18. AALE-Konferenz
Pforzheim, 09.03.-11.03.2022

Warum wir ein Security-Engineering-Informationsmodell brauchen

Motivation, Anwendungsfälle und Konzept für ein neues Domänenmodell für Security-Engineering

Emre Taştan[1], Sarah Fluchs[2,3], Rainer Drath[4]

Zusammenfassung

Security ist eine der größten Herausforderungen bei der industriellen Digitalisierung und der Einführung von Internettechnologien. Während die funktionale Sicherheit tief in die Entwicklung von Produkten oder Prozessen integriert ist, ist dies bei der Security nicht der Fall. Security-Engineering muss sich also – analog zur funktionalen Sicherheit – in den bestehenden und sich gerade stark verändernden Automation-Engineering-Prozess eingliedern, vor allem muss es aber für Automatisierungsingenieure effizient durchführbar sein. Dieser Beitrag begründet den Bedarf an einem Security-Engineering-Modell und berichtet über die laufenden Arbeiten zu den Anwendungsfällen und einem Modellierungsansatz mit AutomationML.

Stichwörter

Security, Security-Engineering, Domänenmodell, AutomationML, Anwendungsfälle, Funktionen

1 Motivation und Zielstellung

Industrielle Anlagen und Maschinen sind auf Lebenszyklen von 20 Jahren und länger ausgelegt und verfügen oftmals über keine oder schwach ausgeprägte Security-Eigenschaften, zum Beispiel unverschlüsselte und nicht-authentifizierte Kommunikation zwischen Sensoren, Steuerungen und Leitsystemen [1]. Prozess- und Fertigungsautomatisierungssysteme werden jedoch zunehmend über Internettechnologien miteinander vernetzt, was wiederum das Risiko von Schäden durch Ausfälle oder Cyberangriffe erhöht.
Eine große Herausforderung auch für moderne Anlagen ist, dass sie meist nicht aus dem Blickwinkel der Security konzipiert und errichtet wurden. Während der Bereich der funktionalen Sicherheit (Schutz von Menschen und Umwelt) seit Jahrzehnten durch weitreichende gesetzliche und normative Vorschriften reguliert ist, ist die Security in vielen Branchen, beispielsweise in der Chemieindustrie, nicht reguliert. Zwischenfälle wie Stuxnet (2010) [2] und die zunehmende Zahl von Ransomware-Vorfällen, die zu Kollateralschäden an Automatisierungssystemen führen (siehe Maersk (2017) [3], verdeutlichen die Notwendigkeit der methodischen Integration von Security in die Planung kritischer IT-Infrastrukturen einschließlich ihrer Automatisierungssysteme.

[1] Hochschule Pforzheim, Pforzheim, Wissenschaftlicher Projektmitarbeiter
[2] admeritia GmbH, Langenfeld, Chief Technology Officer (CTO)
[3] Helmut-Schmidt-Universität / Universität der Bunderwehr Hamburg, Hamburg, Doktorandin
[4] Hochschule Pforzheim, Pforzheim, Professor für Mechatronische Systementwicklung

Ein intuitiver und verbreiteter Ansatz zur Vermeidung von Security-Risiken ist der Verzicht auf Security-Maßnahmen und stattdessen die Isolation des Produktionssystems. Aber das ist weder zukunftstauglich, da die Produktion im Rahmen von Digitalisierung und Industrie 4.0 immer stärker vernetzt wird, noch wirksam, da eine Isolation beim zunehmenden Einsatz von drahtlosen Verbindungen und Wechseldatenträgern kaum durchzuhalten ist. Security ist deshalb eine der größten Herausforderungen in der industriellen Digitalisierung.

Nach heutigem Stand der Technik wird die Security üblicherweise in bestehenden Anlagen nachgerüstet. In neueren Anlagen gibt es Versuche, Security bei der Planung zu berücksichtigen – dann aber meist ganz am Ende des Prozesses, wenn die wichtigen Design-Entscheidungen bereits getroffen sind, was den Lösungsraum für die Security-Maßnahmen stark einschränkt. Künftig muss Security-Engineering ein selbstverständlicher und organischer Bestandteil des Automatisierungs-Engineering-Prozesses werden („Security by Design“). Das erfordert neue Methoden und in der Folge Veränderungen im Engineering, analog zur Etablierung der funktionalen Sicherheit in der Vergangenheit. Damit derartige Methoden von der Industrie akzeptiert werden, müssen das Security-Engineering und das klassische Automatisierungs-Engineering zusammenwachsen und für die beteiligten Automatisierungsingenieure gemeinsam effizient durchführbar sein.

Wie solch ein integrierter Automation-Security-Engineering-Prozess aussehen kann und wie ein Security-Domänenmodell im Engineering und auch in der späteren Betriebsphase helfen kann, diesen Prozess für Automatisierungsingenieure alltagstauglich zu machen, untersucht das Forschungsvorhaben IDEAS „Integrated Data Models for the engineering of Automation Security“ (FKZ: 16KIS1269K). Das vom Bundesministerium für Bildung und Forschung geförderte Forschungsvorhaben wird von der admeritia GmbH in Kooperation mit der Hochschule Pforzheim durchgeführt. Als weitere assoziierte Partner unterstützen die INEOS Manufacturing Deutschland GmbH, die HIMA Paul Hildebrandt GmbH & Co KG sowie der NAMUR e. V.

Das Ziel des Forschungsvorhabens ist "Security by Design". Dafür wird ermittelt, in welchen Phasen des bestehenden Automatisierungs-Engineerings security-relevante Informationen für ein elektronisches Informationsmodell systematisch erfasst werden können. Es werden bestehende Workflows untersucht, ein Security-Domänenmodell sowie Software-Werkzeuge entwickelt. Zielgruppe sind Automatisierungs- bzw. Leittechnikingenieure, die befähigt werden sollen, Security bei der Entwicklung und Pflege ihrer Systeme im Sinne von „Security by Design“ direkt zu berücksichtigen.

Ausgangspunkt ist ein vom Projektpartner admeritia GmbH erarbeiteter Ansatz zur Strukturierung des Security-Engineering-Prozesses. Um bestehende Vorgehensweisen vergleichen und einordnen zu können, wurde das in Bild 1 dargestellte methodenneutrale Prozessmodell für das Security-Engineering entwickelt. Es besteht von unten nach oben aus den vier aufeinander aufbauenden Ebenen, in die sich bestehende Vorgehensweisen einordnen lassen. Die vier Ebenen sind wie die Ebenen eines Turms: keine Ebene funktioniert ohne die darunterliegende. Der Turm beschreibt ein allgemeines Security-Engineering-Prozessmodell für den gesamten Security-Engineering-Prozess: Ausgehend von der Identifikation schutzbedürftiger Funktionen (FC) werden Risiken (RI) abgeleitet, Security-Anforderungen (RE) gegen diese Risiken definiert und in einer Security-Lösung (IM) implementiert. [4]

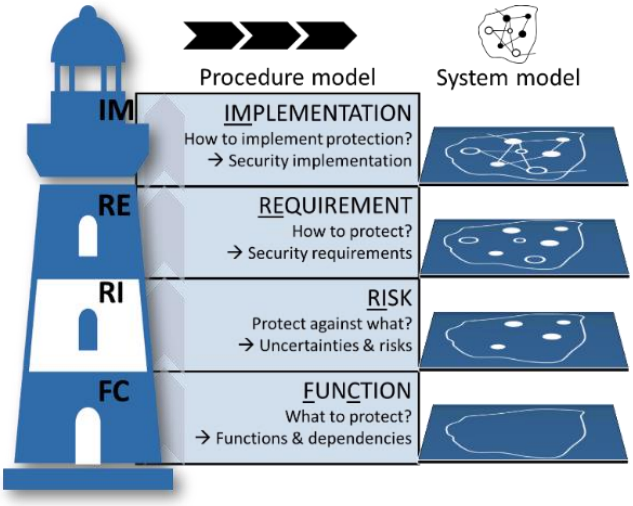

Bild 1: Allgemeines Prozessmodell für Security-Engineering [4]

Die verschiedenen in der Automatisierungstechnik verwendeten Security-Risikoanalyse- oder Systems-Security-Engineering-Methoden lassen sich alle entlang der vier Ebenen des Prozessmodells einordnen, sodass keine Entscheidung für oder gegen

einen bestehenden Standard getroffen werden muss – daher die Bezeichnung des Modells als „methodenneutral“. [4]
Im Rahmen dieses Beitrags werden die Autoren die Anforderungen an ein Security-Domänenmodell, dessen Systemmodellierung sowie einen Ansatz für ein konkretes Modell für die erste Ebene des Turmes (FC) mit einer Bibliothek und Beispielen beschreiben. Die anderen Ebenen sind Gegenstand zukünftiger Arbeiten.

2 Anwendungsfälle für ein Security-Engineering-Domänenmodell

In diesem Kapitel werden vier Anwendungsfälle (Use Case, UC) für ein elektronisches, das heißt maschinenles- und verarbeitbares Security-Engineering-Domänenmodell beschrieben. Diese Anwendungsfälle stellen die Basis für die Anforderungsanalyse an das Domänenmodell dar.

UC1: Informationsaustausch zwischen security-relevanten Planungswerkzeugen
Security-Informationen finden sich keineswegs nur in Security-Werkzeugen. Vielmehr können eine große Zahl von Informationen und Werkzeugen als „security-relevant“ bezeichnet werden. Da Security ein interdisziplinäres Gebiet ist, das sich mit vielen anderen Disziplinen überschneidet oder diese tangiert, finden sich diese security-relevanten Informationen in vielen verschiedenen, meist untereinander inkompatiblen Entwicklungsphasen und Softwarewerkzeugen. Informationen, die eigentlich zentral gesucht, analysiert und korreliert werden sollten, sind somit über viele Datensilos verteilt. Security-relevante Informationen gibt es in IT-Administrationstools, wie Asset-Inventare, Konfigurationsmanagement- oder Versionierungstools, in dedizierten Security-Tools wie Anomalieerkennungs- oder Intrusion-Detection-Systemen, aber auch in Engineeringwerkzeugen, die Risikobetrachtungen oder architekturelle Entscheidungen enthalten.
Es ist unwahrscheinlich, dass diese verschiedenen Werkzeuge ihre Datenformate in absehbarer Zeit harmonisieren werden, weshalb ein neutrales Informationsmodell die pragmatischere Lösung zu sein scheint. Mit so einem neutralen Informationsmodell kann jedes beteiligte Werkzeug seine relevanten Informationen (einschließlich Identifikations-, Versions-, Semantik- und Typinformationen) exportieren, während seine interne Datenverarbeitung unverändert bleibt.
Genau das gleiche Problem, nur für Engineeringwerkzeuge für die Automatisierung und nicht für die Security, war der Grund, warum AutomationML als Datenformat für den Austausch von Engineering-Informationen entwickelt wurde. Damit ist es ein natürlicher Kandidat für die Modellierung und den Austausch auch von Security-Engineering-Informationen zwischen inkompatiblen Werkzeugen.
UC2: Aufrechterhaltung der Security während des Betriebs
Mit der Möglichkeit, Informationen zwischen security-relevanten Werkzeugen digital auszutauschen, besteht die Aussicht auf ein effizientes Security-Management im laufenden Betrieb einer Produktionsanlage. Mindestens zwei Teilanwendungsfälle sind relevant:

- **UC 2.1:** Effizienzgewinne im Betrieb von Security-Lösungen ergeben sich oft aus der Standardisierung von Komponenten und ihren Konfigurationen. Diese Standards müssen maschinenverarbeitbar gespeichert, gepflegt und verwaltet werden. Selten deckt ein Tool alle relevanten Informationen ab. Solche Standardkonfigurationen über viele Tools verteilt zu speichern und zu pflegen ist jedoch fehleranfällig und ineffizient.
- **UC 2.2:** Die Lebenszyklen von Security-Lösungen sind kürzer als die der meisten Produktionssysteme, denn neue Bedrohungen und Schwachstellen können in Abständen von Tagen oder Wochen auftreten. Daher ist es oft notwendig, die Security-Einstellungen während des Anlagenbetriebs anzupassen – unabhängig davon, ob die Komponenten standardisiert sind oder nicht. Security-Entscheidungen wie das Patchen einer Schwachstelle oder das Anwenden einer Alternativmaßnahme für Schwachstellen, für die kein Patch verfügbar ist, erfordern jedoch Kontextinformationen aus

typischerweise verschiedenen Quellen. Relevant sind zum Beispiel der Schweregrad der Schwachstelle, die bestehenden Risiken und frühere Vorfälle für eine Komponente, die Kritikalität des Versagens oder der Manipulation der Komponente, die Netzwerkexposition der Komponente und die Kritikalität der daran angeschlossenen Komponenten. Diese Informationen sind jedoch wahrscheinlich an verschiedenen Orten gespeichert und müssten zeitaufwändig gesammelt und verarbeitet werden - sofern sie überhaupt verfügbar sind. Ein Informationsmodell hilft, alle security-relevanten Engineering-Informationen auch in der Betriebsphase noch parat zu haben.

UC3: Visualisierungen und modellbasiertes Security-Engineering

Dem Security-Engineering fehlen nicht nur ein Informationsmodell, das von Computern verarbeitet werden kann, sondern auch Diagramme und Visualisierungen, die Menschen helfen, die Security-Probleme des betrachteten Systems wirklich zu verstehen und die Lösungen systematisch zu durchdenken. Solche Visualisierungen sind notwendig, da für Security-Engineering Informationen aus einer Vielzahl von technischen Disziplinen verwendet werden, z. B. Netzwerkpläne, Gebäude- und Standortpläne, Analyseergebnisse der funktionalen Sicherheit oder Softwarespezifikationen für Kontrollsysteme – und diese Informationen müssen oft in Kombinationen oder Abstraktionsebenen dargestellt werden, die für andere Ingenieurdisziplinen nicht relevant sind.

Auch die Security fügt ihre eigenen Informationen hinzu. Ein Beispiel ist die Rolle des Menschen, die in anderen technischen Modellen selten dargestellt wird. Darunter fällt die Interaktion von Menschen mit Systemkomponenten und von Komponenten mit anderen Komponenten. All dies erfordert neu gestaltete Visualisierungen aus verschiedenen Perspektiven, die manuell nur mühsam zu erstellen wären, aber aus einem Informationsmodell, das alle Security-relevanten Informationen an einem Ort enthält, leicht zu generieren sind.

Der Mangel an effizienten Visualisierungen für Security-Engineering-Modelle ist nach Ansicht der Autoren einer der Hauptgründe, warum modellbasiertes Security-Engineering, das stark auf die Betrachtung verschiedener Perspektiven und Detaillierungsgrade von security-relevanten Informationen und deren Auswertung während des Security-Engineering-Prozesses angewiesen ist, derzeit schnell als „in der Praxis zu aufwendig“ gilt.

UC4: Integration von Security in den Prozess der Automatisierungstechnik - "Security by Design"

Es ist von Vorteil, bereits in der Engineering-Phase (und allen späteren Re-Engineering-Phasen) über ein Security-Engineering-Informationsmodell zu verfügen. Wie eingangs erwähnt, wird das Thema „Security“ bislang oft erst ganz am Ende des Engineering-Prozesses einer automatisierten Anlage betrachtet, nur für einzelne Teile der Anlage, oder sogar erst nach der Inbetriebnahme einer Anlage.

In jedem Fall hat Security-Engineering auf diese Weise keinen Einfluss auf allgemeine Konstruktionsentscheidungen und kann lediglich noch auf die Security-Risiken einer fertig entworfenen Anlage reagieren. Dies führt unweigerlich dazu, dass Security als schlechter Kompromiss im Nachhinein die Komplexität erhöht oder die Nutzbarkeit des Systems einschränkt, während wünschenswerte Security-Lösungen das Gegenteil bewirken würden.

Solche wünschenswerten Lösungen erfordern jedoch oft grundlegende Designänderungen, wie z. B. die Neugestaltung der Netzwerkarchitektur. Diese Änderungen sind nicht mehr durchführbar, wenn das Engineering einer Anlage bereits abgeschlossen ist. Security-Engineering beginnt auch deshalb zu spät im Automation-Engineering-Prozess, weil Security-Fachleute keine guten Antworten auf die Frage haben, welche Informationen sie von den anderen relevanten Ingenieurgewerken bei der Planung einer Anlage benötigen – also was eigentlich „security-relevante“ Informationen sind. Security-Ingenieure haben im Gegensatz zu vielen anderen Disziplinen bislang kein gemeinsames, bewährtes Modell, das ihnen beim Denken hilft [4] – und schon gar keine Visualisierung dessen (siehe UC3). Sie können nirgendwo alle Informationen speichern, die relevant sein könnten, diese mit ihren eigenen security-spezifischen Informationen ergänzen und diese als Grundlage für die frühzeitige Kommunikation von Security-Anforderungen an andere Gewerke nutzen.

3 Stand der Technik

Zur speicherbaren und elektronisch verarbeitbaren Beschreibung eines Security-Domänenmodells haben sich die Autoren für die standardisierte Beschreibungssprache **AutomationML (AML)** entschieden, da AutomationML seine Fähigkeit zur Beschreibung von Domänenmodellen bereits in verschiedenen industriellen Domänen nachgewiesen hat [5] [6]. Die Zielsetzung von AutomationML – ein einheitliches Informationsmodell für verschiedene Ingenieurdisziplinen bei der Entwicklung einer automatisierten Anlage – passt sehr gut zur Zielsetzung, Security-Engineering in die bestehenden Engineeringprozesse anderer Ingenieurdomänen zu integrieren und Interoperabilität der Security-Engineering-Informationen mit bestehenden Planungsdaten zu gewährleisten.
Zudem eignen sich AML-Modelle hervorragend als Teilmodell und somit **Datenlieferant für Verwaltungsschalen**. Die Verwaltungsschale ist eine digitale Repräsentation jedes industriellen Assets innerhalb eines „Industrie 4.0"-Netzes. Sie stellt ein standardisiertes, maschineninterpretierbares Informationsmodell eines Geräts, mit relevanten Parametern, Schnittstellen etc., dar [7]. Die Kompatibilität mit der Verwaltungsschale ist ein relevanter Aspekt für die Zukunftstauglichkeit des Security-Domänenmodells und für die langfristige Erfüllung der o.g. Anwendungsfälle ein.
In AML gibt es einige Ansätze, auf denen das neu zu entwickelnde Security-Domänenmodell aufbauen kann. AML besitzt bereits eine große Anzahl von Informationsmodellen für die **Modellierung von Teilaspekten automatisierter Systeme** wie Topologie, Geometrie, Dokumentation, Vernetzung, sogar Icons, elektrische/pneumatische/hydraulische Schnittstellen oder Logik. Sie können so detailliert sein, dass sie sich für die Modellierung elektronischer Produktkataloge eignen [8]. Für das Security-Domänenmodell ist hinsichtlich vieler Teilaspekte ein weitaus geringerer Detailgrad vonnöten.
Für Security besonders relevant ist allerdings die **Modellierung von Kommunikationsbeziehungen**. Es existieren bereits AML-Modellierungsempfehlungen für Kommunikationsnetzwerke [9], d.h. von Gerätesystemen und ihren physischen und logischen Verbindungen. Diese Aktivität befindet sich derzeit auf dem Weg zur Standardisierung als Teil 1 und 5 im Rahmen der AutomationML-Reihe IEC62714. Diese Ansätze zur Modellierung von Netzwerken sind vielversprechende Kandidaten für die Modellierung von Netzwerken aus Security-Perspektive. Bereits 2019 haben Fluchs et al. basierend auf dieser AML-Modellierung von Kommunikationsbeziehungen einen ersten Ansatz für ein **Security-Systemmodell in AML** vorgestellt und offene Modellierungsprobleme herausgearbeitet [10]. Eine Analyse, der für das Security-Engineering zu modellierenden Informationen und Vorschläge für ihre Abbildung in der Verwaltungsschale ist in [11] erfolgt.
Eine dieser offenen Modellierungsfragen ist die Beschreibung von Funktionen beziehungsweise von Interaktionen zwischen Systemkomponenten zur Erfüllung einer bestimmten Funktion. Dazu gibt es mit der **Modellierung von Produkt-, Prozess- und Ressourcendomänen („PPR-Konzept")** ein Konzept zur Erleichterung der Generierung von Prozessabläufen und Systemkonfigurationen [5].
Mit **AMLsec** existiert ein umfassendes AML-Modell, um eine **Risikobetrachtung nach ISA/IEC 62443-3-2** [12] durchzuführen, entwickelt von Eckhart et al. [13]. AMLsec erweitert existierende AML-Bibliotheken, sodass bestehende Engineering-Informationen durch security-relevante Informationen wie Security-Geräte und Security-Konfigurationen erweitert werden. Der Schwerpunkt des Modells liegt auf der Modellierung der Semantik ab dem Beginn der Risikoanalyse (Ebene 2 des Security-Engineering-Prozessmodells aus Kapitel 1), weniger auf der Modellierung des darunterliegenden Systems aus Security-Perspektive, die den Schwerpunkt des vorliegenden Beitrags bildet. Auch beinhaltet das AML Modell AMLsec sehr spezifische Konzepte der ISA/IEC 62443, beispielsweise „Zones und Conduits". Eine Security-Analyse mit anderen Methoden auf Basis des Modells erscheint möglich, würde aber einige Anpassungen erfordern.
Glawe et al. [14] nutzen das AML zugrundeliegende Datenformat CAEX, um **security-relevante Engineeringdaten** für die Nutzung in ihrer Security-Ontologie einzulesen. Die vorgeschlagene Ontologie für die Security-Domäne beinhaltet jedoch keine AML-Modellierung, wenngleich die Autoren einen Export ihrer OWL-basierten Ontologie in AML erwägen.

4 Konzept für ein Domänenmodell

Für die effiziente Integration von Security- und Automatisierungs-Engineering ist ein maschinenlesbarer Datenaustausch zwischen relevanten Werkzeugen erforderlich. Basierend auf Kapitel 2 und 3 stellen die Autoren in diesem Abschnitt eine Reihe von Anforderungen (A1 – A4) an das Security-Domänenmodell auf. Anschließend werden Ansätze zur Erfüllung dieser Anforderungen dargelegt.

4.1 Anforderungen an das Domänenmodell

A1 – objektorientierteres, interoperables Systemmodell:
Das Security-Domänenmodell soll ein objektorientiertes Systemmodell sein. Zugleich soll die Austauschbarkeit der Informationen mit anderen Domänen gewährleistet sein.
A2 – Abstraktionsgrad und Hierarchisierung:
Da so viele Informationen aus verschiedenen Domänen potenziell security-relevant sind, ist eine der wichtigsten Eigenschaften des Security-Domänenmodells die Komplexitätsreduktion. Damit das Modell aussagekräftig bleibt, muss es auf einem höheren Abstraktionsgrad angesiedelt sein als die Domänenmodelle, aus denen es Informationen bezieht. Gleichzeitig sollen Möglichkeiten zur Hierarchisierung gegeben sein, die „Drill-Downs“ auf niedrigere Abstraktionsebenen für Ausschnitte des Modells ermöglichen.
A3 - funktionaler Ansatz unter Einbeziehung des Menschen:
Security-Engineering erfordert zusätzliche Informationen zur Modellierung eines rein technischen Systems: Modellierung von Funktionen, bestehend aus Interaktionen und Kommunikation zwischen beteiligten menschlichen Rollen und IT/OT-Systemen oder IT/OT-Systemen untereinander, die zur Ausführung der Funktion erforderlich sind. Jede Funktion zeigt den Teil des Systems, der für die Erfüllung eines bestimmten Zwecks relevant ist. Damit bilden sie eine Einheit aus technischen Komponenten, Menschen, Interaktion und Kommunikationsverbindungen, die für weitere Security-Analysen gut geeignet ist [15]. Um Eigenschaften von Objekten in einer Funktion modellieren zu können, werden Attribute spezifiziert. In diesen kann bspw. eine Verbindung zum Risiko (Prozessmodell: RI) hergestellt werden, indem eine Beschreibung der Wahrscheinlichkeit und die Konsequenz der Bedrohung bzw. des Schadens aufgelistet wird. Zudem ist der Zielgruppe des Domänenmodells, Automatisierungsingenieuren in der Prozessindustrie, ein funktionsbasierter Ansatz vertraut – beispielsweise durch Funktionsblöcke in der Steuerungsprogrammierung oder Leitsystemparametrierung [16] oder durch Safety-Funktionen (SIFs) in der funktionalen Sicherheit [17].
A4 – vordefinierte Bibliotheken für Funktionen:
Im Sinne der Wiederverwendung kann eine zusätzliche Bibliothek für die wichtigsten Funktionen des Systems aufgebaut werden. Damit werden alle notwendigen Informationen wie betroffene Entitäten aus dem Netzwerk, Verantwortliche, Rollen sowie die Zugehörigkeit von Risikoszenarien (Hinführung zu der Ebene RI in Bild 1) für eine Funktion als Vorlage in AutomationML beschrieben. Zudem erscheint es sinnvoll, in solch einer Bibliothek bereits etablierte Funktionsvorschläge abzulegen.

4.2 AutomationML-Modellierungsansatz

Wie in Kapitel 3 beschrieben, kann mit AutomationML die Struktur oder Topologie eines Systems modelliert werden. Dazu gehört die Hierarchie von Objekten, die jeweils durch einzelne Datenobjekte dargestellt werden, sowie ihre Zusammenhänge bzw. Verbindungen. AutomationML bietet umfangreiche objektorientierte Modellierungskonzepte, die für die Beschreibung von Anlagenstrukturen verwendet werden: dies erfüllt die **Anforderung A1**. Um dies zu verdeutlichen, wird als Beispiel ein vereinfachtes Netzwerk (Bild 2) für die Anforderungen aufgeführt.

Bei der Modellierung kommt das von AutomationML empfohlene Konzept zur Modellierung von Kommunikationsnetzwerken zum Einsatz. Dafür stellt AutomationML Bibliotheken für Kommunikationsnetzwerke zur Verfügung. Mithilfe der Bibliotheken aus der IEC 62714-5 können physische sowie logische Geräte und Verbindungen dargestellt werden.
Die Rollenklassen aus der *CommunicationRoleClassLib* beschreiben abstrakte Objekte, ohne dabei deren technische Realisierung festzulegen – dies ist wichtig für die Erfüllung von **Anforderung A2**.
Physikalische/logische Netzwerke, Geräte sowie Verbindungen werden in der Bibliothek abgedeckt. Dennoch werden nicht alle Objekte aus Bild 2 beschrieben. Die Autoren schlagen eine neue Rolle „HumanRole“ vor, um das Beispiel modellieren zu können. Die *CommunicationInterfaceClassLib* bietet die Klassen für die Schnittstellen. Die Interfaceklasse beschreibt die abstrakte physische oder logische Relation zwischen zwei Elementen oder die Referenz auf eine Information. Somit können Kommunikationsgeräte über ihre Steuerungsanwendungen Protokolle oder Daten direkt miteinander austauschen, auch wenn diese nicht direkt physisch verbunden sind. Auf Basis dieser Technik kann ein System auf einer höheren Abstraktionsebene modelliert werden, was zur Erfüllung von **Anforderung A2** beiträgt. In Bild 3 wird das vereinfachte System in abstrakter Form dargestellt. Um die vorgestellten Vorschläge umzusetzen, werden spezialisierte Bibliotheken erstellt, die von der IEC 62714-5 abgeleitet sind. Bild 4 und 5 zeigen den aktuellen Stand.
Im vereinfachten Netzwerk aus Bild 2 kann eine Funktion abgeleitet werden, wie beispielsweise, dass das Personal über das tragbare Programmiergerät „Laptop“ das physikalische Gerät „Sensor“ auslesen kann. Bei der Strukturierung solcher Systeme hat sich in der Praxis der AutomationML die Dreiteilung der Daten in Ressourcen, Prozesse und Produkte bewährt, die auch als PPR-Konzept bezeichnet wird [6]. Dies ist eines der Konzepte, das Mittel zur Darstellung der Modellierung der Funktionen in **Anforderung A3** bietet.

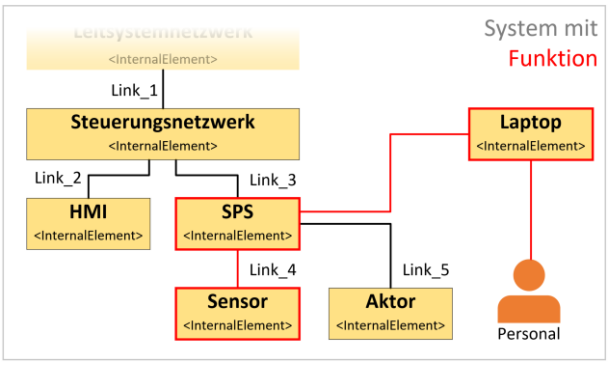

Bild 2: Darstellung eines vereinfachten Systems (vgl. [4])

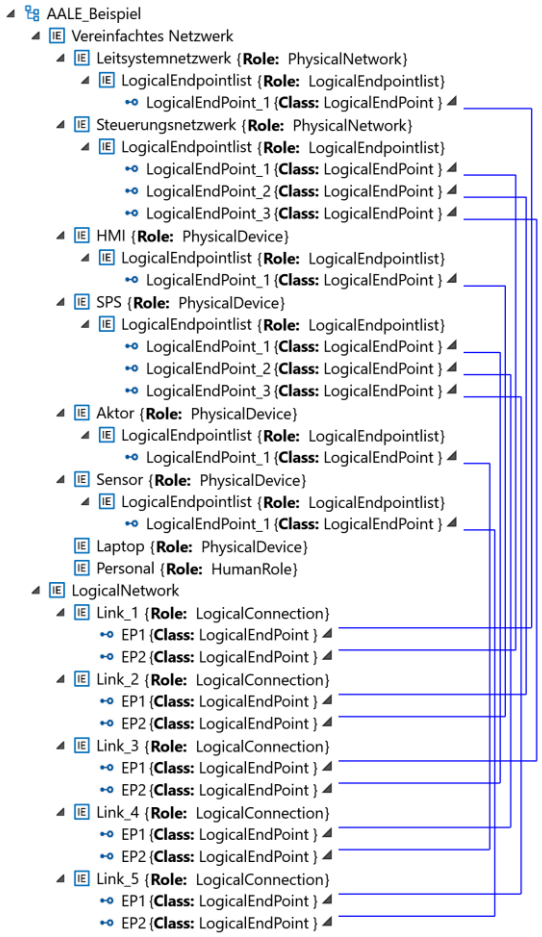

Bild 3: Abstrakte Darstellung des vereinfachten Systems

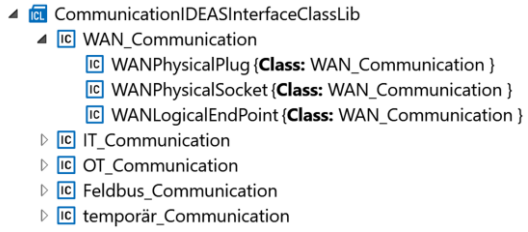

Bild 4: Abgeleitete Schnittstellenbibliothek

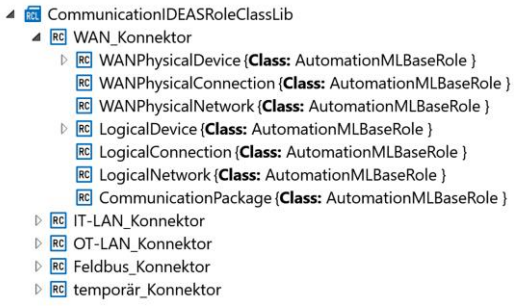

Bild 5: Abgeleitete Rollenbibliothek

Das klassische PPR-Konzept kann jedoch eine Funktion, die ausschließlich durch Maschine-zu-Maschine-Kommunikation aufgebaut ist, nicht darstellen. Folglich kann das PPR-Konzept Produkt sowie Ressource nicht unterscheiden. Daher schlagen die Autoren eine Erweiterung des PPR-Konzeptes aus der *AutomationMLBaseRoleClassLib* für das Security-Domänenmodell vor.
Folgende Rollen werden benötigt: Sender, Prozess und Receiver (siehe Bild 6) und die Schnittstelle: SPRConnector. Ein Sender führt einen Prozess am Receiver (Empfänger) durch – damit ergibt sich ein abgewandeltes „*SPR-Konzept*“.
Mit diesem Konzept können die Funktionen wie einfache Sätze gelesen werden: "Techniker liest Messwert von Sensor aus". Jeder Satz besteht aus einem „Interaktionsdreieck“ aus Sender (im Beispiel: Techniker), Prozess (liest Messwert aus) und Receiver (Sensor). Damit kann eine Funktion mit ihren Objekten und Rollen aus drei Blickrichtungen betrachtet werden. Jede Sicht kann dem Benutzer eine zugehörige Darstellung zeigen, wie die verknüpften „Interaktionsdreiecke“ aufgebaut sind. Mithilfe des Sequenzdiagramms in Bild 7 können die Elemente aus der Dreiteilung des SPR-Konzeptes für die Modellierung einer Funktion dargestellt werden. Ein Pfeil mit den jeweiligen zwei betroffenen Objekten stellt ein Dreieck (maximal sechs in Bild 7) aus dem SPR-Konzept dar. Die Sequenzdiagrammdarstellung bietet eine Alternative zur Netzmodelldarstellung in Bild 2. Im Gegensatz zu Bild 2 kann im Sequenzdiagramm die genaue Reihenfolge der Interaktionen abgebildet werden.

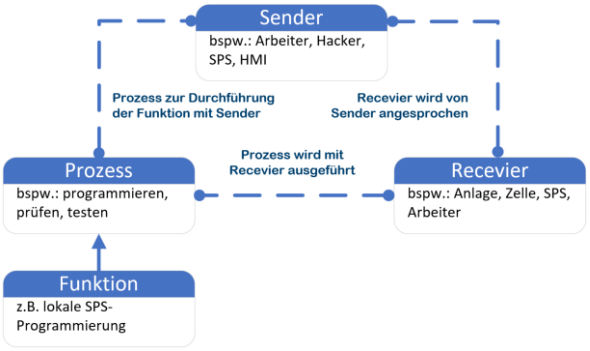

Bild 6: SPR-Konzept - Überblick über die Rollen: Sender, Prozess und Receiver

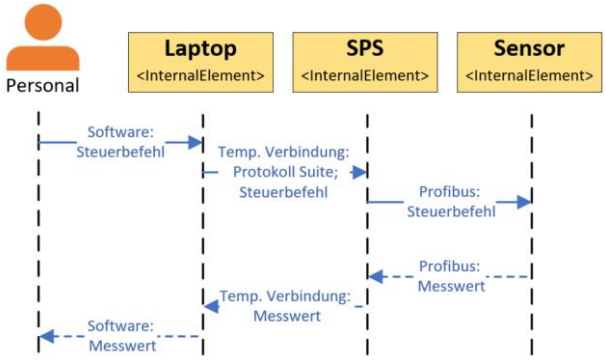

Bild 7: Sequenzdiagrammdarstellung einer Funktion

Die Modellierung der Reihenfolge der „Interaktionsdreiecke“ in AML wird mit der InterfaceClass „Order“ realisiert. Somit werden in der Funktion die Interaktion und Kommunikation zwischen allen beteiligten Entitäten aufgelistet, dass die **Anforderung A3** erfüllt. Dennoch ist bei der Darstellung des Sequenzdiagramms zu unterscheiden, ob die Modellierung aus der physischen oder logischen Ebene entnommen wird, da in der logischen Verbindung nicht alle Entitäten gelistet sind.
Um eine Basis für die Informationsmodellierung von Funktionen bereitstellen zu können, wird eine Bibliothek, wie in **Anforderung A4** aufgeführt, beschrieben. Diese Bibliothek enthält Funktionen, Entitäten (ggf. menschlich), Prozesse, Rollen sowie Attribute und stellen die Grundlage für die Modellierung des Systemmodells und der Funktionen dar. Ein Ausschnitt aus der Funktionsbibliothek kann aus Bild 8 entnommen werden. Eine Beschreibung sowie zusätzliche Informationen sind in den jeweiligen Funktionsobjekten enthalten. Darüber hinaus werden Attribute wie eine sprechende ID, Auswirkung bei Beeinträchtigung der Verfügbarkeit, Integrität oder Vertraulichkeit der Funktion, menschliche Interaktion und Information, in welcher Netzwerkebene sich das Objekt befindet, vergeben. Darüber hinaus werden in der Funktion alle betroffenen Objekte aufgelistet. Die verantwortliche Person für die Funktion wird unter „*Responsible*“ abgebildet.

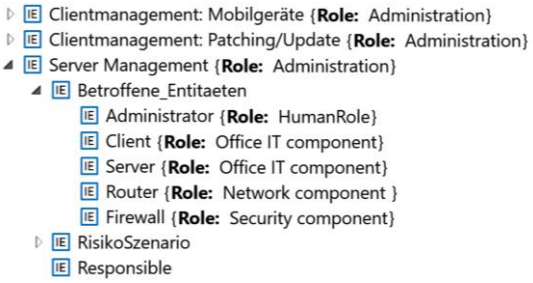

Bild 8: Ausschnitt - Funktionsbibliothek

Damit ein Übergang in die noch zu modellierende Risikoanalyse der Ebene RI des Security-Engineering-Prozessmodells (siehe Bild 1) gewährleistet werden kann, werden Risikoszenarien mit der Funktion durch InternalLinks verknüpft. Mittels des Konzeptes der Rollenbibliotheken kann einzelnen Objekten in der SystemUnitClassLibrary eine bestimmte Semantik zugeordnet werden. Hierfür wurde eine zusätzliche Rollenbibliothek erstellt, die in Bild 9 abgebildet ist. Mithilfe der Bibliothek kann der Abstraktionsgrad für **Anforderung A2** in weiteren Kategorien klassifiziert werden.

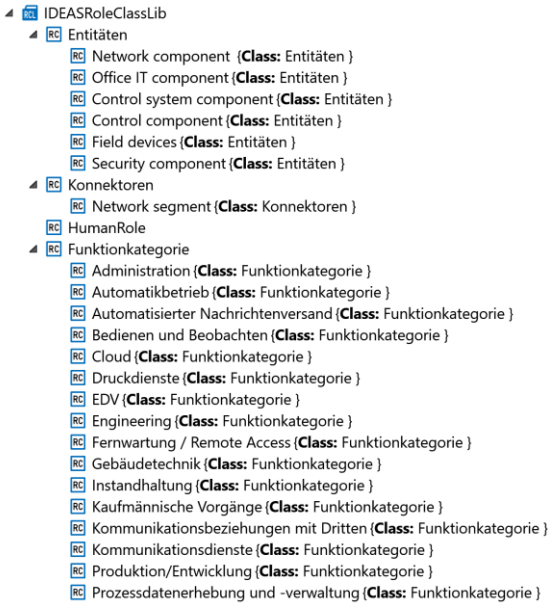

Bild 9: Zusätzliche Rollenbibliothek – Semantik für Entitäten im Modell sowie für Funktionen

5 Zusammenfassung und Ausblick

Die vorgestellten Ansätze verstehen sich als erster Schritt, um die Workflows von Security- und Automation-Engineering elektronisch zu verweben, indem die security-relevanten Informationen der zu schützenden Systeme in einem Informationsmodell abgebildet werden. Damit ist die Grundlage für die Durchführung einer Security-Analyse, also die Ableitung von Risiken, Security-Anforderungen und Security-Lösungen, modelliert. Dies ist der erste Schritt zu einem elektronischen Domänenmodell für das Security-Engineering. So ein Domänenmodell ist neu und ein schlagkräftiger digitaler Enabler für „Security by Design“. Ein elektronisches Denkmodell eröffnet umfassende Möglichkeiten des digitalen Security-Engineerings: digitaler Datenfluss zwischen security-relevanten Planungswerkzeugen, Änderungsmanagement, automatische Konflikterkennung und Konsistenzprüfung auch während des Betriebs, neuartige Assistenzsysteme für Security-Engineering, Impact-Analyse, Mustererkennung und Musterlösungen.

Die Integration von security-relevanten Informationen in maschinenlesbare, maschinenverarbeitbare und maschinen-verständliche Informationsmodelle wie AutomationML, die bereits im Bereich der Automatisierungstechnik verwendet werden, ist ein wichtiger Schritt zur Integration von Security in den gesamten Prozess der Automatisierungstechnik. AutomationML war bereits Grundlage für eine Vielzahl von Domänenmodellen in der Industrie und ist als Teilmodell der Industrie 4.0 Verwaltungsschale direkt im Fahrwasser der Engineering-Digitalisierung eingebettet. Allerdings sind noch diverse Probleme zu lösen:

- Bisher haben die Autoren Modellierungsempfehlungen (Basis für das Security-Modell) für das zu schützende System gemacht. Die Modellierung der nächsten Schritte im Security-Engineering-Prozess (Risiken, Anforderungen und Implementierung) bleibt ein offenes Thema, das unter Berücksichtigung bestehender Arbeiten zu diesem Thema als nächstes behandelt werden soll.
- Um das Security-Engineering wirklich in den Prozess des Automation-Engineering zu integrieren, müssen security-relevante Informationen und Entscheidungen im bestehenden Automation-Engineering-Prozess identifiziert und in das Security-Engineering-Modell aufgenommen werden. Diesbezügliche Forschung wird derzeit von den Autoren auf der Grundlage bestehender Arbeiten wie [18], von Vorgehensmodellen des Automation-Engineering wie [19] [20] sowie von den assoziierenden Partner INEOS Manufacturing Deutschland GmbH und der HIMA Paul Hildebrandt GmbH & Co KG durchgeführt.
- Das Informationsmodell, in diesem Beitrag in AutomationML modelliert, wird im Rahmen des oben genannten Forschungsprojektes in Zusammenarbeit mit dem NAMUR-Arbeitskreis 1.3 ebenfalls als UML-Modell modelliert. Als weiteres Ergebnis dieses Arbeitskreises wird ein Teilmodell der Verwaltungsschale für Security-Engineering definiert werden.

– Damit das Informationsmodell für Automatisierungsingenieure im Alltag nutzbar ist, werden grafische Notationen erstellt, die die Informationen effizient von Menschen verarbeitbar machen. Ein Software-Demonstrator wird das Befüllen und Pflegen des Datenmodells erleichtern.

Literatur

[1] BMWi, „Der IT-Sicherheitsmarkt in Deutschland: Grundstein für eine makroökonomische Erfassung der Branche.," 2013.

[2] K. Zetter, „Countdown to Zero Day: Stuxnet and the launch of the world's first digital weapon, First Edition," Crown Publishers, 2014.

[3] G. Ashton, „Maersk, me & notPetya," [Online]. Available: https://gvnshtn.com/maersk-me-notpetya/ (accessed 06.16.21).

[4] S. Fluchs und H. Rudolph, „Wie OT-Security-Engineering eine Ingenieurwissenschaft wird - Ein Denkmodell und ein Datenmodell," atp magazin, 2019.

[5] „DIN EN 62714-1: Datenaustauschformat für Planungsdaten industrieller Automatisierungssysteme - Automation markup language - Teil 1: Architektur und allgemeine Festlegungen," 2018.

[6] R. Drath (Ed.), AutomationML – The Industrial Cookbook, Berlin: De Gruyter Oldenbourg, 2021.

[7] R. Drath, S. Malakuti, S. Grüner, J. Grothoff, C. Wagner, U. Epple und M. Hoffmeister, „Die Rolle der Industrie 4.0 „Verwaltungsschale" und des „digitalen Zwillings" im Lebenszyklus einer Anlage - Navigationshilfe, Begriffsbestimmung und Abgrenzung," VDI-Verlag - Tagungsband zur Automation 2017, Baden-Baden, 2017.

[8] M. Rentschler, R. Drath, J. Hinze und A. Gatterburg, „AutomationML als generische Beschreibungssprache für den Digitalen Zwilling," VDI-Verlag, Baden-Baden, 2019.

[9] „DIN EN 62714-5: Datenaustauschformat für Planungsdaten industrieller Automatisierungssysteme - Automation markup language - Teil 5: Kommunikation," 2020.

[10] S. Fluchs, N. Schmidt und A. Mendl-Heinisch, „Ein Systemmodell für Security-Engineering," TeSi, vol. 9, no. 11–12, 2019.

[11] S. Fluchs, „On Modelling for Security Engineering. fluchsfriction 37," 2021.

[12] „ISA/IEC 62443-3-2: Security for industrial automation and control systems - Part 3-2: Security risk assessment for system design," 2020.

[13] M. Eckhart, A. Ekelhart und E. R. Weippl, „Automated Security Risk Identification Using AutomationML-based Engineering Data," IEEE Trans. Dependable and Secure Comput., 2020.

[14] M. Glawe, C. Tebbe, A. Fay und K.-H. Niemann, „Knowledge-based Engineering of Automation Systems using Ontologies and Engineering Data," in: Proceedings of the 7th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management. Presented at the 7th International Conference on Knowledge Engineering and Ontology Development, SCITEPRESS, Lisbon, Portugal, 2015.

[15] S. Fluchs, „For security, think functions - not systems," 2020. [Online]. Available: https://fluchsfriction.medium.com/for-security-think-functions-not-systems-b0e08a9d89b6.

[16] „DIN EN 61131: Speicherprogrammierbare Steuerungen," Beuth Verlag GmbH, 2004.

[17] „DIN EN 61511: Funktionale Sicherheit - PLT-Sicherheitseinrichtungen für die Prozessindustrie," Beuth Verlag GmbH, 2019.

[18] C. Tebbe, K.-H. Niemann und A. Fay, „Ontology and life cycle of knowledge for ICS security assessments. Presented at the 4th International Symposium for ICS & SCADA Cyber Security Research 2016," 2016.

[19] NAMUR (Ed.), „NA35: Engineering and execution of PCT projects in process industry," 2019.

[20] M. Hollender, „Collaborative process automation systems," ISA, Research Triangle Park, NC, 2010.