PLATTFORM INDUSTRIE 4.0

DISKUSSIONSPAPIER

Sichere Implementierung von OPC UA für Betreiber, Integratoren und Hersteller

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
April 2018

Druck
Silber Druck oHG, Niestetal

Bildnachweis
BlackJack3D – gettyimages (Titel), sdecoret – Fotolia (S. 6), patpongstock – Fotolia (S. 8), zapp2photo – Fotolia (S. 9), NicoElNino – Fotolia (S. 13), Gorodenkoff – Fotolia (S. 21), Sikov – Fotolia (S. 24), kras99 – Fotolia (S. 25)

Zertifikat seit 2002
audit berufundfamilie

Das Bundesministerium für Wirtschaft und Energie ist mit dem audit berufundfamilie® für seine familienfreundliche Personalpolitik ausgezeichnet worden. Das Zertifikat wird von der berufundfamilie gGmbH, einer Initiative der Gemeinnützigen Hertie-Stiftung, verliehen.

FSC
www.fsc.org
MIX
Papier aus verantwortungsvollen Quellen
FSC® C044084

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

Einleitung

Industrie 4.0 schafft mit innovativen Konzepten und Vorgehensweisen völlig neue Möglichkeiten in der Zusammenarbeit – insbesondere auch auf technischer Ebene. Anlagen, 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.

Die Bedeutung von OPC UA

OPC UA (OPC[1] 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 (2) als eine wichtige Technologie empfohlen und ist Bestandteil der „Kriterien für Industrie-4.0-Produkte“ des ZVEI (3). Dieses Papier fokussiert entsprechend auf OPC UA.

Einsortierung von OPC UA in der M2M-Kommunikation

Standardisierungsarbeiten zur Maschine-zu-Maschine-Kommunikation erfolgen seit mehreren Jahren und zum Teil parallel in unterschiedlichen Organisationen, wie OPC-Foundation, IETF, oneM2M, OASIS, NIST, ITU und anderen. Dadurch sind unterschiedliche Architekturen, Protokolle und Sicherheitskonzepte mit unterschiedlichem Funktionsumfang entstanden.

Berücksichtigung der Security-Anforderungen

Für Aufgaben mit sich immer mehr öffnenden Security-Domänen der Automatisierung wird bereits heute intensiv auf Software und Netzwerkkommunikation zurückgegriffen. Entsprechend sind auch die Aspekte der Security[2] zu berücksichtigen, um den entstehenden Schutzbedarf zu erfüllen. Zwar sind grundsätzlich keine neuen Bedrohungen zu erwarten, durch die notwendige Öffnung des Perimeterschutzes, d.h. des Schutzes an der Außengrenze der Security-Domäne, wird die Angriffsfläche aber größer. Im Bereich der kritischen Infrastrukturen wird den Betreibern daher mittlerweile vorgeschrieben, Security-Maßnahmen zur Sicherstellung der Versorgung zu ergreifen. Im Bereich der industriellen Automation mit zunehmender Vernetzung nimmt die Security-Awareness ebenfalls zu. Mit dem Ziel einer intelligenten Produktion in der Industrie 4.0 und der damit verbundenen Vernetzung von IT, Produktion, Anlagen, Komponenten und Produkten ist die Betrachtung der Security elementarer Bestandteil der Konzepte, wie ebenfalls in der Umsetzungsstrategie (2) beschrieben.

Etablierte Normen und Standards beschreiben die technischen und organisatorischen Maßnahmen, die die Basis für einen sicheren Betrieb bilden, siehe Kapitel „Security“. Für den sicheren Einsatz des OPC-UA-Standards müssen die Anforderungen aus diesen Normen und Richtlinien in der Praxis umgesetzt werden. Der OPC-UA-Standard bietet viele Lösungskonzepte und Ideen an. Jetzt kommt es darauf an, zu beschreiben, wie die einzelnen Aspekte zusammenspielen müssen, um das Ziel des sicheren Einsatzes zu erreichen.

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. Dazu wird beispielhaft die Einbindung einer Maschine in die Infrastruktur eines Betreibers über den Lebenszyklus betrachtet.

1 OPC: Ursprünglich „OLE for Process Control”, heute „Open Platform Communications“

2 In diesem Dokument immer kurz für IT-Security

Ziel ist es, den beteiligten Stakeholdern, Herstellern, Integratoren und Betreibern 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. Dabei wird das Ziel verfolgt, möglichst alle notwendigen Aspekte nur durch OPC UA abzudecken, damit keine weiteren Anforderungen etwa durch eine weitere Schnittstelle wie ein Web Based Management erfüllt werden müssen. Entsprechend müssen Konfiguration und Parametrierung unternehmensübergreifend einheitlich gestaltet werden. Durch diesen Ansatz wird die Durchgängigkeit und Interoperabilität verbessert.

Dieses Papier basiert auf dem OPC-UA-Standard in der Version 1.04, 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.

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

Security

Security ist ein ganzheitliches Thema, das nur im Zusammenwirken aller Stakeholder erreicht werden kann. In den relevanten Standards für die industrielle Automatisierung, IEC 62443 (4) und der deutschen VDI 2182 (5), wird daher stets das Zusammenwirken von Betreibern, Integratoren und Herstellern betrachtet.

Management der Informationssicherheit

Die Security-Anforderungen für den sicheren Betrieb müssen sich am betrieblichen Rahmen orientieren, siehe auch „IT-Security in der Industrie 4.0 – Handlungsfelder für Betreiber“ (6). Entsprechende Informationssicherheitsmanagementsysteme (ISMS) werden in der ISO 27000 (7) und der IEC 62443-2-1 (4) beschrieben. Welche Bedrohungen für Daten und Systeme bestehen, kann nur spezifisch, je nach Anwendungsfall bestimmt werden. Für ein Vorgehen mit mehreren Stakeholdern, wie später diskutiert und in Abbildung 2 dargestellt, sind die Anforderungen aller Beteiligten zu berücksichtigen. Hierbei kann es zu Zielkonflikten kommen.

Bedrohungsanalyse

Basis für die Bedrohungsanalyse ist die Bestimmung der zu schützenden Unternehmenswerte. Bei einem Betreiber sind dies typischerweise Know-how, die Verfügbarkeit der Anlagen, die Effizienz der Produktion und die Qualität der Produkte. Das Dokument „Integrität von Daten, Systemen und Prozessen“ (8) geht auf die häufig unterschätzte Bedeutung des Schutzziels Integrität als Voraussetzung ein. Sind die zu schützenden Unternehmensziele identifiziert, können die Bedrohungen, etwa Abfluss von Know-how oder Störungen der Produktion, beschrieben werden.

Schutzziele und Richtlinien

Sind die Bedrohungen identifiziert, werden entsprechend die Schutzziele formuliert und Maßnahmen ergriffen, die sich an der Schwere der Auswirkung und der angenommenen Wahrscheinlichkeit orientieren. Die primären Schutzziele sind dabei:

- **Vertraulichkeit:** Schutz vor unbefugter Preisgabe von Informationen
- **Integrität:** Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen
- **Verfügbarkeit:** Dienste, Funktionen, Informationen können stets wie vorgesehen genutzt werden

Weitergehende Schutzziele werden unter anderem aus dem Bereich des Datenschutzes formuliert, etwa der Europäischen Datenschutzgrundverordnung (EU-DSGVO). Technisch lassen sich dabei diese Anforderungen auf die primären Schutzziele abbilden. Im Rahmen dieses Dokuments werden nur die primären Schutzziele im Zusammenhang mit Kommunikationsvorgängen berücksichtigt. Die weitere Umsetzung, etwa in der Datenspeicherung im Gerät, wird hier nicht betrachtet.

Bei der Auswahl und Umsetzung der Maßnahmen sind häufig Abwägungen zu treffen. Eine verschlüsselte Kommunikation schützt Inhalte vor Abhören (Schutzziel Vertraulichkeit), erschwert aber die Fehlersuche (Schutzziel Verfügbarkeit) und die Überwachung der Kommunikation. Entsprechend sind die Security-Maßnahmen anforderungsorientiert zu wählen. In einem internen Automatisierungsnetzwerk mit weniger leistungsstarken Komponenten kann gegebenenfalls auf Verschlüsselung verzichtet werden, der Schutz der Integrität ist hiervon technisch unabhängig möglich. Für den Informationsaustausch über ungeschützte Netzwerke ist zusätzlich die Vertraulichkeit relevant. Sichere Kommunikationsprotokolle bieten daher typischerweise die Optionen „Integritätsschutz“ (bei OPC UA: „Sign“) und „Vertraulichkeitsschutz + Integritätsschutz“ (bei OPC UA: „Sign and Encrypt“).

Detektion und Reaktion

Im Security-Management ist grundsätzlich davon auszugehen, dass eine 100 %ige Sicherheit nicht möglich ist. Insofern sind Mechanismen vorzusehen, die die Detektion eines Angriffs ermöglichen, wie Ereignisprotokollierung und inspizierbare Kommunikation, sowie Notfall- und Wiederherstellungskonzepte.

Security von Komponenten und Systemen

Die IEC 62443 (4) beschreibt in verschiedenen Teilen die Anforderungen an Security-Funktionen wie Benutzerverwaltung, Integritätsschutz, sichere Speicherung von elektronischen Schlüsseln und Logging ebenso wie Anforderungen an die Prozesse in der Integration und in der Entwicklung von Komponenten. Die Security-Funktionen werden dabei in „Security-Level" von SL-1 bis SL-4 eingeordnet, die eine Widerstandsstärke des Systems ausdrücken sollen. Der Security-Level wird ebenfalls in der Bedrohungsanalyse bestimmt. Wichtig ist es, dabei zu berücksichtigen, dass Security nicht nur das Vorhandensein von Funktionen bedeutet, sondern insbesondere die Anwendung nach Security-Gesichtspunkten gestalteter Entwicklungs- und Integrationsprozesse voraussetzt.

Die NAMUR-Empfehlung NE 153 (9) beschreibt prägnant die vier Aspekte der Security von Komponenten und Systemen:

- **Security by Design:** Security muss schon in der Konzeption mitgeplant werden
- **Security by Implementation:** Security als Qualität durch weitestmögliche Vermeidung von Fehlern
- **Security by Default:** Grundeinstellung sollte immer ein sicherer Zustand sein, keine nachträgliche Härtung
- **Security in Deployment:** Sicherer Betrieb durch Security-Dokumentation und Produktpflege

Anwendungsszenario

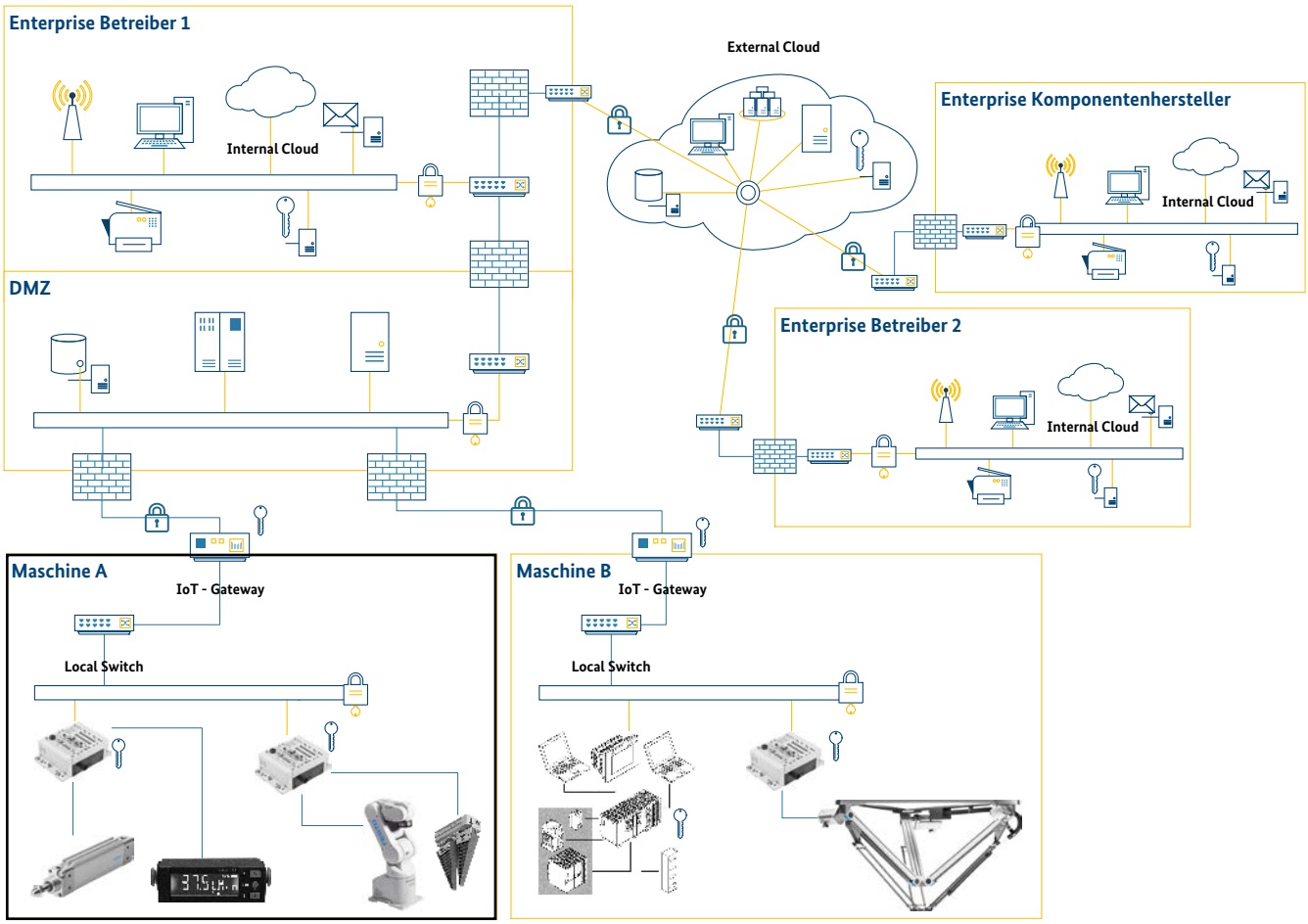
Zur Illustration einer entsprechenden Anwendung wird das Szenario „Kollaborative Fabrik“ verwendet. Dieses Industrie-4.0-Szenario zeigt die Einbindung verschiedener Maschinen in einer Fabrik mit Anbindungen an Cloud-Lösungen und weitere externe Unternehmen (Abbildung 1). Eine Übersicht über das Anwendungsszenario findet sich im Anhang. Die Kommunikation im unternehmensübergreifenden Verbund stellt eine Vielzahl von Anforderungen an die sichere Gestaltung. Diese Anforderungen und Ansätze werden im technischen Überblick „Sichere unternehmensübergreifende Kommunikation“ bereits diskutiert (10).

Für die Diskussion in diesem Dokument soll zunächst nur die Einbindung einer Maschine A in die Infrastruktur eines Betreibers betrachtet werden, siehe Kasten in Abbildung 1. Dabei wird die Maschine als Einheit betrachtet, die mit der Umgebung interagieren muss. Der Aufbau der Maschine spielt in dieser Betrachtung keine Rolle.

Abbildung 2 zeigt die logischen Kommunikationsbeziehungen der Maschine. Die Maschine muss einerseits in die Fertigung integriert werden und daher mit den Systemen beim Betreiber interagieren. Die Verwaltung von Fertigungsaufträgen muss ebenso möglich sein wie die Erfassung von Betriebsdaten und die Behandlung von Alarmen. Diese Kommunikationsbeziehung, in Abbildung 2 mit einem grünen Pfeil gekennzeichnet, steht im Mittelpunkt dieses Diskussionspapiers.

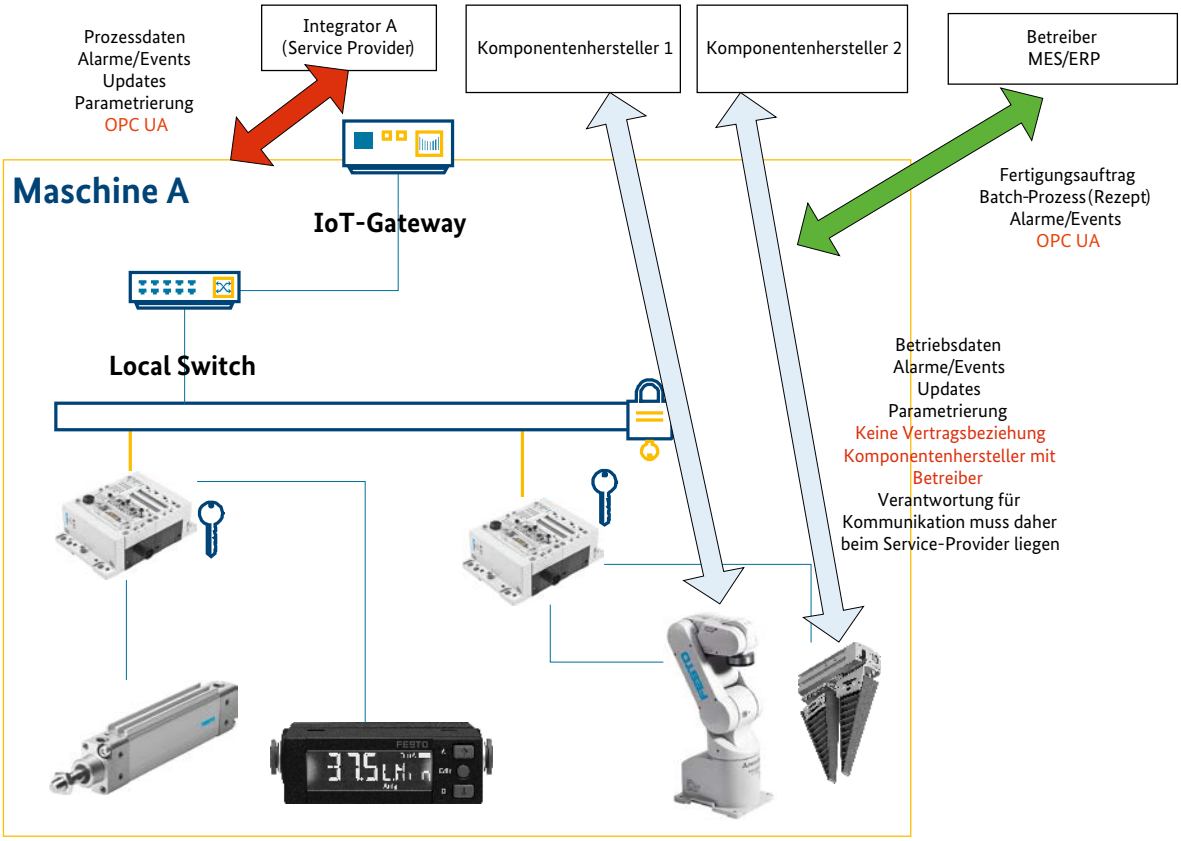
In einer erweiterten Betrachtung ist die Interaktion der Maschine mit einem externen Service-Provider zu berücksichtigen, in Abbildung 2 mit einem roten Pfeil gekennzeichnet. Dieser Service-Provider könnte der Integrator oder Maschinenbauer selbst sein, der je nach Ausprägung nur im Fernwartungsfall zugreifen würde, die Maschine passiv überwachen könnte („Condition Monitoring“) oder im Betreibermodell die Maschine sogar aktiv parametrieren

Abbildung 1: Gesamtszenario „Kollaborative Fabrik“



Quelle: Plattform Industrie 4.0

Abbildung 2: Logische Schnittstellen von Maschine A



Quelle: Plattform Industrie 4.0

könnte. Daraus erwachsende Besonderheiten, wie mögliche Anforderungen an die Überwachung der Kommunikation durch den Betreiber, werden in diesem Dokument jedoch noch nicht betrachtet. Auch weitergehende Möglichkeiten, wie individuelle Kommunikation einzelner Maschinenkomponenten mit deren Herstellern, werden nicht betrachtet.

Die in diesem Dokument vorgenommenen Betrachtungen beziehen sich auf die logischen Kommunikationsbeziehungen, also den Austausch der Informationen. Welche unterliegenden Übertragungstechniken zum Einsatz kommen (drahtgebunden, drahtlos, kurze oder weite Distanz), ist nicht Gegenstand der Überlegungen.

Anwendung von OPC UA im Szenario

Es wird weithin davon ausgegangen, dass OPC UA eine wesentliche Bedeutung in der vernetzten Industrie einnehmen wird, da der Austausch von Parametrierung, Betriebsdaten und Alarmen wesentliche Merkmale von OPC UA sind. Daher soll in dem vorliegenden Papier OPC UA für die Einbindung einer neuen Maschine in die Systeme des Betreibers verwendet werden. Die Einbindung der Maschine findet innerhalb eines lokalen Netzwerks statt, das sich in der Kontrolle des Betreibers befindet. Diese lokale Einbindung, die auf die Security-Domäne des Betreibers abzielt, steht im Mittelpunkt dieses Dokuments.

Die logische Anbindung an den externen Service-Provider findet über eine Fernverbindung statt. Hierbei ist es zum einen möglich, dass die Kommunikation physisch durch das Netzwerk des Betreibers und dann über das Internet zum Service-Provider läuft. Hierdurch können vorhandene Ressourcen effizient genutzt werden. Auch bietet diese Gestaltung dem Betreiber die Möglichkeit, die Kommunikation zu überwachen und zu beeinflussen. Ebenso ist eine dedizierte Anbindung über eine eigene Internet-Konnektivität denkbar, mit der Wechselwirkungen im Betreibernetzwerk reduziert werden. In jedem Fall wird eine Kommunikation zwischen der Security-Domäne des Betreibers

und der Security-Domäne des Service-Providers etabliert. Daher müssen die Security-Maßnahmen der Akteure abgestimmt und im jeweiligen Security-Managementsystem berücksichtigt sein, siehe technischer Überblick „Sichere unternehmensübergreifende Kommunikation“ (10). Diese Kommunikationsbeziehung wird in einem zukünftigen Nachfolgepapier behandelt werden.

In den folgenden Betrachtungen wird lediglich der sichere Einsatz von OPC UA diskutiert. Die Qualität der Umsetzung etwa durch einen Sicheren Entwicklungsprozess (Security Development Lifecycle, SDL) und weitergehende Security-Funktionen werden hier nicht betrachtet.

Lebenszyklus

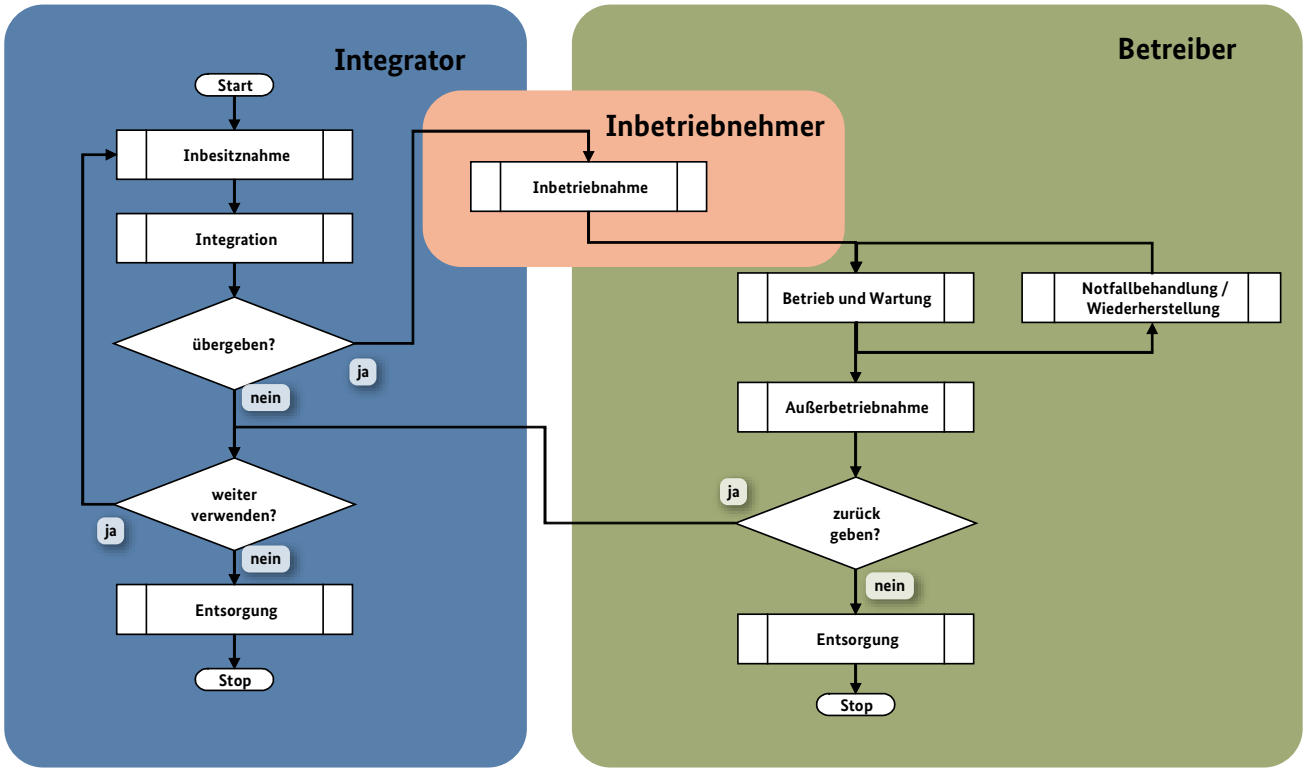
Um die Anforderungen der Beteiligten an die Security der zu integrierenden Maschine analysieren zu können, wird der Lebenszyklus ausgehend von der Bereitstellung der notwendigen Komponenten bis zur Außerbetriebnahme der Maschine betrachtet (vgl. Abbildung 3). Die hier beleuchteten Phasen sind:

- Bereitstellung und Inbesitznahme einer Komponente
- Integration mehrerer Komponenten zu einem System (z. B. Maschine oder (Teil-)Anlage)
- Inbetriebnahme des Systems beim Betreiber
- Betrieb und Wartung
- Außerbetriebnahme des Systems oder Außerbetriebnahme von Systemkomponenten
- Entsorgung nach endgültiger Außerbetriebnahme

Die Analyse ist dabei grundsätzlich zuerst generisch, da die spezifischen Schutzziele der Beteiligten nicht bekannt sind. Es müssen also alle möglichen Anforderungen auf dem höchsten Security-Niveau beleuchtet werden, um sicherstellen zu können, dass alle notwendigen Schutzziele erreicht werden können. Außerdem ist die Betrachtung auf Anforderungsniveau unabhängig von verwendeten Technologien.

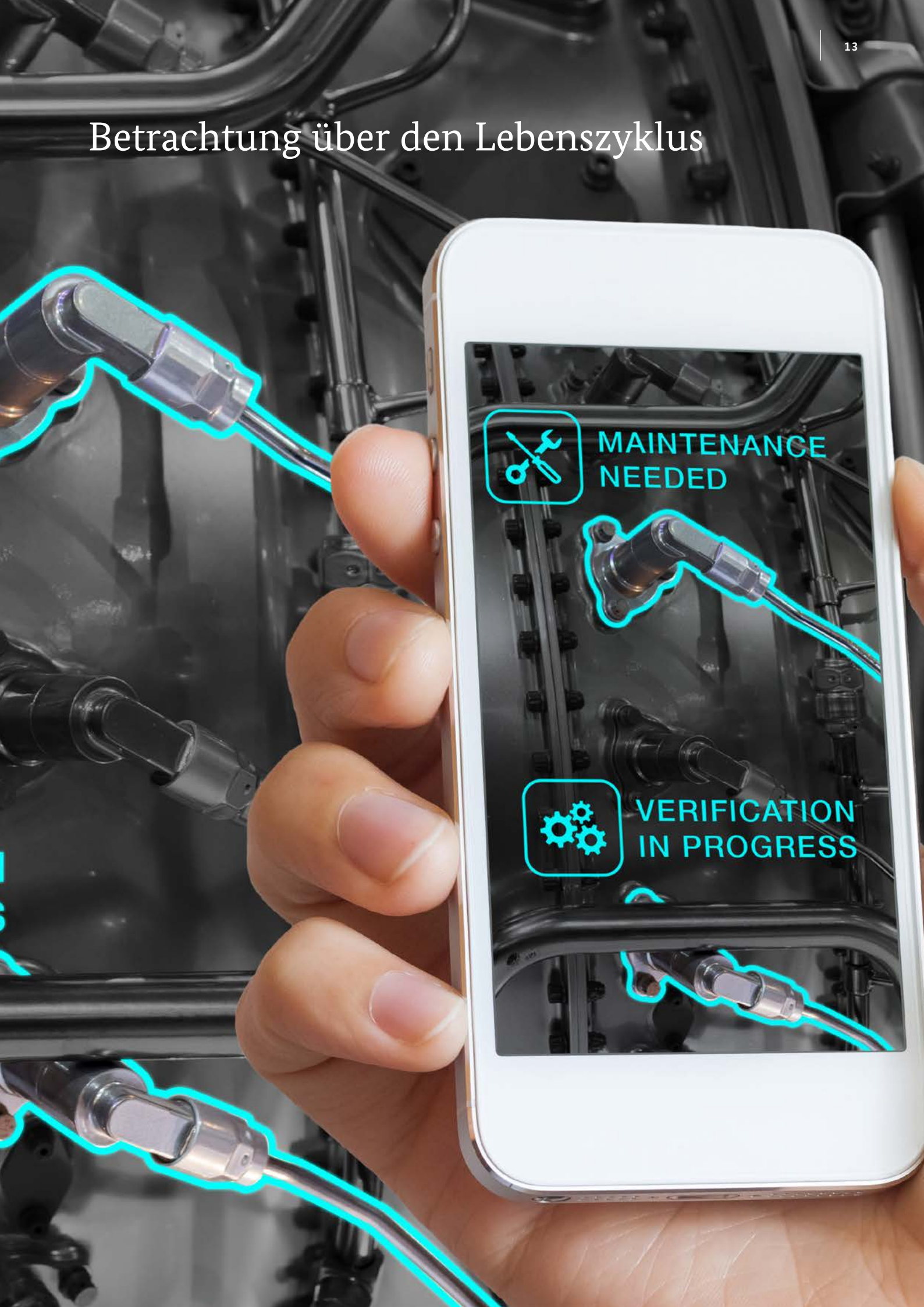
Eine Untersuchung des ersten Teils des Lebenszyklus, der Inbesitznahme und Integration von Komponenten zu einem System, findet sich bereits im Papier „Security der Verwaltungsschale“ (11).

Abbildung 3: Lebenszyklusphasen



Quelle: Plattform Industrie 4.0

Betrachtung über den Lebenszyklus



Die Betrachtung der Sicherheits-Anforderungen an eine Komponente erfolgt anhand der oben beschriebenen Phasen des Lebenszyklus zuzüglich eines Abschnittes für Notfall- und Betriebswiederherstellungsmaßnahmen.

Am Ende der Betrachtung einer jeden Phase werden in abstrakter Form die Security-Anforderungen zusammenfassend wiederholt, die im freien Text formuliert wurden.

Nach der Betrachtung wird eine Lösung skizziert, anhand derer deutlich wird, welche Anforderungen bereits mit Mitteln gemäß OPC-UA-Standard oder/und sinnvollerweise über andere übliche Maßnahmen erfüllbar sind und an welchen Stellen offene Punkte zur Diskussion sichtbar werden.

Schon während der Diskussion des Lebenszyklus wird der Bedarf von Identitäten aus verschiedenen Quellen offensichtlich. Damit sie auseinandergehalten werden können, sind hier vorweg die Quellen beschrieben, nämlich:

1. vom Komponentenersteller vergebene Identitäten (z. B. Herstellerzertifikate ZH_N),

2. vom Integrator vergebene Identitäten (z. B. Zertifikate ZI_N),

3. optional in der Anlage gültige Identitäten (z. B. Zertifikate ZA_N) und

4. vom Betreiber vergebene Identitäten (z. B. Zertifikate ZB_N).

Inbesitznahme

Unter Inbesitznahme einer Komponente ist der erste Einsatz bei einem Integrator oder direkt beim Betreiber zu verstehen. Der Integrator nimmt dabei eine generische Komponente und konfiguriert sie so, dass er eine ausschließliche Kontrolle über sie erlangt. Dies geschieht z. B. durch das Ersetzen von Default-Passwörtern oder das Aufspielen von Zertifikaten des Integrators. Abstrakt bezeichnet sind dies die Identitätsinformationen und Authentifizierungskriterien, anhand derer die Komponente die Identitäten ihrer Kommunikationspartner prüft.

Der erste Einsatz einer Komponente kann sich dabei sowohl auf eine fabrikneue Komponente beziehen als auch auf eine Komponente, die auf Werkseinstellungen zurückgesetzt wurde (und damit in ihrer Konfiguration einer fabrikneuen Komponente entspricht). Als Erstes muss sichergestellt werden, dass es sich bei der Komponente um ein Original handelt und dass keine Manipulation der Hard- und Software (auch Firmware) stattgefunden hat. Während bei Hardware die Authentizität durch physische Merkmale, wie z. B. Hologramme, geprüft werden kann, kann dies bei Software und Firmware durch Code-Signaturen erfolgen.

Zusätzlich oder alternativ kann die Echtheit der Komponente mitsamt ihrer Firmware auch über das Netzwerk geprüft werden. Das ermöglicht Arbeitsabläufe, bei denen unterschiedliche Personen für die physikalische Montage und die Inbesitznahme zuständig sind. Jede Komponente sollte dafür ein individuelles, vom Hersteller ausgestelltes Zertifikat besitzen. Das Gerät bestätigt dann mit der Verwendung des zugehörigen privaten Schlüssels, dass sich sein Zustand in einem vom Hersteller als authentisch definierten Zustand befindet. Um zu verifizieren, ob dieses Zertifikat gültig ist, gibt es zwei Möglichkeiten: 1.) Wenn das vom Hersteller ausgestellte Zertifikat von einer vertrauenswürdigen Wurzelinstanz (Root Certification Authority, kurz Root-CA) ausgestellt ist, muss die gesamte Zertifikatskette geprüft werden. 2.) Ist das Zertifikat individuell selbst signiert, so muss der Fingerabdruck (Finger Print) des Zertifikats separat vom Hersteller zum Vergleich bereitgestellt werden. Dieser Fingerabdruck muss über einen anderen Weg zum Kunden gelangen als die Komponente selbst, z. B. über die Veröffentlichung des Fingerprints auf der mit HTTPS gesicherten Webseite des Herstellers. Ein Mitsenden des Fingerabdrucks in der Anleitung der Komponente oder in einer Prüfsoftware auf einer CD im Lieferumfang ist zu unsicher, da ein Angreifer beide Stellen (Gerät und Dokumentation/Prüfsoftware) auf dem Lieferweg verändern kann.

Es sind Mischformen der beiden Varianten zum Prüfen des vom Hersteller ausgestellten Zertifikates denkbar. Zum Beispiel kann der Hersteller aus Kostengründen die Root-CA für die von ihm ausgestellten Gerätezertifikate selbst betreiben. In dem Falle muss er nur noch für das von ihm erstellte Root-Zertifikat den Finger Print über einen separaten Kanal bereitstellen. Der Finger Print ist dann für sehr viele Geräte gleich, zum Beispiel alle Geräte einer Serie oder gar alle Geräte des Herstellers.

Der zum öffentlichen Schlüssel (Public Key) des Zertifikats gehörige private Schlüssel (Private Key) muss unter Verschluss gehalten werden. Dies geschieht im Idealfall in sicherer Hardware, einem sogenannten „Secure Element“. Alle Operationen auf dem privaten Schlüssel finden dann in der sicheren Umgebung des „Secure Element“ statt. Um sicher-

zugehen, dass hier keine Manipulation stattgefunden hat, sollte, falls möglich, die Unversehrtheit des „Secure Element“ bei der Inbesitznahme überprüft werden. Auch hierfür gibt es über das Netzwerk durchführbare Verfahren.

Selbst wenn Gründe der Verwendung eines Secure Element entgegenstehen, erzeugt die Verwendung von asymmetrischen Schlüsselpaaren aus Public und Private Key hier einen Mehrwert an Sicherheit. Wenn eine Komponente nicht einmal über die Ressourcen für die Verwendung von asymmetrischen Schlüsselpaaren verfügt, können andere Komponenten als Vermittlungsstellen eingesetzt werden. Zum Beispiel kann in einem kleinen, relativ abgetrennten Bereich eine vermittelnde Komponente asymmetrische Schlüsselpaare verwenden und stellvertretend für die anderen Komponenten ohne Schlüsselpaare kommunizieren. Es wäre dann ratsam, die von dort weitergeführte Kommunikation zu den anderen Komponenten in einem Medium mit entsprechend beschränkten Zugriffsmöglichkeiten zu führen.

Ein wichtiger Bestandteil der Sicherheit einer Komponente ergibt sich aus deren sicherer Konfiguration. Im Auslieferungszustand einer Komponente sollte deren Default-Konfiguration so sicher wie möglich parametriert sein, um Angriffe während der Inbesitznahme oder unsichere Folgekonfigurationen durch Bedienfehler zu unterbinden. Dies wird auch als „Security by Default“ bezeichnet. Für die OPC-UA-Kommunikation wäre dafür zum Beispiel die Security-Policy None auszuschließen, also nicht anzubieten. Ist die höchste Sicherheitsstufe für einen Einsatzzweck nicht erforderlich, so sollte die Komponente gewährleisten, dass die Konfigurationsänderung nur autorisiert erfolgen kann, was ein Konzept für die Zugriffskontrolle mit abgestuften Rechten erfordert. Gleichfalls muss es möglich sein, die Konfiguration der Komponente wieder auf die (sicheren) Werkseinstellungen zurückzusetzen.

Als Security-Anforderungen an eine Komponente ergeben sich also folgende Punkte für die Inbesitznahme:

1. Die Echtheit der Komponente sollte anhand eines Zertifikates des Herstellers prüfbar sein.

2. Sämtliche Einstellungen der Komponente sollten sich auf den Auslieferzustand des Herstellers zurücksetzen lassen.

3. Die Grundkonfiguration sollte nicht unsicher gestaltet werden, sondern das Gerät sollte mit einer sicheren Konfiguration ausgeliefert werden, so dass während der Inbetriebnahme eine gleichzeitige Angreifbarkeit unwahrscheinlich ist.

4. Alle Authentifizierungskriterien der Komponente zur Prüfung anderer Identitäten sollten vom Integrator definiert werden können. Dies umfasst alle Passwörter und alle Zertifikate, denen die Komponente vertraut, ausgenommen von wenigen Zertifikaten, welche vom Hersteller zu besonderen Zwecken, wie der Authentifizierung von Firmware-Updates, gedacht sind.

Integration

Im Anschluss an die Inbesitznahme der Einzelkomponenten stellt der Integrator aus ihnen eine Gesamtfunktion her. Er setzt die Komponenten sowohl logisch als auch physisch in Beziehung und modelliert das für die Gesamtfunktion notwendige Verhalten der Einzelkomponenten. Die Vorgänge in diesem Schritt sind für die Sicherheit von besonderer Bedeutung, da sowohl die Beziehungen zwischen den Einzelkomponenten als auch die Funktion der Einzelkomponenten für den sicheren und korrekten Betrieb der sich aus ihnen ergebenden Maschine oder Anlage entscheidend sind. Insbesondere lassen sich folgende besonders sicherheitskritische Vorgänge in der Integrationsphase identifizieren:

a. Die Festlegung der digitalen Identitäten der jeweiligen Einzelkomponenten.

b. Die Modellierung und Umsetzung der Beziehungen der Komponente und anderer Entitäten, wie

    1. zu anderen Geräten und Software-Prozessen innerhalb und außerhalb der Maschine oder Anlage und

    2. zu in bestimmter Funktion agierenden Personen.

c. Die Einstellung (Parametrierung) der Zugriffskontrollmechanismen nach dem Modell der Beziehungen der Komponente zu anderen Entitäten.

d. Die Kontrolle des Zugriffs auf interne Geräteeigenschaften und Funktionen, mit dem Ziel des Schutzes der Geschäftsgeheimnisse, die der Integrator in die Maschine oder Anlage einbringt.

Bei der Inbeziehungsetzung einzelner Komponenten mit anderen Entitäten sind sowohl die Funktionen der Geräte als auch die sich daraus ergebenen Zugriffsrechte einzelner Geräte und Softwarekomponenten untereinander zu regeln. Eine wichtige Grundlage der Modellierung der Komponentenbeziehungen ist die Möglichkeit, die Komponenten eindeutig und sicher zu identifizieren und zu referenzieren. Dies kann auf Basis sicherer digitaler Identitäten (z. B. digitale Zertifikate und Hardwareunterstützung) geschehen. Die Zuweisung einer digitalen Identität zu einer Komponente kann entweder über eine Public-Key-Infrastruktur (Certification Authority und Vergabe von Zertifikaten) oder durch eine manuelle Konfiguration von zertifikatsbasierten Identitäten auf den jeweiligen Komponenten geschehen. Hierbei ist anzumerken, dass die Identitäten entweder innerhalb der Anlage selbst und/oder durch den Integrator vergeben werden. Würde für die Inbeziehungsetzung die Identität des Herstellers verwendet, ermöglichte das später einem Angreifer eventuell mit einem von ihm erworbenen und parametrierten Gerät, das ebenfalls ein gültiges Herstellerzertifikat besitzt, die Anlage durch einen Gerätetausch zu unterwandern.

Nachdem die Geräte mit einer sicheren Identität (Zertifikat ZI_N samt Public/Private Key) ausgestattet wurden, können Vertrauensbeziehungen zwischen diesen Geräten modelliert werden. Dies geschieht durch die Aufnahme der Identität eines Gerätes in die Vertrauensliste (Trust List) eines anderen Gerätes. Alternativ kann die Identität einer Certification Authority (CA), welche weitere digitale Identitäten beglaubigen kann, in eine Trust List einer Komponente aufgenommen werden. Durch die Alternative wird allen von der CA ausgestellten Identitäten vertraut und der Konfigurationsaufwand reduziert, weil die zu prüfenden Zertifikate von anderen Geräten nicht mehr explizit aufgenommen werden müssen. Die direkte Aufnahme von Identitäten in die entsprechenden Trust Lists bzw. die Aufnahme einer Certification Authority bestimmt, welche Komponenten der Integrator prinzipiell für eine Interaktion vorsieht. Jede Komponente sollte dabei so konfiguriert werden, dass sie mit einer minimalen Anzahl an anderen Komponenten interagieren kann. Dies reduziert die Möglichkeiten eines Angreifers nach der Kompromittierung einer einzelnen Komponente.

Nach der Konfiguration der erlaubten Kommunikationsbeziehungen muss eine weitere Modellierung der Zugriffsrechte der jeweiligen Komponenten geschehen. So wird der Integrator den Zugriff auf einzelne Werte einer Komponente für andere Komponenten oder andere Benutzer einschränken, um entweder Angriffe, Fehlbedienungen oder die Preisgabe von Firmengeheimnissen des Integrators zu unterbinden. Zugriffe auf Funktionen und Daten der Komponente sollten dabei so gestaltet werden, dass jeder Zugreifer (andere Komponente oder Benutzer) nur das Mindestmaß der für seine Funktionserfüllung notwendigen Zugriffsrechte erhält. Der Integrator legt diese Zugriffsrechte fest und wird sich in vielen Fällen das alleinige Recht vorbehalten, die Zugriffsrechte und Zugriffsbeschränkungen anzupassen und die Zugriffsrechte zu erteilen (einer Komponente oder Person zuzuweisen). Dies ist notwendig, da der Integrator sonst keine Beschränkungen zum Schutz der Funktion einer Maschine oder zum Schutz seiner eigenen Firmengeheimnisse (z. B. der exakten Konfiguration von Komponenten und deren Zusammenspiel) vorsehen kann. Weitere Rechte kann der Integrator dem späteren Betreiber einräumen, damit dieser die Maschine bestimmungsgemäß bedienen bzw. sie in die eigene Unternehmensinfrastruktur einbinden kann. Auf das Szenario bezogen bedeutet dies, dass der Integrator einigen Benutzern oder Komponenten des Betreibers lesenden Zugriff auf bestimmte Werte und Alarme ermöglicht. Dies ermöglicht die Überwachung der Maschine. Zusätzlich kann der Betreiber schreibenden Zugriff auf bestimmte Parameter der Maschine erhalten, um diese an die zu fertigenden Produkte anzupassen.

In komplexeren Anlagen und Maschinen, in denen eine Vielzahl von Zugriffsrechten ähnlich oder identisch für verschiedene andere Komponenten oder Personen konfiguriert werden muss, erleichtert eine rollenbasierte oder eine attributbasierte Rechtevergabe das Management dieser Zugriffsrechte. So können Rechte für eine Rolle (z. B. Wartungsmitarbeiter, Bediener, Überwachung, ...) definiert werden oder für Inhaber von Attributen (z. B. Zugehörigkeit zum Unternehmen und Zuständigkeit für die Wartung). Die Besonderheit dabei ist die Durchführung der Rechtespezifikation, ohne die spezifische digitale Identität bereits in der Integrationsphase festzulegen. Die Rollenzugehörigkeit oder die Attribute müssen dann über geeignete Maßnahmen im Betrieb (z. B. basierend auf einem zentralen Authentifizierungssystem in der Umgebung des Betreibers) einer Identität zugewiesen werden. So kann der Integrator bestimmte Interaktionsmuster vorsehen, die der Betreiber später einzelnen konkreten Identitäten zuweist.

Als Security-Anforderungen an eine Komponente ergeben sich also folgende Punkte für die Integration:

1. Der Komponente sollte eine integratorspezifische Identität mit zugehörigem Zertifikat ZI_N vergeben werden können.

2. Die Komponente sollte für die Kommunikation in der Anlage

   2.1 eine anlagenspezifische Identität samt Zertifikat ZA_N (welches die integratorspezifische Identität sein kann, aber nicht muss) eingestellt bekommen und verwenden können sowie

   2.2 eine anlagenspezifische Vertrauensliste eingestellt bekommen und verwenden können.

3. Die Komponente sollte für die Kommunikation mit Prozessen und Personen des Integrators die integratorspezifische Identität samt Zertifikat ZI_N verwenden können sowie eine integratorspezifische Vertrauensliste eingestellt bekommen und verwenden können.

4. Die Komponente sollte einen Zugriffskontrollmechanismus unterstützen, über den unabhängig von konkreten Identitäten Rechte definiert werden können.

5. Die Rechte in der Komponente sollten so einstellbar sein, dass auch die Veränderung von Rechten bestimmter Rechte bedarf.

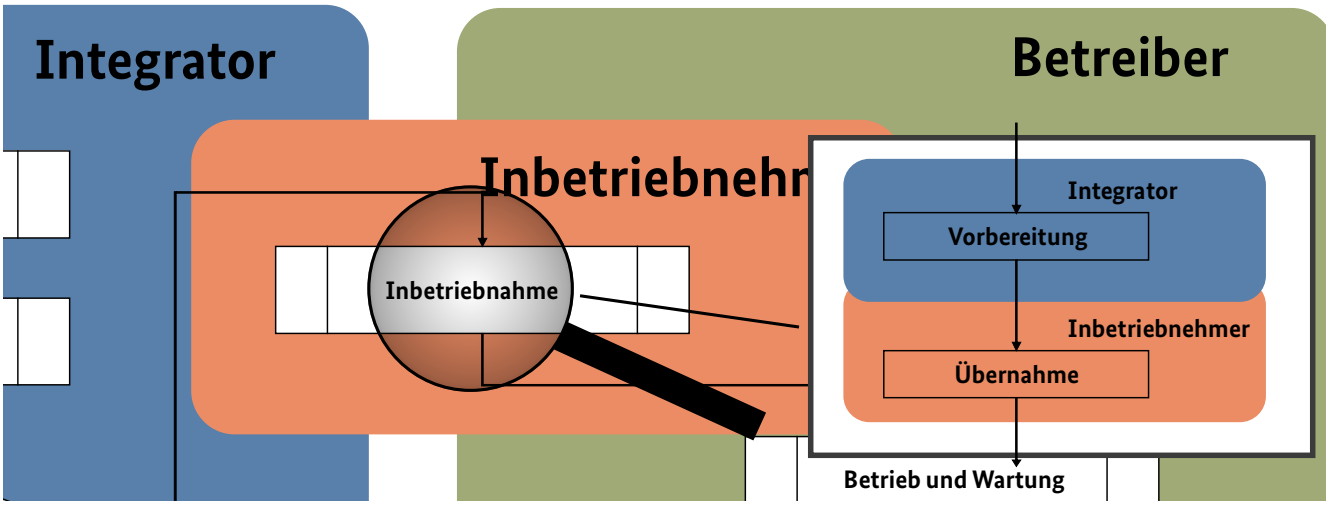
6. Die Rechte in der Komponente sollten so einstellbar sein, dass es bestimmter Rechte bedarf, um die Regeln der Rechtezuordnung zu Identitäten einzustellen.

Inbetriebnahme

Während der Inbetriebnahme findet ein Gefahrenübergang statt. Die vom Integrator erstellte Anlage geht vom Verantwortungsbereich des Integrators in den des Betreibers über. Die Inbetriebnahme kann in zwei Phasen unterteilt werden: In der ersten Phase bereitet der Integrator die Übernahme durch den Betreiber vor. In der zweiten Phase übernimmt der Betreiber die Anlage. Häufig wird auch der Teil der Übernahme durch den Betreiber von Personal des Integrators begleitet. Hier wird das Personal, welches die Übernahme durch, für oder mit dem Betreiber durchführt, als „Inbetriebnehmer“ bezeichnet. Dies geschieht unabhängig davon, ob dieses Personal nun dem Betreiber zugeordnet ist, ein Auftragnehmer des Betreibers ist oder Personal des Integrators ist, welches das Personal des Betreibers begleitet. Die Vorbereitung der Inbetriebnahme der Anlage wird durch den Integrator vorgenommen, die Übernahme wird durch den Inbetriebnehmer durchgeführt.

Mit der Inbetriebnahme wechselt nicht nur die Zuständigkeit für die Anlage. Häufig wechselt auch der Besitz daran (im hiesigen Szenario aber ohne Eigentumsübergang). Damit wird vor allem die Einbindung der Anlage in Security-Domänen verändert. Sie bestimmt schließlich zu einem Teil, wer oder was wozu auf die Komponenten zugreifen

Abbildung 4: Aufteilung der Inbetriebnahme in zwei Phasen



Quelle: Plattform Industrie 4.0

darf, und umgekehrt, mit wem oder was die Komponente kommunizieren darf. Andere Anteile dieser Rechte bestimmen die bereits in der Integration eingestellten Zugriffskontrollmechanismen mit ihren Möglichkeiten für Rechtezuordnungen.

Vorbereitung der Übergabe durch den Integrator

Die Vorbereitung der Übergabe an den Betreiber wird durch den Integrator vorgenommen.

Für das Beispiel-Szenario geschieht die Vorbereitung der Übergabe in der Reihenfolge der folgenden Schritte:

- Der Integrator definiert Zugriffsrechte für Wartungspersonal und Wartungsprozesse in Form von weiteren Rechten und Zuordnungsregeln. Dabei werden auch konkrete Zuweisungen der Rechte aktiviert, zum Beispiel indem Mengen von Identitäten mit konkreten Regeln zu Rollen zugeordnet werden. In einigen Anwendungsfällen ist es notwendig, dass zu diesen Rechten auch gehören muss, Software und Firmware der Anlage zu Anfang der Inbetriebnahme auf einen neuen Stand zu bringen. Der Lieferweg hat eventuell Wochen gedauert. In der Zwischenzeit können sich bei der Software und Firmware Neuerungen ergeben haben. Die dadurch entstehende Komplexität der Rechte – und wie deren Definition eine Erneuerung von Software und Firmware übersteht –, ist in diesem Papier nicht weiter diskutiert, sondern eher Aufgabe für ein Nachfolgepapier.

- Der Integrator hinterlegt und aktiviert in den Komponenten der Anlage Authentifizierungskriterien und Rechte für den Inbetriebnehmer, damit dieser bei der Übernahme durch die Anlage erkannt wird.

    - In vielen Fällen müssen diese Authentifizierungskriterien von der Anlage geprüft werden können, ohne dass eine funktionierende Einbindung in ein IT-Netzwerk besteht, weil die Anlage ja erst noch am neuen Ort in solch ein Netz integriert werden muss.

    - Außerdem ist die Arbeit des Inbetriebnehmers von einmaliger und vorübergehender Natur. Seine Arbeit ist getan, wenn die Anlage übernommen ist. Für die Wartung ist nicht der Inbetriebnehmer, sondern nach hiesigem Modell der Integrator zuständig. Entsprechend sollen nach den Grundsätzen der Zuordnung der geringsten notwendigen Rechte die speziellen Rechtezuordnungen für den Inbetriebnehmer nach erfolgter Arbeit wieder deaktiviert werden können. Seine Authentifizierungskriterien und Rechtezuordnungen sollten daher auch in der Anlage nur temporär vorhanden sein.

- Zuletzt entfernt der Integrator überflüssige Authentifizierungskriterien und Zugriffsrechte und -möglichkeiten, die er nach der Übergabe nicht mehr benötigt.

- Gegebenenfalls hat der Integrator in seiner Security-Domäne der Anlage und/oder ihren Komponenten Zugriffsmöglichkeiten und Rechte eingeräumt, die während einer Integration von Komponenten notwendig waren, zum Beispiel für einen Testbetrieb. Der Integrator sperrt oder löscht daher in seiner Security-Domäne überflüssige Zugriffswege und Rechte für die Anlage. Er löscht nicht die von ihm vergebenen Identitäten und zugehörigen Zertifikate ZI_N und sperrt sie auch nicht, sondern reduziert nur deren Zugriffsmöglichkeiten. Diese Identitäten können für die Fernwartung sinnvoll verwendet werden.

Als Security-Anforderungen an eine Anlage mit Komponenten der Industrie 4.0 ergeben sich also die folgenden Punkte aus der Vorbereitung der Inbetriebnahme:

1. Vom Integrator definierte, Authentifizierungskriterien, Rechte und Rechtezuordnungen (zu Rollen oder Attributregeln) für Wartungszugriffe sollten in der Anlage eingestellt werden können.

2. Vom Integrator sollten vorübergehend notwendige Authentifizierungskriterien und Rechte für den Inbetriebnehmer in der Anlage aktiviert werden können, so dass die Anlage bei Bedarf auch ohne Netzwerkverbindung den Inbetriebnehmer authentifizieren kann und die Rechtezuordnungen und Authentifizierungskriterien für den Inbetriebnehmer auch wieder entfernt werden können.

3. Der Integrator sollte überflüssige Zugriffswege, Authentifizierungskriterien und Rechte aus der Anlage löschen können.

Übernahme während der Inbetriebnahme

Während die Vorbereitung der Inbetriebnahme zum Beispiel vor der Verschiffung einer Anlage stattfinden kann, so findet die tatsächliche Übernahme dann bei diesem Beispiel nach der Verschiffung und dem physikalischen Aufbau der Anlage vor Ort statt.

Die Aufgabe des Inbetriebnehmers ist es, die Anlage vom Integrator zu übernehmen und am Standort des Betreibers so in Betrieb zu nehmen, dass der Betreiber nachfolgend im regulären Betrieb (ggf. nur von Wartung unterbrochen) die Anlage in gewünschter Weise zu seinem Nutzen betreiben kann. Hierfür verbindet der Inbetriebnehmer am Standort des Betreibers die Anlage mit der dortigen Umgebung. Dies umfasst neben physikalischen Anschlüssen auch die Anbindung an die Informationstechnologie des Betreibers, insbesondere die Aufnahme in bestimmte Security-Domänen:

- Zunächst prüft der Inbetriebnehmer die Authentizität und Integrität der Anlage zur Klärung der Frage, ob die Anlage vom Integrator stammt und in dem Zustand ist, wie sie der Integrator vorbereitet hat. Dies ist insbesondere notwendig, wenn die Anlage oder Anlagenteile zwischen der Vorbereitung und der Übernahme unter der Kontrolle von dritten Personen waren, zum Beispiel durch eine Spedition und deren Auftragnehmer transportiert wurden.

- Wenn die Anlage vertrauenswürdig ist, bringt der Inbetriebnehmer vom Betreiber erstellte Identitäten samt Zertifikaten ZB_N in die Anlage ein, um eine sichere Interaktion mit der Security-Domäne des Betreibers zu erlauben.

- Die Anlage und ihre Komponenten werden mit zwei Teilschritten in die Security-Domäne der Informationstechnologie des Betreibers aufgenommen.

    - Vom Betreiber bereitgestellte Authentifizierungskriterien werden in die Anlage und ihre Komponenten eingebracht.

    - Die Identitäten der Anlage und ihrer Komponenten werden mittels Freischaltung der zugehörigen Zertifikate in der Infrastruktur des Betreibers bekannt gemacht. Dabei wird für die Anlage die Möglichkeit eingerichtet, bei Bedarf die Zertifikate ZB_N zu erneuern, zum Beispiel rechtzeitig vor Ablauf der Gültigkeit. Auch erhält die Anlage die Möglichkeit, aktuelle Versionen der vom Betreiber ausgestellten Authentifizierungskriterien zu erhalten. Denn von Zeit zu Zeit muss der Betreiber eventuell neue vertrauenswürdige Wurzelzertifikate (Root-CA-Zertifikate) in den Betrieb einführen oder Sperrinformation verteilen, wenn andere Komponenten vor Ablauf ihres Zertifikates außer Betrieb genommen wurden.

- Der Inbetriebnehmer stellt in der Anlage die Authentifizierungskriterien für das Personal und die Prozesse des Betreibers ein. Besonders muss er dabei beachten, dass Rollen, Attribute und ihre Ausprägungen in der Security-Domäne des Betreibers eventuell ganz andere Namen oder Bezeichnungen tragen, als der Integrator vorausgesehen hat. Ein Serienmaschinenbauer wird ggf. gar keinen gemeinsamen Nenner für die Bezeichnungen finden, die bei seinen Kunden Anwendung finden. Also müssen vom Integrator vorgesehene Bezeichnungen innerhalb der Zugriffskontrollmechanismen der Anlage auf tatsächliche Bezeichnungen eingestellt werden können. Abbildungsregeln von tatsächlichen (externen) auf logische (interne) Bezeichnungen sind hierbei ein hilfreiches Mittel (mit extern ist außerhalb der Anlage und mit intern innerhalb der Anlage gemeint).

- Der Inbetriebnehmer testet zusammen mit dem Betreiber und dem in der Ferne arbeitenden Wartungspersonal den Fernwartungszugriff. Dabei erklärt er dem Betreiber auch den Zugriffsweg und die darüber wahrnehmbaren Rechte. Dieses bedeutet nicht, dass hier eine permanente und unbeobachtete Wartungsmöglichkeit aktiviert wird, sondern dass im Wartungsfall eine Authentifizierung und Autorisierung des Wartungspersonals vorhanden ist. In welcher Weise ein tatsächlicher Wartungszugriff später noch durch den Betreiber freigegeben werden muss, zum Beispiel durch einen Schlüsselschalter, hängt von dem Zweck der Anlage ab. Bei manchen Anlagen kann eine dauerhafte Überwachung durch den Integrator oder einen Dienstleister erwünscht sein, zum Beispiel im Rahmen von Predictive Maintenance oder Condition Monitoring. Wie oben schon während der Erklärung des Anwendungsszenarios erwähnt, ist für manchen Betreiber die Auditierbarkeit tatsächlich stattfindender Wartungszugriffe ein Thema. Doch dessen sichere Realisierung ist Gegenstand für eine Diskussion in einem späteren Papier.

- Nach erfolgter Abnahme der Anlage durch den Betreiber löscht der Inbetriebnehmer seine Zugriffsmöglichkeiten, die nun überflüssig sind.

Als Security-Anforderungen an eine Anlage mit Komponenten der Industrie 4.0 ergeben sich also die folgenden Punkte aus der Übernahme:

1. Es sollte geprüft werden können, dass die Anlage vom Integrator stammt und im vom Integrator definierten Zustand ist.

2. Es sollten Identitäten des Betreibers samt von ihm vergebenen Zertifikaten ZB_N in die Anlage eingebracht werden können, während die bisherigen Identitäten und zugehörigen Zertifikate (z. B. Zertifikate des Integrators ZI_N und Zertifikate der Komponentenhersteller ZH_N) erhalten bleiben.

3. Authentifizierungskriterien zu Identitäten von verschiedenen Security-Domänen sollten getrennt voneinander und gleichzeitig in der Anlage hinterlegt werden können.

4. Rechte sollten mit Bezug auf die Authentifizierungskriterien der Identitäten einer Security-Domäne in der Anlage eingestellt und gleichzeitig aktiviert werden können, damit die Anlage zwischen Betreiber und Integrator (für die Wartung) unterscheiden und die entsprechenden Rechte durchsetzen kann.

5. Tatsächlich vom Betreiber verwendete Bezeichnungen (externe Rollen, externe Attribute und ihre Ausprägungen) zu den Identitäten seines Personals und seiner Prozesse sollten in der Anlage auf Bezeichnungen abgebildet werden können, die durch den Integrator definiert wurden (interne Bezeichnungen).

6. Die vorübergehend in der Anlage eingestellten Zugriffsrechte und Authentifizierungskriterien bezüglich der Identitäten für den Zugriff des Inbetriebnehmers müssen gelöscht werden können.

Betrieb und Sicherheits-Wartung

In der Betriebsphase müssen in regelmäßigen Abständen die privaten Schlüssel und Zertifikate zur Authentisierung für OPC UA auf sicherem Weg gewechselt werden, zum Beispiel, wenn die kryptographischen Algorithmen durch den technischen Fortschritt oder durch Angriffe stetig unsicherer werden. Ein Wechsel kann im Fall der absehbaren kryptographischen Alterung von Methoden und Algorithmen geplant erfolgen, während ein Angriff, bei dem z. B. Private Keys entwendet wurden, einen schnellen und nicht langfristig planbaren Austausch verursachen. Es sind bei dem Wechsel grundsätzlich zu unterscheiden:

- Eine Komponente/ein Nutzer erhält einen neuen privaten Schlüssel und es muss ein neues Zertifikat erstellt werden.

- Eine Komponente/Nutzer hat ein neues Zertifikat erhalten und das Zertifikat soll berechtigt werden (um z. B. per OPC UA zu kommunizieren). Im besten Fall müssen die Authentifizierungskriterien (Vertrauenslisten) der anderen Komponenten dafür nicht aktualisiert werden. In manchen Fällen ist es notwendig, das neue Zertifikat in Verzeichnisdiensten zu hinterlegen oder gar ein zugehöriges neues Ausstellerzertifikat (Sub-CA-Zertifikat) über einen Verteilmechanismus an andere Komponenten zu verteilen.

- Die ausstellende Zertifizierungsstelle wird gewechselt und alle Komponenten müssen darüber informiert werden. Für einen Übergangszeitraum kann es daher Zertifikate aus mehreren Zertifizierungsstellen geben. Die Komponenten müssen dies unterstützen und akzeptieren.

Bei den Zertifikaten für Komponenten muss noch zwischen zwei Arten von Inhabern unterschieden werden. Die Zertifikate können entweder vom Betreiber oder vom Integrator stammen. Beide sind für ihre jeweiligen Zertifikate verantwortlich und müssen diese entsprechend der Gültigkeitsdauer austauschen. Für den Austausch müssen gar jeweils Zugriffsrechte definiert sein. Dazu muss die Komponente in der Lage sein, Rechte für die Erneuerung der Zertifikate unterschiedlichen Nutzerkreisen zuzuordnen. Analog gilt das für die Erneuerung der zu den Zertifikaten gehörenden Schlüsselpaare. Die Zuständigkeit für das Zertifikat bestimmt, wer die Erneuerung des Schlüsselpaares veranlassen kann.

Über die Zeit können sich Berechtigungen der Nutzer ändern. Es sollte daher möglich sein, die von den Komponenten genutzten Berechtigungen zu verändern bzw. Authentifizierungsserver zu wechseln. Auch hier ist wieder zwischen den unterschiedlichen Nutzerkreisen des Betreibers und Integrators zu unterscheiden, da die Zugriffsberechtigungen nicht gegenseitig überschrieben werden dürfen. Sogar Nutzerkreiszuordnungen sollten mit der Zeit änderbar sein, weil zum Beispiel Anpassungen bei Zuständigkeiten des Personals aufgrund von Änderungen der Organisationsstruktur notwendig werden oder Änderungen in der technischen Infrastruktur des Betreibers oder Integrators Änderungen bei den Prozessen erforderlich machen.

Bei dem Austausch der privaten Schlüssel und Zertifikate muss berücksichtigt werden, dass in manchen Anlagen oder Maschinen nur begrenzte Wartungsfenster zur Verfügung stehen. Daher sollte dies frühzeitig geschehen oder ohne eine Unterbrechung des Betriebs der Anlage möglich sein.

Wenn aus dem Bereich des Betreibers eine Verbindung zu der Anlage oder ihren Komponenten aufgebaut wird oder umgekehrt, sollte die Anlage mit einem Zertifikat ZB_N ihre Zugehörigkeit zum Betreiber nachweisen. Auch sollte die Anlage dabei das Zertifikat der Gegenstelle mit Kriterien des Betreibers prüfen, zum Beispiel einer Vertrauensliste (Trust List) aus Zertifikaten des Betreibers. Erst durch gegenseitige Verifikation entsteht hier eine sichere Verbindung. Wenn die Anlage oder ihre Komponenten eine Verbindung zum Integrator aufbaut oder umgekehrt, zum Beispiel zu Wartungszwecken, sind analog die Zertifikate und Kriterien des Integrators zu verwenden. Diese Regeln gelten ganz besonders für Verbindungen, in denen die Schlüssel und/oder Zertifikate regelmäßig erneuert werden.

Ein Grundsatz in der Security-Praxis ist, Risiken zu minimieren, indem für verschiedene Aufgabe auch verschiedene Schlüsselpaare verwendet werden. Wenn zum Beispiel ein Schlüsselpaar samt Zertifikat für die vertrauliche, also verschlüsselte, Kommunikation mit einer Komponente dient, sollte dasselbe Schlüsselpaar nicht für die Authentisierung der Komponente und auch nicht für durch die Komponente zu erstellende Signaturen verwendet werden, siehe hierzu auch Tabelle 7, Punkt 4 in der „Sicherheitsanalyse OPC UA“ des Bundesamtes für Sicherheit in der Informationstechnik (12). Verschiedene Risiken werden dadurch reduziert, welche sowohl in Security-Verfahren als auch in der organisatorischen Anwendung begründet sind. Wenn zum Beispiel dasselbe Schlüsselpaar für die vertrauliche Kommunikation und die Authentifizierung dient, kann bei manchen Authentifizierungsverfahren der Schlüsselinhaber, also die Komponente, dazu gebracht werden, eigentlich für sie gedachtes vertrauliches Material gegenüber anderen zu entschlüsseln. Denn manches Authentifizierungsverfahren besteht darin, dass die Komponente nachweisen muss, eine ihr unbekannte, aber mit ihrem öffentlichen Schlüssel verschlüsselte Zufallszahl entschlüsseln zu können. Wenn der Angreifer nun aber nicht eine verschlüsselte Zufallszahl neu erfindet, sondern eine andere für die Komponente gedachte vertraulich verschlüsselte Nachricht als Aufgabe wählt, erhält er die Entschlüsselung im Zuge des Authentifizierungsverfahrens quasi frei Haus.

Die Security-Praxis der Verwendung unterschiedlicher Schlüsselpaare für die Authentisierung und die Aushandlung von symmetrischen Schlüsseln für die Verschlüsselung von Nachrichten würde auch den Einsatz von sogenannten Middleboxen an Vertrauensgrenzen dahingehend unterstützen, dass der Nachrichtenverkehr durch Schlüsselhinterlegungsmaßnahmen oder Sub-CA-Instanzen in einer Middlebox mitgelesen werden kann, ohne dass die Authentizität des Nachrichtenverkehrs dadurch ebenfalls

kompromittiert ist. Denn für Middleboxen würden nur für die Entschlüsselung hinterlegte Schlüssel oder Sub-CA-Instanzen benötigt. Für die Authentisierung und damit Fälschung von Nachrichten müssten sie nicht ertüchtigt werden. Die Auditierbarkeit des über Vertrauensgrenzen hinweg stattfindenden Datenverkehrs ist Gegenstand für ein zukünftiges Papier. Dort wird der hier genannte Umstand wieder aufgegriffen.

Als Security-Anforderungen an eine Anlage mit Komponenten der Industrie 4.0 ergeben sich also die folgenden Punkte aus dem regulären Betrieb mit Wartung:

1. Identitäten und zugehörige Zertifikate sowie Schlüsselmaterial sollten

   1.1 unterbrechungsfrei erneuert werden können und

   1.2 je nach Aussteller auf unterschiedlichen Wegen erneuert werden können (Zertifikate des Integrators versus Zertifikate des Betreibers).

2. Authentifizierungs- und Autorisierungskriterien zu Identitäten sollten

   2.1 regelmäßig und

   2.2 getrennt nach Verantwortlichem erneuert werden können (Integrator versus Betreiber).

3. Beim Verbindungsaufbau zur Anlage oder ihren Komponenten oder in umgekehrter Richtung sollte ausgewählt werden können,

   3.1 welche Identität und welches Zertifikat relevant sind (Integrator versus Betreiber) und

   3.2 welche Prüfkriterien für das Verifizieren der Gegenstelle und deren Benutzer relevant sind.

4. Für die Verschlüsselung und Authentisierung/Signierung sollten unterschiedliche Schlüssel und Zertifikate verwendet werden können.

Außerbetriebnahme

Komponenten und Anlagen der Industrie 4.0 enthalten sensible Daten zum Beispiel in Form von Schlüsseln, Zugangsdaten und vertraulicher Information in Logdaten. Sensible Daten umfassen also nicht nur für die Security relevante Daten, sondern auch dem Datenschutz unterliegende Daten. Geraten die sensiblen Daten in falsche Hände, so stellt das für alle Kommunikationspartner eine Gefahr dar, weil zum Beispiel mit den Daten Aktionen veranlasst und eventuell weitere vertrauliche Daten erbeutet oder gar Sicherheitseinstellungen verändert werden können. Insbesondere wird es gefährlich, wenn ein Gerät kompromittiert oder gestohlen wird und seine sensiblen Daten nicht durch spezielle Hardwaremaßnahmen gesichert wurden.

Während für den ungeplanten Verlust (Diebstahl) die Sperrung der Identitäten der verlorenen Komponenten erfolgen muss, ist für die Außerbetriebnahme eine Löschung von sensiblen Daten vorzusehen. Verallgemeinert wird beides durch eine gesonderte Sicherheitsrichtlinie beschrieben: eine End-of-Life Policy. Diese Policy ist je nach Anwendungsfall zu definieren. So kann es individuelle Richtlinien für unterschiedliche Typen von Anlagen und/oder Komponenten geben.

Sicherheitsrichtlinien und die daraus abgeleiteten Sicherheitsprozeduren müssen definieren, welche Schritte durchzuführen sind, um ein Gerät sicher außer Betrieb zu nehmen oder nach Verlust zu sperren. Eine Außerbetriebnahme oder Sperrung kann entweder dauerhaft vorgesehen sein oder vorübergehend. Es kann vorgesehen sein, ein Gerät sicher von allen sensiblen Daten zu bereinigen, um es in einem anderen Kontext weiter zu verwerten oder sicher einer Entsorgung zuzuführen. Weiterhin ist zu definieren, wie das Gerät im Falle eines Defektes ersetzt werden kann, um die Systemfunktionalität weiter zu gewährleisten und die Informationen auf dem ausgetauschten Gerät zu löschen.

Die Fähigkeit von Software, sich Angriffen zu entziehen, nimmt über die Lebensdauer ab, da neue Gefahren entdeckt werden oder sich durch den technologischen Fortschritt ergeben. Im Zuge der Ersetzung sollte daher durch eine neue Risiko- und Gefahrenanalyse überprüft werden, ob vormals getroffene Sicherheitsentscheidungen noch ausreichen oder ggf. stärkere Absicherungen benötigt werden.

Als Security-Anforderungen ergeben sich für die Außerbetriebnahme die folgenden Punkte:

1. Sensible Daten sollten von Komponenten sicher gelöscht werden können.

2. In der jeweiligen Infrastruktur des Betreibers und des Integrators sollte der Zugriff teilweise oder komplett gesperrt werden können, für Komponenten bzw. ganze Anlagen.

3. Für temporäre Sperren sollten Sperren in der Infrastruktur des Betreibers und/oder des Integrators aktiviert und wieder aufgehoben werden können.

Entsorgung

Bei der Entsorgung ist sicherzustellen, dass bei einer vorhergehenden Außerbetriebnahme wirklich alle sensiblen Daten von den betroffenen Anlagenteilen und Komponenten gelöscht wurden. Die Sicherstellung ist nicht nur wegen der IT-Sicherheit, sondern auch wegen des Datenschutzes relevant, insbesondere wegen der Datenschutzgrundverordnung (EU-DSGVO). Im Zweifelsfall sind die Prozeduren aus der Außerbetriebnahme zum Löschen der sensiblen Daten zu wiederholen. Alternativ kann eine physikalische Zerstörung der Speicher mit sensiblen Daten vorgesehen werden. Für diese Phase sind also keine weiteren abstrakten Security-Anforderungen erfasst.

Notfallmaßnahmen/Betriebswiederherstellung

Aus dem Sichtwinkel der Security besteht ein Notfall, wenn im Betrieb einer Anlage festgestellt wird, dass aufgrund einer unautorisierten Manipulation der Anlage diese sich ggf. anders als vorgesehen verhält. In der Regel ist der Betreiber dadurch gehindert, die Anlage sicher oder effizient zu nutzen. Bei der Behandlung von Sicherheitsvorfällen auf einer Produktionsanlage entsteht damit ein Zielkonflikt: Einerseits muss die Ursache erforscht werden, um das Ausmaß des Schadens festzustellen und solchen Vorfällen zukünftig vorbeugen zu können, andererseits muss der Betrieb schnell wiederhergestellt werden, um die Folgeschäden (z. B. durch Produktionsausfall) zu minimieren. Da eine unautorisierte Manipulation in der Regel unvorhergesehen und damit zunächst unbekannt ist, kann oft die Ursache nur am manipulierten Objekt gefunden werden und die Untersuchung benötigt Zeit, in der die Wiederherstellung des Betriebes warten muss. Eine schnelle Wiederherstellung des Betriebes verwischt oft die Spuren, welche die nachträgliche Analyse der Ursache eines Security-Vorfalls ermöglichen.

Bewährt hat sich, für Security-Vorfälle eine Momentaufnahme von Daten und Zuständen der betroffenen Anlage zwecks späterer Analyse anzufertigen und anschließend schon vor dem Abschluss der Analyse die Daten und Zustände der Anlage wieder auf einen betriebsfähigen Stand zu bringen. Dieser Stand kann durch das Zurückspielen aus einer Sicherheitskopie von einem (vermutlich) noch nicht manipulierten Zustand erfolgen. Damit dies dem Betreiber möglich ist, muss er also in der Lage sein, Sicherheitskopien anzufertigen und diese auch wieder zurückzuspielen. Weiterhin muss er in der Lage sein, allein oder mit Hilfe des Integrators möglichst schnell eine Momentaufnahme anzufertigen. Sowohl beim Anfertigen und Zurückspielen von Sicherheitskopien als auch beim Anfertigen von Momentaufnahmen müssen sensible Daten geschützt bleiben. Weder dem Betreiber dürfen sensible Daten des Integrators (zum Beispiel Know-how der Anlagenapplikation) in die Hände gelangen noch umgekehrt (zum Beispiel private Schlüssel zu Zertifikaten des Betreibers oder auf Personal des Betreibers bezogene Logdaten).

Ein einfaches Zurückspielen einer sicheren Konfiguration ist nicht immer problemlos möglich, da zu diesem Zeitpunkt das Zielsystem sich in unsicherem und ggf. unbekanntem Zustand befindet. Von Fall zu Fall sind daher unterschiedliche Maßnahmen zu wählen (z. B. Konfigurations-Reset, Software neu aufspielen oder Komponente komplett austauschen).

Ein einfaches Zurückspielen eines ehemals sicheren Zustandes ist leider oft nicht hinreichend. Bei einem unautorisierten Zugriff könnten private Schlüssel zu Zertifikaten erbeutet worden sein. In solch einem Fall wäre es dem Angreifer sogar noch leichter als vorher möglich, wiederholt manipulierend einzugreifen – dieses Mal quasi nicht unterscheidbar von autorisierten Stellen, so dass nach einem einfachen Zurückspielen der falsche Eindruck des regulären Betriebs besteht, während tatsächlich weitere Angriffe erfolgreich sind. Deshalb müssen bei dem Verdacht auf Kompromittierung von solch sensiblem Datenmaterial wie privaten Schlüsseln sicherheitshalber neue Schlüsselpaare generiert und neue Zertifikate ausgestellt werden. Passwörter sind in solchen Fällen wesentlich schwieriger zu ersetzen, wenn ihre Vergleichswerte (die sogenannten Passwort-Hashes) auf den Geräten gespeichert sind. Deshalb sollte bei einer

auf Passwörtern basierten Authentisierung die Passwortprüfung gegen einen Authentifizierungsdienst erfolgen, wie zum Beispiel einen LDAP-Server, ein Active Directory oder ein Kerberos-System. Dort können Passwörter für ganze Bereiche erneuert werden.

Eine Vorbeugung gegen das unbefugte Manipulieren oder Kopieren von privaten Schlüsseln ist deren Verwahrung in Hardware-Sicherheitsmodulen (Secure Elements). In solchen Fällen müssen private Schlüssel und zugehörige Zertifikate nicht erneuert werden, solange die Hardware, also die Komponente samt Secure Element, noch unversehrt vorhanden ist. Denn ein Angreifer kann dieser dann nicht habhaft geworden sein. Die oben beschriebene Notwendigkeit, nach einem Angriff auch private Schlüssel und Zertifikate zu erneuern, kann entfallen. Eine weitergehende Betrachtung der Anforderungen an Secure Elements geschieht in diesem Papier nicht, da sie nicht Kern der Diskussion sind. Es sei nur darauf hingewiesen, dass wegen der Verwendung mehrerer Zertifikate und zugehöriger Schlüsselpaare, die im Zuge der Diskussion oben schon offensichtlich geworden ist, durchaus Anforderungen an Secure Elements zu diskutieren wären.

Für die Unterstützung der Betriebswiederherstellung und der Notfallmaßnahmen ergeben sich die folgenden Security-Anforderungen:

1. Momentaufnahmen von Daten (Logdaten, temporären Daten, ...) und Zuständen sollten von Anlagen und Komponenten zu Forensikzwecken angefertigt werden können, sodass darin kein sensibles Material enthalten ist und dennoch daran eine Analyse von Security-Vorfällen möglich ist.

2. Es sollte möglich sein, Sicherheitskopien von Anlagen und Komponenten so anzufertigen und zurückzuspielen, dass dabei in den Sicherheitskopien der Schutz von sensiblen Daten gewahrt bleibt und ein Zurückspielen die sensiblen Daten nur Komponenten in vertrauenswürdigem Zustand übergibt.

3. Ein schneller Austausch von Schlüsselpaaren und zugehörigen Zertifikaten sollte für Komponenten möglich sein, die vermutlich kompromittiert wurden.

4. Für Benutzer sollten Komponenten die Authentifizierung per Zertifikat unterstützen und/oder Passwörter gegen einen Authentifizierungsdienst prüfen.

Lösungsskizze/Diskussion

Das Ziel dieses Abschnitts ist es, Anforderungen und aktuell offene Diskussionspunkte aufzuzeigen und damit weitergehende Diskussionen zu der sicheren Anwendung des OPC-UA-Standards anzuregen. Gewollt sind Impulse zur Diskussion über die Anwendung des OPC-UA-Standards. Deshalb wird hier mit Absicht eine Lösung für eine Anforderung nicht weiter diskutiert, sobald sie gefunden und erwähnt wurde. Das Dokument stützt sich dabei sowohl auf den veröffentlichten OPC-UA-Standard (13) sowie weiterentwickelte Versionen seiner Teile. Der entsprechende Status ist an der jeweiligen Stelle referenziert. Die OPC Foundation hat zudem ein aktuelles Whitepaper (14) zum Thema veröffentlicht.

Im Folgenden werden mit je einer Tabelle je Phase des Lebenszyklus Lösungen skizziert, jeweils bezogen auf die einzelnen, oben erklärten Security-Anforderungen der Phase. Bei der Beschreibung der Lösungsskizzen sind zwei Farben für den Text gewählt, die eine schnelle Erfassung ermöglichen sollen: Ein Text in der Farbe Grün bedeutet, dass zumindest eine Lösung basierend auf etablierten Standards oder üblichen Technologien skizziert ist. Texte in der Farbe Blau sollen auf offene Diskussionspunkte hinweisen.

Vorwegnahme wiederholender Skizzen

Bevor auf die einzelnen Security-Anforderungen Bezug genommen wird, werden einige wiederkehrende Lösungsskizzen anhand einer Übersicht erklärt.

Anhand der Security-Anforderungen ist zu erkennen, dass aus verschiedenen Quellen digitale Identitäten benötigt werden. Zur Erinnerung sind hier die verwendeten Begriffe für die Quellen und Identitäten wiederholt:

1. vom Komponentenersteller vergebene Identitäten (z. B. Herstellerzertifikate ZH_N),
2. vom Integrator vergebene Identitäten (z. B. Zertifikate ZI_N),
3. optional in der Anlage gültige Identitäten (z. B. Zertifikate ZA_N) und
4. vom Betreiber vergebene Identitäten (z. B. Zertifikate ZB_N).

Security-Domänen

Die Quellen von Identitäten stimmen mit den verschiedenen Security-Domänen überein, von denen besonders zwischen der Security-Domäne des Integrators und der Security-Domäne des Betreibers unterschieden wird. Die verschiedenen Domänen und ihre Verortung zeigt Abbildung 5 auf der nächsten Seite. Dabei wird auf die Darstellung der Security-Domäne des Herstellers der Übersichtlichkeit halber verzichtet. In der Abbildung ist eine Security-Domäne „SD-I“ für den Integrator gezeigt. Mit „SD-A“ ist eine Security-Domäne innerhalb der Anlage bezeichnet. Die Domäne für den Betreiber trägt die Bezeichnung „SD-B“.

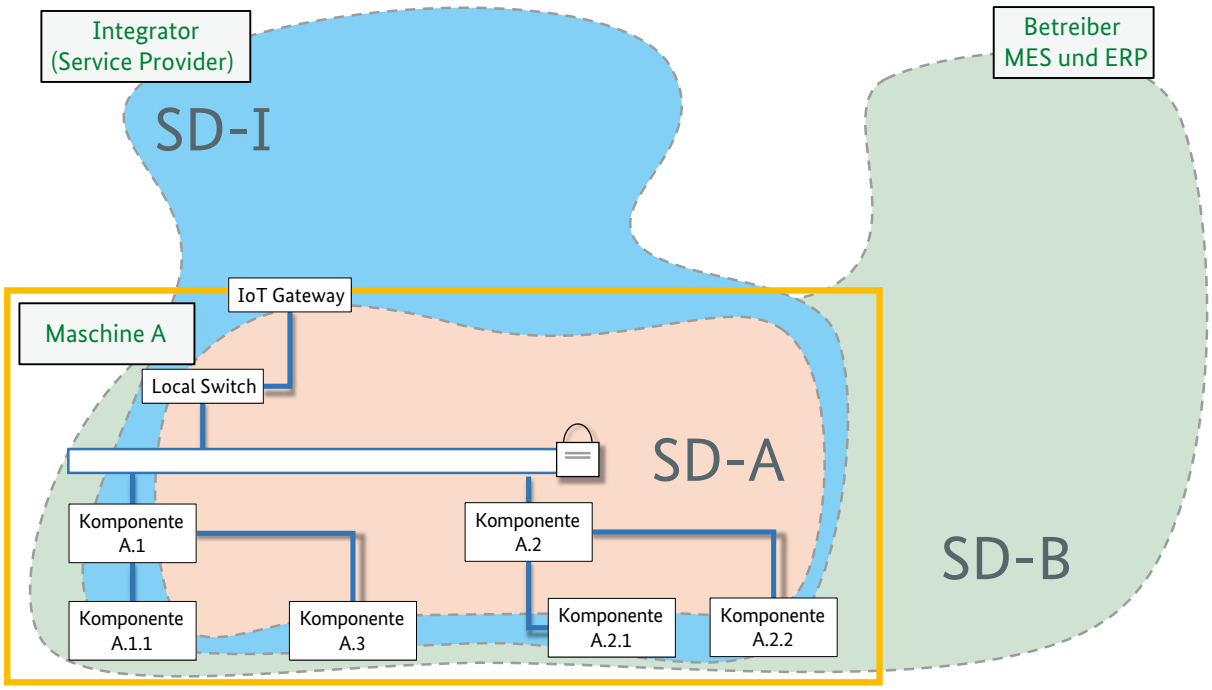
Versorgung mit Authentifizierungskriterien (z. B. Vertrauenslisten)

Mit dem Teil 12 des OPC-UA-Standards (15) werden zwei Mechanismen für das automatische Verwalten von Zertifikaten (Certificate Management) definiert:

- Mit dem „Pull-Management“ kann eine OPC-UA-Applikation sich regelmäßig verschiedene Vertrauenslisten (Trust Lists) von einem OPC-UA-Server holen, der im Standard als Gobal Discovery Server (GDS) bezeichnet wird. Im Standard wird ein Informationsmodell (Sammlung von Objekten, deren Typen und Methoden) definiert, welche ein Interface im GDS beschreiben, über das OPC-UA-Applikationen das „Pull-Management“ durchführen können. Sie kopieren sich damit regelmäßig die Vertrauenslisten.

- Der zweite Mechanismus ist als „Push-Management“ bezeichnet und definiert ein Informationsmodell für OPC-UA-Applikationen, die ein OPC-UA-Server sind. Über dieses Interface kann eine Management-Applikation die Vertrauenslisten vom GDS nach einem Zeitplan im Ziel-Server aktualisieren, also dorthin kopieren. Die Management-Applikation arbeitet in beide Richtungen als OPC-UA-Client, sowohl zum GDS als auch zum Ziel-Server. Wo die Management-Applikation läuft, definiert der Standard nicht. Denkbar ist, dass diese Applikation in der Nähe des GDS angesiedelt ist und mehrere OPC-UA-Server mit neuer Information für Vertrauenslisten versorgt. Genauer wird im Standard für einen Server mit Fähigkeit zum „Push-Management“ definiert, dass im Ziel-Server ein Objekt namens „ServerConfiguration“

Abbildung 5: Verortung der Security-Domänen am Beispiel von Maschine A – ohne Domäne des Herstellers



Quelle: Plattform Industrie 4.0

existieren muss, unter dem verschiedene Zertifikatsgruppen referenziert werden, wobei jede Gruppe eine Vertrauensliste (Trust List) umfasst.

Eine Vertrauensliste umfasst bei OPC UA genau die erforderliche Information zum Prüfen von Zertifikaten einer Security-Domäne in Form von vertrauenswürdigen Zertifikaten (Trusted Certificates), optional zusätzlichen Zertifikaten zur Vervollständigung von Zertifikatsketten (Issuer Certificates) und optional Sperrinformation. OPC UA definiert im Standard (über die Zertifikatsgruppen) gleich zwei Arten von Vertrauenslisten, solche zur Prüfung von Applikationszertifikaten und solche zur Prüfung von Benutzerzertifikaten. Diese Separation passt zu den oben genannten Security-Anforderungen.

Die nachfolgend beschriebenen Lösungsskizzen verfolgen den Ansatz, dass die Verwendung der beiden Verfahren des Certificate Managements über OPC UA und Global Discovery Server (GDS) dazu dient, in jeder Security-Domäne mit einem GDS und dahinterliegenden Certification Authorities (CAs) alle Komponenten oder relevanten Anlagenteile mit Kopien der Vertrauenslisten zu versorgen. Dabei können mehrere CAs eine Rolle spielen:

- eine CA für Geräte und Software-Prozesse und
- optional eine CA für Benutzeridentitäten.

Entsprechend sind die Vertrauenslisten zu verwalten:

- eine Vertrauensliste für Geräte und Software-Prozesse, ausgestellt von derzugehörigen CA, und
- optional eine Vertrauensliste für Benutzeridentitäten, ausgestellt von der dazugehörigen CA.

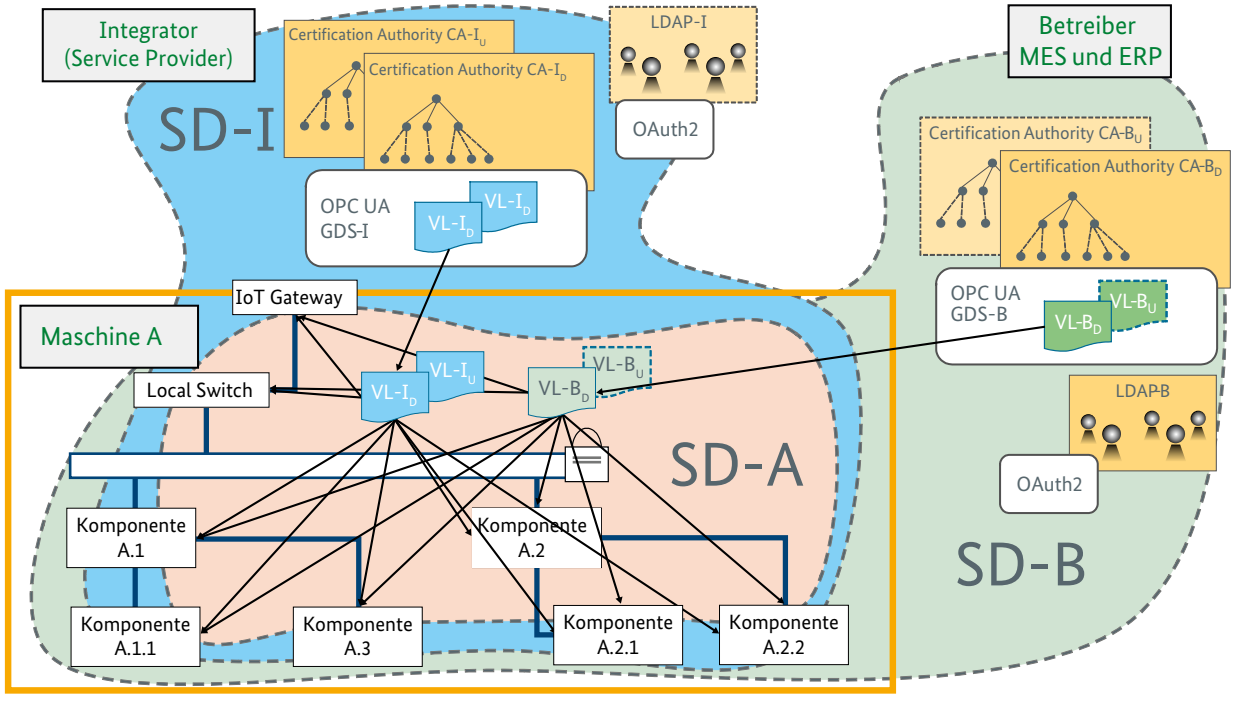
Es ist durchaus möglich, dass diese Information auch auf anderen Wegen verteilt wird. Der Ansatz trägt der bereits einleitend mit der Bedeutung von OPC UA erklärten Anforderung Rechnung, möglichst wenig zusätzlich zu OPC UA vorzuschlagen.

Anstatt der Verwendung eines Satzes von Vertrauenslisten je Security-Domäne wäre auch denkbar, innerhalb eines GDS denselben Satz von Vertrauenslisten für verschiedene Domänen bereitzustellen. Dann entstünde allerdings die Frage nach der Zuständigkeit der Pflege der Security-Domäne. Sobald weitere Security-Domänen zum Beispiel durch Zulieferer in ein Szenario mit aufgenommen werden, wird klar, dass eine solche gemischt verwaltete Vertrauensliste eher mehr Komplexität einführt als der Sache hilft. Ähnlich ist es möglich, in einer Vertrauensliste nur Teile einer Zertifizierungshierarchie einer anderen Certification Authority aufzunehmen, zum Beispiel um bestimmte Werksteile einer anderen Security-Domäne als vertrauenswürdig zu deklarieren. Hier entsteht ebenfalls die Notwendigkeit der Abwägung zwischen der Komplexität der Zuständigkeitsfragen und der technischen Vereinfachung in Form der Reduktion von zu verteilenden Vertrauenslisten. In diesem Papier werden die organisatorisch komplexeren Verfahren nicht weiter betrachtet, sondern die Lösungsansätze beschreiben vereinfachend den Ansatz streng getrennter Vertrauenslisten je Security-Domäne.

Seit der im November 2017 freigegebenen Version 1.04 beschreibt der OPC-UA-Standard in den Teildokumenten „Services“ (16) und „Mappings“ (17) neue Möglichkeiten zum Authentifizieren von Benutzern, zum Beispiel die Verwendung von OAuth2 mit JSON-Web-Tokens zur Prüfung von Passwörtern, deren Prüfkriterien in einem LDAP-Server hinterlegt sein können.

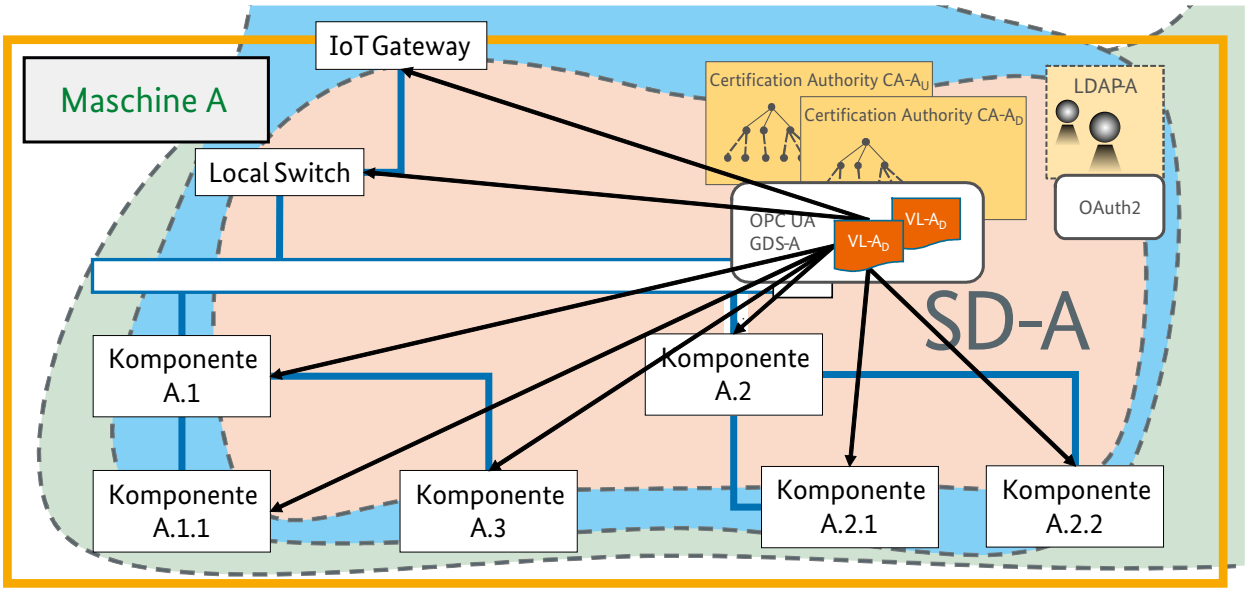
Die Versorgung der Anlage mit verschiedenen Vertrauenslisten, eigenen Zertifikaten und Passwortprüfkriterien ist in der Abbildung 6 unten am Beispiel der Security-Domänen SD-I und SD-B dargestellt. Vertrauenslisten und eigene Zertifikate werden von jeder per OPC UA kommunizierenden Komponente benötigt. Bei komplexeren Anlagen macht es Sinn, die Vertrauenslisten aus einer Domäne jeweils einmal regelmäßig in die Anlage zu kopieren und dort weiter zu verteilen, zum Beispiel mit einem lokalen OPC-UA-Server, der in der Anlage gegenüber den Komponenten als GDS-Proxy mit Cache dient. Dieses Konzept soll hier nur skizziert und nicht weiter diskutiert werden. In der Abbildung 6 ist in der Security-Domäne SD-I die Certification Authority (CA)

Abbildung 6: Versorgung mit (Kopien) von Vertrauenslisten und Passwortprüfinformation



Quelle: Plattform Industrie 4.0

Abbildung 7: Versorgung mit (Kopien) von Vertrauenslisten und Passwortprüfinformation



Quelle: Plattform Industrie 4.0

für die Geräte und Software-Prozesse als CA-I_D und die CA für die Benutzer als CA-I_U dargestellt. Über den GDS namens „GDS-I" werden die zugehörigen Vertrauenslisten VL-I_D und VL-I_U, bereitgestellt und verteilt. Für die Domäne SD-B geschieht dies analog von den CAs namens CA-B_D und CA-B_U aus mit den Vertrauenslisten VL-B_D und VL-B_U über den GDS-B.

Anhand der Abbildung 6 oben ist auch verbildlicht, dass statt Zertifikaten für die Authentisierung von Benutzern Passwörter verwendet werden können. Neben einer herkömmlichen Methode, der Verwendung von lokal in Komponenten konfigurierten Passwörtern und zugehörigen Prüfkriterien (Tabellen mit Benutzernamen und Passwörtern), beschreibt der OPC-UA-Standard wie oben erwähnt die Verwendung von OAuth2 als Netzwerkverfahren zur Authentifizierung von Benutzern. Lokal konfigurierte Passworttabellen haben Nachteile, die schon mit der Betrachtung des Lebenszyklus diskutiert wurden. Die Verwendung von OAuth2 hat auch Nachteile: Neben OPC UA benötigt man bei der Verwendung von OAuth2 ein weiteres Protokoll und verursacht einen Ausfall der Benutzerauthentifizierung, wenn der oder die OAuth2-Server nicht verfügbar sind. Zertifikate für Benutzer erlauben hingegen, für eine Überbrückungszeit ohne aktuelle Replikation von Vertrauenslisten dennoch neue Authentifizierungsvorgänge durchzuführen. In der Hauptsache bildet veraltete Sperrinformation hierbei das Limit für die überbrückbare Zeit. Wie lange Sperrinformation verwendet werden kann, definiert in der Regel die Certification Authority.

Keine Security-Domäne muss (kann aber) beide Methoden der Benutzerauthentifizierung unterstützen, per Zertifikat und/oder per OAuth2. In der Abbildung 6 ist beispielhaft in der Domäne SD-I ein LDAP-Server namens „LDAP-I" mit vorgeschaltetem OAuth2-Mechanismus und in der Domäne SD-B analog ein LDAP-Server namens „LDAP-B" dargestellt. Eine Replikation von Passwortprüfinformation findet hier nicht statt, sondern eine indirekte Kommunikation mit den OAuth2-Servern.

Dass auch innerhalb einer Anlage in der Security-Domäne SD-A eine Certification Authority Vertrauenslisten verteilen kann, ist mit der Abbildung 7 unten als Beispiel dargestellt. Dabei sind die Certification Authorities, der LDAP-Server und die Vertrauenslisten analog zu den vorherigen Beispielen bezeichnet.

Versorgung mit Identitäten (Zertifikaten und Schlüsselpaaren)

Für das Pull-Management und das Push-Management erklärt der Teil 12 des OPC-UA-Standards „Discovery“ (15) nicht nur die Versorgung mit Kopien von Vertrauenslisten, sondern auch die Versorgung mit digitalen Identitäten in Form von asymmetrischen Schlüsselpaaren und zugehörigen Zertifikaten. Über beide Verfahren kann sich eine OPC-UA-Applikation mit der benötigten Anzahl Zertifikate versorgen (Pull-Management) beziehungsweise darüber versorgen lassen (Push-Management). Der Applikation ist dabei überlassen, ob sie das zugehörige Schlüsselpaar selbst generiert oder von der versorgenden Stelle erhält. Dies ist ideal für die Unterstützung kryptographisch schwacher Geräte, die nicht über Quellen für gute Zufallszahlen für die Schlüsselgenerierung verfügen. Gleichzeitig werden Geräte unterstützt, die ein Secure Element für die Generierung und den Schutz von Schlüsselpaaren und besonders dem Private Key besitzen, wie zum Beispiel Geräten mit Trusted Platform Modul (TPM), wie dies bei den meisten PC-Plattformen heute schon der Fall ist.

Der OPC-UA-Standard erlaubt es, dass ein OPC-UA-Client im Zuge eines sicheren Verbindungsaufbaus wählen kann, welches Zertifikat er gegenüber dem Server verwenden möchte. Ein OPC-UA-Server kann mehrere Endpunkte anbieten und für jeden Endpunkt (Endpoint) ein Zertifikat samt Schlüsselpaar definieren, das er dafür verwendet. Verwendet ein OPC-UA-Server mehrere Endpoints, so ist er dennoch ein einzelner Prozess innerhalb eines Betriebssystems. Intern lassen sich hinter jedem Endpoint derselbe Adressraum sowie leicht oder völlig unterschiedliche Adressräume darstellen, also Mengen von Knoten und ihren Referenzen. Der OPC-UA-Server bleibt eine einzige OPC-UA-Applikation. Wenn ein Client zu einem Server eine Verbindung aufbaut, gibt der Client dem Server gegenüber den URL des Endpoints an, mit welchem sich der Client verbinden möchte.

Die Lösungsskizzen hier setzen voraus, dass ein OPC-UA-Server innerhalb einer Anlage genauso viele Endpoints anbietet, wie er Kommunikationsbeziehungen in Security-Domänen unterstützt. Eine Komponente mit einem OPC-UA-Server, der sowohl innerhalb der Anlage, mit dem Betreiber als auch mit dem Integrator kommunizieren können soll, hat also drei Endpunkte, jeweils einen für die Domänen SD-A, SD-I und SD-B. Für jeden dieser Endpunkte verwendet er ein Zertifikat, das er über den GDS der jeweiligen Domäne erhalten hat. Analog erhalten die OPC-UA-Clients aller Komponenten der Anlage ihre Zertifikate über den GDS der jeweiligen Domäne. Dafür notwendige Kommunikationsbeziehungen sind bereits mit Abbildungen in der vorhergehenden Diskussion dargestellt.

Autorisierung von Kommunikations- und Interaktionspartnern (Partnern)

Während der Betrachtung des Lebenszyklus oben ist bezüglich der Autorisierung von Benutzern etwas umständlich von Zugriffskontrollmechanismen und Autorisierungskriterien, wie zum Beispiel Rollen und Rechten sowie alternativ von Attributen und Regeln, gesprochen worden. Diese Umständlichkeit hat ihre Ursache darin, dass inzwischen unterschiedliche Konzepte in unterschiedlichen Standards zu finden sind.

Rollenbasierte Zugriffsmechanismen (Role Based Access Control, kurz RBAC) sind zum Beispiel

- im OPC-UA-Standard ab der im November 2017 freigegebenen Version 1.04 als Option für OPC-UA-Server in den Teilen „Address Space Model“ (18) und „Information Model“ (19) beschrieben.
    - Server-Hersteller können frei entscheiden, ein anderes Verfahren zu implementieren.
    - Der OPC-UA-Standard beschreibt nicht nur die Wirkung von Rollen und Rechten im OPC-UA-Server, er definiert auch
        - ihre Darstellung gegenüber Clients und Benutzern, welche diese Information einsehen dürfen,
        - Erweiterungen des Informationsmodells zur Veränderung von Rechte- und Rollenzuordnungen auf den einzelnen Knoten im Adressraum des Servers,
        - einen Mechanismus (IdentityMappingRuleType) zur Abbildung von Identitäten von OPC-UA-Clients und Benutzern anhand von
            - Attributen von Benutzern aus ihren Authentisierungs-Tokens (z. B. Attributen aus ihrem JSON-Web-Token wie ihrer Gruppen- oder Rollenzugehörigkeit),
            - ihren Zertifikaten,
            - dem für die Kommunikation ausgewählten Endpunkt und
            - bestimmten Kombinationen davon.

- Im Teil 4-1 der IEC 62443 (4) wird für Komponenten mit der Anforderung CR 2.1 und deren Erweiterung RE2 definiert, dass sie die Durchsetzung der Autorisierung für menschliche Benutzer auf Rollen basieren muss und die Zuordnung von Rollen zu menschlichen Benutzern direkt festlegbar oder modifizierbar sein muss, oder über Ausgleichsmechanismen der IT-Sicherheit.

- Im Standard IEC/TS 62351-8 (20), der für die Energiewirtschaft verbindlich ist, wird für die Autorisierung beim Datenaustausch mit Geräten für die Energiewirtschaft festgelegt, dass die Autorisierung auf einem rollenbasierten Zugriffskontrollsystem implementiert sein muss.

Attributbasierte Zugriffskontrollsysteme (Attribute Based Access Control, kurz ABAC) hingegen sind vergleichsweise jung und in der Industrie noch wenig verbreitet. Eine technisch fundierte Definition ist beispielsweise in der NIST SP 800-162 „Guide to Attribute based Access Control ...“ (21) zu finden. ABAC-Systeme können als Übermenge von RBAC-Systemen gesehen werden, wobei anstatt direkter Zuordnungen zwischen Identitäten und Rollen Regelsätze verwendet werden können, um komplexe Abbildungsfunktionen zwischen Attributwerten, die einer Identität, Objekten oder der Umgebung zugeordnet sind, und den Rollen zu definieren, denen Rechte zugeordnet sind. Ein Stück weit geht der OPC-UA-Standard schon in die Richtung ABAC, weil er bereits Abbildungsregeln zwischen Attributen aus einem Authentisierungs-Token und zugeordneten Rollen beschreibt.

Wegen der Verbreitung von RBAC in den einschlägigen industriellen Standards wird in den hiesigen Lösungsskizzen auf die im OPC-UA-Standard beschriebene rollenbasierte Zugriffskontrolle referenziert.

Inbesitznahme

Anforderung	Erfüllbar durch/Offener Diskussionspunkt
1. Die Echtheit der Komponente sollte anhand eines Zertifikates des Herstellers prüfbar sein.	Der von der OPC Foundation herausgegebene Companion-Standard „Devices“ (22) erklärt ein Informationsmodell für die Beschreibung von Geräten. Darin ist eine Echtheitsprüfung von Geräten noch nicht vorgesehen. Ein dedizierter, immer vorhandener „Endpoint“ im OPC-UA-Server einer Komponente, der hier Hersteller-Endpoint genannt werden soll, könnte ein Zertifikat des Herstellers ZH_N direkt zur Authentisierung des Servers gegenüber Clients verwenden. Allein mit solch einem Endpunkt kann die „Echtheit“ der Hardware nicht nachgewiesen werden. Als Kommunikationsprotokoll und Informationsmodell mit Sicherheitseigenschaften kann OPC UA hierbei aber unterstützen. Eine Erweiterung des „Hersteller-Endpoints“ um per OPC UA aufrufbare Methoden und abrufbare Objekte wäre möglich, die einen Nachweis über die Integrität und Authentizität der Hardware und Software der Komponente geben. Dies wird im Bereich des „Trusted Computing“ als „Remote Attestation“ bezeichnet und basiert in der Regel auf Hardware-Sicherheitsmodulen (Secure Elements). Statt der komplizierten Remote Attestation wäre auch denkbar, dass das Gerät den privaten Schlüssel für den o. g. Endpoint nur bei integrer Hard- und Software nutzen kann, ein Secure Element den privaten Schlüssel also nur freigibt, wenn ein sicherer Startvorgang (Trusted Boot/Secure Boot) erfolgte. Aus Sicherheitsgründen sollte der „Hersteller-Endpoint“ nicht die volle Funktionalität des Gerätes zugänglich machen, sondern ideal nur zur Echtheitsprüfung und Inbesitznahme des Gerätes dienen, damit das Vergeben eines spezifischen Zertifikates durch den Besitzer erforderlich bleibt[3].
2. Sämtliche Einstellungen der Komponente sollte sich auf den Auslieferzustand des Herstellers zurücksetzen lassen.	Eine Reset-Mechanik kann am Gerät das Zurücksetzen in den Auslieferungszustand erlauben. Ein OPC-UA-Standard könnte (zusätzlich) eine Reset-Methode für Geräte definieren. Sichere Komponenten müssen sensibles Datenmaterial löschen, wenn sie in den Auslieferungszustand versetzt werden.
3. Die Grundkonfiguration sollte nicht unsicher gestaltet werden, sondern das Gerät sollte mit einer sicheren Konfiguration ausgeliefert werden.	Durch die Anwendung des Prinzips „Security by Design“ während der Produktentwicklung, wie es zum Beispiel im Teil 4-1 der IEC 62443 (4) für Komponentenhersteller erklärt ist, kennt der Hersteller eine sichere Grundkonfiguration und kann die Geräte solchermaßen eingestellt im Sinne des Prinzips „Security by Default“ in Verkehr bringen. Aktuell verfügbare Produkte sind nur in Einzelfällen nach dem Prinzip „Security by Design“ entwickelt. Ebenso wenig sind Produkte ab Werk gemäß „Security by Default“ eingestellt. Für die Zukunftssicherheit von Produkten ist dringend zu empfehlen, dass Hersteller beide Prinzipien anwenden.

3 Denn die Unterlassung würde bedeuten, dass der Betrieb mit Zertifikaten erfolgt, die weder vom Integrator noch vom Betreiber gesperrt werden können und deretwegen ein Angreifer von ihm eingerichtete Geräte desselben Herstellers in den Kommunikationsverbund einbringen kann.

Inbesitznahme (Fortsetzung)

Anforderung	Erfüllbar durch/Offener Diskussionspunkt
4. Alle Authentifizierungskriterien der Komponente zur Prüfung anderer Identitäten sollten vom Integrator definiert werden können. Dies umfasst alle Passwörter und alle Zertifikate, denen die Komponente vertraut, ausgenommen von wenigen Zertifikaten, welche vom Hersteller zu besonderen Zwecken wie der Authentifizierung von Firmware-Updates gedacht sind.	Unter Verwendung des oben beschriebenen Certificate Managements über Global Discovery Server (GDS) nach OPC UA „Discovery“ (15) könnten Komponenten automatisch durch die Einstellbarkeit von GDS-Beziehungen für jede Security-Domäne mit spezifischen Authentifizierungskriterien versorgt werden. Benutzer-Passwörter wären automatisch spezifisch eingestellt, wenn Komponenten OAuth2 (zum Beispiel mit dahinterliegenden LDAP-Servern) unterstützten. Es bleibt eventuell ein Anfangs-Passwort, das für einen administrativen Benutzer im Auslieferungszustand definiert sein muss, damit eine Komponente sicher in Betrieb genommen werden kann. Ein gebräuchliches Verfahren für die sichere Individualisierung dieses Passwortes ist zum Beispiel, es ab Werk geräteindividuell einzustellen und auf das Gehäuse an einer üblicherweise verborgenen Stelle zu drucken. Andere Verfahren stehen zur Verfügung, sind hier aber nicht weiter diskutiert. Die konkrete Wahl hängt stark von dem Einsatzgebiet der Komponente ab. In einem Anhang von OPC UA „Discovery“ (15) ist grob skizziert, wie eine erste Versorgung (Provisioning) einer OPC-UA-Applikation mit einer Identität und einem Zertifikat versorgt werden kann. Dabei wird empfohlen, dass hierfür beidseitig eine explizite und einmalig manuelle Bekanntmachung aus Security-Gründen durchgeführt werden sollte. Der Applikation sollte der GDS bekannt gemacht werden. Denn die Applikation kennt noch keine Identität des GDS. Dem GDS muss das Gerät bekannt gemacht werden. Er kann es noch nicht an einer von ihm vergebenen Identität erkennen. Im OPC-UA-Standard wird das Verfahren nur grob erklärt, eine Unterstützung dieses Verfahrens durch standardisierte Anteile im Informationsmodell (Objekte und Methoden) wäre hilfreich. Zwar existiert laut Standard eine Möglichkeit, über Local Discovery Server mit Multicast Extension (LDS ME) neuen OPC-UA-Applikationen mit entsprechender Multicast-Fähigkeit einen GDS bekannt zu machen, doch hat dieser Weg Security-Probleme, auf die im Standard selbst hingewiesen werden sollte.

Quelle: Plattform Industrie 4.0

Integration

Anforderung	Erfüllbar durch/Offener Diskussionspunkt
1. Der Komponente sollte eine integratorspezifische Identität mit zugehörigem Zertifikat ZI_N vergeben werden können.	Der OPC-UA-Standard definiert Wege zum Einstellen von Zertifikaten für Server und Clients. Beispiele sind oben bereits mit dem Certificate Management nach OPC UA „Discovery“ (15) erklärt.
2. Die Komponente sollte für die Kommunikation in der Anlage 2.1 eine anlagenspezifische Identität samt Zertifikat ZA_N (welches die integratorspezifische Identität sein kann, aber nicht muss) eingestellt bekommen und verwenden können, sowie	Im Teil 4 „Services“ des OPC-UA-Standards (16) ist erklärt, dass derselbe Server verschiedene Endpunkte (Endpoints) haben kann. Jeder Endpoint kann mit einem eigenen Zertifikat ausgestattet sein. So könnte eine Komponente in ihrem OPC-UA-Server mehrere Endpoints anbieten, zum Beispiel für jede Identität einen Endpoint. In eine Anlage integrierte OPC-UA-Clients können vor dem Verbindungsaufbau entscheiden, welche Identität sie mit welchem Zertifikat gegenüber einem OPC-UA-Server verwenden. Das ist über die individuelle Belegung des Feldes „clientCertificate“ in der Anfrage (Request) zum Dienst (Service) „OpenSecureChannel“ möglich, den ein Client gegenüber einem Server aufrufen muss, um eine sichere Verbindung herzustellen.
2.2 eine anlagenspezifische Vertrauensliste eingestellt bekommen und verwenden können.	Im Teil 12 „Discovery“ des OPC-UA-Standards (15) ist erklärt, wie über das „Certificate Management“ eines „Global Discovery Server“ (GDS) sowohl OPC-UA-Clients als auch OPC-UA-Server mit Vertrauenslisten versorgt werden können. Die erste Versorgung geschieht in der Regel mit der Vergabe der Identität und des zugehörigen Zertifikates. So kann das auch für Komponenten umgesetzt werden. Für komplexere Anlagen macht es Sinn, dass das Vertrauen innerhalb der Anlage über nur innerhalb der Anlage gültige Zertifikate autonom aufgebaut und verwaltet wird. Hierfür kann eine „kleine“ Ausgabe eines GDS mit integrierter Certification Authority vorgesehen werden. Für Anlagen mit geringer Komplexität, bei der die Verwendung eines GDS zu komplex wäre, kann eine Verteilung über Dateisystemoperationen umgesetzt werden. Allerdings müssen hier die Versorgungswege und Zugriffberechtigungen proprietär geschehen. Statt eines automatischen Certificate Managements über einen GDS kann auch eine manuelle Verteilung über frei verfügbare OPC-UA-Clients mit Bedienoberfläche realisiert werden, zum Beispiel über UaExpert.

→

Integration (Fortsetzung)

Anforderung	Erfüllbar durch/Offener Diskussionspunkt
3. Die Komponente sollte für die Kommunikation mit Prozessen und Personen des Integrators die integratorspezifische Identität samt Zertifikat ZI_N verwenden können sowie eine integratorspezifische Vertrauensliste eingestellt bekommen und verwenden können.	Die oben bereits skizzierte Verteilung von Vertrauenslisten und Identitäts-Zertifikaten basierend auf dem Certificate Management über einen Global Discovery Server (GDS) lässt spezifische Verteilwege je Security-Domäne zu. Weil die Vertrauenslisten nach dem Verfahren „Push-Management“ über jeweils eigene Objekte mit Methoden realisiert werden, kann gemäß dem RBAC-Konzept nach OPC UA „Address Space Model“ (18) und „Information Model“ (19) an diesen Objekten eingestellt werden, dass sie nur aus der entsprechenden Domäne verändert werden können, zum Beispiel indem die Rechte einer Rolle zugeordnet werden, für die Zuordnungskriterien (IdentityMappingRules) definieren, dass sie nur bei einer Kommunikation über den Endpunkt gilt, der für die jeweilige Security-Domäne verwendet wird. Mit OPC UA „Discovery“ (15) sind drei Arten von Vertrauenslisten (Trust Lists) definiert, eine für Applikationszertifikate, eine für Benutzerzertifikate und eine für HTTPS-Zertifikate. Alle Arten sind direkt vom ServerConfiguration-Objekt aus referenziert. Darüber kann das jeweilige Push-Management realisiert werden. Gemäß oben bereits erklärter Lösungsskizze wird allerdings ein Satz von Vertrauenslisten pro Endpoint eines Servers benötigt. Hierfür müsste jeder Endpoint die Menge von Trust Lists unterhalb des ServerConfiguration-Objektes anders darstellen, was im Rahmen des Standards möglich wäre. Es fehlt im Standard nur die Möglichkeit, über einen vorhandenen Endpunkt die Versorgung eines anderen Endpunktes initial herzustellen.
4. Die Komponente sollte einen Zugriffskontrollmechanismus unterstützen, für den unabhängig von konkreten Identitäten Rechte definiert werden können.	Wie oben in der Vorwegnahme wiederholender Skizzen erklärt, ist mit OPC UA „Information Model“ (19) erklärt, dass nach OPC-UA-Standard Regeln in Form von IdentityMappingRules für die Zuordnung von Identitäten auf Rollen im OPC-UA-Server dargestellt und eingestellt werden können. Aktuell sind noch keine Werkzeuge am Markt bekannt, welche die herstellerunabhängige Verwaltung von IdentityMappingRules erlauben.
5. Die Rechte in der Komponente sollten so einstellbar sein, dass auch für die Veränderung von Rechten bestimmte Rechte erforderlich sind.	Gemäß OPC UA „Address Space Model“ (18) ist ein für einen Knoten im OPC-UA-Server definierbares Recht, die Erlaubnis, die Rechte dieses Knotens zu verändern. Ist dieses Recht einer Rolle nicht zugewiesen, können die Rechte an diesem Knoten nicht verändert werden.
6. Die Rechte in der Komponente sollten so einstellbar sein, dass bestimmte Rechte erforderlich sind, um die Regeln der Rechtezuordnung zu Identitäten einzustellen.	Gemäß OPC UA „Address Space Model“ (18) ist an den einzelnen Knoten eines OPC-UA-Servers darstellbar und (bei entsprechenden Rechten) auch optional einstellbar, welche Rolle welches Recht an diesem Knoten hat. Rollen werden bei einzelnen Verbindungen von Clients zur Sitzung zugewiesen. Für welche Sitzung welchen Clients welche Rolle zugewiesen wird, ist mit den IdentityMappingRules nach OPC UA „Information Model“ (19) für jede Rolle darstellbar und einstellbar, weil die IdentityMappingRules selbst als Knoten dargestellt werden und mit Rechten belegt werden können. Weil zu jeder Rolle laut Standard auch Methoden definierbar sind, über welche die Eigenschaften der IdentityMappingRules verändert werden können, und diese Methoden naturgemäß wiederum eigene Knoten im Adressraum des OPC-UA-Servers sind, können für ihre Verwendung ebenfalls Rechte eingestellt werden.

Quelle: Plattform Industrie 4.0

Vorbereitung der Übergabe durch den Integrator

Anforderung	Erfüllbar durch/Offener Diskussionspunkt
1. Vom Integrator definierte Authentifizierungskriterien, Rechte und Rechtezuordnungen (zu Rollen oder Attributregeln) für Wartungszugriffe sollten in der Anlage eingestellt werden können.	Wie oben in der Vorwegnahme wiederholender Skizzen erklärt, ist mit OPC UA „Information Model“ (19) erklärt, dass nach OPC-UA-Standard Regeln in Form von IdentityMappingRules für die Zuordnung von Identitäten auf Rollen im OPC-UA-Server dargestellt und eingestellt werden können. Aktuell sind noch keine Werkzeuge am Markt bekannt, welche die herstellerunabhängige Verwaltung von IdentityMappingRules erlauben.
2. Vom Integrator sollten vorübergehend notwendige Authentifizierungskriterien und Rechte für den Inbetriebnehmer in der Anlage aktiviert werden können, so dass die Anlage bei Bedarf auch ohne Netzwerkverbindung den Inbetriebnehmer authentifizieren kann und die Rechtezuordnungen und Authentifizierungskriterien für den Inbetriebnehmer auch wieder entfernt werden können.	Wenn in der Anlage Benutzer-Authentifizierung per Benutzername und Passwort möglich ist (zum Beispiel per Passwort-Tabellen oder per integriertem LDAP-Server), dann kann temporär ein Benutzer mit Passwort für den Inbetriebnehmer eingestellt werden. Die Entfernung dieses Benutzers kann auf gleichem Wege wie die dessen Einrichtung erfolgen. Alternativ kann in der Security-Domäne der Anlage oder in der Domäne des Integrators temporär ein Benutzerzertifikat für den Inbetriebnehmer in die Liste vertrauenswürdiger Zertifikate aufgenommen werden. Bei der Verwendung eines selbst-signierten Zertifikates ist sogar eine Offline-Verwendung ohne den Bedarf an aktuellen Sperrinformationen möglich. Die Entfernung dieses Zertifikates sperrt automatisch diesen expliziten Zugriffsweg.

→

Vorbereitung der Übergabe durch den Integrator (Fortsetzung)

Anforderung	Erfüllbar durch/Offener Diskussionspunkt
3. Der Integrator sollte überflüssige Zugriffswege, Authentifizierungskriterien und Rechte aus der Anlage löschen können.	Über die bereits erwähnten Mechanismen zur Verwaltung von Authentifizierungskriterien, Rollen und Rechten lässt sich deren Entfernung auch über zum OPC-UA-Standard konforme Mechanismen realisieren. Die Abschaltung von Zugriffswegen wie zum Beispiel Endpunkten (Endpoints) in den OPC UA-Servern von Anlagen hingegen ist so spezifisch für die Anlage, dass der Integrator hier eigene Wege definieren sollte.

Quelle: Plattform Industrie 4.0

Übernahme während der Inbetriebnahme

Anforderung	Erfüllbar durch/Offener Diskussionspunkt
1. Es sollte geprüft werden können, dass die Anlage vom Integrator stammt und im vom Integrator definierten Zustand ist.	Die Prüfbarkeit der Authentizität der Anlage kann über einen Endpunkt in einem OPC-UA-Server der Anlage unterstützt werden, wenn zum Beispiel dieser Endpunkt genau für den Zweck definiert wird und stets das vom Integrator vergebene Zertifikat gegenüber OPC-UA-Clients verwendet. Es ist dem Anlagenhersteller überlassen, das genaue Verfahren für die Prüfung zu definieren. Es ist zu erwarten, dass innerhalb der Umgebung des Betreibers die Anlage andere DNS-Namen und/oder IP-Adressen verwendet, als in der Umgebung des Integrators verwendet wurden. Gleichzeitig sieht der OPC-UA-Standard aus Sicherheitsgründen auch vor, dass Clients die DNS-Namen und/oder IP-Adressen des Endpoint-URLs in den Zertifikaten suchen und vergleichen sollen. Aus diesen beiden Gründen ist hier eine Ausnahme vorzusehen, zum Beispiel indem der OPC-UA-Client bei der Verifikation den fehlschlagenden Vergleich von DNS-Namen und/oder IP-Adressen ignoriert oder indem das vom Integrator vergebene Zertifikat für die Anlage gar keine DNS-Namen und/oder IP-Adressen enthält.
2. Es sollten Identitäten des Betreibers samt von ihm vergebene Zertifikate ZB_N in die Anlage eingebracht werden können, während die bisherigen Identitäten und zugehörigen Zertifikate (z. B. Zertifikate des Integrators ZI_N und Zertifikate der Komponentenhersteller ZH_N) erhalten bleiben.	OPC-UA-Server und -Clients können konform zum OPC-UA-Standard so gestaltet werden, dass sie mehrere Identitäten und zugehörige Zertifikate haben und verwenden können.
3. Authentifizierungskriterien zu Identitäten von verschiedenen Security-Domänen sollten getrennt voneinander und gleichzeitig in der Anlage hinterlegt werden können.	Die oben bereits skizzierte Verteilung von Vertrauenslisten und Identitäts-Zertifikaten basierend auf dem Certificate Management über einen Global Discovery Server (GDS) lässt spezifische Verteilwege je Security-Domäne zu. Mit OPC UA „Discovery“ (15) sind drei Arten von Vertrauenslisten (Trust Lists) definiert, eine für Applikationszertifikate, eine für Benutzerzertifikate und eine für HTTPS-Zertifikate. Alle Arten sind direkt vom ServerConfiguration-Objekt aus referenziert. Darüber kann das jeweilige Push-Management realisiert werden. Gemäß oben bereits erklärter Lösungsskizze wird allerdings ein Satz von Vertrauenslisten pro Endpoint eines Servers benötigt. Hierfür müsste jeder Endpoint die Menge von Trust Lists unterhalb des ServerConfiguration-Objektes anders darstellen, was im Rahmen des Standards möglich wäre. Es fehlt im Standard nur die Möglichkeit, über einen vorhandenen Endpunkt die Versorgung eines anderen Endpunktes initial herzustellen. Es handelt sich dabei um eine Komfort-Funktion, welche wegen der Arbeitsvermeidung und -erleichterung die Akzeptanz des Verfahrens fördern könnte. Außerdem wäre damit eine herstellerunabhängige Möglichkeit geschaffen.

→

Übernahme während der Inbetriebnahme (Fortsetzung)

Anforderung	Erfüllbar durch/Offener Diskussionspunkt
4. Rechte sollten mit Bezug auf die Authentifizierungskriterien der Identitäten einer Security-Domäne in der Anlage eingestellt und gleichzeitig aktiviert werden können, damit die Anlage zwischen Betreiber und Integrator (für die Wartung) unterscheiden und die entsprechenden Rechte durchsetzen kann.	Die Spezifikationen OPC UA „Address Space Model“ (18) und „Information Model“ (19) definieren Rollen als vollwertige Knoten im OPC-UA-Adressraum – mit einem Identifikator (Rollenname) und dem zugehörigen Namensraum. Derselbe Name in Kombination mit verschiedenen Namensräumen ergibt unterschiedliche Knoten. Je Security-Domäne kann ein eigener Namensraum definiert werden. Weil Rechte gemäß dem OPC-UA-Standard immer in Bezug auf Rollen definiert werden, ist es möglich, ohne Überschneidung und Kollision Rollen mit gleichen Namen und zugehörige Rechte mit Bezug auf verschiedene Security-Domänen zu definieren, indem die Namen durch Kombination mit dem Namensraum der Security-Domäne eindeutig gemacht werden. Aus technischer Sicht von OPC UA handelt es sich trotz Namensgleichheit um unterschiedliche Rollen. In den IdentityMappingRules für domänenspezifische Rollen kann weiter definiert werden, dass sie nur für bestimmte Endpoints anwendbar sind. Die Endpoints sind nach der obigen Vorwegnahme wiederkehrender Skizzen jeweils genau einer Security-Domäne zugeordnet. Die Anforderung lässt sich über diesen Weg erfüllen. Weil verschiedene Security-Domänen unterschiedliche Zertifikatshierarchien nutzen sollten, und jeweils autonom bestimmen, welche Applikation welche Identität hat (Application URI laut OPC-UA-Standard), sollte darauf verzichtet werden, bei den IdentityMappingRules die vom OPC-UA-Standard erlaubten Einschränkungen oder Erlaubnisse für bestimmte Applikationen per Nennung des Application URI zu definieren. Denn diese haben keinen festen Bezug zu einer Security-Domäne und das könnte durch einen Angreifer ausgenutzt werden, um eine Rechteausweitung von einer Domäne in die andere Domäne herbeizuführen. Eine Abhilfe gegen diese Gefahr ist, Application URIs immer nur in Kombination mit genau dem Endpoint für die Rolle zu erlauben, welcher der Security-Domäne zugeordnet ist, aus welcher die Application URIs stammen.
5. Tatsächlich vom Betreiber verwendete Bezeichnungen (externe Rollen, externe Attribute und ihre Ausprägungen) zu den Identitäten seines Personals und seiner Prozesse sollten in der Anlage auf Bezeichnungen abgebildet werden können, die durch den Integrator definiert wurden (interne Bezeichnungen).	Der OPC-UA-Standard definiert Wege zum Einstellen von Zertifikaten für Server und Clients. Beispiele sind oben bereits mit dem Certificate Management nach OPC UA „Discovery“ (15) erklärt.
6. Die vorübergehend in der Anlage eingestellten Zugriffsrechte und Authentifizierungskriterien bezüglich der Identitäten für den Zugriff des Inbetriebnehmers müssen gelöscht werden können.	Die oben beschriebenen Lösungsansätze zur Einstellung vorübergehend aktiver Zugriffsrechte und Authentifizierungskriterien sind reversibel.

Quelle: Plattform Industrie 4.0

Betrieb und Sicherheits-Wartung

Anforderung	Erfüllbar durch/Offener Diskussionspunkt
1. Identitäten und zugehörige Zertifikate sowie Schlüsselmaterial sollten 1.1. unterbrechungsfrei erneuert werden können und	Das Certificate Management über einen GDS erlaubt die Erneuerung von Zertifikaten und Schlüsselmaterial. Es impliziert die Verwendung des neuen Materials beim nächsten Verbindungsaufbau. Die Unterstützung des Certificate Managements über GDS ist bei OPC-UA-Applikationen noch nicht weit verbreitet. Bei vielen OPC-UA-Applikationen erfordert die Anwendung von erneuertem Schlüsselmaterial und/oder zugehörigem Zertifikat einen Neustart der Applikation.
1.2. je nach Aussteller auf unterschiedlichen Wegen erneuert werden können (Zertifikate des Integrators versus Zertifikate des Betreibers).	Es ist umsetzbar, dass eine OPC-UA-Applikation (Client oder Server) ihre Zertifikate von verschiedenen Global Discovery Servern (GDSen) gleichzeitig bezieht, jeweils für eine unterschiedliche Menge von Zertifikaten je GDS. Ein Ansatz ist oben bereits bei der Vorwegnahme wiederholender Skizzen erklärt.
2. Authentifizierungs- und Autorisierungskriterien zu Identitäten sollten 2.1. regelmäßig und	Das Certificate Management über einen GDS erlaubt die Erneuerung von Vertrauenslisten. Es impliziert die Verwendung des neuen Materials beim nächsten Verbindungsaufbau. Für die Verwaltung von Rechten und der Zuordnung von Rollen in einem OPC-UA-Server zu Identitäten beschreibt OPC UA „Information Model“ (19) ein Informationsmodell mit welchen Methodn. Rollen- und Gruppenzuordnungen können auch über LDAP-Server administriert werden, wenn die Benutzerauthentisierung über OAuth2 erfolgt. Weil die neueste Version des OPC UA „Information Model“ (19) so jung ist, sind aktuell keine Werkzeuge bekannt, über welche herstellerübergreifend die Autorisierungskriterien in OPC UA-Servern verwaltet werden können.

→

Betrieb und Sicherheits-Wartung (Fortsetzung)

Anforderung	Erfüllbar durch/Offener Diskussionspunkt
2.2. getrennt nach Verantwortlichem erneuert werden können (Integrator versus Betreiber).	Je Security-Domäne können unterschiedliche Global Discovery Server (GDS) eingesetzt werden. Damit werden auch unterschiedliche Laufzeiten der Gültigkeitsdauern von Zertifikaten unterstützt, was besonders bei vergleichsweise seltenen Wartungszugriffen von Vorteil sein kann. Je Security-Domäne können getrennte Server für die Passwortauthentifizierung von Benutzern eingesetzt werden, wie es in der Vorwegnahme wiederholender Skizzen bereits erklärt ist. Der aktuelle OPC-UA-Standard definiert keinen Weg, über den die passwortbasierte Authentifizierung von Benutzern konfiguriert werden kann, wenn die Passwortprüfkriterien direkt auf dem Gerät hinterlegt werden. Es ist daher zu empfehlen, bei passwortbasierter Authentifizierung Dienste wie LDAP und OAuth2 zu verwenden, welche die Passwortverwaltung ermöglichen.
3. Beim Verbindungsaufbau zur Anlage oder ihren Komponenten oder in umgekehrter Richtung sollte ausgewählt werden können, 3.1. welche Identität und welches Zertifikat relevant sind (Integrator versus Betreiber) und	Im Rahmen des OPC-UA-Standards ist es möglich, dass OPC-UA-Server unterschiedliche Endpunkte (Endpoints) definieren und hierfür unterschiedliche Zertifikate verwenden. Also können verschiedene Endpunkte für die OPC-UA-Clients der verschiedenen Security-Domänen angeboten werden. Ein OPC-UA-Client kann im Rahmen des OPC-UA-Standards für jeden Verbindungsaufbau entscheiden, welche Identität (Application URI) er verwendet und mit welchem Zertifikat er sich ausweist.
3.2. welche Prüfkriterien für das Verifizieren der Gegenstelle und deren Benutzer relevant sind.	OPC-UA-Clients können beim Verbindungsaufbau entscheiden, welche Vertrauensliste (Trust List) sie zur Prüfung des Zertifikates des OPC-UA-Servers verwenden. Für OPC-UA-Server kann über die zum Endpunkt (Endpoint) gehörende Identität und das jeweilige Zertifikat definiert werden, mit welchen Vertrauenslisten (Trust Lists) er Clients und deren Benutzer verifiziert.
4. Für die Verschlüsselung und Authentisierung/ Signierung sollten unterschiedliche Schlüssel und Zertifikate verwendet werden können.	Aktuelle Software Development Kits für OPC-UA-Applikationen sehen nicht die Verwendung von unterschiedlichen Schlüsseln für Signatur, Authentisierung und Verschlüsselung vor; auch im OPC-UA-Standard ist es nicht vorgesehen. Weil die Verfahren im OPC-UA-Protokoll in sich sicher sind und dort ein Übergriff zwischen den Verfahren nicht gegeben ist, sollten die Schlüsselpaare für die OPC-UA-Applikationen nur für das OPC-UA-Protokoll benutzt werden. Wenn eine Komponente über das OPC-UA-Protokoll hinaus den Bedarf hat, Zertifikate zu verwenden, zum Beispiel, um mit anderen Protokollen eine sichere Kommunikation aufzubauen, Dateien verschlüsselt zu empfangen oder Signaturen zu Dateien zu erstellen, sollten hierfür jeweils getrennte Schlüsselpaare und zugehörige Zertifikate verwendet werden. Solange OPC-UA-Applikationen dasselbe Schlüsselpaar für die Authentisierung und die Aushandlung der symmetrischen Schlüssel für die Verschlüsselung der Kommunikation nutzen, muss eine Kommunikationsinspektion an Vertrauensgrenzen zum Beispiel durch eine sogenannte Middlebox immer auch die Authentizität kompromittieren. Der OPC-UA-Standard könnte hierfür unterstützende Eigenschaften im Protokollanteil von OPC UA aufweisen, die in anderen Protokollen allerdings auch noch nicht vorgesehen sind, zum Beispiel in Form der Empfehlung unterschiedlicher Schlüsselpaare und Erklärung der Mechanismen dafür.

Quelle: Plattform Industrie 4.0

Außerbetriebnahme

Anforderung	Erfüllbar durch/Offener Diskussionspunkt
1. Sensible Daten sollten von Komponenten sicher gelöscht werden können.	Üblicherweise wird diese Anforderung durch Reset-Mechanismen gelöst, durch welche Geräte in einen Werkszustand versetzt werden. Dabei werden sämtliche Daten gelöscht, die im Vergleich zum Auslieferungszustand hinzugekommen sind, also auch sensible Daten, die durch den Integrator oder den Betreiber in die Komponente eingebracht wurden. Zum Beispiel ist hierfür ein Reset-Knopf vorgesehen.
2. In der jeweiligen Infrastruktur des Betreibers und des Integrators sollte der Zugriff teilweise oder komplett gesperrt werden können, für Komponenten bzw. ganze Anlagen.	Wenn wie vorgeschlagen Vertrauenslisten über das „Certificate Management“ per Global Discovery Server (GDS) verteilt werden, ist die Sperrung von Komponenten und ganzen Anlagen darüber möglich. Typischerweise wird im GDS eine Deregistrierung der Applikationen einer Anlage oder Komponente vorgenommen und damit werden zugehörige Zertifikate gesperrt, so dass diese Sperrinformation bei nächster Gelegenheit verteilt wird. Für feinere Sperrungen können die Mechanismen verwendet werden, welche nach OPC UA „Address Space Model“ (18) und „Information Model“ (19) die Veränderungen der Rechte und Rollen eines OPC-UA-Servers ermöglichen.
3. Für temporäre Sperren sollten Sperren in der Infrastruktur des Betreibers und/oder des Integrators aktiviert und wieder aufgehoben werden können.	Die oben genannten Mechanismen für die Sperren können auch mit temporärer Wirkung angewendet werden, weil über dieselben Wege auch die Aufhebung einer Sperre möglich ist. Achtung: Temporäre Sperren erfordern eine wirksame Zeitsynchronisation. Die korrekte Uhrzeit ist generell für die Security wichtig, zum Beispiel auch für die Zeitstempel von Auditdaten. An dieser Stelle sei auch auf die Bedrohung Nummer 37 „Manipulieren der Uhrzeit“ aus der „Sicherheitsanalyse OPC UA“ des Bundesamtes für Sicherheit in der Informationstechnik (12) verwiesen.

Quelle: Plattform Industrie 4.0

Notfallbehandlung/Wiederherstellung

Schon die Diskussion der Notfallbehandlung und Wiederherstellung in der Betrachtung des Lebenszyklus zeigt, dass für beides sehr weitgehend am System orientierte Lösungen vorzusehen sind, welche die Fähigkeiten der einzelnen Komponenten nutzen. Letztere sind bei großen und kleinen Geräten in sehr spezifischer Ausprägung zu erwarten, so dass es hier bei der Lösungsdiskussion sehr schwierig und zu weitgehend ist, eine generelle Lösung zu skizzieren. Darauf wird in diesem Papier deshalb verzichtet. Hier wird nur auf einzelne, ausgewählte Security-Anforderungen aus der Notfallbehandlung/Wiederherstellung eingegangen:

Anforderung	Erfüllbar durch/Offener Diskussionspunkt
1. Momentaufnahmen von Daten (Logdaten, temporären Daten, ...) und Zuständen sollten von Anlagen und Komponenten zu Forensikzwecken angefertigt werden können, sodass darin kein sensibles Material enthalten ist und dennoch daran eine Analyse von Security-Vorfällen möglich ist.	Das wird hier nicht diskutiert, weil es zu sehr vom System abhängt, besonders wegen der allgemeinen Daten des Systems und des Zusammenhangs mit dem Datenschutz. Der OPC-UA-Standard definiert in seinem Teil 3 „Address Space Model“ (18) das Konzept der Audit Events. Sie sind für die Meldung sicherheitsrelevanter Vorgänge geeignet und können zu zentralen Systemen weitergeleitet werden. Die Aufzeichnung dieser Events und ihre Einbeziehung in eine Momentaufnahme ist allerdings systemabhängig zu realisieren.
2. Es sollte möglich sein, Sicherheitskopien von Anlagen und Komponenten so anzufertigen und zurückzuspielen, dass dabei in den Sicherheitskopien der Schutz von sensiblen Daten gewahrt bleibt und ein Zurückspielen die sensiblen Daten nur Komponenten in vertrauenswürdigem Zustand übergibt.	Das wird hier nicht diskutiert, weil es zu sehr vom System abhängt.
3. Ein schneller Austausch von Schlüsselpaaren und zugehörigen Zertifikaten sollte für Komponenten möglich sein, die vermutlich kompromittiert wurden.	Dieses kann durch die Verteilung über OPC-UA-GDS gewährleistet werden. Ist der Schlüssel einer Komponente aufgrund des Notfalls kompromittiert, dann reicht eine automatische Erneuerung des Zertifikates über das Certificate Management nicht aus. Die Automatik darf nur für Komponenten genutzt werden, deren Schlüssel nicht kompromittiert wurde. Für kompromittierte Schlüssel ist eine Erneuerung des Schlüsselpaares und des zugehörigen Zertifikates über manuell unterstützte Wege wie bei einer erstmaligen Versorgung mit diesem Material (Provisioning) vorzusehen. Anlagen und Komponenten sollten für das außerplanmäßige Veranlassen der Erneuerung von Zertifikaten und Schlüsseln das bereits erwähnte Push-Management (15) unterstützen oder eine spezielle Methode oder Mechanik zur Veranlassung eines Erneuerungszyklus per Pull-Management anbieten.
4. Für Benutzer sollten Komponenten die Authentifizierung per Zertifikat unterstützen und/oder Passwörter gegen einen Authentifizierungsdienst prüfen.	Das Certificate Management nach OPC-UA-GDS sieht getrennte Vertrauenslisten für Benutzer und damit auch von Applikationen (Geräten und Software-Prozessen) getrennte Zertifikate und Schlüsselpaare vor. Diese können bei der Verwendung von OPC-UA-GDS also getrennt verteilt werden. Für die Verteilung von anderen Authentifizierungskriterien, wie Passwörtern, unterstützt OPC UA die Authentifizierung per Token, zum Beispiel über ein von einem OAuth2-Server vergebenen JSON-Web-Token. Dahinter kann die Passwortprüfung über LDAP-Server geschehen. Entsprechend kann dort die Erneuerung der Passwortprüfkriterien im Bedarfsfall schnell erfolgen. Komponenten und Anlagen wären nicht direkt betroffen.

Quelle: Plattform Industrie 4.0

Zusammenfassung und Ausblick

Im vorliegenden Dokument wird die sichere Einbindung einer Maschine in ein Betreibernetz mit OPC UA diskutiert. Bei der Untersuchung der Anforderungen über die Lebenszeit der Maschine ergibt sich, dass OPC UA in der neuesten Version des Standards die notwendigen Funktionen unterstützt. Basierend auf den Ergebnissen können Anbieter von OPC-UA-Toolkits sowie die Komponentenhersteller und Maschinenbauer ihre Angebote so weiterentwickeln, dass die Security-Funktionen von OPC UA interoperabel und leistungsfähig eingesetzt werden können.

In einem weiterführenden Dokument wird die unternehmensübergreifende Kommunikation mit OPC UA betrachtet werden. Als Beispiel wird dabei ein Betreibermodell dienen, bei dem zwei Stakeholder, ein Service-Provider und ein Fabrikbetreiber, mit der gleichen Maschine sicher interagieren müssen. Dabei wird die Wechselwirkung zwischen den beiden Security-Domänen und den entsprechenden Anforderungen an Integrität, Vertraulichkeit und Überwachbarkeit eine zentrale Rolle spielen.

Glossar

Authentisierungsdaten – Daten, mit denen ein Kommunikations- oder Interaktionspartner (zusammengefasst Partner) gegenüber anderen Partnern seine Identität nachweist, sich authentisiert. Partner können Personen, Geräte und Software-Prozesse sein. Die anderen Partner verwenden Authentifizierungskriterien, um die Identität entsprechend zu prüfen. Authentisierungsdaten können zum Beispiel ein Benutzername und Passwort eines Benutzers sein, die er oder sie beim Anmelden verwendet. Authentisierungsdaten für Geräte können zum Beispiel ein Zertifikat und ein asymmetrisches Schlüsselpaar sein.

Authentifizierungskriterien – Kriterien, anhand deren die Identität von Kommunikations- und Interaktionspartnern geprüft werden kann, wobei diese Partner Personen, Geräte oder Software-Prozesse sein können. Beispielsweise umfasst eine Tabelle mit Benutzernamen und Passwort-Hashes Authentifizierungskriterien, um die Passwörter einzelner Benutzer überprüfen zu können. Die Benutzernamen sind dabei die Identität. Sogenannte Trust Lists können Authentifizierungskriterien darstellen. Dies sind Listen, welche vertrauenswürdige Zertifikate, Ausstellerzertifikate und Sperrinformation umfassen, um Zertifikate zu überprüfen. Einzelne Zertifikate werden dabei als Identitätsnachweis von Kommunikationspartnern verwendet.

Integrator – Ein Anlagenbauer, welcher aus Komponenten Anlagen erstellt und diese an Betreiber verleiht oder diese durch den Betreiber leasen lässt. In diesem Szenario übernimmt der Integrator die Wartung der Anlage.

Trust List – Siehe Vertrauensliste

Vertrauensliste – Mengen von Zertifikaten, welche einer Komponente dazu dienen, die Zertifikate von Kommunikations- und Interaktionspartnern (zusammen: Partnern) zu sammeln. Siehe auch Authentifizierungskriterien: Vertrauenslisten sind damit eine spezifische Art von Authentifizierungskriterien. In OPC UA „Discovery“ (15) ist der Begriff „Trust List“ (auch in der Schreibweise TrustList) für die Vertrauensliste verwendet. Dort umfasst eine Trust List jeweils eine Menge von per Definition vertrauenswürdigen Zertifikaten. Optional umfasst eine Trust List eine weitere Menge von Zertifikaten, mit denen Zertifikatspfade von den Zertifikaten der Partner zu den zugehörigen Wurzelzertifikaten (Root-CA-Zertifikaten) vervollständigt werden können. Zusätzlich kann eine Trust List noch mittels Sperrinformation eine Menge von gesperrten Zertifikaten umfassen.

ZI_N – Zertifikate des Integrators, welche dieser zu von ihm erstellen Identitäten für die Anlage und deren Komponenten ausstellt, um bei einer Kommunikation mit der Anlage oder Komponenten zweifelsfrei feststellen zu können, dass die Kommunikation mit einer von ihm erstellten Anlage beziehungsweise von ihm verbauten Komponente stattfindet.

ZB_N – Zertifikate des Betreibers, welche dieser zu von ihm erstellten Identitäten für die Anlage und deren Komponenten ausstellt, um bei einer Kommunikation mit der Anlage oder Komponenten zweifelsfrei feststellen zu können, dass die Kommunikation mit einer von ihm betriebenen Anlage beziehungsweise darin verbauten Komponenten stattfindet.

ZA_N – Zertifikate innerhalb einer Anlage, welche die Anlage für von ihr erstellte Identitäten ausstellt, zum Beispiel um eine Security-Domäne innerhalb einer Anlage für die sichere Kommunikation ihrer Komponenten zu ermöglichen.

ZH_N – Zertifikate des Herstellers, welche dieser zu von ihm erstellten Identitäten für von ihm erstellte Geräte ausstellt, zum Beispiel um bei einer Kommunikation mit dem Gerät die Herkunft des Gerätes zweifelsfrei feststellen zu können.

Abbildungsverzeichnis

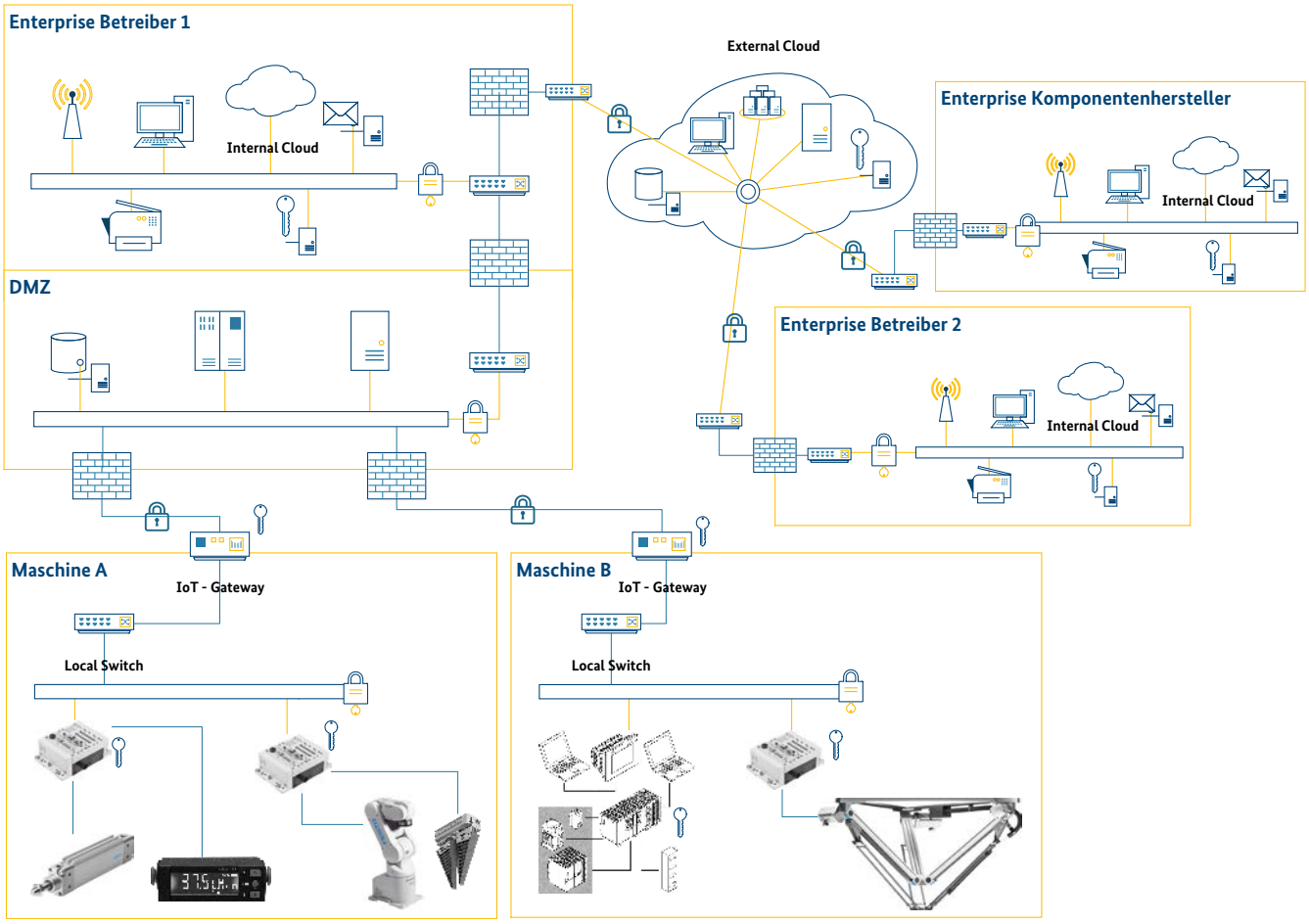
Literaturverzeichnis

1. *Diskussionspapier „Sichere Kommunikation für Industrie 4.0“*. Berlin: Plattform Industrie 4.0, 2017.
2. *Umsetzungsstrategie Industrie 4.0*. Berlin/Frankfurt: Plattform Industrie 4.0, 2015.
3. *Welche Kriterien müssen Industrie 4.0 Produkte erfüllen?* Frankfurt/Main: ZVEI, 2016.
4. *Industrial Communication Networks – Network and System Security.* IEC 62443.
5. *Informationssicherheit in der industriellen Automatisierung*. VDI/VDE 2182.
6. *IT-Security in der Industrie 4.0: Handlungsfelder für Betreiber.* Berlin: Plattform Industrie 4.0, 2016.
7. *Information technology – Security Techniques – Information Security Management System*. ISO/IEC 27000:2014.
8. *Integrität von Daten, Systemen und Prozessen als Kernelement der Digitalisierung*. Frankfurt: ZVEI, 2018.
9. *NE 153: Automation Security 2020 – Anforderungen an Design, Implementierung und Betrieb künftiger industrieller Automatisierungssysteme*. Leverkusen: NAMUR, 2015.
10. *Technischer Überblick „Sichere unternehmensübergreifende Kommunikation“*. Berlin: Plattform Industrie 4.0, 2016.
11. *Security der Verwaltungsschale.* Berlin/Frankfurt: Plattform Industrie 4.0/ZVEI, 2017.
12. *Sicherheitsanalyse OPC UA. s.l.*: Bundesamt für Sicherheit in der Informationstechnik (BSI), 25. April 2016.
13. *OPC Unified Architectur*. IEC 62541.
14. *Practical Security Recommendations for building OPC UA Applications*. Scottsdale, AZ: OPC Foundation, 2017.
15. OPC Unified Architecture Part 12: Discovery. *OPC Unified Architecture Specification Part 12*: Discovery Release 1.03. s.l.: OPC Foundation, July 19, 2015.
16. OPC Unified Architecture Part 4: Services. *OPC Unified Architecture Specification Part 4*: Services Release 1.04. s.l.: OPC Foundation, 22. November 2017.
17. OPC Unified Architecture Mappings. *OPC Unified Architecture Specifications Part 6*: Mappings Release 1.04. s.l.: OPC Foundation, 22. November 2017.
18. OPC Unified Architecture Part 3: Address Space. *OPC Unified Architecture Specification Part 3*: Address Space Model Release 1.04. s.l.: OPC Foundation, 22. November 2017.
19. OPC Unified Architecture Part 5: Information Model. *OPC Unified Architecture Specification Part 5*: Information Model Release 1.04. s.l.: OPC Foundation, 22. November 2017.
20. IEC/TS 62351-8. *Technical Specification: Power systems management and associated information exxchange – Data and communications security – Part 8: Role-based access control. s.l.* : International Electrotechnical Commission (IEC).
21. NIST Special Publication 800-162. *Guide to Attribute Based Access Control (ABAC) Definition and Considerations. s.l.*: National Institute of Standards and Technology (NIST), January 2014.
22. OPC Unified Architecture for Devices. *OPC UA Unified Architecture for Devices Companion Specification Release 1.01. s.l.*: OPC Foundation, July 25, 2013.

Anhang: Kollaborative Fabrik

Abbildung 8 zeigt das Gesamtszenario „Kollaborative Fabrik“. Das Szenario beschreibt das Zusammenwirken diverser beteiligter Akteure in der vernetzten Produktion.

Abbildung 8: Gesamtszenario „Kollaborative Fabrik“



Quelle: Plattform Industrie 4.0

Betreiber

Ein Fabrikbetreiber, hier „Betreiber 1“, betreibt eine Fertigung, in der Maschinen verschiedener Anbieter zum Einsatz kommen. Für das Beispiel wird eine bewährte Struktur angenommen. Die Unternehmensprozesse werden durch eine zentrale Infrastruktur gekoppelt, das „Enterprise“-Netzwerk. Zwischen dem Enterprise-Netzwerk und den Fertigungsanlagen ist eine Security-Zone (Demilitarized Zone „DMZ“) aufgebaut, die die beiden Teile sicher entkoppelt. Die Gestaltung der DMZ und der sie durchlaufenden Verbindungen (indirekter Zugriff über DMZ-Systeme, direkter Durchgriff durch die DMZ, ...) muss sich aus den Anforderungen an die Kommunikation und die Security ergeben.

Maschinen im „Betreibermodell“

Die in der Fertigung installierten Maschinen sollen im vorliegenden Beispiel im „Betreibermodell“ operieren. Sie gehören also nicht dem Fabrikbetreiber, sondern den spezialisierten Dienstleistern oder den Maschinenherstellern selbst. Im zugehörigen Geschäftsmodell könnte „Pay per Use“ die Möglichkeit sein. Die Anbieter entlasten den Fabrikbetreiber durch die Übernahme von Wartung und Optimierung. Dieses Modell ist für die vorliegende Betrachtung interessant, da aufgrund der gegebenen Eigentums- und Verantwortungsverhältnisse der Fabrikbetreiber nicht die volle Verantwortung und Verfügung über die Maschinen hat und insofern eine unternehmensübergreifende Betrachtung von Security-Domänen notwendig wird.

Kollaboration

Die wichtigste Forderung ist natürlich, dass die in der Fabrik betriebenen Maschinen der verschiedenen Anbieter zusammenarbeiten müssen, um die wirtschaftlichen Ziele des Fabrikbetreibers zu erreichen. Entsprechend ist die volle Interoperabilität aller beteiligten Anlagen und Systeme notwendig.

Cloud-Dienste

Die Angebote externer Unternehmen zur Optimierung der Unternehmensprozesse werden durch die „External Cloud“ dargestellt. In diesen Angeboten sind die Dienste der Maschinenanbieter enthalten sowie weitere mögliche Angebote anderer Unternehmen. Die „External Cloud“ steht insofern symbolisch für externe Dienste außerhalb des Bereichs des Fabrikbetreibers und kann mehrere unabhängige Angebote umfassen.

Weitere beteiligte Unternehmen

Im vorliegenden Beispiel sind die Anbieter der Maschinen und der entsprechenden Dienste relevante Partner. Weitere Angebote könnten zum Beispiel von den Herstellern der in den Maschinen verbauten Komponenten kommen.

Grundsätzlich ist zu beachten, dass die Dienstanbieter nicht nur den einen Fabrikbetreiber „Betreiber 1“ betreuen werden. So wie der Fabrikbetreiber auf die Dienste mehrerer Anbieter zurückgreift, werden die Dienstanbieter wiederum andere Fabrikbetreiber unterstützen. Bezogen auf das Modell bedeutet das, dass bei den Dienstanbietern Daten und Informationen von im Wettbewerb befindlichen Fabrikbetreibern verarbeitet werden.

AUTOREN

Carsten Angeli, KUKA Roboter GmbH | André Braunmandl, Bundesamt für Sicherheit in der Informationstechnik | Kai Fischer, Siemens AG | Torsten Förder, PHOENIX CONTACT Software GmbH | Prof. Dr. Tobias Heer, Hirschmann Automation & Control GmbH | Dr. Detlef Houdeau, Infineon Technologies AG | Dr. Lutz Jänicke (Leitung), PHOENIX CONTACT GmbH & Co KG | Dr. Christian Krug, Geschäftsstelle der Plattform Industrie 4.0 | Fabian Mackenthun, NXP Semiconductors Germany GmbH | Jens Mehrfeld, Bundesamt für Sicherheit in der Informationstechnik | Andreas Pfaff, Mitsubishi Electric Europe B.V. | Tobias Pfeiffer, Festo AG & Co. KG | Uwe Pohlmann, Fraunhofer-Institut für Entwurfstechnik Mechatronik | Martin Regen, Microsoft Deutschland GmbH | Andreas Teuscher, SICK AG | Klaus Theuerkauf, Institut für Automation und Kommunikation e.V. | Dmitry Tikhonov, Assystem 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