PLATTFORM INDUSTRIE 4.0

DISKUSSIONSPAPIER

Security der Verwaltungsschale

In Zusammenarbeit mit

ZVEI: Die Elektroindustrie

entstanden.

Impressum

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

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

Gestaltung und Produktion
PRpetuum GmbH, München

Stand
April 2017

Druck
MKL Druck GmbH & Co. KG, Ostbevern

Bildnachweis
Jamrooferpix – Fotolia (Titel),
arrow – Fotolia (S. 3)

Zertifikat seit 2002
audit berufundfamilie

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

FSC
www.fsc.org
MIX
Papier aus verantwortungsvollen Quellen
FSC® C108626

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

Zentraler Bestellservice:
Telefon: 030 182722721
Bestellfax: 030 18102722721

Inhalt

1. Zielsetzung und Methodologie

Dieses Dokument bündelt die technischen Diskussionen der Spiegelgruppe Sicherheit des ZVEI hinsichtlich der Security-Anforderungen und Umsetzungsmöglichkeiten der Verwaltungsschale der Industrie 4.0-(I4.0)Komponente. Die Spiegelgruppe ist Bestandteil des Führungskreises Industrie 4.0 im ZVEI. Sie übernimmt dort alle Aspekte zur Industrie 4.0-Security und unterstützt die Arbeiten der AG 3 Sicherheit vernetzter Systeme der Plattform Industrie 4.0.

Zielsetzung des Dokuments ist, ein gemeinsames Verständnis zum Thema Security der Verwaltungsschale zu entwickeln und dieses als Diskussionsgrundlage und Orientierungshilfe für andere Arbeitsgruppen im Bereich Industrie 4.0 beizusteuern.

Hauptaugenmerk des Dokuments liegt auf der Fragestellung, welche Merkmale, Daten und Funktionen generell in einer Verwaltungsschale abgelegt werden sollen und wie diese sicher verwendet werden können. Die Ausführungen sollen es anderen Beteiligten, etwa der Gesellschaft Mess- und Automatisierungstechnik, Fachauschuss 7.21 (GMA FA 7.21) des VDI/VDE, erlauben, Vorschläge zu IT-Strukturen, IT-Diensten und inhaltlichen Teilmodellen zu machen. Es ist kein Ziel, eine abschließende Spezifikation oder eine abschließende inhaltliche Vorgabe für die Implementierung eines einzelnen Geräts oder Systems zu leisten. Vielmehr soll belastbar eine Richtung aufgezeigt werden, in welche sich die inhaltliche Diskussion und Standardisierung bezüglich der Sicherheit einer I4.0-Komponente in den nächsten Monaten bewegen wird.

Die Ausführungen dieses Dokuments richten sich gleichermaßen an die Industrien der Fabrik- wie auch der Prozessautomatisierung. Begriffe wie „Fabrik“, „Fertigung“ und „Shopfloor“ meinen damit auch die Einrichtungen der prozesstechnischen Industrie.

Dieses Dokument entwickelt die Sicherheitsanforderungen und mögliche Lösungen anhand eines praktischen Use-Case/Anwendungsbeispiels. Es liegt in der Natur dieses Vorgehens, dass nicht alle Aspekte einer Verwaltungsschale in diesem Use-Case berücksichtigt werden können. Daher haben das verwendete Beispiel sowie die sich daraus ableitenden Diskussionen keinen einschränkenden Charakter. Im Speziellen soll weder die Funktionalität noch die Sicherheit der Verwaltungsschale auf die beispielhaft diskutierten Bestandteile reduziert werden. Der Use-Case ist bewusst einfach gewählt, um die Diskussion auf wesentliche Aspekte der Verwaltungsschale anhand eines leicht verständlichen Beispiels zu fokussieren. Insbesondere beschränkt er sich auf die Lebenszyklusphasen „Inbetriebnahme“ und „Produktion“ aus Sicht eines Integrators und eines Betreibers einer Maschine. Aspekte der Sicherheit weiterer Lebenszyklusphasen der Verwaltungsschalen können in späteren Dokumenten oder Dokumentversionen betrachtet werden.

Zukünftige Dokumente zum Thema Sicherheit und Verwaltungsschale können komplexere und umfassendere Use-Cases und Betrachtungen enthalten, die ein vollständigeres Bild des Umfangs der Verwaltungsschale und ihrer Sicherheitsanforderungen ergeben.

2. Relevante Inhalte aus verschiedenen Quellen

Dieser Abschnitt zeigt wichtige Inhalte aus vorangegangenen Diskussionen oder aus anderen Arbeitskreisen auf. Er soll damit die Vernetzung zu anderen Themen aufzeigen.

2.1 Security für das „Referenzarchitekturmodell Industrie 4.0“ (RAMI4.0)

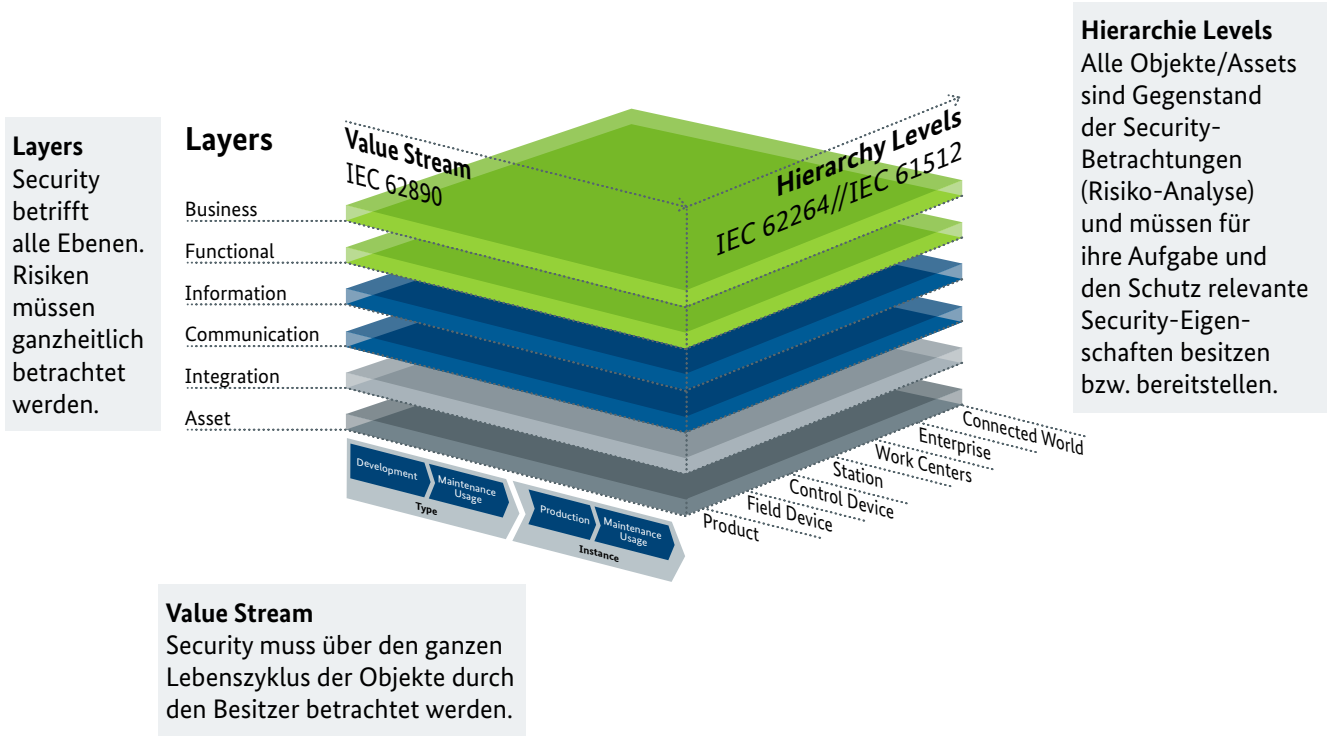
Das Referenzarchitekturmodell Industrie 4.0 (RAMI4.0) führt die wesentlichen Elemente von Industrie 4.0 in einem dreidimensionalen Schichtenmodell zusammen. Anhand dieses Gerüsts kann Industrie 4.0-Technologie systematisch eingeordnet und weiterentwickelt werden.[1] Es besteht aus einem dreidimensionalen Koordinatensystem, das die wesentlichen Aspekte von Industrie 4.0 beinhaltet. Komplexe Zusammenhänge können so in kleinere, überschaubare Pakete aufgegliedert werden. Die nachstehende Abbildung zeigt die Einbettung der Security im RAMI4.0[2] in allen drei Achsen und verdeutlicht den integralen Charakter der Security.

Die Security 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.

An allen Schnittpunkten der verschiedenen Ebenen spielt Security eine Rolle. Das heißt, dass sich für jeden Punkt zunächst Anforderungen (Requirements) aus der Analyse ergeben, die auf Basis des konkreten Anwendungsfalls mit entsprechenden Funktionalitäten (Capabilities) seitens der involvierten Industrie 4.0-Komponenten zu beantworten sind. Betreiber, Hersteller und Kunden sind gemeinsam gefordert. Das Design von Security in RAMI4.0 ermöglicht die Umsetzung jeglicher Security-Anforderung für alle denkbaren Anwendungsfälle.

Das Modell ermöglicht die Einbeziehung bereits existierender Security-Standards, insbesondere VDI 2182 und IEC 62443.

Abbildung 1: Security in RAMI4.0



Quelle: ZVEI SG Modelle und Standards

1 www.zvei.org/Downloads/Automation/ZVEI-Faktenblatt-Industrie4_0-RAMI-4_0.pdf

2 www.plattform-i40.de/I40/Redaktion/DE/Downloads/Publikation/security-rami40.pdf?__blob=publicationFile&v=7

In der VDI 2182 wird z. B. die Rückkopplung der Anforderungen von den verschiedenen Prozessbeteiligten bereits adressiert. Dort wird die Kommunikation zwischen Betreiber, Integrator bzw. Maschinenbauer und Komponentenhersteller als wesentlicher Bestandteil für Security beschrieben, sodass die jeweiligen Anforderungen weitergegeben und umgesetzt werden können. IEC 62443 skizziert ein Referenzmodell für industrielle Kommunikationsnetze und zeigt auf, wie auf dieser Basis Sicherheitsanforderungen erhoben und Sicherheitstechnologien identifiziert werden können.

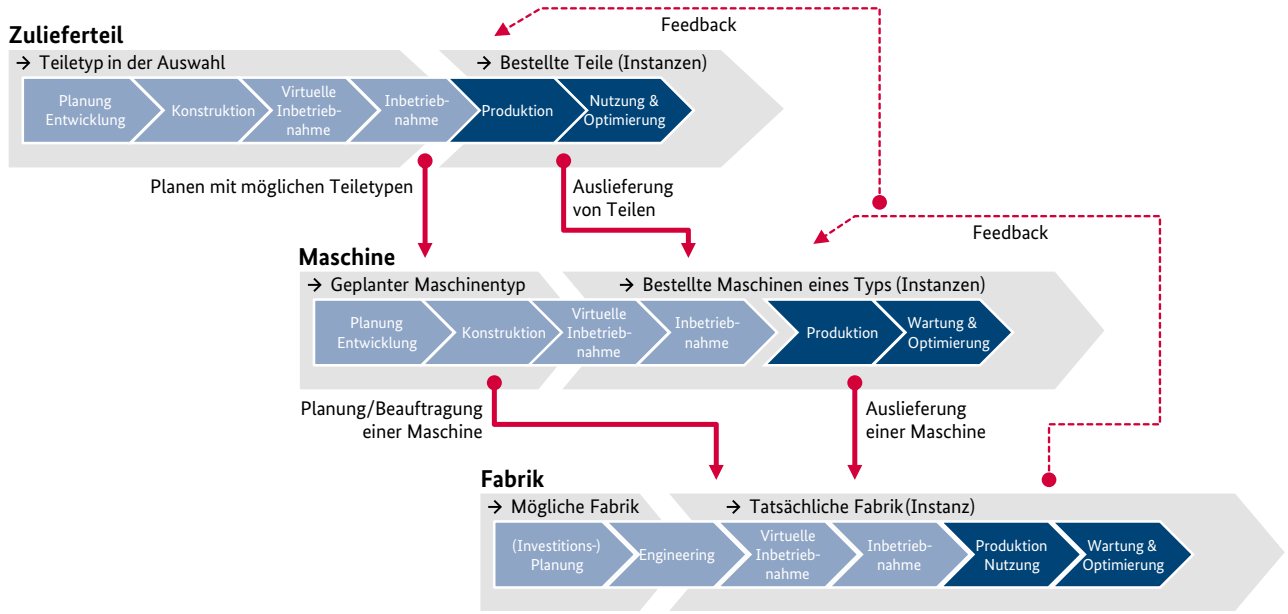
2.2 Industrie 4.0-Komponente in der Umsetzung; Stand 2015

Die I4.0-Komponente wurde in der „Umsetzungsstrategie Industrie 4.0“[3] der Plattform im April 2015 vorgestellt. Kernpunkte dieser Vorstellung waren:

- der Aufbau auf die Definitionen der GMA FA 7.21
- die Eignung der I4.0-Komponente für verschiedenste Lebenszyklen bei den unterschiedlichen Partnern eines Wertschöpfungsnetzwerks (siehe Bild unten)
- die Möglichkeit, die I4.0-Komponente im RAMI4.0 zu verorten (z. B. auf der Entwicklungsseite und der Produktions-/Nutzungsseite sowie auf verschiedensten Hierarchie-Ebenen)
- die Möglichkeit, die I4.0-konforme Kommunikation sowohl für aktiv als auch passiv angebundene Gegenstände gleichwertig zu betreiben

Die Definition der Verwaltungsschale mit virtueller Repräsentation und fachlicher Funktionalität war auch ein zentraler Bestandteil dieser Vorstellung. Die Verwaltungsschale kann sich auf einen oder mehrere Gegenstände beziehen. Als ein wichtiger Teil der virtuellen Repräsentation wurde das „Manifest“ erwähnt, das als Verzeichnis der einzelnen Dateninhalte dieser Repräsentation angesehen werden kann. Damit enthält es auch sogenannte Meta-Informationen. Es beinhaltet außerdem verpflichtende Angaben zur I4.0-Komponente, unter anderem zu Verbindungen mit

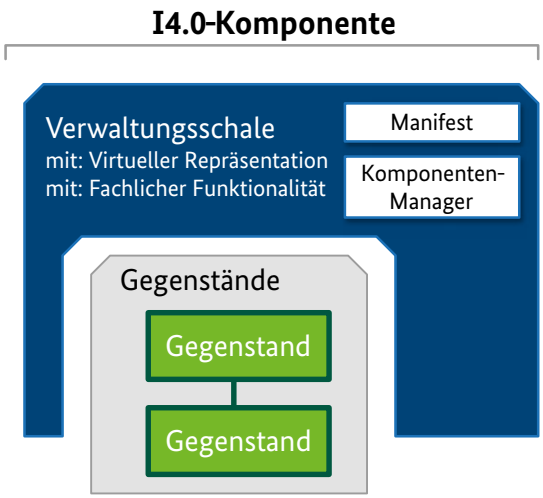
Abbildung 2: Typen und Instanzen im Lebenszyklus



Quelle: ZVEI SG Modelle und Standards

3 www.zvei.org/Verband/Publikationen/Seiten/Umsetzungsstrategie-Industrie-40.aspx

Abbildung 3: Struktur I4.0-Komponente



Quelle: ZVEI SG Modelle und Standards

weiteren Gegenständen sowie ihrer Identifikationsmöglichkeit und Angaben zur Security. Die Security-Fähigkeiten eines Gegenstands müssen konform zu den geforderten Security-Fähigkeiten der Verwaltungsschale sein. Der Komponenten-Manager stellt die Verbindung zu den IT-technischen Diensten der I4.0-Komponente dar, mit denen von außen auf die virtuelle Repräsentation und fachliche Funktionalität zugegriffen werden kann. Der Komponenten-Manager[4] kann also z. B. eine serviceorientierte Architektur (SOA) anbinden oder die Verwaltungsschale in ein Repository abbilden.

Die Struktur der Verwaltungsschale der Industrie 4.0-Komponente ist in einem Ergebnispapier[5] dokumentiert worden und wird in Abschnitt 3.1 mit Hinblick auf die für die Security-Arbeiten relevanten Inhalte detaillierter vorgestellt.

2.3 Ausführliche Anwendungsszenarien

Die Struktur der Verwaltungsschale soll geeignet sein, die entsprechenden Anwendungsfälle der Industrie 4.0 in geeigneter Weise zu unterstützen. Notwendige Daten, Funktionen und mögliche Security-Anforderungen müssen identifiziert werden, unnötiger Mehraufwand an Definitionen sollte vermieden werden. Einen Überblick über mögliche Anwendungsfälle liefert die Online-Landkarte[6] der Plattform Industrie 4.0. Anwendungsszenarien[7] wurden von der Arbeitsgruppe 2 der Plattform Industrie 4.0 zusammengestellt. Beispielhaft seien hier die Anwendungsszenarien „Auftragsgesteuerte Produktion“ oder „Wandlungsfähige Fabrik“ genannt, die aus unterschiedlichen Sichten die zu erwartenden Möglichkeiten und Vorteile der Industrie 4.0 darstellen. Das Anwendungsszenario „Auftragsgesteuerte Produktion“ fokussiert beispielsweise auf die Sicht des Auftrags durch die Wertschöpfungskette, wohingegen „Wandlungsfähige Fabrik“ die Sicht der Produktionsressourcen einnimmt, die sich als modulare und intelligente Module mit standardisierten Schnittstellen weitgehend selbstständig an veränderte Umstände anpassen. In diesem Umfeld positioniert sich auch der in Abschnitt 3.2 beschriebene einfache Use-Case, der dem vorliegenden Papier als Basis für die Analyse der Security-Anforderungen dient.

4 In den bisherigen Dokumenten wird der Komponenten-Manager als Ressourcen-Managern bezeichnet; dieser soll in Zukunft aber als Komponenten-Manager bezeichnet werden.

5 www.plattform-i40.de/I40/Redaktion/DE/Downloads/Publikation/struktur-der-verwaltungsschale.pdf?__blob=publicationFile&v=8

6 www.plattform-i40.de/I40/Landkarte

7 www.plattform-i40.de/I40/Redaktion/DE/Downloads/Publikation/anwendungsszenarien-auf-forschungsroadmap.html

3. Security der Verwaltungsschale

In diesem Abschnitt soll ein erstes Konzept für die Security der Verwaltungsschale entworfen werden, das den Anforderungen von Industrie 4.0 im Allgemeinen und den bereits formulierten Definitionen der verschiedenen Arbeitskreise gerecht wird. Der Entwurf baut auf etablierte Konzepte sowohl in den Automatisierungs- als auch in den IT-Technologien auf und soll für zukünftige Entwicklungen bezüglich der relevanten I4.0-Aspekte (horizontale Integration, vertikale Integration, durchgängiges Engineering und Interaktion mit dem Menschen) gewappnet sein.

In Abschnitt 3.1 werden die Aspekte der Verwaltungsschale eingeführt, welche für die weitere Erarbeitung der Security der Verwaltungsschale relevant sind.

Um entsprechende Security-Anforderungen an die Verwaltungsschale sowie, darauf aufbauend, Security-Konzepte für die Verwaltungsschale abzuleiten, wird in Abschnitt 3.2 ein erster, einfacher Use-Case „Engineering“ definiert. Aus den detailliert dargestellten Abläufen werden für die einzelnen Schritte Security-Aspekte identifiziert und daraus dann die Anforderungen an die Security der Verwaltungsschale hergeleitet. Abschließend werden in Abschnitt 3.3 die Anforderungen weiter analysiert und Empfehlungen formuliert. Zudem werden im Verlauf der Analyse offene Punkte identifiziert und zur weiteren Diskussion in den entsprechenden Gremien klar benannt.

3.1 Struktur der Verwaltungsschale als Ausgangsbasis

Der vorliegende Entwurf der Verwaltungsschale unterscheidet, wie ein „DF Asset“ der Digitalen Fabrik, zwischen „Header“ und „Body“. Im „**Header**“ sorgt eine Liste von Merkmalen für eine Identifikation und Bezeichnung der konkreten Gegenstände und der Verwaltungsschale im jeweiligen Kontext und verweist auf die Fähigkeiten der Gegenstände und Sichten.

Die Angaben des Headers (inklusive der Identifikation von Verwaltungsschale und Gegenständen) sind als Merkmale im Sinne von Anforderung (s) im Kapitel 3.4 der Publikation „Struktur der Verwaltungsschale“ abzusichern.

Im **Body** findet sich der **Komponenten-/Ressourcen-Manager**[8], der einzelne **Teilmodelle** innerhalb der Verwaltungsschale verwaltet. Jedes Teilmodell verfügt über hierarchisch organisierte **Merkmale**, die auf individuelle **Daten und Funktionen** (weiße geometrische Elemente) referenzieren. Nicht dargestellt, aber möglich, sind das gegenseitige Referenzieren und das Bilden von Sichten.

Die Gesamtheit der Merkmale aller Teilmodelle bildet somit das **Manifest** der Verwaltungsschale, das damit als eindeutig aufzufindendes Inhaltsverzeichnis aller Daten und Funktionen dienen kann. Auf diese Weise wird es möglich, dass die jeweiligen Merkmalsstrukturen in einem strengen, **einheitlichen Format** (aufbauend auf IEC 61360, Kapitel 2.7.1 „Struktur der Verwaltungsschale“) vorliegen, während für die unterschiedlichen Daten und Funktionen unterschiedliche, sich ergänzende **Datenformate und Zugriffsmethoden** möglich sind.

Nach außen hin kann die Verwaltungsschale gegebenenfalls **Laufzeitdaten** (vom Gegenstand) aufnehmen und abbilden, z. B. die Istposition und Istströme bei einem Servoverstärker. Die Informationsmengen sollen nach außen mittels Sichten dargestellt werden können (Kapitel 4.1 „Struktur der Verwaltungsschale“). Ein I4.0-konformes, serviceorientiertes **API** (application programmers interface) soll die **Dienste** des Komponenten-Managers nach außen zur Verfügung stellen. Teil dieser Dienste ist die lebenslange **Pflege der Merkmale, Daten und Funktionen** innerhalb der Verwaltungsschale, die **Adressierung und Identifikation von Verwaltungsschalen und Gegenständen** (Kapitel 3.2 (h), (i) „Struktur der Verwaltungsschale“) und eine **leistungsfähige Suche** nach Merkmalen und referenzierten Daten und Funktionen.

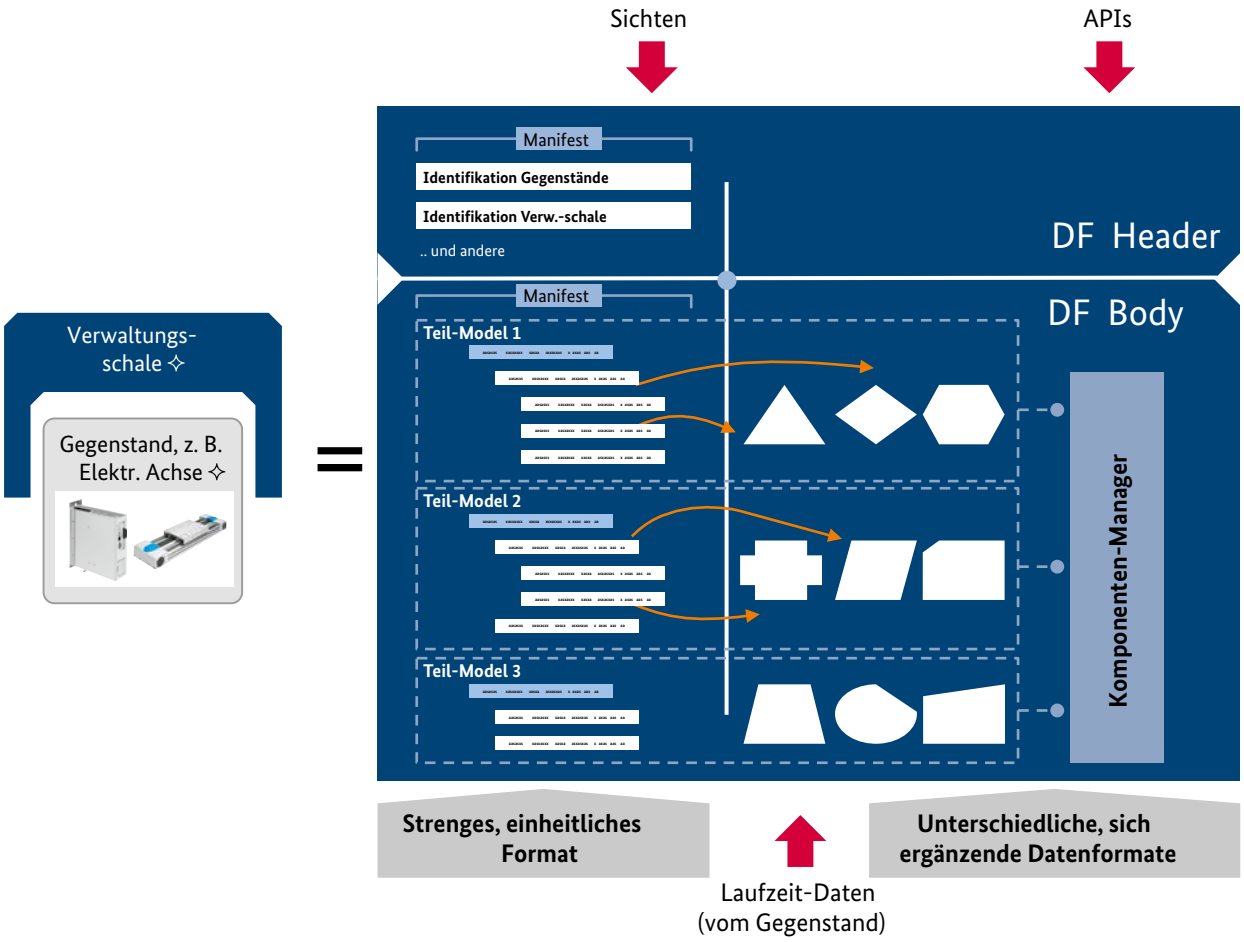
Für die Ausprägung von Verwaltungsschalen ist es relevant, für welche Gegenstände[9] sie konzipiert sind:

- So kann auch eine bereitgestellte **Software** ein wichtiges Asset eines Produktionssystems und damit einen Gegenstand darstellen.

8 Wie in Abschnitt 1.2 bereits erwähnt, wird heute der Begriff **Komponenten-Manager** anstelle von Ressourcen-Manager bevorzugt verwendet

9 Siehe erste Version der Industrie 4.0-Komponente in der „Umsetzungsstrategie Industrie 4.0“ der Plattform vom April 2014

Abbildung 4: Mögliche Header-/Body-Struktur



Quelle: ZVEI SG Modelle und Standards

- Ein **Gegenstand kann mehrere Verwaltungsschalen** haben, die für unterschiedliche Referenzrahmen, also RAMI-Modelle, relevant sind. So kann beispielsweise der Hersteller eines Servoverstärkers für seine internen Zwecke eine Verwaltungsschale unter „Type/Development“ (Kapitel 3.1 „Struktur der Verwaltungsschale“) vorhalten und dort seine internen Entwicklungsdaten ablegen. Für die Zwecke seiner Kunden kann dieser beispielhafte Hersteller eine externe Verwaltungsschale der Baureihe unter „Type/Usage“ bereitstellen. Und letztendlich kann beispielsweise für jede ausgelieferte Instanz der jeweilige Verwender eine Verwaltungsschale unter „Instance/Usage“ ableiten und weiterpflegen.

Anforderung: Verschiedene Verwaltungsschalen zu einem Gegenstand müssen sich aufeinander beziehen können. Im Besonderen sollen Anteile einer Verwaltungsschale die Rolle einer „Kopie“ der entsprechenden Anteile aus einer anderen Verwaltungsschale spielen können.

- **Ein oder mehrere Gegenstände können in einer Verwaltungsschale** abgebildet werden, beispielsweise wenn mechanische Teile wie Achse, Motor, Servoverstärker und weitere Gegenstände eine „kapselfähige“ I4.0-Komponente bilden.[10]

10 Siehe ebenfalls die „Umsetzungsstrategie Industrie 4.0“ der Plattform im April 2015, Abschnitt „Kapselfähigkeit“

Abbildung 5: Industrie 4.0-Komponente, bestehend aus mehreren Gegenständen

Quelle: ZVEI SG Modelle und Standards

Das obige Beispiel motiviert eine Situation, bei der die Verwaltungsschalen mehrerer Einzelgegenstände, die beispielsweise ein Hersteller einzeln in Verkehr bringt, in eine Verwaltungsschale zusammengefasst werden, wenn dieser beispielhafte Hersteller auch ein ganzes Achssystem verkauft. Daher gilt, auch mit den Vorgaben der Digitalen Fabrik (Kapitel 2.4 „Struktur der Verwaltungsschale“[11]):

Anforderung: Einzelne Verwaltungsschalen sollen sich zu einer gesamthaften Verwaltungsschale zusammenfassen lassen.

11 www.plattform-i40.de/I40/Redaktion/DE/Downloads/Publikation/struktur-der-verwaltungsschale.pdf?__blob=publicationFile&v=8

3.2 Use-Case „Engineering“

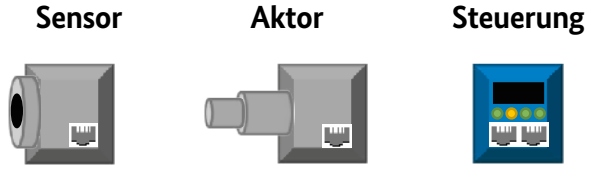
Security-Eigenschaften und -Anforderungen lassen sich nicht abstrakt und generisch formulieren, ohne grundlegende Annahmen über ein System zu machen. Zum besseren Verständnis des Gesamtkontexts „Verwaltungsschale“ und der entsprechenden Security-Anforderungen werden im Folgenden ein erster, einfacher Use-Case „Engineering: Inbetriebnahme von Sensor, Aktor, Steuerung innerhalb einer Fabrik eines Betreibers“ und seine Prozessschritte beispielhaft definiert.

Ziel des Use-Cases ist, anhand eines Minimalbeispiels zur Interaktion von Gegenständen und ihren Verwaltungsschalen – also anhand der Interaktion von I4.0-Komponenten[12] – Anforderungen für die Security der Verwaltungsschale zu sammeln. Das Minimalbeispiel kann später schrittweise ausgebaut werden, z. B. um den Herstellungsprozess der Komponenten, herstellerübergreifende Wertschöpfungsnetzwerke oder eine Cloud-Anbindung. Fast alle der beschriebenen Schritte können entweder automatisch oder manuell durchgeführt werden. Im Folgenden wird beschrieben, wie eine manuelle Durchführung geschehen würde. Dies beschränkt nicht die Möglichkeit, genau diese Schritte durch ein Managementsystem oder ein verteiltes Programm ausführen zu lassen.

3.2.1 Annahmen

Der Use-Case fokussiert dabei auf die Inbetriebnahme von drei Komponenten, die von unterschiedlichen Herstellern geliefert wurden und bereits beim Betreiber eingetroffen sind: Sensor, Aktor und Steuerung (s. Abb. 6). Der Betreiber will die Komponenten nun miteinander verbinden und im Sinne einer vereinfachten Anlage in Betrieb nehmen. Die Komponenten sind dabei räumlich zusammenhängend, das heißt, sie werden innerhalb einer Fabrik genutzt. Zudem werden die Komponenten innerhalb einer gemeinsamen Sicherheitsdomäne eingesetzt sowie durch den Administrator bzw. Integrator in Betrieb genommen und konfiguriert.

Abbildung 6: Komponenten des Use-Cases „Engineering“



Quelle: ZVEI SG Modelle und Standards

Bezüglich der Verwaltungsschalen der Komponenten wurden die folgenden, teilweise vereinfachenden Annahmen getroffen, welche die Allgemeingültigkeit des Beispiels aber nicht einschränken:

- Es wird im Beispiel genau eine Verwaltungsschale (VWS) pro Komponente betrachtet; es kann allerdings unterschiedliche Sichten auf die VWS geben.
- Jede Komponente stellt ihre eigene Verwaltungsschale jeweils direkt zur Verfügung, das heißt, es ist keine Kommunikation mit entfernten Repositories/Clouds erforderlich.[13]

Um möglichst viele Security-Aspekte identifizieren zu können, wurde als fiktives Ergebnis der initialen Risikobewertung die Notwendigkeit eines vergleichsweise hohen Security-Niveaus angenommen:

- Dem Betreiber ist die Integrität der Daten und Komponenten wichtig.
- Dem Betreiber ist die Vertraulichkeit der Kommunikation und des Zugriffs wichtig.
- Der Prozess, in dem die Komponenten genutzt werden, ist echtzeitkritisch und erfordert eine hohe Verfügbarkeit.
- Das Kommunikationsnetzwerk ist nicht derart abgesichert, dass keine weiteren Sicherungsmaßnahmen mehr ergriffen werden müssen, das heißt, es muss damit gerechnet werden, dass potenzielle Angreifer Zugang zum Netzwerk haben.

12 Im Folgenden zur Vereinfachung nur noch Komponente genannt.

13 Diese Einschränkung wurde zur Begrenzung der Komplexität des Beispiels gewählt und sollte später um ein Beispiel erweitert werden, in dem einzelne Geräte nicht die Verwaltungsschale selbst bereitstellen oder eine dynamische Vorgehensweise gewählt wird.

3.2.2 Prozessschritte

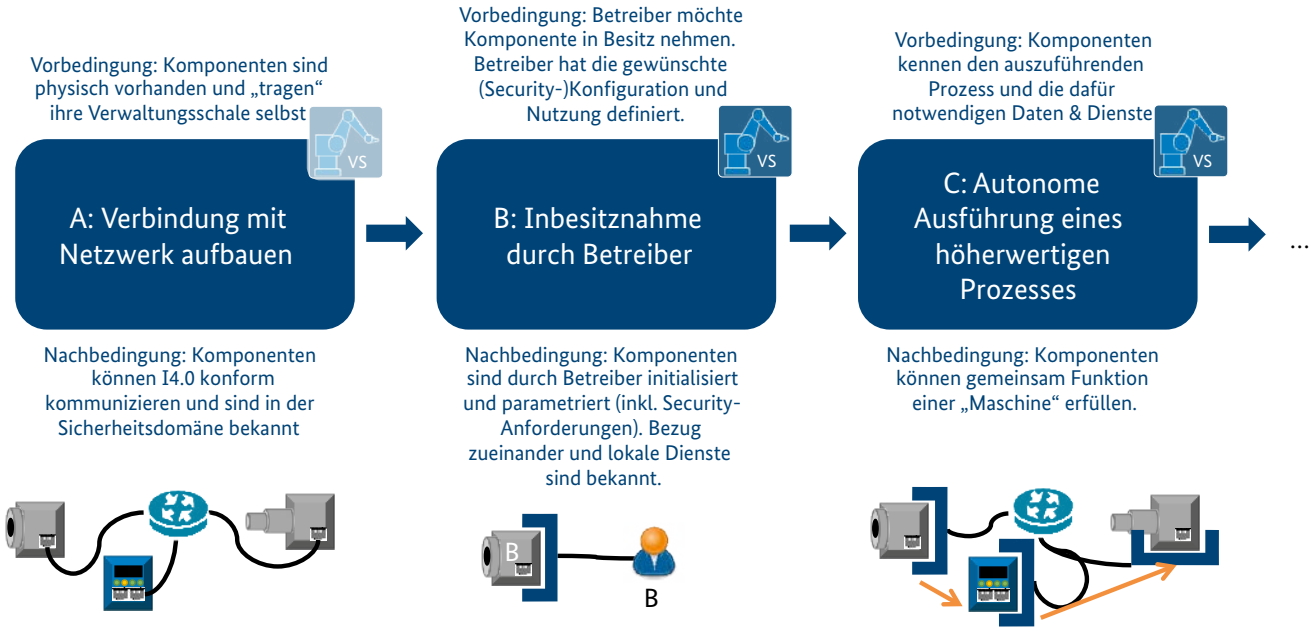
Zur Inbetriebnahme der drei Komponenten müssen die folgenden drei Prozessschritte ausgeführt werden (s. Abbildung 7):

A. Zuerst muss eine Verbindung mit dem Netzwerk aufgebaut werden. Hierzu müssen die Komponenten physisch vorhanden sein. Konnte dieser Prozessschritt erfolgreich durchgeführt werden, können die drei Komponenten nun I4.0-konform miteinander kommunizieren und sind in der Sicherheitsdomäne des Betreibers, in der sie nach Inbetriebnahme operieren sollen, bekannt. Eine direkte Interaktion mit der Verwaltungsschale erfolgt in diesem Schritt, wie in der Abbildung auch grafisch angedeutet, nicht.

B. Im zweiten Schritt erfolgt die Inbesitznahme der Komponenten durch den Anlagenbetreiber (im Folgenden „Betreiber"). Hier ist die Annahme, wie zuvor beschrieben, dass alle Komponenten ihre Verwaltungsschale direkt zur Verfügung stellen können. Zudem wird direkt mit der Verwaltungsschale interagiert. Zur Inbesitznahme ersetzt der Betreiber z. B. Default-Passwörter und Default-Einstellungen des Komponentenherstellers. Hierzu sollte der Betreiber für sich die gewünschte (Security-)Parametrierung und -Nutzung der Komponenten bereits definiert haben. Konnte dieser Prozessschritt erfolgreich durchgeführt werden, sind die Komponenten nun initialisiert und parametriert. Zudem haben die Komponenten einen Bezug zueinander und ihre lokalen Dienste sind untereinander bekannt.

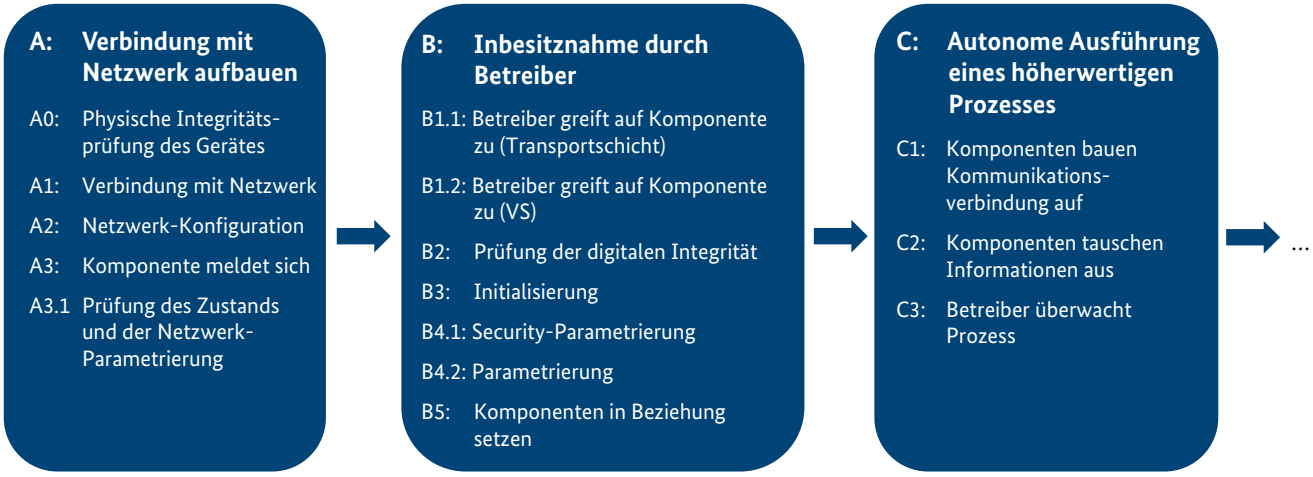
C. Im letzten Schritt führen die Komponenten autonom einen höherwertigen Prozess aus. Hierzu müssen die Komponenten den auszuführenden Prozess sowie die zur Ausführung notwendigen Dienste und Daten kennen. Konnte dieser Prozessschritt erfolgreich durchgeführt werden, erfüllen die Komponenten nun gemeinsam die Funktion einer Maschine.

Abbildung 7: High-level-Sicht auf die Prozessschritte des Use-Cases „Engineering". Die Schritte B und C werden gegenüber der Verwaltungsschale ausgeführt, während Schritt A zur Vorbereitung der Kommunikation mit der Verwaltungsschale dient.



Quelle: ZVEI SG Modelle und Standards

Abbildung 8: Detaillierung der Prozessschritte des Use-Cases „Engineering“



Quelle: ZVEI SG Modelle und Standards

In Abbildung 8 sind die drei Prozessschritte etwas detaillierter dargestellt. Weitere Details finden sich im Anhang A.

Der Verbindungsaufbau mit dem Netzwerk beinhaltet beispielsweise die Sichtprüfung auf Beschädigungen oder Zeichen der Manipulation der Geräte, die physische Verbindung mit dem Netzwerk, die Netzwerkkonfiguration der Geräte inklusive der Security-Parameter auf OSI Layer 2 + 3 (Link und Netzwerk) sowie die Anmeldung der Komponente im Netzwerk. Abschließend sollte die Integrität der Netzwerkkonfiguration geprüft werden.

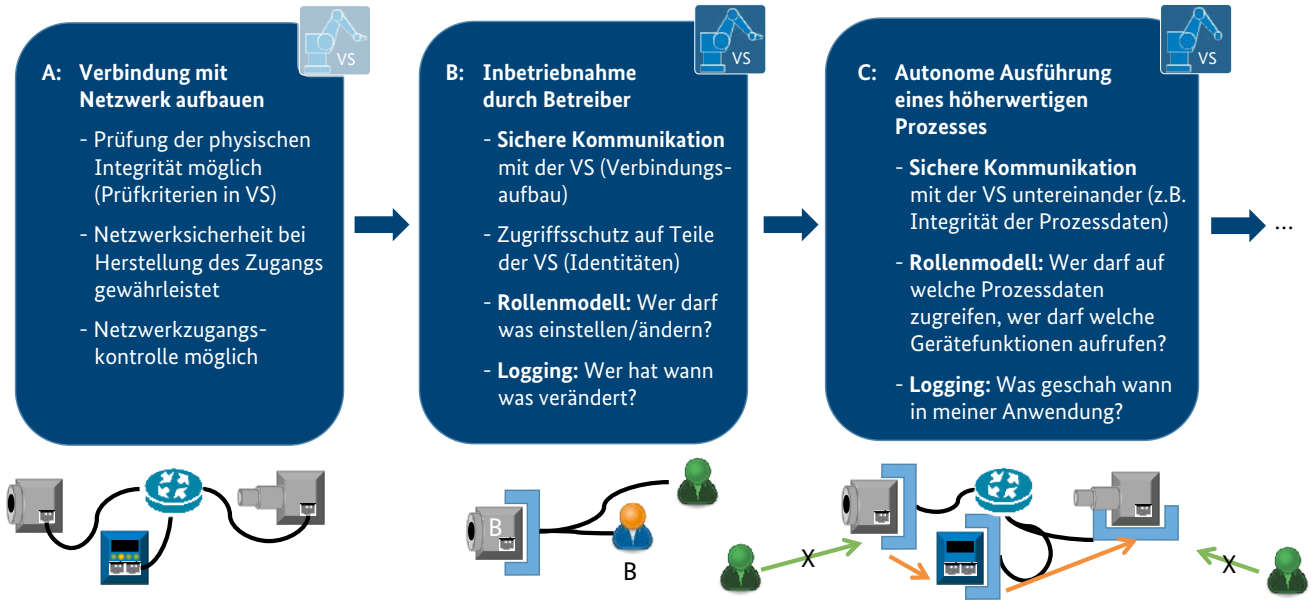
Um die Komponenten in Besitz zu nehmen, greift der Betreiber auf die Komponente zu. Hierbei wird zwischen der reinen Kommunikationssicht, das heißt, dem Aufbau einer I4.0-konformen Kommunikation zur Verwaltungsschale, und dem eigentlichen Zugriff auf die Verwaltungsschale der Komponente unterschieden. Anschließend sollte überprüft werden, ob die Daten der Verwaltungsschale mit den physischen Eigenschaften des Gegenstands übereinstimmen, beispielsweise Hersteller, Abmessungen oder Funktionen. Bei der Initialisierung der Komponente durch den Betreiber wird diese inventarisiert und erhält beispielsweise ein Betreiberzertifikat als neue Identifikation. Auch die Parametrierung kann in zwei Aspekte aufgeteilt werden: das Setzen der Security-Eigenschaften wie Nutzerrollen und Zugriffsrechte sowie das Setzen der funktionalen Parameter der Komponente, basierend auf den zuvor festgelegten Schutzmechanismen. Abschließend müssen die Komponenten anhand ihrer Identifikatoren zueinander in Bezug gesetzt und ihre Dienste bekannt gemacht werden.

Zur Ausführung eines höherwertigen Prozesses können die Komponenten nun auf Basis ihres bekannten Bezugs zueinander eine entsprechende Kommunikationsverbindung aufbauen und über die jeweils zur Verfügung gestellten Dienste Daten austauschen. Zudem kann der Betreiber den Prozess überwachen, indem er sich mit den Komponenten verbindet und auf die Daten zugreift, um den Prozesszustand zu bewerten.

3.2.3 Ableitung relevanter Security-Aspekte

Abschließend wurde für die in Abbildung 8 dargestellten detaillierten Prozessschritte eine Analyse durchgeführt, welche Security-Aspekte jeweils relevant sind und welche Security-Anforderungen sich daraus für die Verwaltungsschale selbst sowie für die Teilmodelle der Verwaltungsschale ableiten lassen. Wie in Abbildung 9 dargestellt, sind im ersten Prozessschritt eher wenige Basis-Security-Aspekte zu betrachten, wie z. B. IEEE 802.1x oder OSI-Schicht-2-Sicherheitsmechanismen, auch weil die Verwaltungsschale noch nicht durch den Betreiber in Besitz genommen wurde und daher vor allem allgemeingültige Informationen enthält. Im Prozessschritt der Inbesitznahme spielen die sichere Kommunikation mit der Verwaltungsschale, der Zugriffsschutz mittels Benutzer- und Rollenmodell sowie Ereignisprotokollierung eine zentrale Rolle. Speziell beim Zugriffsschutz sind (sichere) Identitäten ein zentraler Aspekt. Dieselben Security-Aspekte sind auch während der Ausführung des Prozesses (Prozessschritt C) relevant, der Kontext unterscheidet sich jedoch. Sichere Kommunikation bezieht

Abbildung 9: Security-Aspekte der einzelnen Prozessschritte des Use-Cases „Engineering“



Quelle: ZVEI SG Modelle und Standards

sich hier auf die Kommunikation der Komponenten untereinander, das Rollenmodell auf Zugriffe auf die Prozessdaten und die Ereignisprotokollierung eher auf die Anwendung.

Mehr Details zu den konkreten Security-Anforderungen, aus denen sich die genannten Security-Aspekte: Sichere Kommunikation, Rollenmodel, Identitäten und Ereignisprotokollierung ableiten, finden sich im Anhang A. Eine Vertiefung der vier genannten Aspekte erfolgt in Abschnitt 3.3.

3.3 Im Use-Case nicht betrachtete Aspekte der Verwaltungsschale

Der beschriebene Use-Case umreißt nur einen kleinen Teil der Funktion der Verwaltungsschale und der Interaktion mit ihr. Ebenso wird nur ein Teil des Lebenszyklus der Industrie 4.0-Komponenten beleuchtet. Daher ergeben sich weitere sicherheitsrelevante Fragestellungen, die nicht im Use-Case abgebildet wurden.

Aus heutiger Sicht ist noch offen, wie die Verwaltungsschale für aktive und passive I4.0-Komponenten im Lebenszyklus aussieht. Insbesondere unterscheiden sich die Sicherheitsanforderungen in den Phasen: Planung, Entwicklung, Konstruktion und virtuelle Inbetriebnahme deutlich von den Anforderungen während der Integration und im Betrieb. Ebenso geht das Beispiel davon aus, dass die Verwaltungsschale Einfluss auf die aktiven Teile einer Komponente nimmt. Im Falle einer passiven Komponente ohne eigene Kommunikationsmöglichkeiten unterscheiden sich die Integrations- und Betriebsschritte deutlich vom beschriebenen Use-Case.

Ein häufig erwähntes Einsatzszenario ist die Simulation einer Maschine unter Einbeziehung von Verwaltungsschalen. In diesem Einsatzszenario werden über die Verwaltungsschale keine physisch vorhandenen Komponenten, sondern simulierte Komponenten angesprochen. Der beschriebene Use-Case geht auf diese Möglichkeit nicht ein.

4. Detailbetrachtung der Sicherheitsanforderungen im Use-Case „Engineering“

4.1 Basissicherheitsanforderungen

Die hier aufgeführten Sicherheitsanforderungen beziehen sich nicht nur auf den beschriebenen Use-Case, sondern können auf allgemeine Anwendungen übertragen werden. Diese Basissicherheitsanforderung sind mit dem nachfolgenden Use-Case bestätigt worden:

- Identitäten und Authentifizierung :

  Wie kann sichergestellt werden, dass die richtigen Komponenten und Benutzer miteinander interagieren?

- Benutzer- und Rechteverwaltung:

  Wie kann der Zugriff auf die Verwaltungsschale und ihre Inhalte beschränkt und gesteuert werden?

- Kommunikationssicherheit:

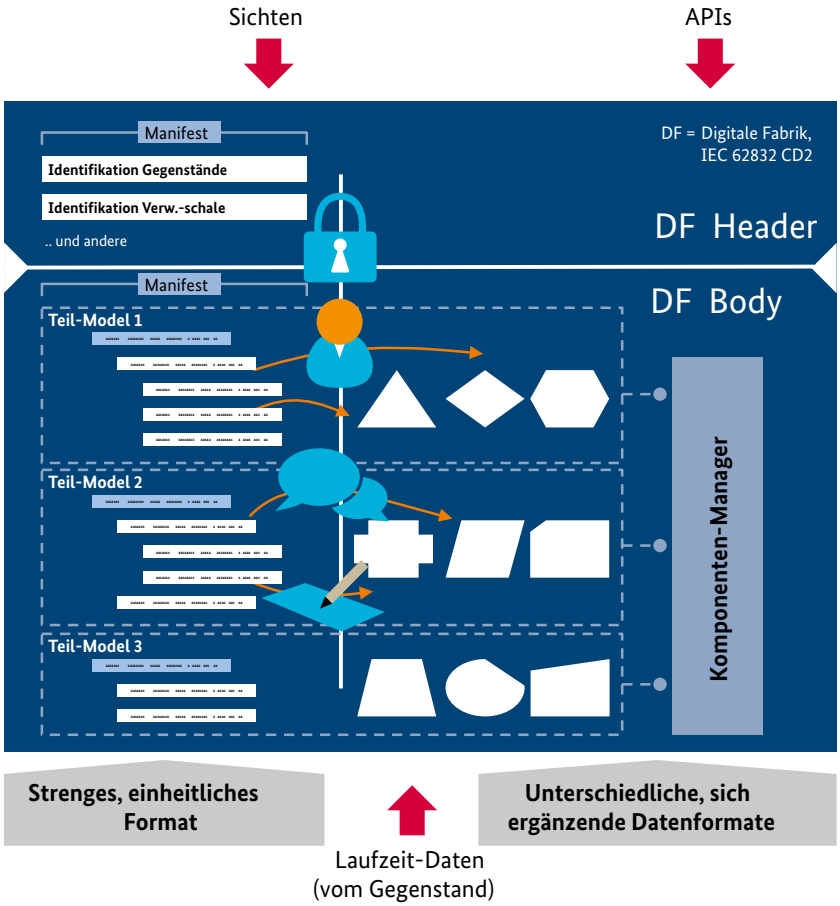
  Wie können Daten vertraulich und integritätsgesichert zwischen der Verwaltungsschale und ihren Kommunikationspartnern ausgetauscht werden?

- Ereignisprotokollierung (Logging):

  Wie kann nachvollzogen werden, wer wann welche Interaktion mit der Verwaltungsschale durchgeführt hat?

Da diese vier Fragen und Anforderungen von essenzieller Bedeutung für den sicheren Betrieb einer Industrie 4.0-Komponente sind, wird die Verwaltungsschale der I4.0-Komponente um die Teile Authentifizierung der Identifikatoren, Benutzer- und Rechteverwaltung, Kommunikation und der Ereignisprotokollierung ergänzt.

Abbildung 10: Dauerhafte Sicherheitsanforderungen für die Verwaltungsschale



Quelle: ZVEI SG Modelle und Standards

4.1.1 Identitäten und Authentifizierung

Identifizierung und Authentifizierung beziehen sich auf unterschiedliche Ebenen. Wird eine Identität festgestellt, geht es umgangssprachlich um die Prüfung: „Wer bist du?“. Eine Identität wird aus einer groben, allgemeinen Masse heraus kenntlich gemacht. Dieser Vorgang hat insofern noch nichts mit Security-Maßnahmen zu tun. Bei der Authentifizierung handelt es sich im Gegensatz dazu um eine dezidierte Security-Maßnahme. Es wird überprüft, ob die gegebene Information über die Identität „Der bin ich“ tatsächlich stimmt. Dazu wird z. B. eine vertrauenswürdige (dritte) Stelle herangezogen, die die Angabe der Identität bestätigt. Dadurch soll die Frage „Kann ich der Identitäten-Angabe vertrauen?“ adressiert werden.

Mit Blick auf die VDI/VDE 2182 (Komponentenhersteller, Integrator und Betreiber) sind unterschiedliche security-relevante Rollen zu berücksichtigen. So kann man annehmen, dass in der Verwaltungsschale eines Sensors ein Identifikator für die Verwaltungsschale und für das Asset vorhanden ist.

Ein Identifikator wird zur Bestimmung einer Identität, einer Entität (in diesem Fall der Aktor) verwendet. Der Identifikator setzt sich aus einem oder mehreren Attributen zusammen (z. B. einer Seriennummer oder einem Namen, der zur Identifikation dient).

Die Authentifizierung dient als Nachweis einer behaupteten Identität. Sie setzt eine Möglichkeit zu deren Überprüfung voraus. Im beschriebenen Use-Case könnte der Identifikator die vom Hersteller vergebene Seriennummer sein. Zusätzlich kann die Komponente noch digitale Zertifikate enthalten, um sich zweifelsfrei gegenüber Dritten auszuweisen, also authentifizieren.

Es ist auch denkbar, dass eine Publik-Key-Infrastruktur (PKI) eingesetzt wird. Eine solche Infrastruktur erlaubt es, die Identitäten von Geräten durch eine unabhängige dritte Stelle (Certification Authority) bestätigen zu lassen. So kann z. B. die Verwaltungsschale sowohl mit einem Zertifikat des Herstellers als auch des Betreibers versehen werden. Die sich ergebenden Aussagen sind: „Diese Komponente wurde durch Hersteller ABC hergestellt und ist eine Komponente von Typ ABC123 mit der Seriennummer 123456“ oder „Diese Komponente wurde durch Betreiber XYZ in Betrieb genommen und besitzt die Identität XYZ789“. Diese Aussagen lassen sich durch die Verwendung geeigneter Maßnahmen (z. B. digitaler Signaturen und Zertifikate) untermauern.

Der Mehrwert in der Benutzung von sicheren Identitäten ist, dass solche Systeme es einem Angreifer sehr schwer machen, selbst Teil des Systems zu werden, da er in der Regel nicht über die geheimen Informationen (z. B. Private Keys) der Systemteilnehmer verfügt.

4.1.2 Benutzer- und Rollenverwaltung

Jede Verwaltungsschale wird mit einem Rechte- und Rollenmodell (noch zu detaillieren) von dem Komponentenhersteller ausgeliefert.

Das Rollenmodell sollte den im Lebenszyklus einer Industrie 4.0-Komponente relevanten Interaktions- und Benutzerrollen entsprechen. Bezüglich der Mächtigkeit des Rollenmodells gibt es verschiedene mögliche Abstufungen, die sich in vier Kategorien untergliedern lassen.

Im Folgenden wird unter dem Begriff „Benutzer“ jeweils eine Rolle im Lebenszyklus der Verwaltungsschale verstanden. Rollen können z. B. sein:

a. ein Integrator, der aus verschiedenen Komponenten eine höherwertige Funktion zusammenstellt und konfiguriert,

b. ein Maschinenbediener, der nach der Anmeldung verschiedene Funktionen einer Komponente verwenden kann oder

c. eine andere Industrie 4.0-Komponente, die im Rahmen ihres Betriebs auf die Verwaltungsschale einer anderen Komponente zugreift.

Objekte, für die eine Zugriffssteuerung nötig ist, können z. B. sein:

a. die Werte, die in der Verwaltungsschale verfügbar und veränderbar sind, sowohl in Teilmodellen als auch in generell verfügbaren Teilen der Verwaltungsschale,

b. Metadaten über die Verwaltungsschale und die Interaktion mit ihr (z. B. Ereignisprotokollierung, Monitoring von Änderungen etc.),

c. die Parametrierung und Überwachung von Sicherheitseigenschaften der Verwaltungsschale (Einstellungen des Rollenmodells und der Sicherheitsmechanismen) etc.

Um die Zugriffssteuerung zentral in der Verwaltungsschale verfügbar zu machen und alle Teilaspekte darüber sichern zu können, sollte sie zwingend in jeder Verwaltungsschale verfügbar sein. Jedoch gibt es unterschiedliche Möglichkeiten der Ausprägung:

1. **Regelung des globalen Zugriffs auf eine Komponente für einen oder mehrere authentifizierte Benutzer:** Es wird nur unterschieden, ob sich ein Benutzer anmelden kann. Nach der Anmeldung kann der Benutzer auf alle Aspekte der Komponente, die in der Verwaltungsschale modelliert sind, zugreifen.

2. **Regelung der Sichtbarkeit einzelner Funktionen und Werte der Verwaltungsschale für einen oder mehrere authentifizierte Benutzer:** Es wird nach Berechtigungen verschiedener Benutzer unterschieden, sodass verschiedene Benutzer jeweils nur auf für sie relevante Funktionen und Werte zugreifen können. Eine Unterscheidung nach Lesen bzw. Schreiben wird jedoch noch nicht gemacht.

3. **Regelung der Sichtbarkeit und Modifizierbarkeit (lesen/modifizieren) für einen oder mehrere authentifizierte Benutzer:** Wie in Punkt 2 können verschiedene Benutzer, je nach Rolle, verschiedene Werte und Funktionen der Verwaltungsschale verwenden. Es ist jedoch eine Unterscheidung nach Lese- und Schreibrecht pro Wert möglich. So lassen sich auch sicherheitsförderliche Rollen wie ein Auditor mit umfassenden Leserechten, aber ohne jegliche Schreibrechte, realisieren.

4. **Regelung der Modifizierbarkeit (lesen/modifizieren) innerhalb vorgegebener Wertebereiche abhängig von der Authentifizierung eines oder mehrerer Benutzer:** In dieser Ausprägung sind, abhängig von der Rolle des authentifizierten Benutzers, Modifikationen nur innerhalb vorgegebener Wertgrenzen möglich. Ein Bediener könnte so z. B. eine Achse gegebenenfalls nur um für den Produktionsbetrieb zulässige +/−45° drehen, während ein Einsteller oder Integrator bei der Wartung oder Installation die Achse bis über die für den Regelbetrieb zulässigen Werte auf +/−60° drehen kann.

Im weiteren Verlauf des Lebenszyklus bzw. auch bei dem Besitzübergang (siehe unter anderem VDI 2182 mit den Rollen des Komponentenherstellers, Integrators und Betreibers) wird die von dem Inbesitznehmer vorgesehene (gewünschte) Benutzer- und Rollenverwaltung mit ihren Bestandteilen in der Verwaltungsschale gespeichert und aktiviert. Der aktuelle Besitzer entscheidet, ob und welche Benutzer und Rollen dem Vorbesitzer weiterhin zur Verfügung stehen bzw. welche Accounts weiter gültig sind. Insbesondere wirken sich die Einstellungen des Rechtemodells auf alle anderen Teilmodelle der Verwaltungsschale aus, da die Sichtbarkeit und die Modifizierbarkeit von Werten bzw. Funktionen dieser Teilmodelle durch das Rechtemodell bestimmt werden.

4.1.3 Kommunikation

Industrie 4.0 folgt einer serviceorientierten Architektur. Dazu müssen Dienste aufgerufen und Daten ausgetauscht werden können. Daher wurden generelle Anforderungen an die Nachrichtenübertragung zwischen zwei I4.0-Komponenten formuliert, die „I4.0-Kommunikation“. Die konkreten Anforderungen an die I4.0-Kommunikation werden zurzeit noch definiert.

Die Kommunikation in industriellen Anlagen kann über verschiedenste Physical Layer und MAC Layer erfolgen. So ist eine Kommunikation über Funk genauso denkbar wie eine Kommunikation über kabelgebundene Netzwerke. Aufgrund der verschiedenen Eigenschaften dieser Netzwerkarten kann sich die Definition der Verwaltungsschale nicht auf die Sicherheitseigenschaften dieser Netzwerke stützen. Daher müssen angemessene Sicherheitsmaßnahmen oberhalb der Schicht 3 im ISO/OSI-Schichtenmodell bereitgestellt werden. Insbesondere müssen die von der Verwaltungsschale benötigten Sicherheitskernfunktionen Vertraulichkeit, Integrität und Authentifizierung durch die Verwaltungsschale selbst bereitgestellt werden. Da die Verfügbarkeit der Kommunikation nur schwer in den höheren Schichten eines Protokollstapels geschaffen werden kann, muss diese Sicherheitseigenschaft durch die unteren Schichten des Kommunikationssystems in einem für die Anwendung ausreichenden Maße bereitgestellt werden.

Die I4.0-Kommunikation soll nicht neu ausgearbeitet werden, sondern aus den vorhandenen und bereits in Entwicklung befindlichen Standards sollen Vorzugsstandards herausgefiltert werden, die sich für die I4.0-Kommunikation am besten eignen.

Im RAMI4.0 ist die I4.0-Kommunikation der „Communication Layer“. Alle anderen Kommunikationsarten und Protokolle sind dort im „Integration Layer“ verortet.

4.1.4 Ereignisprotokollierung (Logging)

Zugriffe auf Funktionen und Werte, sowohl des Headers als auch des Bodys, werden bei Bedarf und in der entsprechenden Granularität mitprotokolliert. Die Ereignisprotokollierung bezieht sich auf sämtliche Zugriffe der Verwaltungsschale als Gesamtheit.

Da jede Veränderung eines Wertes der Komponente Einfluss auf Security und Safety einer Komponente haben kann, wird eine gemeinsame Funktion für die Ereignisprotokollierung benötigt, sodass alle Informationen in allen Teilmodellen davon erfasst werden können. Anderenfalls bliebe es jedem Teilmodell und potenziell jedem Datum in der Verwaltungsschale selbst überlassen, für eine Protokollierung zu sorgen. Eine einheitliche Ereignisprotokollierung-Funktionalität erleichtert hier die Erfassung relevanter Ereignisse.

Auch aus Sicht der Security ist eine gemeinsame Ereignisprotokollierung-Funktion für alle Teilaspekte der Verwaltungsschale unabdingbar. Im Speziellen werden aus Security-Gesichtspunkten oftmals weitere Anforderungen an die Erstellung, Speicherung und Entfernung von Informationen zur Ereignisprotokollierung gestellt. Ereignisprotokollierung mit securityrelevanten Informationen sollten dabei vor Veränderungen durch Angreifer geschützt werden, sodass ein Angreifer nicht in der Lage ist, die Inhalte der Ereignisprotokollierung im Nachhinein zu verändern, um seine Spuren zu verwischen. Hierfür werden veränderungsfreie (tamper-free) Ereignisprotokolle benötigt.

Ebenso ist der sichere Zugriff auf die Ereignisprotokollierung durch das oben beschriebene Rollenmodell zu gestalten. Es muss möglich sein, verschiedene Standardrollen in der Security abzubilden. So sollte eine Unterscheidung zwischen Rollen, die ein Log einsehen können (Auditor) und solchen, die ein Log nicht einsehen können (Verwender einer Komponente/andere I4.0-Komponente) umsetzbar sein. Ebenso muss zwischen Rollen, die Log-Einträge anlegen oder gar löschen können, differenziert werden.

Die Frage, was in welchem Umfang geloggt werden soll, ist von großer Bedeutung. Ein pauschales Loggen aller Ereignisse (z. B. auch Änderungen aller in der Verwaltungsschale vorhandenen Werte) kann schnell die Rechen- und Speicherkapazitäten von industriellen Systemen übersteigen. Insbesondere wenn Änderungen an hochvolatilen Werten mit vielen Änderungen protokolliert werden, können große Datenmengen anfallen. Daher ist es wichtig, spezifizieren zu können, welche Teile der Verwaltungsschale in welcher zeitlichen Auflösung durch die Ereigniserfassung protokolliert werden sollen.

Die Möglichkeit, die Log-Informationen an einen Log-Server weitergeben zu können, sollte je nach Funktion und Fähigkeiten einer Komponente erwogen werden. Eine solche Weitergabe erleichtert das Zusammenführen von Ereignisinformationen verschiedener Industrie 4.0-Komponenten, um eine bessere Gesamtübersicht in einem System zu erreichen. Zur Übertragung von Log-Informationen sollte auf bereits standardisierte Protokolle und Mechanismen zurückgegriffen werden, um eine möglichst große Verträglichkeit mit bestehenden Archivierungs- und Analysesystemen (z. B. Security-Information and Event Management Systeme, SIEM) zu erreichen.

Hinsichtlich Art und Umfang der zu speichernden Daten sind zusätzlich die jeweiligen regulatorischen Vorgaben zu berücksichtigen. So können Rollen wie Auditor oder die Forderung nach veränderungsfreier Ereignisprotokollierung oder Mindest- oder Höchstaufbewahrungsfristen auch bereits durch regulatorische Anforderungen für den Einsatz in einer bestimmten Branche gefordert sein. Daher ist die Spezifikation eines für möglichst viele Branchen und Anwendungen geeigneten Systems zur Ereignisprotokollierung nötig.

4.2 Einstufung und Vergleich von Sicherheitseigenschaften

Basierend auf einer noch festzulegenden Einstufung (z. B. ähnlich Security Level 1 (SL1) bis SL4 nach IEC 62443) werden die domänenspezifischen Security-Anforderungen an eine Komponente definiert.

Die Umsetzung (Implementierung) der Security-Anforderungen kann auch im Rahmen eines Teilmodells erfolgen. Die gewünschte Stufe legt den Umfang der umzusetzenden Funktionen fest. Die Security-Fähigkeiten der I4.0-Komponente entsprechen der Stufe der umgesetzten Funktionen und werden als Merkmal von der I4.0-Komponente geliefert.

Die Security-Fähigkeiten entwickeln sich zu einer Produkteigenschaft mit einer bewertbaren Qualität auf einer noch festzulegenden Skala und bilden neben den Safety-Fähigkeiten, Privacy-Fähigkeiten, der Resilienz und der Zuverlässigkeit die charakteristischen Merkmale (Industrial Trustworthiness Criteria) mit Security (Industrial Security Trustworthiness Criteria – ISTC) einer vertrauenswürdigen I4.0-Komponente. Ein abgestuftes Niveau der Vertrauens-

würdigkeit auf einer Skala erlaubt die Einschätzung der Einsetzbarkeit einer I4.0-Komponente in einem Gesamtsystem und gestattet, den Level der Vertrauenswürdigkeit eines Wertschöpfungsnetzwerks automatisch zu ermitteln anhand der aktuellen Vernetzung der Teilnehmer des Wertschöpfungsnetzwerks. Zu dem Zeitpunkt der Integration von Komponenten zu einer Maschine muss sich der resultierende Level der Vertrauenswürdigkeit aus der Komposition der Komponenten ergeben. Es ist ein Konzept zu erarbeiten, wie diese Werte ermittelt und bestätigt werden können.

4.3 Komposition

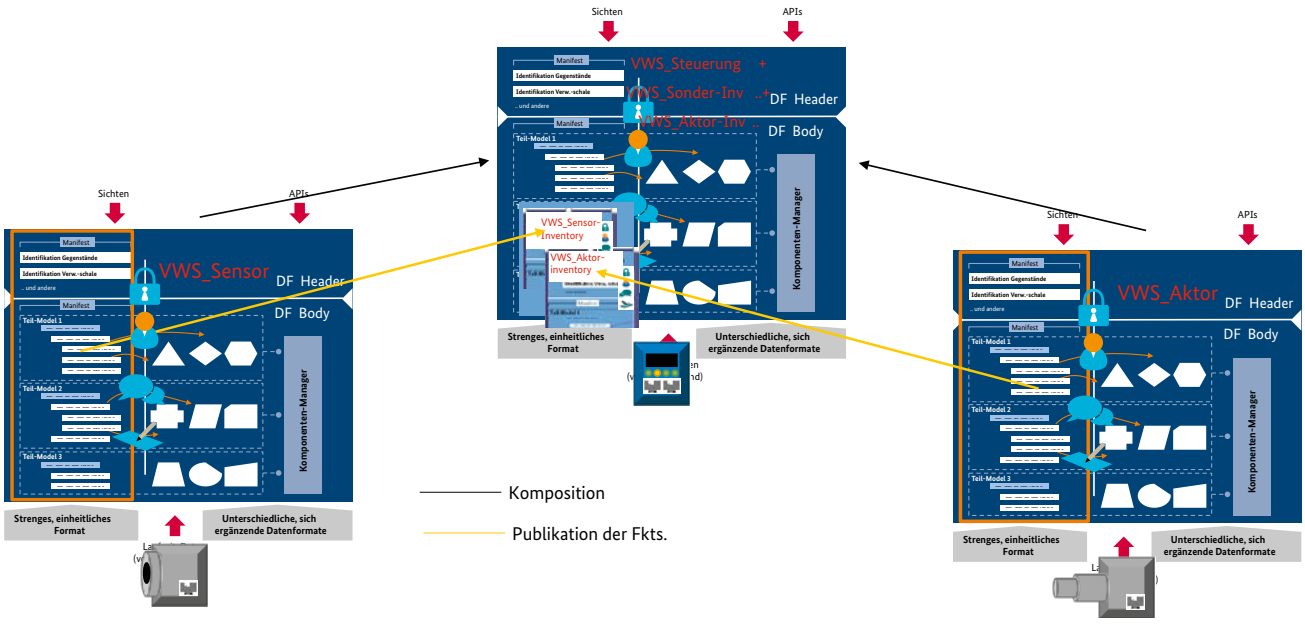
Verwaltungsschalen sollen eine Komposition von Einzelkomponenten zu ganzen Systemen, Maschinen oder Anlagen erlauben. Dabei wird für das zusammengesetzte System wieder eine Verwaltungsschale geschaffen, durch die mit dem Gesamtsystem interagiert werden kann.

Es ist wichtig, dass der Verbund aus Verwaltungsschalen in sich wieder sicher ist. Diese Anforderung wird durch die oben beschriebenen Maßnahmen (Rollenmodell, Kommunikationssicherheit, Ereignisprotokollierung, Zugriffsschutz) unterstützt. Bei der Komposition der Verwaltungsschalen ist darauf zu achten, dass die Security-Eigenschaften der Einzelteile und der zusammengesetzten Verwaltungsschale kompatibel sind.

Die nachfolgende Darstellung zeigt eine der möglichen Varianten der Komposition: Die Komposition von VWS_Sensor und VWS_Aktor in VWS_Steuerung entsteht durch Bekanntmachen und Publizieren des Inventory VWS_Sensors und VWS_Aktors in die VWS_Steuerung. Die VWS_Steuerung enthält damit sowohl die eigenen Funktionen als auch die publizierten Funktionen des Sensors und Aktors.

Das unten aufgeführte Beispiel zeigt die Kombinierbarkeit von Verwaltungsschalen. In einem Anwendungsbeispiel könnte die oberste Verwaltungsschale einen Befehl oder Auftrag erhalten und diesen durch die Verwendung der unteren Verwaltungsschalen ausführen. In diesem Fall müssen die Daten integer und unveränderbar weitergegeben werden, sodass die in der Grafik weiter unten befindlichen Verwaltungsschalen die gewünschte Aktion korrekt ausführen können.

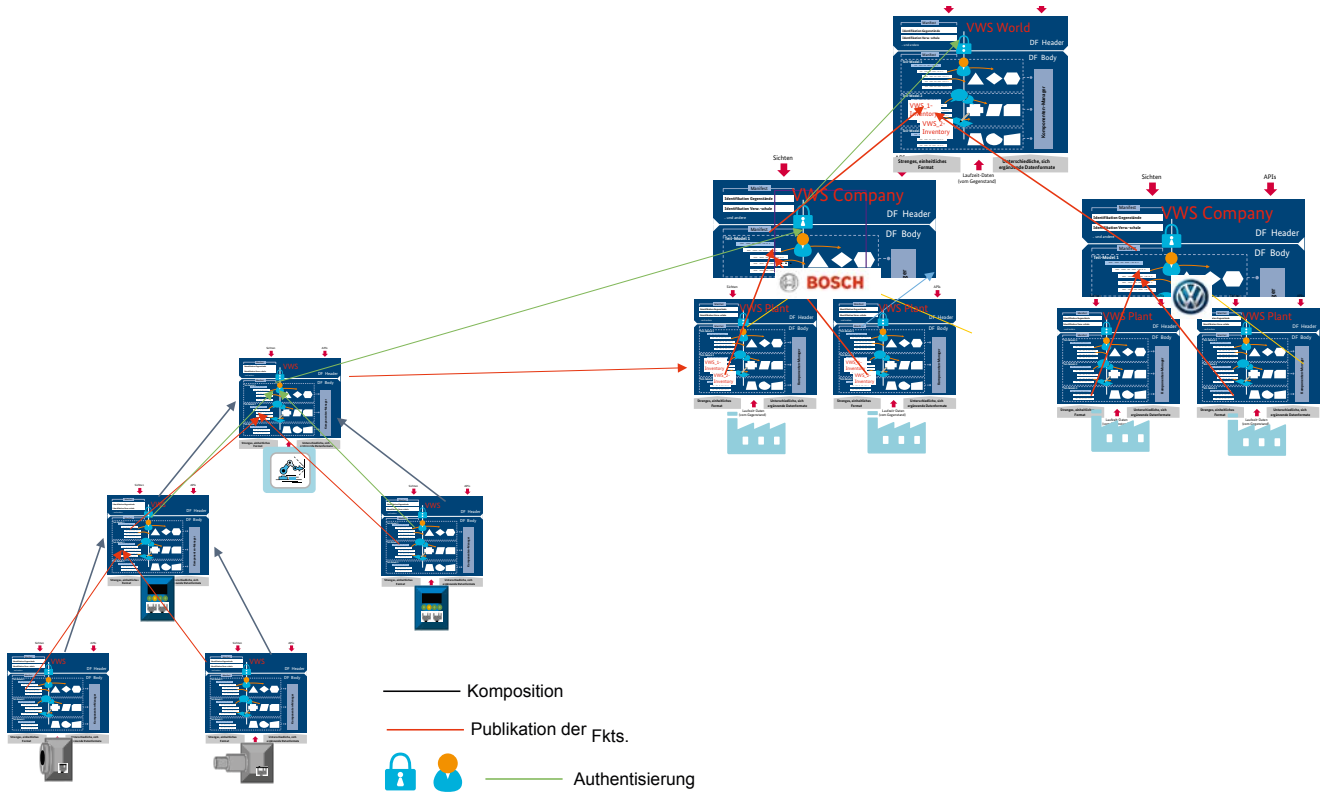
Abbildung 11: Komposition 1



Quelle: ZVEI SG Modelle und Standards

Aus der Komposition und dem Zusammenfügen/Bekanntmachen von I4.0-Komponenten im Kontext einer Fabrik, eines Unternehmens, national und international ergibt sich folgende Struktur:

Abbildung 12: Komposition 2



Quelle: ZVEI SG Modelle und Standards

Anhang Use-Case „Engineering“ im Detail

Detaillierung der Prozessschritte Ax, Bx und Cx. Diese Detaillierung enthält die Betrachtung der Security-Aspekte, die Security-Anforderungen an die Teilmodelle sowie die Anforderungen an die Verwaltungsschale (VWS). Es wird darauf hingewiesen, dass Security kein Teilmodell in der Verwaltungsschale darstellt, sondern dass die Security Anforderungen an die Verwaltungsschale selbst sowie an alle Teilmodelle einer Verwaltungsschale stellt und somit übergreifend wirkt.

Prozessschritt	Beschreibung	Security-Aspekte	Security-Anforderung an Teilmodelle	Security-Anforderungen an die Verwaltungsschale
A0 Physische Integritätsprüfung des Geräts	Sichtprüfung auf Beschädigungen oder Zeichen von Manipulationen des Geräts	Manipulationen sollten durch Verpackungsmerkmale (z. B. Label, die sich bei der Entfernung zerstören) erkennbar sein.	Die physischen Security-Aspekte eines Gegenstands sind nicht zentral. Eventuell könnte der gerätebeschreibende Teil der Verwaltungsschale Hinweise zu physischen Schutzmechanismen enthalten.	
A1 Verbindung mit Netzwerk	Sensor, Steuerung und Aktor werden physisch mit dem I4.0-Netzwerk verbunden (z. B. Geräte werden mechanisch „eingesteckt“). Die folgende Kommunikation kann drahtgebunden oder drahtlos erfolgen.	Bei der physischen Verbindung sollte darauf geachtet werden, dass das Gerät mit dem richtigen Netzwerk verbunden wird. Eine weitergehende Prüfung kann in den nächsten Schritten durch eine Kommunikation mit Netzwerkkomponenten und I4.0-Komponenten im Netzwerk geschehen.	Wie oben: Die rein physische Verbindung ist nicht zentral. Die Verbindung mit dem korrekten Netzwerk sollte später digital geprüft werden. Im drahtlosen Fall sollten Sicherheitsinformationen aus dem Netzwerk-Teilmodell verfügbar sein. Im drahtlosen Fall wäre dies: SSID, BSSID, Verbindungsstatus, Sicherheitsaspekte: WPA2/Chiffren, …	
A2 Netzwerkkonfiguration (Kommunikation)	Die Netzwerkkonfiguration (OSI Layer 2 + 3: Link und Network Layer) kann manuell oder automatisch erfolgen; Partner könnten jetzt (ggf. ungesichert) miteinander kommunizieren (wenn sie wüssten, wer noch da ist).	Security-Parameter werden gesetzt, z. B. auf OSI Layer 2. Findet eher in einem logisch oder sogar physikalisch getrennten Netzwerk statt. Sollte mittelfristig für I4.0 auch im produktiven Netzwerk möglich sein. Eventuell sind Schritte der Network Access Control hier zu berücksichtigen. So kann ein Netzwerk zuerst eine Authentisierung über Techniken wie IEEE 802.1X (sehr üblich im drahtlosen Umfeld, auch sehr nützlich im drahtgebundenen Umfeld) erfordern. Eine Konfiguration dieser vorgeschalteten Schritte kann prinzipbedingt noch nicht im Produktivnetzwerk stattfinden, sondern muss über ein Konfigurationsnetzwerk (ggf. nur bestehend aus dem Gerät und dem PC des Inbetriebnehmers) geschehen.		Vorgeschaltete Sicherheitsmechanismen wie IEEE 802.1X und OSI Layer 2 (z. B. Pre-Shared Key oder WPA2 Enterprise Key bei WLAN) sollten im direkten Kontakt zum Gerät über die Verwaltungsschale einheitlich konfigurierbar und zugreifbar sein. Achtung: Anmeldedaten von IEEE 802.1X stellen bereits eine digitale Identität des Geräts dar!
A3 Komponente (Gerät + VWS) meldet sich **(Netzwerkinfrastruktur-Komponente)** **(Logging)**	Die Komponente meldet sich manuell oder automatisch im Netzwerk an und ist nun digital (im Sinne der Verwaltungsschale) für andere I4.0-Komponenten verfügbar Netzwerkinfrastuktur-Komponente wird benötigt (auch I4.0-Komponente)	Im Anmeldeprozess authentisiert sich die Komponente über eine entsprechend sichere Identität.[14] Im Gegensatz zum vorigen Schritt (Anmeldung auf Schicht 2 des ISO/OSI-Modells) geht es hier um eine Anmeldung bei Verzeichnisdiensten/ Repositories oder Serverdiensten, die die Verwaltungsschale auffindbar oder zugreifbar machen. Eine Anmeldung über den Identifikator und ggf. Authentifizierung (Übermittlung des Zertifikates des Herstellers der Komponente) ist erforderlich Offene Frage: Was für ein Protokoll soll verwendet werden?		

→

14 Siehe Technischer Überblick: Sichere Identitäten bzgl. Definition der Abstufung sicherer Identitäten

Prozessschritt	Beschreibung	Security-Aspekte	Security-Anforderung an Teilmodelle	Security-Anforderungen an die Verwaltungsschale
A3.1. Prüfung des Zustands und der Netzwerk-Parametrierung	Die Integrität der Netzwerkkonfiguration des Geräts wird überprüft.			
B1.1 Betreiber greift auf Komponente zu (Transportschicht) **(Logging)**	Betreiber greift auf Komponente (Verwaltungsschale + Gerät) zu. Dazu wird eine sichere Basiskommunikation zum Gerät aufgebaut.	Transportsicherheitsmechanismen werden verwendet, um eine gesicherte Transportverbindung (z. B. TLS/DTLS) zur Verwaltungsschale aufzubauen. Ggf. sind bereits (Default-)Anmeldeinformationen notwendig, um Zugriff auf die Verwaltungsschale zu erhalten. Am Ende ist eine entsprechend gesicherte Kommunikation mit der Komponente (Gerät + VWS) möglich.	Die Parametrierung der Sicherheitsmechanismen auf der erlaubten Transportschicht (Chiffren/Algorithmen und Methoden) sollte über ein Teilmodell (Netzwerk? Transport?) der VWS abfragbar und parametrierbar sein (z. B. Entfernung von nicht mehr dem Stand der Zeit entsprechenden Chiffren). Dies geschieht nicht zum Zeitpunkt der Verbindungsaufnahme, definiert jedoch die zur Verbindungsaufnahme möglichen Optionen.	Zugriffsschutzmechanismen für die TCP/IP/TLS Kommunikation
B1.2 Betreiber greift auf Komponente zu (VWS) **(Logging)**	Betreiber greift auf Komponente (Verwaltungsschale + Gerät) zu.	Anmelden mit Default-Password/Standard Credentials Es sind nur die Teile änderbar, die der Hersteller zur Änderung vorgesehen hat. Auslesen der Security-Fähigkeiten (Capabilities), d. h., VWS liefert mögliche Security-Mechanismen zum Schutz der Kommunikation (z. B. „Ich kann Security-Level 1 bis 4 erreichen“) Abgleich mit Security-Anforderungen (Requirements) bzw. unterstützten Methoden und Algorithmen/Chiffren/Verfahren Anmeldung des (Default-)Benutzers an der VWS	Genormte Kommunikation von Sicherheitsniveaus und genormte Beschreibung von Algorithmen zur Anmeldung. Informationen, ob es einen Standardbenutzer gibt. Konfiguration des Standardbenutzers. Festlegung von Fehlerbildern (DoS-Angriffe durch zu häufige Anmeldung, Passwortraten, Begrenzung von Login-Versuchen etc.). Da der Benutzer sich noch nicht eingewählt hat, werden hier die werksseitigen Mechanismen verwendet.	Zugriffsschutzmechanismen für gesamte VWS (z. B. Vertraulichkeits-anforderungen, DoS-Schutz). Integritätsschutz der VWS, inkl. Header-Daten
B2 Prüfung der digitalen Integrität **(Logging)**	Es wird überprüft, ob die Daten in der Verwaltungsschale zu den physischen Eigenschaften des Gegenstands passen (z. B. Hersteller, Abmessungen, Funktionen, Leistungen etc.). Kann manuell oder teilweise automatisch erfolgen	Integritätsprüfung der Komponente Integritätsprüfung kann, z. B. über Abgleich mit Produktdatenblatt des Herstellers oder Signatur der einzelnen Einträge in der VWS, durch Hersteller erfolgen. Ggf. kann das Gerät eine digital geschützte Selbstauskunft (z. B. Remote Attestation bei TPM) geben, um die Unversehrtheit der Software zu bescheinigen. Beschreibung des Vorgehens (Überprüfung der Herkunft und Integrität von SW etc.), Prüfung von Ereignisprotokolle	Falls es ein Teilmodell zur Ereigniserfassung geben sollte, muss dieses auch Optionen zur veränderungsfreien Speicherung von sicherheitsrelevanten Log-Einträgen aufweisen.	Informationen über Echtheitsmerkmale in der Verwaltungsschale (ggf. zur digitalen Prüfung genormt). Informationen über Sicherheitszustand der Software einschließlich Prüfsummen und ggf. TPM erzeugte Integritätsinformationen. Zugriff auf ein sicheres Log, um Veränderungen am Gerät zu sehen Informationen zur Existenz von sicheren Ereignisprotokolle sollten in der VWS existieren.

→

Prozessschritt	Beschreibung	Security-Aspekte	Security-Anforderung an Teilmodelle	Security-Anforderungen an die Verwaltungsschale
B3 Initialisierung (Identitäten/Logging)	Der Betreiber nimmt die Komponenten in Besitz und inventarisiert (mit einem entsprechend sicheren Identifikator) die Komponenten. Funktionen und Methoden der Verwaltungsschale werden in einem Inventar registriert. Das Inventar (Repository) kann zentral oder dezentral vorliegen.	Ausstellung eines Betreiberzertifikats (und ggf. Passwort und Key) für Komponente.	Falls bspw. ein Betreiber-Teilmodell existiert, kann dieses auch die Sicherheitsparameter und Zertifikate enthalten. Wahrscheinlich aber eher Teil der VWS und kein eigenes Teilmodell?	Setzen der Betreiber-Sicherheitsparameter (Identifikator, Public/Private-Keys und Zertifikate erzeugen sowie Zertifikate hinzufügen (Betreiberzertifikat), Passwörter, Administrator-Nutzer, ...) über die Verwaltungsschale
B4.1 Security-Parametrierung (parallel jeweils für Sensor, Steuerung, Aktor) (Benutzer- und Rechteverwaltung wird konfiguriert, Logging)	Digitale Parametrierung der Verwaltungsschale bzgl. Nutzerrollen, Zugriffsrechten und Zugriffsmechanismen (z.B. welche Art von Verschlüsselung ist zu verwenden) wird manuell oder automatisch vorgenommen.	Festlegung der Rechte- und Zugriffsrollen aus Security-Sicht (z. B. für Datenfelder von Teilmodellen) Ideal: Für jedes Merkmal aller Teilmodelle wird ein Zugriffsrecht definiert. Realistisch: Es werden Profile gebildet/mitgeliefert, die sich leicht anpassen lassen.	Security-Anforderungen aus Risikobewertung müssen in Teilmodellen dokumentierbar sein. Fraglich ist, wo die Anforderungen dokumentiert sind (VWS der Anlage bestehend aus Sensor, Aktor und Steuerung, z. B. Verfügbarkeit der Kommunikationsschnittstelle des Sensors, Integrität der Sensordaten, Vertraulichkeit der Steuerbefehle, ...). Eine Auswahl des Benutzer- und Rechtemodells ist zu treffen, das alle Teilmodelle betrifft. Benutzer und Rollen sind festzulegen und mit dem Rechtemodell der Teilmodelle zu verknüpfen.	Mindest-Security-Level, das zur Nutzung der Komponente immer erfüllt sein muss (z. B. SL-T 2). Evtl. Profile für Zugriffsrechte Die Teilmodelle sollten die Profile unterstützen, indem sie markieren, welche Aspekte des Teilmodells durch verschiedene standardisierte Rollen (Hersteller, Administrator, Auditor, Bediener, ...) zugreifbar bzw. sichtbar oder veränderbar sind.
B4.2 Parametrierung (parallel jeweils für Sensor, Steuerung, Aktor) (Anwendung der Benutzer- und Rechteverwaltung, Identitäten, Logging in welchem Umfang?)	Digitale Parametrierung der Komponente wird manuell oder automatisch vorgenommen (ab jetzt kann das Gerät produktiv verwendet werden).	Entsprechend sichere Parametrierung über die zuvor festgelegten Zugriffs- und Transportsicherheitsmechanismen. Dies kann auch durch eine andere Person, mittels der in Schritt 4.1 festgelegten Benutzerrechte, geschehen. Die Komponente überprüft, ob die Werte der Parametrierung richtig angekommen sind: Konsistenzprüfung (z.B. Anomalie-Erkennung), Integritätsprüfung, Signaturprüfung, ... Auch möglich: Festlegung einer Nutzungsbeschränkung über Schwellenwerte etc. (auch über eine Rollenabhängigkeit)	Die Teilmodelle sollten Regeln zur Konsistenzprüfung enthalten. Z. B. Maximaldrehzahl, Maximaldrehzahl in Abhängigkeit zu anderen Parametern, ...	Ein Security-Mechanismus sollte (z. B. über Listen) verletzte Konsistenzprüfungen wiedergeben können, um diese an einem Ort abfragbar zu machen.

→

Prozessschritt	Beschreibung	Security-Aspekte	Security-Anforderung an Teilmodelle	Security-Anforderungen an die Verwaltungsschale
B5 In-Beziehung-Setzen der Komponenten	Komponenten werden manuell oder automatisch miteinander bekannt gemacht (Beispiel: zwei Komponenten werden demselben VLAN zugewiesen): Dienste werden bekannt gemacht und Komponenten werden in Bezug zueinander gestellt („Steuerung, das ist dein Sensor“). Dies wird anhand ihrer Identifikatoren (sicher oder unsicher) getan.	Sichere Bekanntmachung und Verbindung von Diensten. Automatische Bekanntmachung beispielsweise über Repositories (zentral) oder DHTs (verteilt). Bezug zueinander kann manuell (z. B. Engineering-Tool) oder automatisch (M2M) hergestellt werden. In jedem Fall sollten die Mechanismen sicher sein (Authentifizierung, Autorisierung, Integrität).	Standardisierte Art und Weise der Bekanntmachung von Geräten entweder über ein Teilmodell „Composition“ oder „Interaction“ oder „System“.	Abhängigkeiten zwischen Diensten müssen dokumentierbar sein, um mögliche security-relevante Seiteneffekte anderer Dienste auf einen bestimmten Dienst abschätzen zu können (z. B. Verfügbarkeit -> Ressourcen oder Angreifbarkeit über abhängige Dienste).
C1 Komponenten bauen Kommunikationsverbindung auf (Anwendung der Benutzer- und Rechteverwaltung, Identitäten, Logging in welchem Umfang?)	Komponenten bauen Kommunikationsverbindung untereinander auf, durch zur Verfügung gestellte Methoden. (Beispiel: In dem VLAN fangen sie an, miteinander zu kommunizieren und Daten auszutauschen)	Hier sollten Standardmethoden und ihre Sicherheitsanforderungen definiert werden. Diese Methoden müssen dann auch in die Sicherheitsbetrachtungen und eine resultierende Sicherheitsmetrik einfließen.	Netzwerk-Teilmodell(e) sollte(n) eventuelle Beschränkungen und Zugriffsmuster enthalten.	Überwachung der Kommunikation und Kommunikationsmuster einer Komponente. Eventuell sollten auch weitere Beschränkungen der Kommunikation (vgl. ACLs und Firewalls) bzw. Zugriffsmuster auf sekundäre Kommunikationsprotokolle konfigurierbar und abfragbar sein.
C2 Komponenten tauschen Informationen aus (Anwendung der Benutzer- und Rechteverwaltung, Logging in welchem Umfang?, Kommunikation)	Komponenten tauschen über die aufgebaute Kommunikations-verbindung und die zur Verfügung gestellten Dienste Informationen aus (lesend oder auch schreibend), um den Prozess zu steuern.	Zugriffsmuster und Aktivitäten sollten in einem sicheren Log in einstellbarer Granularität zur Verfügung stehen. Eventuell ist es nötig, (sichere) Alerts (vgl. SNMP Traps) bei atypischem Verhalten zu senden. Dieses Senden kann aus den Teilmodellen angestoßen werden, sollte jedoch an einem zentralen Punkt konfigurierbar sein.	Möglichkeit, Alerts für atypische Werte oder Wertüberschreitungen in den Teilmodellen zu definieren. Dies muss dann sicher gespeichert und übertragen werden.	Konfiguration von Alerts und Alert-Zielen müssen zentral einstellbar sein. Ereignisprotokolle sollten entsprechend der eingestellten Granularität erhoben werden sowie sicher und zugriffsbeschränkt sein.
C3 Betreiber überwacht Prozess (Logging)	Betreiber verbindet sich mit den Komponenten und greift auf benötigte Daten zu, um den Prozesszustand zu bewerten (z. B. Historiendaten, aktuellen Zustand einer Komponente, Abgleich von Parametern mehrerer Komponenten usw.) Ggf. ist auch eine zentrale Sammlung von Prozess- und Sicherheitsinformationen in einem Syslog-Server nötig.	Sichere Kommunikation zu einem Art-Syslog-Server (kann auch als I4.0-Komponente gestaltet sein)	Ggf. Teilmodell „Systemüberwachung“	Parametrierung von sicherem Logging und Überwachungskommunikation. Ggf. auch in einem Teilmodell „Systemüberwachung“

AUTOREN

Nicole Dönicke, Kjellberg Finsterwalde Schweißtechnik und Verschleißschutzsysteme GmbH | Dr. Thomas Gamer, ABB AG | Prof. Dr. Tobias Heer, Hirschmann Automation and Control GmbH | Dr. Lutz Jänicke, PHOENIX CONTACT GmbH & Co. KG | Michael Jochem, Robert Bosch GmbH | Dr. Wolfgang Klasen, Siemens AG | Thomas Lantermann, Mitsubishi Electric Europe B.V. | Lukas Linke, Zentralverband Elektrotechnik- und Elektronikindustrie e.V. | Jens Mehrfeld, Bundesamt für Sicherheit in der Informationstechnik | Tobias Pfeiffer, Festo AG & Co. KG | Andreas Teuscher, SICK AG

Diese Publikation ist ein Ergebnis der AG Sicherheit vernetzter Systeme in Zusammenarbeit mit dem ZVEI – Zentralverband Elektrotechnik- und Elektronikindustrie e.V.

www.plattform-i40.de