PLATTFORM INDUSTRIE4.0

DISKUSSIONSPAPIER

Durchsetzung von Nutzungsbedingungen auf Basis der Verwaltungsschale

Impressum

Herausgeber
Bundesministerium für Wirtschaft und Klimaschutz (BMWK)
Öffentlichkeitsarbeit
11019 Berlin
www.bmwk.de

Redaktionelle Verantwortung
Plattform Industrie 4.0
Bülowstraße 78
10783 Berlin

Stand
April 2024

Diese Broschüre wird ausschließlich als Download angeboten.

Gestaltung
PRpetuum GmbH, 80801 München

Bildnachweis
Torsten Asmus / iStock / Titel

Zentraler Bestellservice für Publikationen der Bundesregierung:
E-Mail: publikationen@bundesregierung.de
Telefon: 030 182722721
Bestellfax: 030 18102722721

Inhalt

1 Ausgangssituation und Zielsetzung

Das Konzept der Asset Administration Shell (AAS) [1], der digitale Zwilling der Industrie 4.0, hat sich für die Strukturierung von Informationen, für die semantische Interoperabilität und für den Zugriff auf bzw. die Nutzung von Inhalten etabliert.

Jegliche Informationen eines Assets können in Submodellen der AAS abgelegt werden. Sowohl im Industrie 4.0-Kontext als auch im Kontext von Datenräumen wie Catena-X [2] oder Manufacturing-X [3] [4] wird sie verwendet.

Die Verwendungsformen sind vielseitig, z. B.:

- als digitaler Zwilling eines Assets [5]
- referenziert über das digitale Typenschild [6]
- als digitaler Zwilling eines Assets [5] kombiniert mit einer Digital Twin Registry, über die Suchanfragen gestellt werden können [7]
- als technische Implementierung des Digitalen Produktpasses (DPP) für Industrie 4.0 [8]

Aus der vielfältigen Nutzung der Industrie 4.0-Verwaltungsschale AAS ergeben sich Anforderungen an die Gestaltung und Durchsetzung von Nutzungsbedingungen für Industrie 4.0-Daten im Allgemeinen und für den Zugriff auf die Verwaltungsschale AAS bzw. deren Teilmodelle im Besonderen.

Dieses Dokument untersucht detailliert die Möglichkeiten, den Zugriff auf Industrie 4.0-Daten in Abhängigkeit von deren Nutzungsbedingungen zu definieren. Dies erfordert mehr oder weniger komplexe Zugriffsregeln, die u. a. abhängig sein können von der Nutzungsvariante (s. o.), von Informationen über das anfragende Subjekt, von den Daten selbst, auf die zugegriffen werden soll, von der Umgebung oder von rechtlichen/regulatorischen Nebenbedingungen. Die Untersuchungen gelten sowohl für den Datenzugriff zwischen Menschen und Maschine als auch zwischen Maschinen.

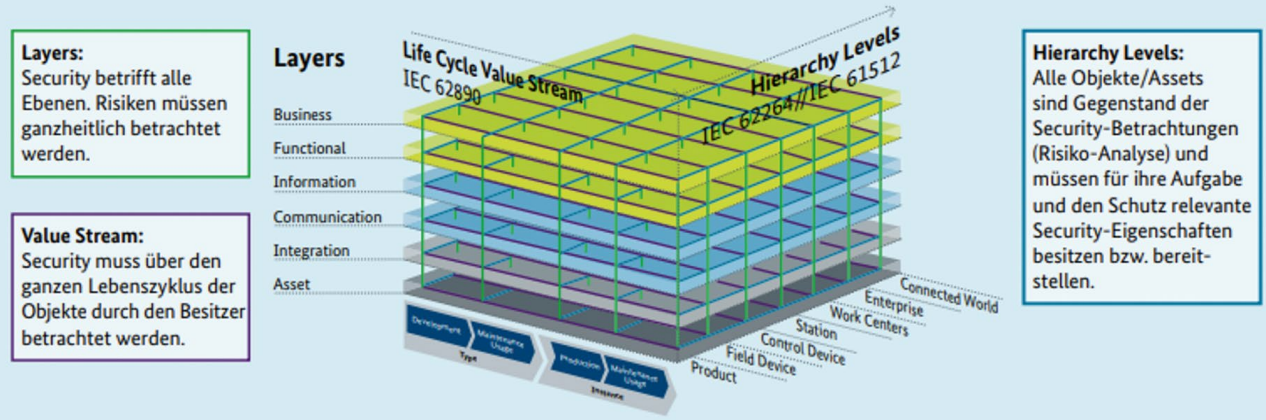
Daher wird in diesem Dokument die attributbasierte bzw. regelbasierte Zugriffskontrolle [9] als Methode zur Abbildung von Nutzungsbedingungen diskutiert. Insbesondere wird die Bedeutung der Zugriffskontrolle im Kontext von Industrie 4.0 dargestellt und anhand detaillierter Beispiele erläutert.

Das Dokument befasst sich auch mit der Semantik von Attributen, die für die Zugriffskontrolle auch über ein geschlossenes (Daten-)Ökosystem hinaus einheitlich interpretierbar sein sollten, bzw. mit den Problemen, die auftreten, wenn eine semantische Einheitlichkeit nicht gegeben ist.

Der vorliegende Ansatz umfasst den gesamten Lebenszyklus eines Assets, da die Security-Maßnahmen umfassend wirksam sein müssen, um das gewünschte Schutzniveau für das Asset erreichen zu können (vgl. Publikation „Security in RAMI4.0“) [10]. RAMI4.0 beschreibt strukturiert die wesentlichen Elemente eines Objekts/Assets mittels eines aus drei Achsen bestehenden Schichtenmodells (vgl. Abbildung 1). Komplexe Zusammenhänge können so in kleinere, überschaubare Abschnitte aufgegliedert werden, indem durch Kombination aller drei Achsen zu jedem Zeitpunkt im Lebenslauf eines Assets der jeweils relevante Aspekt dargestellt wird. Die drei Achsen sind:

- Architektur-Achse (Layers) mit sechs Schichten zur Darstellung der für die Rolle des Assets relevanten Informationen;
- Verlauf-Achse (Value Stream) zur Darstellung des Lebenslaufs eines Assets und des Wertschöpfungsprozesses in Anlehnung an die Norm IEC 62890;
- Hierarchie-Achse (Hierarchy Levels) zur Zuweisung funktionaler Modelle zu einzelnen Ebenen in Anlehnung an die Normen DIN EN 62264-1 und DIN EN 61512-1.

Abbildung 1: Referenzarchitekturmodell Industrie 4.0 (RAMI4.0)



Quelle: Plattform Industrie 4.0 und ZVEI

Abbildung 1 zeigt die Einbettung der Security im RAMI4.0 in allen drei Achsen und verdeutlicht den integralen Charakter der Security. Sie stellt keine separate Schicht oder zusätzliche Hierarchie-Ebene dar, sondern ist über den gesamten Lebenszyklus auf allen Schichten und Hierarchie-Ebenen wirksam. Vergleichbar mit einem Gebäude, das mit Stahl armiert wurde, gewährleistet die Security damit die Stabilität von RAMI4.0 und schützt gegen mögliche Angriffe.

Kapitelübersicht

Kapitel 1 beschreibt die Ausgangssituation und Zielsetzung

Kapitel 2 betrachtet den Industrie 4.0-Kontext

Kapitel 3 analysiert Use Cases und Anforderungen

Kapitel 4 beschreibt Anwendungsbeispiele zum Produktionsmittel der Zukunft

Kapitel 5 betrachtet Pfadabhängigkeiten und semantische Einheitlichkeit

Kapitel 6 schließt mit einem Fazit und einer Zusammenfassung

Kapitel 7 bis 9 zeigen die Verzeichnisse (Literatur, Abbildungen, Tabellen)

Kapitel 10 enthält als Anhang Beispiele und Vorteile des Lösungsvorschlags

1.1 Attributbasierte Zugriffskontrolle

Motivation

Traditionelle Zugriffskontrollmodelle, die auf starren Rollen und Berechtigungen basieren, stoßen in dynamischen und komplexen IT-Umgebungen an ihre Grenzen, da sie häufig nicht in der Lage sind, die feingranulare Kontrolle und Flexibilität zu bieten, die moderne Systeme erfordern. Attributbasierte Zugriffskontrollmodelle (ABAC) wurden als Lösung für die Probleme traditioneller Modelle entwickelt. ABAC bietet eine Reihe von Vorteilen und gilt als zukunftsträchtige Lösung für die Zugriffskontrolle in modernen Systemen.

Konzeption

ABAC basiert auf der Idee, dass der Zugang zu Ressourcen nicht nur von den technischen und menschlichen Identitäten abhängt, sondern auch von den Attributen der Entitäten und den Attributen der Ressourcen.

Die Notwendigkeit, Zugriffskontrollen flexibler zu gestalten, wurde um das Jahr 2000 formuliert. Dies betrifft insbesondere logische Zugriffskontrollen [11], die von einfachen Zugriffskontrolllisten über leistungsfähigere, rollenbasierte Zugriffe bis hin zu einer hochflexiblen Methode der Zugriffsgewährung auf Basis von Attributbewertungen reichen.

Es wurden Konzepte veröffentlicht, wie große Organisationen „übergreifend“ die Attributbewertung als Zugriffsmöglichkeit innerhalb und zwischen Organisationen nutzen können, um die Weiterentwicklung ihrer logischen Zugriffskontrollarchitekturen zu unterstützen. Kurz darauf wurde die attributbasierte Zugriffskontrolle (ABAC) als Zugriffskontrollmodell zur Förderung des Informationsaustauschs zwischen unterschiedlichen und ungleichen Organisationen empfohlen. ABAC ist ein logisches Zugriffskontrollmodell, das sich dadurch auszeichnet, dass es den Zugriff auf Objekte kontrolliert, indem es die Regeln anhand der Attribute der Entitäten (Subjekte und Objekte), der Aktionen und der für eine Anfrage relevanten Umgebung bewertet.

i In seiner einfachsten Form basiert ABAC auf der Bewertung von Subjektattributen, Objektattributen, Umgebungsbedingungen und einer formalen Beziehung oder Zugriffskontrollregel, die die zulässigen Operationen für Subjekt-Objekt-Attribut- und Umgebungsbedingungskombinationen definiert.

Lösungsraum

Alle ABAC-Lösungen enthalten diese zuvor genannten grundlegenden Kernfähigkeiten und sind in der Lage, sowohl Discretionary Access Control- (DAC; „Benutzerbestimmbare Zugriffskontrolle“) [12] als auch Mandatory Access Control (MAC)-Modelle (berücksichtigen die Sensitivität von Informationen) [12] durchzusetzen. Darüber hinaus können ABAC-Systeme risikoadaptierbare Zugangskontrolllösungen (RAdAC) [13] ermöglichen, wobei Risikowerte als variable Attribute ausgedrückt werden.

Die Regeln oder Richtlinien, die in einem ABAC-Modell implementiert werden können, sind nur in dem Maße begrenzt, wie es die verwendete Programmiersprache vorgibt. Diese Flexibilität ermöglicht es einer großen Anzahl von Subjekten, auf eine große Anzahl von Objekten zuzugreifen, ohne individuelle Beziehungen zwischen jedem Subjekt und jedem Objekt festzulegen.

i Einem **Subjekt** werden beispielsweise bei seiner Einstellung eine Reihe von Subjekt-Attributen zugewiesen *(z. B. „Klaus Mustermann ist Servicespezialist in der Industrial Space Service SE“).*

Einem **Objekt** werden seine Objekt-Attribute bei der Erstellung zugewiesen *(z. B. Inline-Automatisierung für Prozessmaschinen mit integriertem Puffersystem und Produktionsleitrechner mit Bildverarbeitung für Bruchratenreduzierung unter Reinraumbedingungen).*

Ressourcenobjekte können ihre Attribute z. B. als Ergebnis automatischer Sensorik erhalten.

Der Betreiber eines Objekts erstellt eine **Zugriffskontrollregel**, um die Menge der zulässigen Operationen zu regeln *(z. B. alle Servicetechniker mit einer bestimmten Zertifizierung eines bestimmten Service-Unternehmens können die Fernwartung der KI-Bildverarbeitung eines bestimmten Produktionsleitrechners einer Produktionsmaschine in einem bestimmten Zeitfenster durchführen).*

Diese Zugriffskontrollregel ist jedoch flüchtig, da sie sich mit dem Zustand des Ressourcenobjekts ändern kann *(im genannten Beispiel könnte sich der Zustand des Produktionsleitrechners ändern, wenn die Produktionsmaschine ausfällt. In diesem Fall müsste die Zugriffskontrollregel z. B. flexibel reagieren, um die Fernwartung zu verhindern).*

Die Flüchtigkeit von Zugriffsentscheidungen ist eine wichtige Eigenschaft von ABAC-Systemen. Sie ermöglicht es, Zugriffsentscheidungen an den aktuellen Zustand der Ressourcenobjekte anzupassen. Dies kann dazu beitragen, die Sicherheit und Integrität der Systeme zu erhöhen.

1.2 Flexibilisierung der Zugriffssteuerung

Die Flexibilität des logischen Zugriffskontrollmodells wird dadurch erhöht, dass Attribute und ihre Werte während des gesamten Lebenszyklus von Subjekten, Objekten und Attributen geändert werden können, ohne dass jede einzelne Subjekt-/Objekt-Beziehung geändert werden muss. So wird eine dynamische Zugriffskontrolle ermöglicht, da sich Zugriffsentscheidungen zwischen Anfragen ändern können, wenn sich Attributwerte ändern.

Solange dem Subjekt die Attribute zugewiesen werden, die für den Zugriff auf die benötigten Objekte erforderlich sind (z. B. werden diese Attribute dem Servicepersonal mit einer bestimmten Zertifizierung eines bestimmten Dienstleistungsunternehmens zugewiesen), sind keine Änderungen an bestehenden Regeln oder Objektattributen erforderlich. Dies ist einer der Hauptvorteile von ABAC.

Hinweis: Zusätzliche Attribute-Schutzmechanismen können die Integrität der Attribute während der API-Kommunikation gewährleisten.

1.3 Stakeholder (Existierende Organisationen und Standards)

Liste (nicht abschließend) von Stakeholdern zum Thema ABAC in der Industrie 4.0:

- **W3C** (World Wide Web Consortium) ist eine internationale Organisation, die Standards für das World Wide Web entwickelt. W3C hat verschiedene Standards im Bereich der Web-Technologien entwickelt, die auch für die Implementierung von ABAC in der Industrie 4.0 relevant sind.
- **NIST** (National Institute of Standards and Technology) ist eine US-amerikanische Bundesbehörde, die Standards und Richtlinien für die Informationssicherheit entwickelt. NIST bietet Richtlinien und Empfehlungen für ABAC in verschiedenen Kontexten, einschließlich der Industrie 4.0.
- **OASIS** (Organization for the Advancement of Structured Information Standards) ist eine internationale Organisation, die Standards für verteilte Systeme, Webservices und andere Arten von Informationssystemen entwickelt. OASIS hat den ABAC-Standard XACML (eXtensible Access Control Markup Language) entwickelt, der auch in der Industrie 4.0 verwendet wird.
- **IEEE** (Institute of Electrical and Electronics Engineers) ist eine internationale Organisation, die Standards für die Elektrotechnik, Elektronik und Informationstechnologie entwickelt. IEEE hat den Standard 802.1X entwickelt, der auch in der Industrie 4.0 verwendet wird, um Zugriffskontrollen auf Netzwerkressourcen zu implementieren.
- **ISO** (International Organization for Standardization) ist eine internationale Organisation, die Standards für eine Vielzahl von Bereichen entwickelt. ISO hat den Standard ISO/IEC 27701 entwickelt, der eine Erweiterung des ISO/IEC 27001-Standards für Informationssicherheit ist und auch ABAC-Konzepte enthält.

Organisationen und Standards spielen eine wichtige Rolle bei der Entwicklung und Verbreitung von ABAC-Konzepten in der Industrie 4.0. Sie tragen dazu bei, dass ABAC-Systeme interoperabel und sicher sind und die spezifischen Anforderungen der Industrie 4.0 erfüllen.

Organisation	Standard	Beschreibung
OASIS	XACML (eXtensible Access Control Markup Language)	XML-basierter Standard für die Definition von Zugriffskontrollregeln. XACML wird in der Industrie 4.0 verwendet, um Zugriffskontrollen auf Ressourcenobjekte zu implementieren. [14]
IEEE	802.1X	Standard für die Implementierung von Zugriffskontrollen auf Netzwerkressourcen. IEEE 802.1X wird in der Industrie 4.0 verwendet, um zu verhindern, dass nicht autorisierte Entitäten auf Netzwerkressourcen zugreifen können.
ISO	ISO/IEC 27701	Standard für die Implementierung von Datenschutzmanagementsystemen. ISO/IEC 27701 enthält auch ABAC-Konzepte, die zur Implementierung von Zugriffskontrollen auf personenbezogene Daten verwendet werden können.

Hinweis: Die Verwendung von JSON als zusätzliches Datenformat für ABAC-Systeme neben XML wird im Rahmen von Industrie 4.0 zunehmend an Bedeutung gewinnen. JSON ist ein leichtgewichtiges, flexibles und erweiterbares Format, das sich gut für die Definition von Zugriffskontrollregeln eignet.

2 Der betrachtete Industrie 4.0-Kontext

Zugriffskontrolle erfolgt (oder sollte erfolgen) auf allen Ebenen der Kommunikation bzw. des Datenaustauschs. Dies beinhaltet sowohl interne und lokale Kommunikation (z. B. innerhalb eines lokalen Netzwerks, in einer Lokation eines Unternehmens, ohne Wechsel des Netzwerks oder dessen Sicherheitslevels) als auch Kommunikation über das Internet (z. B. innerhalb eines Unternehmens, zwischen verschiedenen Lokationen oder zwischen verschiedenen Unternehmen und Geschäftspartnern).

Der betrachtete Industrie 4.0-Kontext geht von einer unternehmensübergreifenden Kommunikation im Rahmen globaler Wertschöpfungsketten mit einer Vielzahl von Beteiligten aus. Die Kommunikation erfolgt u. a. im Rahmen von Produktionsprozessen, produktionsvorbereitenden Prozessen (inkl. Vertragsprozessen) sowie im Rahmen eines allgemeinen Informations- und Datenaustausches (z. B. durch Mitgliedschaft in einem Datenraum). Darüber hinaus wird zunehmend der Einsatz von AAS als zentraler Endpunkt für jeglichen Datenzugriff im Kontext von Industrie 4.0 sowie abgeleiteten Kontexten diskutiert und mittlerweile erfolgreich umgesetzt. Diese besondere Rolle (bzw. der potenzielle De-facto-Standard) der Kommunikation über AAS wird hier näher beleuchtet.

2.1 Wichtige Fragestellungen der Zugriffssteuerung am Beispiel „Collaborative Condition Monitoring“

Im Rahmen der Veröffentlichung „Der Weg zum digitalen Champion – Durch digitale Transformation zur Datenökonomie“ [15] wird das physikalische Asset bzw. dessen digitaler Zwilling auch als „Produktionsmittel der Zukunft“ bezeichnet.

Anhand der Abbildung 2 können Aspekte der Zugriffskontrolle aus der Perspektive verschiedener Akteure betrachtet werden:

- **Sicht des Fabrik-Betreibers:** Der Fabrikbetreiber möchte i. d. R. (und ggf. nach der Inbesitznahme des Assets) Zugriff auf alle Bestandteile der AAS haben. Sofern keine vertraglichen oder technischen Restriktionen dagegensprechen, kann der Fabrikbetreiber die AASen des Assets selbst und die der verbauten Komponenten in einer flachen Struktur aufbauen und über sehr einfache Regeln den Zugriff erlangen. In diesem Falle wären aus Betreiber-Sicht alle Submodelle der AAS „public“.

  Wenn der Zugriff auf AAS-Submodelle durch vertragliche Bestimmungen (hier Vertrag des Betreibers mit dem Maschinenlieferanten) restringiert ist bzw. diese vertraglichen Restriktionen durch den Lieferanten auch durchgesetzt werden sollen (Art und Weise der Durchsetzung wird später diskutiert), erscheinen in der AAS „Public“- und „Restricted“-Anteile der Submodelle. Dies ist in Abbildung 3 dargestellt, in Form grüner („Public“-) und roter („Restricted“-)Anteile (nur dem Lieferanten vorbehalten) der AAS. Eine flache Struktur der AAS ist im Falle solcher Restriktionen nicht mehr geeignet, um Zugriffskontrolle bzgl. der Einhaltung der Verträge zu ermöglichen. In diesem Falle muss zwecks des technischen Enforcements der Vertragsbedingungen eine separate Zugriffskontrolle erfolgen, die nicht mehr vollständig in der Hand des Betreibers liegen kann.

  Gleichzeitig möchte der Betreiber dem Lieferanten den Zugriff auf bestimmte produktionsrelevante Submodelle des Assets verweigern, da sich in diesen ggf. Firmengeheimnisse befinden. D. h., einige der „Public“-Submodelle sind zwar für Betreiber „public“, für Lieferanten jedoch „restricted“. Entsprechend einem Regelwerk zur Durchsetzung des Zugriffs ist der Zugriff für diese Submodelle dynamisch geregelt. In Abbildung 4 sind die Submodelle mit dynamischer Zugriffskontrolle als rot-grün schraffiert dargestellt.

- **Sicht des Maschinenlieferanten:** Dieser möchte (z. B. zum Zweck des Condition Monitorings) auf die Submodelle der AAS zugreifen, wie vertraglich mit dem Betreiber vereinbart. Dies beinhaltet auch die „Restricted“-Submodelle des Assets, die sein Eigentum sind. Er erwartet vom Betreiber, dass ihm der Zugriff gewährt wird. Gleichzeitig darf er auf bestimmte Submodelle, die Eigentum des Betreibers sind, nicht zugreifen.

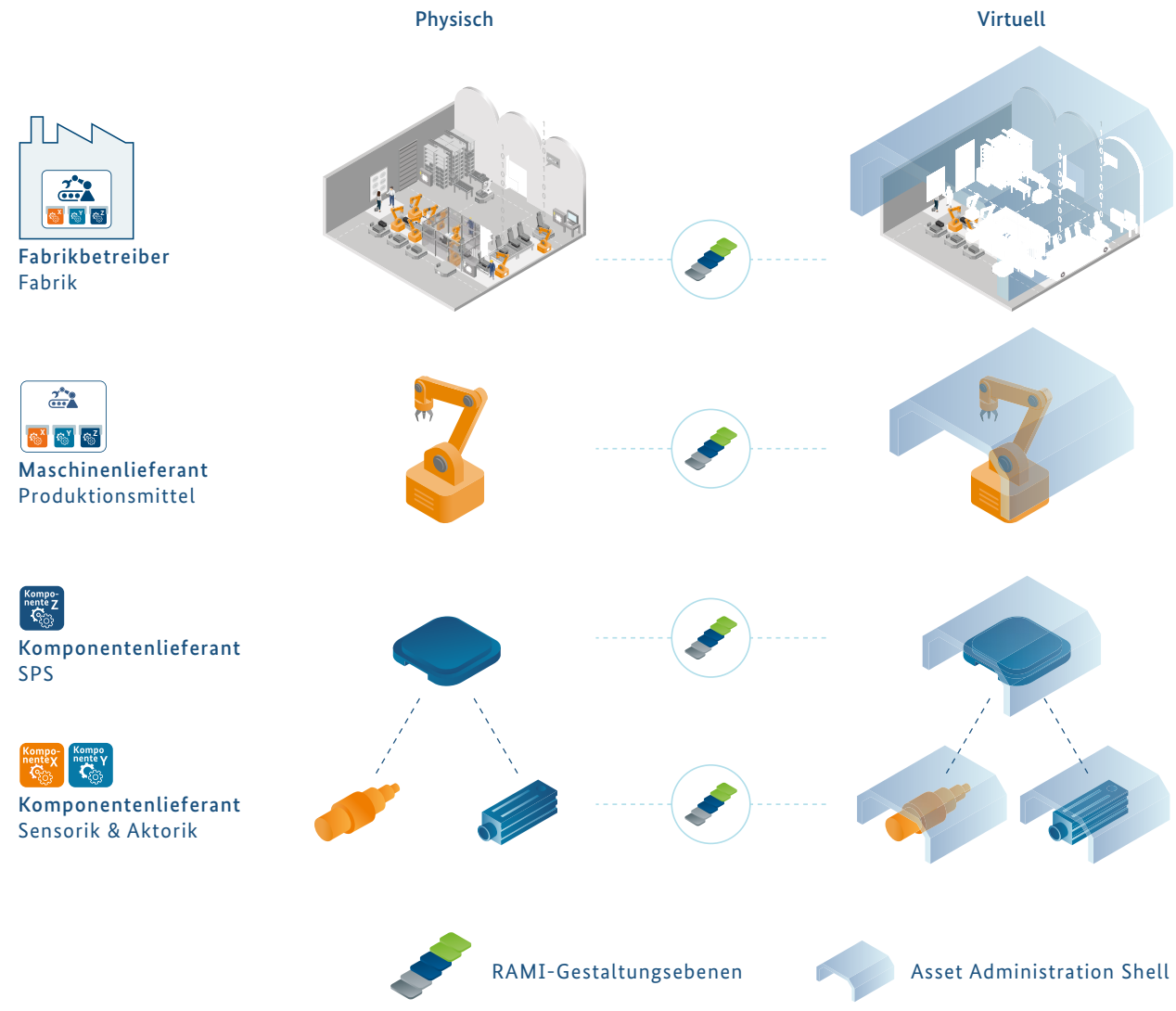
- **Sicht der Komponentenlieferanten:** Diese haben sich (z. B. für das Condition Monitoring ihrer zugelieferten Komponenten) vom Maschinenlieferanten vertraglich zusichern lassen, dass sie auf Submodelle zugreifen können, die in ihrem Eigentum stehen, auf die aber weder der Betreiber noch der Lieferant Zugriff haben. Diese Verträge sind dem Betreiber nicht bekannt. Daher kann die Durchsetzung des Zugriffs auf die Teilmodelle der Komponenten nicht durch den Betreiber geregelt werden, sondern muss über eine separate Durchsetzung durch den Lieferanten erfolgen.

Im Zusammenhang mit den verschiedenen Interessengruppen und deren Zugriffsanforderungen stellt sich die Frage, wie die automatisierte Durchsetzung von ggf. vertraglich vereinbarten Nutzungsbedingungen der AAS-Submodelle zwischen dem Fabrikbetreiber, dem Maschinenlieferanten und den Komponentenherstellern erfolgen kann. Dabei ist keine der genannten Parteien als Alleinverfügungsberechtigte oder als Allein-Entscheiderin für die Erstellung von Zugriffsberechtigungen auf Submodelle für andere legitimiert.

Hinweis: Aus dem Wunsch (bzw. der Notwendigkeit) heraus, die Durchsetzung der Nutzungsbedingungen sowohl auf dem physikalischen Asset als auch in der virtuellen Welt durchführen zu können (Abbildung 2), ergeben sich Anforderungen an das Zusammenspiel der physischen und virtuellen Welt:

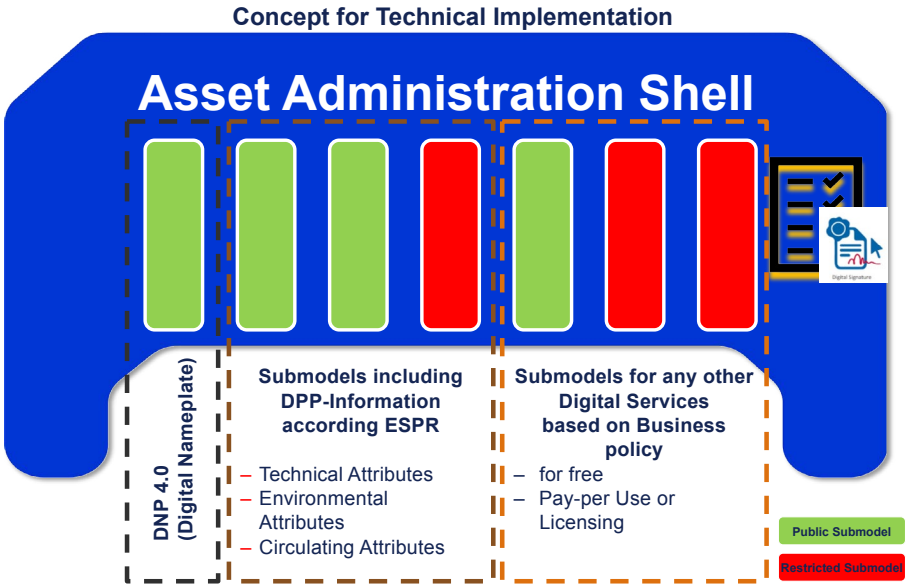
- Das physische Asset und jeweilige AAS sind untrennbar miteinander verbunden.
- Physisches Asset und dazugehörige AAS synchronisieren sich fortlaufend.

Abbildung 2: Zusammenspiel der physischen und virtuellen Welt via AAS



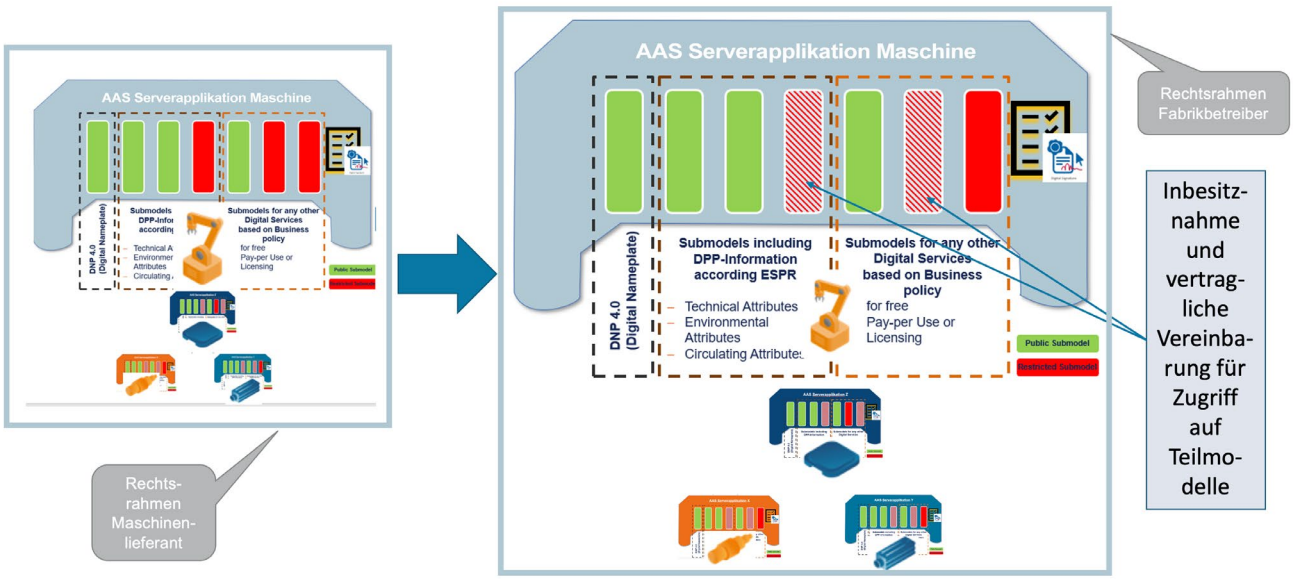
Quelle: Plattform Industrie 4.0

Abbildung 3: AAS mit Submodellen, die „public“ bzw. „restricted“ sind



Quelle: IDTA AAS Tech Days, „DPP4.0 – Big Picture“, Frankfurt, 15.09.2023, Prof. Dieter Wegener

Abbildung 4: AAS mit Submodellen, auf die zusätzlich dynamische Zugriffsregeln angewandt werden



Quelle: Plattform Industrie 4.0 basierend auf Abbildung 3

Im Folgenden wird diskutiert, wie die Durchsetzung der Nutzungsbedingungen für die verschiedenen Interessengruppen gewährleistet werden kann. Hierzu wird im folgenden Kapitel ein Vorschlag zur logischen Hierarchisierung der AAS und zum Datenzugriff über diese logischen Hierarchien gemacht.

2.2 Möglicher Lösungsweg über die Einführung logischer Zugriffspfade/Baumstrukturen

Um den zuvor erwähnten vertragsgemäßen Zugriff auf AAS-Submodelle zu ermöglichen und auch das Problem des ungewollten Zugriffs auf AAS-Submodelle des Maschinenlieferanten und der Hersteller anderer Komponenten als der eigenen wirkungsvoll zu verhindern, besteht ein Weg darin, den Zugriff auf bestimmte Daten nur über einen bestimmten Zugriffspfad zu ermöglichen.

Dieser mögliche Weg impliziert eine logische Hierarchisierung der AAS-Submodelle entsprechend dem Eigentum der Submodelle und entsprechend der separaten Durchsetzung der Zugriffskontrolle, die sich dem Einfluss des Eigentümers des Assets (Betreiber) ganz oder teilweise entzieht. D. h., das Folgen eines Zugriffspfades ist mit jedem weiteren Schritt auf diesem Pfad jeweils durchzusetzen, mit Regeln und Attribut-Anreicherungen, die vom Besitzer der Submodelle verwaltet werden. Abbildung 5 bildet beispielhaft den Pfadzugriff von der Betreiber-AAS über die Maschinenlieferanten-AAS in die Komponenten-AAS eines Komponenten-Lieferanten ab.

Bei der Prüfung der Nutzungsbedingungen entlang einer logischen Pfad-Hierarchie kann man zwischen zwei Zugriffsmustern unterscheiden, welche bzgl. der Resultate gleichwertig sind:

Zugriffsmuster A: Das Subjekt (z. B. ein Komponentenhersteller, Client) fragt über das Asset und die Angabe des logischen Pfads an der aktiven Komponente der AAS des Assets einmalig an. Die AAS des Assets der Maschine führt in ihrer aktiven Komponente ein Enforcement durch und gibt die Anfrage an die AAS der Komponente weiter.

Zugriffsmuster B: Das Subjekt fragt ebenfalls beim Asset der Maschine an, bekommt aber einen Rückverweis auf die im Pfad als Nächstes anzufragende Komponente. Das Subjekt hangelt sich in diesem Fall von Komponente zu Komponente durch und fragt daher mehrfach an.

Eine genaue Beschreibung der Zugriffsmuster befindet sich im Anhang (Kapitel 10) sowie in Abbildung 10 und Abbildung 11. Eine Mischung der beiden Zugriffsmuster mit Beschreibung ist in Abbildung 12 dargestellt.

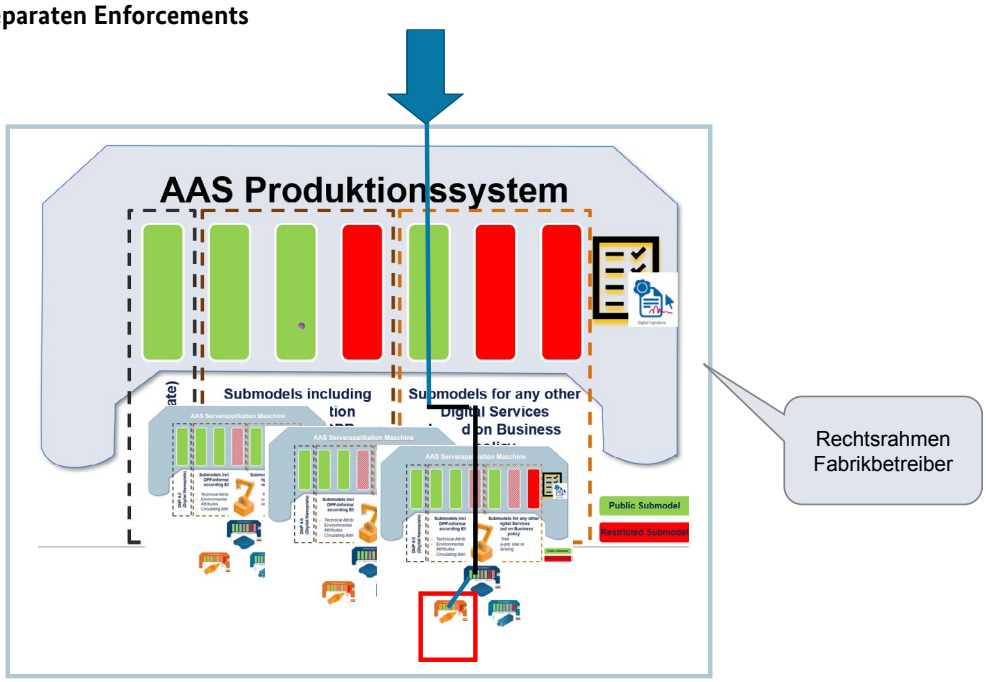
2.3 Selbstauskunft zu logischen Abhängigkeiten

Eine weitere Anforderung an die AAS im Zusammenhang mit der Ermittlung logischer Abhängigkeiten innerhalb der AAS ist die Möglichkeit der Selbstauskunftsfähigkeit zu logischen Abhängigkeiten. Konkret bedeutet das, dass eine jeweilige Komponente in einer AAS das Wissen über ihre technischen Abhängigkeiten besitzen muss, in Bezug auf die AASen der untergeordneten Komponenten, mit denen diese Komponente kommuniziert. Die erzeugte logische Pfadinformation erfolgt daher entlang der internen Kommunikationswege zwischen den verbauten Komponenten.

Das Thema Selbstauskunftsfähigkeit (engl. „Discovery Service“) wird auch in anderen Arbeitsgruppen diskutiert, z. B. in der IDTA in der Spezifikation „Hierarchische Strukturen ermöglichen Stücklisten“ [16]. Bisherige Bill of Materials Referenz-Spezifikationen (bzw. Publikationen zum Aufbau der AAS [17]) wären für eine Bereitstellung der Kommunikationsabhängigkeiten und entsprechende Pfad-Informationen noch nicht ausreichend. In der Arbeitsgruppe AG1 der Plattform Industrie 4.0 gibt es zusätzlich die Taskforce „Discovery“, die sich ebenfalls intensiv mit dem Thema „Selbsterkennung/Discovery“ beschäftigt [18].

Details und Ideen zur Umsetzung logischer Hierarchien, die u. a. die Themen Selbstauskunft, automatische Erzeugung der logischen Hierarchie und Findung von Zugriffsregeln behandeln, befinden sich im Anhang in Kapitel 10.

Abbildung 5: Exemplarische Zugriffsdarstellung über einen Pfad einer logisch hierarchisierten Baumstruktur, mit separaten Enforcements



Quelle: Plattform Industrie 4.0 basierend auf Abbildung 3

Die detaillierte technische Umsetzung von Nutzungsbedingungen wird in einem Folgepapier behandelt.

Je nach Zugriffs-Szenario müssen verschiedene Anforderungen an die AAS oder deren Umgebung gestellt werden, die hier in einer Kriterien-Sammlung zusammengefasst sind.

Die Kriterien-Sammlung wird nun pro Beispiel im folgenden Kapitel 3 jeweils als Anforderungsprüfung angewandt.

Kriterium	Fähigkeit der AAS oder der Umgebung	Beschreibung	Fähigkeit existiert bereits
AAS-Typ	AAS	Wird eine AAS-Ablage benötigt (Typ 1) oder ein dynamischer Bestandteil der AAS (Typ 2 oder 3)?	Existent
Bill of Materials (BOM) der AAS	AAS	Wird eine BOM (bzw. BOM-Referenz) benötigt, welche alle Submodelle der AAS auflisten kann?	Existent: Es sei hier auf die beiden oben genannten Quellen verwiesen (Spezifikation zur AAS, IDTA-Papier)
Erweiterte BOM, die logische Abhängigkeiten und Hierarchien abbildet	AAS oder Umgebung	Wird eine Selbstauskunftsfähigkeit (Discovery Service) benötigt, die die AAS als logische Hierarchie darstellen kann?	Nicht existent: Es sei hier auf die beiden oben genannten Quellen verwiesen (IDTA-Papier, Task Force der AG1 zu „Discovery Services“)
Selbstauskunftsfähigkeit entlang der Kommunikationswege im Asset	AAS oder Umgebung	Wird eine Selbstauskunftsfähigkeit (Discovery Service) benötigt, die die AAS als logische Hierarchie entsprechend den Kommunikationswegen abbilden kann?	Nicht existent
Unternehmensübergreifender Zugriff/Nutzung	AAS und Umgebung	Muss (z. B. zwecks Regelausführung oder Anreicherung von Zugriffsattributen) eine Verbindung der AAS und deren Umgebung ins Internet bestehen?	Existent
Unternehmensinterner Zugriff/Nutzung	AAS und Umgebung	Muss (z. B. zwecks Regelausführung oder Anreicherung von Zugriffsattributen) eine Verbindung der AAS und deren Umgebung ins Intranet bestehen?	Existent
Externer Policy Decision Point (PDP)	Umgebung	Wird der Zugriff auf einen externen PDP benötigt, um eine (externe) Regelausführung der Zugriffsregeln zu triggern?	Existent: Externe/verteilte PDPs sind Bestandteil des ABAC-Konzeptes

3 Analyse von Use Cases und zugehörigen Anforderungen

Im Zusammenhang mit der im vorigen Kapitel erwähnten topologischen Betrachtung der Einhaltung der Nutzungsbedingungen durch die dort vorgestellte Methodik mittels Zugriffen über logische Hierarchien werden im Folgenden verschiedene Anwendungsfälle mit ihren jeweiligen Anforderungen dargestellt. Diese werden anschließend analysiert, um einen umfassenden Einblick in die Funktionsweise und die Möglichkeiten der vorgestellten Methodik zu geben.

3.1 Szenario 1: Collaborative Condition Monitoring (CCM)

Vertraglich vereinbarte Nutzungsbedingungen der AAS-Submodelle zwischen dem Fabrikbetreiber, dem Maschinenlieferanten und den Komponentenherstellern sollen umgesetzt werden können. Dabei soll ein Komponentenhersteller auf AAS-Submodelle seiner zugelieferten Komponente zugreifen können, jedoch nicht auf die AAS des gesamten Assets (der Maschine) oder der anderen Komponentenhersteller. Auch der Betreiber hat ggf. keine Berechtigung, bestimmte Daten (z. B. Laufzeit- und Abnutzungsdaten einer Komponente) einzusehen. Dabei ergibt sich, dass keine der genannten Parteien als Alleinverfügungsberechtigte oder Allein-Entscheiderin für die Erstellung von Zugriffsberechtigungen auf Submodelle gelten kann bzw. legitimiert ist.

Problemstellung:

- *Wie wird der Zugriff auf Maschinen-Komponenten gewährleistet, ohne die Möglichkeit einer generellen Ausspionage der anderen verbauten Komponenten?*
- *Wie wird der Zugriff auf Maschinen-Komponenten gewährleistet, ohne dass eine Partei das Alleinbestimmungsrecht für den Zugriff hat?*

Lösungsansatz mittels logischer Hierarchien

Mit Hilfe von logischen Hierarchien und getrennten Enforcements auf verschiedenen aktiven AAS können pro Hierarchieebene die nicht öffentlich bekannten Vertragsbestandteile zur Nutzung zwischen z. B. Hersteller und Komponentenherstellern der Maschine geprüft und durchgesetzt werden. Dabei muss der Betreiber dem Hersteller einen vertraglich geregelten Zugang eröffnen, über den dann der Komponentenhersteller nach gesonderten Regeln auf die Daten seiner Komponente zugreifen kann.

Dieses Beispiel wird in Kapitel 4.1 detailliert erläutert.

Voraussetzungen/Zusammenhänge

Kriterium	Wert	Kommentar
AAS-Typ	2 oder 3	Enforcements erfordern eine aktive AAS (AAS-Datenserver)
Bill of Materials (BOM) der AAS	n/a	Eine BOM ohne Hierarchie-Informationen ist nicht ausreichend
Erweiterte BOM, die logische Abhängigkeiten und Hierarchien abbildet	n/a	Es reicht nicht, wenn die BOM eine beliebige Hierarchie abbildet
Selbstauskunftsfähigkeit entlang der Kommunikationswege im Asset	erforderlich	Es können nur die Pfade zwischen Komponenten beschritten werden, die auch miteinander kommunizieren können. Die aktuellen Pfade sollen dynamisch ermittelbar sein. (z. B. bzgl. ihrer Gültigkeit)
Unternehmensübergreifender Zugriff/Nutzung	erforderlich	Enforcements außerhalb des Einflussbereichs des Betreibers würden ggf. im Internet stattfinden
Unternehmensinterner Zugriff/Nutzung	erforderlich	Enforcements innerhalb des Einflussbereichs des Betreibers würden ggf. im Intranet stattfinden
Externer Policy Decision Point (PDP)	erforderlich	Enforcements außerhalb des Einflussbereichs des Betreibers würden ggf. auf einem externen PDP stattfinden

3.2 Szenario 2: Support und Beurteilung von Maschinenfehlern

Bei auftretenden Maschinenfehlern kann ein nicht geprüfter Austausch von ggf. funktionierenden Komponenten zu erheblichen Mehrkosten (Personal- und Materialkosten) führen. Daher ist ein Zugriff auf die AAS-Submodelle der Komponente durch den Komponentenhersteller erforderlich, um den Austausch (z. B. im Rahmen eines Gewährleistungsfalles) zu beurteilen und ggf. zu genehmigen/abzulehnen. Siehe dazu auch den Use Case Collaborative Quality Management (Robert Bosch GmbH) im Appendix des in der Fußnote erwähnten Dokumentes.

Problemstellung:

- *Wie kann man garantieren, dass die Zugriffe compliant sind?*
- *Wie kann garantiert werden, dass der Hersteller der Komponente nicht mit falschen Kosten belastet wird?*

Lösungsansatz mittels logischer Hierarchien

Mit Hilfe logischer Hierarchien und separaten Enforcements wird es dem Komponentenhersteller überhaupt erst ermöglicht, seine Komponente – entsprechend den Vertragsvereinbarungen zur Gewährleistung zwischen z. B. Hersteller und Komponentenhersteller – technisch zu erreichen, zu prüfen und dann ggf. sein Einverständnis für den Austausch zu geben, oder anderweitig zu entscheiden.

Voraussetzungen/Zusammenhänge

Kriterium	Wert	Kommentar
AAS-Typ	2 oder 3	s. Szenario 1
Bill of Materials (BOM) der AAS	n/a	s. Szenario 1
Erweiterte BOM, die logische Abhängigkeiten und Hierarchien abbildet	n/a	s. Szenario 1
Selbstauskunftsfähigkeit entlang der Kommunikationswege	erforderlich	s. Szenario 1
Unternehmensübergreifender Zugriff/Nutzung	erforderlich	s. Szenario 1
Unternehmensinterner Zugriff/Nutzung	erforderlich	s. Szenario 1
Externer Policy Decision Point (PDP)	erforderlich	s. Szenario 1

3.3 Szenario 3: Durchsetzung aufgrund nicht öffentlich bekannter vertraglicher Vereinbarungen

Es gibt dem Betreiber unbekannte vertragliche Vereinbarungen zwischen Asset-(Maschinen-) Hersteller und Komponentenhersteller (oder Komponentenhersteller und Sub-Komponentenhersteller etc.). Diese gewährleistet dem Komponentenhersteller den Zugriff auf seine im Asset verbauten Komponenten. Die vertraglichen Vereinbarungen sind individuell zwischen den beiden Parteien und sowohl dem Betreiber als auch anderen Komponentenherstellern nicht bekannt.

Problemstellung:

- *Wie kann die Durchsetzung dieser Vereinbarung(en) gewährleistet werden, ohne dass sie im Asset verankert ist?*
- *Wie kann der Subkomponentenzugriff selektiv durchgesetzt werden?*

Lösungsansatz mittels logischer Hierarchien

Mit Hilfe logischer Hierarchien und separater Enforcements können Regeln geprüft werden, die nicht fest im Asset oder deren AAS verankert sind, sondern entsprechend den gültigen Vertragsvereinbarungen hochdynamisch sein können, ggf. auch invalidiert sein können. Eine delegierte Regelausführung außerhalb des Assets selbst (Weiterleitung zur Prüfung aus einer aktiven AAS der verbauten Komponente heraus, auf die zugegriffen werden soll) ermöglicht sowohl die dynamische Prüfung als auch die dynamische Anpassung von Regeln im Bedarfsfall.

Voraussetzungen/Zusammenhänge

Kriterium	Wert	Kommentar
AAS-Typ	2 oder 3	s. Szenario 1
Bill of Materials (BOM) der AAS	n/a	s. Szenario 1
Erweiterte BOM, die logische Abhängigkeiten und Hierarchien abbildet	n/a	s. Szenario 1
Selbstauskunftsfähigkeit entlang der Kommunikationswege	erforderlich	s. Szenario 1
Unternehmensübergreifender Zugriff/Nutzung	erforderlich	s. Szenario 1
Unternehmensinterner Zugriff/Nutzung	erforderlich	s. Szenario 1
Externer Policy Decision Point (PDP)	erforderlich	s. Szenario 1

3.4 Szenario 4: Auslagerung an Dienstleister

Hersteller haben (manchmal/häufig) ihre Wartungs- und Monitoring-Aufgaben an Dienstleister ausgelagert. Gleichzeitig arbeitet der Dienstleister für mehrere Hersteller und benötigt jeweils herstellerspezifische Zugriffsrechte. In diesem Falle muss der Dienstleister wissen, wo er die entsprechende Komponenten-AAS finden kann, ohne dass er zwangsläufig alle Assets des Betreibers im Detail kennt. Er muss daher die Zugriffspfade, startend von der Gesamt-AAS des Betreibers, kennen, um zielgerecht die AASen der verbauten Komponenten, die er prüfen soll, zu finden. Dabei ist zu berücksichtigen, dass sich die Rechtevergabe hochdynamisch verändern kann. Z. B. könnte der Dienstleister ausgetauscht werden, oder Dienstleister-Personal darf aus bestimmten Ländern nicht mehr zugreifen.

Problemstellung:

- *Wie kann die Komplexität der Zugriffsregeln reduziert werden bei gleichzeitiger Aufrechterhaltung der Service-Qualität?*
- *Wie wird in Anbetracht der hohen Dynamik eine managebare Konsistenz der Nutzungsbedingungen und daraus resultierenden Zugriffsregeln erzielt?*

Lösungsansatz mittels logischer Hierarchien

Mit Hilfe logischer Hierarchien und separater Enforcements können Regeln geprüft werden, die nicht fest im Asset oder dessen AAS verankert sind. Eine delegierte Regelausführung außerhalb des Assets selbst kann durch Regeländerung den kompletten Austausch eines (Wartungs-) Dienstleisters direkt auf der Ebene der passenden logischen Hierarchie ermöglichen, ohne dass auf Betreiber- bzw. Asset-Ebene eine Veränderung stattfinden muss.

Voraussetzungen/Zusammenhänge

Kriterium	Wert	Kommentar
AAS-Typ	2 oder 3	s. Szenario 1
Bill of Materials (BOM) der AAS	n/a	s. Szenario 1
Erweiterte BOM, die logische Abhängigkeiten und Hierarchien abbildet	n/a	s. Szenario 1
Selbstauskunftsfähigkeit entlang der Kommunikationswege	erforderlich	s. Szenario 1
Unternehmensübergreifender Zugriff/Nutzung	erforderlich	s. Szenario 1
Unternehmensinterner Zugriff/Nutzung	erforderlich	s. Szenario 1
Externer Policy Decision Point (PDP)	erforderlich	s. Szenario 1

3.5 Szenario 5: Kein komplexer Zugriffsschutz möglich oder dieser wird nicht benötigt

In einem Asset sind nur allgemein bekannte Komponenten verbaut, die keinen speziellen Zugriffsschutz benötigen oder auch keinen entsprechenden Schutz besitzen (z. B. Klein-IOT-Komponenten, ältere/bekannte Komponenten). Hierunter fallen auch ältere Industrie-Anlagen („Brownfield"). In diesem Fall muss der notwendige Mindest-Zugriffsschutz ersatzweise ggf. über Gateways oder auch in der Edge erfolgen.

Problemstellung:

- *Wie kann eine reduzierte Komplexität mit einfachen Zugriffsregeln abgebildet werden?*
- *Wie kann eine konsistente Prüfung der Nutzungsbedingungen und der daraus resultierenden Zugriffsregeln in gemischten (d. h. „Greenfield"/„Brownfield") Umgebungen erfolgen?*

Lösungsansatz mittels logischer Hierarchien

Der Ansatz logischer Hierarchien mit jeweils aktiven AAS-Komponenten legt nicht fest, an welcher Stelle die Zugriffsprüfung erfolgt. In einem gemischten Szenario („Greenfield"/„Brownfield") kann ein passendes Enforcement für eine Komponente ohne AAS ersatzweise an ein Gateway oder eine Edge ausgelagert werden, während Industrie 4.0-Komponenten (d. h. AAS ist vorhanden) z. B. in der aktiven Komponente der AAS eine Prüfung durchführen können bzw. diese an andere Enforcements auslagern können.

Voraussetzungen/Zusammenhänge

Kriterium	Wert	Kommentar
AAS-Typ	optional	Ggf. existiert die AAS in Brownfield-Szenarien nicht, sondern ausschließlich der digitale Zwilling, oder eine andere, von der AAS unabhängige Regelprüfung (z. B. in der Edge/Cloud)
Bill of Materials (BOM) der AAS	n/a	s. Szenario 1
Erweiterte BOM, die logische Abhängigkeiten und Hierarchien abbildet	n/a	s. Szenario 1
Selbstauskunftsfähigkeit entlang der Kommunikationswege	erforderlich	In diesem Fall müsste die Auskunft stellvertretend durch die Umgebung erteilt werden, wenn die AAS nicht existent wäre
Unternehmensübergreifender Zugriff/Nutzung	unklar, eher n/a	Die Regel-Prüfung benötigt ggf. den Zugang, wenn ein Industrie 4.0-Szenario für die Brownfield-Komponente vorliegt
Unternehmensinterner Zugriff/Nutzung	erforderlich	s. Szenario 1
Externer Policy Decision Point (PDP)	unklar, eher n/a	Die Regel-Prüfung benötigt ggf. den Zugang, wenn ein Industrie 4.0-Szenario für die Brownfield-Komponente vorliegt

3.6 Szenario 6: Administrationsaufgaben

Typische Administrationsaufgaben sind z. B. die Prüfung aller Zugriffsregeln auf Konsistenz über alle Assets und deren AAS von Betreibern, Herstellern, Komponentenherstellern hinweg. Der Administrator möchte dann bspw. folgende Metadaten abfragen:

- Selektiere alle Zugriffsrechte auf alle Submodelle.
- Selektiere alle Submodelle, auf die der Zugriff generell erlaubt ist.

Problemstellung:

- *Sind alle Zugriffsregeln konsistent vergeben?*
- *Wie kann das Auffinden bestimmter Bestandteile der AAS zuverlässig und performant erfolgen?*

Lösungsansatz mittels logischer Hierarchien

Der Ansatz logischer Hierarchien erlaubt die rekursive Erkundigung über die Gesamt-AAS eines Betreibers hinweg (z. B. alle AAS, die sich in einem zentralen Repository befinden). Jede logische Hierarchie-Ebene weiß dann, welche darunter liegenden Komponenten verwendet wurden, und diese Komponenten wissen das dann auch. Daraus ergibt sich automatisch durch Abfrage die logische Hierarchisierung. Siehe hierzu auch die beispielhafte Abfrage mit Hilfe von Xpath-Ausdrücken im Anhang, Kapitel 10.

Voraussetzungen/Zusammenhänge

Kriterium	Wert	Kommentar
AAS-Typ	2 oder 3	Wird benötigt für die Extraktion der relevanten Daten
Bill of Materials (BOM) der AAS	erforderlich	Eine Administration benötigt grundsätzlich verschiedene/flexible Sichten auf die Liste der Assets, entsprechend den Administrationsaufgaben
Erweiterte BOM, die logische Abhängigkeiten und Hierarchien abbildet	erforderlich	Eine Administration benötigt grundsätzlich verschiedene/flexible Sichten auf die Liste der Assets, entsprechend den Administrationsaufgaben
Selbstauskunftsfähigkeit entlang der Kommunikationswege	erforderlich	Eine Administration benötigt grundsätzlich verschiedene/flexible Sichten auf die Liste der Assets, entsprechend den Administrationsaufgaben
Unternehmensübergreifender Zugriff/Nutzung	n/a	
Unternehmensinterner Zugriff/Nutzung	erforderlich	Der Zugriff wird für Administrationsaufgaben benötigt
Externer Policy Decision Point (PDP)	n/a	

3.7 Szenario 7: Verwendung von Teilen der AAS als technische Implementierung des DPP4.0

Für die Verwendung der AAS als technische Implementierung des Digital Product Passports (DPP4.0) werden in einigen Daten-Ökosystemen Auszüge der AAS in einer Registry persistiert, die dann als „öffentliche Daten" (d.h. öffentlich innerhalb des Ökosystems) gelten und über die Mitglieder des Ökosystems detailliert und performant suchen können. Im Anschluss an das vorhergehende Szenario (3.6) müssen die Registry-Kataloge automatisiert und regelmäßig erneuert werden, was der Administrationsaufgabe entspricht, Submodelle zu suchen/finden, auf die der Zugriff generell erlaubt ist.

Problemstellung:

- *Wie kann/muss die AAS gestaltet werden, dass sie eine technologische Basis für DPP4.0 darstellt?*

Lösungsansatz mittels logischer Hierarchien

Wie in Kapitel 3.6 beschrieben, erlaubt der Ansatz logischer Hierarchien die rekursive Erkundigung über alle AASen eines Betreibers und die Findung sowie auch die Extraktion der DPP-Teilmodelle, zwecks Bereitstellung dieser Teilmodelle in einer speziellen DPP Registry.

Hinweis: Use Cases, wie z.B. der Zugriff von Marktaufsichtsbehörden auf zugriffsgeschützte Daten, werden in diesem Beispiel nicht betrachtet.

Voraussetzungen/Zusammenhänge

Kriterium	Wert	Kommentar
AAS-Typ	2 oder 3	Wird benötigt für die Extraktion der DPP-relevanten Submodelle
Bill of Materials (BOM) der AAS	erforderlich	Die BOM könnte für die Extraktion des DPP ausreichen
Erweiterte BOM, die logische Abhängigkeiten und Hierarchien abbildet	n/a	
Selbstauskunftsfähigkeit entlang der Kommunikationswege	n/a	
Unternehmensübergreifender Zugriff/Nutzung	n/a	Wird ggf. nicht benötigt, wenn nur öffentliche Daten im DPP erscheinen, und das Enforcement auf diese Daten keine externe Regelausführung benötigt
Unternehmensinterner Zugriff/Nutzung	erforderlich	Der Zugriff wird für Administrationsaufgaben benötigt
Externer Policy Decision Point (PDP)	n/a	

Hinweis: Auch in diesem Fall werden zur Erzeugung der BOM Autorisierungsprüfungen durchgeführt, die im Fall von öffentlichen (öffentlich innerhalb des Ökosystems) DPP-Daten immer „true" zurückgeben.

Sofern man davon ausgehen würde, dass beim Zugriff auf DPP-Daten grundsätzlich auf öffentliche Daten zugegriffen würde, wäre kein aktiver Teil der AAS erforderlich, da die zusätzliche Autorisierungsprüfung entfiele, die im aktiven Teil der AAS stattfindet (oder von dort delegiert wird).

3.8 Antworten auf Fragestellungen im Rahmen des Use Cases CCM, die mit Hilfe der Einführung einer logischen Hierarchisierung beantwortet werden können

Im Rahmen der Veröffentlichung „Der Weg zum digitalen Champion – Durch digitale Transformation zur Datenökonomie“ [15] ergeben sich für das „Produktionsmittel der Zukunft“ einige sehr detaillierte Fragen, die mit Hilfe einer logischen Hierarchisierung der AAS beantwortet werden können. Siehe dazu die Fragen in Tabelle 1.

Tabelle 1: Antworten auf die Fragen, die im Rahmen des Use Cases CCM entstanden

Frage	Antwort	Technische Implementierung
1. Wie erfolgt die technische und rechtliche Inbesitznahme des physischen Assets und der dazugehörigen AAS der Komponenten durch den Maschinenlieferanten?	Die technische Inbesitznahme erfolgt durch die Bereitstellung der AAS für die Komponenten des physischen Assets durch den Maschinenlieferanten. Die AAS werden in einem geeigneten Format bereitgestellt, z. B. als XML-Datei oder als Softwarepaket. Die rechtliche Inbesitznahme erfolgt durch die Übertragung der Eigentumsrechte an den AAS vom Maschinenlieferanten auf den Fabrikbetreiber.	Die Bereitstellung der AAS kann über verschiedene Mechanismen erfolgen, z. B.: • Bereitstellung der AAS auf einem USB-Stick oder einer SD-Karte • Bereitstellung der AAS über ein Webinterface • Bereitstellung der AAS über eine Schnittstelle zur Integration in ein Asset-Management-System Die Übertragung der Eigentumsrechte an der AAS kann durch eine schriftliche Vereinbarung zwischen dem Maschinenlieferanten und dem Fabrikbetreiber erfolgen.
2. Wie erfolgt das Zusammenfügen der AAS zu dieser logischen Baumstruktur unter Beachtung der technischen und rechtlichen Rahmenbedingungen?	Die Zusammenführung der AAS zu einer logischen Baumstruktur erfolgt durch den Fabrikbetreiber. Dabei sind die technischen und rechtlichen Rahmenbedingungen zu beachten.	Die Zusammenführung der AAS kann durch verschiedene Mechanismen erfolgen, z. B.: • Manuelle Zuordnung der AAS untereinander • Automatische Zuordnung der AAS zueinander auf Basis von Metadaten Rechtliche Rahmenbedingungen sind zu beachten, z. B. Eigentumsrechte an den AAS. **Konkretisierung**: Die technische Umsetzung der Verknüpfung von AAS zu einer logischen Baumstruktur mit XPATH oder JSONPath erfolgt in zwei Schritten: 1. Erstellung eines XPATH- bzw. JSONPath-Ausdrucks 2. Ausführen des Ausdrucks auf die Baumstruktur Der XPATH- oder JSONPath-Ausdruck beschreibt, wie die AAS miteinander in Beziehung stehen sollen. Der Ausdruck kann z. B. folgende Elemente enthalten: · **Knotennamen:** Der Knotenname identifiziert einen einzelnen Knoten in der Baumstruktur. · **Attribute:** Ein Attribut beschreibt eine Eigenschaft eines Knotens. · **Relationen:** Eine Relation beschreibt das Verhältnis zwischen zwei Knoten. *(siehe Beispiele in Kapitel 3.1 bis 3.4).*

→

Frage	Antwort	Technische Implementierung
3. Wie erfolgt die Inbesitznahme des Produktionsmittels durch den Fabrikbetreiber?	Die Inbesitznahme des Produktionsmittels durch den Fabrikbetreiber erfolgt durch die Übergabe des physischen Assets und der zugehörigen AAS durch den Maschinenlieferanten an den Fabrikbetreiber. **Zugriffskontrolle:** Daten vor unberechtigtem Zugriff schützen. Das Zugriffsschutzkonzept ermöglicht es, den Zugriff auf einzelne Knoten in einer Datenstruktur zu kontrollieren. Dies kann durch die Definition von Zugriffsschutzattributen für die Knoten erreicht werden.	Die Übergabe des physischen Assets und der AAS kann durch verschiedene Mechanismen erfolgen, z. B.: • Übergabe des physischen Assets und der AAS durch den Maschinenlieferanten an den Fabrikbetreiber • Installation der AAS durch den Fabrikbetreiber Beachtung von ABAC-Zugriffsschutz und -Policies Zugriffsschutzattribute können verwendet werden, um folgende Aspekte des Zugriffs zu kontrollieren: · Ob der Zugriff auf den Knoten überhaupt erlaubt ist · Welche Aktionen der Benutzer auf dem Knoten ausführen darf · Welche Daten der Benutzer auf dem Knoten lesen oder schreiben darf Das Zugriffsschutzkonzept bietet eine flexible Möglichkeit, den Zugriff auf Daten zu kontrollieren. Es kann verwendet werden, um die Sicherheit der Daten zu erhöhen und gleichzeitig die Benutzerfreundlichkeit zu gewährleisten. *(siehe Beispiel 3.6)*
4. Wie kann in dieser Struktur eine Suche nach der „richtigen" AAS erfolgen? (bspw. durch die Realisierung eines Katalogs o. Ä.)?	In der hierarchischen Baumstruktur kann eine Suche nach der „richtigen" AAS durch verschiedene Mechanismen erfolgen, z. B.: • Durchsuchen der Baumstruktur nach einem bestimmten Attribut, z. B. dem Namen der Komponente • Durchsuchen der Baumstruktur nach einem bestimmten Merkmal, z. B. der Version der AAS • Erstellung eines Katalogs, in dem die AAS nach verschiedenen Kriterien sortiert sind *(siehe Beispiele in Kapitel 3.1 bis 3.4)*	
5. Wie kann aus der Perspektive eines Fabrikbetreibers z. B. auf die AAS der Komponente X (orange) zugegriffen werden (s. Abbildung 6)	Aus Sicht eines Fabrikbetreibers kann auf die AAS der orangen Komponente über die hierarchische Baumstruktur zugegriffen werden. Dazu muss der Anlagenbetreiber zunächst die orange Komponente in der Baumstruktur finden (siehe Antworten zur Frage 2). Anschließend kann der Fabrikbetreiber auf die AAS der orangen Komponente zugreifen.	Der Zugriff auf die AAS der orangen Komponente kann über verschiedene Mechanismen erfolgen, z. B.: • Durch Aufruf einer API-Funktion, die die AAS der orangen Komponente zurückgibt (siehe Beispiele in Kapitel 3.1 bis 3.4) • Durch Abfrage eines Repositories, in dem die AAS der orangen Komponente gespeichert sind

4 Anwendungsbeispiel zum Produktionsmittel der Zukunft

Zum besseren Verständnis seien im Folgenden einige Beispiele genannt, die das Thema auf Teilaspekte herunterbrechen, jedoch wieder auf den in Kapitel 2 genannten, übergeordneten Industrie 4.0-Kontext zurückzuführen sind. In allen Beispielen kann der Zugriff auf Industrie 4.0-Entitäten, oder auf digitale Zwillinge der Produkte, über eine entsprechende AAS erfolgen. Anfragen bei anerkannten Auskunftsstellen bzgl. der Reputation oder Bonität von Unternehmen, wie in Beispiel 4.2 dargestellt, würden wohl nach heutiger Kenntnis nicht über einen AAS API-Zugriff erfolgen (obwohl eine solche Vereinheitlichung von Zugriffen natürlich prinzipiell möglich wäre). Selbstauskünfte wären ebenso über digitale Zwillinge als Abbild des Unternehmens denkbar.

Legale und ökonomische Aspekte (z. B. Voraussetzungen zum Zustandekommen von Verträgen) werden in diesen Beispielen zwar als Zugriffsregel beschrieben, die tiefgreifende Diskussion dieser Aspekte wird jedoch in anderen Gremien diskutiert und ist entsprechend nicht Bestandteil dieses Dokuments.

Die Regel-Erstellung geht vom Grundprinzip „Alles ist verboten“ aus, es sei denn, es existiert eine Erlaubnis-Regel, die bei Prüfung „Erlaubt“ zurückliefert.

In der AAS der I40 Entität existieren öffentliche Daten (öffentliche Submodelle), die in keinem Fall einer Regel bedürfen bzw. die Regel liefert immer „Erlaubt“ zurück. Dies können z. B. allgemeine Angaben des Herstellers sein, das Herstellungsdatum, allgemeine Stromverbrauchsangaben etc. Außerdem existieren private Daten, die von vornherein nur einem vordefinierten Zugriff vorbehalten sind (z. B. Daten, auf die nur der Komponentenhersteller einer Komponente der Entität zugreifen darf). Siehe hierzu Abbildung 3.

In den Fällen der öffentlichen und privaten Daten sind die angewandten Regeln statisch, d. h. sie liefern bei allen Anfragen, unabhängig von Umgebungs- und Objekt-Attributen, immer den gleichen Wert zurück.

Auf Daten, die weder öffentlich noch privat sind, erfolgt der Zugriff über entsprechende (dynamische) Regeln. Siehe hierzu Abbildung 4.

Der Zugriff des Herstellers auf die I40 Entität (z. B. im Rahmen des Condition Monitorings, s. Kapitel 4.1) ist generell in einem Vertrag zwischen Hersteller und Betreiber geregelt. Das Zugriffsrecht der Komponenten-Hersteller auf ihre eigenen Komponentendaten ist Gegenstand weiterer Vertragsvereinbarungen, die dem Betreiber nicht zwangsläufig bekannt sind.

Um den vertragsgemäßen Zugriff von Komponentenherstellern auf Daten ihrer Komponenten über den Vertrag mit dem Hersteller zu ermöglichen sowie auch um das Problem des ungewollten Zugriffs auf Komponentendaten anderer Hersteller wirkungsvoll zu verhindern, besteht ein Weg darin, den Zugriff auf bestimmte Daten nur über einen bestimmten Zugriffspfad zu ermöglichen (s. Kapitel 2.2).

Es soll z. B. ein privater Zugriff auf eine nicht direkt erreichbare Komponente der I40 Entität erfolgen. Durch das Mitbringen herstellerqualifizierender Attribute wird automatisch beim Enforcement eine Anreicherung um ein wichtiges internes (geheimes) Subjekt-Attribut durchgeführt, das den Zugriff auf die ansonsten nicht direkt erreichbare Komponente regelbasiert ermöglicht.

In Abbildung 6 ist dargestellt, wie eine Abhängigkeit zwischen Betreiber, Hersteller der I40 Entität M, Hersteller einer Sub-Komponente Z und den Herstellern der Sub-Komponenten X und Y aufgelöst werden kann.

Der Zugriff auf die Komponente X oder Y ist dann ggf. nur über Regeln, die der Hersteller für die darunter liegende Komponente erzeugt, möglich. Zugriff auf bspw. Komponente X wird dann nur über hierarchisch ausgeführte Regeln via Pfad von oberster AAS des Betreibers (blau) → I40 Entität M (grau) → Komponente Z (dunkelblau) → Komponente X (gelb) möglich. Über diese Pfade wird die ansonsten physisch nicht hierarchisch aufgebaute AAS über die Regelausführung logisch hierarchisiert. Der Zugriff erfolgt in diesem Beispiel über drei logische, hierarchische Pfade mit separatem Enforcement.

In der Abbildung ist der Zugriff eines Clients (Subjekt ID 4711) auf eine Komponente der Maschine (Objekt X123) unter Vorlage der zur Regelausführung benötigten Subjekt-

Attribute „Policy“ (S815) und anderer Attribute (z. B. eine Information zu einem abgeschlossenen Vertrag) dargestellt.

Das Subjekt könnte auch den Zugriffspfad mitgeben, da sich jedoch die Landschaft der Assets beim Betreiber dynamisch ändern kann, ist es nötig, den Pfad, über den der Zugriff auf Komponente X erfolgt, aufzulösen. In der Abbildung wird dies auf Ebene der Betreiber-AAS durch Weitergabe an eine „Discovery“-Funktion erreicht, die letztendlich den aktuellen Pfad auflöst und zurückgibt.

Hinweis: Die „Discovery“-Funktion befindet sich noch in der Diskussion (s. Kapitel 2.3 zur Selbstauskunft), daher ist sie in der Abbildung nicht als direkt zugehörig zur AAS dargestellt, sondern über eine gestrichelte Linie.

In Abbildung 6 ist zusätzlich beispielhaft dargestellt, wie die Anreicherung des internen/geheimen Subjekt-Attributs aus einer externen Quelle ablaufen kann. Auf Ebene der Maschine M wird unter Vorlage der Subjekt-Attribute O(bjekt) und P(olicy) auf einen PDP des Herstellers weitergeleitet, der nach Prüfung der Regeln das geheime Attribut K (F%9A) zurückgibt. Dieses wird dann der Regelausführung für die Komponente Z zusammen mit den anderen Subjekt-Attributen vorgelegt. Die Anreicherung dient in diesem Fall der Prüfung und Gewährung eines Zugriffs eines Komponentenherstellers auf AAS-Submodelle seiner eigenen Komponente über den Pfad, der mit dem Maschinenhersteller (vertraglich) vereinbart wurde. Schließlich wird auf der Ebene der Komponente X nach entsprechenden Prüfungen das Ergebnis der Anfrage direkt an die AAS des Betreibers (blau) zurückgegeben und von dort an den Client weitergegeben. Diese Art des Zugriffs entspricht dem in Kapitel 2 und im Anhang (Kapitel 10) dargestellten Zugriffsmuster A.

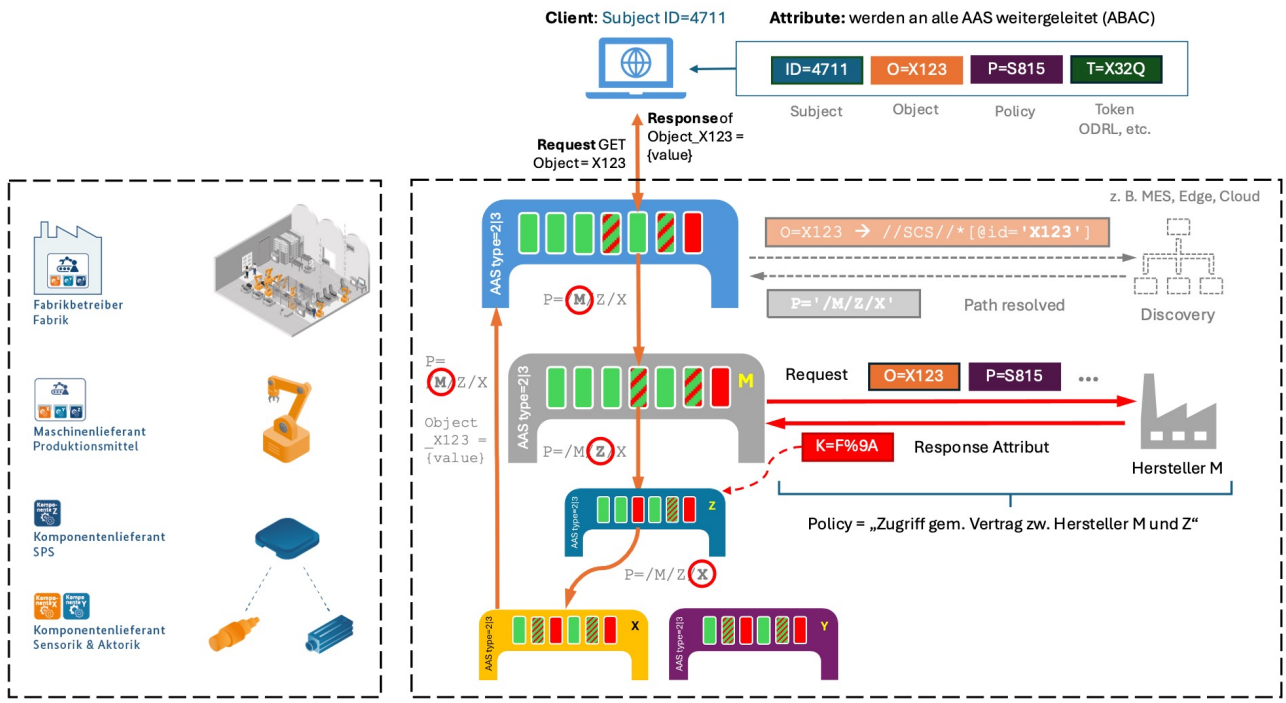
Hinweis: Die Regeln werden aufgrund der vertraglichen Vereinbarungen („Policies“) zwischen dem Betreiber und dem Hersteller oder dem Hersteller und den Komponentenherstellern modelliert und ausgeführt.

Anmerkung: Es ist selbstverständlich und notwendig, dass die übergebenen Attribute und deren Werte gegen Manipulation geschützt sein müssen. Dies ist mit gängigen Standard-Verfahren, wie z. B. Verschlüsselung oder Signatur, möglich.

In den unten genannten Beispielen und Abbildungen wird generell der Erfolgsfall diskutiert. Im Falle einer Ablehnung (die Regel wurde nicht erfüllt) wird an dieser Stelle die weitere Prüfung beendet und über den Zugriffspfad der Wert „false“ zurückgegeben.

Es ist zu beachten, dass je nach Zugriffsanfrage unterschiedliche und nicht immer notwendige Attribute benötigt werden. Ist die Kombinatorik der für den spezifischen Zugriff relevanten Attribute nicht bekannt, müssten entweder immer alle Attribute bei der Anfrage mitgeliefert bzw. angereichert werden oder die Zugriffsanfrage würde in vielen Fällen abgewiesen. Eine Alternative zur vollständigen Lieferung aller Attribute ist eine iterative Prozessverarbeitung, die es dem Enforcement erlaubt, beim Subjekt nachzufragen, wenn sonst nicht benötigte Attribute fehlen. Ein Beispiel hierfür ist das Attribut „Usage Control“, das ggf. nur bei Eintritt eines bestimmten Nutzungsfalles benötigt wird und auf Anforderung z. B. einen digitalen Nutzungsvertrag vorzulegen oder automatisiert zu signieren hat.

Abbildung 6: Zugriffspfade über logische Hierarchien zu den Komponenten Z, X bzw. Y der Maschine M



Quelle: Plattform Industrie 4.0 basierend auf Abbildung 3

4.1 Kommunikation und Zugriffskontrolle im Rahmen der Benutzungsvariante „Collaborative Condition Monitoring (CCM)“

In diesem Szenario erfolgt das Condition Monitoring für eine Industrie 4.0-Entität durch den Hersteller der Entität (z. B. einen Roboter) sowie durch Hersteller von zugelieferten Komponenten für die Entität (z. B. den Roboter-Arm oder ein spezielles Werkzeug, welches der Roboter verwendet). Der Zugriff erfolgt auf die AAS und deren relevante Submodelle mit den entsprechenden, dedizierten Zugriffsregeln.

Hierbei sind letztendlich verschiedene Nebenbedingungen zu beachten, die in die Zugriffsregeln einfließen müssen.

In der Abbildung 4 werden öffentliche Daten in grüner Farbe dargestellt. Private Daten sind in roter Farbe dargestellt. Daten mit dynamischen Zugriffsregeln werden in rot-schraffierter Farbe dargestellt.

Ein mögliches Ergebnis ist z. B., dass Komponentendaten, die nicht als „privat“ markiert sind, für den Betreiber zugänglich sein sollen, wenn er die I40 Entität besitzt, und auch für den Hersteller der Komponente selbst zugänglich sein sollen. Sie sollen/dürfen implizit (d. h. nach dem „Alles ist verboten“-Prinzip) jedoch nicht von Herstellern anderer Komponenten zugreifbar sein. Dies impliziert auch, dass der Zugriff vom Status der Entität abhängig ist.

Der Zugriff des Herstellers auf die I40 Entität im Rahmen des Condition Monitorings ist generell in einem Vertrag

zwischen Hersteller und Betreiber geregelt. Das Zugriffsrecht der Komponenten-Hersteller auf ihre eigenen Komponentendaten ist Gegenstand weiterer Vertragsvereinbarungen, die nicht zwangsläufig mit dem Betreiber vereinbart sind, sondern mit dem Hersteller der Maschine. Diese Vereinbarungen sind weiterhin dem Betreiber nicht bekannt.

Die Beschreibung des Zugriffs-Kontroll-Beispiels ist wie folgt:

Involvierte Parteien:

- Betreiber B der Maschine
- Maschinenlieferant/Integrator/Hersteller M der Maschine
- Hersteller H1 der Komponente X
- Hersteller H2 der Komponente Y

Szenario:

Grundsätzlich gilt bei der Beschreibung das oben genannte „Alles ist verboten"-Prinzip. Zusätzlich existieren Verträge zwischen den Parteien, die den Zugriff auf die Daten im Rahmen des Condition Monitorings beinhalten.

Der Hersteller/Integrator M soll im Rahmen des Condition Monitorings der I40 Entität Zugriff auf alle Daten der I40 Entität haben, außer den privaten Daten der Komponentenhersteller H1 und H2. Dies sind die öffentlichen Daten, die von ihm bereitgestellten nicht öffentlichen Daten, die nicht privaten Daten der Komponentenhersteller sowie die von ihm eingerichteten privaten Daten der Entität.

Der Hersteller H1 soll Zugriff auf die öffentlichen Daten der I40 Entität haben, die von ihm bereitgestellten nicht öffentlichen Daten sowie die von ihm eingerichteten privaten Daten für Komponente X. Er soll keinen Zugriff auf nicht private Daten von Komponente Y (und anderen Komponentenherstellern) haben. Der Zugriff soll über drei separate Enforcements 1, 2 und 3 über den Pfad „Daten mit dynamischer Zugriffskontrolle von Hersteller M" → „Nicht öffentliche und private Daten von Komponente Z" → „Nicht öffentliche und private Daten von Komponentenhersteller H1" erfolgen.

Der Hersteller H2 soll Zugriff auf die öffentlichen Daten der I40 Entität haben, die von ihm bereitgestellten nicht öffentlichen Daten sowie die von ihm eingerichteten privaten Daten für Komponente Y. Er soll keinen Zugriff auf nicht private Daten von Komponente X (und anderen Komponentenherstellern) haben. Der Zugriff soll über drei separate Enforcements 1, 2 und 3 über den Pfad „Daten mit dynamischer Zugriffskontrolle von Hersteller M" → „Nicht öffentliche und private Daten von Komponente Z" → „Nicht öffentliche und private Daten von Komponentenhersteller H2" erfolgen.

Der Betreiber B soll Zugriff auf alle öffentlichen und nicht privaten Daten des Herstellers sowie auch der Komponentenhersteller haben, jedoch nicht auf deren private Daten.

Daraus entstehen komplexe und jeweils unterschiedliche Regeln für die Parteien B, M, H1 und H2. Die generellen Grundbedingungen für den Zugriff sind jedoch der existierende Monitoring- und Wartungsvertrag zwischen dem Hersteller und dem Betreiber sowie implizite Zugriffsregeln auf nicht direkt erreichbare Komponenten.

Zusätzliche dynamische Regeln:

Neben den statischen Regeln enthalten die dynamischen Regeln weitere Subjekt-, Objekt- und Umgebungs-Attribute.

Neben den obigen, vertraglich vereinbarten Zugriffs-Grundbedingungen sollen in diesem Beispiel weitere dynamisch geprüfte Regeln gelten:

- Der Zugriff auf die Maschine und deren Komponenten darf nur dann erfolgen, wenn die beauftragten Berechtigten der Unternehmen M, H1, und H2 sich in der Lokation ihres eigenen Unternehmens befinden oder in einer Lokation des Betreibers
- Der Zugriff darf grundsätzlich nur in einem Zeitraum von 15:00 bis 17:00 Uhr erfolgen
- Die Maschine muss vom Betreiber B in Besitz genommen worden sein und muss sich im Wartungsmodus befinden
- Sollte es sich um eine halbjährliche teilweise vor Ort stattfindende Inspektion handeln, muss die Maschine auf unter 50 °C abgekühlt sein.

Benötigte Subjekt-Attribute:

Für das erste und das zweite Enforcement werden jeweils folgende Subjekt-Attribute benötigt:

- Company ID: Identität des anfragenden Subjekts

- Company Type (1=Betreiber, 2=Hersteller, 3=Komponentenhersteller)
- Policy ID (s. Abbildung 6)
- Contract ID: Verweis auf den Vertrag zwischen Betreiber B und Hersteller M als Basis für den Datenzugriff (Hinweis: Für diesen Vertrag wird auch häufig der Begriff „Usage Control“ verwendet). Dieses Attribut kann bspw. aus dem Standard ODRL (Open Digital Rights Language) [19] stammen.
- Current Subject Location

Speziell für das zweite und dritte Enforcement im Rahmen des Pfadzugriffs „Daten mit dynamischer Zugriffskontrolle von M“ → „Nicht öffentliche und private Daten von Komponente Z“ → „Nicht öffentliche und private Daten von H1 oder H2“ werden noch weitere Subjekt-Attribute benötigt:

- Requested Path: Pfad, der benutzt werden soll, um auf Komponente X oder Y zugreifen zu können. Z. B. M/Z/X (s. Abbildung 6). Dieser muss ggf. auf der AAS der Betreiber-Ebene durch einen Discovery Service dynamisch ermittelt werden (s. Kapitel 2.3).

Zusätzlich soll im Enforcement auf Ebene M vor der Weitergabe an das nächste Enforcement ein weiteres flüchtiges Subjekt-Attribut (K) angereichert werden, welches, wie in Abbildung 6 dargestellt, von Remote (hier vom Hersteller M) angereichert wird. Dies kann auch im folgenden Enforcement auf Ebene Z stattfinden, ist aber in Abbildung 6 nicht dargestellt.

Benötigte Umgebungsattribute:

- Local Time

Benötigte Objekt-Attribute:

- Entity Ownership Company ID (zur Prüfung der Inbesitznahme durch den Betreiber B)
- Asset State
- Asset Temperature
- Inspection Today (true/false)

Pro Sub-Modell der AAS der Maschine werden folgende Objekt-Attribute benötigt:

- Sub Model Ownership Company ID
- Data Type (1 = öffentlich, 2 = nicht öffentlich/nicht privat, 3 = privat). Dieses Attribut kann als Hilfsattribut zur Vereinfachung der Erstellung von Regeln verwendet werden. Es wird hier beispielhaft verwendet.
- Direct Access (true/false) (Ist das Submodell direkt erreichbar, also nicht nur indirekt über einen Pfad bzw. eine logische Hierarchie). Dieses Attribut kann als Hilfsattribut zur Vereinfachung der Erstellung von Regeln verwendet werden. Es wird hier beispielhaft verwendet.

Durchgeführte Regelprüfungen:

- Regel 0 (Vorprüfung Subjekt-Attribute)
  - Sind die Contract ID und die Company ID gültig/bekannt?
  - → Falls ja, weiter mit den Prüfungen, ansonsten mit „Verbot“ zurück
  - Ist die Policy ID bekannt und passend zur Contract ID und/oder zur Company ID?
  - → Falls ja, weiter mit den Prüfungen, ansonsten mit „Verbot“ zurück
    Hinweis: Die Policy ID kann an mehreren Stellen zur Prüfung herangezogen werden und jeweils die Ausführung spezifischer Regeln pro Enforcement triggern
  - Ist das angefragte Submodell direkt erreichbar?
    - Falls nein, und es handelt sich um Enforcement 1: Anreicherung der Subjekt-Attribute mit dem internen, von Remote abgefragten Attribut 1, und weiter mit den Prüfungen.
    - Falls nein, und es handelt sich um Enforcement 2: Prüfung, ob das interne Subjekt-Attribut aus Enforcement 1 sowie die aktuellen und angefragten Pfade mit dem richtigen Wert vorhanden sind: Ist dies nicht der Fall, mit „Verbot“ zurück. Ansonsten (ggf. nach Anreicherung der Subjekt-Attribute mit dem internen, von Remote abgefragten Attribut 2) weiter mit den Prüfungen.
    - Falls nein, und es handelt sich um Enforcement 3: Prüfung, ob das ggf. intern angereicherte Subjekt-Attribut aus Enforcement 2 sowie die aktuellen und angefragten Pfade mit dem richtigen Wert vorhanden sind: Ist dies nicht der Fall, mit „Verbot“ zurück, ansonsten weiter mit den Prüfungen.

- Regel 1 (öffentliche Daten):
  - Ist der Datentyp des Typs 1 (öffentlich)?
    - → Falls „true“, mit „Erlaubnis“ und angefragten Daten zurück, oder Weitergabe an Enforcement 2 bzw. Enforcement 3, ansonsten (falls „false“) nächste Regel ausführen

- Regel 2 (private Daten):
  - Ist der Datentyp des Typs 3 (privat) → Falls nein, nächste Regel ausführen
  - Entspricht die übergebene Company ID der Ownership Company ID des angefragten Submodells?
    - → Falls die letzte Regel mit „true“ beantwortbar ist, dann zurück mit „Erlaubnis“ oder Weitergabe an Enforcement 2 (bzw. Enforcement 3), ansonsten zurück mit „Verbot“

- Regel 3 (Unterscheidungsregeln Hersteller, Komponentenhersteller, Betreiber):
  - Wenn es sich um den Betreiber handelt (Company Type = 1 ?)
  - Ist der Datentyp des Typs 1 (öffentlich) oder 2 (weder öffentlich noch privat)?
  - Ist der Betreiber gleichzeitig der Owner (Company ID = Entity Ownership Company ID)
    - → Falls alle 3 Regeln mit „true“, beantwortet werden, zurück mit „Erlaubnis“, oder Weitergabe an Enforcement 2
    - → Falls die letzte Regel mit „false“ beantwortet ist, zurück mit „Verbot“

  - Wenn es sich um den Hersteller oder einen Komponentenhersteller handelt (Company Type = 2 oder 3 ?)
    - Ist die lokale Zeit im Gültigkeitsintervall?
    - Befindet sich der Unternehmensbeauftragte in einer erlaubten Lokation (Current Subject Location = Betreiber-Lokation oder Unternehmens-Lokation)?
    - Befindet sich die I40 Entität im Wartungsmodus (Asset State = Wartungsmodus)
    - Befindet sich die I40 Entität im Besitz des Betreibers (Entity Ownership Company ID = ID des Betreibers)?
    - Befindet sich die I40 Entität im Inspektionsmodus (Inspection Today = true) UND ist deren Temperatur kleiner 50 °C (Asset Temperature <50 °C), ODER befindet sie sich nicht im Inspektionsmodus (Inspection Today = false)
    - → Falls alle Regeln mit „true“ beantwortet werden können, weiter zur nächsten Regel
    - → Falls nicht, zurück mit „Verbot“
  - Wenn es sich um den Hersteller handelt (Company Type = 2 ?)
    - Ist der Datentyp vom Type 2 (weder öffentlich noch privat)?
    - → Falls beide Regeln „true“ sind, zurück mit „Erlaubnis“ oder Weitergabe an Enforcement 2 (bzw. 3), ansonsten zurück mit „Verbot“

  - Wenn es sich um den Komponentenhersteller handelt (Company Type = 3 ?)
    - Ist der Datentyp vom Type 2 (weder öffentlich noch privat) oder 3 (privat)?
    - Gehört das Submodell dem Komponentenhersteller (Sub Model Ownership Company ID = Company ID)?
    - → Falls alle Regeln „true” sind, zurück mit „Erlaubnis” oder Weitergabe an Enforcement 2, ansonsten zurück mit „Verbot“

- Regel 4: Keine der Regeln wurde ausgeführt:
  - Zurück mit „Verbot“ nach dem „Alles ist verboten“-Prinzip.

Die Weitergabe an Enforcement 2 erfolgt nur, wenn man sich im Enforcement 1 befand, eine der Regeln für das aktuell zu prüfende Submodell, über das der Pfad hinwegläuft, mit „true“ beantwortet wurde und das angefragte Submodell nur indirekt erreichbar ist. Danach werden alle Regeln im Rahmen von Enforcement 2 wiederum durchlaufen, unter zusätzlicher Prüfung der Einhaltung der Pfade (durch weitere Anreicherungen mit internen Subjekt-Attributen) und unter Prüfung, ob man nun am Ende des Pfades (am Ziel-Submodell) angekommen ist. Ist dies der Fall, können die Daten des indirekt erreichten Submodells zurückgegeben werden. So können zirkulär auch weitere Enforcements 3, 4, ... aufgerufen werden, die jeweils das gleiche Regelwerk durchlaufen.

4.2 Informationsdatenzugriff auf einen „Industrie Data Space“

In diesem Szenario möchte ein Data-Space-Mitglied des imaginären Data Space CAMAGA-IDX innerhalb dieses Datenraums erkunden, ob er als Zulieferer für die Firma X-Industrie einen Zulieferauftrag erhalten kann und nach

der Interessensbekundung oder Auftragszusage Zugriff auf weitere Daten benötigt.

Beteiligte:

- Data Space Administration (bzw. zugehörige Administrationsberechtigte, welche den grundsätzlichen Zugang seitens der Data-Space-Mitglieder verwalten)
- Unternehmen A, welches einen Auftrag 1 im Data Space bekanntmacht oder bereitstellt
- Unternehmen B (bzw. Berechtigte des Unternehmens), welches Aufträge sucht und ggf. an Auftrag 1 interessiert ist
- Verschiedene anerkannte Auskunftsstellen

Voraussetzungen:

Unternehmen A hat bereits einen Mitgliedsvertrag mit dem Data Space abgeschlossen und hat daher Zugriff auf allgemeine Informationen innerhalb des Data Space, wie z. B. Auftragsausschreibungen. Die Identitäten [20] von Unternehmen A und B gelten als aktuell sicher/verifiziert.

Szenarien:

1. Unternehmen B sucht aktiv nach Auftrags-Ausschreibungen und benötigt Zugriff auf die Ausschreibungs-Kriterien (z. B. technische, vertragstechnische Kriterien und Nebenbedingungen). Unternehmen A stellt als Voraussetzung für den Lese-Zugriff auf dessen Auftrags-Ausschreibungen zusätzliche Regeln auf, wie z. B. eine erfolgreiche Vorab-Prüfung der Existenz und Bonität des Interessenten, sowie Verhinderungen von Lesezugriffen durch Konkurrenzunternehmen, die ebenfalls am Data Space teilnehmen. Auftrag 1 obliegt außerdem einer industriespezifischen Art der Geheimhaltung, so dass als Auftragnehmer nur zertifizierte Unternehmen in Frage kommen, die entsprechende Erklärungen unterzeichnet haben. Unternehmen B gibt schließlich ein Angebot zu Auftrag 1 ab.

2. Unternehmen A prüft das Angebot. Dies beinhaltet u. a. eine detaillierte Prüfung des potenziellen und neuen Zulieferers sowie der Angebotsinformationen. Es benötigt hierbei Zugriff auf zusätzliche Unternehmensinformationen zu Unternehmen B. Es erteilt den Auftrag 1 an Unternehmen B.

3. Unternehmen A und B benötigen nach Auftragsabschluss Zugriff auf jeweilige technische Daten, die im Rahmen der eingebetteten Folge der Produktionsschritte erforderlich sind. Dies sind z. B. Zugriffe auf den Produktions- und Lieferstatus von Vorprodukten, die Unternehmen B verarbeitet und von Unternehmen A zur Verfügung gestellt werden, oder Produktionsfortschritts- und Qualitäts-Informationen, die Unternehmen A von Unternehmen B benötigt.

Regel für Szenario 1:

Subjekt: Unternehmen B bzw. dessen Berechtigte

Objekt: Liste Auftragsausschreibungen von Unternehmen bzw. entsprechende Liste von Unternehmen A

Subjekt-Attribute:
- Unternehmens-ID
- Such-Kriterien (z. B. Schlüsselwörter zur Eingrenzung der Suche)
- Link zu einer Zugehörigkeits-Bescheinigung seitens der Data Space Administration
- Link zu einer anerkannten Bonitäts-Auskunftsstelle
- Link zu einer anerkannten Reputations-Auskunftsstelle
- Selbstauskunfts-Attribute zu Bonität, Reputation und Geheimhaltungs-Zertifizierung
- Link zu einer anerkannten Auskunftsstelle, die den Beweis für eine Geheimhaltungszertifizierung erbringt
- Erlaubnis, dass Unternehmen A die anerkannten Auskunftsstellen innerhalb von 2 Wochen anfragen darf

Objekt-Attribute:
- Auftrag im Status „ausgeschrieben“ (nicht vergeben)
- Geheimhaltungslevel des Auftrags/der Ausschreibung

Umgebungs-Attribute:
- keine

Anfrage: Lesezugriff auf Auftragsausschreibungen und deren Details

Regel für Szenario 2:

Subjekt: Unternehmen A bzw. dessen Berechtigte

Objekt: Bonitäts- und Reputationsinformationen zu Unternehmen A, zur Verfügung gestellt durch anerkannte Auskunftsstellen

Subjekt-Attribute:
- Unternehmens-ID
- Erlaubnis von Unternehmen B zur Anfrage an die anerkannte Auskunftsstelle
- Such-Kriterien (z. B. Link-Informationen, von Unternehmen B zur Verfügung gestellt)

Objekt-Attribute:
- Keine

Umgebungs-Attribute:
- Anfragedatum (innerhalb von 14 Tagen nach Angebotsabgabe seitens Unternehmen B)

Anfrage: Lesezugriff auf Dokumente der anerkannten Auskunftsstellen

Regel für Szenario 3:

Subjekt: Unternehmen A oder B bzw. deren Berechtigte

Objekt: Produktions- und Lieferketteninformationen für Vorprodukte und Zulieferer-Produkt(e)

Subjekt-Attribute:
- Unternehmens-ID
- Vertrags-ID, unter der der Zugriff gewährt wird

Objekt-Attribute:
- Vertrags-ID
- Auftrags-ID
- Auftrags-Status (nicht fertiggestellt/geliefert)

Umgebungs-Attribute:
- Anfragedatum (Zwecks Prüfung der Vertragsgültigkeit)

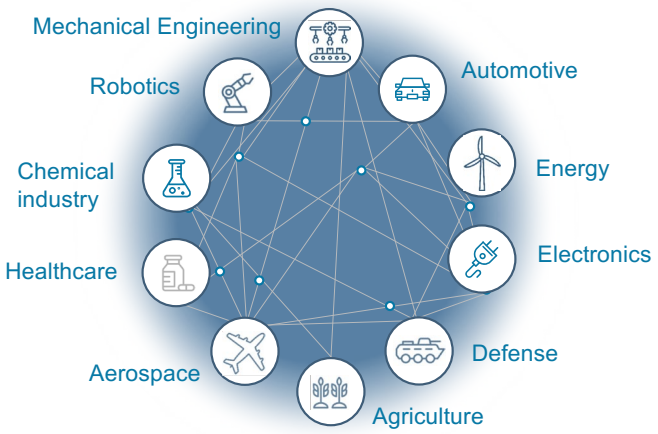
Anfrage 1: Lesezugriff seitens Unternehmen A auf den Produktionsstatus von Auftrag 1 bei Unternehmen B

Anfrage 2: Lesezugriff seitens Unternehmen B auf den Lieferstatus von Vorprodukten bei Unternehmen A

5 Pfadabhängigkeiten und semantische Einheitlichkeit

Wie im vorherigen Kapitel dargestellt, können Pfadabhängigkeiten auch in Bezug auf I4.0-Ökosysteme auftreten: Zuerst muss einem I4.0-Ökosystem beigetreten werden, bevor der spezielle Zugriff möglich ist. Bspw. muss zuerst einem Catena-X-Verbund beigetreten werden, bevor Zugriff auf ein spezielles Datum angefragt werden kann. Auch können verschiedene Branchen mit ihren speziellen Wertschöpfungsketten als unterschiedliche I4.0-Ökosysteme betrachtet werden (Abbildung 7). Wer Teil einer solchen Wertschöpfungskette sein will, muss wiederum die richtigen Anforderungen erfüllen: z.B. Handelserlaubnisse, IT-Sicherheitsnachweise, aber auch Kompatibilität bei der Digitalisierung und Vernetzung. [20]

Abbildung 7: Vernetzung unterschiedlicher Wertschöpfungsketten



Quelle: Plattform Industrie 4.0

5.1 Semantische Einheitlichkeit bei attributbasierter Zugriffskontrolle (ABAC)

Wie in den Publikationen [9] [11] gezeigt, bietet sich eine attributbasierte Zugriffskontrolle (ABAC) für die Industrie 4.0 an. Zu berücksichtigen sind jedoch die Dynamik und die damit verbundene Komplexität eines ABAC in der Industrie 4.0. So können im Laufe der Zeit neue Attribute hinzukommen, alte Attribute können wegfallen oder die Bedeutung von Attributen kann sich ändern. Darüber hinaus können Attribute je nach I4.0-Ökosystem unterschiedliche Bedeutungen haben.

Diese Publikation schlägt daher Basis-Attribute vor, die semantisch einheitlich interpretierbar sein sollten, um eine Interoperabilität über verschiedene I4.0-Ökosysteme hinweg zu gewährleisten (siehe Abbildung 8 und Tabelle 2). Diese Basisattribute werden in einem VWS-Submodell benötigt.

Innerhalb eines I4.0-Ökosystems können die Attribute dann einen anderen Umfang oder eine andere Bedeutung haben.

Darüber hinaus stellen wir die These auf, dass die I4.0-Ökosysteme selbst eindeutig gekennzeichnet sein müssen. Sie müssen also eine Identität sowie eine Versionsnummer haben, damit für alle Berechtigten klar ist, welcher Attribut-Satz zu verwenden ist.

Hier seien einige semantisch einheitliche und standardisierte Attribute genannt, die sich außerhalb dieser Betrachtung befinden, jedoch auch für den Industrie 4.0-Kontext geeignet sind.

- OASIS-Profil zur Prüfung von US-Exportbeschränkungen [26]

  Es wird eine Definition von Attributen eingeführt, die für die Erstellung von Regeln für Exportkontrollen geeignet sind.

- OASIS-Profil zur Prüfung von vertragsbasierten Intellectual-Property-Zugriffen [27]

  Es wird eine Definition von Attributen eingeführt, die für die Erstellung von Regeln zum Zugriff von Partei A auf Intellectual Properties von Partei B geeignet sind.

- Open Digital Rights Language (ODRL) [19]

  ODRL stellt eine Policy-Sprache dar, die vertragliche Rechte bei der Benutzung von digitalen Dokumenten ausdrücken kann. ODRL wird im Industrie 4.0-Kontext bereits genutzt (z. B. Catena-X) und kann als eine Quelle von semantisch einheitlichen Attributen angesehen werden, die zur Regelprüfung mit herangezogen werden können.

Abbildung 8: Basis- und ökosystemspezifische Attribute

Quelle: Plattform Industrie 4.0

Tabelle 2: Beispiele für Basis-Attribute

Aktion	Erzeugen
	Lesen
	Ändern
	Löschen
Umgebungsattribute	Zeitstempel
	Ökosystemsprache
	Rechtliche Rahmenbedingungen, Rechtsnorm
Subjekt-Attribute	Identität des Subjekts [20]
	Ort des Subjekts
	Rechtliche Rahmenbedingungen
	Ökosystemzugehörigkeit
Objekt-Attribute	Identität des Objekts
	Ort des Objekts
	Rechtliche Rahmenbedingungen
	Ökosystemzugehörigkeit
	Zustände des Objekts

6 Fazit und Ausblick

Industrie 4.0 erfordert Zugriffs- und Nutzungskontrolle in einem Wertschöpfungsnetzwerk mit unterschiedlichen Stakeholdern.

Die AAS kann eine zentrale Rolle als Endpunkt für den Datenzugriff/die Datennutzung spielen.

Aus den in Kapitel 2 skizzierten Anforderungen aus Sicht der drei Beteiligten am Beispiel des Use Cases „Collaborative Condition Monitoring (CCM)"...

- **Fabrikbetreiber:** Zugriff/Nutzung auf alle Submodelle der AAS, sofern keine vertraglichen Restriktionen bestehen
- **Maschinenlieferant:** Zugriff/Nutzung auf vertraglich vereinbarte Submodelle, z. B. für Condition Monitoring
- **Komponentenlieferanten:** Zugriff/Nutzung auf Submodelle ihrer Komponenten, vertraglich geregelt mit dem Maschinenlieferanten

... ergeben sich vielfältige Herausforderungen. Technische Lösungen und vertragliche Regelungen müssen Hand in Hand gehen, um die Datensicherheit zu gewährleisten und gleichzeitig den notwendigen Datenzugriff/die Datennutzung für alle Beteiligten zu ermöglichen.

Ausgangsbasis für die technische Lösung ist das in Abbildung 2 exemplarisch für eine Maschine in einer Fabrik/in einem Unternehmen illustrierte Zusammenspiel von physischen und virtuellen Assets. Vorausgesetzt werden:

- Physisches Asset und jeweilige AAS sind untrennbar miteinander verbunden
- Physisches Asset und dazugehörige AAS synchronisieren sich fortlaufend

In der virtuellen Repräsentanz des Produktionsmittels entsteht eine **logisch-hierarchische „Baumstruktur"**.

Der Lösungsansatz mittels logischer Hierarchien in Verbindung mit attributbasierter Zugriffskontrolle (ABAC) wird in mehreren Szenarien in Kapitel 3 verprobt.

Als **Grundansatz** aus allen Szenarien ergibt sich Folgendes:

- Das logisch übergeordnete Element prüft den Zugriff/die Nutzung des darunter liegenden Elements (Eltern-Kind-Beziehung).
- Die untergeordnete Ebene ist nur über die logisch übergeordnete Ebene erreichbar (durch Regelwerk sicherzustellen).
- Die Regeln für den Zugriff/die Nutzung werden vertraglich auf den Lieferstufen vereinbart.
- Die Durchsetzung der Regeln übernimmt entweder der Policy Decision Point (PDP) der VWS der übergeordneten Ebene oder ein von ihr beauftragter PDP.

Dynamischer Aufbau der logisch-hierarchischen Baumstruktur:

Die logisch-hierarchische Baumstruktur entsteht im Rahmen der Lieferbeziehungen des Wertschöpfungsnetzwerks. Exemplarisch heißt das für den Use Case CCM aus Kapitel 2:

- **Komponentenlieferant:** Muss in der Lage sein, seine Komponenten im Betrieb zu finden. Er liefert seine Komponenten (physische Assets) mit den jeweiligen AASen inkl. der Zugriffs-/Nutzungsrechte für die Submodelle aus.
- **Maschinenlieferant:** Erzeugt eine AAS der Maschine, die ein Verzeichnis aller logisch darunter liegenden AASen beinhaltet, typischerweise die kommunikationsfähigen AASen der Komponenten. Auf Basis der vertraglichen Vereinbarungen erfolgt die Anpassung für den Zugriff/die Nutzung der Submodelle der Komponenten, z. B. für Condition Monitoring.
- **Fabrikbetreiber:** Die VWS der Maschine mitsamt den logisch darunter liegenden Komponenten wird der übergeordneten Ebene des Fabrikbetreibers (typischerweise dem MES-System) bekannt gemacht. Zugriff/Nutzung auf alle logisch-hierarchisch untergeordneten Submodelle erfolgt analog zu den vertraglichen Vereinbarungen der AAS, sofern keine vertraglichen Restriktionen bestehen.

Suchen und Finden von AASen bzw. relevanter Submodelle:

- Ausgangspunkt für die Suche ist immer der oberste Knoten in der jeweiligen Hierarchie. Im Anwendungsfall CCM ist dies der Anlagenbetreiber.

- Durch das Absteigen innerhalb der logisch-hierarchischen Baumstruktur entlang des logischen Pfades werden die relevanten VWS bzw. Submodelle identifiziert und die jeweilige VWS entscheidet über den Zugriff bzw. die Nutzung der VWS bzw. deren Submodelle.

Greenfield vs. Brownfield:

- Der in der Publikation vorgestellte Ansatz ist nicht nur für „Greenfield"-Anlagen anwendbar, sofern das betreffende physische Asset mit einem digitalen Zwilling ausgestattet ist. Auch „Brownfield"-Assets können mit einem Gateway/Konnektor ausgestattet werden, der die Funktion eines digitalen Zwillings übernimmt. Durch die damit mögliche Integration in die logisch-hierarchische Baumstruktur ist ein nahtloses Zusammenspiel und ein sanfter Übergang von Brownfield zu Greenfield möglich.

Der vorgestellte Ansatz ist geeignet, die Industrie 4.0-Sprache [21] um den Aspekt des Nutzungsmanagements zu erweitern. Sinnvollerweise sollten hier die Erkenntnisse aus dem Projekt „VWS Vernetzt" [22] mit einfließen.

Logische Hierarchien als Grundlage für souveräne Hierarchien in der Industrie 4.0:

Die zuvor vorgestellte Lösung von logischen Hierarchien und attributbasierter Zugriffskontrolle (ABAC) legt den Grundstein für die Umsetzung souveräner Hierarchien in der Industrie 4.0.

- Logische Baumstruktur: Die hierarchische Organisation der Assets in einer Baumstruktur ermöglicht eine granulare Kontrolle des Datenzugriffs und der Datennutzung.
- Durchsetzung auf aktiven AASen: Die Regeln für den Zugriff und die Nutzung von Daten werden auf den AASen der einzelnen Assets hinterlegt und durchgesetzt.

Detaillierte Regelausführung: Die Verwendung von ABAC ermöglicht die Definition fein abgestufter Regeln, die den individuellen Anforderungen der einzelnen Unternehmen gerecht werden.

Souveränität: Die Unternehmen behalten die Kontrolle über ihre Daten und können selbstständig entscheiden, wer auf welche Daten zugreifen kann und wie diese Daten verwendet werden dürfen.

Souveräne Hierarchien ermöglichen somit das eigenverantwortliche Handeln der Unternehmen innerhalb klar definierter Hierarchieebenen im Zusammenspiel mit AAS, die diese Umsetzung durch Flexibilität und genaue Kontrolle der AAS-Daten und deren Nutzung unterstützen. Dies fördert die vertrauensvolle Zusammenarbeit in der unternehmensübergreifenden Kommunikation und ermöglicht gleichzeitig die dynamische Anpassung an neue Anforderungen und Regulierungen. Souveräne Hierarchien in Industrie 4.0 bilden ein zentrales Instrument zur Sicherung der Datensouveränität von AAS.

Bezug zu den Anforderungen aktueller und zukünftiger EU-Regulierungen:

Das Konzept der souveränen Hierarchien mit AAS und logischen Hierarchien ist geeignet, um Anforderungen des Cyber Resilience Act (CRA) [23],) des EU Data Act [24] und der EcoDesign for Sustainable Products Regulation [25] zu unterstützen.

Details zu diesen Themen sollen in einem geplanten Dokument erläutert werden.

7 Literaturverzeichnis

[1] Plattform Industrie 4.0, „Was ist die Verwaltungsschale aus technischer Sicht?“, 2021. [Online]. Available: https://industrialdigitaltwin.org/wp-content/uploads/2021/10/2021_Was-ist-die-AAS-3.pdf.

[2] Catena-X, Automotive Network, „Catena-X“, [Online]. Available: https://catena-x.net/de/.

[3] Plattfrom Industrie 4.0, „Manufacturing-X“, [Online]. Available: https://www.plattform-i40.de/IP/Navigation/DE/Manufacturing-X/Initiative/initiative-manufacturing-x.html. [Zugriff am 07.03.2024].

[4] Plattform Industrie 4.0, „Initiative zur Digitalisierung der Lieferketten in der Industrie“, [Online]. Available: https://www.plattform-i40.de/IP/Navigation/DE/Manufacturing-X/Initiative/initiative-manufacturing-x.html. [Zugriff am 07.03.2024].

[5] IDTA, „Digitaler Zwilling“, [Online]. Available: https://industrialdigitaltwin.org/?gclid=EAIaIQobChMIztWcxNjFgwMVZpGDBx1x7wDkEAAYASAAEgIlGvD_BwE.

[6] IDTA, „Digitales Typenschild – ein Scan spart unendlich viele Ressourcen“, [Online]. Available: https://industrialdigitaltwin.org/use-cases/digitales-typenschild-ein-scan-spart-unendlich-viele-ressourcen.

[7] Catena-X, „Semantic Layer/Digital Twins“, [Online]. Available: https://catena-x.net/de/angebote-standards/digitaler-zwilling.

[8] IDTA, „DPP4.0 – The Digital Product Passport for Industry 4.0“, [Online]. Available: https://dpp40.eu/.

[9] Plattform Industrie 4.0, „Zugriffssteuerung für Industrie 4.0-Komponenten zur Anwendung von Herstellern, Betreibern und Integratoren“, 2018. [Online]. Available: https://www.plattform-i40.de/IP/Redaktion/DE/Downloads/Publikation/zugriffssteuerung-industrie40-komponenten.html.

[10] Plattform Industrie 4.0, „Security in RAMI4.0“, 2016. [Online]. Available: https://www.plattform-i40.de/IP/Redaktion/DE/Downloads/Publikation/security-rami40.html.

[11] NIST, „NIST Special Publication 800-162: ‚Guide to Attribute Based Access Control (ABAC)‘“, 2019. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/162/upd2/final.

[12] NIST, „NIST Special Publication 800-192: „Verification and Test Methods for Access Control Policies/Models““, 2017. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-192.pdf.

[13] National Security Agency, „Risk Adaptable Access Control (RAdAC)“, 2009. [Online]. Available: https://csrc.nist.gov/csrc/media/events/privilege-management-workshop/documents/presentations/bob_mcgraw.pdf.

[14] NIST, „NIST Special Publication 800-178: „A Comparison of Attribute Based Access Control (ABAC) Standards for Data Service Applications““, 2019. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/178/final.

[15] Plattform Industrie 4.0, „Der Weg zum digitalen Champion – Durch digitale Transformation zur Datenökonomie“, 2024. [Online]. Available: TBD.

[16] IDTA, „IDTA 02011-1-0 Hierarchical Structures enabling Bills of Material“, 04 2023. [Online]. Available: https://industrialdigitaltwin.org/wp-content/uploads/2023/04/IDTA-02011-1-0_Submodel_HierarchicalStructuresEnablingBoM.pdf.

[17] Plattform Industrie 4.0, „Details of the Asset Administration Shell – Part 1“, 2022. [Online]. Available: https://www.plattform-i40.de/IP/Redaktion/DE/Downloads/Publikation/Details_of_the_Asset_Administration_Shell_Part1_V3.html.

[18] Plattform Industrie 4.0, „Discovery in Industrie 4.0 System Environment“ (geplant), 2024. [Online]. Available: TBD.

[19] W3C, „ODRL Information Model 2.2“, 2018. [Online]. Available: https://www.w3.org/TR/odrl-model/.

[20] Plattform Industrie 4.0, „Vertrauensinfrastrukturen im Kontext von Industrie 4.0 – Anforderungen und Lösungsbausteine“, 2021. [Online]. Available: https://www.plattform-i40.de/Redaktion/DE/Publikationen/Industrie/industrie-4-0-Vertrauensinfrastrukturen.pdf?__blob=publicationFile&v=1.

[21] Plattform Industrie 4.0, „I4.0-Sprache“, 2018. [Online]. Available: https://www.plattform-i40.de/IP/Redaktion/DE/Downloads/Publikation/hm-2018-sprache.html.

[22] IFAT LIA, „Projekt ‚Verwaltungsschale vernetzt‘“, [Online]. Available: https://vwsvernetzt.de/.

[23] EU-COM, „EU Cyber Resilience Act“, [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act.

[24] EU-COM, „Data Act“, [Online]. Available: https://digital-strategy.ec.europa.eu/de/policies/data-act.

[25] EU-COM, „Ecodesign for Sustainable Products Regulation“, [Online]. Available: https://commission.europa.eu/energy-climate-change-environment/standards-tools-and-labels/products-labelling-rules-and-requirements/sustainable-products/ecodesign-sustainable-products-regulation_en.

[26] OASIS, „XACML 3.0 Export Compliance-US (EC-US) Profile Version 1.0“, 2015. [Online]. Available: http://docs.oasis-open.org/xacml/3.0/ec-us/v1.0/os/xacml-3.0-ec-us-v1.0-os.pdf.

[27] OASIS, „XACML Intellectual Property Control (IPC) Profile Version 1.0“, 2015. [Online]. Available: http://docs.oasis-open.org/xacml/3.0/ipc/v1.0/os/xacml-3.0-ipc-v1.0-os-en.html.

8 Abbildungsverzeichnis

9 Tabellenverzeichnis

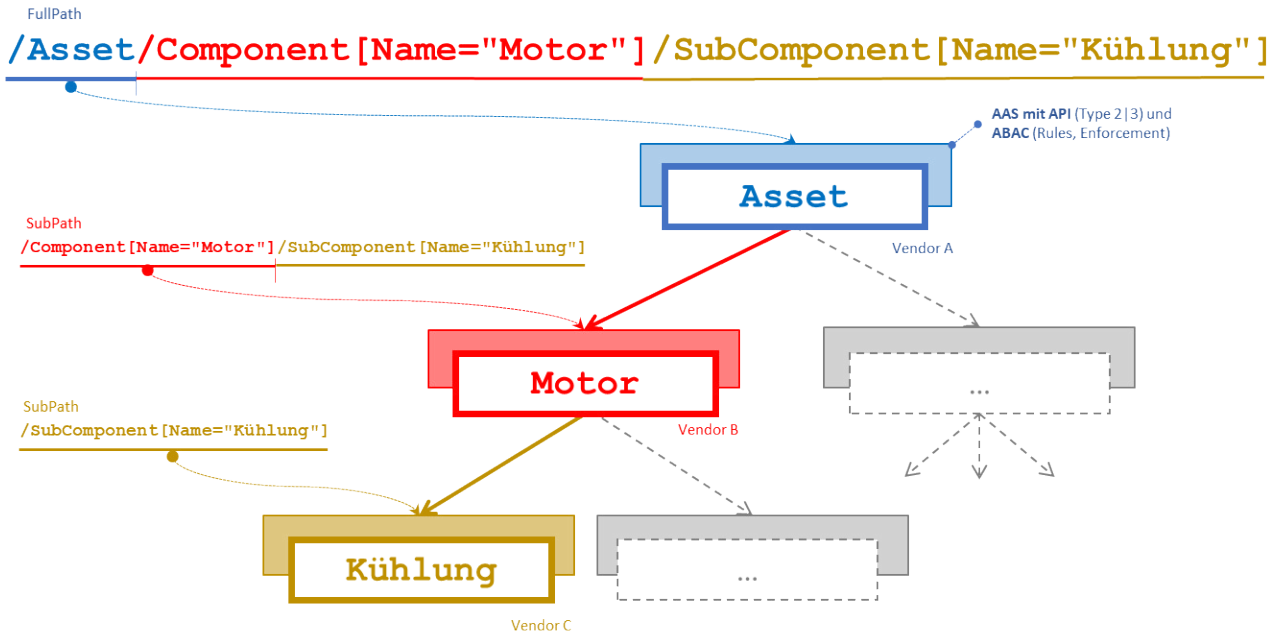
10 Anhang

10.1 Beispiel einer technischen Implementierung einer Zugriffskontrolle mit Hilfe logischer Zugriffspfade

Der in Kapitel 2 beschriebene mögliche Weg mittels logischer Hierarchisierung der AAS-Bestandteile entsprechend dem Eigentum der Bestandteile und entsprechend dem separaten Enforcement (=Prüfung der Regel und Feststellung, ob der Zugriff gewährt wird) der Zugriffskontrolle, die sich dem Einfluss des Besitzers des Assets (Betreiber) ganz oder teilweise entzieht. D.h. das Folgen eines Zugriffspfads ist mit jedem weiteren Schritt auf diesem Pfad jeweils zu enforcen, mit Regeln und Attribut-Anreicherungen, die vom Datenverfügungsberechtigten der Submodelle verwaltet werden.

Eine solche logische Hierarchisierung ist in Abbildung 9 dargestellt. In diesem Fall wird eine logische Hierarchisierung zwischen Asset, Motor (als Komponente des Assets) und Kühlung (als Komponente des Motors) veranschaulicht.

Abbildung 9: Autonome AAS-Knoten über API mittels Pfadbeschreibung



Quelle: Plattform Industrie 4.0

Insbesondere in den Beispielen CCM (0), Gewährleistung (3.2) und nicht öffentliche Verträge (3.3) spielt der Zugriff über logische Pfade eine entscheidende Rolle. Zum einen ist der Betreiber vertraglich verpflichtet, dem Asset-Hersteller bestimmte Zugriffe zu gewähren, zum anderen kennt er die vertraglichen Nebenbedingungen zwischen Asset-Hersteller und Komponentenhersteller nicht. Der Komponentenhersteller einer im Asset verbauten Komponente kann dann genau über diesen vom Betreiber gewährten Eingang zugreifen und über separate Enforcements Zugriff auf seine Komponente erlangen. Dabei kann die Einhaltung des Zugriffspfades geprüft werden, und die Subjekt-Attribute, die im nächsten Enforcement benötigt werden, können entsprechend angereichert werden (z. B. Anreicherung mit einem Verifikations-Token mit nur kurzer Gültigkeitsdauer (um Replay-Angriffe zu verhindern)).

Da **logische Zugriffspfade mit Hilfe von Standard-Mechanismen modelliert** werden können (z. B. eine XML- oder JSON-artige Darstellung), kann eine solche **logische Hierarchie** sehr performant abgefragt werden, wodurch die Beispiele 3.6 und 3.7 realisiert werden können.

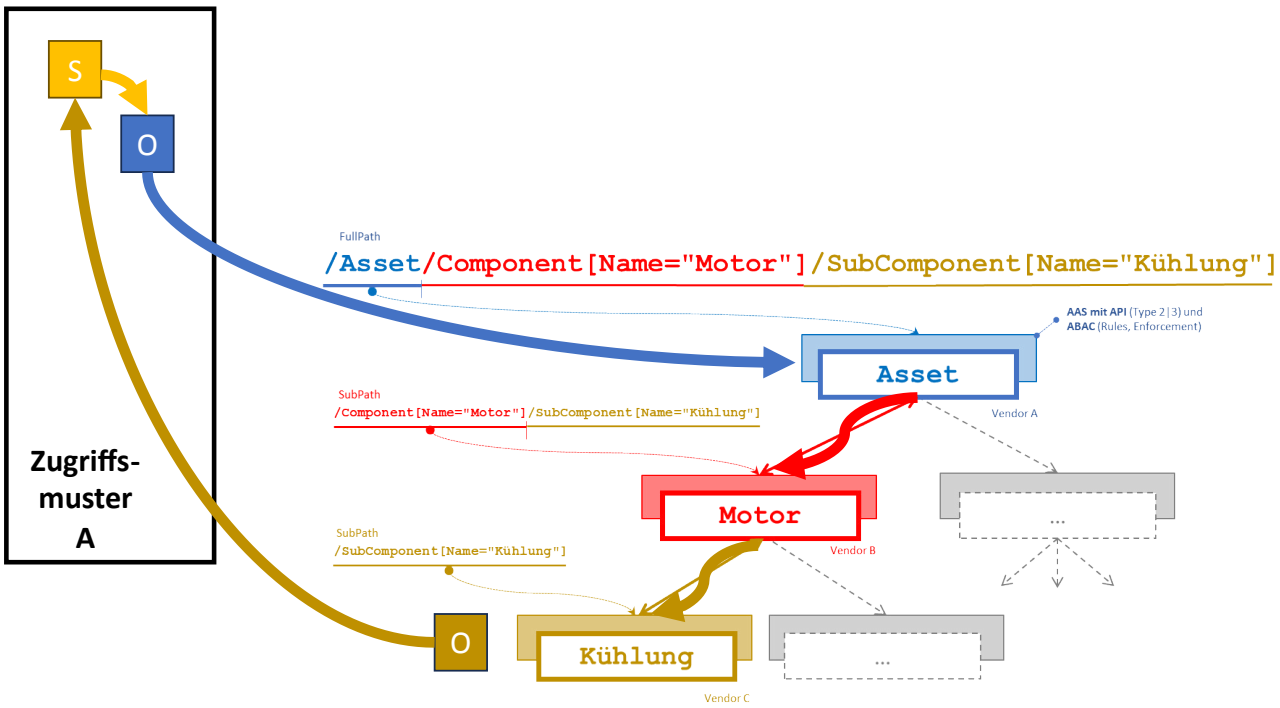
Durch die Erzielung des Komplettüberblicks über die Regelwerke, die hinter den Nutzungsbedingungen stehen, kann das Regelwerk auch hochdynamisch angepasst werden, um neue Gegebenheiten abzubilden (z. B. Austausch des Dienstleisters für einen Teil der Komponenten eines

Komponentenherstellers (3.4)). Da das Modell der logischen Hierarchisierung und logischer Zugriffspfade nicht an eine physikalische Struktur gebunden ist, kann eine solche Prüfung auch auf den jeweiligen digitalen Zwillingen oder in der Edge geschehen (3.5).

Hinweis: Durch jeweils notwendige separate Enforcements entlang des logischen Zugriffspfades entsteht die Notwendigkeit, dass die zugehörigen AAS-Komponenten auch aktive Komponenten beinhalten, d. h. aktive Anteile, die entweder die Nutzungsbedingungen selbst prüfen können (d. h. als „Policy Enforcement Point“ agieren) oder auf eine Prüfungs-Komponente an anderer Stelle verweisen (d. h. als „Policy Decision Point“ agieren).

In Abbildung 10 und Abbildung 11 werden Zugriffe über logische Hierarchien in zwei verschiedenen und funktional äquivalenten Zugriffsmustern abgebildet.

Abbildung 10: Zugriffsmuster A – topologisch dynamisch

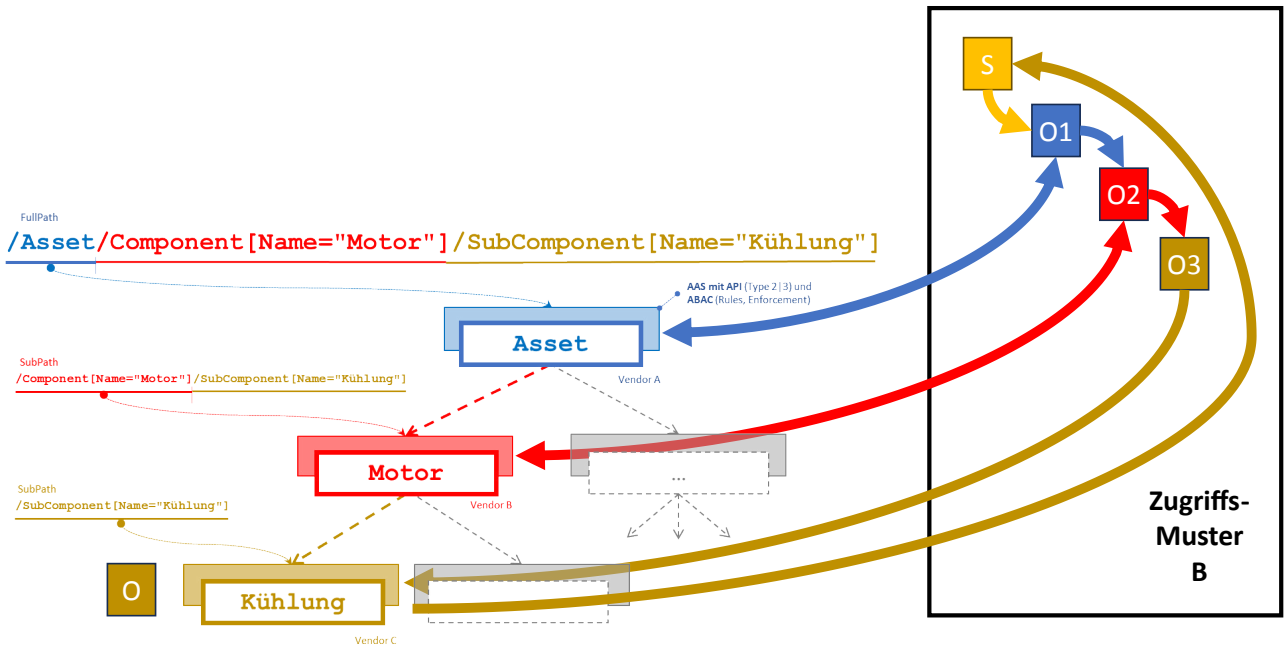


Quelle: Plattform Industrie 4.0

Beim **Zugriffsmuster A** stellt das Subjekt (z. B. der Komponentenhersteller für die Komponente „Kühlung“) über das Asset und die Angabe des logischen Pfads eine einmalige Anfrage an die AAS des Assets für die aktive Komponente. Die AAS des Assets führt in ihrer aktiven Komponente ein Enforcement durch und leitet die Anfrage an die AAS „Kühlung“ über den vorgegebenen Pfad an die aktive Komponente und das Enforcement der AAS „Motor“ weiter.

Dabei erfolgt in diesem Beispiel entsprechend der weiteren Prüfung eine Anreicherung mit einem geheimen (öffentlich unbekannten) Attribut und Wert, der die Legitimation (durch vertragliche Vereinbarung) des Zugriffs nachweist. Gleiches geschieht bei der Übergabe von „Motor“ an „Kühlung“. Die Rückgabe der angeforderten Daten erfolgt bei Regel- und Attributwert-Erfolg direkt an das Subjekt.

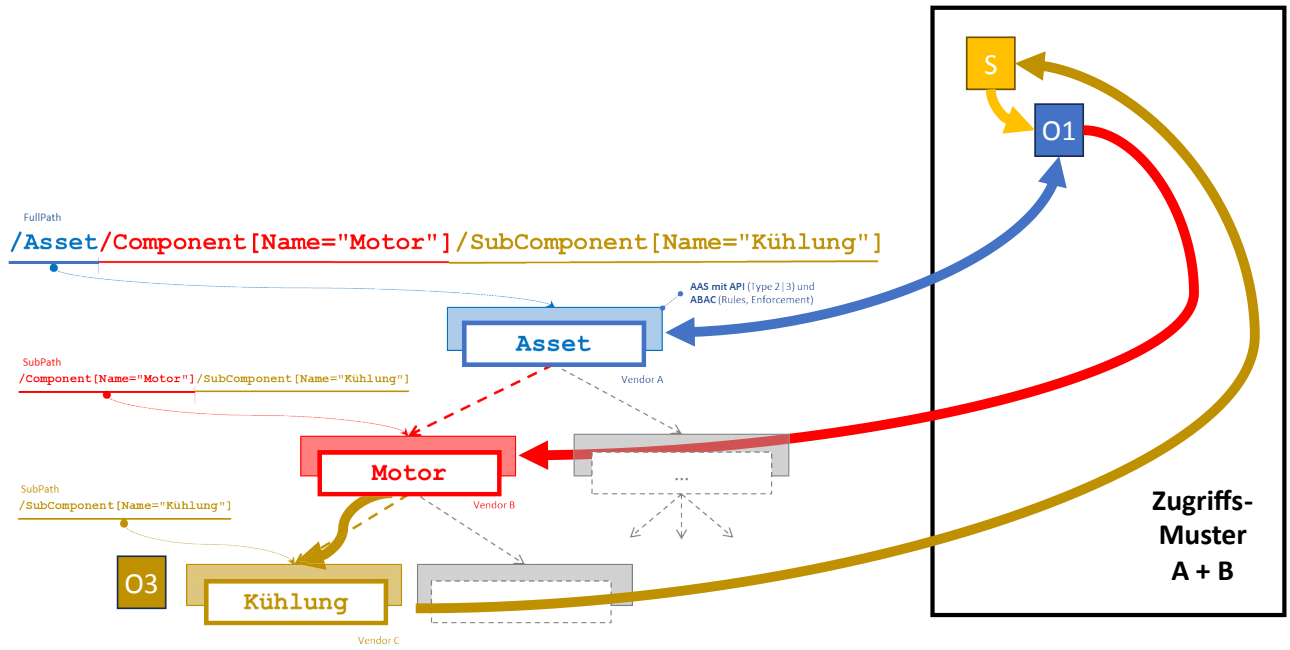
Abbildung 11: Zugriffsmuster B – logisch-hierarchisch



Quelle: Plattform Industrie 4.0

Bei **Zugriffsmuster B** fragt das Subjekt ebenfalls das Asset an, erhält aber einen Verweis auf die im Pfad als Nächstes anzufragende Komponente. Die Prüfung des logischen Pfades sowie die Anreicherung der Attribute mit öffentlich nicht bekannten Attributen/Werten erfolgt bei Zugriffsmuster A in gleicher Weise und die Anreicherung wird vom Subjekt-Prozess (Client) entsprechend an das nächste Enforcement weitergegeben. Entsprechende Anreicherungs-Attribute – wie oben bereits beschrieben – könnten z. B. Verifikationstoken mit nur kurzer Gültigkeitsdauer sein (um z. B. Replay-Attacken zu verhindern bzw. um zu verhindern, dass sich der Zugriffsprozess das Anreicherungs-Attribut mit dem Ziel der Umgehung zukünftiger Regeländerungen merken kann). Auch hier erfolgt die Rückgabe der angeforderten Daten direkt an den Beteiligten bzw. das Subjekt, wenn die Regel und der Attributwert erfolgreich sind.

Abbildung 12: Zugriffsmuster A und B



Quelle: Plattform Industrie 4.0

In beiden Zugriffsmustern ist die Topologie der logischen Hierarchisierung nicht statisch festgelegt, sondern kann hochdynamisch in Abhängigkeit vom Subjekt und den Anfrageumständen variieren.

Bei **Zugriffmuster A + B** (s. Abbildung 12) sind beide Methoden angewendet worden, um auch zu zeigen, dass Zugriffsmuster A und B innerhalb einer Anfrage grundsätzlich auch beliebig mischbar sind.

In Abbildung 3, Abbildung 4 und Abbildung 5 erfolgt eine Übertragung der obigen Überlegungen auf bisher diskutierte Abbildungen der AAS. In vielen Fällen wird die AAS als flache, nicht logisch- und nicht physikalisch-hierarchisierte Datenablage wahrgenommen und der Zugriff erfolgt auf jedes AAS-Submodell direkt. Im Falle des Enforcements beim Zugriff auf ein „Public Submodel“ (grün) gibt die Regel (wie im Falle des DPP-Beispiels 3.7) immer „true“ zurück. Im Falle des Enforcements auf ein „Restricted Submodel“ gibt es eine „statische“ Regel, die immer nur unter speziellen, fixen Bedingungen „true“ zurückgibt, ansonsten „false“.

In Abbildung 4 erhöht sich nun die Dynamik der Regeln aufgrund der Erfüllung von Nutzungsbedingungen (z. B.: Das Asset wurde vom Betreiber in Besitz genommen, es gelten nunmehr vertraglich zugesicherte Nutzungsbedingungen/Nutzungsrechte für Betreiber, Asset-Hersteller und Komponentenhersteller). Der Zugriff auf die entsprechenden AAS-Submodelle ist entsprechend den Abbildungsregeln für die Nutzungsbedingungen dynamisch zu ermitteln, d. h. die Nutzungsregeln sind nicht von vornherein im Submodell verankert.

In Abbildung 5 wird schließlich der Zugriff über logische Zugriffspfade gezeigt, um die nicht öffentlich bekannten Verträge einhalten zu können und (durch Attribut-Anreicherung und Einhaltung des Pfades) die entsprechende Legitimierung zu beweisen.

10.2 Zusätzliche Vorteile der diskutierten Ansätze

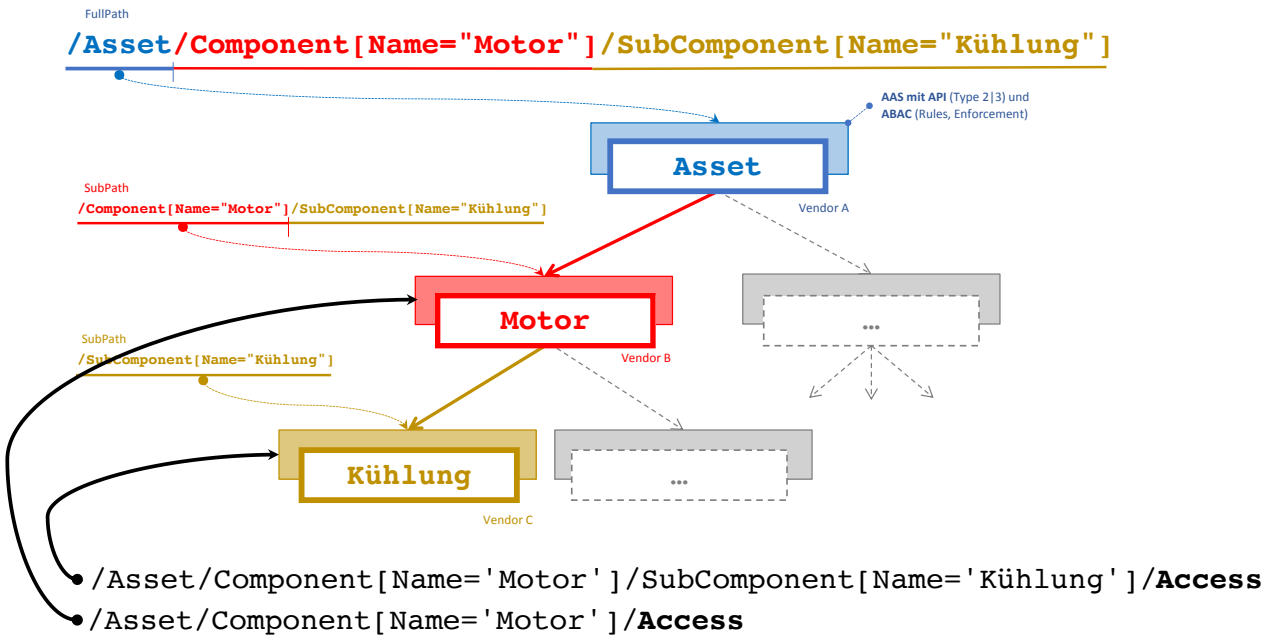
Der oben diskutierte Ansatz hat neben dem hauptsächlichen Nutzen, die genannten (und andere) Problemstellungen zu lösen, noch einige weitere Vorteile:

- Die Gesamt-Topologie einer gesamten Fabrik kann aufgezeigt werden (z. B. vom Betreiber angefragt)
- Die Teil-Topologie der Komponenten eines Komponentenherstellers kann aufgezeigt werden (z. B. vom Komponentenhersteller für seine Komponenten angefragt). Es können bei der Gesamtanfrage sowohl die Lokationen als auch wichtige Daten der Komponenten mit angefragt werden (z. B. Datum der letzten Inspektion, Anzahl der Betriebsstunden, ...)
- Siehe hierzu Abbildung 13 und Abbildung 14

In Abbildung 13 wird z. B. über die Gesamt-Topologie des Betreibers abgefragt, welche Zugriffsregeln für jedes verzeichnete Submodell gelten. Dies wird (zum Beispiel als XPath-Abfrage) über den Abfrageparameter „//Access“ erreicht. Sollten Regeln nicht vorhanden/gepflegt sein, gibt die Abfrage entsprechende Fehlermeldungen zurück, so dass mit der Abfrage auch gleich eine **Konsistenzprüfung** der Zugriffsregeln erfolgt. Die **Bereitstellung der Zugriffsregeln in ihrer Gesamtheit obliegt hierbei nicht einem Verantwortlichen allein** (s. Beispiele 3.1, 3.2, 3.3), sondern hängt, wie bereits beschrieben, teilweise von nicht öffentlich bekannten Verträgen ab.

Die entsprechenden Anfrageergebnisse werden erst durch logische Hierarchisierung interpretierbar, wenn man sich eine Betreiber-AAS aller Assets eines Unternehmens mit vielen tausenden AASen und noch viel mehr Submodellen vorstellt.

Abbildung 13: Zugriffsschutz von AAS-Knoten mittels Pfad-Definitionen für ABAC Access Rights

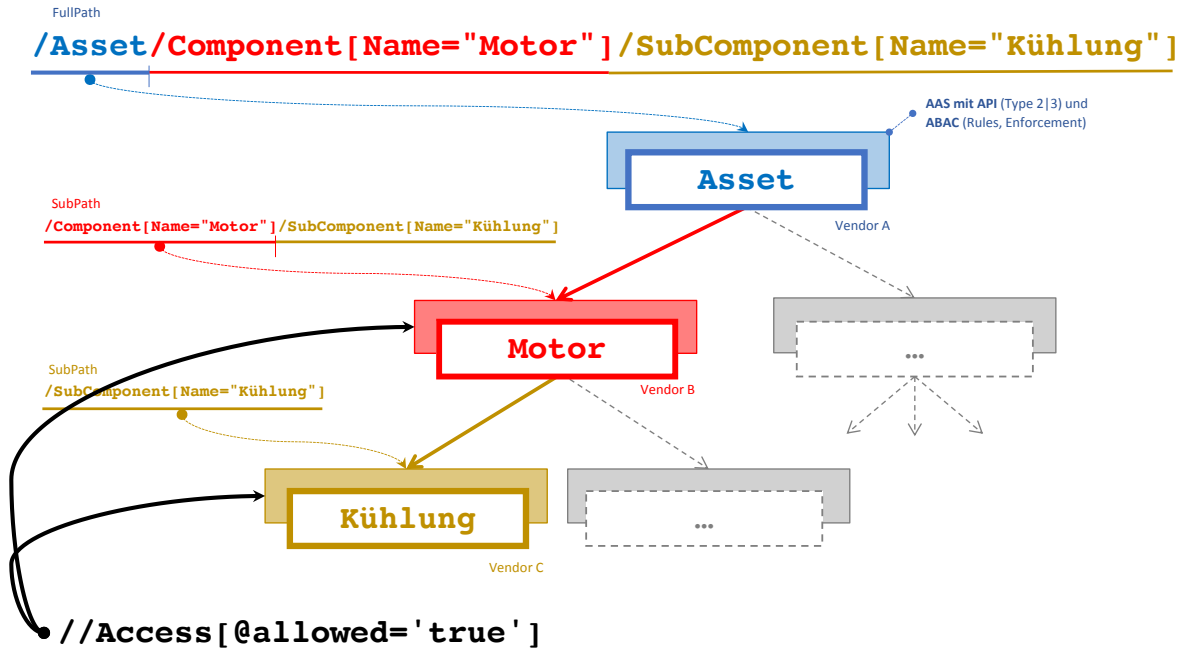


Quelle: Plattform Industrie 4.0

In Abbildung 14 erfolgt, wie im Beispiel zu DPP (3.7), eine einfache Beispiel-Abfrage auf Submodelle der gesamten Topologie der Fima, bei denen der Zugriff generell erlaubt ist (Parameter-Abfrage des Attributs „//Access“, z. B. mit dem Wert „@allowed='true'“).

In einem weiteren Dokument werden die Einzelheiten zu dieser Methodik und die Integration in die ASS erläutert.

Abbildung 14: Query: Knotenauswahl mit erlaubtem Zugriff



Quelle: Plattform Industrie 4.0

AUTORINNEN UND AUTOREN

Vanessa Bellinghausen (Bundesamt für Sicherheit in der Informationstechnik) | Björn Flubacher (Bundesamt für Sicherheit in der Informationstechnik) | Michael Jochem (Robert Bosch GmbH) | Dr. Michael Schmitt (SAP SE) | Thomas Walloschke (Leitung, secon trust consult)

Diese Publikation ist ein Ergebnis der Unterarbeitsgruppe „Zugriffssteuerung“ der Arbeitsgruppe „Sicherheit vernetzter Systeme“ der Plattform Industrie 4.0.

www.plattform-i40.de