PLATTFORM INDUSTRIE4.0

DISKUSSIONSPAPIER

Sicherer Bezug von CAE-Daten

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
PRpetuum GmbH, München

Stand
November 2018

Bildnachweis
Monty Rakusen – Getty Images (Titel)
Gorodenkoff – istock (S. 4)
BlackJack3D – istock (S. 8)
Juice Images – Getty Images (S. 9)
Luis Alvarez – Getty Images (S. 11)
Monkeybusinessimages – istock (S. 13)
10'000 Hours – Getty Images (S. 14)

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

Die Kommunikation zwischen Industrie 4.0-Komponenten ist ein Eckpfeiler für die Weiterentwicklung in Richtung vernetzter, autonom agierender Systeme. Erst der standardisierte und interoperable Austausch von Informationen in allen Bereichen des Lebenszyklus von Produkten und Systemen schafft die Voraussetzungen zur Effizienzsteigerung und zum Erschließen der neuen technischen Möglichkeiten und neuer Geschäftsmodelle.

Einordnung im Lebenszyklus/RAMI4.0

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

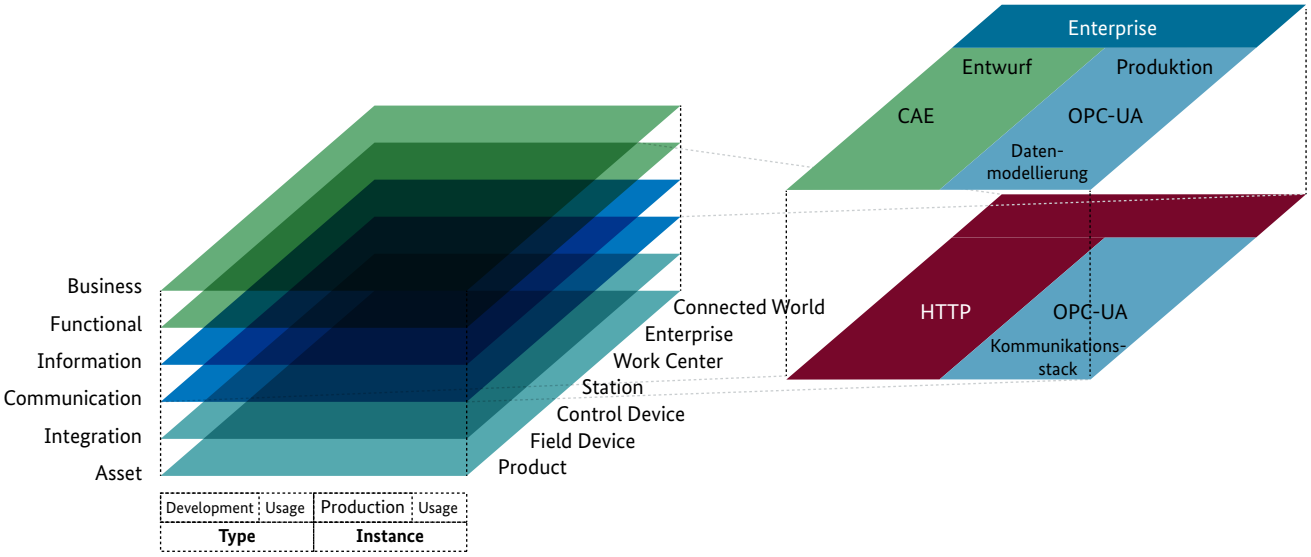
- Im Produktionsumfeld kommunizieren einzelne Geräte und Systeme („Instanzen“) miteinander. Die Systeme im Produktionsumfeld sind für die Betreiber zumeist Mission Critical und tauschen prozessbezogene Daten aus. Die Plattform Industrie 4.0 erwartet und unterstützt, dass hier OPC UA als Architektur mit den zugehörigen Kommunikationsprotokollen zum Einsatz kommt.
- Im Bereich der Enterprise-Kommunikation und übergreifender Wertschöpfungsnetzwerke sind andere Anforderungen an die unterschiedlichen informationstechnischen Schutzziele zu erfüllen.
- Im Bereich des Engineerings, also der Behandlung von „Typen“, sind wiederum andere Anforderungen zu erfüllen. Datensätze können hier sehr detailliert und groß sein. Je nach Vorgang sind die Entwurfs- und Entwicklungsvorgänge auch längerfristig angelegt.

Inhalt und Ziel dieses Diskussionspapiers

In diesem Diskussionspapier werden die Anforderungen an die sichere Kommunikation im Engineering-Prozess (grün) anhand eines Anwendungsszenarios erarbeitet. Es werden die beteiligten Stakeholder ermittelt und deren Sicherheitsanforderungen formuliert. Auf Basis der Sicherheitsanforderungen werden aktuell verfügbare und in Entwicklung befindliche Konzepte der Industrie 4.0 betrachtet, um einen Lösungsvorschlag auf höherer Beschreibungsebene zu entwickeln.

Ziel der Diskussion und des Lösungsvorschlags ist es, Interessenten und Beteiligten an der Gestaltung von Industrie 4.0 Hinweise für die weitere Ausgestaltung zu geben. Das Dokument erhebt nicht den Anspruch, eine vollständige, detaillierte Lösung zu präsentieren. Es richtet sich an den technisch interessierten Leser.

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



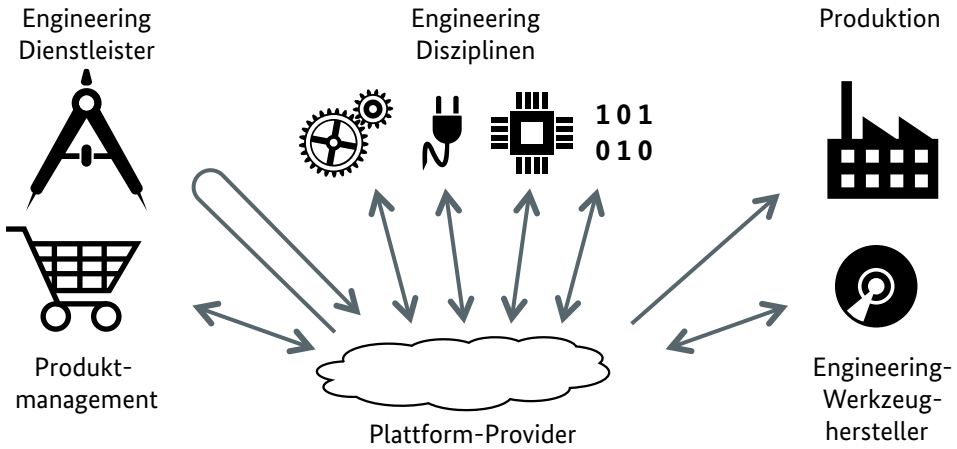
Quelle: Plattform Industrie 4.0

Anwendungsszenario „Smarte Produktentwicklung“

Zur Veranschaulichung einer entsprechenden Anwendung dient das Szenario „Smarte Produktentwicklung für die smarte Produktion (SP2)“ (1). Das Szenario sieht vor, dass beispielsweise Informationen zu Material, Komponenten, Produktionsprozess oder Nutzung eines Produkts in einer übergeordneten Plattform bereitgestellt werden. Die Plattform ermöglicht neue Formen der Zusammenarbeit in der Produktentwicklung und die Automatisierung von Engineering-Tätigkeiten.

Ein mögliches Anwendungsbeispiel für diese Art des Informationsbezugs ist die Erstellung eines elektrischen Antriebs. Dieses Szenario bildet die Grundlage für die im Rahmen dieses Schriftstückes vorgenommene Diskussion zum sicheren Informationsbezug und wird im Folgenden näher beschrieben. Dabei wird die übergeordnete Plattform für das Anwendungsbeispiel nicht betrachtet und der Fokus auf den Informationsbezug gerichtet.

Abbildung 2: Wertschöpfungsnetz „Smarte Produktentwicklung für die smarte Produktion“ (1)



Quelle: Plattform Industrie 4.0

Überblick

Abbildung 3 zeigt das Modell der Zusammenarbeit in der klassischen Aufteilung eines Herstellers, eines Integrators und eines Betreibers. Dabei wurde als Beispiel ein Antrieb gewählt, der aus einem Umrichter und einem Motor entsteht, die beim Integrator zusammengefügt und aufeinander abgestimmt werden.

Der Hersteller liefert Informationen über den Typ der Produkte an den Integrator, der aus den Produkten das höherwertige Gesamtprodukt erzeugt. Für dieses Gesamtprodukt entsteht wiederum eine Typbeschreibung, die der Integrator seinem Kunden, dem Betreiber, zur Verfügung stellt. Typinformationen können klassischen Datenblättern entsprechen, 3D-Modelle enthalten, Daten oder Software für die Simulation oder den Betrieb des Produktes (CAE-Daten) umfassen oder weitere Angebote bereitstellen.

Für die ausgelieferten physischen Produkte können nun zusätzlich Daten anfallen, die für die jeweilige Instanz spezifisch sind, etwa Kalibrierungs- oder Qualitätsdaten. Ebenso könnten z. B. elektronische Informationen für eine Echtheitsprüfung oder Chargenverfolgung enthalten sein.

Übertragung von Typinformationen

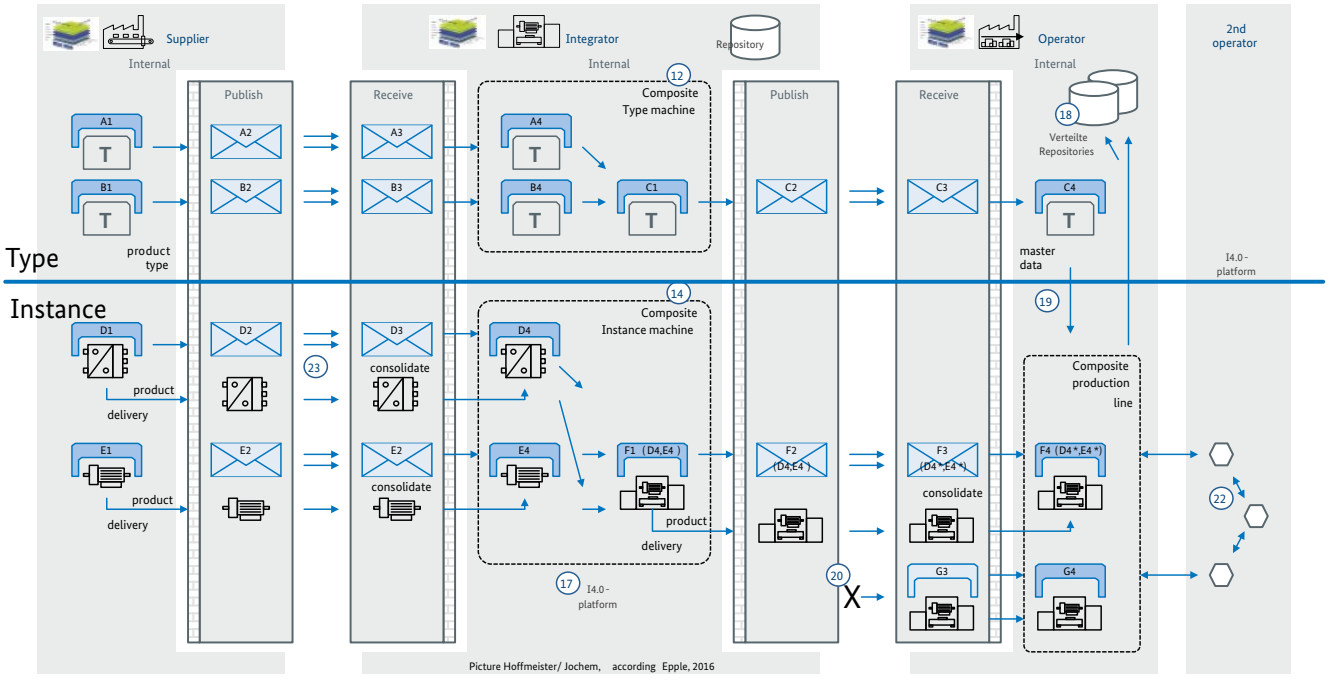
Im vorliegenden Diskussionspapier liegt der Fokus auf der Übertragung von Typinformationen, die für das Engineering eines Gesamtprodukts, hier eines Antriebs, benötigt werden („CAE-Daten“), siehe Abbildung 4. Im Kontext des Lebenszyklusmodells des RAMI4.0 (3) bzw. der IEC 62890 werden Typinformationen ausgetauscht (siehe Abbildung 1). Aus Sicht des Komponentenherstellers werden die vorhandenen Typinformationen genutzt, während sie beim Integrator in dessen Entwicklungsprozess einfließen.

Grundsätzlich kann die Übertragung der Daten entweder offline oder online erfolgen, wobei letzterer Fall in Industrie 4.0 die größte Bedeutung haben wird.

Für das Szenario wird der folgende Fall betrachtet:

- Ein Mitarbeiter beim Integrator soll einen Antrieb entwerfen.
- Der Hersteller von Antriebskomponenten stellt die notwendigen CAE-Daten über seine Produkte bereit.

Abbildung 3: Gesamtszenario aus (2). Oben: Typinformationen; unten: Instanzdaten



Quelle: ZVEI

- Eine Online-Verbindung ist vorausgesetzt.
- Für seine Aufgabe kann der Mitarbeiter auf die Produktdaten der Antriebskomponenten zugreifen, wobei die Unterstützung bei der Auswahl (nach Eigenschaften, nach Bestellnummern oder Ähnlichem) hier nicht weiter betrachtet wird.
- Die Zusammenstellung der CAE-Daten kann kundenspezifisch zur Laufzeit erfolgen. Nicht jeder Kunde erhält alle bzw. die gleichen Daten. So könnten zum Beispiel bestimmte Informationen nur bei Vorliegen einer Vertraulichkeitsvereinbarung bereitgestellt werden.

Betrachtet wird die Interaktion zwischen den Systemen beim Hersteller und beim Integrator. Der Einfachheit der Darstellung wegen wird nur ein Hersteller dargestellt, die Betrachtung gilt aber uneingeschränkt auch für das Vorgehen bei mehreren Herstellern.

Abbildung 5 zeigt die technischen Systeme, die im Rahmen der Betrachtung eine Rolle spielen werden:

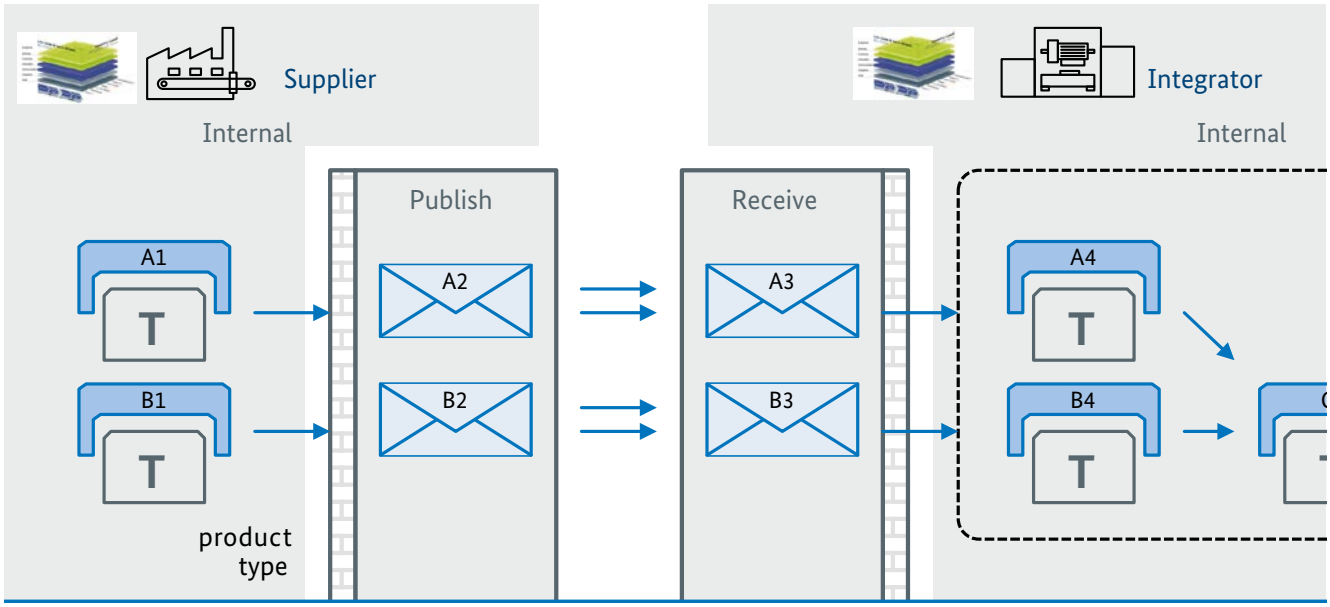
- Beim Hersteller werden die Typinformationen in einem entsprechenden System abgelegt sein, das sie bei Abfrage im notwendigen Format bereitstellt. Um entscheiden zu können, ob und welche Daten auf Anfrage bereitgestellt werden, könnte eine CRM-Datenbank (Customer Relationship Management) einbezogen werden.
- Beim Integrator arbeitet ein Mitarbeiter an einer Engineering-Station, um seine Aufgabe zu erfüllen.
- Die Interaktion wird zwischen den beiden Unternehmen stattfinden, die jeweils eine eigene Sicherheitsdomäne darstellen und entsprechende Sicherheitsmaßnahmen umgesetzt haben – hier durch die Sicherheitsgateways dargestellt.

Annahmen und Abgrenzungen

Für die Übertragung der Typinformationen wird davon ausgegangen, dass es sich um Daten handelt, die sich, anders als Prozessdaten, nicht permanent ändern. Die Übertragung wird also zu einem bestimmten Zeitpunkt stattfinden und einen größeren Datensatz umfassen. Ein Modell zur Verteilung von Aktualisierungen der Daten wird hier nicht betrachtet. Die Übertragung von Prozessdaten stellt andere Anforderungen an die Kommunikation.

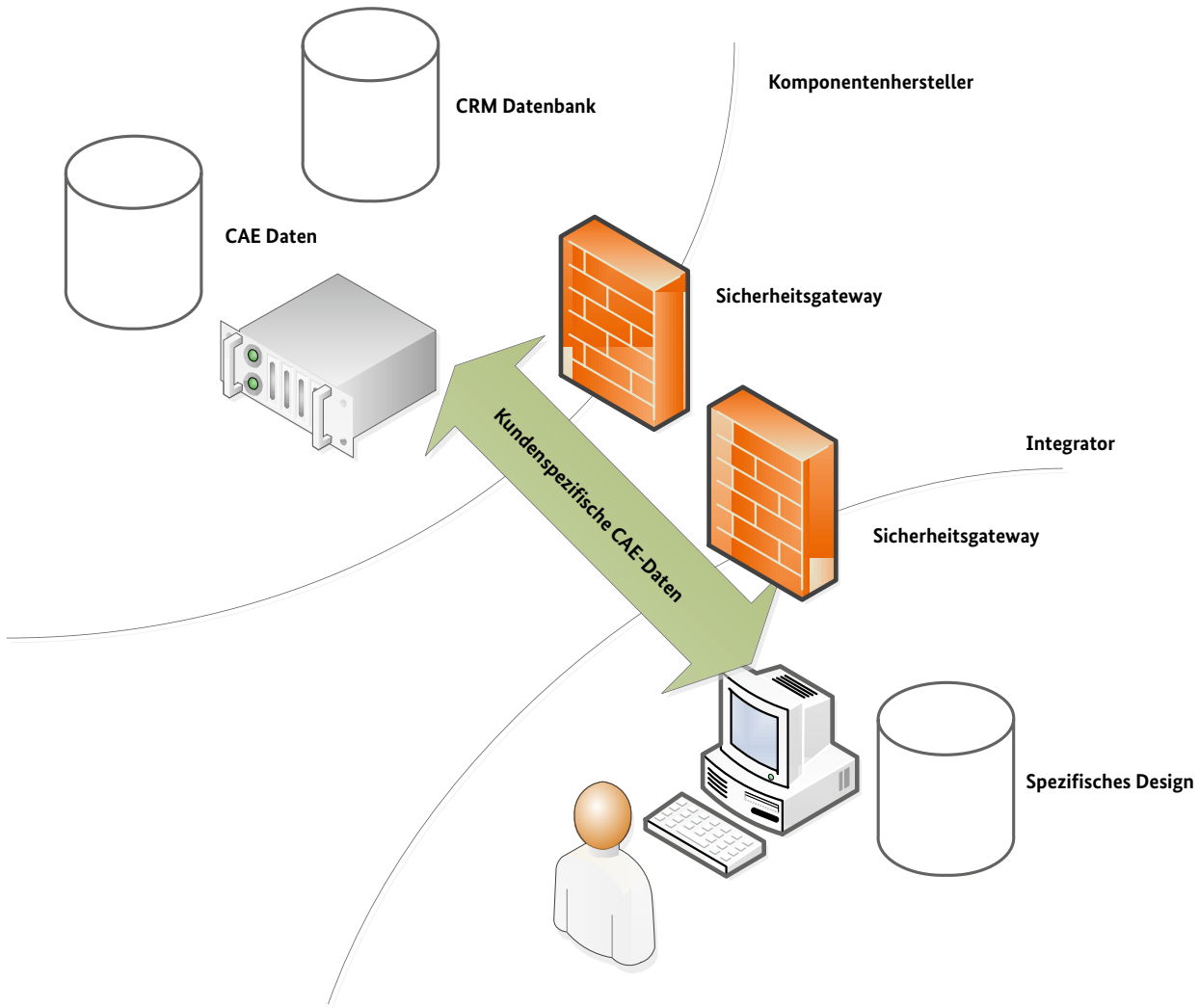
Es wird angenommen, dass es sich um eine oder mehrere Dateien handelt, die gegebenenfalls in einem Archiv zusammengefasst sein können. Das Papier „Details of the

Abbildung 4: Übertragung von Typinformationen



Quelle: ZVEI

Abbildung 5: Beteiligte Systeme



Quelle: Plattform Industrie 4.0

Asset Administration Shell (2) schlägt ein Format basierend auf den Open Packaging Conventions (4) vor. Es werden keine Einschränkungen der Typinformationen vorausgesetzt, sodass z. B. auch ausführbare Programme enthalten sein können und in der Security-Betrachtung berücksichtigt werden müssen.

Die Ausgestaltung der übertragenen Daten, ihre Struktur und Darstellung, wird im vorliegenden Dokument nicht betrachtet. Die kundenspezifische Erzeugung des Datensatzes und das Einladen in das Engineering-System liegen ebenso außerhalb der Betrachtung dieses Dokuments wie die weitere Verwendung der Daten. So könnten Geschäftsmodelle eine beschränkte Nutzungserlaubnis etwa hinsichtlich der Dauer der Nutzung enthalten. Die Durchsetzung derartiger Beschränkungen wird typischerweise als Digital Rights Management (DRM) bezeichnet und ist wiederum ein eigenes technisches Thema, das nur wenig mit dem eigentlichen Kommunikationsvorgang zu tun hat.

In der vorliegenden Betrachtung liegt der Fokus auf den technischen und sie begleitenden organisatorischen Maßnahmen. Weitergehende rechtliche Betrachtungen, etwa zu Vertraulichkeitsvereinbarungen, werden nicht vorgenommen.

Security

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

- Vertraulichkeit
- Integrität
- Verfügbarkeit

Weitere Schutzziele werden ergänzend oder unterstützend verwendet:

- Authentizität
- Verbindlichkeit
- Nichtabstreitbarkeit

Im Bereich der Produktion wird zusätzlich der Begriff der Zuverlässigkeit verwendet. Verfügbarkeit ist zumeist ein statistischer Wert für Ausfall oder Wiederherstellung, z. B. eine Stunde pro Jahr. Zuverlässigkeit betrachtet die Freiheit von Störungen. In einem physikalischen Prozess kann auch eine einzelne Störung von zehn Sekunden relevante Auswirkungen haben, die im statistischen Mittel nicht bewertbar wäre.

Risikobasierter Ansatz

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

- In der im Unternehmensumfeld üblicherweise angewendeten ISO 27001 (5) verwendet man daher eine Klassifizierung der Schutzanforderungen (z. B. öffentlich, intern, vertraulich, streng vertraulich) als Unterstützung bei der Risikobewertung und der Aufstellung des Maßnahmenkatalogs.
- Die für die Automatisierung erarbeitete Normenreihe IEC 62443 (6) verwendet zusätzlich ein Angreifermodell, um darauf basierend Security Level für Automatisierungssysteme und -komponenten anzugeben.

Sicherheit in der Kommunikation

Im vorliegenden Fall des Austauschs von CAE-Daten wird davon ausgegangen, dass die Kommunikation zwischen IT-Systemen stattfindet und insofern die Systematik der ISO 27001 Anwendung findet.

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

Für die Erkennung und Vermeidung von Angriffen ist es notwendig, interne Systeme und den Datenaustausch mit externen Geschäftspartnern zu überwachen (ISO 27001: A12.4 Überwachung und Protokollierung. A12.2 Schutz vor Schadsoftware. A13.2 Informationsübertragung). Dabei ist neben der Protokollierung von Vorgängen und der Auswertung dieser Protokolle die Beschränkung und Überwachung der Kommunikation ein wichtiges Mittel. Die Verwendung von Firewalls und Proxy-Funktionen am Netzübergang (Sicherheitsgateway) entsprechen dem Stand der Technik. In vielen Unternehmen ist die direkte Kommunikation interner Systeme nach außen auf das HTTP-Protokoll beschränkt. Eine besondere Herausforderung in der Überwachung ist verschlüsselte Kommunikation. Die Verschlüsselung stellt auf der einen Seite die Vertraulichkeit des Informationsaustauschs sicher, erlaubt aber gleichzeitig etwa den unkontrollierten Transfer interner Daten aus dem Unternehmen oder das Eindringen von Schadsoftware in das Unternehmen. Insofern ist es heute gängige Praxis, verschlüsselte Kommunikation am Sicherheitsgateway aufzubrechen, um diese dann entsprechend des Protokolls zu analysieren. Inhalte, die nicht protokollkonform sind oder aus anderen Gründen nicht analysiert werden können, werden üblicherweise abgewiesen, um unerwünschten oder gefährlichen Datentransfer zu unterbinden. Ausnahmen können eingerichtet werden, wobei der Nutzen der Ausnahme, z. B. Ermöglichung anderweitig blockierter Kommunikation, mit den zusätzlich entstehenden Risiken abgewogen werden muss. Dies geht zumeist einher mit einer Bewertung der Vertrauenswürdigkeit des Kommunikationspartners, so könnte z. B. die Kommunikationsüberwachung für Banktransaktionen zwischen Mitarbeitern der Buchhaltung und bekannten Kreditinstituten deaktiviert sein, da der Schutz der Zugangsdaten schwerer wiegen könnte als die Bedrohung durch die Interaktion mit dem Kreditinstitut.

Beteiligte Interessengruppen

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

Auch bereits innerhalb eines Unternehmens können sich Sicherheitsdomänen herausbilden. Eine Sicherheitsdomäne ist ein technologisch, organisatorisch oder räumlich zusammengehöriger Bereich mit einheitlichen Sicherheitsanforderungen und/oder einheitlicher Sicherheitsadministration. In vielen Unternehmen sind heute zumindest Bürobereich/IT und Produktionsbereich jeweils eigene Sicherheitsdomänen.

Stakeholder

Anhand des vorgestellten Anwendungsszenarios lassen sich im Hinblick auf den Lebenszyklus gemäß des Referenzarchitekturmodells Industrie 4.0 (RAMI4.0) verschiedene Stakeholder identifizieren. Das Zusammenspiel der Stakeholder ist in Abbildung 6 gezeigt, wobei nur die grün hinterlegten Stakeholder im Rahmen dieses Diskussionspapiers betrachtet werden. Hierbei besitzt jeder der betrachteten Stakeholder unterschiedliche Anforderungen an die Sicherheit seiner Informationen. Diese Interessen werden in diesem Abschnitt näher beschrieben.

Ergänzend werden für jeden Stakeholder mögliche Bedrohungen beschrieben. Die Umsetzungsstrategien zur Risikobehandlung werden in einer exemplarischen Lösungsskizze diskutiert.

Komponentenhersteller

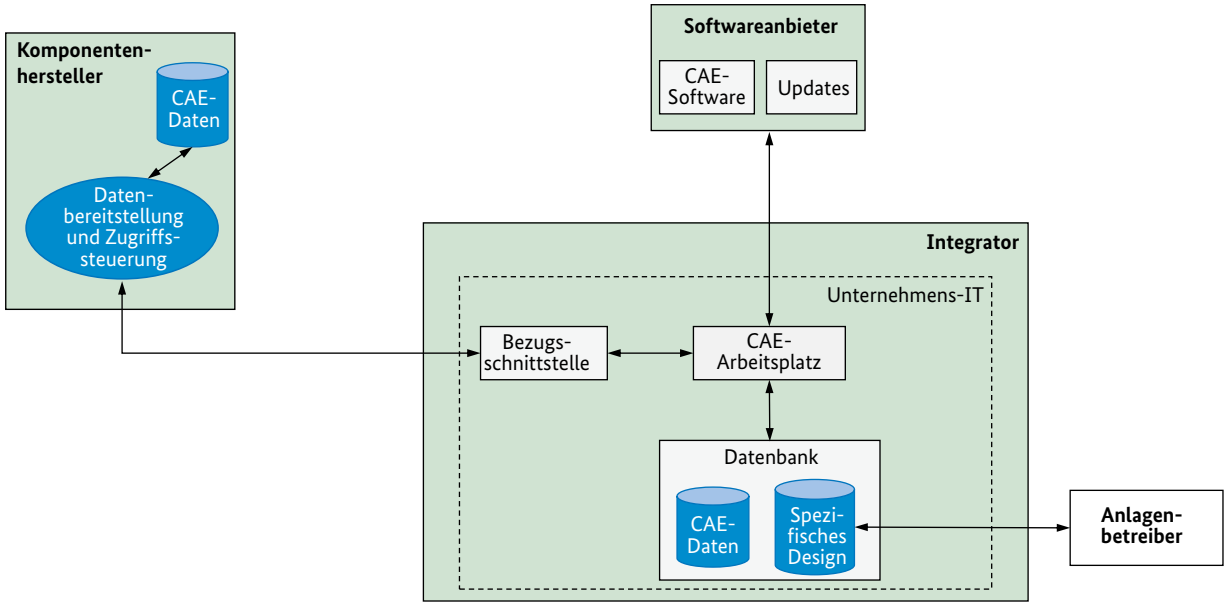
Rollen und Aufgaben

Der Komponentenhersteller stellt sein Know-how für die Integration und Verwendung der eigenen Produkte bereit. Beispielsweise könnte es sich hierbei um die Drehzahlkennlinie eines Motors handeln. Um die Daten vor unberechtigter Nutzung zu schützen, muss der Komponentenhersteller geeignete Maßnahmen ergreifen. Dabei ist der Vertraulichkeit der Daten eine hohe Bedeutung zuzuschreiben und sicherzustellen, dass der richtige Empfänger die Daten empfängt. Darüber hinausgehende DRM-Maßnahmen werden hier nicht betrachtet.

Der Komponentenhersteller und der Integrator schließen einen initialen Datennutzungsvertrag ab, in dem neben der Art und Weise des Bezugs der Typinformationen auch die Berechtigungen der am Geschäftsvorgang beteiligten Mitarbeiter des Herstellers geregelt sind. Hierzu werden heute zumeist beim Hersteller Nutzerkonten angelegt und die Authentizität des Herstellers mittels Zertifikaten nachgewiesen. Dabei ist die Nutzung der Konten mittels einer Laufzeit einzuschränken, um bei einer möglichen Beendigung des Beschäftigungsverhältnisses deren Weiternutzung zu verhindern.

Die Zugriffssteuerung mittels Nutzerkonten wird Role Based Access Control (RBAC) genannt und ist als Stand der Technik etabliert (siehe Abschnitt „Verwendete Technologien“). Die Ablage der Nutzungsberechtigungen erfolgt in einer Datenbank, welche in das Sicherheitskonzept mit einbezogen werden muss. Zusätzlich bietet diese Datenbank die Möglichkeit, neue Geschäftsmodelle entsprechend den Anwendungsszenarien der Plattform Industrie 4.0 zu etablieren.

Abbildung 6: Interaktion der Stakeholder



Quelle: Plattform Industrie 4.0

So wäre es für den Komponentenhersteller denkbar, CAE-Daten für den Kunden je nach Bezahlmodell individuell zusammenzustellen.

In die Sicherheitsbetrachtung des Komponentenherstellers sollten zudem Maßnahmen zur Wahrung der Integrität der Informationen einbezogen werden (7). Die Integrität bzw. Unversehrtheit von Informationen hat direkten Einfluss auf die Qualität eines Produktes. So können kleinste Änderungen im Parametersatz der vom Integrator einzusetzenden Antriebssteuerung zu einer Abweichung von der geplanten Sollfunktion führen. Dies kann so weit führen, dass die Qualität der mit Hilfe des projektierten Antriebs hergestellten Produkte nicht mehr der Spezifikation entspricht und somit Produkthaftungsfälle auslöst.

Der Komponentenhersteller bietet dem Integrator eine Schnittstelle zum Bezug der gewünschten Daten an. Die Schnittstelle wird von der zentralen IT betrieben und funktioniert vollautomatisch. Im Sinne der Industrie 4.0 bedeutet dies, dass die Freigabe der angefragten CAE-Daten ohne Intervention von Mitarbeitern des Herstellers geschieht, etwa aus dem Vertriebsinnendienst.

Risiken

Der Komponentenhersteller betreibt eine CRM-Datenbank zur Pflege der Kundeninformationen. Inhalt dieser Datenbank sind neben den Kontaktdaten die vertraglich festgehaltenen Regularien zum Bezug der CAE-Daten. Um dem Nutzer die angefragten Daten zur Verfügung zu stellen, muss dieser entsprechend autorisiert werden. Dabei besteht die Gefahr, dass ein potenzieller Angreifer die Kommunikation während des Anmeldungsvorgangs mitschneidet und im Fall der häufig angewendeten Authentifizierung mit Benutzername und Passwort dann die Zugangsdaten erhalten würde. Mit Hilfe der Zugangsdaten kann dann unter Vortäuschung einer falschen Identität das Know-how des Komponentenherstellers unerlaubt bezogen werden. Denkbar wäre auch das gewaltsame Erlangen von Zugriff auf die Bezugsschnittstelle mittels Brute-Force-Attacken, also dem vollautomatischen Durchprobieren von Zugangsdaten.

Je nach Art und Umfang eines Angriffs kann ein Angreifer unter Umständen die gesamte IT-Infrastruktur des Komponentenherstellers übernehmen. Bezogen auf den Anwendungsfall kann er dies ausnutzen, um die CAE-Daten zu manipulieren. Denkbar wäre in diesem Fall eine Verfälschung der zu beziehenden Informationen oder das Anhängen von Schadsoftware, d.h. die Integrität der angefragten Informationen kann nicht mehr gewährleistet werden.

Grundlage hierfür ist das Öffnen der CAE-Daten mit Schreibzugriffsrechten. Um dies zu verhindern, sollten CAE-Daten und weitere sensible Informationen in der CAE-Datenbank nur lesend geöffnet werden können. Zudem könnte ein Angreifer seine erlangten Zugriffsrechte ausnutzen, um Informationsabzug zu betreiben. Das bedeutet, es könnten beispielsweise alle CAE-Daten des Herstellers auf einmal abgeschöpft werden, etwa indem die Daten sämtlicher Komponenten bezogen werden.

Des Weiteren werden die kundenspezifischen Informationen (Datenblatt des physischen Produktes, CAE-Daten, Kalibrierungsdaten etc.) über eine dedizierte Schnittstelle, z. B. einen Webservice, bereitgestellt. Dabei ist die Robustheit dieser Schnittstelle gegenüber sogenannten Denial of Service (DoS)-Attacken sicherzustellen, um die Verfügbarkeit des angebotenen Dienstes zu gewährleisten.

Integrator

Rollen und Aufgaben

Im betrachteten Anwendungsfall ist der Integrator die Instanz der Wertschöpfungskette, die eine technische Lösung entsprechend der Kundenwünsche entwickelt und diese dem Kunden zur Verwendung in seinen eigenen Produkten und Anlagen bereitstellt. Zu diesem Zweck bezieht der Integrator die benötigten Informationen vom Komponentenhersteller.

Als wertvollste zu schützende Güter sind die Integrität und Authentizität der Information anzusehen, um eine fehlerfreie Leistung liefern zu können. Grundsätzlich sind technische und organisatorische Maßnahmen zu treffen, um zum Beispiel die internen Systeme/Infrastrukturen vor der Infektion mit Schadsoftware zu schützen und aufgetretene Sicherheitsvorfälle zu protokollieren. Hierzu bietet es sich an, ein Informationssicherheitsmanagementsystem (ISMS) zu etablieren, das geeignete IT-Sicherheitsmaßnahmen auf Grund einer vorangegangenen Risikoanalyse beschreibt (siehe Abschnitt „Risikobasierter Ansatz“). Weiterhin ist die Überwachung der ausgehenden Kommunikation eine wichtige Aufgabe der Unternehmens-IT (Firewalls, Gateways etc.), wodurch unerwünschte Kommunikation detektiert werden kann.

Besonderes Augenmerk gilt den CAE-Arbeitsplätzen. Diese stellen normale Mitarbeiter-PCs mit einer dedizierten Engineering-Software dar und unterliegen mindestens den gleichen Gefahren wie die anderen an der internen Kommunikation beteiligten Systeme. Hierzu zählt insbesondere Schadsoftware. Zusätzlich werden solche Engineering-Stationen auch häufig in Sondernetzen, wie dem Prototypenbau, eingesetzt, die zusätzliche Gefährdungen aufgrund des zumeist geringeren Sicherheitsniveaus mitbringen.

Risiken

Die IT-Infrastruktur bildet das Rückgrat zur Abwicklung der Geschäftsprozesse und ist gegenüber potenziellen Angreifern abzusichern. Das Hauptaugenmerk liegt dabei auf dem Schutz vor Einspeisung von Schadsoftware und dem Diebstahl von Geschäftsgeheimnissen. Hierbei ist auch zu betrachten, dass Mitarbeiter etwa an den CAE-Arbeitsplätzen die Daten des Komponentenherstellers kopieren können. Zudem wäre es möglich, die Produktdaten zu manipulieren, um eine Fehlfunktion beim Anlagenbetreiber herbeizuführen.

Anbieter der CAE-Software

Rollen und Aufgaben

Der Anbieter der CAE-Software stellt dem Integrator ein Softwaretool zur Entwicklung seiner Produkte bereit. Diese Software besitzt zwei Schnittstellen: Eine Bezugsschnittstelle für die Daten der Komponentenhersteller und eine Bezugsschnittstelle zum Lesen und Schreiben auf die firmeneigene CAE-Datenbank des Integrators. Das bedeutet, potenziellen Angreifern stehen zwei mögliche Einfallstore zur Verfügung.

Um die Vertrauenswürdigkeit gegenüber dem Endnutzer zu gewährleisten, obliegt es daher dem Softwarehersteller, regelmäßige Sicherheitsupdates aufgrund von Schwachstellen zu veröffentlichen. In Bezugnahme auf die umfangreiche Vernetzung in der Industrie 4.0 sind die Updates auch anzuwenden, sobald ein Teilnehmer an der Industrie 4.0-Kommunikation teilnehmen will, um die anderen Beteiligten nicht zu bedrohen.

Risiken

Ein von der CAE-Software ausgehendes Risiko für den Integrator besteht in der Ausnutzung von Schwachstellen. Diese könnten unter Umständen zur Infizierung des CAE-Arbeitsplatzes mit Schadsoftware ausgenutzt werden, welche wiederum den Zugriff auf die Unternehmens-IT des Integrators ermöglichen kann. Daher steht der Softwarehersteller in der Pflicht, seine Software nach bestem Wissen und dem Stand der Technik zu implementieren und mit den notwendigen Sicherheitsupdates zu versorgen.

Der Zugriff auf die CAE-Daten (siehe Abbildung 2) könnte z. B. mittels eines Plugins innerhalb der CAE-Software erfolgen. Je nach Komponentenhersteller muss unter Umständen ein separates Plugin installiert werden. Hierbei besteht die Gefahr, dass der Anwender eine nicht vertrauenswürdige Software installiert, die bei ihrer Verwendung beispielsweise einen zweiten Kommunikationskanal zu einer unberechtigten Partei aufbaut. Dies stellt den Softwareanbieter vor die Pflicht, nur die Installation von vertrauenswürdigen und geprüften Erweiterungen zu gestatten.

Dabei sind auch externe Bezugsquellen (USB-Speichermedien, CD/DVD) und alle Datentypen (3D-Modelle, ausführbare Dateien etc.) zu berücksichtigen. Die Authentizität der Daten sollte mittels digitaler Signaturen geprüft werden. Um Risiken durch einen Schadsoftwarebefall der heruntergeladenen CAE-Daten zu reduzieren, sollten die Daten vor ihrer Verwendung durch einen Virenscanner geprüft werden. Dies könnte durch die CAE-Software technisch unterstützt werden.

Mitarbeiter am CAE-Arbeitsplatz

Rollen und Aufgaben

Das Projektieren der elektrischen Antriebe übernimmt der Mitarbeiter am CAE-Arbeitsplatz. Dieser Arbeitsplatz kann ein spezifischer Entwicklungs-PC oder die eigene Workstation des Mitarbeiters mit weiteren Programmen, z. B. Office-Anwendungen, sein.

Das Hauptschutzziel ist hierbei die Vertraulichkeit der Informationen. Es müssen technische und organisatorische Maßnahmen getroffen werden, die verhindern, dass kundenspezifische Projektdaten auf nicht dafür vorgesehenen Pfaden nach außen gelangen, etwa durch Kopieren auf USB-Speichermedien.

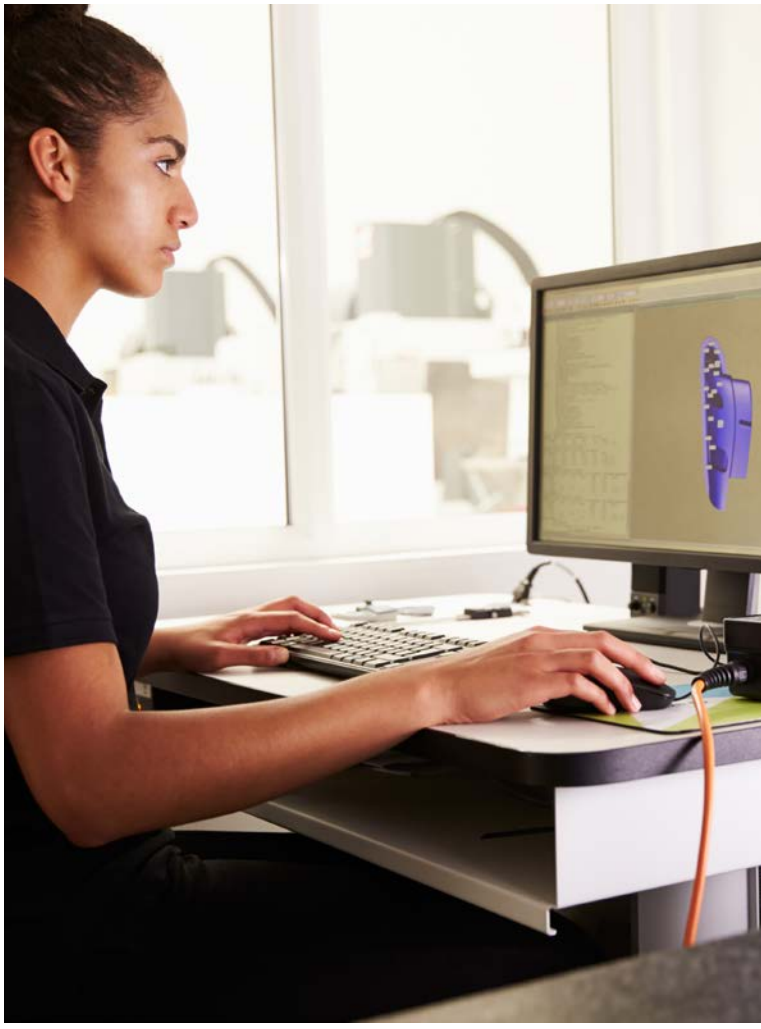
Ein weiterer Aspekt ist die Wahrung der Persönlichkeitsrechte des Mitarbeiters, denen mit der Einführung der Datenschutzgrundverordnung (DSGVO) eine besondere Rolle zugesprochen wird. Bezogen auf das Anwendungsszenario, sollte dem Nutzer mitgeteilt werden, dass für jeden Geschäftsvorgang eine Logdatei angelegt wird. Im Falle möglicher Produkthaftungsfälle kann somit zweifelsfrei geklärt werden, ob die CAE-Daten bei der Auslieferung fehlerbehaftet waren oder beim Integrator falsch verwendet wurden.

Risiken durch den Mitarbeiter

Für den Mitarbeiter am CAE-Arbeitsplatz muss eine Differenzierung der Bedrohungsszenarien vorgenommen werden: Dem Schaden, den der Mitarbeiter als potenzieller Innentäter verursachen kann, müssen die Auswirkungen durch unbeabsichtigtes Fehlverhalten gegenübergestellt werden.

Die größte Bedrohung stellt der Mitarbeiter als Innentäter dar. Mit seinen Kenntnissen über die IT-Infrastruktur kann er gezielt die Sicherheitsmaßnahmen umgehen, um Schadsoftware zu installieren bzw. geistiges Eigentum zu entwenden.

Der Mitarbeiter kann auch unbeabsichtigt zum Innentäter werden, wenn beispielsweise über eine vertrauenswürdig erscheinende E-Mail-Nachricht Schadcode auf dem CAE-Arbeitsplatz installiert wird.



Lösungsskizze/Diskussion

Im folgenden Abschnitt wird ein exemplarischer Lösungsvorschlag für die zuvor beschriebenen Anforderungen vorgestellt. Dieser Lösungsvorschlag kombiniert vorhandene, bekannte technische Lösungen mit aktuellen Ergebnissen anderer Arbeitsgruppen der Plattform Industrie 4.0. Er soll als Diskussionsgrundlage für die weitere Arbeit dienen.

Im Lösungsvorschlag werden die Gedanken aus den vorherigen Publikationen „Sichere unternehmensübergreifende Kommunikation“ (8) und „Sichere Kommunikation für Industrie 4.0“ (9) aufgegriffen. Dabei werden insbesondere die Diskussionen aus (9) zur Realisierung der Security-Maßnahmen entweder mit Mitteln des Transportkanals oder mit Hilfe der übertragenen Nachricht genutzt.

Verwendete Technologien

Bevor der eigentliche Lösungsansatz zum sicheren Bezug von Typinformationen diskutiert wird, werden zunächst gängige Methoden der webbasierten Kommunikation und Autorisierung von Geschäftsbeziehungen erklärt.

Webbasierte Kommunikation

Um eine stabile Kommunikation zu ermöglichen, die möglichst bei allen Kommunikationspartnern zuverlässig funktioniert, ergeben sich verschiedene Anforderungen an die Kommunikation.

Bestehende IT-Infrastruktur wie Firewalls oder Proxys kann Kommunikationsverbindungen unter Bezug auf Quelle oder Ziel oder den verwendeten Kommunikations-Port blockieren. Eine Protokollanalyse kann auch die Protokollkonformität und übertragene Inhalte bewerten. Entsprechend sind bekannte und etablierte Verfahren und Protokolle zu bevorzugen, die dem anerkannten Stand der Technik entsprechen und in der Breite unterstützt werden. Um sicherzustellen, dass beide Kommunikationspartner eine gemeinsame Kommunikationsbasis finden, ist es das Ziel, ein möglichst einheitliches Konzept zu verwenden.

Mögliche Beispiele für Protokolle in den anwendungsorientierten Schichten (Schichten 5–7) im ISO/OSI-Modell, die im unternehmensübergreifenden Kontext etabliert sind, sind HTTP oder FTP. Beide Basisprotokolle erlauben die Verwendung von zumeist explizit konfigurierten Proxys, über die der Informationsfluss kanalisiert und je nach Umsetzung auch kontrolliert werden kann. Informationen werden häufig auch per E-Mail, also mit Hilfe des Protokolls SMTP ausgetauscht. Im vorliegenden Beispiel des Online-Bezugs wird diese Möglichkeit jedoch nicht weiter diskutiert.

Es wird die Nutzung von HTTPS, der mit TLS gesicherten Variante von HTTP, empfohlen und die Verwendung von aktuellen Versionen von TLS (≥ v1.2) vorausgesetzt. Den Kommunikationsteilnehmern ist grundsätzlich überlassen, ob sie die TLS-Verbindung zu den jeweiligen Endgeräten oder von einer Infrastruktur im Kommunikationsweg aufbauen lassen, z. B. durch einen Proxy (Ende-zu-Ende- vs. Transportverschlüsselung). Bei der Verwendung einer direkten Verbindung mittels TLS kann mit Hilfe von Zertifikaten auf Client- und Serverseite eine Identifizierung und Authentifizierung beider an der Kommunikation beteiligten Systeme bereits mit den Mitteln von TLS erreicht werden, so eine gegenseitige Anerkennung der Zertifikate erfolgt. Auf der Anwendungsschicht kann dann auf die Informationen aus den Zertifikaten zurückgegriffen werden. Ist dies nicht möglich, da keine direkte Verbindung aufgebaut wird

oder die Informationen zur Identität im Protokollstack nicht weitergegeben werden, muss die Authentifizierung auf der Anwendungsschicht implementiert werden.

Auf der Präsentationsschicht bzw. Anwendungsschicht werden Webservices verwendet, die mit Protokollen wie REST oder SOAP arbeiten, siehe Beispiel in Abbildung 7 aus dem Diskussionspapier „Sichere Kommunikation für Industrie 4.0“ (9). Eine wesentliche Konsequenz insbesondere aus der möglichen Verwendung von Proxys ist die Verlagerung von Authentifizierungsmechanismen in die höheren Protokollebenen in der Anwendungsschicht.

Authentifizierung und Autorisierung

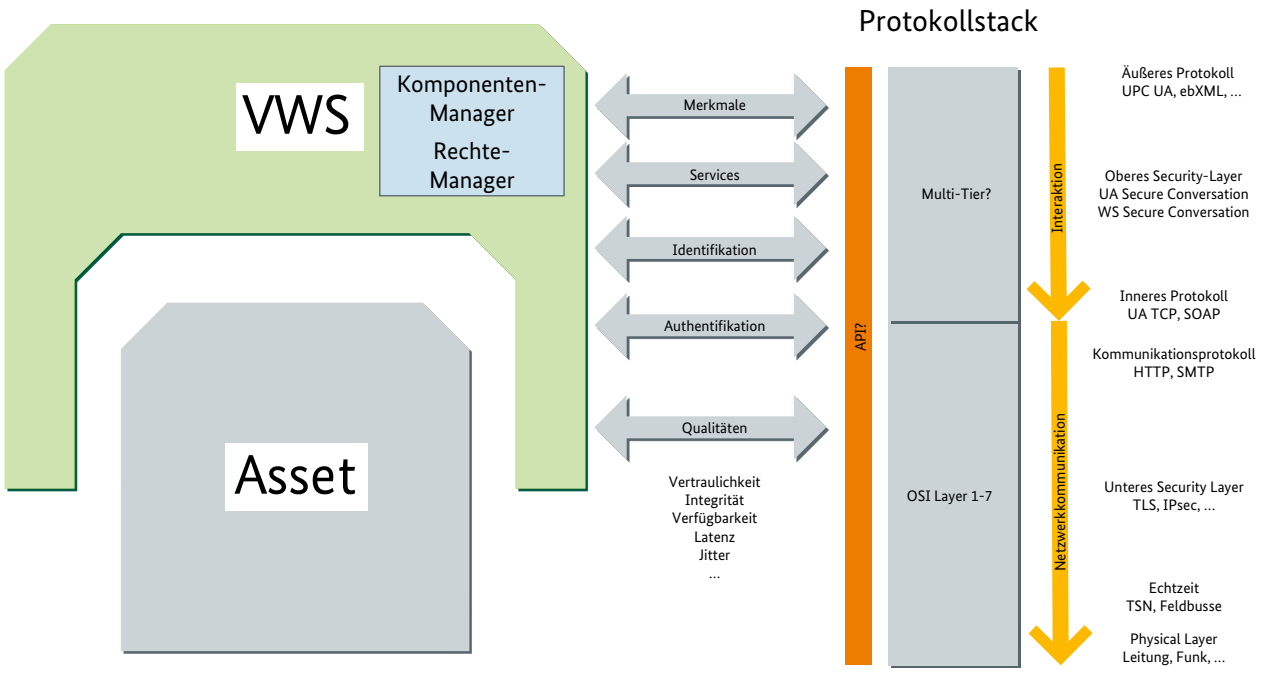
Basierend auf der Authentifizierung kann die Anwendung die Autorisierung vornehmen, also entscheiden, ob bzw. welche Operationen erlaubt sind. Im vorliegenden Fall des Bezugs von CAE-Daten ist dies die Entscheidung, ob und gegebenenfalls welche Daten dem Anfragenden bereitgestellt werden. Im Kontext der Autorisierung wird in vielen Dokumenten, zum Beispiel in den Teilen 3–3 „Systemanforderungen zur IT-Sicherheit und Security-Level“ und 4–2 „Anforderungen an Komponenten industrieller Automatisierungssysteme“ der IEC 62443 (6), auf rollenbasierte Zugriffssteuerung (RBAC) verwiesen. Das Konzept soll daher hier vorgestellt werden, um im Lösungsvorschlag dann auf das mächtigere Attribute Based Access Control (ABAC) einzugehen.

Roll Based Access Control (RBAC)

Der RBAC-Mechanismus beschreibt den klassischen Ansatz zur Autorisierung. Die Realisierung für das Anwendungsszenario ist in Abbildung 8 gezeigt.

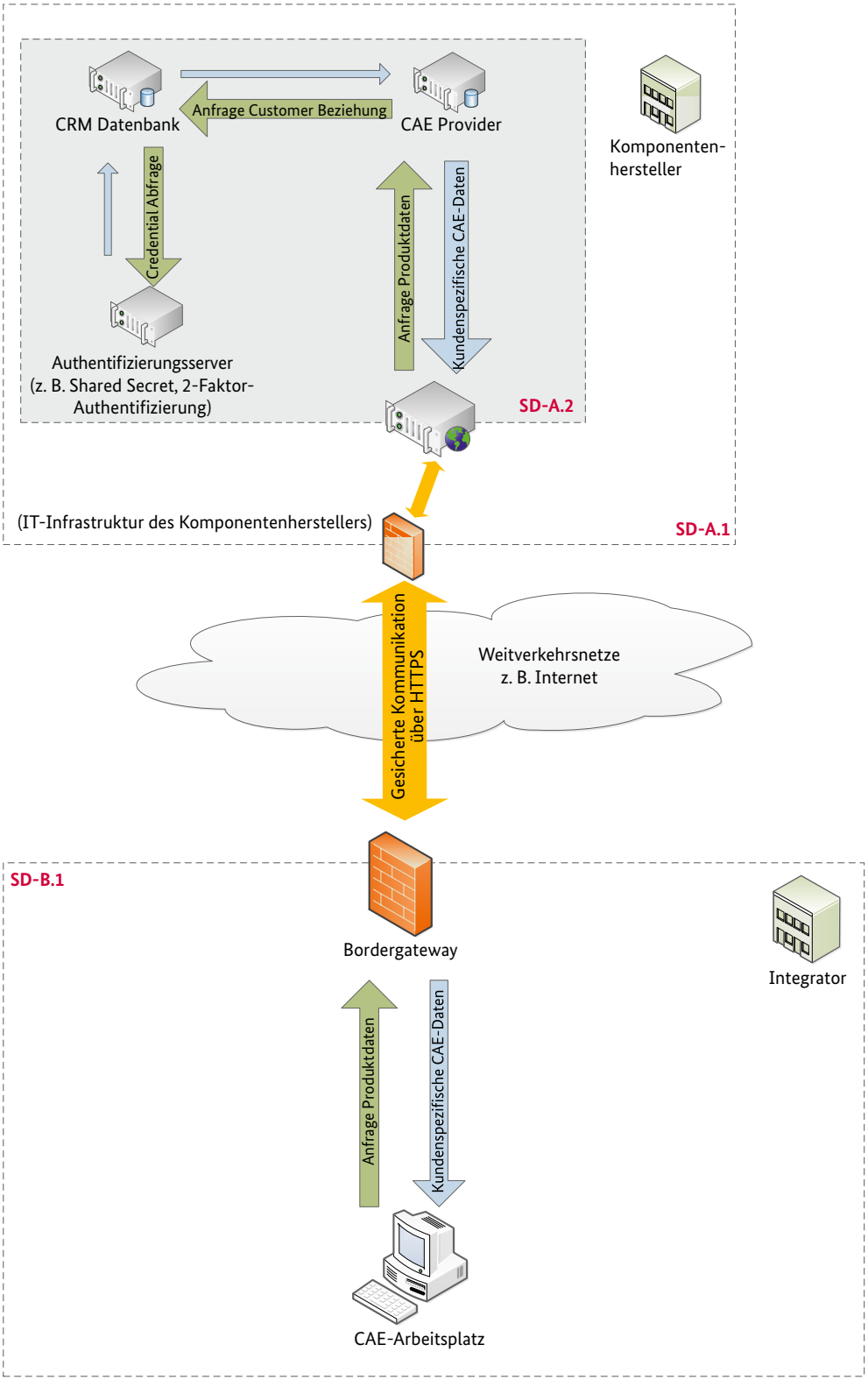
Der Mitarbeiter am CAE-Arbeitsplatz erzeugt eine Anfrage zum Bezug der CAE-Daten zur Entwicklung des elektrischen Antriebs. Eine Anfrage beinhaltet die Kenngrößen der einzusetzenden Komponente, beispielsweise die Nenndrehzahl des Motors. Die Anfrage selbst wird verschlüsselt und über einen gesicherten Kommunikationskanal an den Komponentenhersteller übertragen. Als Übertragungsprotokoll wird HTTPS eingesetzt, welches eine Überprüfung der Authentizität des CAE-Datenservers ermöglicht und die vertrauliche und integre Übertragung erlaubt.

Abbildung 7: Industrie 4.0-Komponente und Protokollstack (9)



Quelle: Plattform Industrie 4.0

Abbildung 8: RBAC-Mechanismus für das gewählte Anwendungsszenario



Quelle: Plattform Industrie 4.0

Bevor die Anfrage in den RBAC-Mechanismus eingespeist wird, siehe Abbildung 8, muss die Anfrage zunächst das an der Grenze zur Sicherheitsdomäne A.1 des Komponentenherstellers (SD-A.1) befindliche Sicherheitsgateway passieren, in dem sie nach den Security-Richtlinien des Herstellers validiert wird. Anschließend wird die geprüfte Anfrage an den Web Server des Komponentenherstellers, der sich in der Sicherheitsdomäne A.2 (SD-A.2) befindet, übermittelt.

Zunächst muss sich jeder Mitarbeiter des Integrators für den Bezug der CAE-Daten beim Komponentenhersteller registrieren und dort ein Nutzerkonto angelegt werden. Der Bezug wird anschließend durch die Anmeldung der Mitarbeiter im System des Herstellers eingeleitet. Zu diesem Zweck werden die Zugangsdaten über die gesicherte HTTPS-Verbindung an den Hersteller übertragen und mit den im Authentifizierungsserver hinterlegten Zugangsdaten verglichen. Im klassischen Fall handelt es sich bei den Zugangsdaten um einen Nutzernamen und ein Passwort oder die 2-Faktor-Authentifizierung.

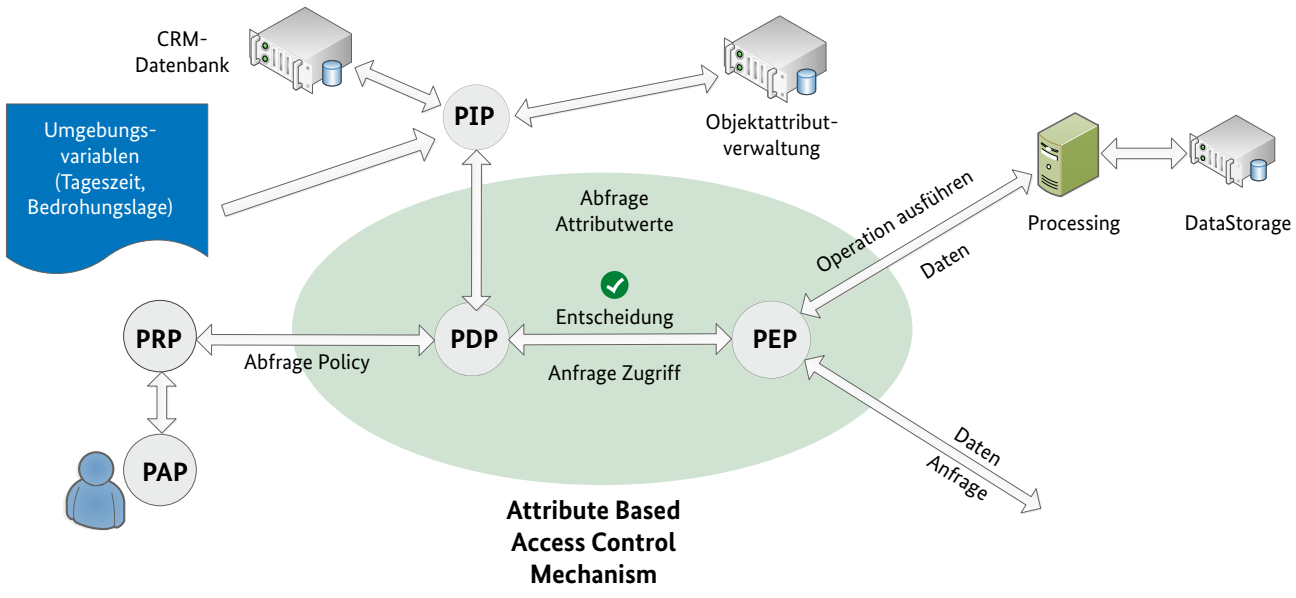
Die CRM-Datenbank überprüft bei erfolgreicher Authentifizierung die Berechtigungen auf die angefragten CAE-Daten. Hierbei ist es möglich, dass je nach Geschäftsmodell für jeden Integrator unterschiedliche CAE-Daten bereitgestellt werden können. Abschließend muss der Mitarbeiter die Auslösung des Geschäftsvorgangs mittels Passwort oder 2-Faktor-Authentifizierung autorisieren. Die abschließende Übertragung der CAE-Daten an den Arbeitsplatz erfolgt über den gleichen gesicherten Kommunikationskanal.

Attribute Based Access Control (ABAC)

Eine flexiblere Weiterentwicklung des rollenbasierten Ansatzes sieht die Verwendung von Attributen anstelle von Rollen vor: „Attribute Based Access Control“ (ABAC). ABAC ist noch vergleichsweise jung und in der Industrie noch wenig verbreitet, für Industrie 4.0 wird aber die Mächtigkeit des Konzepts benötigt (10). Eine technisch fundierte Umsetzungsstrategie ist beispielsweise in der NIST SP 800-162 „Guide to Attribute Based Access Control“ (11) zu finden, welche die Grundlage für die Lösungsskizze bildet.

Zunächst werden zur Schaffung eines einheitlichen Verständnisses die wichtigsten Begrifflichkeiten erläutert.

Abbildung 9: Vorgehen ABAC



Quelle: Plattform Industrie 4.0

- **Subjekt:** Ein Subjekt beschreibt die Entität, die Anfragen stellt, um Operationen auf einem Objekt auszuführen. Dabei kann es sich um einen menschlichen Nutzer oder um eine selbständig agierende Anwendung handeln. Im Rahmen dieses Dokuments ist Subjekt gleich dem Mitarbeiter/Nutzer zu setzen.

- **Objekt:** Ein Objekt beschreibt die Ressource, auf die das Subjekt eine Operation ausführen möchte, beispielsweise ein Gerät, eine Datei oder ein Prozess.

- **Attribut:** beschreibt die Eigenschaften von Subjekt, Objekt oder Umgebungsvariable. Attribute bestehen immer aus einem Name-Werte-Paar.

- **Policy:** Eine Policy beinhaltet die Regeln und Beziehungen zwischen dem Subjekt und dem Objekt. Für den ABAC-Mechanismus besteht die Policy aus den Zugriffsrechten des Subjektes auf dieses Objekt.

Gegenüber der verhältnismäßig einfach zu realisierenden rollenbasierten Zugriffssteuerung sind bei ABAC eine Vielzahl an Komponenten am Entscheidungsprozess beteiligt. Deren Zusammenspiel zeigt Abbildung 9. Für die interne Verarbeitung und Verwaltung der Policy-Informationen könnte das eXtensible Access Control Markup Language-Format (XACML) zum Einsatz kommen (12).

Als ausführendes Organ des ABAC-Mechanismus ist der Policy Enforcement Point (PEP) vorgesehen. Im ersten Schritt fängt der PEP die Anfrage ab und konvertiert sie in eine operative Anforderung, beispielsweise darf Mitarbeiter X (Subjekt) auf das Dokument YZ (Objekt) zugreifen (Operation).

Der Policy Decision Point (PDP) besitzt die Aufgabe, zu entscheiden, ob der Zugriff auf die angefragten Daten gewährt wird. Hierzu nutzt er zwei Quellen: den Policy Retrieval Point (PRP) und den Policy Information Point (PIP).

Der Policy Retrieval Point (PRP) kann in Form einer Datenbank realisiert werden und beinhaltet die aktuell gültigen Policies des Unternehmens. Die Verwaltung der Policies übernimmt der Policy Administration Point (PAP), mit dessen Hilfe Anpassungen am PRP vorgenommen werden können. Während des ABAC-Prozesses lädt der PDP die Policies aus dieser Datenbank herunter.

Der Policy Information Point (PIP) unterstützt den PDP bei der Auswertung der Policies. Als Quellen für den PIP dienen die Objektattributverwaltung, die aktuellen Umgebungsvariablen (Tageszeit, aktuelle Bedrohungslage etc.) und die CRM-Datenbank.

In der CRM-Datenbank können weitergehende Subjektattribute hinterlegt sein, die zum Beispiel vertragliche Vereinbarungen zwischen Komponentenhersteller und Integrator betreffen. Die Objektattributverwaltung enthält wiederum die freigegebenen Objekteigenschaften für das anfragende Subjekt. Als einfaches Beispiel wären hier Dokumente mit dem Vermerk „geheim“ zu nennen.

Nachdem der PDP alle notwendigen Informationen erhalten hat, erfolgt die Evaluierung der Anfrage gegenüber der Policy. Die Entscheidung wird abschließend an den PEP übermittelt, welcher bei einer positiven Entscheidung die Freigabe zur Ausführung der Operation mit den relevanten Angaben zur Bearbeitung gewährt. Entsprechend den Angaben können im Processing die richtigen Daten zusammengestellt und Aufzeichnungen für Nachverfolgungs- oder Abrechnungszwecke erzeugt werden.

AASX-Dateiformat

Im Dokument „Details of the Asset Administration Shell“ (2) wird ein Dateiformat für die Übertragung von Informationen zwischen Industrie 4.0-Komponenten vorgeschlagen, das auf den Open Packaging Conventions (4) basiert. Dieses „AASX“ genannte Dateiformat kann die zugrundeliegenden Eigenschaften nutzen. Es bietet einen Container, in dem sich Informationen aller Art transportieren lassen.

Im Konzept der Open Packaging Conventions und der Verwendung im AASX-Format ist unterstützt, den Inhalt durch digitale Signaturen zu beglaubigen, so dass die Authentizität der übertragenen Informationen jederzeit unabhängig vom verwendeten Transportweg überprüft werden kann. Bei Verwendung des AASX-Dateiformats entfällt also die Notwendigkeit, die Authentizität über die Kommunikationsprotokolle sicherzustellen.

Eine Verschlüsselung der Daten ist in Open Packaging Conventions nicht festgelegt. Für das AASX-Format sind in „Details of the Asset Administration Shell“ (2) Möglichkeiten für den Schutz der Vertraulichkeit diskutiert. Im Rahmen des vorliegenden Dokuments wird davon ausgegangen, dass der Schutz der Vertraulichkeit durch die verwendete Transportmethode, hier das HTTPS-Protokoll, sichergestellt wird.

Lösungsvorschlag

Der Lösungsansatz in diesem Diskussionspapier sieht die Nutzung einer attributbasierten Zugriffssteuerung (Attribute Based Access Control, kurz ABAC) vor, um die höhere Flexibilität für zukünftige Konzepte der Zusammenarbeit zwischen Unternehmen nutzen zu können. Da die Verwendung von ABAC Anforderungen an die Kommunikation stellt, wird in diesem Lösungsvorschlag auf Details der Verwendung von ABAC eingegangen.

Sicherheitsdomänen

Das für die Realisierung des beschriebenen Anwendungsfalls gedachte System ist in Abbildung 10 gezeigt. Hierbei können zunächst drei Sicherheitsdomänen identifiziert werden: Die Domäne „SD-A“ ist beim Komponentenhersteller verortet und gliedert sich in die Bereiche IT-Infrastruktur („SD-A.1“) und „SD-A.2“, welcher den webservicebasierten ABAC-Mechanismus beinhaltet. Der Integrator besitzt die dritte Sicherheitsdomäne „SD-B“, die den CAE-Arbeitsplatz zum Bezug der Typinformationen beinhaltet.

Vorgehensbeschreibung

Der skizzierte Lösungsvorschlag beschreibt die logischen Schritte zum Bezug von CAE-Daten, wobei auf Seiten des Komponentenherstellers ABAC zum Einsatz kommt, siehe Abbildung 10. Ein Vorschlag für die technische Realisierung kann dem Diskussionspapier der UAG „Rechte und Rollen“ der Plattform Industrie 4.0 (10) entnommen werden. Abbildung 11 zeigt die Schritte im Swimlane-Diagramm. Im Einzelnen sind folgende Schritte auszuführen:

Anfrage an den Komponentenhersteller

Der Mitarbeiter beim Integrator hat die Aufgabe, einen elektrischen Antrieb zu projektieren [1] und nutzt dazu den CAE-Arbeitsplatz. Da die von ihm benötigten Informationen noch nicht im System hinterlegt sind, stellt er mit Hilfe der CAE-Software eine Anfrage an den Komponentenhersteller [2]. Diese Anfrage beinhaltet die für den ABAC-Prozess notwendigen Objekt- und Subjekt-Attribute sowie die auszuführende Operation. Eine Abstimmung zu den Attributen und ihrer Bedeutung ist eine notwendige Voraussetzung im unternehmensübergreifenden Kontext. Als relevante Attribute, deren Übertragung im verwendeten Protokoll für die Webservices unterstützt sein muss, sind im vorliegenden Beispiel vorgesehen:

- Anfragende Stelle (Subjekt):
  - Mitarbeiter mit weiteren Attributen, wie Rolle
  - Anfragendes Unternehmen mit weiteren Attributen
  - CAE-Software mit weiteren Attributen, wie Softwarestand oder Lizenzschlüssel
- Angefragte Information (Objekt):
  - Art/Teilenummer/Auswahlparameter
- Gewünschte Operation:
  - Lesen/Kopieren

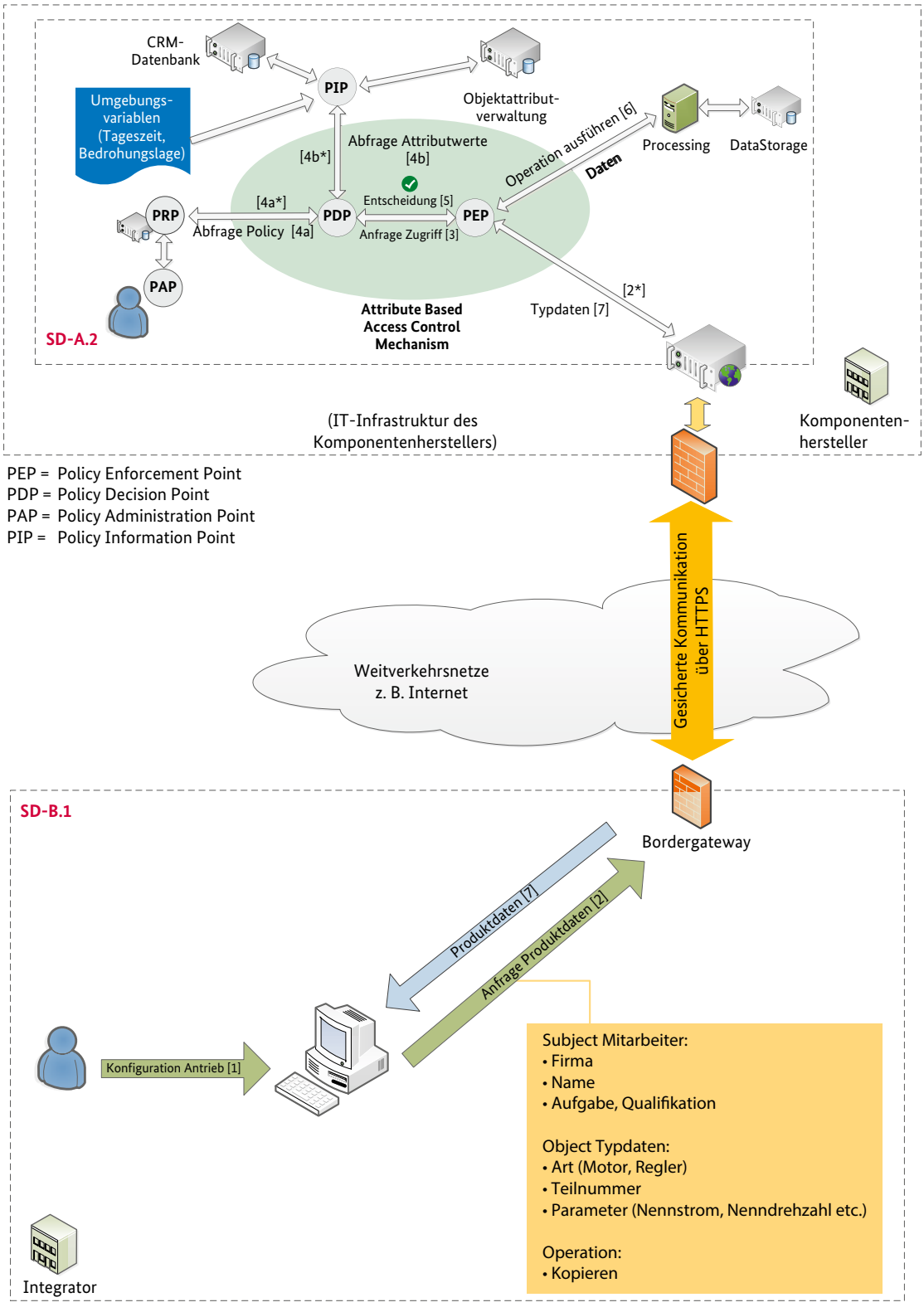
Übertragung der Anfrage

Die Anfrage muss nun über einen gesicherten Kommunikationskanal an den Komponentenhersteller übertragen werden. Hierfür ist als Übertragungsprotokoll HTTPS vorgesehen, das eine Überprüfung der Authentizität des Downloaddienstes des Komponentenherstellers ermöglicht und die vertrauliche und integre Übertragung erlaubt.

Im ersten Schritt muss die Anfrage das an der Grenze der Sicherheitsdomäne „SD-B.1“ befindliche Sicherheitsgateway passieren. Hier sind mehrere Arten von Sicherheitsgateways üblich, die einen direkten Einfluss auf die Kommunikation haben:

- Handelt es sich hier nur um eine simple Firewall, könnte die Anfrage direkt passieren.
- Bei einem einfachen Proxy würde der Proxy den Datenstrom der Anfrage unverändert übertragen.
- Bei einem Proxy mit Authentifizierung müsste sich das Subjekt beim Integrator gegenüber dem Proxy des Integrators ausweisen. Dies erfolgt häufig über die Kennung des Benutzers und eine Einbindung in ein lokales Active Directory. Nur wenn der Benutzer (oder ein System) die Erlaubnis hat, mit dem Internet zu kommunizieren, wird die Verbindung durchgelassen.

Abbildung 10: Realisierung des ABAC-Mechanismus zum sicheren Download von Typinformationen



Quelle: Plattform Industrie 4.0

- Bei einem filternden Webgateway wird zusätzlich der Inhalt des HTTP-Datenstroms analysiert und nicht erlaubte oder gefährliche Inhalte, zum Beispiel Viren, werden blockiert. Bei HTTPS-Verbindungen ist dies damit verbunden, dass die verschlüsselte Verbindung aufgebrochen wird, damit die Inhalte gefiltert werden können. Dieses Aufbrechen der Verbindung unterbricht die Integritäts- und Vertraulichkeitskette zwischen Arbeitsplatz und Komponentenhersteller und macht zugleich die Verwendung von Clientzertifikaten zur Authentifizierung unmöglich. Konzepte zur Lösung dieser Schwierigkeit existieren in Vorschlägen wie Multi-Context TLS für Middleboxes (13), haben aber wenigstens bisher keinen Eingang in die Standardisierung gefunden.

  Am Ausgang des Webgateways wird eine neue, verschlüsselte Kommunikationsverbindung zum Komponentenhersteller aufgebaut.

Im professionellen Unternehmensumfeld ist davon auszugehen, dass filternde Webgateways zum Einsatz kommen, und die Kommunikation ist entsprechend zu gestalten. Eine Umsetzung für die vorgeschlagene Verwendung von Webservices könnte mittels Webservice-Security (WS-Security) in SOAP erfolgen. In der Anfrage wären die Zugangsdaten in Form von Security-Tokens enthalten und die Anfrage wäre digital signiert.

Auf Seiten des Komponentenherstellers muss die Anfrage zunächst das an der Grenze zur Sicherheitsdomäne „SD-A.1“ befindliche Sicherheitsgateway passieren, in dem sie nach den Security-Richtlinien des Herstellers validiert wird. Anschließend wird die geprüfte Anfrage an den Web Server der Sicherheitsdomäne „SD-A.2“ übermittelt. Im Web Server wird eingangs eine initiale Prüfung der Konsistenz der Anfrage durchgeführt, dann wird die Zugriffsberechtigung mittels ABAC ermittelt (siehe Abbildung 10 Prozess 2*).

Authentifizierung und Autorisierung

Die in Abbildung 10 gezeigte Zugriffssteuerung validiert die Anfrage entsprechend dem in Abschnitt „Attribute Based Access Control“ beschriebenen Vorgehen. Hierbei muss die Authentizität der Anfrage geprüft werden. Dies könnte anhand einer digitalen Signatur der Anfrage und einer Bestätigung der Identität und Attribute des Anfragenden durch ein X.590-Zertifikat erfolgen.

Wichtig ist, dass der Nachrichtenaustausch der beteiligten Systeme im ABAC-Aufbau des Komponentenherstellers in den Prozessschritten [3], [4] und [5] in Abbildung 10 über einen gesicherten Kommunikationskanal erfolgt. Auch wäre es denkbar und unter Umständen angebracht, den Policy Decision Point (PDP) und den Policy Enforcement Point (PEP) in eine weitere Sicherheitsdomäne auszulagern. Diese böte den Vorteil, dass ein Angreifer eine weitere Hürde überwinden müsste, um die Entscheidung manipulieren zu können.

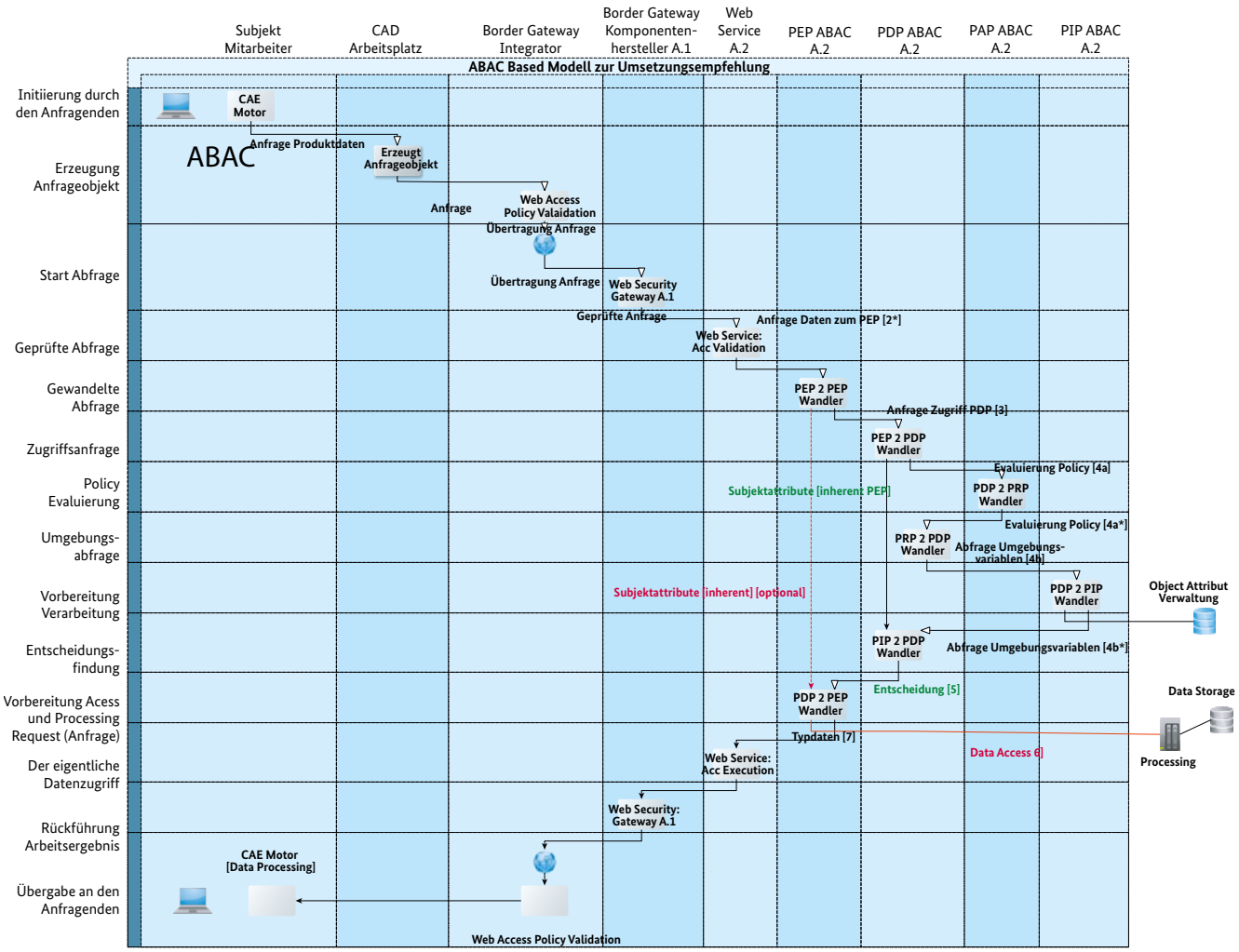
Um die Objekt- und Subjekt-Attribute der Anfrage gegen die geltende Policy zu validieren, sollte diese ebenfalls attributbasiert aufgebaut sein. Hierzu bietet sich die Verwendung des eXtensible Access Control Markup Language-Format (XACML) an, welches von der OASIS standardisiert wurde (12). Nach diesem Standard besteht eine Policy aus Regeln, welche das anfragende Subjekt in Form eines Targets modelliert.

Konnte die Anfrage vom PDP erfolgreich validiert werden, gestattet der PEP die Ausführung der Operation [6]. Bezogen auf den Anwendungsfall wird mittels Webservices auf den mit „Processing“ bezeichneten Rechner zugegriffen. Dieser erstellt entsprechend den übermittelten Objektattributen eine Instanz der angefragten CAE-Daten.

Übertragung des Datensatzes an den Anfragenden

Im abschließenden Prozessschritt [7] werden die Typdaten an den CAE-Rechner gesendet. Hierzu werden die Daten verschlüsselt und über die gleiche gesicherte Verbindung übertragen. Dabei bleibt der Datensatz während und nach der Übertragung durch die Verwendung der Signaturmechanismen des AASX-Formats überprüfbar. Die Unterstützung des AASX-Formats im Sicherheitsgateway ist vorausgesetzt.

Abbildung 11: Swimlane-Diagramm zur Veranschaulichung des Lösungsvorschlags



Quelle: Plattform Industrie 4.0

Zusammenfassung und Ausblick

Dieses Dokument beschreibt die Security-Anforderungen an den sicheren Bezug von CAE-Daten, also Typ-Informationen, aus Sicht der beteiligten Stakeholder. Basierend auf den Anforderungen wird ein Lösungsvorschlag erarbeitet, der weitere Konzepte der Plattform Industrie 4.0 wie das Dateiformat für den Austausch von Informationen von Verwaltungsschalen und zum Rechtemanagement bei Industrie 4.0-Komponenten aufgreift.

Kernaussagen

Für den unternehmensübergreifenden Bezug von CAE-Daten ist die Verwendung von Webservices über HTTPS zu empfehlen. Aufgrund der häufigen Verwendung von Sicherheitsgateways sollte die Authentifizierung mit X.509-Zertifikaten nicht auf der TLS-Transportschicht vorausgesetzt werden. Die Daten werden im Beispiel mit dem AASX-Datenformat ausgetauscht, das bereits Mechanismen für den Schutz von Integrität und Authentizität bereitstellt.

Verknüpfung mit anderen Themen

Die Ausgestaltung sicherer Kommunikation lässt sich nicht von anderen Themen trennen, die parallel diskutiert und erarbeitet werden. Insbesondere die Umsetzung des Rechtemanagements im Industrie 4.0-Kontext erfordert die sichere Bereitstellung von Informationen zur Identität des Kommunikationspartners. Die Kommunikation muss dies technisch unterstützen, etwa indem eine sichere Authentifikation und die sichere Übertragung von Attributinformationen unterstützt werden. Auch ist es notwendig, eine Struktur zur gegenseitigen Anerkennung von Identitäten und digitalen Zertifikaten zu realisieren.

Die International Data Spaces Association arbeitet an einem eigenen Konzept zum sicheren Austausch von Daten unter anderem im Industrieumfeld. Es ist geplant, ein vergleichendes Diskussionspapier zu erstellen.

Übertragung von Instanzinformationen

Ein verwandtes Thema ist der Austausch von Informationen zu einzelnen Entitäten („Instanzen“), bei dem möglicherweise der gleiche oder ein weiterentwickelter Lösungsvorschlag zum Einsatz kommen kann. Die Betrachtung der Security bedarf eines entsprechenden Anwendungsszenarios und wird andere oder zusätzliche Anforderungen ergeben.

Informationen zu einer Entität könnte grundsätzlich die Entität selbst beziehen. Im Fall eines technischen Produkts könnten dies z. B. Lizenzrechte sein, durch die das Produkt weiß, welche Leistungen es anbieten kann. In diesem Fall wäre die Entität selbst in der Lage, sich auszuweisen.

In anderen möglichen Szenarien könnte ein Benutzer oder ein System instanzspezifische Daten beziehen wollen, etwa Kalibrierdaten. In diesem Szenario wird die zusätzliche Schwierigkeit zu betrachten sein, wie der Benutzer im Fall vertraulicher Daten nachweisen könnte, dass er tatsächlich Anrecht auf die Daten hat, etwa, weil er Eigentümer der Entität ist oder die Entität sich in seinem Besitz befindet. Die Bedeutung und Verwendung (sicherer) Identitäten wird eine deutlich größere Bedeutung haben.

Glossar

ABAC	Attribute Based Access Control
Brute Force Attack	Lösen eines Geheimnisses durch Ausprobieren aller möglichen Kombinationen
CAE	Computer Aided Engineering
CRM	Customer Relationship Management
DRM	Digital Rights Management
HTTPS	HyperText Transport Protocol (S: secured via TLS)
PAP	Policy Administration Point
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PIP	Policy Information Point
PRP	Policy Retrieval Point
RBAC	Role Based Access Control
SD	Sicherheitsdomäne
TLS	Transportation Layer Security
XACML	eXtensible Access Control Markup Language

Abbildungsverzeichnis

Literaturverzeichnis

1. **Ergebnispapier „Fortschreibung der Anwendungsszenarien der Plattform Industrie 4.0“**. Berlin: *Plattform Industrie 4.0*, 2016.

2. **Details of the Asset Administration Shell:** *Part 1 – The exchange of information between partners in the value chain of Industrie 4.0.* Frankfurt: ZVEI, 2018.

3. **DIN SPEC 91345:2016-04**: *Referenzarchitekturmodell Industrie 4.0 (RAMI4.0).* Berlin: Beuth Verlag, 2016.

4. **Information technology** – *Document description and processing languages – Office Open XML File Formats – Part 2*: Open Packaging Conventions. ISO/IEC 29500-2:2012.

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

6. **Industrial Communication Networks** – *Security for industrial automation and control systems*. IEC 62443.

7. **Diskussionspapier „Integrität von Daten, Systemen und Prozessen als Kernelement der Digitalisierung“.** Berlin: *Plattform Industrie 4.0*, 2018.

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

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

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

11. **Guide to Attribute Based Access Control (ABAC)** – *Definition and Considerations. s.l.*: NIST, 2014.

12. **eXtensible Access Control Markup Language (XACML) Version 3.0**. [PDF] OASIS 2017.

13. **And Then There Were More: Secure Communication for More Than Two Parties.** Nayler, David et al., *Proceedings of the 13th International Conference on emerging Networking EXperiments and Technologies*. 2017.

AUTOREN

Carsten Angeli, KUKA Roboter GmbH | André Braunmandl, Bundesamt für Sicherheit in der Informationstechnik | Prof. Dr. Tobias Heer, Hirschmann Automation & Control GmbH | Dr. Christian Haas, Fraunhofer IOSB | Markus Heintel, Siemens AG | Dr. James Hunt, Aicas GmbH | Dr. Lutz Jänicke (Leitung), PHOENIX CONTACT GmbH & Co. KG | Fabian Mackenthun, NXP Semiconductors Germany GmbH | Jens Mehrfeld, Bundesamt für Sicherheit in der Informationstechnik | Till Oefler, Institut für Automation und Kommunikation e.V. | Florian Patzer, Fraunhofer IOSB | Tobias Pfeiffer, Festo AG & Co. KG | Wolfgang Stadler, SICK AG | Detlef Tenhagen, HARTING Stiftung GmbH & Co. KG | Klaus Theuerkauf, Siemens Mobility GmbH | 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