PLATTFORM INDUSTRIE4.0

DISKUSSIONSPAPIER

Sichere unternehmensübergreifende Kommunikation mit OPC UA

Impressum

Herausgeber
Bundesministerium für Wirtschaft und Energie (BMWi)
Öffentlichkeitsarbeit
11019 Berlin
www.bmwi.de

Redaktionelle Verantwortung
Plattform Industrie 4.0
Bertolt-Brecht-Platz 3
10117 Berlin

Gestaltung und Produktion
PRpetuum GmbH, München

Stand
März 2019

Bildnachweis
Getty Images – gvinpin (Titel)
Getty Images – Busakorn Pongparnit (S. 3)
Getty Images – Andriy Onufriyenko (S. 5)
Getty Images – skynesher (S. 7)
Getty Images – Fertnig (S. 11)
Getty Images – Bloom Productions (S. 22)

Diese Broschüre ist Teil der Öffentlichkeitsarbeit des Bundesministeriums für Wirtschaft und Energie. Sie wird kostenlos abgegeben und ist nicht zum Verkauf bestimmt. Nicht zulässig ist die Verteilung auf Wahlveranstaltungen und an Informationsständen der Parteien sowie das Einlegen, Aufdrucken oder Aufkleben von Informationen oder Werbemitteln.

Diese und weitere Broschüren erhalten Sie bei:
Bundesministerium für Wirtschaft und Energie
Referat Öffentlichkeitsarbeit
E-Mail: publikationen@bundesregierung.de
www.bmwi.de

Zentraler Bestellservice:
Telefon: 030 182722721
Bestellfax: 030 18102722721

Inhalt

1 Einleitung 3
1.1 Inhalt und Ziel dieses Diskussionspapiers 3
1.2 Einordnung im Lebenszyklus/RAMI4.0 4
1.3 Die Bedeutung von OPC UA 4

2 Security 5
2.1 Risikobasierter Ansatz 5
2.2 Sicherheit in der Kommunikation 6
2.3 Beteiligte Interessengruppen 6

3 Anwendungsszenario „Condition Monitoring und Parametrierung“ 7
3.1 Akteur: Betreiber 8
3.2 Akteur: Dienstleister 9
3.3 Anforderungen an die Lösungsansätze 10

4 Lösungsansätze 11
4.1 Lösungsansatz: Direkte Verbindung 12
4.1.1 Variante A: Client to Server 12
4.1.2 Variante B: Reverse-Connect 14
4.1.3 Ablauf/Voraussetzungen 15
4.1.4 Bewertung 15
4.2 Lösungsansatz: Aggregating Server 16
4.2.1 Szenario A: Der Betreiber stellt und verwaltet einen Aggregating Server 18
4.2.2 Szenario B: Die Dienstleister stellen eigene Aggregating Server beim Betreiber auf 19
4.2.3 Bewertung und Vergleich der Szenarien 20
4.3 Vergleich der Lösungsansätze 21

5 Zusammenfassung und Ausblick 22

6 Anhang 23
6.1 Glossar 23
6.2 Abbildungsverzeichnis 23
6.3 Literaturverzeichnis 24

Autoren 25

1 Einleitung

Industrie 4.0 schafft mit innovativen Konzepten und Vorgehensweisen völlig neue Möglichkeiten in der Zusammenarbeit – insbesondere auch auf technischer Ebene. Menschen, Maschinen und Produkte interagieren, tauschen Daten und Informationen aus und korrespondieren stets. Dabei spielt es keine Rolle, ob mit einer Maschine in derselben Fabrikhalle oder mit einer Anlage in einem Betrieb auf der anderen Seite der Welt kommuniziert wird und damit Vertrauensgrenzen überschritten werden. Doch das funktioniert nur, wenn technische Kommunikationsmechanismen dafür sorgen, dass Industrie 4.0-Komponenten (Assets) sicher und interoperabel in Kontakt treten können (1) und so Vertrauen über Unternehmensgrenzen hinweg ermöglichen.

1.1 Inhalt und Ziel dieses Diskussionspapiers

Ziel des vorliegenden Diskussionspapiers ist es, die Anforderungen an die sichere Verwendung von OPC UA zur Kommunikation in Industrie 4.0-Szenarien herauszustellen, Umsetzungsmöglichkeiten vorzustellen und Diskussionspunkte zu identifizieren. Im Diskussionspapier „Sichere Implementierung von OPC UA für Betreiber, Integratoren und Hersteller“ (2) wurde beispielhaft die Einbindung einer Maschine in die Infrastruktur eines Betreibers über den Lebenszyklus betrachtet. In diesem Diskussionspapier wird die unternehmensübergreifende Verwendung anhand eines beispielhaften Anwendungsszenarios adressiert. Durch die Beteiligung mehrerer Unternehmen ist es notwendig, die Security-Anforderungen der verschiedenen Stakeholder in Einklang zu bringen, wie im technischen Überblick „Sichere unternehmensübergreifende Kommunikation“ (3) beschrieben.

Ziel ist es, den beteiligten Stakeholdern – Betreiber und Dienstleister – konkrete Hinweise auf notwendige Funktionen und Maßnahmen zu geben und Best Practices zu beschreiben. Gleichzeitig soll die Betrachtung zeigen, inwieweit sich mit der Umsetzung der Security-Maßnahmen noch weitergehende Anforderungen ergeben, welche Ergänzungen im OPC UA-Standard oder in vorhandenen Toolkits und Produkten erfordern. Durch diesen Ansatz wird die Durchgängigkeit und Interoperabilität verbessert.

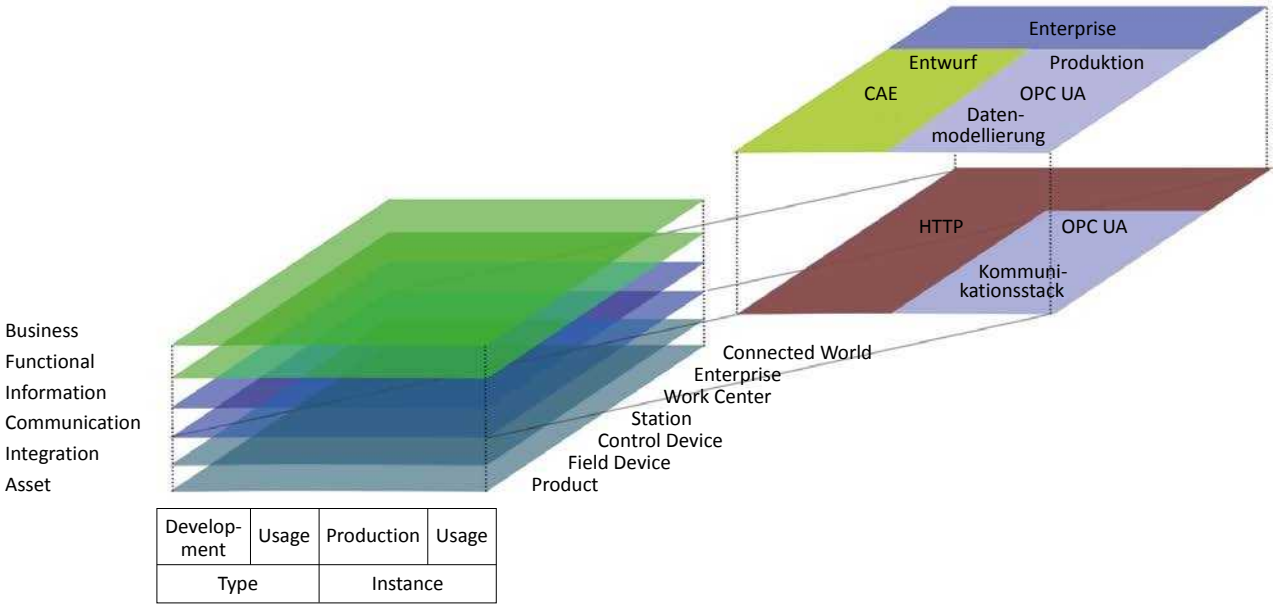
Dieses Papier basiert auf dem OPC UA-Standard in der Version 1.04[1], der insbesondere im Bereich der Security deutliche Weiterentwicklungen bietet. Es ist allerdings davon auszugehen, dass im Markt verfügbare Implementierungen und Entwicklungswerkzeuge noch nicht auf diesem Stand sind. Ein Ziel dieses Papiers ist es, die Anbieter und Anwender bei der Transition zu unterstützen.

Die betrachteten Lösungsansätze beziehen sich auf das Client-Server-Modell von OPC UA. Alternative Lösungsansätze könnten mit dem Publish-Subscribe-Modell (PubSub) umgesetzt werden. Das PubSub-Konzept wird in einer Folgeveröffentlichung betrachtet werden. Eine abschließende Bewertung der besten Umsetzungsvariante aus Sicht der Security-Anforderungen kann erst am Ende dieser weiteren Betrachtungen vorgenommen werden.

Das Papier richtet sich an den technisch fundierten Leser, ideal mit Kenntnissen über die Anwendung von OPC UA.

1 https://opcfoundation.org/developer-tools/specifications-unified-architecture

Abbildung 1: Exemplarische Betrachtung von Kommunikationsbeziehungen auf der Kommunikations- und Informationsschicht im RAMI4.0



1.2 Einordnung im Lebenszyklus/RAMI4.0

Abbildung 1 zeigt die drei Bereiche Engineering/Entwurf, Produktion und Enterprise im RAMI4.0, deren Anforderungen an die Kommunikation sich deutlich unterscheiden. In der Konsequenz ist abzusehen, dass entsprechend unterschiedliche technische Lösungen und Protokolle zum Einsatz kommen werden:

- Im Produktionsumfeld kommunizieren einzelne Geräte und Systeme (Instanzen) miteinander. Die Systeme im Produktionsumfeld sind für die Betreiber zumeist Mission Critical und tauschen prozessbezogene Daten aus. Die Plattform Industrie 4.0 erwartet und unterstützt, dass hier OPC UA als Architektur mit den zugehörigen Kommunikationsprotokollen zum Einsatz kommt.

- Im Bereich der Enterprise-Kommunikation und übergreifender Wertschöpfungsnetzwerke sind andere Anforderungen an die unterschiedlichen informationstechnischen Schutzziele zu erfüllen.

- Im Bereich des Engineerings, also der Behandlung von Typen, sind wiederum andere Anforderungen zu erfüllen. Datensätze können hier sehr detailliert und groß sein. Je nach Vorgang sind die Entwurfs- und Entwicklungsvorgänge auch längerfristig angelegt.

Das in diesem Papier beschriebene Anwendungsszenario „Condition Monitoring und Parametrierung“ bezieht sich auf den Einsatzbereich im Produktionsumfeld und wird deswegen mittels OPC UA umgesetzt.

1.3 Die Bedeutung von OPC UA

OPC UA (OPC[2] Unified Architecture) ist eine Architektur zur Beschreibung und zum Austausch von Maschinendaten. Insofern ist OPC UA mehr als nur ein Kommunikationsprotokoll – die Architektur umfasst auch Datenmodelle und Interaktionskonzepte. In der Automatisierungstechnik kommt OPC seit längerer Zeit erfolgreich zur Anwendung. Die Weiterentwicklung OPC UA wird heute von einer breiten Basis unterstützt und wurde in der Umsetzungsstrategie der Plattform Industrie 4.0 (4) als eine wichtige Technologie empfohlen und ist Bestandteil der „Kriterien für Industrie 4.0-Produkte“ des ZVEI (5).

2 OPC: Ursprünglich „OLE for Process Control“, heute „Open Platform Communications“.

2 Security

Maßnahmen zur Informationssicherheit dienen dazu, Unternehmenswerte zu schützen und gesetzliche Vorgaben einzuhalten. Die wesentlichen Schutzziele sind dabei:

- Vertraulichkeit
- Integrität
- Verfügbarkeit

Weitere Schutzziele werden ergänzend oder unterstützend verwendet:

- Authentizität
- Verbindlichkeit
- Nichtabstreitbarkeit

Verfügbarkeit ist zumeist ein statistischer Wert für Ausfall oder Wiederherstellung, zum Beispiel eine Stunde pro Jahr.

Im Bereich der Produktion wird zusätzlich der Begriff der Zuverlässigkeit verwendet: Zuverlässigkeit betrachtet die Freiheit von Störungen. In einem physikalischen Prozess kann auch eine einzelne Störung von zehn Sekunden relevante Auswirkungen haben, die im statistischen Mittel nicht bewertbar wäre.

2.1 Risikobasierter Ansatz

Für die Ermittlung der zu erfüllenden Schutzziele bzw. der daraus abzuleitenden Maßnahmen müssen die Unternehmenswerte ermittelt und die auf sie einwirkenden Bedrohungen beschrieben werden. Darauf basierend können Gefährdungen und Risiken ermittelt und bewertet werden. Dabei ist eine besondere Herausforderung, dass das Risiko aus dem maximalen Schaden und der Eintrittswahrscheinlichkeit berechnet wird. Die Eintrittswahrscheinlichkeit ist aber aufgrund sich stetig ändernder Gefährdungen nur schwer greifbar. Einflussgrößen sind hierbei die Motivation von Angreifern ebenso wie das Bekanntwerden von Sicherheitslücken, die sich nicht in klassischen Konzepten des Risikomanagements abbilden lassen:

- In der im Unternehmensumfeld üblicherweise angewendeten ISO 27001 (6) verwendet man daher eine Klassifizierung der Schutzanforderungen (z. B. öffentlich, intern, vertraulich, streng vertraulich) als Unterstützung bei der Risikobewertung und der Aufstellung des Maßnahmenkatalogs.
- Die für die Automatisierung erarbeitete Normenreihe IEC 62443 (7) verwendet zusätzlich ein Angreifermodell, um darauf basierend Security-Level für Automatisierungssysteme und Komponenten anzugeben.

2.2 Sicherheit in der Kommunikation

Im Fall einer unternehmensübergreifenden Kooperation zwischen Dienstleistern und dem Unternehmen werden im betrachteten Fall Prozessdaten und Parametrierung ausgetauscht. Die Dienstleister betreiben dabei IT-Systeme, die auch in einer Cloud angesiedelt sein können. Die Systematik der Dienstleister sollte sich entsprechend an der ISO 27001 (6) orientieren. Eine spezielle Ausprägung für den sicheren Betrieb von Cloud-Diensten ist die ISO 27017 (8). Auf Betreiberseite sind Produktionssysteme involviert, sodass ein Informationssicherheitsmanagementsystem auf Basis der IEC 62443 (7) zugrunde gelegt werden sollte.

Das Vorgehen in der Security befasst sich in vielen Bereichen mit der Prävention von Security-Vorfällen durch geeignete Maßnahmen. Ein 100-%-Schutz ist jedoch nicht möglich, sodass in den entsprechenden Normen (sowohl ISO 27001 als auch IEC 62443 und anderen) immer auch die Bereiche Detektion (Erkennung von Angriffen) und Reaktion (Gegenmaßnahmen) adressiert sind.

Insbesondere bei der unternehmensübergreifenden Kommunikation von Prozessparametern sowie einer unternehmensübergreifenden Parametrierung von Anlagen(-teilen) stellen sich verschiedene Herausforderungen für die Wahrung der drei essenziellen Security-Ziele Vertraulichkeit, Integrität und Verfügbarkeit sowie der darauf basierenden Ziele Authentizität, Verbindlichkeit und Nichtabstreitbarkeit. Daher ist bei der Gestaltung der Kommunikation darauf zu achten, dass mögliche Angriffe bereits strukturell verhindert werden. Ebenso müssen Sicherheitsanforderungen, wie sie sich aus den oben genannten Sicherheitsnormen ergeben (z. B. das Prinzip der Zonen und Conduits), auch in der unternehmensübergreifenden Kommunikation abbildbar sein. Dieses Papier geht daher auf verschiedene Möglichkeiten der Kommunikation ein, welche jeweils Vor- und Nachteile für die Erreichung dieser Sicherheitsziele aufweisen.

2.3 Beteiligte Interessengruppen

Die Informationssicherheit betrachtet immer einen Stakeholder und seine Unternehmenswerte, die entsprechend seinen relevanten Schutzzielen und seiner Risikobewertung behandelt werden. Werden die Interessen verschiedener Stakeholder berührt, können daher unterschiedliche Bewertungen des gleichen Risikos auftreten. Um dies auszugleichen, sind Vereinbarungen zwischen den Stakeholdern notwendig (Vertraulichkeitsvereinbarungen, Service Level Agreements, Lieferantenmanagement), da Risiken sonst nicht ausgeglichen bewertet und berücksichtigt werden können. Diese Aushandlung entsprechender Verträge ist essenzieller Bestandteil einschlägiger Standards und wird z. B. in der ISO 27036 „Information security for supplier relationships“ (9) beschrieben. In diesem Papier wird grundsätzlich zwischen zwei Stakeholdern unterschieden:

a) Ein Betreiber betreibt eine Maschine oder Anlage. Es wird davon ausgegangen, dass der Betreiber mehrere Anlagen oder Maschinen betreibt.

b) Ein Dienstleister, welcher für den Betreiber Aufgaben, wie die Überwachung von Parametern oder die Parametrierung von einzelnen Anlagen bzw. Anlagenteilen, übernimmt. Es wird davon ausgegangen, dass der Dienstleister nur begrenzten Zugriff auf die Infrastruktur des Betreibers hat und nicht den Betrieb der Anlagen des Betreibers in seiner Gänze betreut.

Die im Folgenden diskutierten Maßnahmen zielen darauf ab, das Risiko für den Betreiber durch

a) ein Fehlverhalten des Dienstleisters

oder

b) Angriffe durch Dritte zu reduzieren.

Ebenso werden die Interessen des Dienstleisters betrachtet, wenn es um den Schutz seiner eigenen Firmengeheimnisse bzw. um den Schutz der vom Dienstleister bereitgestellten Infrastruktur geht.

Es wird davon ausgegangen, dass das Netzwerk des Betreibers und das Netzwerk des Dienstleisters bzw. der Dienstleister unterschiedliche Sicherheitsdomänen darstellen. Eine Sicherheitsdomäne ist ein technologisch, organisatorisch oder räumlich zusammengehöriger Bereich mit einheitlichen Sicherheitsanforderungen und/oder einheitlicher Sicherheitsadministration. In vielen Unternehmen sind heute zumindest Bürobereich/IT und Produktionsbereich jeweils eigene Sicherheitsdomänen. Beim Übergang von Informationen über die Grenzen der Sicherheitsdomänen hinweg ist spezielle Vorsicht geboten, um die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Prozessen aufrechtzuerhalten.

3 Anwendungsszenario „Condition Monitoring und Parametrierung“

Ein Betreiber hat verschiedene Maschinen in einer oder mehreren Anlagen im Einsatz. Diese Maschinen und Anlagen lassen sich sowohl funktional als auch aus Sicherheitsgesichtspunkten in verschiedene Gruppen gliedern. Diese Gliederung wird in der Regel als Zone bezeichnet. Die Geräte innerhalb einer Zone können dabei ohne größere Einschränkung miteinander kommunizieren, während die Kommunikation über Zonengrenzen hinweg klar definiert und reglementiert werden muss. Praxisübliche Möglichkeiten, Zonen zu bilden, sind die Trennung eines Netzwerks in verschiedene Teilnetze bzw. die Zuweisung von Geräten zu verschiedenen Virtual LANs (VLANs). Die Übergänge (so genannte Conduits) zwischen den Zonen werden meist durch konfigurierbare Paketfilter wie z. B. Firewalls realisiert. Es wird im Folgenden davon ausgegangen, dass ein Betreiber sein Netzwerk in unterschiedliche Zonen gegliedert hat und dass bei der Kommunikation zu einem Gerät in einer Zone eine oder mehrere Firewalls durchschritten werden müssen. Auf die Maschinen innerhalb der Zonen haben in diesem Szenario ein oder mehrere Dienstleister Zugriff.

Der Dienstleister bietet dem Betreiber die Leistungen „Condition Monitoring“ und „Parametrieren der Maschine“ an (siehe Abbildung 2). Mit diesen Dienstleistungen soll die Effektivität und/oder Effizienz der Betreiberproduktion gesteigert werden, indem beispielsweise Verschleiß an den Werkzeugen reduziert oder der Ausfall der Maschine vermieden wird.

Der Dienstleister benötigt für das Condition Monitoring kontinuierlichen Lesezugriff auf die Prozessdaten. Für die gelegentliche Parametrierung benötigt der Dienstleister gelegentlichen Schreibzugriff, um Parameter der Maschine anzupassen.

Für das Condition Monitoring sind typische Qualitäts- und Produktivitätsdaten relevant. Dazu zählen zum Beispiel:

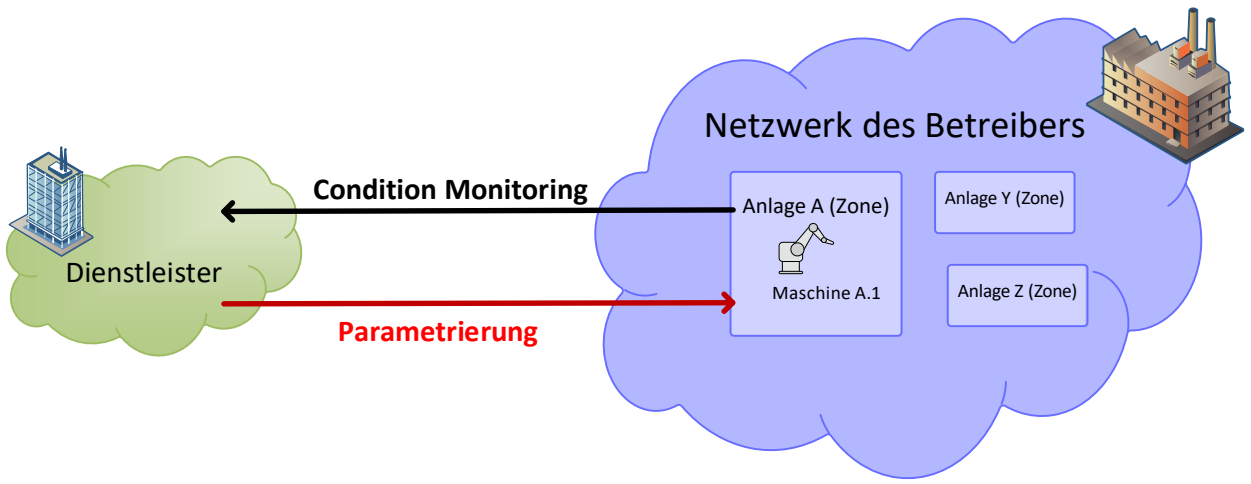
a) Daten aus dem Prozess wie Temperaturen, Drehzahlen, Drehmomente etc.

b) Daten zum Prozessergebnis wie Maßhaltigkeit, Stückzahlen etc.

Für die Parametrierung sind Konfigurationen, Kennlinien und Sollwerte relevant. Die veränderlichen Parameter sind zuvor vertraglich festzulegen.

Im Folgenden werden die Security-Anforderungen an die Kommunikation aus Sicht der beiden Akteure Betreiber und Dienstleister beschrieben.

Abbildung 2: Anwendungsszenario „Condition Monitoring und Parametrierung“



3.1 Akteur: Betreiber

Der Betreiber ist verantwortlich für den Betrieb der Maschine. Für den Betreiber bestehen in dem Szenario die in der Tabelle 1 aufgeführten Bedrohungen bei entsprechender krimineller Energie eines Angreifers. Als Angreifer gesehen werden können auch Innentäter, die beim Dienstleister beschäftigt sind. Auch ein Verhalten des Dienstleisters, das den vertraglichen Ansprachen zwischen Betreiber und Dienstleister widerspricht, kann in diesem Sinne als Angriff gewertet werden.

Grundsätzlich lassen sich weitere Bedrohungen identifizieren, die in diesem Dokument aber nicht betrachtet werden und daher in der Tabelle nicht aufgeführt sind.

Einige der beschriebenen Bedrohungen lassen sich mit den verfügbaren technischen Mitteln von OPC UA adressieren.

Tabelle 1: Betreiber: Anwendungsszenario und Bedrohungen

Anwendungsszenario	Bedrohung
Condition Monitoring	Dienstleister kann unberechtigten Zugriff auf Daten des Betreibers erhalten.
	Externe Angreifer nutzen unbemerkt den Dienstleister, um Zugang zu erlangen.
	Die Daten können (durch fehlerhafte Konfiguration) unverschlüsselt übertragen und so durch unberechtigte Personen ausgespäht werden.
Parametrierung	Die Verfügbarkeit oder Betriebssicherheit der Maschine kann durch eine fehlerhafte, unberechtigte, manipulierte oder willentlich gestörte Parametrierung eingeschränkt/verringert werden.
	In Fehlerfällen und bei Problemen ist es für den Betreiber zum Auffinden der Ursache wichtig, vorausgegangene Änderungen an der Maschine nachvollziehen zu können.
	Aktivitäten bei der Parametrierung können im Nachgang nicht nachvollziehbar sein.

So wird durch die OPC UA-Security-Policies (mit Ausnahme der Security-Policy “None”) sichergestellt, das Hash- bzw. Verschlüsselungs-Algorithmen in der Kommunikation zum Einsatz kommen. Dabei ist zu berücksichtigen, dass der Stand der Technik sich fortentwickelt und somit neue Algorithmen hinzukommen und alte Algorithmen nicht länger verwendet werden sollten. Dies wird im Standard durch die Ergänzung und Abkündigung von Policies abgebildet.

Bei den in der Maschine gespeicherten Daten kann es sich z. B. um Auslastungsinformationen der Maschine oder spezifisches Wissen des Betreibers handeln. Es ist zudem möglich, dass es sich um personenbezogene Daten handelt, die dem Datenschutz unterliegen. Unter Umständen dürfen Daten gar nicht übertragen werden oder es sind zusätzliche vertragliche Regelungen notwendig.

Risiken bei der Parametrierung entstehen durch fehlerhafte oder manipulierte Daten. Diese können beispielsweise von einer unberechtigten Person oder einem unberechtigten System an die Maschine übertragen werden. Die erneute Übermittlung von Daten, die bei der Übertragung verfälscht wurden, wird durch die unterlagerten Protokolle sichergestellt. Die Verwendung des OPC UA-Modus „Sign“ (und auch „Sign and Encrypt“) fügt der Übertragung eine weitere Sicherheitsschicht hinzu, die neben zufällig entstandenen Fehlern auch absichtliche Manipulation zuverlässig ausschließt.

Da der Betreiber für die Maschine verantwortlich ist, muss er die Kontrolle über die Maschine besitzen und den Betriebszustand der Maschine kennen. Dies ist eng verbunden mit der Betriebssicherheit.

Für die Parametrierung durch den Dienstleister ist es daher unerlässlich, dass klare Regelungen getroffen werden. Betreiber und Dienstleister müssen explizit abstimmen, welche Parameter verändert werden dürfen. Zusätzlich muss je nach Umfang der Parametrierung deren Rückwirkung auf die Security der Anlage berücksichtigt werden.

Kommt es zu einem Vorfall, ist die Nachvollziehbarkeit von vorangegangenen Operationen wichtig, um gegebenenfalls die Ursachen feststellen zu können.

3.2 Akteur: Dienstleister

Für den Dienstleister bestehen in dem Szenario die in der Tabelle 2 aufgeführten Bedrohungen bei entsprechender krimineller Energie eines Angreifers. Wie auch beim Betreiber kommen hier sowohl Innentäter als auch externe Angreifer in Betracht. Ebenso ist ein Verhalten des Dienstleisters, das den vertraglichen Vereinbarungen widerspricht, als Angriff (auf die Vertraulichkeit und/oder Integrität der Daten oder die Verfügbarkeit der Maschine) zu werten.

Auch für den Dienstleister lassen sich weitere Bedrohungsszenarios identifizieren, die in diesem Dokument aber nicht betrachtet werden und daher in der Tabelle nicht aufgeführt sind.

Die übertragenen Condition-Monitoring-Daten sind für den Dienstleister gegebenenfalls Grundlage seiner Tätigkeit und stellen damit einen der zentralen Werte für dessen Geschäftsbetrieb dar. Daher müssen die Vertraulichkeit und insbesondere die Integrität der übertragenen Daten gewährleistet sein. Dies gilt sowohl bei der Übermittlung als

Tabelle 2: Dienstleister: Anwendungsszenario und Bedrohungen

Anwendungsszenario	Bedrohung
Condition Monitoring	Unberechtigter Zugriff oder Manipulation der Condition-Monitoring-Daten durch den Betreiber oder einen Angreifer
	Ausfall der Kommunikation zum Condition Monitoring
Parametrierung	Zugriff auf Parameter durch einen Unberechtigten oder den Betreiber
	Beeinträchtigung der Verfügbarkeit oder Betriebssicherheit der Maschine durch manipulierte Parameter
	Nicht nachvollziehbare Auswirkungen der Parametrierung

auch bei der Verarbeitung und Speicherung der Daten des Condition Monitoring.

Für die Funktion der Parametrierung sind die Folgen von Manipulationen äußerst kritisch. Hier besteht das Risiko, dass die Anlage negativ beeinflusst wird. Dies kann von einem Ausfall bis hin zur Gefährdung der Betriebssicherheit reichen. Die Integrität der Daten ist daher besonders wichtig.

Bei den übertragenen Daten zur Parametrierung kann es sich zudem um schützenwertes Wissen des Dienstleisters handeln, das der Betreiber möglicherweise nicht einsehen soll oder darf. In diesem Fall muss die Vertraulichkeit der Daten gewährleistet sein, um das Geschäftsmodell des Dienstleisters nicht zu gefährden.

Kommt es zu einem Vorfall, ist die Nachweisbarkeit, ob und welche Handlungen vorgenommen wurden, relevant, um gegebenenfalls die Ursachen ermitteln und Folgeschäden vermeiden zu können.

3.3 Anforderungen an die Lösungsansätze

Eine mögliche technische Umsetzung zur Realisierung der oben beschriebenen Kommunikation zwischen Dienstleister und Betreiber muss sowohl funktional als auch aus Sicht der Sicherheit eine tragfähige Lösung darstellen. Dabei müssen die funktionalen Aspekte (Ermöglichung der Kommunikation) sowie die Sicherheitsaspekte (Reduktion des entstehenden Risikos) gegeneinander abgewogen werden. Zusätzlich muss die Komplexität der sich ergebenden Lösung beachtet werden, da durch eine hohe Komplexität Fehler, Sicherheitsprobleme oder Folgekosten (z. B. durch hohe Betriebs- oder Wartungskosten) entstehen können.

Unter folgenden Gesichtspunkten sollte die Lösung akzeptabel sein:

A1) Unternehmensübergreifende Kommunikation ermöglichen: Die Lösung muss zur Schaffung unternehmensübergreifender Kommunikationsbeziehungen geeignet sein. Im Speziellen muss sie dazu geeignet sein, über verschiedene Sicherheitsdomänen hinweg zu kommunizieren. Dies schließt insbesondere eine Lösung zur unternehmensübergreifenden Authentifizierung ein.

A2) Kompatibilität: Die Lösung sollte mit existierenden Best-Practices, Netzwerkstrukturen, Geräten und Softwareprodukten verschiedener Hersteller kompatibel sein. Es sollte ergänzend zu OPC UA nur auf offene und nicht proprietäre Standards zurückgegriffen werden, sodass unterschiedliche Umsetzungen möglich sowie Verfügbarkeit und Wartbarkeit langfristig gegeben sind.

A3) Eignung für verschiedene Netzwerkgrößen und Netzwerktopologien: Die Lösung sollte sowohl für sehr große als auch für kleinste Netzwerke skalierbar sein. Ebenso sollten topologische Eigenschaften wie z. B. eine Segmentierung des Netzwerks in verschiedene Zonen unterstützt, aber nicht erzwungen werden.

A4) Wartbarkeit und Kontrolle: Die Lösung sollte sowohl eine feingranulare Zugriffssteuerung für einzelne Stakeholder und Daten erlauben, gleichzeitig jedoch eine effiziente Konfiguration und Pflege der Regeln für die Zugriffssteuerung ermöglichen. So sollen sowohl Benutzerrechte als auch Firewall-Regeln transparent und effizient zu konfigurieren sein.

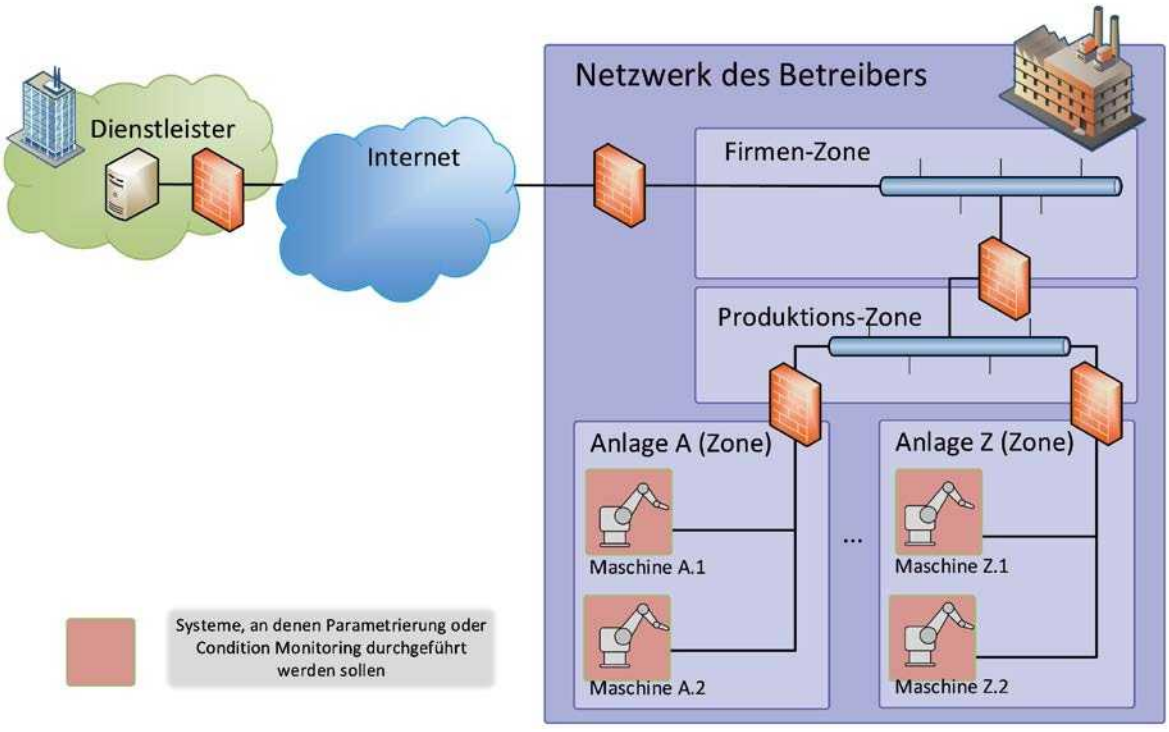
A5) Nachvollziehbarkeit: Zugriffe sowie Veränderungen an den beteiligten technischen Systemen sollten nachvollziehbar sein. Dies bedeutet, dass im Falle eines Zwischenfalls nachvollzogen werden kann, auf welche Daten von wem zugegriffen wurde und welche Parameter durch welchen Teilnehmer verändert wurden.

Weitere funktionale Eigenschaften, wie die erreichbare Leistung (Latenz oder Durchsatz) oder die Echtzeitfähigkeit, können für die Einsetzbarkeit einer Lösung entscheidend sein. Jedoch variieren diese Eigenschaften oftmals aufgrund der eingesetzten Hard- und Software bzw. der eingesetzten Produkte. Diese Eigenschaften sind daher nicht Gegenstand dieses Papiers, da vor allem die unterschiedlichen Lösungen auf Spezifikationsebene des OPC UA-Standards betrachtet werden.

4 Lösungsansätze

Die folgenden Abschnitte beschreiben unterschiedliche Lösungsansätze. Dabei werden Vor- und Nachteile erläutert. Abbildung 3 zeigt, angelehnt an die Netzwerkarchitektur der modularen Fabrik, eine mögliche Umsetzung für das beschriebene Anwendungsszenario. Auf eine detaillierte Abbildung der Infrastruktur aufseiten des Dienstleisters wird an dieser Stelle verzichtet.

Abbildung 3: Anwendungsszenario mit Dienstleister und Betreiber



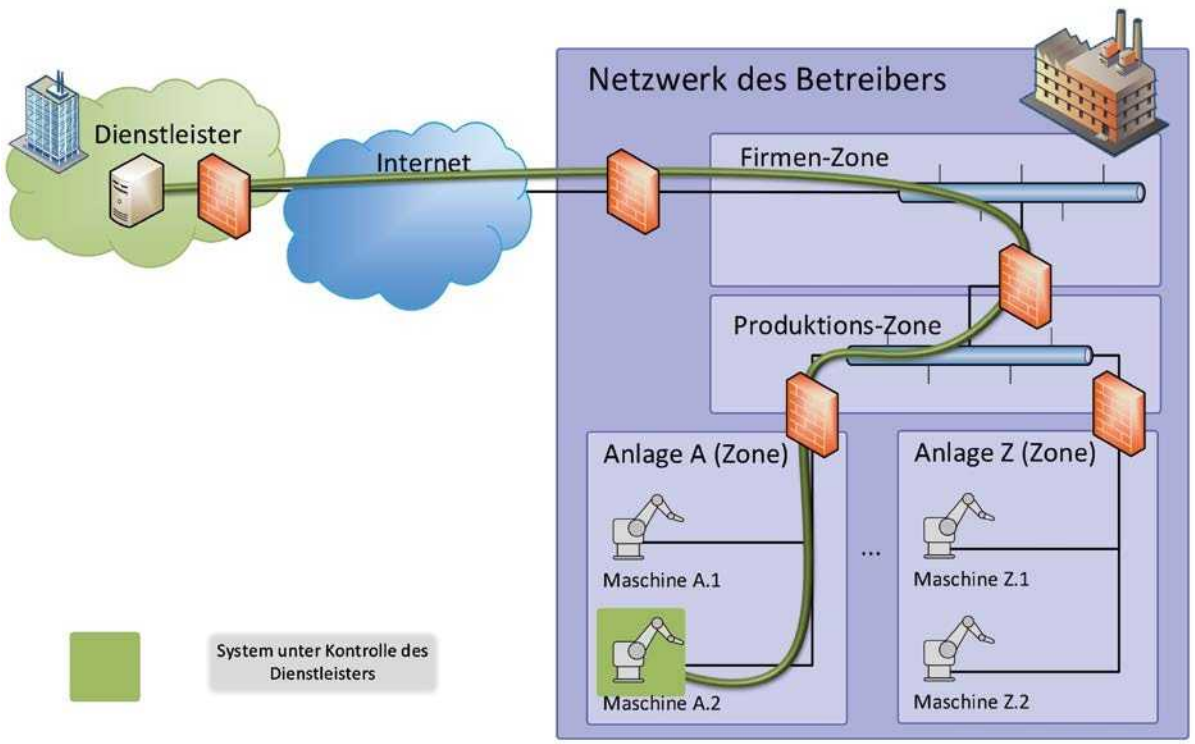
4.1 Lösungsansatz: Direkte Verbindung

Die direkte Verbindung ist die technisch am einfachsten zu realisierende Möglichkeit. Der Ablauf des Verbindungsaufbaus zwischen OPC UA-Client und OPC UA-Server wird für das Condition Monitoring und die Parametrierung gemeinsam beschrieben. Die Kommunikation findet direkt zwischen der Maschine und dem Dienstleister statt, siehe Abbildung 4. Dabei bietet OPC UA zwei Varianten, dies umzusetzen.

4.1.1 Variante A: Client to Server

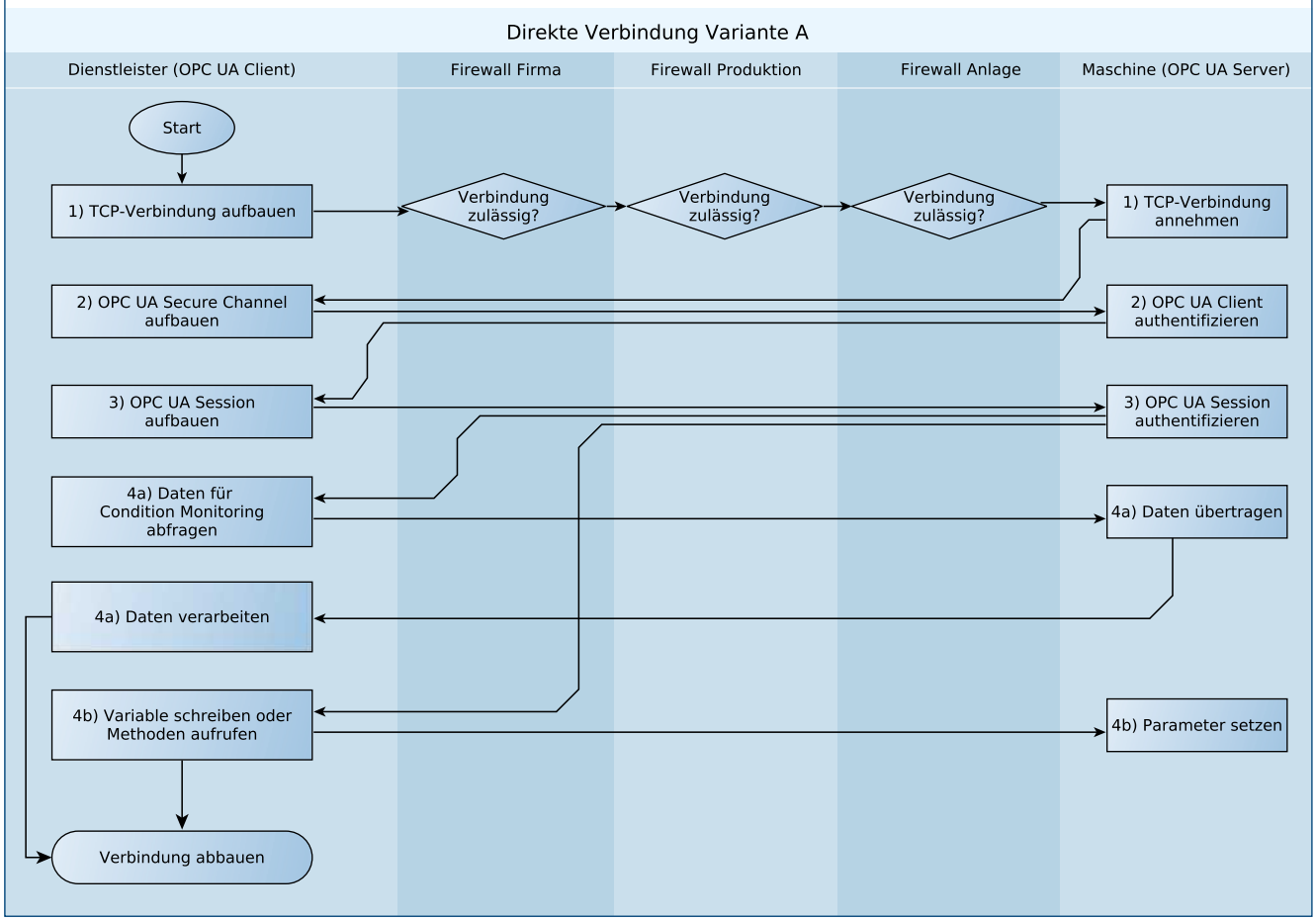
Der OPC UA-Client des Dienstleisters verbindet sich mit dem OPC UA-Server auf der Maschine (siehe Abbildung 5). Es sind nur autorisierte Zugriffe erlaubt.[3]

Abbildung 4: Netzwerkschema zur Umsetzung mit direkter Verbindung



3 Diskussionspapier „Zugriffssteuerung für Industrie 4.0-Komponenten zur Anwendung von Herstellern, Betreibern und Integratoren“ (10), Abschnitt 3.3.

Abbildung 5: Ablaufplan des direkten Verbindungsaufbaus



Der Ablauf dazu sieht wie folgt aus:

1. Es wird eine Verbindung vom OPC UA-Client des Dienstleisters zum OPC UA-Server der Maschine aufgebaut. Diese Kommunikation muss durch die Infrastruktur des Betreibers autorisiert und durchgeleitet werden.

2. Die OPC UA-Verbindung wird aufgebaut. Der OPC UA-Client authentifiziert den OPC UA-Server über dessen Zertifikat. Der OPC UA-Server authentifiziert den OPC UA-Client über dessen Zertifikat.

3. Zusätzlich kann sich der User im Rahmen der Session am Client über [Zertifikat oder Username + Passwort oder Token] authentifizieren.

   Die Verbindung wird über den OPC UA-Modus „Sign and Encrypt“ verschlüsselt und die ausgetauschten Nachrichten werden signiert. An der Session werden die Rechte festgemacht, wie sie sich aus den User- oder aus den Verbindungsinformationen ergeben.

4. Nach erfolgreichem Verbindungsaufbau können die Datenzugriffe der verschiedenen Funktionen Condition Monitoring (a) und Parametrierung (b) erfolgen:

   a) Der OPC UA-Client ruft Daten der Maschine ab. Hierbei sind unterschiedliche Varianten möglich:
      ii) Der OPC UA-Client fragt periodisch die gewünschten Werte beim OPC UA-Server ab.
      iii) Der OPC UA-Client registriert sich für einen Datenpunkt und der OPC UA-Server sendet periodisch oder bei Änderungen den Wert an den Client.

   b) Der OPC UA-Client parametriert die Maschine. Dazu verändert er Variablen im Informationsmodell durch direkte OPC UA-Schreibanfragen oder -Methodenaufrufe.

4.1.2 Variante B: Reverse-Connect

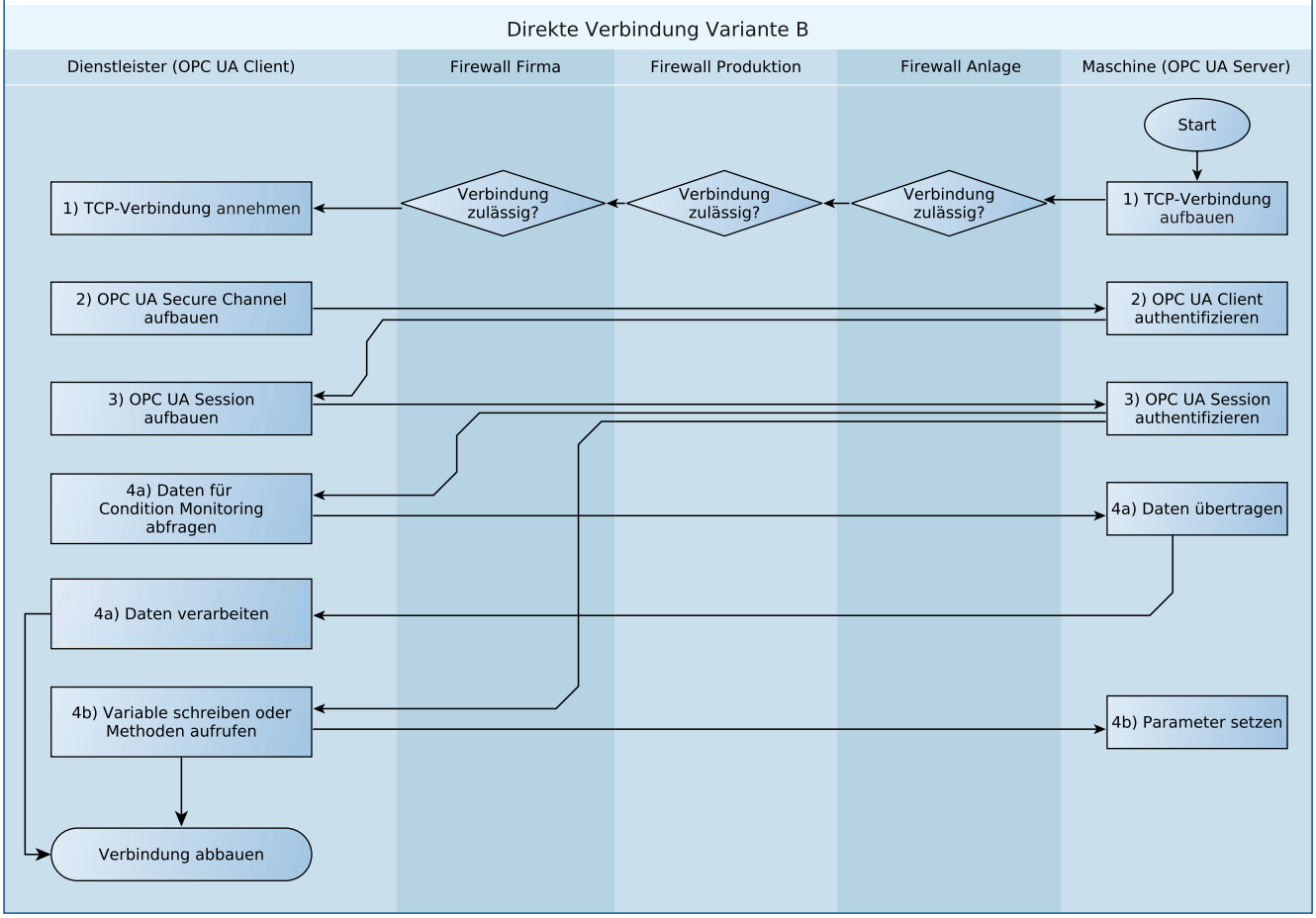
Der OPC UA-Server auf der Komponente verbindet sich mit dem OPC UA-Client des Dienstleisters (siehe Abbildung 6). Es sind nur autorisierte Zugriffe erlaubt.[4] Diese Variante unterscheidet sich zur vorigen Variante A ausschließlich in Schritt 1, der Richtung des Aufbaus der TCP-Verbindung.

Die Authentifizierung, Autorisierung und der Zugriff auf die Daten bzw. Methoden bei Reverse-Connect unterscheidet sich nicht vom normalen Verbindungsaufbau im Client-Server-Betrieb und muss daher nicht gesondert betrachtet werden.

Der Verbindungsaufbau wird von der Maschine initiiert. Hierzu wird ein inverser Verbindungsaufbau (Reverse-Connect-Verfahren) verwendet. Im OPC UA-Standard wird dieses Verfahren unter „Reverse Hello Message“ beschrieben.[5]

1. Es wird eine TCP-Verbindung durch den OPC UA-Server der Maschine zum OPC UA-Client des Dienstleisters aufgebaut.

Abbildung 6: Ablaufplan des direkten Verbindungsaufbaus mit Reverse-Connection



4 Diskussionspapier „Zugriffssteuerung für Industrie 4.0-Komponenten zur Anwendung von Herstellern, Betreibern und Integratoren“ (10), Abschnitt 3.3.

5 OPC Unified Architecture, Part 6, 1.04, Abschnitt 7.1.3: „Establishing a connection“.

2. Der OPC UA-Client des Dienstleisters nutzt diese TCP-Verbindung, um auf der Anwendungsebene eine OPC UA-Verbindung zum OPC UA-Server der Maschine herzustellen. Der OPC UA-Client authentifiziert den OPC UA-Server über dessen Zertifikat. Der OPC UA-Server authentifiziert den OPC UA-Client über dessen Zertifikat.

3. Zusätzlich kann sich der User im Rahmen der Session am Client über [Zertifikat oder Username + Passwort oder Token] authentifizieren, wie in Variante A.

4. Nach erfolgreichem Verbindungsaufbau können die Datenzugriffe der verschiedenen Funktionen „Condition Monitoring“ (a) und „Parametrierung“ (b) wie in Variante A erfolgen.

4.1.3 Ablauf/Voraussetzungen

Um einen Verbindungsaufbau entsprechend der Variante A etablieren zu können, muss in allen Firewalls des Betreibers bis zur Komponente der Standardport (TCP 4840) für eingehende Verbindungen freigeschaltet werden. Die Erreichbarkeit und Adressierbarkeit des OPC UA-Servers der Komponente muss vonseiten des Dienstleisters über entsprechende NAT-Regeln oder Port-Weiterleitungen beim Betreiber gewährleistet sein:

- Bei der Variante B ist es ausreichend, wenn die Firewalls im Netz des Betreibers den Aufbau von Verbindungen ins Internet zulassen. Dabei ist es möglich, dass die Verbindung auf einen bestimmten Host oder eine Domain des Dienstleisters eingeschränkt wird. Das Reverse-Connect-Protokoll (vgl. oben) muss entsprechend den OPC UA-Standards implementiert werden.

- In beiden Fällen handelt es sich um Maßnahmen, die beim Einsatz zu berücksichtigen sind. Die Konfiguration von Firewalls ist Aufgabe des Betreibers und unabhängig von OPC UA.

- In Schritt 2 erfolgt die Authentifizierung der OPC UA-Verbindung. Dazu müssen die entsprechenden Zertifikate in OPC UA-Server und -Client vorliegen, siehe Diskussionspapier „Sichere Implementierung von OPC UA für Betreiber, Integratoren und Hersteller“ (2). Zur Verwaltung der ausgegebenen Zertifikate könnten OPC UA-Trust-Listen aufgestellt und benutzt werden.

- Die so aufgebaute Verbindung kann dazu genutzt werden, Daten vom OPC UA-Server abzurufen, Variablen auf dem Server zu setzen oder Methoden aufzurufen. Der am OPC UA-Server angemeldete Benutzer muss dazu für den Zugriff auf die notwendigen Daten oder Methoden autorisiert sein.

4.1.4 Bewertung

Die Wahl der zu verwendenden Variante hat in der Praxis weitreichende Konsequenzen für die sich ergebende Sicherheit bzw. für die Komplexität der Verwaltung.

Im Folgenden werden daher die Eigenschaften der beiden Varianten diskutiert.

4.1.4.1 Variante A: Client to Server

Der Vorteil einer direkten Verbindung liegt darin, dass diese Variante das gebräuchlichste Verfahren zum Verbindungsaufbau zwischen OPC UA-Geräten darstellt und damit von allen OPC UA-fähigen Geräten unterstützt werden sollte. In diesem Sinne werden die Anforderungen A1 und A2, also die unternehmensübergreifende Kommunikation mit möglichst großer Kompatibilität erfüllt.

Demgegenüber steht der Nachteil, dass ein direkter Zugriff auf das OT-Netz von externen Systemen stattfindet, da die Komponente direkt mit dem Internet verbunden ist. Die Umsetzung der Anbindung und die Freigabe im Netzwerk des Betreibers erzeugen Aufwand, der mit steigender Anzahl von Komponenten unterschiedlicher Hersteller zunimmt. Dies steht im Gegensatz zu Anforderung A3, der Skalierbarkeit über verschiedene Netzwerkgrößen und Geräteanzahl.

Eingehende Verbindungen ins OT-Netzwerk sind ebenfalls kritisch zu betrachten, da hierüber auch ein Angreifer direkten Zugriff auf die Komponenten im Produktionsnetzwerk erlangen kann. Als Schutzmaßnahme kann der Zugriff auf einzelne IP-Adressen eines Dienstleisters eingeschränkt werden. Dies ist allerdings bei einer steigenden Anzahl an Dienstleistern mit zunehmendem administrativem Aufwand verbunden, was Anforderung A4, der Wartbarkeit und Kontrolle der Kommunikation, entgegensteht.

Durch die Verwendung des Security-Modes „Sign and Encrypt“ wird die Verbindung Ende-zu-Ende verschlüsselt aufgebaut und verwendet. Den netzwerkbasierten Sicherheitsmechanismen des Betreibers (z. B. IDS, IPS) ist es daher nicht möglich, die kommunizierten Daten einzusehen und zu überwachen. Betreiber verwenden häufig IP-Adressen aus privaten Bereichen oder vergeben IP-Adressen dynamisch. Die Adressierbarkeit der Maschine im Betreibernetz ist vom Dienstleister aus deshalb schwierig. Sie kann durch NAT- oder Port-Forwarding oder die Verwendung eines „Reverse Proxy“ im Netzwerk des Betreibers hergestellt und muss gepflegt werden. Damit sind zusätzliche Aufwände verbunden.

Auch diese Eigenschaften stehen mit den Zielen A3 und A4, also der Skalierbarkeit, Wartbarkeit und der Kontrolle des Zugriffs, im Konflikt.

Da der OPC UA-Server in dieser Variante unter Kontrolle des Betreibers steht, kann der Betreiber durch geeignete Protokollierungsmechanismen feingranular erfassen, welche Zugriffe und Veränderungen auf dem Server stattgefunden haben. Die Protokollierung kann außerhalb des Zugriffs des Dienstleisters geschehen, sodass das Ziel der Nachvollziehbarkeit (A5) für den Betreiber gewährleistet werden kann. Zusätzlich sollten alle eingehenden Verbindungen protokolliert werden, jedoch ist dies nicht Teil des OPC UA-Servers.

4.1.4.2 Variante B: Reverse-Connect

Bei dieser Verbindungsvariante müssen nur von der Komponente ausgehende Verbindungen zugelassen werden. Die Antwortpakete des OPC UA-Client auf die Reverse-Connect-Verbindungsanfrage des Servers werden von den Firewalls in aller Regel zugelassen. Für den Dienstleister ergibt sich der Vorteil, dass der Zugriff auf die Daten nicht eingeschränkt ist. Ausgehende Verbindungen sollten jedoch trotzdem durch den Betreiber überwacht und spezifisch zugelassen werden. Für den Betreiber ist positiv festzuhalten, dass der Aufwand für Freigaben in den Firewalls im Vergleich zur Variante A trotzdem in der Regel geringer ist. Im Gegensatz zu Variante A werden daher die Ziele A3 (Skalierbarkeit) und A4 (Wartbarkeit) besser erfüllt. Falls sich das Produktionsnetz hinter einem Network Address Translator (NAT) befindet, gestaltet sich der Einsatz der Variante B ebenfalls einfacher, da auf die zusätzliche Einrichtung von Port-Forwarding-Regeln (in Kombination mit Firewall-Regeln für die Reglementierung des Port-Forwardings) verzichtet werden kann. Auch dies trägt zu einer besseren Skalierbarkeit und Wartbarkeit (A3 und A4) bei.

Anderseits ist die Kontrolle des Betreibers über die Kommunikation eingeschränkt, da die Komponente autonom Verbindungen zum Dienstleister aufbauen kann. Eine direkte Verbindung zwischen einem externen System und dem OT-Netz des Betreibers besteht auch bei dieser Verbindungsvariante, sodass auch hier das Ziel A4 (Kontrolle) nur bedingt als erfüllt angesehen werden kann. Auch das Ziel A5 (Nachvollziehbarkeit) kann unter dem autonomen Verbindungsaufbau der Komponente zu den Servern des Dienstleisters leiden.

Die Adresse des OPC UA-Clients des Dienstleisters muss auf der Maschine konfiguriert werden. Dies skaliert bei vielen Maschinen linear und verursacht bei Änderung oder Umzug des OPC UA-Clients gegebenenfalls viel Aufwand.

Eine Überwachung der übertragenen Daten durch den Betreiber ist nicht möglich, da diese Ende-zu-Ende verschlüsselt übertragen werden. Eine Protokollierung durch die Komponente selbst ist jedoch weiterhin möglich und dient der Nachvollziehbarkeit, also dem Ziel A5. Sollte der Betreiber jedoch nicht in der Lage sein, auf die erfassten Ereignisprotokolle der Komponente zuzugreifen (weil diese z. B. vom Dienstleister konfiguriert und verwaltet wird), kann das Ziel der Nachvollziehbarkeit nicht vom Betreiber, sondern nur vom Dienstleister erreicht werden. Je nach Zugriff auf die Log-Daten des Servers der Komponente lässt sich das Ziel der Nachvollziehbarkeit (A5) also entweder für den Betreiber, den Dienstleister oder beide Parteien erreichen.

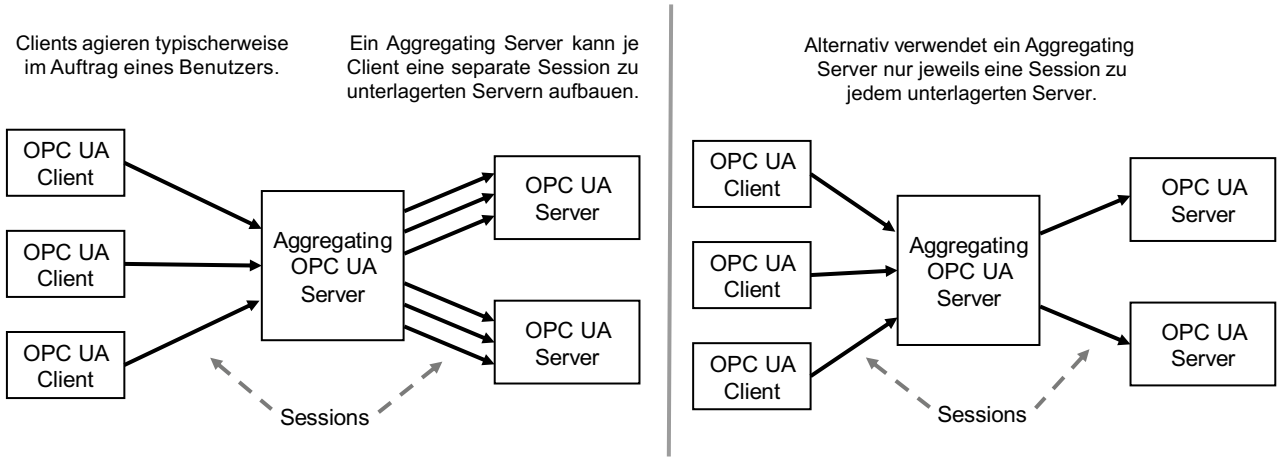
4.2 Lösungsansatz: Aggregating Server

Die OPC UA-Kommunikation soll hierbei über eine zwischengeschaltete Instanz (Aggregating Server[6]) erfolgen. Ein Aggregating Server kann agieren als:

a) zentraler Zugriffspunkt, welcher Anfragen annimmt und weiterleitet.

6 Gemäß der Spezifikation von OPC UA wird dies als Aggregating Server bezeichnet, siehe OPC Unified Architecture, Part 4, Release 1.04, Abschnitt 5.6.2 Create Session und dort besonders Abbildung 14. Aufnahme als Referenz in der finalen Dokumentation/Version.

Abbildung 7: Verschiedene Verwendungen eines Aggregating Servers



b) zentraler Datenkonzentrator und Datenlieferant, welcher Informationen der untergelagerten Quellen abruft und stellvertretend in einem eigenen (neuen) Informationsmodell bereitstellt.

Er hält oder etabliert stellvertretend für außenstehende OPC UA-Clients Verbindungen zu den OPC UA-Servern der untergelagerten Komponenten. Im Auftrag dieser OPC UA-Clients kann er unter anderem Zugriffe an OPC UA-Server in unterlagerten Komponenten weiterleiten. Bei Datenzugriffen ist ihm optional eine Zwischenspeicherung (Caching), Verarbeitung/Aufbereitung der Daten sowie eine Anpassung der aggregierten Informationsmodelle möglich.

Ein Aggregating Server kann jeweils nur eine Session zu jedem unterlagerten OPC UA-Server aufbauen, über welche dann alle Datenzugriffe erfolgen oder weitergeleitet werden (Abbildung 6, rechts). Alternativ kann ein Aggregating Server eine zusätzliche Security-Stufe einführen, indem er für jeden OPC UA-Client unabhängige Sessions aufbaut, über welche dann nur die Datenzugriffe vom jeweiligen OPC UA-Client erfolgen (Abbildung 7, links).

Es ist möglich, mehrere Aggregating Server hintereinander zu schalten (Kaskadierung).

Darüber hinaus sind folgende vorteilhafte Punkte des Einsatzes eines Aggregating Servers zu erwähnen:

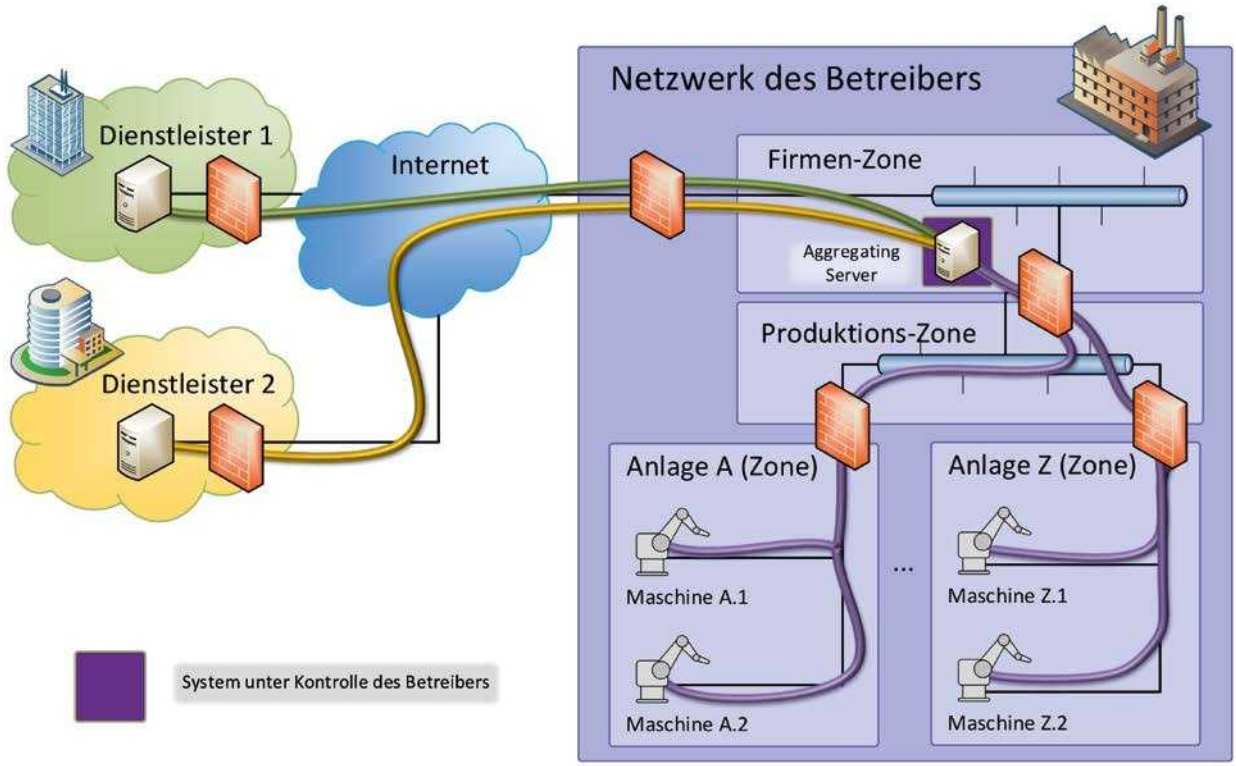
a) Er kann die Menge der TCP/IP-Verbindungen, die durch Firewalls gehen, reduzieren, indem er stellvertretend nur jeweils eine Verbindung zu den unterlagerten Komponenten oder weiteren untergelagerten aggregierenden Servern aufbaut/unterhält;

b) Er vereinfacht die Handhabung, weil nur ein OPC UA-Server (Aggregating Server) von außen adressiert werden muss, um auf die Daten/Informationsmodelle von mehreren untergelagerten Komponenten zugreifen zu können.

Ein Aggregating Server kann entweder vom Betreiber oder vom Dienstleister gestellt und verwaltet werden, selbst wenn er – wie hier gezeigt – beim Betreiber aufgestellt ist.

Hierdurch ergeben sich die im Folgenden beschriebenen Vor- und Nachteile.

Abbildung 8: Netzwerkschema zum Kommunikationsaufbau via Aggregating Server



4.2.1 Szenario A: Der Betreiber stellt und verwaltet einen Aggregating Server

Zuerst wird hier diejenige Lösungsvariante beschrieben und erörtert, bei welcher der Betreiber den Aggregating Server in seiner Umgebung aufstellt, konfiguriert und selbst verwaltet. Er konfiguriert die Verbindungen, die der Aggregating Server zu bei ihm betriebenen Komponenten aufbaut.

Dem Dienstleister gewährt der Betreiber Zugriff auf den Aggregating Server und die entsprechenden Teile des Informationsmodells. Eventuell gewährt der Betreiber verschiedenen Dienstleistern den Zugriff auf den Aggregating Server, jeweils auf die für sie relevanten Teile des Modells und damit auf die relevanten Komponenten.

4.2.1.1 Vorteile

Bei der Bewertung des Szenarios „Betreiber-Verwaltung“ fällt positiv auf, dass das „Proxy“-Szenario den IT-Administratoren bereits von anderen Kommunikationsprotokollen hinreichend bekannt sein dürfte. Es lässt sich in der Regel gut in bestehende Netzwerk-Entwurfskonzepte integrieren. Das Konzept erlaubt daher eine mit bestehenden Strukturen kompatible unternehmensübergreifende Kommunikation (Anforderungen A2 und A3).

Die Kontrolle des Datenflusses durch den Betreiber ist möglich: Der Betreiber kann definieren, welche Zugriffe er zulässt und welche Daten fließen dürfen, was das Ziel der skalierbaren Kontrolle (A4) unterstützt.

Mit diesem Ansatz ist ein einheitlicher Zugang in das Netz des Betreibers für unterschiedliche Dienstleister realisierbar. Dies reduziert den Aufwand für die Freigabe und die Überwachung, weil nur ein Aggregating Server für mehrere Dienstleister betrieben werden muss. Dies unterstützt ebenfalls die Erreichung der Kontrolle und Wartbarkeit (A4) sowie die Nachvollziehbarkeit (A5).

Der Betreiber legt die Security-Policies für die Kommunikation zwischen dem Aggregating Server und den OPC UA-Servern der Komponenten beziehungsweise unterge-

lagerten Aggregating Servern fest, insoweit es die OPC UA-Server der Komponenten zulassen bzw. unterstützen. Dadurch kann er einheitliche Sicherheitsrichtlinien für die Kommunikation innerhalb seines Netzes, beispielsweise die Mitlesbarkeit interner Kommunikation, durchsetzen, was ebenfalls die Anforderung A4 bedient. Ebenso kann der Betreiber eines Aggregating Servers detaillierte Log-Daten auf dem eigenverwalteten Aggregating Server erfassen, was zur Erreichung des Ziels A5 (Nachvollziehbarkeit) beiträgt.

4.2.1.2 Nachteile

Der Aufwand (Beschaffung, Management und Betrieb) eines Aggregating Servers liegt beim Betreiber und erfordert den Einsatz zusätzlicher Infrastruktur und Software. Weiterhin stellt der Aggregating Server aufgrund seiner Rolle als zentraler Vermittler mit vielfältigen Verbindungen innerhalb und außerhalb des Unternehmensnetzes einen zentralen Angriffspunkt dar und muss dementsprechend ausgewählt und betrieben werden.

Für den Dienstleister ergibt sich der Nachteil, dass der Betreiber beim Condition Monitoring und bei der Parametrierung mithören und/oder Daten manipulieren kann. Für manche Geschäftsmodelle (z. B. wenn die Komponente im Besitz und unter Kontrolle des Dienstleisters bleibt) kann dies inakzeptabel sein.

Aus Sicht des Dienstleisters steht dies daher in Konflikt mit den Zielen der Kontrolle (A4) sowie der Vertraulichkeit, insbesondere wenn sensible Daten zwischen Dienstleister und Komponente ausgetauscht werden. Ein Beispiel hierfür ist die Parametrierung geheimer Rezepte oder wenn beim Condition Monitoring der Informationsgehalt der Zustandsdaten geistiges Eigentum enthält.

Aus Sicht des Dienstleisters hat dieses Szenario auch einen Nachteil bezüglich der Nachvollziehbarkeit (A5), da der Besitz der Auditinformationen komplett beim Betreiber liegt.

Die Credentials (Anmeldedaten wie Benutzername und Passwort) für den Verbindungsaufbau vom Aggregating Server zur Komponente müssen vom Betreiber eingestellt werden und sind damit dem Betreiber bekannt. Die damit verbundenen Rechte müssen alle Zugriffe erlauben, die ein Dienstleister durch den Aggregating Server auf die Komponenten vornehmen soll. Auch dies steht gegebenenfalls in Konflikt mit dem Ziel der Kontrolle (A4) durch den Dienstleister.

4.2.2 Szenario B: Die Dienstleister stellen eigene Aggregating Server beim Betreiber auf

Das zweite Szenario des Einsatzes eines Aggregating Servers besteht darin, dass der Dienstleister einen Aggregating Server beim Betreiber aufstellt, konfiguriert und fortan wartet, damit er sich von Ferne aus dorthin verbinden kann und darüber alle für ihn relevanten Komponenten erreicht.

Der Dienstleister konfiguriert im Aggregating Server, von welchen Komponenten welche Informationsmodelle dort zur Verfügung gestellt werden sollen. Er konfiguriert also insbesondere, mit welchen Credentials (Anmeldedaten) der Aggregating Server Verbindungen zu den unterlagerten Komponenten aufbaut.

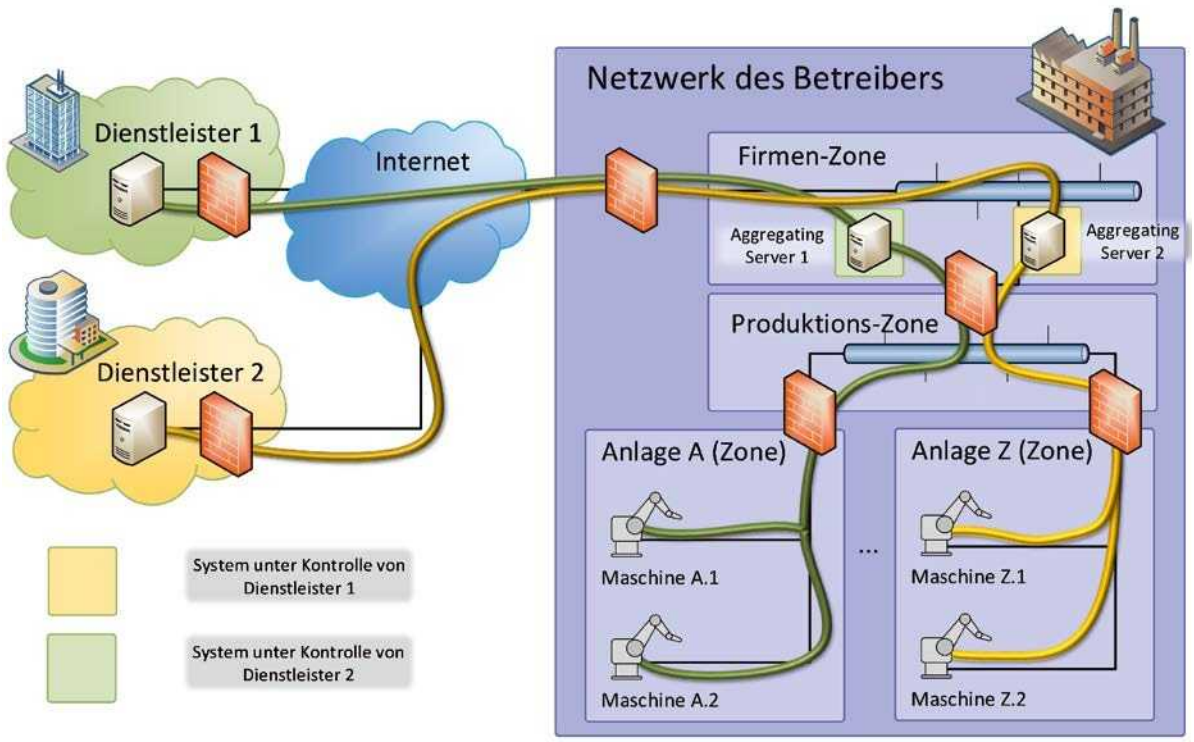
4.2.2.1 Vorteile

Das Fernwartungsszenario mit Fremdkomponenten eines Dienstleisters ist den IT-Administratoren eines Betreibers bereits bekannt. Da ähnliche Lösungen im Industrieumfeld etabliert sind, kann diese Integration als vereinbar mit Anforderungen A1 und A2 erachtet werden. Verbessernd kommt hinzu (wie auch beim vorherigen Szenario), dass nicht direkte Verbindungen von ganz außen bis nach ganz innen erlaubt werden müssen, sondern nur bis zu einem definierten Punkt (dem Aggregating Server des Dienstleisters). Dies unterstützt die Erreichung der Ziele Kontrolle und Skalierbarkeit (A3 und A4).

Das Aufstellen, Konfigurieren und Warten des Aggregating Servers durch den Dienstleister kann eine Entlastung für den Betreiber sein, was wiederum zur Erreichbarkeit einer skalierbaren unternehmensübergreifenden Kommunikation beiträgt (Anforderungen A3 und A4).

Der Dienstleister bestimmt durchgängig den Sicherheitsgrad der Verschlüsselung der Kommunikation von seiner Stelle bis zur Komponente. Das Geheimnis der Parametrierungsdaten und der Daten aus dem Condition Monitoring kann für den Dienstleister durchgängig gewahrt werden, da er die Kontrolle über die Verschlüsselung der Kommunikation des Aggregating Servers mit unterlagerten Komponenten hat und so das Mitlesen der Kommunikation durch den Betreiber ausschließen kann. Dies unterstützt aus Sicht des Dienstleisters die Ziele Kontrolle und Nachvollziehbarkeit (A4 und A5).

Abbildung 9: Netzwerkschema zur Verwaltung des Aggregating Servers durch die Dienstleister



4.2.2.2 Nachteile

Durch den Einsatz dieser Lösung ergeben sich jedoch auch Nachteile, insbesondere für den Betreiber. Der Betreiber hat keine Kontrolle, welche Information der Dienstleister von den Komponenten erhält und welche Parametrierungen der Dienstleister an den Komponenten vornimmt. Darüber hinaus kann der Dienstleister ungesehen Komponenten im Netz des Betreibers fernsteuern. Deshalb muss der Betreiber dem Dienstleister hohes Vertrauen entgegenbringen. Dies steht den Zielen der Kontrolle und Nachvollziehbarkeit des Betreibers im Wege (A4 und A5).

Ebenso führt eine zusätzliche Einschränkung der Kommunikation zu einem erhöhten Aufwand beim Betreiber, da mit Fremdkomponenten im eigenen Netzwerk umgegangen werden muss. Dies kann die Skalierbarkeit und Wartbarkeit des Netzwerks (A3, A4) beeinträchtigen.

Der Betreiber muss die Installation einer Vielzahl von Aggregating Servern akzeptieren, wenn Komponenten von verschiedenen Dienstleistern überwacht (Condition Monitoring) und parametriert werden sollen. Dies ist insbesondere problematisch, da die Dienstleister nicht untereinander abgestimmt sein müssen bzw. können. Falls mehrere Dienstleister Zugriff auf eine größere Anlage haben müssen, nimmt die Komplexität im Netzwerk des Betreibers zu und beeinträchtigt dessen Kontrolle über die Geschehnisse im eigenen Netzwerk (Anforderung A4).

Durch die Verwaltung des Aggregating Servers durch den Dienstleister hat dieser vornehmlich Zugriff auf die Ereignisdatenerfassung des Servers und kann so Zugriffe und Veränderungen genau nachvollziehen (Anforderung A5). Der Betreiber ist auf die Kooperation des Dienstleisters angewiesen, um ebenfalls Zugriff auf die Protokolle zu erhalten und das Ziel der Nachvollziehbarkeit (A5) für sich selbst zu erreichen.

4.2.3 Bewertung und Vergleich der Szenarien

Bei der Verwendung eines Aggregating Servers gibt es grundsätzlich die zwei oben beschriebenen Möglichkeiten, die Konfiguration, die Administration und den Betrieb zu organisieren: Entweder durch den Betreiber oder durch

den Dienstleister. Dabei hat immer derjenige, der die Administration des Aggregating Servers übernimmt, den Aufwand und auch die Verantwortung für die richtige und sichere Konfiguration. Die andere Partei spart sich diesen Aufwand, muss aber dem, der den Aggregating Server administriert, das Vertrauen entgegenbringen, dass die Vertraulichkeit und Integrität aller Daten und Metadaten nicht verletzt wird. Es ist hervorzuheben, dass eine Verletzung der Vertraulichkeit oder Integrität immer einen bewussten Eingriff erfordert und nicht schon alleine durch die Entscheidung für ein Betriebskonzept bedingt ist.

Das Szenario A mit der Verwaltung des Aggregating Servers durch den Betreiber ist insgesamt sinnvoll, wenn der Betreiber komplette Transparenz und Kontrolle wünscht und der Dienstleister bereit ist, sie zu gewähren. Für den Dienstleister stellt sie jedoch einen Kompromiss bei der Wahrung der Kontrolle über die Komponente sowie bei der Wahrung der Vertraulichkeit der Kommunikation mit der Komponente dar. Der Dienstleister muss hierbei allerdings in Kauf nehmen, dass er sowohl Rechte gewähren als auch gegebenenfalls Geschäftsgeheimnisse offenlegen muss, da der Betreiber alles mitlesen kann.

Das Szenario A ist offensichtlich dann gut geeignet, wenn verschiedenste Dienstleister für denselben Betreiber aktiv sind und diese auch nichts gegen die Einsicht des Betreibers in die von ihnen übertragenen Daten einzuwenden haben.

Das Szenario B, bei dem ein Dienstleister einen Aggregating Server beim Betreiber installiert und administriert, ist vor allem aus Sicht des Dienstleisters sinnvoll, wenn dieser ein Höchstmaß an Kontrolle über die Interaktion mit der Komponente ausüben möchte.

Dieses Szenario ist aber umso problematischer, je mehr Dienstleister für denselben Betreiber aktiv sind. Es funktioniert also besonders dann gut, wenn ein Dienstleister viele vertrauensvolle Betreiber betreut und diese hauptsächlich nur einen Dienstleister beauftragen.

Zusätzlich ist zu erwähnen, dass in beiden Szenarien das Reverse-Connect-Verfahren (insbesondere für die Verbindungen zwischen dem Aggregating Server und den unterlagerten OPC UA-Servern der Komponenten) angewendet werden kann, was ein zusätzliches Maß an Security einbringt, da die Firewalls dann immer in die übliche Richtung durchquert werden müssen.

4.3 Vergleich der Lösungsansätze

Welche der oben beschriebenen Varianten, direkte Verbindung oder Aggregating Server, verwendet wird, muss zwischen Betreiber und Dienstleister abgestimmt werden. Dabei ist darauf zu achten, dass auch zukünftige Erweiterungen von Anlagen, auch mit Komponenten anderer Hersteller, bedacht werden. Aus Sicht der Security erscheinen die Verwaltung wie die Überwachung einer größeren Zahl direkter Verbindungen im Alltagsbetrieb entsprechend Skalierbarkeit (A3), Kontrolle (A4) und Nachvollziehbarkeit (A5) nicht realistisch. Der Betreiber muss zudem, auf einem Wege außerhalb der OPC UA-Kommunikation, zum Schutz vor zeitlich nicht passenden Parametrierungen eine entsprechende Zugriffssteuerung einführen. Zum Beispiel kann dies durch einen Schlüsselschalter an der Komponente oder Anlage erfolgen, mit dem die Parametrierbarkeit zeitlich befristet freigeschaltet werden kann. Dieses gilt besonders, wenn während Parametrierungsarbeiten Gefährdungen von Leib und Leben möglich sind, entsprechend den Anforderungen zur Kontrolle (A4).

Unabhängig vom Betriebskonzept vereinfacht der Einsatz eines Aggregating Servers den Zugriff auf mehrere Komponenten: Die Anzahl notwendiger Verbindungen (bei entsprechender Zonierung des Netzwerks auch durch Firewalls) wird reduziert. Durch die durchgängige Verwendung von OPC UA geht das Informationsmodell der Komponenten nicht verloren, sondern wird auf dem Aggregating Server repräsentiert und kann gegebenenfalls durch die Informationsmodelle und Daten weiterer Komponenten ergänzt werden. Der Wechsel des Betriebskonzepts für den/die Aggregating Server ist mit größerem Aufwand verbunden. Dies betrifft sowohl einen Austausch der Hard- und Software wie auch die erforderlichen Prozesse für den Betrieb und die Wartung. Liegt der Betrieb des Aggregating Servers beim Betreiber, kann dieser über dessen Einstellungen den schreibenden Zugriff für die Parametrierung beschränken. Aufgrund möglicher Gefährdungen für Maschinenbediener sollten weitere Maßnahmen wie der Schlüsselschalter an der Maschine selbst angewendet werden.

Das Reverse-Connect-Verfahren erweitert die Möglichkeiten für den Verbindungsaufbau zwischen OPC UA-Client und Server. Damit ist es möglich, einen OPC UA-Server auch hinter einer Firewall zu betreiben, die in ihrer Funktion ansonsten die Verbindungsaufnahme seitens eines Clients verhindern würde.

5 Zusammenfassung und Ausblick

Im Dokument werden Lösungsansätze für die unternehmensübergreifende Kommunikation mit OPC UA diskutiert, die auf dem Client-Server-Konzept basieren. Eine Kontrolle des Informationsflusses ist nur bei Verwendung der Aggregating-Server-Lösung möglich. Aus Sicht eines Betreibers, der die Verantwortung für seine Sicherheitsdomäne trägt, kommt nur der Eigenbetrieb eines Aggregating Servers in Betracht.

Ein Problem des Aggregating Servers, wie bei vielen anderen Proxy-Lösungen auch, ist, dass die Verbindung zwischen Client und Server aufgebrochen wird und damit der Schutz der Authentizität, wie er bei Ende-zu-Ende-Verbindungen möglich wäre, verloren geht. Es stünde zu prüfen, inwieweit eine Ergänzung des Konzepts zur Erreichung dieses Ziels möglich ist oder die Anwendung des Publish-Subscribe-Modells hier eine Lösung bietet.

Zusätzlich zum in diesem Dokument beschriebenen Verbindungsverfahren Client-Server bietet OPC UA auch die Möglichkeit, mittels Publish-Subscribe-Modell, kurz PubSub, zu kommunizieren. Neben dem primären Vorteil der höheren Leistungsfähigkeit bzw. geringeren Hardwareanforderung durch die Verwendung verbindungsloser Protokolle (UDP) können mittels PubSub auch andere Kommunikationsstrukturen aufgebaut werden.

Die in diesem Dokument beschriebene Client-Server-Architektur basiert per se auf 1:1-Verbindungen. Dies gilt auch bei Verwendung eines Aggregating Servers, der, wie gezeigt, gleichzeitig mehrere 1:1-Verbindungen aufbauen und halten kann. Demgegenüber definiert PubSub eine 1:n- oder One-to-many-Kommunikation, bei der eine Komponente (Publisher) ihre Daten an mehrere Empfänger (Subscriber) verteilt. Da für Publish-Subscribe-Kommunikation andere Voraussetzungen gelten, sowohl aus Sicht des Kommunikationslayers im Netzwerk wie auch hinsichtlich der Topologie, wird dieses Kommunikationsverfahren in diesem Dokument nicht betrachtet, sondern in einem zukünftigen Dokument diskutiert.

6 Anhang

6.1 Glossar

Authentifizierung	Vorgang, die Identität einer Person oder eines Rechnersystems anhand eines bestimmten Merkmals zu überprüfen
Authentisierung	Authentisierung bezeichnet den Nachweis oder die Überprüfung der Authentizität
Autorisierung	Bei einer Autorisierung wird geprüft, ob eine Person, IT-Komponente oder Anwendung zur Durchführung einer bestimmten Aktion berechtigt ist
ABAC	Attribute Based Access Control
Credentials	Anmeldedaten wie Benutzername und Passwort für die Verwendung bei Authentifizierung/ Authentisierung
Sicherheitsdomäne	Technologisch, organisatorisch oder räumlich zusammengehöriger Bereich mit einheitlichen Sicherheitsanforderungen und/oder einheitlicher Sicherheitsadministration
TLS	Transportation Layer Security
Zonen und Conduits	Konzept der IEC 62443 (7) zur Unterteilung von Automatisierungssystemen in Zonen unterschiedlicher Security-Anforderungen und deren Kopplung etwa durch Firewalls (Zones and Conduits)

6.2 Abbildungsverzeichnis

Abbildung 1: Exemplarische Betrachtung von Kommunikationsbeziehungen auf der Kommunikations- und Informationsschicht im RAMI4.0 4

Abbildung 2: Anwendungsszenario Condition Monitoring und Parametrierung 8

Abbildung 3: Anwendungsszenario mit Dienstleister und Betreiber 11

Abbildung 4: Netzwerkschema zur Umsetzung mit direkter Verbindung 12

Abbildung 5: Ablaufplan des direkten Verbindungsaufbaus 13

Abbildung 6: Ablaufplan des direkten Verbindungsaufbaus mit Reverse-Connection 14

Abbildung 7: Verschiedene Verwendungen eines Aggregating Servers 17

Abbildung 8: Netzwerkschema zum Kommunikationsaufbau via Aggregating Server 18

Abbildung 9: Netzwerkschema zur Verwaltung des Aggregating Servers durch die Dienstleister 20

6.3 Literaturverzeichnis

1. *Diskussionspapier „Sichere Kommunikation für Industrie 4.0“.* Berlin: Plattform Industrie 4.0, 2017.

2. *Diskussionspapier „Sichere Implementierung von OPC UA für Betreiber, Integratoren und Hersteller“.* Berlin: Plattform Industrie 4.0, 2018.

3. *Technischer Überblick „Sichere unternehmensübergreifende Kommunikation“* Berlin: Plattform Industrie 4.0, 2016.

4. *Umsetzungsstrategie Industrie 4.0.* Berlin/Frankfurt: Plattform Industrie 4.0, 2015.

5. *Welche Kriterien müssen Industrie 4.0 Produkte erfüllen?* Frankfurt/Main: ZVEI, 2016.

6. Information technology – Security Techniques – Information Security Management System. *ISO/IEC 27000:2014.*

7. Security for industrial automation and control systems. *IEC 62443*.

8. Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services. *ISO/IEC 27017:2015*.

9. Information technology – Security techniques – Information security for supplier relationships. *ISO/IEC 27036.*

10. *Diskussionspapier „Zugriffssteuerung für Industrie 4.0-Komponenten zur Anwendung von Herstellern, Betreibern und Integratoren“.* Berlin: Plattform Industrie 4.0, 2018.

AUTOREN

Carsten Angeli, KUKA Roboter GmbH | Dr. Hans-Peter Bock, TRUMPF Werkzeugmaschinen GmbH & Co. KG | André Braunmandl, Bundesamt für Sicherheit in der Informationstechnik | Torsten Förder, PHOENIX CONTACT Software GmbH | Prof. Dr. Tobias Heer, Hirschmann Automation & Control GmbH, Hochschule Albstadt-Sigmaringen | Dr. Christian Haas, Fraunhofer IOSB | Dr. Detlef Houdeau, Infineon Technologies AG | Dr. Lutz Jänicke (Leitung), PHOENIX CONTACT GmbH & Co. KG | Jens Mehrfeld, Bundesamt für Sicherheit in der Informationstechnik | Florian Patzer, Fraunhofer IOSB | Andreas Pfaff, Mitsubishi Electric Europe B.V. | Tobias Pfeiffer, Festo AG & Co. KG | Julius Pfrommer, Fraunhofer IOSB | Wolfgang Stadler, SICK AG | Detlef Tenhagen, HARTING Stiftung GmbH & Co. KG | Dmitry Tikhonov, Expleo Germany GmbH | Thomas Walloschke, Fujitsu Technology Solutions GmbH

Diese Publikation ist ein gemeinsames Ergebnis der Arbeitsgruppen „Sicherheit vernetzter Systeme“ und „Referenzarchitekturen, Standards und Normung“ (Plattform Industrie 4.0).

www.plattform-i40.de