaltung von Daten zu ermöglichen.[Geo17a; Geo17b]

2.2. Nutzbare Technologien für Verzeichnisdienste

In diesem Kapitel werden weitere Technologien vorgestellt, welche in den Vergleich, den diese Arbeit beinhaltet, aufgenommen wurden. Auch hier erfolgt wieder eine Unterteilung in Technologien welche aus der IT und welche aus der Produktion stammen.

2.2.1. IT

XMPP

Extensible Messaging and Presence Protocol (XMPP) ist ein Protokoll für den nahezu Echtzeit Austausch von Extensible Markup Language (XML) Daten; es ist auch unter dem Namen Jabber® bekannt. Der original Jabber Service mit dem alles begann ist seit 1999 bis heute verfügbar, dieser stellt einen Instant Messaging Dienst zur Verfügung. Viele weitere Instant Messaging Dienste bauen auf diesen Standard auf. Neben dem klassischen Jabber setzen auch ICQ, der Facebook Messanger, Google Talk und diverse andere auf diesen Standard. Ein großer Vorteil dieses Standards ist die Möglichkeit mit Benutzern anderer Plattformen zu kommunizieren. So ist es möglich mit einem Benutzer, welcher ein Konto bei ICQ besitzt zu kommunizieren, auch wenn man selbst nur ein Konto bei einem anderen Anbieter besitzt. So war es auch möglich Nutzer des Facebook Messangers und Google Talk zu kontaktieren, aber sowohl Facebook wie auch Google lassen dies mittlerweile nicht mehr zu.[HB13; Pro18; Ste15]

Während des Einsatzes von XMPP in Google Talk wurde der Standard durch Google um die Voice over IP (VoIP) Funktionalität erweitert, um diese Datenübertragung einzuleiten wurde zusammen mit der XMPP Foundation das Protokoll Jingle entwickelt. Neben dieser sind auch weitere Erweiterungen für andere Einsatzzwecke standardisiert worden. So ist auch die Kommunikation zwischen mehreren Entitäten gleichzeitig möglich und es können bei Veränderungen Benachrichtigungen an Abonnenten eines Nachrichten-Stroms gesendet werden. Doch noch lange bevor diese Erweiterungen zum eigentlichen Standard hinzugefügt wurden, im ersten von der IETF verabschiedeten Standard, war eine Verschlüsselung des Datenstroms mit TLS vorgesehen. Dadurch werden die übermittelten Daten verschlüsselt und sind so nur von den Sendern und Empfängern der Nachrichten lesbar.[KTM+18; LBS+18a; LBS+18b; Sai11; Sai15; Sai18]

Da per XMPP allgemein XML-Daten übertragen werden, sind weitere Einsatzgebiete von der XMPP Foundation vorgesehen. So wird XMPP auch für Videotelefonie und im Bereich des Internet der Dinge (IoT) eingesetzt. Gerade der Einsatz im Bereich des IoT ist im Kontext des Einsatzes innerhalb

der Produktion interessant, so wird der automatische Service Discovery und Publish-Subscribe unterstützt. Es ist also möglich, einen Dienst ähnlich zu einer OPC UA GDS zu entwickeln und weitere Funktionen, die einen Verzeichnisdienst auszeichnen.[Sai11; WL17; WLT+18]

Mögliche Produkte dieser Technologie: jabberd2, ejabberd, OpenFire, prosody. In dieser Arbeit betrachtete Lösung: jabberd2

Zeroconf

Zeroconf steht kurz für Zero Configuration Networking und ist ein Verfahren zur automatischen Konfiguration und des konfigurationsfreien Betriebs von Servern. Weiterhin wird das einfache Auffinden von Diensten in Netzwerken ermöglicht. Diese Funktionalitäten wurden bereits zuvor von Apples Apple Talk gelöst, sollte jedoch mit Zeroconf standardisiert werden. Es sollte auf offene Protokolle und Standards gesetzt werden, dieses Vorhaben wurde jedoch nicht realisiert. Nichts desto trotz wurde auf Basis des Entwurfs Software entwickelt.[Che; ITA]

Zur Konfiguration der IP-Adressen ohne einen entsprechenden Server wird auf Automatic Private IP Adressing oder IPv4 bzw. IPv6 Link-Local Adressing gesetzt, also einen Standard zur automatischen Konfiguration von privaten IP-Adressen. Das Übersetzen von IP-Adressen zu Namen wird mit mDNS, also DNS über Multicast durchgeführt. Die letzte der Funktionalitäten, das automatische Auffinden von Diensten, wird auch hier dezentral über DNS-SD, also per DNS-Service Discovery, realisiert.[Che; ITA]
Wie zu Anfang des Kapitels erwähnt, gab es bereits 1983 mit Apple Talk Software, welche die automatische Konfiguration von Netzwerkteilnehmern ermöglicht. Diese Entwicklung war der Tatsache geschuldet, dass zu dieser Zeit Netzwerkhardware noch so teuer wie ein PC selbst war, weshalb nach einer Lösung ohne Verwendung dieser gesucht wurde. Apple Talk konnte jedoch nur in Netzwerken verwendet werden, welche den Apple Netzwerstapel unterstützten. Da sich aber über die Zeit die Internetprotokollfamilie als Standard etablierte, konnte Apple Talk nicht mehr verwendet werden. Während die Zeroconf Arbeitsgruppe nach einer Lösung für das weiterhin bestehende Problem suchte, wurde im Jahr 2002 von Apple Rendezvous, heute Bonjour, vorgestellt. Drei Jahre später erschien mit Avahi eine komplette Open Source Lösung, welche heute auf vielen Linux Distributionen standardmäßig installiert ist.[App18; Che; PL10]

Zeroconf wird in dieser Arbeit als möglicher Kandidat für einen Verzeichnisdienst betrachtet, da es mit DNS bereits auf einen Verzeichnisdienst aufbaut, in diesem können im TXT-Record, also im Beschreibungsfeld, oder auch in einem eigens dafür geschaffenen Feld die nötigen Informationen gespeichert werden. Weiterhin bietet es die Möglichkeit der automatischen Dienst Ermittlung, was zu einer ähnlichen Funktionalität wie bei OPC UA .Net-GDS führt. Da als Basis auf DNS über Multicast gesetzt wird, welches erst einmal keine Kommunikation über Netzgrenzen hinweg zulässt, muss weiterhin ein Gateway zwischen Netzen eingesetzt werden. Dieser leitet den aufkommenden Multicast Traffic in andere Subnetze weiter. Eine bereits eingesetzte Implementierung wird mit Apple Bonjour Gateways von einigen Herstellern von Netzwerkhardware zur Verfügung gestellt.[Mat13] Eine weitere Implementierung wird von Cisco unter dem Name Service Discovery Gateway vermarktet.[Cis]

Mögliche Produkte dieser Technologie: Bonjour, Avahi, JmDNS, wxWidgets. In dieser Arbeit betrachtete Lösungen: Bonjour und Avahi, da es sich bei beiden um die Standardimplementierung von Zeroconf handelt.[App18; Che; PL10]

2.2.2. Produktion

COM/DCOM

Zu Beginn der 1990er Jahre wurde von Microsoft mit Component Object Model (COM) eine Implementierung für die Interprozesskommunikation vorgestellt, die es ermöglicht, dass ein Programm von einem anderen gesteuert werden kann. So konnte zum Beispiel Microsoft Excel von Microsoft Word gesteuert werden, einen Wert innerhalb einer Zelle zu ändern. Dieser Aufruf war allerdings nur auf einem Rechner nicht von Rechner zu Rechner möglich, also wurde bald darauf Distributed COM (DCOM) entwickelt, welches genau dies ermöglicht. Es konnten nun Objekte, die auf verschiedenen Systemen vorhanden sind, miteinander verlinkt und auch eingebettet werden, dies gab der Technologie auch den Namen Microsoft Object Linking & Embedding (OLE). Da diese Technologie gerade in der Automatisierungstechnik großen Anklang fand, wurde sie von Microsoft um die Prozesskontrolle erweitert und nannte sich dann in dieser Form OLE for Process Control (OPC), wurde aber später in Open Platform Communications (OPC) umbenannt. Leider gestaltet sich die Konfiguration von DCOM über Netzwerkgrenzen hinweg als schwierig, da für je Applikation ein anderer offener Port in der Firewall benötigt wird. Weiterhin sind COM und DCOM nur auf Basis eines Microsoft Windows zu verwenden, dies hat bisher Sinn ergeben, da viele Maschinen in der Produktion bisher eine Form von Windows verwenden. Dies kann sich aber in den kommenden Jahren schwer gestalten, da immer weitere Plattformen in die Produktion eingebunden werden sollen, welche auf offene Standards setzen.[DAT09; DAT11; Mic15a; Pla]

COM und DCOM werden in diesem Vergleich betrachtet, da beide den bisherigen Stand der Technik darstellen und nun durch neue Technologien ersetzt werden sollen.[Pla]

2.3. Weitere nicht betrachtete Technologien

Die in diesem Kapitel genannten Technologien werden aus Gründen der Vollständigkeit betrachtet, werden aber im späteren Verlauf der Arbeit nicht mit den bereits genannten Technologien verglichen.

2.3.1. MT Connect

Bei MT Connect handelt es sich um ein Protokoll entwickelt für den Austausch zwischen Produktionsanlagen und Software für den Zweck der Überwachung und Datenanalyse, die Zugriffe auf Daten erfolgen hierbei nur lesend. Das Projekt wurde 2006 von der US-amerikanischen Association for Manufacturing Technology (AMT), einer Organisation vergleichbar mit der VDMA aus Deutschland, und findet vor allem in Nordamerika Verwendung. Es wird vor allem auf eine schnelle Entwicklung und Implementierung von Standards für abgegrenzte Einsatzgebiete gesetzt und weniger auf die Entwicklung eines generellen für alle Bereich geeigneten Standards. Wobei zum Zeitpunkt des Verfassens nur eine Erweiterung für Werkzeugmaschinen verfügbar war [JNP15a].

Im Bezug auf Verzeichnisdienste macht der Standard bei der Ermittlung von Diensten, die Aussage, dass ein Verzeichnis auf Basis von LDAP Verwendung finden soll. Aus diesem Grund und da MT Connect bisher auf dem europäischen Markt wenig Verbreitung findet, wird in dieser Arbeit auf den Vergleich mit anderen Technologien verzichtet [JNP15a; MT 18].

2.3.2. DDS

Data Distribution Service (DDS) wurde ursprünglich für die Verwendung in der Steuerungstechnik entwickelt und setzt deshalb vor allem auf geringe Latenzen, hohen Datendurchsatz und einfache Skalierbarkeit. Ähnlich zu OPC UA wird auf ein Publish-Subscribe Modell gesetzt, jedoch findet keine vollkommene Implementierung eines Protokollstapels statt, sondern nur die Implementierung eines einzelnen Protokolls, vergleichbar zu MT Connect [Kno16].

Auch bei dieser Technologie wurde auf einen Vergleich mit den weiteren Technologien verzichtet, da DDS vor allem auf dem amerikanischen Markt eine Rolle spielt [Kno16].

3. Technologievergleich

In diesem Kapitel werden die oben genannten Technologien miteinander verglichen, um zu evaluieren, welche dieser für den Einsatz innerhalb der Produktion geeignet sind. Hierzu werden diese auf Grund verschiedener Merkmale verglichen.

3.1. Vorgehen

Die Technologien werden nach den folgenden Eigenschaften verglichen: Verbreitung, Aktualität, Reife der Entwicklung, Quellcode Verfügbarkeit, Anzahl gefundener Sicherheitslücken und Kosten. Diese werden in den folgenden Kapiteln noch ausführlich beschrieben und spezifiziert. Für jedes Merkmal werden Punkte von einem (1) (schlechtest möglich) bis zehn (10) (bestmöglich) Punkten vergeben. Sollte zu einem Merkmal keine Aussagen getroffen werden können, wird dieses mit null (0) Punkten bewertet. Die verschiedenen Merkmale werden zu Ende gewichtet, um die Wichtigkeit bestimmter Merkmale hervorzuheben. Neben den angegebenen Merkmalen wird der Einsatzzweck, für den die Technologie entwickelt wurde, genannt.

Da nicht alle der hier betrachteten Technologien nach diesen Kriterien verglichen werden können, wird bei diesen auf deren Standardimplementierungen zurückgegriffen. Standardimplementierungen zeichnen sich dadurch aus, dass auf ihnen nachweislich der Standard beruht oder diese explizit als Referenzimplementierung für einen Standard gedacht sind.

3.2. Verglichene Merkmale

3.2.1. Verbreitung

Um die Verbreitung von Produkten festzustellen, wurde versucht, sich auf Statistiken zu verlassen. Dies ist aber bei den hier betracheteten Produkten sehr schwer. Bei Open Source Produkten sind im Regelfall keine Statistiken vorhanden, bei Closed Source Produkten wird zumeist von Herstellern kein Einblick in die Nutzung gegeben. So können diese Zahlen nur anhand von Nutzungszahlen der zu Grunde liegenden Plattformen geschätzt werden. So ist es zum Beispiel sehr wahrscheinlich, dass in einem Unternehmen, welches Windows als Betriebssystem für Laptops und Arbeitsplatz Rechner einsetzt, auch Active Directory zur Verwaltung dieser eingesetzt wird. Aus Statistiken geht hervor, dass Windows in diesem Bereiche eine hohe Verbreitung besitzt, also ist auch anzunehmen, dass Active Directory folglich stark verbreitet ist.[Pet17] Bei den weiteren Produkten wurde analog verfahren.

Die Bewertung der Verbreitung geht in die Gesamtpunktzahl mit doppelter Wertung ein, da eine hohe Verbreitung eine gewisse Popularität impliziert und somit eher eine Kompatibilität zu anderen Programmen besteht.

3.2.2. Aktualität

Die Aktualität des betrachteten Produkts wurde am Erscheinungsdatum des letzten Softwareupdates festgemacht. Je neuer das letzte Update ist, desto höher ist die zugewiesene Punktzahl. Die Software mit dem jüngsten Update erhält zehn Punkte, die mit dem ältestem einen Punkt.

Um diese Daten zu erhalten, wurde bei Open Source Projekten auf den Projektwebseiten die letzte Änderung des Codes betrachtet. Bei Closed Source Projekten wurde das Datum des letzten Updates der entsprechenden Produktseite entnommen. Bei Produkten die fest mit dem darunterliegenden Betriebssystem gekoppelt sind, wurden die Support Webseiten des Betriebssystems nach Änderungen durchsucht, welche Angaben zu Änderungen des betrachteten Produkts machen. Sollte solch ein Update gefunden worden sein, wurde das Erscheinungsdatum des Updates als letztes Änderungsdatum angenommen.

Die Bewertung der Aktualität geht in die Gesamtpunktzahl mit einfacher Gewichtung ein, da hier vor allem Standardimplementierungen und Neuimplementierungen von Technologien betrachtet werden. Standardimplementierungen werden auf Grund ihrer fortgeschrittenen Implementierung nur zur Anpassung an einen veränderten Standard oder auf Grund von Sicherheitslücken angepasst. Wohingegen Neuimplementierungen regelmäßig Updates erhalten. Da in dieser Arbeit beiden Gruppen gleichermaßen betrachtet werden sollen, wird auf eine mehrfache Gewichtung verzichtet.

3.2.3. Reife der Entwicklung (Reife)

Die Reife der Entwicklung wurde an der Umsetzung des Standards festgemacht, welcher umgesetzt werden soll. Hierfür wurde sich auf die Angaben, welche auf den Produktwebseiten zu finden sind, verlassen. Anschließend wurde, wenn möglich, die Anzahl der vom Standard gewünschten und ebenso im Quellcode implementierten Funktionen stichprobenartig ermittelt. Wenn zudem zwei ähnliche Technologien betrachtet werden, von denen nachweislich eine der beiden den Standard umsetzt, und beide Technologien vollkommen kompatibel zu einander sind, wird angenommen, dass beide den Standard im gleichen Umfang umsetzen. Dies ist nötig, da bei manchen der betrachteten Technologien keine Angabe zur Umsetzung des Standards gemacht werden.

Dieses Merkmal fließt in die Gesamtpunktzahl der Technologien in doppelter Wertung ein, da nach Erreichen einer hohen Reife wenige bis keine Änderungen an einer Technologie mehr durchzuführen sind. Dies erleichtert den Einsatz in einem neuen Einsatzgebiet und steigert die Interoperabilität bzw. den herstellerunabhängigen Einsatz verschiedener Lösungen, da häufige Änderungen die Anpassung an diesen neuen Bereich verlangsamen können.

3.2.4. Quellcode Verfügbarkeit (Quellcode)

Die Quellcode Verfügbarkeit wird grundsätzlich in zwei Bereiche unterteilt, Closed Source und Open Source, wobei ersteres einen (1) Punkt und letzteres zehn (10) Punkte erhält. Da Open Source nicht gleich Open Source ist, wird hier noch die Lizenz, unter welcher der Code wiederverwendet werden darf, betrachet. Je mehr Freiheiten eine Lizenz bietet, desto besser fällt die Bewertung aus. Als Freiheit wird hier bezeichnet, wie wenig Einschränkung eine Lizenz in Bezug auf Veränderung, Verwendung und Weiterverbreitung macht. Sollte keine Lizenz zu finden sein, wird mit einem Punkt bewertet, da auch keine Lizenz bei späteren Ansprüchen des Urhebers zu Problemen führen kann.

Die Verfügbarkeit des Quellcodes und die damit einhergende Bewertung der Lizenz geht mit dreifacher Gewichtung in die Gesamtpunktzahl ein. Diese hohe Gewichtung ist darin begründet, dass Open Source Software viele Vorteile aber nur wenige Nachteile mit sich bringt. Diese Vorteile sind unter anderem die hohe Softwarequalität und Zuverlässigkeit, geringeren Kosten, höhere Sicherheit und die Unabhängigkeit von Firmen. Ein weiterer im Kontext dieser Arbeit wichtiger Punkt ist die leichte Anpassbarkeit an veränderte Anforderungen oder Umgebungen, auch ohne die direkte Unterstützung des Hauptentwicklers.[AOE; Bal15]

3.2.5. Unterstützte Betriebssysteme (Betriebssysteme)

Für die Anzahl der unterstützen Betriebssysteme werden folgende Betriebssysteme zu Grunde gelegt: Microsoft Windows, Linux, MacOS und BSD. Je unterstütztem Betriebssystem werden 2,5 Punkte vergeben. Es werden diejenigen Betriebssysteme als unterstützt betrachtet, auf denen die Software installiert werden kann. Die Anzahl wurde den Webseiten der Projekte entnommen, sollten durch die Recherche jedoch weitere unterstützte Betriebssysteme gefunden worden sein, werden diese ebenso als unterstützt angesehen.

Auch die Unterstützung der verschiedenen Betriebssysteme geht mit vierfacher Bewertung in die Gesamtpunktzahl ein. Auch hier verhindern Restriktionen Anpassungen und erschweren die Entwicklung neuer Technologien. Des weiteren ist derzeit noch nicht abzusehen welches Betriebssystem in den kommenden Jahren in der Produktion präferierter wird bzw. ob sich überhaupt ein einzelnes Betriebssystem als Lösung herauskristallisiert.

3.2.6. Sicherheit

Die Bewertung der Sicherheit einer Software gestaltet sich grundsätzlich nicht als trivial, da keine oder wenig gefundenen Sicherheitslücken nicht automatisch auf eine sichere Software hinweisen, da trotz allem unentdeckte Lücken vorhanden sein können. Um diese leichter bewerten zu können, wurde ein Industriestandard mit dem Namen Common Vulnerability and Exposure (CVE) ins Leben gerufen, dieser wird dazu verwendet, um für Sicherheitslücken eine einheitliche Bennung einzuführen. Jede gefundene Sicherheitslücken, die eine CVE Nummer besitzt, erhält eine Bewertung nach Common Vulnerability Scoring System (CVSS). Ab einer entsprechenden Menge an gefundenen Sicherheitslücken ist eine Tendenz zu erkennen, wie schwerwiegend weitere Sicherheitslücken sind und ob eine Software eher harmlose oder schwerwiegende Fehler beinhaltet. Deshalb wird auf Grundlage der CVSS Bewertungen aller gefundenen Sicherheitslücken die Sicherheit bewertet. Hierfür wird der Durchschnitt aller Bewertungen errechnet, je nach Produkt ist

dieser auch schon im Internet zu finden. Sollte dies bei einem Produkt nicht der Fall sein wurde auf `www.cvedetails.com` nach den Produkten gesucht und die relevanten Sicherheitslücken und deren Bewertung aufgeschrieben und dann das Mittel gebildet.
Das Produkt mit den im Durchschnitt kleinsten CVSS Bewertungen erhält zehn (10) Punkte, das mit dem höchsten einen (1) Punkt. Alle weiteren werden im Verhältnis zu diesen bewertet. Die gefundenen Sicherheitslücken sind im Anhang zu finden.
Da diese Zahlen nur auf Bewertungen von bisher aufgetretenen Sicherheitslücken beruhen und somit nur einen sehr groben Richtwert ergeben, wird diese Bewertung einfach gewichtet in die Gesamtpunktzahl einbezogen.

3.2.7. Kosten

Die Kosten werden an den wirklichen Kosten des betrachteten Produkts festgelegt. Je höher diese Kosten liegen, desto geringer die Bewertung für dieses Merkmal. Die höchste Bewertung wird also für Projekte vergeben, für deren Verwendung der Software keine Kosten anfallen. Sollten zum Betrieb neben den Kosten des eigentlichen Programms weitere Kosten, ohne Kosten der Hardware und Administration, anfallen, werden diese zu den Gesamtkosten hinzugerechnet. Auch hier werden alle weiteren Produkte in Relation zum höchst- und niedrigstbewertetem eingeordnet.
Die Kosten gehen auch mit einfacher Bewertung in die Gesamtpunktzahl ein, da sie je nach Betreiber der Technologie keine Rolle spielen muss.

3.2.8. Standardisierung

Hierbei wird betrachtet, ob die Software auf einen Standard aufbaut oder nicht. Dies ist ein betrachtetes Merkmal, da ein Standard dafür verantwortlich ist, dass zwei Produkte, die sich an den selben Standard halten, leicht gegeneinander ausgetauscht werden können. Weiterhin wird die Qualität der jeweiligen Software höher, da durch eine Norm bzw. einen Standard ein gewisses Rahmenkonstrukt gegeben ist, welches genau definierte Eigenschaften besitzt, gegen diese Eigenschaften kann getestet werden.[DINa; DINb]

3.2.9. Einsatzzweck

Hier wird der Einsatzzweck, für welchen das genannte Produkt entwickelt wurde, nochmals genannt.

3.3. Vergleich

3.3.1. OpenLDAP

Die Bewertung von OpenLDAP ist in Tabelle 3.1 zu sehen.

Verbreitung: Um die Verbreitung von OpenLDAP zu bestimmen, wurden Umfragen der Linux Foundation und W3Tech zur Hilfe genommen. Aus diesen geht hervor, dass die größte Zahl an Servern in Cloud-Umgebungen und Webservern mit Linux betrieben werden. Weiterhin werden mehr als 60% der Webserver mit Debian-basierten Distributionen betrieben. Da OpenLDAP hier den Standard als Verzeichnisdienst darstellt, kann angenommen werden dass OpenLDAP als Verzeichnisdienst verwendet wird, wenn überhaupt ein Verzeichnisdienst in Betrieb ist. Weiterhin setzt laut den Entwicklern auch Apples Verzeichnisdienst Open Directory auf OpenLDAP auf. Die Verbreitung von OpenLDAP wird also sehr hoch angesetzt und daher mit maximaler Punktzahl bewertet. [Lin14; Ope13a; W3C18]

Aktualität: Das letzte Software Update für OpenLDAP erschien am 22.03.2018, dies ist Verhältnis zu allen andere Produkten etwas besser als der Median, deshalb werden sechs (6) Punkte vergeben.

Reife: Um die Reife der Entwicklung festzustellen, wurde eine Liste der OpenLDAP Foundation aller unterstützter und nicht unterstützer Features von LDAPv3 zu Rate gezogen. Laut dieser wird eines der 32 Features noch nicht unterstützt, dies entspricht 3,1%. Somit können für diese Metrik weitere zehn Punkte vergeben werden.[Ope13b; Ope13c]

Quellcode: Der Quellcode ist frei verfügbar unter folgender URL zu finden: `www.openldap.org/software/repo.html`. Der gesamte Code steht unter der OpenLDAP Public License, diese ist ähnlich zu einer BSD Lizenz und fordert nur die Bennung der Lizenz der Ursprungs-Software und einen Urheberrechtshinweis. Weitere Einschränkungen werden nicht vorgenommen. Daher werden hier 9 Punkte vergeben.

Betriebssysteme: Auf `www.openldap.org` werden native Pakete für Linux, BSD und MacOS genannt, allerdings sind auch Pakete für Windows im Internet zu finden. Deshalb werden zehn (10) Punkte vergeben.

Sicherheit: Der CVSS Score von OpenLDAP wird mit 5,7 angegeben [MIT18b], im Vergleich zu den anderen bewerteten Technologien ist dies ein eher schlechter Wert. Es werden daher drei (3) Punkte vergeben.

Kosten: OpenLDAP ist freie Software und daher kostenlos. Es werden aber auch von Systemhäusern Lösungen auf Basis von OpenLDAP angeboten, dies soll aber nicht in dieser Arbeit betrachtet werden. Daher werden zehn (10) Punkte vergeben.

Standardisierung: OpenLDAP baut auf RFC4511ff. auf, dieser ist ein anerkannter Standard der Internet Engineering Task Force (IETF).[Ser06]

Einsatzzweck: Verzeichnisdienst für die Firmen IT.

Merkmal	Bewertung	Gewichtung	Punktzahl
Verbreitung	10	2	20
Aktualität	6	1	6
Reife	10	2	20
Quellcode	9	3	27
Betriebssysteme	7,5	4	30
Sicherheit	3	1	3
Kosten	10	1	10
		Gesamtpunktzahl	116

Tabelle 3.1.: Die Bewertung der Merkmale für OpenLDAP.

3.3.2. Active Directory

Die Bewertung von Active Directory ist in Tabelle 3.2 zu finden.

Verbreitung: Auch hier wird sich wieder auf die Umfragen der LinuxFoundation und W3CTech gestützt, aus ihnen folgt, dass Windows im Server Einsatz eine wesentliche geringere Verbreitung besitzt als Linux.[Lin14; W3C18] Allerdings setzen laut einer Statistik von Spiceworks 97% aller Unternehmen auf Windows als Betriebssystem für Laptops und Desktop Computer. Diese These wird weiterhin durch [Blu15] verifiziert, welche von einer Verbreitung von 95% in den 1000 größten amerikanischen Unternehmen spricht. Somit ist eine sehr hohe Verbreitung vorhanden und es wird mit zehn (10) Punkten bewertet.[Pet17]

Aktualität: Laut Microsoft Support Webseite wurde das letzte Update von AD am 18.10.2018 unter Windows (10) und Server 2016 verteilt. Deshalb werden hier zehn (10) Punkte vergeben. [Mic18c]

Reife: Es konnte keine Liste unterstützter Features gefunden werden, allerdings ist die Verwendung von Microsoft AD zusammen mit LDAPv3 kompatiblen Verzeichnisdiensten möglich. Es kann also angenommen werden, dass AD alle entsprechenden Features unterstützt [Mic17]. Deshalb werden wie bei OpenLDAP zehn (10) Punkte vergeben.

Quellcode: Es ist kein Quellcode verfügbar, Microsoft AD ist Closed Source. Daher wird ein (1) Punkt vergeben.

Betriebssysteme: Microsoft AD ist nur unter Windows lauffähig. Daher werden 2,5 Punkte vergeben.

Sicherheit: Da AD aus mehr als einer Komponente besteht, wurden diese einzeln betrachtet und die Bewertungen der einzelnen Sicherheitslücken betrachtet und diese gemittelt. Als Wert ergab sich eine 6,3 nach CVSS. Die Berechnungsgrundlage ist im Anhang zu finden. Es wird deshalb nur ein (1) Punkt vergeben. Die gefundenen Sicherheitslücken sind in Tabelle B.1 aufgelistet.

Kosten: Der Mindestbetrag, welcher anfällt um ein Active Directory betreiben zu können, beläuft sich derzeit auf die Kosten der Lizenz für Windows Server 2019. Diese Lizenz kostet 501$ und enthält den AD-Server [Mic18d]. Weiterhin wird Azure Active Directory als Cloudlösung

angeboten, die Kosten dafür sind allerdings sehr variabel, da pro Eintrag und Monat gezahlt, oder eine Azure Subscription vorhanden sein muss. Aus Gründen der Einfachheit findet die Bewertung nur auf Basis der Windows Server Lizenz statt [Mic].

Standardisierung: Microsoft AD baut wie OpenLDAP auf RFC4511 für LDAP und weiterhin auf RFC4120 für Kerberos, RFC2865 für RADIUS und ITU X.509 für die Public Key Infrastruktur für Zertifikate.

Einsatzzweck: Verzeichnisdienst für die Firmen IT.

Merkmal	Bewertung	Gewichtung	Punktzahl
Verbreitung	10	2	20
Aktualität	10	1	10
Reife	10	2	18
Quellcode	1	3	3
Betriebssysteme	2,5	4	10
Sicherheit	1	1	1
Kosten	8	1	8
		Gesamtpunktzahl	72

Tabelle 3.2.: Die Bewertung der Merkmale für Active Directory.

3.3.3. GESI

Die Bewertung der GESI ist in Tabelle 3.3 zu finden.

Verbreitung: Die Gelbe Seiten der Industrie 4.0 befinden sich derzeit noch in Entwicklung, es ist daher mit keiner bzw. minimaler Verbreitung auszugehen. Deshalb wird eine Bewertung von einem (1) Punkt vergeben.

Aktualität: Das letzte Update, welches auf der Github Seite des Projekts zu verzeichnen ist vom 27.09.2018. Es werden daher zehn (10) Punkte vergeben.[Kre18]

Reife: Wie bei der Verbreitung des Projekts muss hier auf die noch anstehende bzw. gerade durchgeführte Entwicklung verwiesen werden. Daher wird auch hier ein (1) Punkt vergeben.

Quellcode: Der Quellcode steht unter der Apache 2.0 Lizenz und ist frei im Github Repsitory des ISW Stuttgart zu finden. Bei der genannten Lizenz müssen alle Veränderungen, die an der Software durchgeführt werden, nachverfolgbar dokumentiert werden und eine Kopie der Lizenz und ein Urheberrechtshinweis beigefügt werden. Daher werden hier acht (8) Punkte vergeben.

Betriebssysteme: Die GESI soll, wie OPC UA, für alle Betriebssysteme frei zur Verfügung stehen. Daher werden hier zehn (10) Punkte vergeben.

Sicherheit: Hierüber sind derzeit keine Daten vorhanden. Es werden keine (0) Punkte vergeben.

Kosten: Bei der GESI soll es sich nach fertiggestellter Entwicklung um freie Software handeln, diese soll kostenlos verfügbar sein. Deshalb werden zehn (10) Punkte vergeben.

Standardisierung: Die GESI implementiert einen Verzeichnisdienst auf Basis von OPC UA. Für ebendiese Implementierung ist bisher allerdings kein Standard vorhanden, die zu Grunde liegende Technologie ist jedoch in Form von IEC62541[IEC15] standardisiert.

Einsatzzweck: Verzeichnisdienst für die Produktion.

Merkmal	Bewertung	Gewichtung	Punktzahl
Verbreitung	1	2	2
Aktualität	10	1	10
Reife	1	2	2
Quellcode	8	3	24
Betriebssysteme	10	4	40
Sicherheit	0	1	0
Kosten	10	1	10
		Gesamtpunktzahl	88

Tabelle 3.3.: Die Bewertung der Merkmale für die GESI.

3.3.4. OPC UA .Net-GDS

Da diese Software unter zwei Arten von Lizenzen verwendet werden kann, werden in den Zeilen Quellcode Verfügbarkeit und Kosten zwei Bewertungen angegeben. Die erste Zahl gibt die Bewertung unter Verwendung von GNU General Public License Version 2 (GPLv2) an, die zweite bei Verwendung unter Verwendung von Reciprocal Community License (RCL). Die Bewertung von OPC UA .Net-GDS ist in Tabelle 3.4 zu finden.

Verbreitung: Laut einer Marktstudie aus dem Jahr 2017 setzen 25% aller Maschinenbauer auf OPC UA, weiterhin wird OPC UA von der OPC Foundation als defacto Standard für die Industrie 4.0 bezeichnet [OPC18]. Dies bedeutet, dass zumindest eine kleine Verbreitung des Produkts vorhanden sein muss, daher wird mit zwei (2) Punkten bewertet.

Aktualität: Die letzte Veränderung des Codes fand am 29.10.2018 statt.

Reife: Laut Angaben auf der Projektseite wird der komplette Umfang eines GDS von diesem Projekt umgesetzt. Nach stichprobenartiger Untersuchung dieser Angabe wurde nichts Gegenteiliges festgestellt. Deshalb werden zehn (10) Punkte vergeben.

Quellcode: Der Quellcode des GDS steht unter den selben Lizenzen wie das OPC Unified Architecture .NET Standard Projekt, da es sich um eine Implementierung dessen handelt. Die erste Lizenz steht nur für Firmenmitglieder der OPC Foundation zur Verfügung und heißt RCL. Diese stellt keine Anforderungen an die Veröffentlichung des Codes und bietet weiterhin alle Freiheiten.[OPC16] Deshalb werden hier zehn (10) Punkte vergeben.
Für alle weiteren Verwender gilt die GPLv2. Diese fordert, dass abgeleitete Programe bei produktiver Verwendung wieder veröffentlicht werden müssen und dass diese Verbreitung wieder unter GPLv2 stattfinden muss. Weiterhin müssen alle Veränderungen, die an der Software durchgeführt werden, nachverfolgbar aufgeschrieben werden und eine Kopie der Lizenz und ein Urheberrechtshinweis beigefügt werden. Aus diesem Grund werden hierfür

drei (3) Punkte vergeben. [OPC16].
Es kann also generell gesagt werden, dass entweder mit Geld oder mit Code bezahlt werden muss. Der Preis für eine Mitgliedschaft ist abhängig vom weltweiten jährlichen Absatz und beginnt bei $3000.

Betriebssysteme: Um OPC UA .Net-GDS verwenden zu können, muss das Programm aus dem Quellcode gebaut werden. Hierfür wird die .Net Bibliothek benötigt, diese steht derzeit für Windows, Linux und MacOS zur Verfügung [Reg18]. Die Unterstützung von .Net für BSD Systeme steht derzeit noch am Anfang der Entwicklung.[Nay18]

Sicherheit: Hierüber sind derzeit keine Daten vorhanden.

Kosten: Für diese Standard Implementierung fallen keine Kosten an, sollte man den Code unter GPLv2 verwenden wollen. Es werden also 10 Punkte vergeben.
Sollte keine Veröffentlichung des Codes gewünscht sein, fallen kosten ab $3000 pro Jahr an, deshalb wird ein (1) Punkt vergeben.

Standardisierung: OPC UA .Net-GDS implementiert den Global Discovery und Zertifikat Verwaltungs Server, welche in der Spezifikation der OPC UA Architektur Teil 12 zu finden ist [Reg18].

Einsatzzweck: Global Discovery und Zertifikat Verwaltungs Server für OPC UA mit möglicher Anbindung an bereits vorhandene Zertifikatsspeicher.

Merkmal	Bewertung	Gewichtung	Punktzahl
Verbreitung	1	2	2
Aktualität	10	1	10
Reife	10	2	20
Quellcode	3|10	3	9|30
Betriebssysteme	7,5	4	30
Sicherheit	0	1	0
Kosten	10|1	1	10|1
		Gesamtpunktzahl	81|93

Tabelle 3.4.: Die Bewertung der Merkmale für OPC UA .Net-GDS.

3.3.5. jabberd2

Die Bewertung für jabberd2 ist in Tabelle 3.5 zu finden.

Verbreitung: Die Verbreitung von jabberd2 kann als minimal angesehen werden, zwar verwendet Apples Chat Server eine modifizierte Version, aber die Verwendung von MacOS als Server Betriebssystem ist eher gering [Lin14; Pet17; W3C18]. Deshalb wird ein (1) Punkt vergeben.

Aktualität: Das letzte Update von jabberd2 fand am 1.11.2018 statt. Es werden deshalb zehn (10) Punkte vergeben.

Reife: jabberd2 implementiert 50 der aktiven und finalen 55 XMPP Erweiterungen, deshalb werden neun (9) Punkte vergeben.

Quellcode: Der Quellcode von jabberd2 ist unter GPLv2 verfügbar, diese fordert, dass abgeleitete Programme bei produktiver Verwendung wieder veröffentlicht werden müssen und dass diese Verbreitung wieder unter GPLv2 stattfinden muss. Weiterhin müssen alle Veränderungen, die an der Software durchgeführt werden, nachverfolgbar aufgeschrieben werden und eine Kopie der Lizenz und ein Urheberrechtshinweis beigefügt werden [OPC Foundation,2016]. Aus diesem Grund werden hierfür drei (3) Punkte vergeben.

Betriebssysteme: Jabberd2 unterstützt nativ nur Linux Betriebssysteme, nur für diese werden Pakete in Paketquellen zur Verfügung gestellt. Da der Quellcode frei verfügbar ist, kann sich das Paket auch für weitere Plattformen kompiliert werden, allerdings ist dieser dafür nicht optimiert und es bestehen Abhängigkeiten zu weiteren Paketen was zu Problemen führen könnte. Deshalb werden 2,5 Punkte vergeben.

Sicherheit: Da es keine genauen Angaben zu Sicherheitslücken in jabberd2 zu finden gibt, wurde nach diesen gesucht, dadurch konnte der Durchschnitt der Bewertungen auf 5,3 festgelegt werden. Es werden deshalb fünf (5) Punkte vergeben. Die gefundenen Sicherheitslücken sind in Tabelle B.4 aufgelistet.

Kosten: Jabberd2 ist ein Open Source Projekt und es fallen für die Verwendung keine Kosten an. Es werden zehn (10) Punkte vergeben.

Standardisierung: Jabberd2 baut auf den XMPP Standard, dieser ist in RFC6120 definiert. Auf weitere definierte Standards der XMPP-Foundation baut jabberd2 ebenso auf.

Einsatzzweck: Jabberd2 wurde für den Austausch von XML basierten Nachrichten entwickelt.

Merkmal	Bewertung	Gewichtung	Punktzahl
Verbreitung	1	2	2
Aktualität	10	1	10
Reife	9	2	18
Quellcode	3	3	9
Betriebssysteme	2,5	4	10
Sicherheit	5	1	5
Kosten	10	1	10
		Gesamtpunktzahl	64

Tabelle 3.5.: Die Bewertung der Merkmale für jabberd2.

3.3.6. COM/DCOM

Die Punktevergabe für COM/DCOM ist in Tabelle 3.6 zu finden.

Verbreitung: Die Verbreitung kann hier ähnlich bewertet werden wie bei Microsoft AD, höchstwahrscheinlich höher. Grundsätzlich wird COM in vielen Technologien von Microsoft verwendet, so zum Beispiel ActiveX. Es werden für die Höhe der Verbreitung zehn (10) Punkte vergeben.

Aktualität: Das letzte Update bezügliche COM wurde am 30.07.2018 für Windows 10 und Server 2016 ausgerollt, deshalb werden neun (9) Punkte vergeben [Mic18b].

Reife: Über die Reife der Entwicklung lässt sich keine Aussage treffen, da hier nicht gegen einen Standard ohne eine öffentlich zugängliche Spezifikation geprüft werden kann. Es werden deshalb null (0) Punkte vergeben.

Quellcode: COM und DCOM sind beide Closed Source, es ist also kein Quellcode verfügbar. Deshalb wird ein (1) Punkt vergeben.

Betriebssysteme: Es werden offiziell, sowohl als Client wie auch als Server, lediglich Windows Betriebssysteme unterstützt. Deshalb werden 2,5 Punkte vergeben.

Sicherheit: Der Durchschnitt der gefundenen Sicherheitslücken beläuft sich auf 6,15. Es wird deshalb ein (1) Punkt vergeben. Die gefundenen Sicherheitslücken sind in Tabelle B.2 aufgelistet.

Kosten: Es fallen keine Kosten an, da COM und DCOM auf Basis des Windows IoT Core Betriebssystems verwendet werden können, welches kostenlos zur Verfügung gestellt wird.[Mic15b] Sollte jedoch ein anderes Betriebssystem gewählt werden, fallen mindestens 145€ für die Verwendung von Windows 10 Home an.[Mic14] Es werden daher zehn (10) Punkte vergeben.

Standardisierung: COM und DCOM bauen auf keinen öffentlich bekannten Standard auf.

Einsatzzweck: Interprozesskommunikation auf lokaler und Netzwerk Ebene.

Merkmal	Bewertung	Gewichtung	Punktzahl
Verbreitung	10	2	20
Aktualität	9	1	9
Reife	0	2	0
Quellcode	1	3	3
Betriebssysteme	2,5	4	10
Sicherheit	1	1	1
Kosten	10	1	10
		Gesamtpunktzahl	53

Tabelle 3.6.: Die Bewertung der Merkmale für COM/DCOM.

3.3.7. Bonjour

Die genaue Punktevergabe für Bonjour ist in Tabelle 3.7 zu finden.

Verbreitung: Bonjour wird bei vielen Apple Produkten mitgeliefert. So liefern zum Beispiel iTunes und Apples Time Capsule Bonjour mit aus. Also kann angenommen werden, dass mindestens auf allen verkauften Apple Geräten Bonjour installiert ist. Weiterhin ist Bonjour auch Teil vieler Drucker, die Apples AirPrint unterstützen. Somit ist auf eine mittelmäßig Verbreitung zu schließen, es werden also fünf (5) Punkte vergeben.

Aktualität: Das letzte Update von Bonjour fand am 31.10.2016 statt. Es wird deshalb ein (1) Punkt vergeben.

Reife: In RFC6763 sind die Features eines zeroconf Clients und Servers beschrieben, diese werden alle von Bonjour erfüllt. Es werden deshalb zehn (10) Punkte vergeben.

Quellcode: Der Quellcode des in Bonjour enthaltetenen mDNSResponder steht unter Apache 2.0 Lizenz, diese fordert die Dokumentation der Änderungen und Kopien der Lizenz und des Urheberrechtshinweis müssen beigefügt werden.[App18] Der restliche Teil von Bonjour ist allerdings nicht frei erhältlich. Deshalb werden fünf (5) Punkte vergeben.

Betriebssysteme: Der Quellcode des mDNSResponders steht offen zur Verfügung, es kann also für alle betrachteten Betriebssysteme gebaut werden. Das komplette Paket nur für Windows und MacOS, deshalb werden fünf (5) Punkte vergeben.

Sicherheit: Bei Bonjour sind nur wenige Sicherheitslücken bekannt, deren Durchschnitt beläuft sich auf 5,5 nach CVSS. Es werden deshalb vier (4) Punkte vergeben. Die gefundenen Sicherheitslücken sind in Tabelle B.3 aufgelistet.

Kosten: Es fallen keine Kosten bei Verwendung an. Es werden zehn (10) Punkte vergeben.

Standardisierung: Bonjour baut auf den Zeroconf Standard auf, welcher nie verabschiedet wurde. Allerdings werden zur Realisierung Standards wie RFC6763 für eine DNS basierte Dienstermittlung und RFC6762 für einen Multicast basierten DNS.

Einsatzzweck: Automatisches entdecken und Einrichten von Netzwerkressourcen, wie Drucker oder Netzwerkspeicher.

Merkmal	Bewertung	Gewichtung	Punktzahl
Verbreitung	5	2	10
Aktualität	1	1	1
Reife	10	2	20
Quellcode	5	3	15
Betriebssysteme	5	4	20
Sicherheit	4	1	4
Kosten	10	1	10
		Gesamtpunktzahl	80

Tabelle 3.7.: Die Bewertung der Merkmale für Bonjour.

3.3.8. Avahi

Die genaue Vergabe der Punkte ist in Tabelle 3.8 zu finden.

Verbreitung: Die Verbreitung von Avahi ist grundsätzlich auf unixoide Betriebssysteme beschränkt, da bisher keine Portierung auf Windows vorgenommen wurde, wobei vor allem eine Lösung für Linux geschaffen werden sollte. Dies führte auch dazu, dass Avahi standardmäßig bei den meisten Linux Distributionen vorinstalliert ist. Linux besitzt auf Laptops und Desktop Rechner wenig Verbreitung, wird aber sehr stark in der Firmen-IT eingesetzt, daher kann von einer mittelmäßigen Verbreitung ausgegangen werden. Es werden auch hier fünf (5) Punkte vergeben [PL10].

Aktualität: Die letzte Veröffentlichung von Avahi auf Version 0.7 war laut Webseite am 10.07.2017, in den Paketquellen von Debian ist allerdings ein Update vom 27.04.2018 und in CentOS vom 09.11.2017 zu finden [HSL+05; Pkg13]. Die Software wird also stetig weiterentwickelt. Es wird deshalb eine Bewertung von drei (3) Punkten vergeben.

Reife: Avahi implementiert wie Bonjour eine Service Discovery auf Basis von DNS und ist vollkommen kompatibel zu Bonjour. Dies lässt auf eine vollkommene Implementierung des Standards schließen. Es werden also zehn (10) Punkte vergeben.

Quellcode: Der Quellcode von Avahi ist frei unter GNU Lesser General Public License v2.1 (LGPL) verfügbar. Diese ermöglicht eine Verwendung ähnlich der GPLv2, allerdings sind von der Veröffentlichung unter gleicher Lizenz Programme ausgeschlossen, welche das Projekt nur als Bibliothek verwenden. Deshalb werden fünf (5) Punkte vergeben.

Betriebssysteme: Avahi ist vor allem für Linux entwickelt worden und ist deshalb in den weitest verbreiteten Linux Distributionen, wie Ubuntu, Debian, CentOS und Red Hat Enterprise Linux, in den Paketquellen erhältlich. Weiterhin ist Avahi auch in den Paketquellen von vielen BSD Systemen erhältlich. Es werden also fünf (5) Punkte vergeben.

Sicherheit: Die Bewertung der Sicherheitslücken liegt im Mittel bei 4,6 nach CVSS, es werden deshalb zehn (10) Punkte vergeben [MIT18a].

Kosten: Der Quellcode von Avahi ist Open Source. Es fallen deshalb keine Kosten für die Verwendung an. Es werden zehn (10) Punkte vergeben.

Standardisierung: Avahi baut wie Bonjour auf RFC6762 und RFC6763 auf.

Einsatzzweck: Automatisches entdecken und Einrichten von Netzwerkressourcen, wie Drucker oder Netzwerkspeicher.

Merkmal	Bewertung	Gewichtung	Punktzahl
Verbreitung	5	2	10
Aktualität	3	1	3
Reife	10	2	20
Quellcode	5	3	15
Betriebssysteme	5	4	20
Sicherheit	10	1	10
Kosten	10	1	10
		Gesamtpunktzahl	88

Tabelle 3.8.: Die Bewertung der Merkmale für Avahi.

3.4. Fazit

Aus Tabelle 3.9 geht hervor, dass OpenLDAP bei Betrachtung aller verglichenen Merkmale am besten abschneidet, so sprechen nur das schlechte Abschneiden in den Kategorien Sicherheit und Aktualität gegen eine Verwendung. Gerade ersteres ist aber, wie schon in der Vorstellung des Merkmals beschrieben, an sich sehr schwer zu bewerten. Des weiteren sind die Entwickler für schnelle Reaktion beim Auftreten von Sicherheitslücken bekannt, dies spielt gerade bei schwerwiegenden Sicherheitsproblemen eine größere Rolle als der CVSS Score. Neben diesen Gründen ist außerdem das lange Bestehen des Projekts hervorzuheben; es feierte im Jahr 2018 20 jähriges Jubiläum. Trotz des langen Existenz sind auf der Webseite des Projekts Pläne für die Zukunft zu finden, somit ist nicht mit einer baldigen Einstellung des Projekts zu rechnen. Bei Verwendung in der Produktion muss allerdings noch sichergestellt werden, dass auch die dienstanfordernden Geräte mit einem LDAP-Server kommunizieren können.

Technologie	Gesamtpunktzahl
OpenLDAP	116
Active Directory	72
GESI	88
.Net-GDS	84|103
jabberd2	64
COM/DCOM	53
Bonjour	80
Avahi	88

Tabelle 3.9.: Ergebnis des Vergleichs.

Neben OpenLDAP sind noch die Technologien OPC UA .Net-GDS, GESI und Avahi hervorzuheben, alle drei sind Open Source, allerdings verlangt erstes auf Grund der Lizenz bei Verwendung für ein neues Produkts die Offenlegung des Quellcodes des entstehenden Produkts, sollte keine Mitgliedschaft bei der OPC Foundation bestehen. Dies ist gerade dann ein Problem, sollten strategische Firmengeheimnisse im Code zu finden sein und der mit der Entwicklung beschäftigten Firma begrenzte finanzielle Mittel zur Verfügung stehen. Ähnliches trifft auch auf Avahi zu, hier allerdings nur sollte der Code an sich verändert und nicht nur als Programm Bibliothek verwendet werden. Dies ist zum derzeitigen Stand des Projekts bei der GESI kein Problem, da sie unter der Lizenz Apache v2 steht und somit bei Verwendung keine weiteren Veröffentlichungen folgen müssen. Jedoch gestaltet es sich zum jetzigen Stand des Projekts noch schwer, definitive Aussagen zu tätigen. Dies ist ein großer Vorteil von OPC UA .Net-GDS und Avahi, da beide volle Marktreife besitzen. Bei allen dreien ist aber auch klar auf die verschiedenen Einsatzgebiete hinzuweisen, hier ähneln sich GESI und OPC UA .Net-GDS am ehesten. Beide sind für den Einsatz in der Produktion geschrieben und benötigen daher keine Anpassungen an dieses Umfeld. Bei Avahi gestaltet sich dies etwas anders. Avahi muss, um im Produktionsumfeld einsetzbar zu sein, entweder angepasst werden oder das Produktionsumfeld muss sich an Avahi anpassen, da es nur auf die Verwendung in der IT ausgelegt ist. Weiterhin besitzt es nicht den selben Funktionsumfang wie GESI und OPC UA .Net-GDS, so können beide zur Verwaltung von Zertifikaten eingesetzt werden und sind netzwerkübergreifend einsetzbar. Dies ist bei Avahi nicht der Fall, da es Multicast zum Finden anderer Dienste verwendet und eine netzwerkübergreifende Kommunikation nicht ohne Weiteres möglich ist. Aber im Gegensatz zu GESI und OPC UA .Net-GDS ist Avahi ein Produkt mit großer Verbreitung und wird seit fast 20 Jahren in der IT eingesetzt. Ein Vorteil gegenüber ersteren ist jedoch eine mögliche Verwendung als dezentrales Protokoll für den Austausch von Fähigkeiten, das heißt es wird kein zentrale Stelle benötigt welche die gespeicherten Daten vorhält.

Auf dem fünften Platz befindet sich Bonjour, es besitzt grundsätzlich die selben Eigenschaften wie Avahi, muss also auch für den Einsatz in der Produktion angepasst werden, ist aber schon ähnlich lang in der IT im Einsatz. Aber anders als Avahi ist der Quellcode nur zum Teil Open Source, was diese Anpassungen schwieriger gestaltet.

Den sechsten Platz teilen sich jabberd2 und Active Directory. Jabber bzw. XMPP besitzt als Technologie großes Potential für die Verwendung als Service Discovery Dienst und für den Daten- und Befehlsaustausch zwischen Teilnehmern. Da Nachrichten in Form von XML verschickt werden, können grundsätzlich alle Arten von Daten versendet werden. Die Protokollerweiterung um eine Service Discovery wird verwendet, damit Clients aber auch Server Netzwerkdienste finden können welche zur Kommunikation genutzt werden können. Daneben sind Erweiterungen spezifiziert, welche eine Publish-Subscribe Architektur ermöglichen. Es ist also möglich XMPP als Kommunikationsdienst für den Austausch von Daten und das automatische Verteilen von Daten zu verwenden, ähnlich einem GDS wie er innerhalb OPC UAs spezifiziert wurde. Die Datenhaltung, also unter anderem der Verzeichnisdienst im Hintergrund, kann auch mit XMPP realisiert werden, da mit den Erweiterungen XEP-0222 und XEP-0223 die persistente Speicherung von Daten möglich ist. Eine Anbindung an einen bereits vorhandenen Verzeichnisdienst ist möglich, aber nicht im Protokoll vorgesehen. Dies ist also vom dann verwendeten Server abhängig. Hier spielt AD wieder seine Stärken aus, es handelt sich schon um einen Verzeichnisdienst und dabei auch um einen mit hoher Verbreitung. Es müssen also kaum Anpassungen vorgenommen werden, sollte er in der Produktion Verwendung finden. Hierbei ist nur darauf zu achten, dass es keine Möglichkeit gibt AD auf Basis eines anderen Betriebssystems als Windows zu verwenden. Es ist zwar möglich Linux-, MacOS- und BSD-basierte Maschinen über ein Active Directory zu verwalten. Dies gestaltet sich

aber wesentlich schwieriger wie die Verwendung von OpenLDAP und ist unter MacOS nicht ohne zusätzliche Software möglich[Mac14; Red]. Diese Eigenschaft ist jedoch gewünscht, da nicht abzusehen ist, welche Betriebssysteme sich in der Produktion in den nächsten Jahren durchsetyen werden. Des weiteren ist eine Anpassung von Active Directory nicht möglich, sollten speziellere Anforderungen gestellt werden. Diese letzten beiden Punkte, die geringe Interoperabilität mit anderen Betriebssystemen als Windows und das nicht Vorhandensein von Programmcode, kosten Microsoft AD sehr viele Punkte, weshalb es erst auf dem sechsten Platz zu finden ist. Für eine Verwendung an sich spricht aber vor allem die extreme Verbreitung von Windows Systemen in der Wirtschaft und die damit einhergehende Verbreitung von AD.

Auf dem letzten Platz findet sich COM/DCOM, es verliert wie schon zuvor AD vor allem Punkte auf Grund der eingeschränkten Einsatzmöglichkeit auf anderen Betriebssystemen und die nicht Verfügbarkeit von Quellcode. Weitere Gründe die gegen eine Verwendung von COM/DCOM in einer modernen vernetzten Produktion sprechen, wie sie in einer Industrie 4.0 vorgesehen ist, sind die Schwierigkeiten die sich bei der netzwerkübergreifenden Kommunikation ergeben. So gestaltet es sich schwer die Kommunikation durch Firewalls zu ermöglichen.

4. Prototypische Implementierung

Im Zuge dieser Arbeit wurde neben der Literaturrecherche und dem Vergleich der dabei gefundenen Technologien auch ein Proof of Concept durchgeführt. Hierzu wurden zwei kurze Programme geschrieben, die zeigen, dass die Integration eines Verzeichnisdiensts in die Produktion möglich ist. Im folgenden werden der Systementwurf und die Systemimplementierung beschrieben.

4.1. Systementwurf

Eine gelungene Kommunikation zwischen der IT und der Produktion besteht aus drei Teilen:

- dem Verzeichnisdienst,
- einem Connector und
- dem Protokoll welches als Schnittstelle zur Produktion fungiert.

Der Connector entspricht dabei dem Proof of Concept. Als Verzeichnisdienst wird hierbei auf OpenLDAP gesetzt, da es im vorangegangenen Vergleich als zu empfehlende Technologie hervorging. Als Dienst für die Produktion wird OPC UA verwendet, da es in der Referenzimplementierung für das Modell der Industrie 4.0 als Maschine zu Maschine Kommunikationsprotokoll ausgewählt wurde. Als Implementierung des Servers wird der Beispiel Server des *open62541* Projekts verwendet. Die Wahl der Programmiersprache für den Connector fiel auf *Python*, da für diese zahlreiche Bibliotheken zur Kommunikation mit OpenLDAP wie auch OPC UA zur Verfügung stehen. Als Bibliotheken wurde *python-ldap* und *python-opcua* verwendet, da es sowohl Client wie auch Server Implementierungen nativ zur Verfügung stellt.[IEC15; JNP15b; Tim18] In Abbildung 4.1 ist der oben beschriebene Verlauf dargestellt.

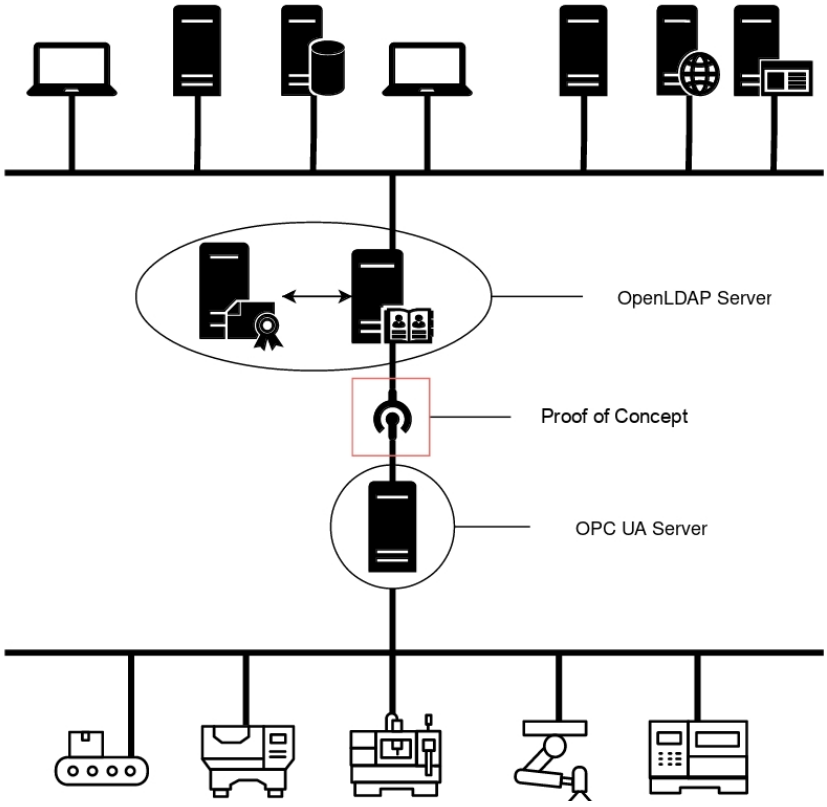

Abbildung 4.1.: Konzept einer möglichen Kommunikation zwischen der IT und der Produktion. Auf Seiten der IT wird dazu ein OpenLDAP Server eingesetzt, der mittels des Proof of Concepts Daten der Produktion mit dem OPC UA Server austauschen kann.

4.2. Systemimplementierung

Als Vorbereitung auf die Implementierung wurde OpenLDAP installiert und nach dem Tutorial im Wiki von Arch Linux konfiguriert. Danach wurde ein OPC UA-Server nach Anleitung installiert und konfiguriert. Da hier sowohl Daten geschrieben als auch ausgelesen werden sollten, wurde so lange dem Tutorial gefolgt, bis eine schreibbare Variable vom Server zur Verfügung gestellt wurde. Hierauf wurde dann mit der Implementierung der Connectoren von OPC UA nach OpenLDAP begonnen und umgekehrt, die Implementierungen sind in den Listings 4.1 und 4.2 zu finden.[HK12; Ope16]

```
import ldap, opcua
from opcua import Client
from opcua import ua

# Verbindung konfigurieren und sich mit Server verbinden
client = Client("opc.tcp://localhost:4840/freeopcua/server/")
client.connect()

# Objekt Knoten in object speichern und Variable ,the answer' in var ablegen
objects = client.get_objects_node()
var = client.get_node("ns=1;s=the.answer")

# Wert auslesen
opc_val = var.get_value()

# Verbindung zu Server trennen
client.disconnect()

# Verbindung mit dem Server auf localhost herstellen und einloggen als Manager
ldap_con = ldap.initialize('ldap://localhost:389', trace_level=0, trace_file=sys.stderr)
ldap_con.protocol_version = ldap.VERSION3
ldap_con.simple_bind_s('cn=Manager,dc=example,dc=com','secret')

# ausgelesenen Wert von int in byte string umwandeln
opc_val = str(opc_val).encode()

# description von Eintrag replica loeschen
ldap_con.modify('cn=replica,dc=example,dc=com', [(ldap.MOD_DELETE, 'description', None)])

# Variable in description eintragen
ldap_con.modify('cn=replica,dc=example,dc=com', [(ldap.MOD_ADD, 'description', opc_val)])

#Verbindung zu Server trennen
ldap_con.unbind_s()
```

Listing 4.1: Code für die Übertragung einer Variablen von OPC UA nach OpenLDAP

```
import ldap, opcua
from opcua import Client
from opcua import ua

# Verbindung mit OpenLDAP Server aufbauen und als Manager einloggen
ldap_con = ldap.initialize('ldap://localhost:389', trace_level=0, trace_file=sys.stderr)
ldap_con.protocol_version = ldap.VERSION3
ldap_con.simple_bind_s('cn=Manager,dc=example,dc=com','secret')

# Nach dem Attribut von replica suchen und und in ldap_val ablegen
ldap_val = ldap_con.search_s('cn=replica,dc=example,dc=com', ldap.SCOPE_SUBTREE,attrlist= ["
description"])

# Wert der Variablen aus Liste, Tupel, Dict und Liste auslesen und dann von Bytestring in
Integer umwandeln
ldap_val = ldap_val[0][1]['description'][0]
ldap_val = int(ldap_val.decode())

# Verbindung zu OpenLDAP trennen
ldap_con.unbind_s()

# Verbindung zu OPC UA Server aufbauen, dann mit ihm verbinden
client = Client("opc.tcp://localhost:4840/freeopcua/server/")
client.connect()

# Objekt welches Variable enthaelt in objects ablegen, dann die Variable in var ablegen
objects = client.get_objects_node()
var = client.get_node("ns=1;s=the.answer")

# Variable mit Angabe des Typs schreiben
var.set_value(ua.Variant(ldap_val, ua.VariantType.Int32))

# Verbindung zu Server trennen
client.disconnect()
```

Listing 4.2: Code für die Übertragung einer Variablen von OpenLDAP nach OPC UA

Wie in den Listings 4.1 und 4.2 zu sehen ist, mussten zur Erreichung der geforderten Funktionalität je unter zwanzig Zeilen Code geschrieben werden. Um sicherzustellen, dass die Übertragung auch funktioniert, wurde nach jeder Ausführung kontrolliert, ob sich die entsprechenden Werte übertragen wurden, hierzu wurde das Bordmittel *ldapsearch* auf Seiten OpenLDAPs und UAExpert für OPC UA verwendet.

Es konnte an dieser Stelle zwar mit relativ geringem Aufwand eine Datenübertragung zwischen OPC UA und OpenLDAP hergestellt werden, jedoch ist dies auch nur ein Proof of Concept mit dem gezeigt werden sollte, dass eine Kommunikation zwischen Technologien aus der IT und der Produktion möglich ist. Die Implementierung einer Software für den produktiven Einsatz, gerade in einem Bereich wie der Produktion, ist mit wesentlich höherem Aufwand verbunden. Dies ist vor allem der nötigen Einhaltung erhöhter Sicherheitsstandards und den einhergehenden Tests geschuldet.

5. Zusammenfassung und Ausblick

Viele Firmen sehen weltweit wachsende Absatzmärkte und damit einhergehende Möglichkeiten zur Expansion, zu Standortneuerschließungen und zur Anschaffung von Produktionsmaschinen. Daraus ergibt sich auch eine sich immer weiterentwickelnde Veränderung hinsichtlich der Verantwortung diese Maschinen zu warten und zu verwalten. Der Simplizität wegen resultiert daraus ein technisches Verlangen danach, diese Verantwortung für die einzelnen Produktionsststätten zu zentralisieren, um den Aufwand zu minimieren. Es muss also eine Möglichkeit geschaffen werden, diese technischen Anforderungen auch von Extern, beispielsweise mittels einer Cloud, bewältigen zu können. Ein sehr ähnliches Problem wurde bereits in der Informationstechnik gelöst, hier sollte allerdings die Verwaltung von Servern und Arbeitsplatzrechnern vereinfacht werden. Hierfür wurden Verzeichnisdienste genutzt, die bis heute eingesetzt werden. In der Industrie 4.0 soll sich nun mit Hilfe von Verzeichnisdiensten diesem Problem angenommen werden.

Wie in 1.3.1 bereits beschrieben, sind Verzeichnisdienste mit weiteren Diensten koppelbar. Ein prominentes Beispiel ist RADIUS. Remote Authentication Dial-In User Service (RADIUS) ist ein Protokoll welches, wie der Name schon sagt, die Authentifizierung für sich einwählende Nutzer bereitstellt. Es enthält aber auch Funktionen das es zu einem sogenannten Authentifizierung-Autorisierungs-Abrechnungs-Dienst (kurz AAA-Dienst) machen. Die Daten für die Authentifizierung können dabei durch einen Verzeichnisdienst zur Verfügung gestellt werden, jedoch werden alle weiteren Funktionen vom RADIUS-Server selbst bereitgestellt. Diese Art von Diensten werden vor allem für Dienstleistungen verwendet, welche eine Zugriffs und Zeit basierte Abrechnung erfordern [RWRS00]. Bei Kerberos handelt es sich dagegen um ein Protokoll für einen verteilten Authentifizierungsdienst, welcher vor allem für offene und unsichere Computernetze gedacht ist. Auch hier können die Daten, die für die Authentifizierung benötigt werden, wieder von einem Verzeichnisdienst bereitgestellt werden, dies muss aber nicht immer der Fall sein [NYHR05].

Eine Literaturrecherche nach solchen Verzeichnisdiensten und deren Vergleich miteinander ist Gegenstand dieser Arbeit. Hierfür wurde zunächst eine Recherche nach Verzeichnisdiensten und Technologien, die sich als solche eignen, angestellt. Die ersten Ergebnisse wurden thematisch nach den Gebieten Informationstechnik und Produktion geordnet. Auffällig war, dass klassische Verzeichnisdienste nur in der IT auftreten. Aus diesen Ergebnissen wurden diejenigen für den Vergleich ausgewählt, die populär und auf dem deutschen Mark relevant sind. Die einzelnen Merkmale des Vergleichs, wie die Sicherheit der Technologie, ihre Kosten, ihre Verbreitung und die Anzahl der unterstützten Betriebssysteme, wurden unterschiedlich gewichtet und somit ein Punktesystem entwickelt. Das Ergebnis des Vergleichs ist in Tabelle 5.1 aufgeführt. Aus der Tabelle wird ersichtlich, dass für OpenLDAP mit dem höchsten Punktestand eine Empfehlung auszusprechen ist. Abschließend wurde ein Proof of Concept durchgeführt, mit dem gezeigt wurde, dass eine Kommunikation zwischen OpenLDAP und OPC UA möglich ist.

Technologie	Verbreitung	Aktualität	Reife	Quellcode Verfügbarkeit
OpenLDAP	20	6	20	36
Active Directory	20	10	20	4
GESI	2	10	2	32
OPC UA .Net GDS	2	10	20	12|40
jabberd2	2	10	18	12
COM/DCOM	20	9	0	4
Bonjour	10	1	20	20
Avahi	10	3	20	20

Technologie	Betriebssysteme	Sicherheit	Kosten	Gesamtpunktzahl
OpenLDAP	30	3	10	125
Active Directory	10	1	8	73
GESI	40	0	10	96
OPC UA .Net GDS	30	0	10|1	84|103
jabberd2	10	5	10	67
COM/DCOM	10	1	6 50	
Bonjour	20	4	10	85
Avahi	20	10	10	93

Tabelle 5.1.: Überblick über des Ergebnis des Vergleichs.

Für die Entscheidung für eine dieser Technologien muss allerdings berücksichtigt werden, dass Aspekte wie deren Bedienbarkeit gänzlich für den Vergleich unbeachtet blieben. Ebenso wurde vernachlässigt, ob die Technologie möglicherweise mit bereits in der Infrastruktur vorhandenen Systemen gekoppelt werden kann. So ist Microsoft AD für ein Unternehmen eventuell besser geeignet als OpenLDAP, wenn es bereits Microsoft Windows als Betriebssystem nutzt. Dadurch können auch bestimmte Funktionalitäten durch Kerberos genutzt werden, ohne diese wie in OpenLDAP selbst implementieren zu müssen.

Zusätzlich konnte die Verbreitung nur geschätzt werden. Weiterhin wurde nicht betrachtet, wie groß der Aufwand wäre, ein bereits bestehendes System um diese Technologie zu erweitern. Ein weiterer zu berücksichtigender Gesichtspunkt ist, dass diese Ergenisse nur auf einer Literaturrecherche basieren. Eine relative Rückkopplung zur Praxis ist beispielsweise durch die untersuchten Sicherheitslücken gegeben, allerdings hinsichtlich der fehlenden Betrachtung aus Sicht der Industrie nicht aussagekräftig genug.

Um diese Ungenauigkeiten zu minimieren, sind weitere Arbeiten in diesem Forschungsbereich nötig. Schätzungen können zum Beispiel durch das Anfertigen fundierter Statistiken mittels Umfragen ersetzt werden. Außerdem ist es noch nicht ersichtlich, welche Technologien sich in der Produktion durchsetzen werden. Eine der neueren Technologien ist beispielsweilse XMPP, welches gerade für das Internet of Things Anwendung findet. Diese neuen und der weitere Entwicklungsverlauf bereits bekannter Technologien sollte in Zukunft verfolgt werden. Auch kann der Proof of Concept ausgeweitet werden, um das Zusammenspiel zwischen OpenLDAP und OPC UA besser bewerten zu können.

Literaturverzeichnis

[AOE] AOE. *Open Source: Vorteile von Open Source Software*. URL: https://www.aoe.com/de/open-source.html (besucht am 08. 01. 2019) (zitiert auf S. 31).

[App18] Apple. *Bonjour*. 2018. URL: https://developer.apple.com/bonjour/ (besucht am 14. 12. 2018) (zitiert auf S. 25, 40).

[Bal15] B. Balter. *6 motivations for consuming or publishing open source software*. 2015. URL: https://opensource.com/life/15/12/why-open-source (besucht am 09. 01. 2019) (zitiert auf S. 31).

[Ben18] P. D. O. Bendel. *Industrie 4.0*. 2018. URL: https://wirtschaftslexikon.gabler.de/definition/industrie-40-54032/version-277087 (besucht am 20. 12. 2018) (zitiert auf S. 15).

[Blu15] E. Blum. „Active Directory facts Infographics“. In: *ITSMdaily* (Nov. 2015). URL: https://www.itsmdaily.com/active-directos-infographics/ (zitiert auf S. 19, 34).

[BSI13] BSI. *IT Grundschutz Glossar*. 2013. URL: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Glossar/glossar%7B%5C_%7Dnode.html (besucht am 04. 12. 2018) (zitiert auf S. 15).

[Bun18] S. Bundesamt. *Ausstattung privater Haushalte mit Informations- und Kommunikationstechnik - Deutschland*. 2018. URL: https://www.destatis.de/DE/ZahlenFakten/GesellschaftStaat/EinkommenKonsumLebensbedingungen/AusstattungGebrauchsguetern/Tabellen/Infotechnik%7B%5C_%7DD.html (besucht am 28. 07. 2018) (zitiert auf S. 13).

[Che] S. Cheshire. *Zeroconf*. URL: http://www.zeroconf.org/ (besucht am 19. 12. 2018) (zitiert auf S. 25).

[Cis] Cisco. *Service Discovery Gateway*. URL: https://www.cisco.com/c/en/us/products/ios-nx-os-software/service-discovery-gateway/index.html (besucht am 09. 01. 2019) (zitiert auf S. 25).

[DAT09] DATACOM. *DCOM (distributed component object model)*. 2009. URL: https://www.itwissen.info/DCOM-distributed-component-object-model.html (besucht am 19. 12. 2018) (zitiert auf S. 26).

[DAT11] DATACOM. *OPC (OLE for process control)*. 2011. URL: https://www.itwissen.info/OPC-OLE-for-process-control.html (besucht am 19. 12. 2018) (zitiert auf S. 26).

[DINa] DIN. *DIN - kurz erklärt*. URL: https://www.din.de/de/ueber-normen-und-standards/basiswissen (besucht am 12. 12. 2018) (zitiert auf S. 32).

[DINb] DIN. *infografik-normung-auf-einen-blick-data*. URL: https://www.din.de/blob/249724/90b7c7913c86fd0dea7c6cc63ad0c316/infografik-normung-auf-einen-blick-data.jpg (besucht am 10. 12. 2018) (zitiert auf S. 32).

[Dud] Duden. *IT*. URL: https://www.duden.de/rechtschreibung/IT (besucht am 04. 12. 2018) (zitiert auf S. 15).

[Fre18] FreeIPA. *FreeIPA*. 2018. URL: www.freeipa.org (besucht am 08. 01. 2019) (zitiert auf S. 19).

[Geo17a] S. George. *Azure IoT Hub Device Provisioning Service preview automates device connection and configuration!* 2017. URL: https://azure.microsoft.com/en-us/blog/azure-iot-hub-device-provisioning-service-preview-automates-device-connection-configuration/ (zitiert auf S. 24).

[Geo17b] S. George. *Simplifying OPC UA security for everyone*. 2017. URL: https://azure.microsoft.com/de-de/blog/simplifying-opc-ua-security-for-everyone/ (zitiert auf S. 24).

[HB13] E. Hamburger, D. Bohn. *Exclusive: Inside Hangouts, Google's big fix for its messaging mess*. 2013. URL: https://www.theverge.com/2013/5/15/4318830/inside-hangouts-googles-big-fix-for-its-messaging-mess (besucht am 06. 12. 2018) (zitiert auf S. 24).

[HK12] Hauptmech, Kynikos. *OpenLDAP*. 2012. URL: https://wiki.archlinux.org/index.php/OpenLDAP (besucht am 20. 12. 2018) (zitiert auf S. 46).

[HSL+05] A. Henriksson, F. Sateler, I. Lane, J. Bicha, L. Bigonville, M. Pitt, M. Biebl, S. McVittie, S. Simons, T. Bechtold. *Avahi*. 2005. URL: https://salsa.debian.org/utopia-team/avahi (besucht am 14. 12. 2018) (zitiert auf S. 41).

[ICA18] ICANN. *Service Name and Transport Protocol Port Number Registry*. 2018 (zitiert auf S. 21).

[IEC15] IEC. *OPC Unified Architecture*. 2015 (zitiert auf S. 36, 45).

[ITA] IT-Administrator. *Zeroconf*. URL: https://www.it-administrator.de/lexikon/zeroconf.html (besucht am 19. 12. 2018) (zitiert auf S. 22, 25).

[ITU16] ITU. *X.500*. Genf, 2016 (zitiert auf S. 18).

[JNP15a] J. Jasperneite, A. Neumann, F. Pethig. „OPC UA versus MTConnect". In: *Computer Automation* July (2015), S. 6 (zitiert auf S. 26, 27).

[JNP15b] P. D. J. Jasperneite, A. Neumann, F. Pethig. *Vergleich zwischen OPC UA und MTConnect*. 2015. URL: https://www.computer-automation.de/steuerungsebene/steuern-regeln/artikel/119808/ (besucht am 19. 12. 2018) (zitiert auf S. 45).

[KLIS18] D. F. Kretschmer, A. Lechler, F. Isw, U. Stuttgart. „Gelbe Seiten für Industrie 4 . 0 Aufbrechen statischer Produktionsstrukturen mittels eines übergeordneten Verzeichnisdienstes". In: (2018) (zitiert auf S. 23).

[Kno16] A. Knoll. „Jeder Anwendung ihr Protokoll". In: *Markt & Technik* (Nov. 2016). URL: https://www.elektroniknet.de/markt-technik/automation/jeder-anwendung-ihr-protokoll-135448.html (zitiert auf S. 27).

[Kre18] F. Kretschmer. *GESI Core*. 2018. URL: https://github.com/iswunistuttgart/gesi (besucht am 12. 12. 2018) (zitiert auf S. 35).

[KTM+18] G. der Kinderen, M. Taylor, E. Mons, J. Schäfer, G. Lukas, J. Timothée. *An Overview of XMPP*. 2018. URL: https://xmpp.org/about/technology-overview.html (besucht am 06. 12. 2018) (zitiert auf S. 24).

[KWH13] H. Kargerman, W. Wahlster, J. Helbig. „Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0“. In: *Bmbf.De* April (2013), S. 1–116. ISSN: 978-3-8047-2549-2 (zitiert auf S. 13, 17).

[LBS+18a] S. Ludwig, J. Beda, P. Saint-Andre, R. McQueen, S. Egan, J. Hildebrand. „Xep-0166: Jingle“. In: *XMPP Standards Foundation* (2018). URL: https://xmpp.org/extensions/xep-0166.html (zitiert auf S. 24).

[LBS+18b] S. Ludwig, J. Beda, P. Saint-Andre, R. McQueen, S. Egan, J. Hildebrand. „XEP-0060 : Publish-Subscribe“. In: *XMPP Standards Foundation* (2018) (zitiert auf S. 24).

[Lin14] Linux Foundation. „2014 Enterprise End User Trends Report: Fourth Annual Survey of Enterprise Linux Users“. In: *Linux Foundation* December (2014), S. 9. URL: http://www.linuxfoundation.org/publications/linux-foundation/linux-end-user-trends-report-2014 (zitiert auf S. 33, 34, 38).

[LS18] P. D. R. Lackes, D. M. Siepermann. *IT*. 2018. URL: https://wirtschaftslexikon.gabler.de/definition/it-38583/version-262004 (besucht am 04. 12. 2018) (zitiert auf S. 15).

[Mac14] MacWelt. *So arbeitet Microsoft Active Directory mit MacOS X*. 2014. URL: https://www.pcwelt.de/ratgeber/Verzeichnisdienst-So-arbeitet-Microsoft-Active-Directory-mit-MacOS-X-364256.html (besucht am 16. 12. 2018) (zitiert auf S. 44).

[Mat13] C. Mathias. *With Apple Bonjour gateways, say hello to cross-network discovery*. 2013. URL: https://searchmobilecomputing.techtarget.com/opinion/With-Apple-Bonjour-gateways-say-hello-to-cross-network-discovery (besucht am 09. 01. 2019) (zitiert auf S. 25).

[Mic] Microsoft. *Azure Active Directory*. URL: https://azure.microsoft.com/de-de/services/active-directory/ (besucht am 06. 12. 2018) (zitiert auf S. 21, 35).

[Mic14] Microsoft. *Windows 10 Home*. 2014. URL: https://www.microsoft.com/de-de/p/windows-10-home/d76qx4bznwk4/1NT3 (besucht am 14. 12. 2018) (zitiert auf S. 39).

[Mic15a] Microsoft. *History of DCOM*. 2015. URL: https://msdn.microsoft.com/en-us/library/6zzy7zky.aspx (besucht am 29. 10. 2018) (zitiert auf S. 26).

[Mic15b] Microsoft IoT. *Windows 10 IoT Core is available for commercial and industrial device builders*. 2015. URL: https://blogs.microsoft.com/iot/2015/12/03/windows-10-iot-core-is-available-for-commercial-and-industrial-device-builders-2/ (besucht am 10. 01. 2019) (zitiert auf S. 39).

[Mic17] Microsoft. *Konfigurieren von AD FS zum Authentifizieren von Benutzern in LDAP-Verzeichnissen gespeichert*. 2017. URL: https://docs.microsoft.com/de-de/windows-server/identity/ad-fs/operations/configure-ad-fs-to-authenticate-users-stored-in-ldap-directories (besucht am 14. 12. 2018) (zitiert auf S. 34).

[Mic18a] Microsoft. *About Active Directory Domain Services*. 2018. URL: https://docs.microsoft.com/en-us/windows/desktop/ad/about-active-directory-domain-services (besucht am 01. 09. 2018) (zitiert auf S. 22).

[Mic18b] Microsoft. *July 30, 2018 - KB4346877 (OS Build 14393.2396)*. 2018. URL: https://support.microsoft.com/en-us/help/4346877 (besucht am 14. 12. 2018) (zitiert auf S. 39).

[Mic18c] Microsoft. *October 18, 2018—KB4462928 (OS Build 14393.2580)*. 2018. URL: https://support.microsoft.com/en-us/help/4462928 (besucht am 14. 12. 2018) (zitiert auf S. 34).

[Mic18d] Microsoft. *Windows Server 2019 Preis*. 2018. URL: https://www.microsoft.com/de-de/cloud-platform/windows-server-pricing (besucht am 03. 12. 2018) (zitiert auf S. 21, 34).

[MIT18a] MITRE. *CVSS Score Avahi*. 2018. URL: https://www.cvedetails.com/cvss-score-charts.php?fromform=1%7B%5C&%7Dvendor%7B%5C_%7Did=%7B%5C&%7Dproduct%7B%5C_%7Did=7747%7B%5C&%7Dstartdate=1999-01-01%7B%5C&%7Denddate=2018-12-20 (besucht am 20. 12. 2018) (zitiert auf S. 41).

[MIT18b] MITRE. *CVSS Scores For Openldap Products Between 1999-01-01 and 2018-12-13*. 2018. URL: https://www.cvedetails.com/cvss-score-charts.php?fromform=1%7B%5C&%7Dvendor%7B%5C_%7Did=439%7B%5C&%7Dproduct%7B%5C_%7Did=%7B%5C&%7Dstartdate=1999-01-01%7B%5C&%7Denddate=2018-12-13 (besucht am 13. 12. 2018) (zitiert auf S. 33).

[MLD09] W. Mahnke, S. H. Leitner, M. Damm. *OPC unified architecture*. 2009. ISBN: 9783540688983. DOI: 10.1007/978-3-540-68899-0. arXiv: arXiv:1011.1669v3 (zitiert auf S. 23).

[MO18] B. Mathers, Olprod. *Was ist eine Hybrididentität?* 2018. URL: https://docs.microsoft.com/de-de/azure/active-directory/hybrid/whatis-hybrid-identity (besucht am 09. 01. 2019) (zitiert auf S. 22).

[MT 18] MT Connect Institute. „MTConnect Standard“. In: (2018). URL: http://www.mtconnect.org/. (zitiert auf S. 27).

[Nay18] D. Naylor. *Building .NET Core 2.x on FreeBSD*. 2018. URL: https://github.com/dotnet/corefx/wiki/Building-.NET-Core--2.x-on-FreeBSD (besucht am 14. 12. 2018) (zitiert auf S. 37).

[NYHR05] C. Neuman, T. Yu, S. Hartman, K. Raeburn. *RFC 4120 - The Kerberos Network Authentication Service (V5)*. Techn. Ber. Juli 2005. DOI: 10.17487/rfc4120. URL: https://www.rfc-editor.org/info/rfc4120 (zitiert auf S. 49).

[OPC16] OPC Foundation. *Build OPC UA .NET applications using .NET StandardLibrary*. 2016. URL: http://opcfoundation.github.io/UA-.NETStandard/ (zitiert auf S. 36, 37).

[OPC18] OPC Foundation. *IoT*. Techn. Ber. June. OPC Foundation, 2018, S. 1–48. URL: https://opcfoundation.org/wp-content/uploads/2017/11/OPC-UA-Interoperability-For-Industrie4-and-IoT-DE.pdf (zitiert auf S. 36).

[Ope13a] OpenLDAP Foundation. *Are "packaged"releases of OpenLDAP Software available?* 2013. URL: http://www.openldap.org/faq/data/cache/108.html (besucht am 01. 09. 2018) (zitiert auf S. 20, 21, 33).

[Ope13b] OpenLDAP Foundation. *What LDAPv3 features/extensions are NOT supported by the OpenLDAP server?* 2013. URL: https://www.openldap.org/faq/data/cache/649.html (besucht am 14. 12. 2018) (zitiert auf S. 33).

[Ope13c] OpenLDAP Foundation. *What LDAPv3 features/extensions are supported by the OpenLDAP server?* 2013. URL: https://www.openldap.org/faq/data/cache/645.html (besucht am 14. 12. 2018) (zitiert auf S. 33).

[Ope16] Open62541authors. *Tutorials*. 2016. URL: https://open62541.org/doc/0.2/tutorials.html (besucht am 20. 12. 2018) (zitiert auf S. 46).

[Pet17] Peter. *Windows 10 Adoption: Who's using it two years after launch?* 2017. URL: https://community.spiceworks.com/networking/articles/2719-windows-10-adoption-who-s-using-it-two-years-after-launch (besucht am 13. 12. 2018) (zitiert auf S. 29, 34, 38).

[Pkg13] Pkgs.org. *avahi-0.6.31-19.el7.x86_64.rpm*. 2013. URL: https://centos.pkgs.org/7/centos-x86%7B%5C_%7D64/avahi-0.6.31-19.el7.x86%7B%5C_%7D64.rpm.html (besucht am 14. 12. 2018) (zitiert auf S. 41).

[PL10] L. Poettering, T. Lloyd. *Welcome to Avahi*. 2010. URL: https://www.avahi.org/ (besucht am 14. 12. 2018) (zitiert auf S. 25, 41).

[Pla] Plattform Industrie 4.0. *Normen & Standards*. URL: https://www.plattform-i40.de/I40/Navigation/DE/Industrie40/Handlungsfelder/NormenStandards/normen-und-standards.html (besucht am 14. 01. 2019) (zitiert auf S. 26).

[Pro18] Prosody.im. *XMPP*. 2018. URL: https://prosody.im/doc/xmpp (besucht am 06. 12. 2018) (zitiert auf S. 24).

[Red] RedHat. *CHAPTER 1. WAYS TO INTEGRATE ACTIVE DIRECTORY AND LINUX ENVIRONMENTS*. URL: https://access.redhat.com/documentation/en-us/red%7B%5C_%7Dhat%7B%5C_%7Denterprise%7B%5C_%7Dlinux/7/html/windows%7B%5C_%7Dintegration%7B%5C_%7Dguide/introduction (zitiert auf S. 44).

[Red19] RedHat. *Red Hat Directory Serer*. 2019. URL: https://www.redhat.com/de/technologies/cloud-computing/directory-server (besucht am 09. 01. 2019) (zitiert auf S. 19).

[Reg18] M. Regen. *UA .Net Standard Global Discovery Server and Client*. 2018. URL: https://github.com/OPCFoundation/UA-.NETStandard/blob/master/SampleApplications/Samples/GDS/ (besucht am 14. 12. 2018) (zitiert auf S. 37).

[RWRS00] C. Rigney, S. Willens, A. Rubens, W. Simpson. „RFC 2865 - Remote Authentication Dial In User Service (RADIUS)“. In: *Request for Comments* (2000) (zitiert auf S. 49).

[Sai11] P. Saint-andre. „RFC:6120 Extensible Messaging and Presence Protocol (XMPP): Core“. In: *Request for Comments* (2011). DOI: 10.17487/rfc6120 (zitiert auf S. 24, 25).

[Sai15] P. Saint-andre. „RFC:7590 Use of Transport Layer Security (TLS) in the Extensible Messaging and Presence Protocol (XMPP)“. In: *Request for Comments* (2015). DOI: 10.17487/rfc7590 (zitiert auf S. 24).

[Sai18] P. Saint-andre. „XEP-0045 : Multi-User Chat“. In: *XMPP Standards Foundation* (2018) (zitiert auf S. 24).

[Sch16a] P. Schnabel. *DNS - Domain Name System*. 2016. URL: https://www.elektronik-kompendium.de/sites/net/0901141.htm (besucht am 10. 01. 2019) (zitiert auf S. 22).

[Sch16b] P. Schnabel. *Verzeichnisdienste (X.500)*. 2016. URL: https://www.elektronik-kompendium.de/sites/net/0905011.htm (besucht am 01. 12. 2018) (zitiert auf S. 14, 18).

[Ser06] J. Sermersheim. „RFC 4511: Lightweight Directory Access Protocol (LDAP): The Protocol“. In: *Request for Comments* (2006) (zitiert auf S. 33).

[Sta17] Statistisches Bundesamt. *IT-Nutzung*. 2017. URL: https://www.destatis.de/DE/ZahlenFakten/GesellschaftStaat/EinkommenKonsumLebensbedingungen/ITNutzung/Tabellen/ZeitvergleichComputernutzung%7B%5C_%7DIKT.html (besucht am 28. 07. 2018) (zitiert auf S. 13).

[Ste10] M. Steinkamp. „Konzeption und Erstellung eines IT-Grundschutz-Bausteins für den Verzeichnisdienst OpenLDAP“. Master Thesis. 2010, S. 246. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Extern/Diplomarbeiten/OpenLDAP%7B%5C_%7DSteinkamp.pdf?%7B%5C_%7D%7B%5C_%7Dblob=publicationFile%7B%5C&%7Dv=1 (zitiert auf S. 19).

[Ste15] Steff. *Facebook schaltet XMPP API ab!* 2015. URL: https://www.jabber.de/facebook-schaltet-xmpp-api-ab/ (besucht am 06. 12. 2018) (zitiert auf S. 24).

[Tim18] A. Timin. *List of Open Source OPC UA Implementations*. 2018. URL: https://github.com/open62541/open62541.wiki.git (besucht am 19. 12. 2018) (zitiert auf S. 45).

[Voi18] P. D. K.-I. Voigt. *Produktion*. 2018. URL: https://wirtschaftslexikon.gabler.de/definition/produktion-42040/version-265395 (besucht am 08. 01. 2018) (zitiert auf S. 15).

[W3C18] W3CTech. *Usage of operating systems for websites*. Techn. Ber. 2018. URL: https://w3techs.com/technologies/overview/operating%7B%5C_%7Dsystem/all (zitiert auf S. 33, 34, 38).

[Wik] Wikipedia. *No Title*. URL: https://de.wikipedia.org/wiki/Thomas%7B%5C_%7DJ.%7B%5C_%7DWatson%7B%5C#%7Dcite%7B%5C_%7Dref-1 (besucht am 30. 08. 2018) (zitiert auf S. 13).

[WL17] P. Waher, J. Lindborg. *Tech pages/IoT systems*. 2017. URL: https://wiki.xmpp.org/web/Tech%7B%5C_%7Dpages/IoT%7B%5C_%7Dsystems (besucht am 09. 12. 2018) (zitiert auf S. 25).

[WLT+18] P. Waher, G. Lukas, M. Taylor, J. Schäfer, A. Brault, T. True. *Internet of Things (IoT)*. 2018. URL: https://xmpp.org/uses/internet-of-things.html (besucht am 09. 12. 2018) (zitiert auf S. 25).

[Zei06] K. Zeilenga. *RFC 4510*. 2006. URL: https://tools.ietf.org/html/rfc4510 (zitiert auf S. 18).

[Zyt17] Zytrax. *Appendix E: LDAP - Object Classes and Attributes*. 2017. URL: http://www.zytrax.com/books/ldap/ape/ (zitiert auf S. 20, 21).

A. Technologieübersicht

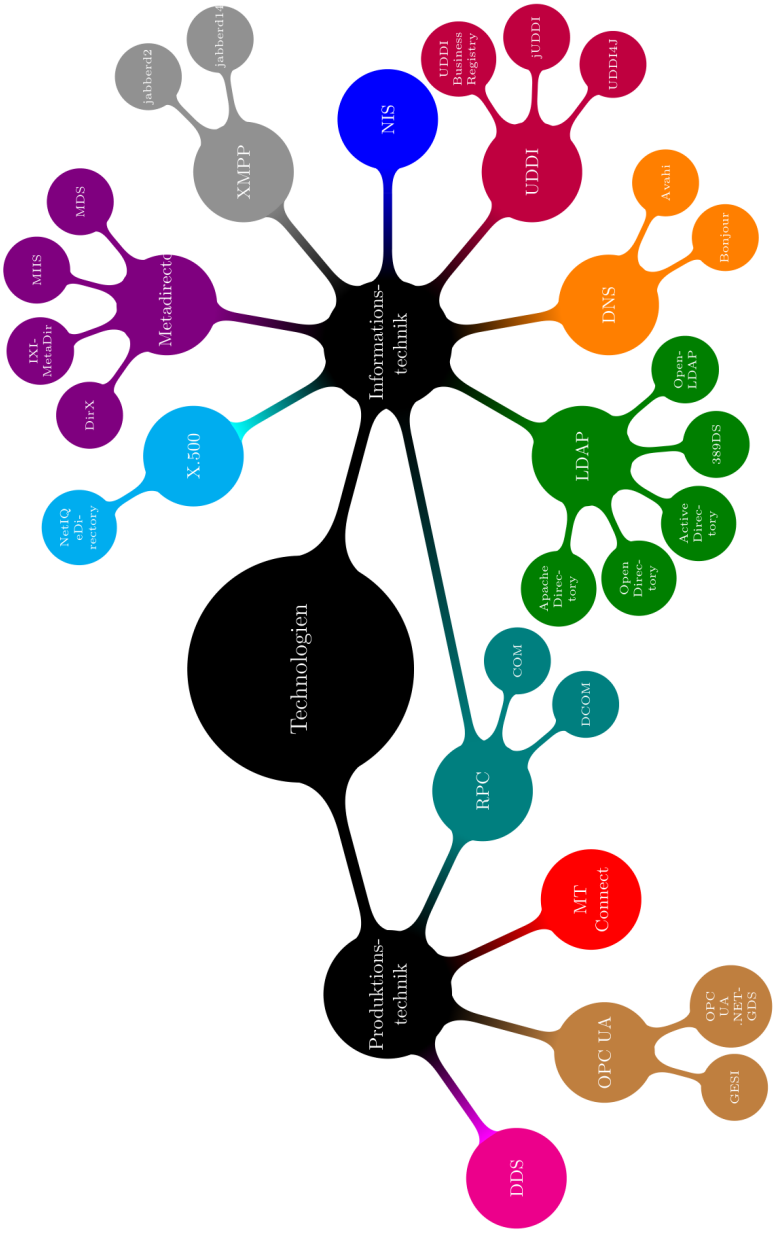

Abbildung A.1.: Übersicht über alle betrachteten Technologien

B. CVE-Bewertungen

B.1. Active Directory

Suchbegriff	CVE-Nummer	Bewertung
Microsoft Active Directory	2013-1282	5
	2013-3868	5
	2013-1282	5
	2009-2928	7,8
	2001-2014	9
	2005-0545	7,2
	2010-0654	10
	2018-1679	5
	2015-1757	4,3
	2014-6331	5
	2013-1438	5
	2013-3185	5
	2011-1264	4,3
	2007-0040	10
	2003-0533	7,5
	2009-1138	10

	2009-2508	6,9
	2009-2509	9
	2015-2535	4
	2008-1445	7,1
	2007-3038	5
	2011-0040	5
	2015-1638	5,8
	2014-3185	5
	2011-3406	9
	2018-8340	4
	2018-0890	3,5
	2009-1928	7,8
	2011-2014	9
	2010-0820	9
	2016-3226	4
	2016-0037	5
	2003-0507	7,5
	2008-0088	6,8
	2017-0043	2,9
	2002-2328	7,1
	2008-5112	5
	2008-4023	10
	2017-0164	3,5
	2018-8326	3,5
Active Directory Application Mode	2009-1139	7,8
Durchschnitt		6,3

Es werden hier nur zwei Suchbegriffe aufgeführt da, Suchen mit den weitern Suchbegriffen lediglich zum Fund der bereits aufgeführten Sicherheitslücken führte. Die überprüften Begriffe waren: Microsoft Active Directory, Active Directory, Active Directory Application Mode, Active Directory Lightweight Directory Service und Active Directory Services.

B.2. Distributed COM

Suchbegriff	CVE-Nummer	Bewertung
Suchbegriff CVE Nummer Score DCOM	2003-0352 7,5	
	2017-0298	4,4
	2003-0715	10
	2004-0124	2,6
	2003-0605	7,5
	2017-0100	4,4
	2003-0813	5,1
	2002-2077	5
	2004-0116	5
	2003-0528	10
Component Object Model	2007-0940	9,3
	2007-5653	9,3
	2002-1257	10
Durchschnitt		6,15

B.3. Bonjour

Suchbegriff	CVE-Nummer	Bewertung
Bonjour	2008-3630	6,4
	2008-2326	5
	2008-2326	5
Durchschnitt		5,5

B.4. Jabberd2

Suchbegriff	CVE	Bewertung
jabberd2	2011-1755	5
	2017-18226	2,1
	2017-18225	4,6
	2017-10807	7,5
	2015-2058	6,5
	2012-3525	5,8
Durchschnitt		5,25

Erklärung

Ich versichere, diese Arbeit selbstständig verfasst zu haben. Ich habe keine anderen als die angegebenen Quellen benutzt und alle wörtlich oder sinngemäß aus anderen Werken übernommene Aussagen als solche gekennzeichnet. Weder diese Arbeit noch wesentliche Teile daraus waren bisher Gegenstand eines anderen Prüfungsverfahrens. Ich habe diese Arbeit bisher weder teilweise noch vollständig veröffentlicht. Das elektronische Exemplar stimmt mit allen eingereichten Exemplaren überein.

Ort, Datum, Unterschrift