Abschlussbericht zum BMBF-Forschungsprojekt

Vorhabendbeschreibung	IDEAS - Integrated Data Models for the engineering of Automation Security
Förderkennzeichen	16KIS1269K
Projektkonsortium	**admeritia GmbH** (KMU + Konsortialführer) **Hochschule Pforzheim** (Forschungseinrichtung) **INEOS Manufacturing Deutschland GmbH** (assoziierter Anwendungspartner) **HIMA Paul Hildebrandt GmbH** (assoziierter Anwendungspartner)
Laufzeit des Vorhabens	01.01.21-30.06.24
Autoren	Sarah Fluchs (admeritia GmbH) Matthias Müller (admeritia GmbH) Emre Taştan (Hochschule Pforzheim) Prof. Dr.-Ing. Rainer Drath (Hochschule Pforzheim)
Datum	19.12.2024

1 Kurze Darstellung zum Projekt

1.1 Motivation und Aufgabenstellung

Abbildung 1-1: IDEAS-Logo

Mit der zunehmenden Vernetzung von Industrie 4.0-Komponenten werden automatisierte Anlagen anfälliger für IT-Angriffe und Schadsoftware.
Während funktionale Sicherheit streng reguliert ist, fehlten bislang vergleichbare Vorschriften für die Cybersecurity für die Entwicklung von Anlagen. Die Implementierung von Security-Maßnahmen kann die Produktionsleistung beeinträchtigen, etwa durch reduzierte Reaktions-zeiten aufgrund von Verschlüsselung. Um das zu vermeiden, ist es wichtig, frühzeitig im Engineering-Prozess Security-Anforderungen zu definieren, um mit den funktionalen Anforderungen verträgliche Security-Maßnahmen zu finden. Security-Engineering muss also wie die funktionale Sicherheit in den Automatisierungsprozess integriert werden. Security-Maßnahmen müssen bereits in der Entwicklungsphase integriert werden, anstatt sie nachträglich hinzuzufügen. Um breite Akzeptanz zu erreichen, müssen die Security-Methoden effizient und praktikabel für Ingenieure umsetzbar sein.
Im Projekt „Integrated Data Models for the Engineering of Automation Security“ (IDEAS) wurde untersucht, wie der Security-Engineering-Prozess effektiv in den bestehenden Automatisierungs-Engineering-Prozess integriert werden kann. Die Forschungsfragen lauteten:

- Forschungsfrage 1 (Analyse): Wie kann sich Security-Engineering künftig frühestmöglich in den Engineering-Prozess einer automatisierten Anlage eingliedern?
- Forschungsfrage 2 (Datenmodellierung): Wie und in welchen Phasen des Automatisierungs-Engineerings können security-relevante Informationen in einem elektronischen Datenmodell systematisch abgebildet werden?
- Forschungsfrage 3 (Wertschöpfung): Wie kann auf Basis des Datenmodells mittels eines Engineering-Werkzeugs der Security-Engineering-Prozess effizient unterstützt werden?

Die Zielgruppe waren Automatisierungs- bzw. Leittechnikingenieure, die im Ergebnis befähigt werden sollen, Security bei der Entwicklung und Pflege ihrer Systeme im Sinne von „Security by Design“ direkt zu berücksichtigen.
Das Projekt wurde von einem Automatisierungstechnik-Hersteller und einem -Betreiber unterstützt, um die praktische Anwendbarkeit der Ergebnisse sicherzustellen.

1.2 Wissenschaftlicher und technischer Stand, an den angeknüpft wurde

Im Projekt wurde auf existierende Methoden für das Threat Modeling und die Security-Risikoanalyse aufgebaut: auf die ISA/IEC 62443-Reihe, das Threat Modeling Framework MITRE ATT&CK sowie anlagennahe OT-Security-Methoden wie das Consequence-Based, Cyber-Informed Engineering und das Security PHA Review, mit dem Ergebnisse der funktionalen Sicherheit für die Cybersecurity nutzbar gemacht werden können. Im Bereich der Datenmodelle entwickelt der AutomationML e.V. Empfehlungen für Automatisierungskomponenten und Kommunikationsnetzwerke, die als Basis verwendet wurden, um zusätzlich Security-Aspekte abzubilden.

1.3 Planung und Ablauf des Vorhabens

Das Projekt IDEAS war ursprünglich für den Zeitraum vom 01.01.2021 bis zum 31.12.2023 geplant. Aufgrund technologiebedingter Herausforderungen wurde eine kostenneutrale Verlängerung bis zum 30.06.2024 gewährt. Das Gesamtvolumen des Vorhabens betrug 1,43 Millionen Euro, wovon 69 % durch das Bundesministerium für Bildung und Forschung (BMBF) finanziert wurden. Die admeritia GmbH leitete das Projekt als Konsortialführer. Zusätzlich haben als assoziierte Anwendungspartner INEOS Manufacturing Deutschland GmbH (Betreiber) sowie die HIMA Paul Hildebrandt GmbH (Hersteller) Anforderungen und Beispieldatensätze aus der Praxis beigetragen und dem Forschungsteam ermöglicht, die Ergebnisse anhand realer Engineering-Projekte zu validieren. Dritter assoziierter Partner war die NAMUR – Interessengemeinschaft Automatisierungstechnik der Prozessindustrie e.V. Gemeinsam mit dem NAMUR-Arbeitskreis AK 1.3 Informationsmodelle hat das Forschungsteam ein UML-Datenmodell für das Security-Engineering entwickelt.

admeritia GmbH

Gesamtmittel: 1.094.873,20 €
BMBF [60 % FÖRDERQUOTE]: 656.923,92 €
EIGENANTEIL: 437.949,28 €

Hochschule Pforzheim – Gestaltung, Technik, Wirtschaft und Recht
Gesamtmittel: 340.074,81 €
BMBF [100 % FÖRDERQUOTE]: 340.074,81 €

1.4 Wesentliche Ergebnisse aus IDEAS

Forschungsfrage 1 (Analyse): Wie kann sich Security-Engineering künftig frühestmöglich in den Engineering-Prozess einer automatisierten Anlage eingliedern?
Nach eingehender Analyse der bestehenden Automation-Security-Engineering-Prozesse wurde die ursprüngliche Idee eines festen Phasenmodells, in das Security integriert wird, verworfen. Stattdessen wurde ein modellbasiertes Konzept entwickelt: Ein Anlagenmodell, das nur security-relevante Informationen enthält, wird als zusätzliche Lieferleistung von Anfang an im Engineering mitgepflegt. Es wird im Vorhinein in Form von „Security-Entscheidungspunkten“ definiert, welche Änderungen am Modell security-relevant sind – zum Beispiel Netzwerkarchitekturentscheidungen, Entscheidungen über die Funktionen von Feldgeräten oder Entscheidungen über die Detailkonfigurationen von Steuerungen. Sobald diese Entscheidungen während des Engineerings getroffen werden, werden ihre Security-Implikationen mitberücksichtigt, sie werden als Security-Entscheidungen dokumentiert und mit einer Begründung versehen.
Forschungsfrage 2 (Datenmodellierung): Wie und in welchen Phasen des Automatisierungs-Engineerings können security-relevante Informationen in einem elektronischen Datenmodell systematisch abgebildet werden?
Es wurde sowohl ein UML-Modell als auch ein AutomationML-Modell entwickelt, um security-relevante Anlageninformationen systematisch abbilden zu können.
Forschungsfrage 3 (Wertschöpfung): Wie kann auf Basis des Datenmodells mittels eines Engineering-Werkzeugs der Security-Engineering-Prozess effizient unterstützt werden?
Die Effizienz in der Security-Entscheidungsfindung kann vor allem durch Bibliotheken erhöht werden. Diese Bibliotheken ermöglichen eine schnellere Modellierung der security-relevanten Aspekte einer Anlage sowie die Wiederverwendbarkeit von Bedrohungsmodellen und Security-Entscheidungen (mitsamt Begründungen) für bestimmte Anlagenmodelle. Auf Basis der entwickelten Ergebnisse wurde ein Software-Demonstrator entwickelt, das den Security-Engineering-Prozess vereinfacht und effizient unterstützt.

2 Projektdurchführung und -ergebnisse

Im folgenden Kapitel werden anhand der bearbeiteten Arbeitspakete die im Rahmen des Projekts durchgeführten Arbeiten dargestellt. Ein Vergleich mit der ursprünglichen Projektbeschreibung ermöglicht die Nachvollziehbarkeit von Abweichungen und Anpassungen im Projektverlauf.

2.1 Übersicht der Arbeitspakete

Tabelle 2-1: Arbeitspakete

Nr.	Arbeitspaket
1	Projektmanagement, Öffentlichkeitsarbeit/Ergebnistransfer
2	Technische Voruntersuchungen und Anforderungserhebung, Pflichtenheft
3	Erweiterung des Engineering-Prozesses für Automatisierungssysteme um Security Engineering
4	Erarbeitung einer Merkmalsbibliothek für die Security-Domäne
5	Entwicklung eines AutomationML-Datenmodells
6	Entwicklung eines Demonstrators für ein Software-Werkzeug
7	Evaluation unter realen Bedingungen bei den Anwendungspartnern (INEOS, HIMA)

2.2 Einhaltung des Projektzeitplans

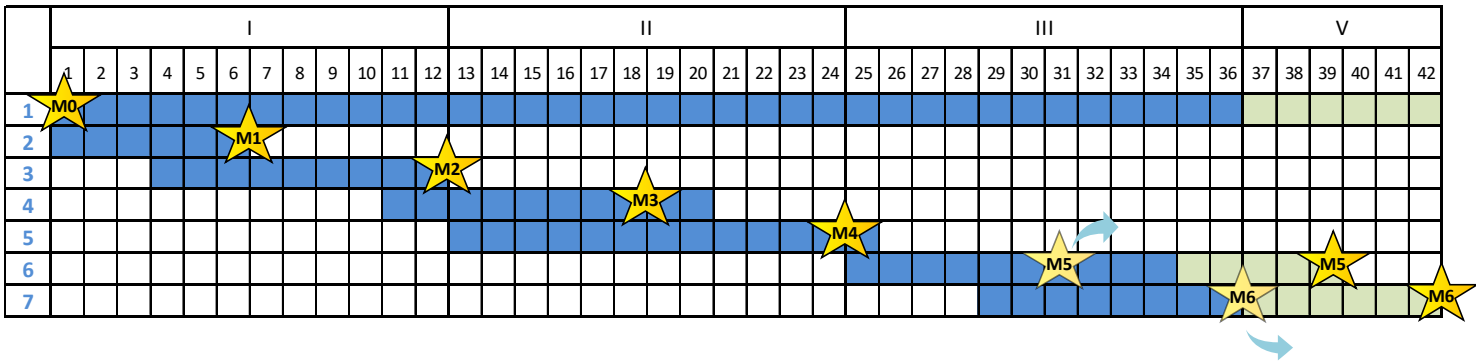

Abbildung 2-1: Zeitplan (Grüne Balken visualisieren die Kostenneutralität der Projektverlängerung)

Der dargestellte Zeitplan (siehe Abbildung 2-1) zeigt, dass die Meilensteine von M0 bis M4 wie geplant erreicht wurden. Die blauen Balken repräsentieren die ursprünglichen Phasen des Projekts, während die grünen Balken die kostenneutrale Verlängerung visualisieren. Die Meilensteine M5 (Entwicklungsarbeiten abgeschlossen und als Demonstrator umgesetzt) und M6 (Projektabschluss) haben sich durch die kostenneutrale Verlängerung nach hinten verschoben, sind aber inhaltlich erfüllt bzw. sogar übererfüllt worden: der Software-Demonstrator wurde ausführlicher validiert und in einer zusätzlichen Iteration auf Basis der Erkenntnisse der Validierung weiter verbessert werden konnte.

2.3 Ergebnisse der Arbeitspakete

2.3.1 Projektmanagement (AP 1)

Im Rahmen des Projekts hat die admeritia als Konsortialführer die Projektkoordination übernommen: Die Organisation und Leitung der regelmäßigen Projekttreffen, bei denen alle Partner – admeritia, HS Pforzheim sowie die assoziierten Partner INEOS und HIMA – zusammenkamen. Die HS Pforzheim hat das Projektmanagement für ihr Teilprojekt durchgeführt. Die assoziierten Partner INEOS und HIMA haben

standen während des gesamten Projektverlaufs für Rückfragen und Feedback zur Verfügung. Ihre Beiträge und das fortlaufende Feedback haben wesentlich zur erfolgreichen Umsetzung des Projekts beigetragen. Für die Standardisierung des Datenmodells und der enthaltenen Security-Merkmale konnten der NAMUR-Arbeitskreis 1.3 sowie die Industrial Digital Twin Association (IDTA) als Partner gewonnen werden. Die Arbeiten im NAMUR-Arbeitskreis 1.3 wurden bereits Anfang 2021 aufgenommen. Im Jahr 2023 wurde die NAMUR-Empfehlung NE193 „Ein Informationsmodell für das Automation Security Engineering“ erstellt, freigegeben und veröffentlicht.

2.3.2 Anforderungserhebung (AP 2)

Zum Zwecke der Anforderungserhebung wurden Workshops mit den assoziierten Anwendungspartnern HIMA und INEOS durchgeführt. Darin wurden die jeweiligen bestehenden Automation-Engineering-Workflows analysiert und mögliche Anknüpfungspunkte für Security identifiziert.

2.3.2.1 Ist-Analyse der Automation-Engineering-Workflows

Obwohl bereits verallgemeinerte Engineering-Workflows existieren (siehe z. B. [1], [2]), hat jede Organisation ihre eigenen spezifischen Vorgehensweisen. Besonders bei Herstellern und Betreibern ist eine Differenzierung erforderlich, da sie in den verschiedenen Phasen des Workflows unterschiedliche Aufgaben ausführen. In den Workshops wurden INEOS und HIMA befragt, um Einblicke in die praktische Umsetzung ihrer Engineering-Workflows zu gewinnen. Das Ergebnis der Workshops ist in Abbildung 2-2 zusammengefasst. Zur besseren Einordnung der Schritte werden oben (graue Kästen) die Phasen des NA35-Modells [1], einem Ablaufmodell für das Engineering von Automatisierungsanlagen, dargestellt. In der Darstellung sind die Schritte des Betreibers (INEOS) in blauen Kästen und die des Herstellers (HIMA) in orangefarbenen Kästen visualisiert.

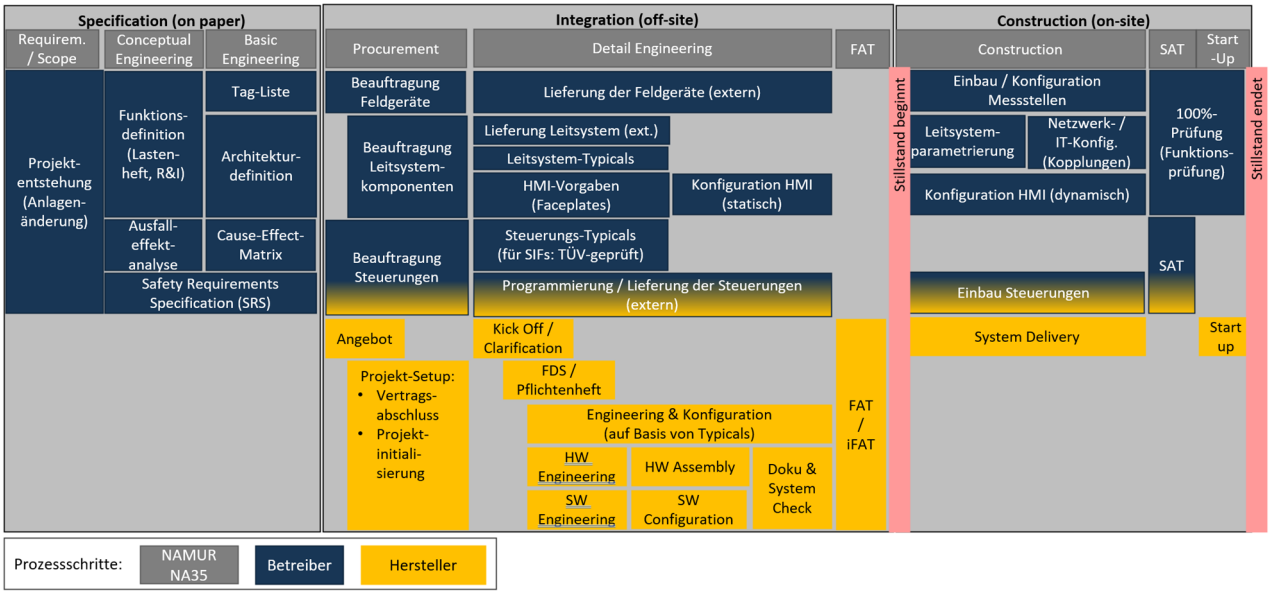

Abbildung 2-2: Abstrakte Darstellung des Engineering-Workflow von HIMA und INEOS

Ausgehend von der Analyse des bestehenden Engineering-Prozesses wurden die praktischen Anforderungen ermittelt, die für die Integration des Security-Engineering-Prozesses in den Automatisierungs-Engineering-Prozess berücksichtigt werden müssen. Diese Erkenntnisse liefern einen wesentlichen Beitrag zu Kapitel 2.3.3.

2.3.2.2 Anforderungen an die Integration von Security in das Automation-Engineering

Abbildung 2-3 zeigt die Grundbegriffe von Security by Design. Ein bestehender Engineering-Workflow, hier Basis-Workflow genannt, dient als Grundlage. Für die Integration von Security-Engineering müssen ein passender Security-Engineering-Workflow und ein Integrationsmechanismus definiert werden. Beim Integrationsmechanismus wird zwischen den folgenden Vorgehensweisen unterschieden: Verschmelzung, Kopplung, Auslösung und Harmonisierung. Eine detailliertere Beschreibung der einzelnen Mechanismen ist in [3] zu finden.

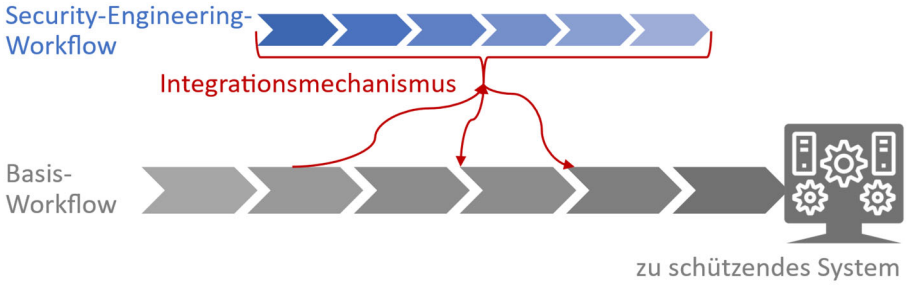

Abbildung 2-3: Security by Design-Grundbegriffe

Die Analyse hat zu den folgenden Anforderungen für die Integration von Security in den Automation-Engineering-Workflow geführt:

- **A1 - Unabhängigkeit vom Basis-Workflow:** Die Analyse der existierenden Ansätze zeigt, dass der Integrationsmechanismus von Security-Engineering in den Basis-Workflow möglichst losgelöst vom Basis-Workflow beschrieben werden muss.
- **A2 - Durchführbarkeit für die Gewerke des Basis-Workflows:** Das „Security by Design"-Konzept sollte ermöglichen, dass jedes Gewerk das Security-Engineering für seinen Einflussbereich durchführt.
- **A3 - Sicherstellung von rechtzeitigen Entscheidungen:** Security-Entscheidungen müssen früh genug getroffen werden, um wichtige Designentscheidungen noch beeinflussen zu können. Dafür ist allerdings die Definition eines genauen Zeitpunkts weniger wichtig als die Definition eines spätestmöglichen Zeitpunkts für eine Security-Entscheidung.
- **A4 - Nutzung systemimmanenter Eigenschaften für Security.** Das „Security by Design"-Konzept soll es ermöglichen, die in den sowieso verbauten Systemkomponenten immanenten Eigenschaften für Security zu nutzen und die zusätzlichen Lösungen nur nach Ausschöpfung dieser Möglichkeiten in Erwägung ziehen.
- **A5 - Methodische Anleitung für das Security-Engineering:** Es soll nicht nur definiert werden, was wann im Basis-Workflow getan oder entschieden werden soll, sondern auch methodische Hilfestellung für das „Wie" gegeben werden.

2.3.2.3 Anforderungen an das Domänenmodell (AutomationML)

Um Security- und Automatisierungs-Engineering effizient zu integrieren, ist ein Datenaustausch zwischen den relevanten Werkzeugen erforderlich, der maschinenlesbar ist. Dazu wurde AutomationML (AML) [4], eine standardisierte neutrale Modellierungssprache, als Technologie für das Informationsmodell ausgewählt. Das Automation-Engineering umfasst viele verschiedene Disziplinen, darunter Verfahrenstechnik, Regelungstechnik, Robotik und funktionale Sicherheit, die eine Vielzahl eigener technischer Sprachen verwenden. Die Herausforderung, diese verschiedenen Sprachen zu harmonisieren, wird durch den Einsatz von AutomationML angegangen. Auf der Grundlage der Anwendungsfälle von [5] wurden spezifische Anforderungen an das Security-Domänenmodell festgelegt:

- **B1 – Objektorientierteres, interoperables Systemmodell:** Das Security-Domänenmodell soll ein objektorientiertes Systemmodell sein, das gleichzeitig die Interoperabilität und den Informationsaustausch mit anderen Domänen gewährleistet.
- **B2 – Abstraktionsgrad und Hierarchisierung:** Das Security-Domänenmodell reduziert die Komplexität, indem es auf höherem Abstraktionsniveau als die zugrunde liegenden Domänenmodelle basiert und Hierarchisierungen für vertiefte Detaillierungen ermöglicht.
- **B3 - Funktionaler Ansatz unter Einbeziehung des Menschen:** Security-Engineering erfordert ergänzende Informationen zur Modellierung eines rein technischen Systems, insbesondere die Darstellung von Interaktionen und Kommunikation zwischen beteiligten menschlichen Rollen sowie IT/OT-Systemen oder zwischen IT/OT-Systemen selbst.
- **B4 – Vordefinierte Bibliotheken:** Zur Förderung der Wiederverwendbarkeit kann eine zentrale Sammlung für die relevanten Systemfunktionen erstellt werden. Diese Sammlung enthält alle notwendigen Informationen, wie betroffene Entitäten im Netzwerk, zuständige Personen, Rollen und die Zuordnung von Risikoszenarien. Es bietet sich außerdem an, bereits etablierte Lösungsvorschläge in dieser Sammlung abzulegen.

2.3.3 Security-Entscheidungsfindung (AP 3 & 4)

2.3.3.1 Konzept

Das Konzept („Security by Design Decisions“ wurde entwickelt, um Security-Entscheidungen in Entscheidungspunkten so zu bündeln, dass sie in verschiedene Engineering-Prozesse integrierbar sind. Ein Security-Entscheidungspunkt fasst eine abgeschlossene Menge von Security-Entscheidungen zusammen, die zu ähnlichen Zeitpunkten und mit Hilfe derselben Expertise getroffen werden müssen. Für die Integration von Security-Entscheidungen in den Automation-Workflow wurde der Kopplungsmechanismus (siehe Abbildung 2-4) als die beste Lösung identifiziert. Eine detaillierte Beschreibung des Konzeptes kann der Veröffentlichung [3] sowie [6] entnommen werden.

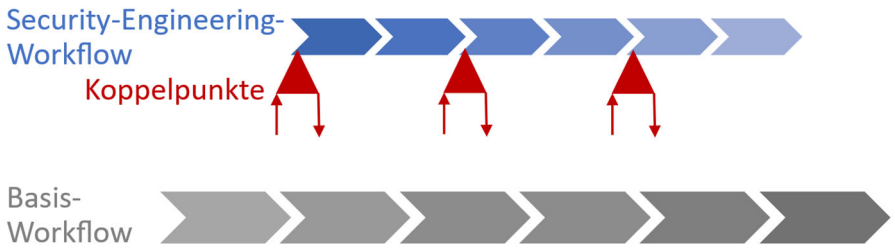

Abbildung 2-4: Kopplungsmechanismus

Das Konzept ermöglicht die Beschreibung der Entscheidungsfindung. Der zugehörige Workflow, der alle zuvor festgelegten Anforderungen erfüllt (siehe [6], [7]), ist in Abbildung 2-5 dargestellt und besteht aus vier Schritten: Zunächst muss die Entscheidungsbasis geschaffen, dann die Entscheidungspunkte im bestehenden Engineering-Workflow platziert werden. Die letzten beiden Schritte verlaufen iterativ: Ein Modell der security-relevanten Aspekte wird erstellt und dabei die in den Entscheidungspunkten enthaltenen Security-Entscheidungen mit Hilfe der Informationen aus der Entscheidungsbasis getroffen und dokumentiert – das verändert wiederum das Anlagenmodell. So entsteht während des Automation-Engineerings Stück für Stück ein Security-Modell mit bewusst getroffenen Security-Entscheidungen.

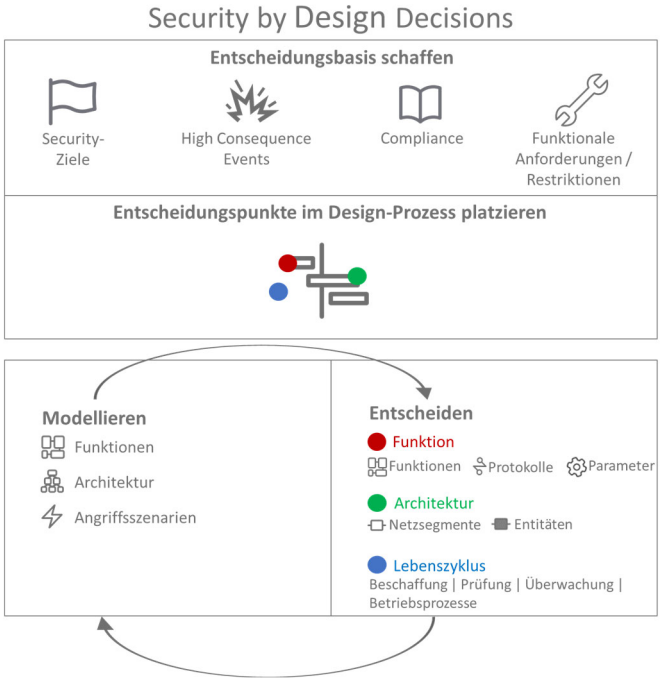

Abbildung 2-5: Workflow für Security-by-Design Entscheidungen

Das **Cybersecurity-Modell** enthält sowohl ein Funktionsmodell als auch ein Architekturmodell. Funktionen enthalten Entitäten (technische Komponenten oder menschliche Rollen) und Interaktionen zwischen diesen Entitäten zu einem bestimmten Zweck, zum Beispiel „Programmierung einer Steuerung". Das Architekturmodell zeigt die Netzwerkarchitektur. Da es für Security hilfreich sein kann, funktionale und architekturelle Aspekte zeitgleich zu sehen, ist es möglich, das Funktionsmodell im Kontext der Architektur anzuzeigen. Zusätzlich können für Funktionen Angriffsszenarien modelliert werden.

Es gibt **drei Typen von Security-Entscheidungen**. Funktions- und Architekturentscheidungen umfassen Änderungen des Cybersecurity-Modells: Hinzufügen oder Entfernen von Funktionen oder Entitäten, Verändern von Funktionen oder der Architektur, Spezifizieren von Protokollen oder von Detail-Eigenschaften der Entitäten. Letztere werden im Konzept der „Security-Parameter" zusammengefasst.

Darüber hinaus gibt es Lebenszyklus-Entscheidungen, die immer an einer bestimmten Stelle im Lebenszyklus einer Anlage getroffen werden müssen, zum Beispiel Abnahmetests vor Inbetriebnahme (in die Security integriert werden sollte).

Bei der Dokumentation der Entscheidungen wird auch eine Begründung angegeben. **Die Begründung kann eine oder mehrere der folgenden Dimensionen enthalten**:

- Zielbasiert: Die Entscheidung wird zur Erreichung eines Security-Ziels getroffen.
- Risikobasiert: Die Entscheidung wird zur Vermeidung eines Security-Risikos getroffen.
- Compliance-basiert: Die Entscheidung wird zur Einhaltung einer Security-Regularie getroffen.
- Basierend auf funktionalen Anforderungen: Die Entscheidung wird aufgrund einer funktionalen Anforderung bzw. Restriktion getroffen.

2.3.3.2 Beispiel

Schritt 1: Entscheidungsbasis schaffen

Die Erstellung der Security-Entscheidungsbasis ist ein wesentlicher Schritt, um die richtigen Prioritäten im folgenden Entscheidungsprozess zu setzen. Mögliche Elemente der Entscheidungsbasis sind in Tabelle 2-2 dargestellt, zusammen mit typischen Beispielen für jedes Element.

Die Elemente der Entscheidungsgrundlage werden nach dem Entscheidungspfad kategorisiert, den sie unterstützen: zielbasiert, risikobasiert, Compliance-basiert oder basierend auf funktionalen Anforderungen. Es ist legitim und sinnvoll, mehrere Entscheidungspfade auf gleichzeitig zu bedienen.

Tabelle 2-2: Beispielhafte Elemente in der Entscheidungsbasis

Decision base element	Examples
Goal-based decision making	
Security goal: specifies what cybersecurity is meant to achieve for an organization / the system under consideration.	• No access to safety PLCs from outside the plant • Engineering station cannot be used for malicious purposes • Availability of safety PLC and alarm server
Risk-based decision making	
High-Consequence Event (HCE): Unwanted state of the system to be protected (also known from INL CCE / CIE [8], [9])	• Ethylene oxide plant explodes • Safety system does not trip despite a demand case
Attack Scenario: Scenario that is harmful to the system under consideration, may lead to a high-consequence event.	• Manipulation of PLC logic • A critical value is bridged so that the safety function is not triggered
Attack point: A cybersecurity decision that provides an opportunity for a security attack.	• Password is stored in plain text • Restarting the controller from the programming device is enabled
Risk: Attack scenario with evaluated impact and likelihood.	See attack scenarios.
Compliance-based decision making	
Security standard / regulation: Standards or regulations that an organization chooses or is forced to comply with.	• Critical infrastructure regulation of country XY • ISA/IEC 62443-3-3
Security requirement: Individual requirement from any of these standards or regulations.	• § 3: Patching • SR 5.1: Network segmentation
Decision making based on functional requirement	
Functional requirements / restrictions: A requirement that defines a system functionality (as opposed to non-functional requirements that address for example security or reliability).	• Signal bridging is needed for maintenance • The service provider can only receive files via FTP

Schritt 2: Entscheidungen im Engineering-Workflow platzieren

Abbildung 2-6 zeigt ein Beispiel für die Zuordnung von Entscheidungspunkten – also bestimmten Veränderungen im Cybersecurity-Modell – zu bestimmten Lieferergebnissen eines Engineering-Workflows. Die Leitfrage ist dabei immer: Wann im Engineering-Prozess (bzw. mit welchem Lieferergebnis) würde ich diese Art von Entscheidung treffen? Die Netzwerkarchitektur und IT-Funktionen beispielsweise werden im „System Architecture Planning“ festgelegt, die Leitsystemfunktionen in der Spezifikation, Details zu Feldgeräten in der Cause-Effect-Liste.

(In der Validierung mit den Anwendungspartnern erwies sich die Platzierung der Entscheidungspunkte im Engineering-Workflow als optional; die Methodik funktioniert auch ohne diesen Schritt, solange das Cybersecurity-Modell während des gesamten Engineering-Workflows aktiv mitgepflegt wird.)

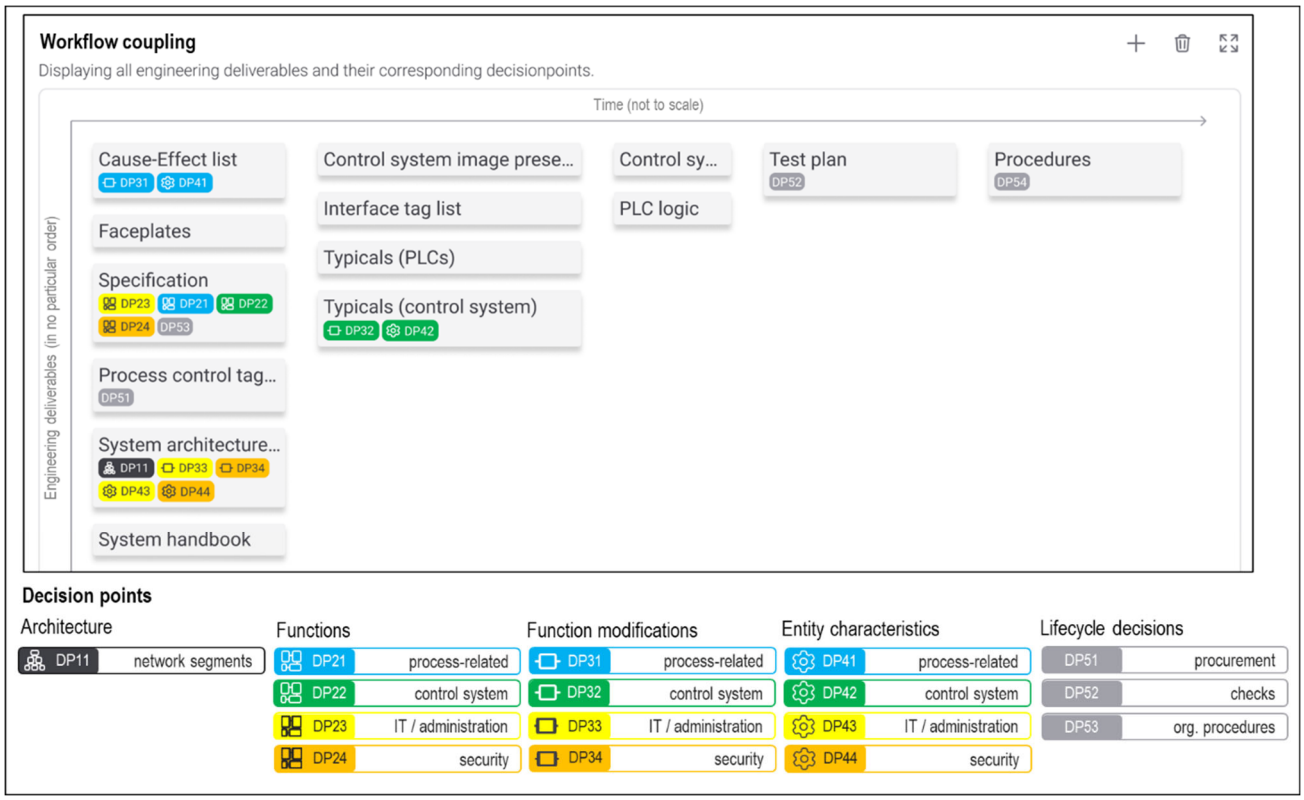

Abbildung 2-6: Beispiel - Automation Engineering Workflow mit Entscheidungspunkten

Schritte 3 und 4: Modellieren und Entscheiden

Das Cybersecurity-Modell des betrachteten Systems wird erstellt. Ein typischer Startpunkt ist die Modellierung von Systemfunktionen. Im IDEAS-Projekt wurden Funktions-, Entitäts- und Protokollbibliotheken erarbeitet, um den Modellierungsprozess zu beschleunigen. Die Bibliothekselemente enthalten auch vordefinierte Security-Entscheidungen. Alle Bibliothekselemente können nach Bedarf geändert werden, und natürlich können auch völlig neue Elemente modelliert werden.

In einem frühen Projektstadium mag das Wissen über die gewünschte Funktionalität vorhanden sein, aber noch wenig darüber entschieden sein, wie die Funktion implementiert werden soll. Mit der Erstellung des Systemmodells kann und sollte jedoch trotzdem bereits begonnen werden, und es können auch schon erste, grundlegende Security-Entscheidungen getroffen werden.

Als Beispiel zeigt Abbildung 2-7 ein abstraktes Funktionsmodell, wie es ganz zu Beginn eines Engineering-Projekts aussehen könnte. Abbildung 2-8 zeigt, wie die Funktion aus Security-Gründen modifiziert wird und diese Security-Entscheidung mitsamt Begründung explizit dokumentiert wird.

Mit dem Fortschreiten des Engineering-Prozesses, wird auch das Cybersecurity-Modell detaillierter, und es können detailliertere Security-Entscheidungen getroffen werden. Zum Beispiel wären als nächstes detailliertere Security-Entscheidungen zu dem soeben hinzugefügten Schlüsselschalter denkbar. Deswegen werden die Schritte 3 und 4 – Verfeinern des Modells und Treffen von Security-Entscheidungen – iterativ wiederholt, bis das Cybersecurity-Modell dem finalen Stand des Systems entspricht.

Zusätzlich kann es für den risikobasierten Entscheidungspfad sinnvoll sein, konkrete Angriffsszenarien ins Systemmodell zu modellieren (siehe Abbildung 2-9).

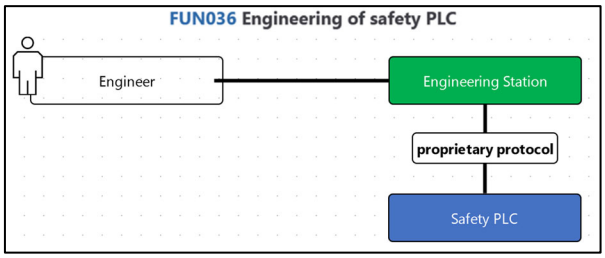

Abbildung 2-7 Abstraktes Funktionsmodell zu Beginn eines Engineering-Projekts

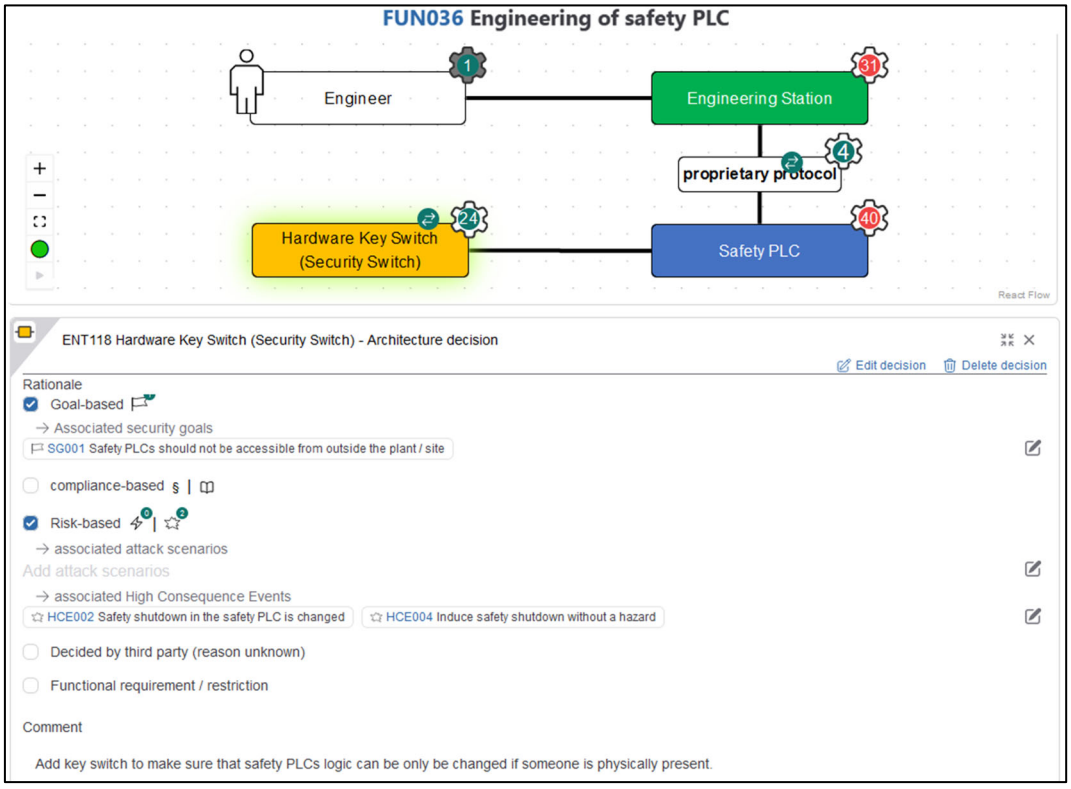

Abbildung 2-8 Dokumentation einer Security-Entscheidung (Hinzufügen des Schlüsselschalters)

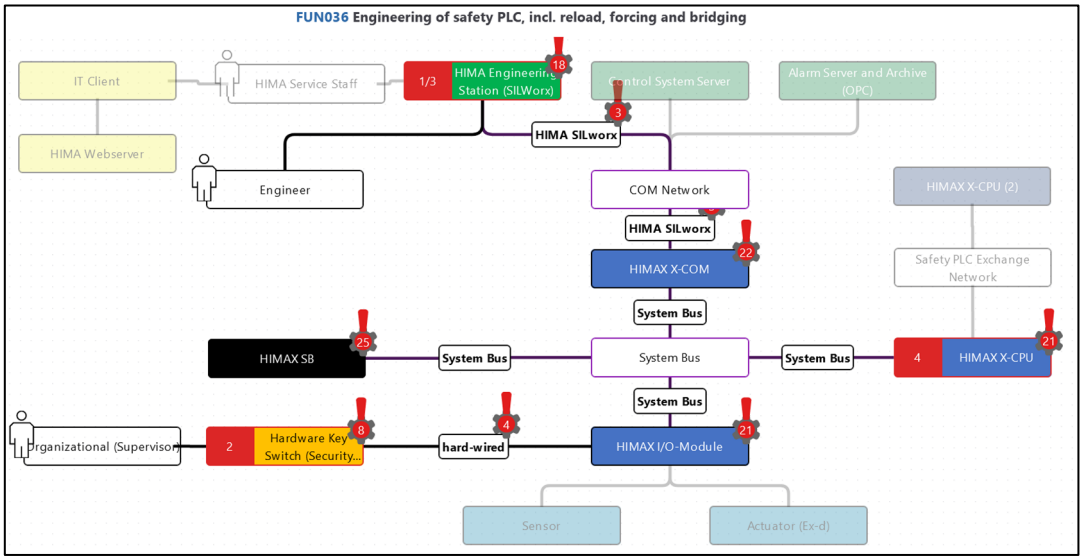

Abbildung 2-9 Modellierung eines Angriffsszenarios für eine detaillierteres Version des Systemmodells

2.3.4 Entwicklung eines AutomationML-Datenmodells (AP 5)

Um ein Informationsmodell in AutomationML schrittweise mit Security-Eigenschaften zu ergänzen, wurde im Projekt ein Leitfaden entwickelt. Die Empfehlungen basieren auf dem Ansatz zur Strukturierung des Security-Engineering-Prozesses aus Kapitel 2.3.3. Der Fokus liegt auf der Modellierung von security-relevanten Informationen, um eine klare Sicht auf das zu schützende System zu ermöglichen. Der Leitfaden verfolgt das Ziel, die Integration von Security-Eigenschaften in maschinenlesbare Informationsmodelle zu fördern, um eine systematische und detaillierte Analyse der Security-Aspekte eines Systems zu ermöglichen. Der Leitfaden besteht aus mehreren aufeinanderfolgenden Schritten, beginnend mit der Modellierung von Funktionen in AML, gefolgt von der Einbindung von Security-Parametern, der Identifikation von Angriffspunkten und der Entwicklung von Risikoszenarien. Im letzten Schritt werden Security-Ziele, Anforderungen und entsprechende Maßnahmen im Zusammenhang mit den identifizierten Risiken dargestellt. In den Abbildungen Abbildung 2-10 bis Abbildung 2-13 werden zwei unterschiedliche Perspektiven gezeigt: Auf der linken Seite ist ein vereinfachtes Netzmodell zu sehen, bei der eine Funktion (in Rot) hervorgehoben ist – als Beispiel wird hier durchgehend das „Firmwareupdate einer SPS durch einen Techniker“ verwendet. Auf der rechten Seite ist das Informationsmodell dargestellt, das in den folgenden Kapiteln schrittweise um security-relevante Eigenschaften ergänzt wird. Da die vollständige Darstellung des Informationsmodells in AML zu umfangreich und unübersichtlich wäre, wird hier eine vereinfachte Version gezeigt. Aus platztechnischen Gründen wird auf eine detaillierte Darstellung des Informationsmodells verzichtet. Ein umfassender Ausschnitt des Modells kann in [10] eingesehen werden. Die Bibliotheken werden zum Abschluss vorgestellt.

2.3.4.1 Modellierung einer Funktion in AutomationML

Im Projekt wurde weiterhin eine Modellierungsmethode entwickelt, die es ermöglicht, das zu schützende System klar darzustellen, ohne dass die vollständige Abbildung des gesamten Systems die Betrachtung beeinträchtigt. Die Modellierung einer Funktion im Informationsmodell erfolgt in AML unter Verwendung der Syntax [11] und der Struktur des Netzmodells aus [12]. Diese sind in Abbildung 2-10 als grüne Datenobjekte ❶ dargestellt.

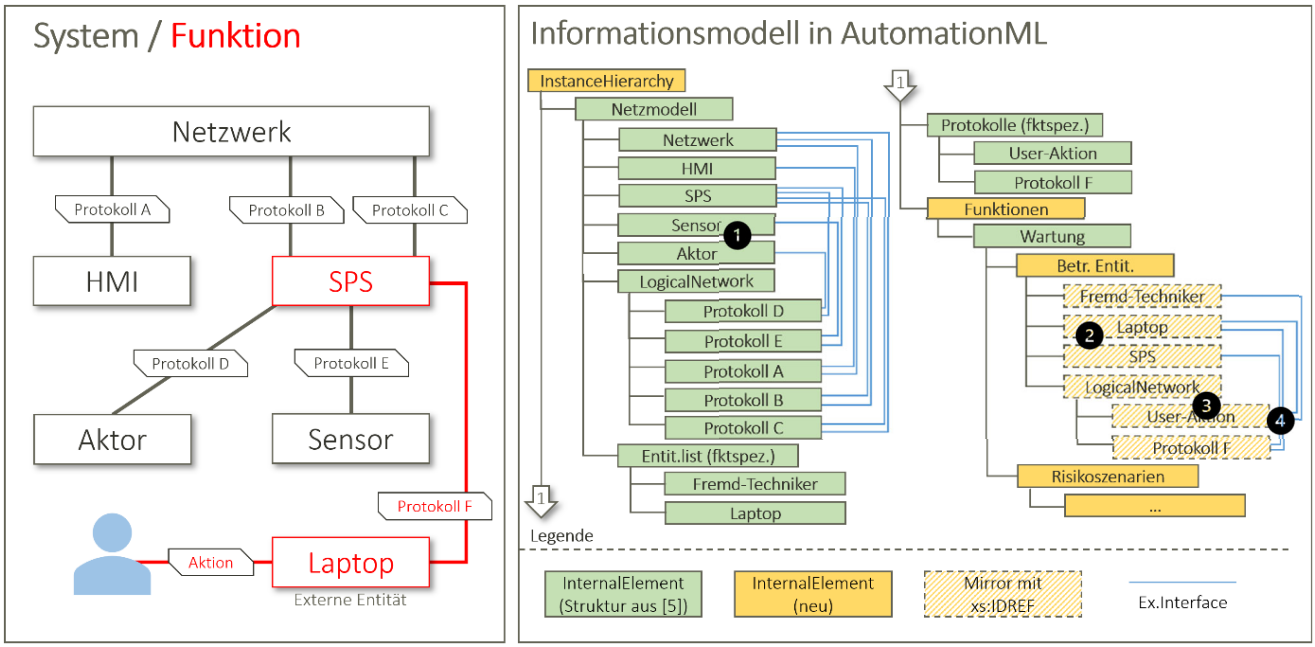

Abbildung 2-10: Links - Darstellung eines einfachen Systems mit einer Funktion; Rechts – Vereinfachte Struktur des Informationsmodells in AutomationML

Der Prozess der Funktionsmodellierung umfasst folgende Schritte:

- **Schritt 1:** Die betroffenen Entitäten aus dem Netzmodell sowie zusätzliche Entitäten, die nicht im Netzmodell enthalten sind (z. B. externe Rolle wie ein Techniker), werden in die Funktionsstruktur ❷ als INTERNALELEMENT ❸ (gelb markiert) übernommen.
- **Schritt 2:** Da die neuen INTERNALELEMENTS keine direkte Beziehung zu den bestehenden Entitäten aufweisen, wird ihnen ein ATTRIBUTETYPE xs:IDREF (Mirror-Konzept) zugewiesen, das auf die GUID der jeweiligen Entität verweist.
- **Schritt 3:** Die Entitäten und die Verbindungen werden als INTERNALELEMENTS abgebildet und über eine INTERFACECLASS ❹ miteinander verknüpft.
- **Schritt 4:** Im nächsten Schritt werden die Verbindungen zwischen den Entitäten sowie die verwendeten Protokolle modelliert.

Dies bildet die Grundlage für die spätere Erweiterung der Funktionsstruktur um Security-Parameter im nächsten Schritt.

2.3.4.2 Modellierung von Security-Parametern

Wie in Kapitel 2.3.3 beschrieben, bieten Security-Parameter eine transparente Grundlage für die Dokumentation und Nachvollziehbarkeit von Security-Entscheidungen. Sie umfassen eine Vielzahl von Konfigurationen, Designentscheidungen und weiteren Aspekten, die potenziell Auswirkungen auf die Security haben und maschinenlesbar umgesetzt werden können.

In Abbildung 2-11 auf der linken Seite ist eine erweiterte Version des Netzmodells dargestellt, bei der die blauen Security-Parameter der SPS zugeordnet sind. Diese Parameter umfassen beispielsweise das Umschalten der Betriebsmodi und die Einstellung der Programmaktualisierung während des Betriebs.

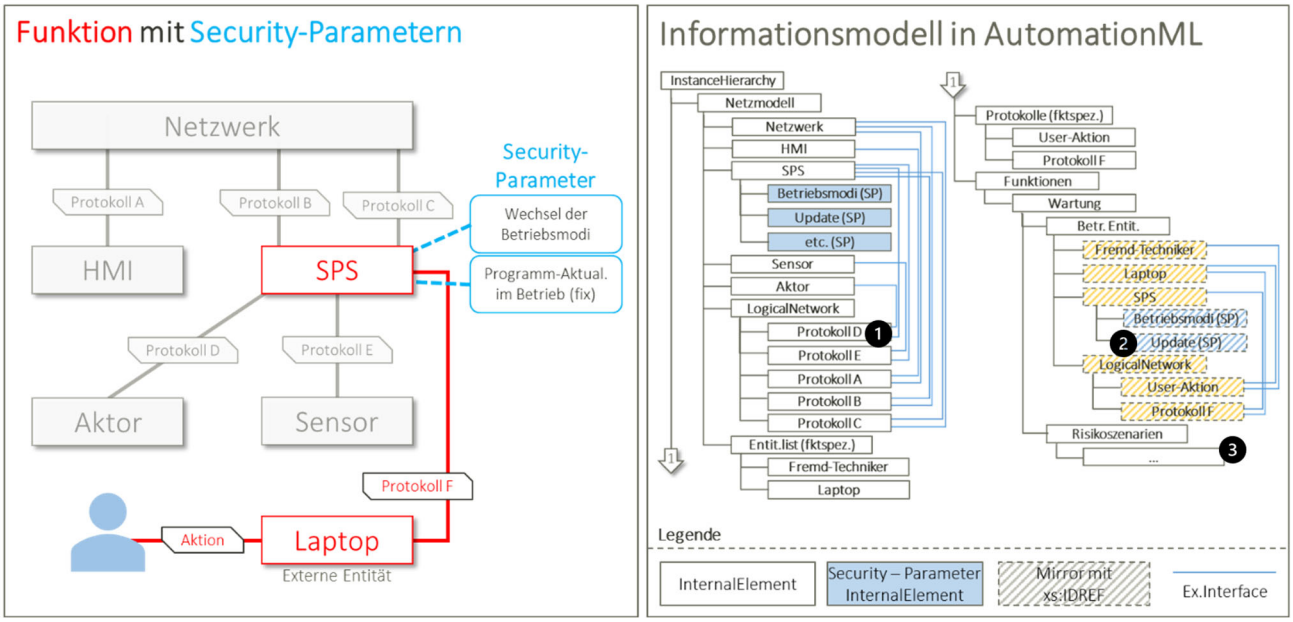

Abbildung 2-11: Links – Erweiterung der Funktion mit security-relevanten Eigenschaften; Rechts – Vereinfachte Struktur des Informationsmodells

Um Security-Parameter im Informationsmodell zu integrieren, sind folgende Schritte erforderlich:

- **Schritt 1**: Die Security-Parameter werden als INTERNALELEMENT ❶ den Entitäten zugewiesen.
- **Schritt 2**: Es erfolgt die Modellierung von Referenzen auf andere Entitäten, Anforderungen oder HCEs mithilfe des CAEX Typs INTERFACECLASS.
- **Schritt 3:** Die INTERNALELEMENTS ❶ werden um Attribute wie "mögliche Werte" und "kritische Werte" erweitert.

- **Schritt 4**: In der Beschreibung des Parameters werden die security-relevante Relevanz und passende Tags aufgeführt.
- **Schritt 5**: Dem Security-Parameter wird eine entsprechende Rolle in AML zugewiesen, die der Gefährdungskategorie entspricht und aus der Bibliothek entnommen wird.
- **Schritt 6**: Um den Bezug zwischen den Datenobjekten zu wahren, wird dem INTERNALELEMENT ❸ in der Funktion ❷ ein zusätzliches Attribut vom Typ xs:IDREF (Mirror-Konzept) hinzugefügt, das auf die GUID des Parameters im Netzmodell verweist. Dies ermöglicht Änderungen an den Parametern der Funktion und des Netzmodells über eine softwaregestützte Anwendung.

2.3.4.3 Modellierung von Angriffspunkten, -pfaden und Risikoszenarien

Abbildung 2-12 zeigt einen Angriffspunkt aus der CVE-Datenbank, der der SPS zugeordnet ist und durch Änderungen der Betriebsmodi zur Manipulation der Drehzahl des Aktors genutzt werden könnte.

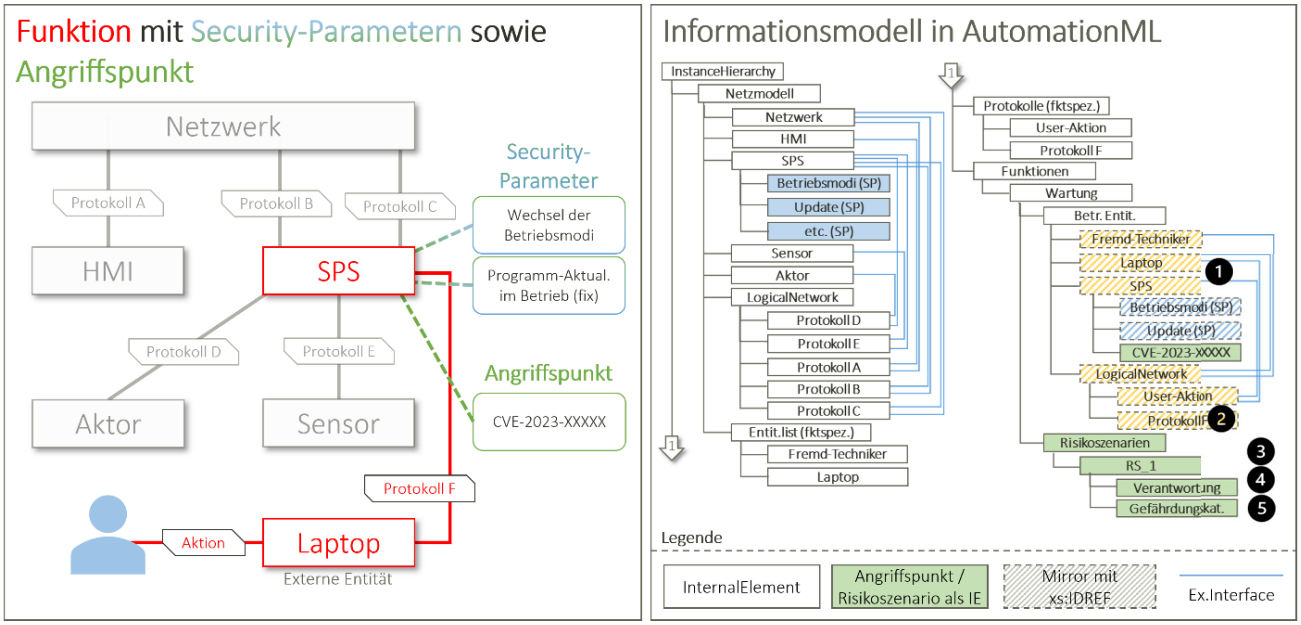

Abbildung 2-12: Links – Erweiterung der Funktion mit einem Angriffspunkt (CVE-2023-XXXXX); Rechts – Vereinfachte Struktur des Informationsmodells (mit Risikoszenarien)

Die Modellierung von Angriffspunkten im Informationsmodell erfolgt wie folgt:

- **Schritt 1**: Zuweisung von INTERNALELEMENTS ❶ (grün), ähnlich wie bei den Security-Parametern, jedoch werden diese direkt in der Funktionshierarchie der jeweiligen Entität erstellt und nicht kopiert, weshalb diese kein Mirror-Attribut erhalten.
- **Schritt 2**: Ein EXTERNALDATAREFERENCE-EXTERNALINTERFACE wird an das INTERNALELEMENT angefügt, wobei die Attribute „refURI“ (Pfad zur Referenz) und „MIMEType“ (Typ der Referenz) verwendet werden, falls eine Datenbank oder Datei referenziert wird.
- **Schritt 3**: Es gibt auch Risiken, die nicht einer Entität, sondern einer gesamten Funktion zugeordnet werden. Diese werden als INTERNALELEMENTS ❸ der Funktion hinzugefügt.
- **Schritt 4**: Jedes Risikoszenario wird ebenfalls als INTERNALELEMENT modelliert und erhält zusätzliche Attribute wie „Zuständigkeit“ ❹, „Referenzen“ (mit EXTERNALINTERFACE) und „Gefährdungskategorie“ ❺. Weitere Attribute wie „Art der Auswirkung“, „Auswirkung“ und „Eintrittswahrscheinlichkeit“ werden aus der Bibliothek übernommen.

Zur Vermeidung oder Minderung solcher Risiken können entsprechende Security-Ziele, Maßnahmen und Anforderungen zugewiesen werden, die im nächsten Kapitel detailliert behandelt werden.

2.3.4.4 Modellierung von Security-Zielen, Anforderungen und Maßnahmen zu den Risikoszenarien

Die Wahl des passenden Security-Ziels hängt von verschiedenen Faktoren ab und ist entscheidend für die Umsetzung von Schutzmaßnahmen. Diese können beispielsweise risikobasiert, compliance-orientiert oder funktional motiviert sein. Die Modellierung von Security-Zielen erfolgt innerhalb der Funktionshierarchie, wobei die zugehörigen Entitäten berücksichtigt werden. In Abbildung 2-13 ist eine Erweiterung des Systems durch das Security-Ziel „Integrität der Ausgangswerte“ dargestellt.
Der Modellierungsprozess von Security-Zielen folgt diesen Schritten:

- **Schritt 1**: Security-Ziele werden als INTERNALELEMENTS ❶ (orange) den entsprechenden Entitäten hinzugefügt.
- **Schritt 2**: Jedem Security-Ziel wird ein ATTRIBUTETYPE wie „Typ“ (z.B. Datenschutz, Integrität) sowie ein EXTERNALINTERFACE für Referenzen hinzugefügt.
- **Schritt 3**: In der Beschreibung des INTERNALELEMENTS ❶ wird die Entscheidung zur Wahl der entsprechenden Security-Parameter dokumentiert.
- **Schritt 4**: Im nächsten Schritt werden die Risikoszenarien modelliert. Für jedes Szenario wird eine Liste von Anforderungen als INTERNALELEMENT ❷ eingefügt. Eine detaillierte Modellierung ist in [AUOTMATION EMRE 2022] beschrieben.
- **Schritt 5**: Diese Anforderungen werden mit weiteren INTERNALELEMENTS wie „Zuständigkeit“ ❸, „Referenzen“ ❹ und „Maßnahmen“ ❺ ergänzt.
- **Schritt 6**: Für jede Maßnahme werden die Quellen mit EXTERNALINTERFACES und zwei ATTRIBUTETYPES („Typ der Umsetzung“ und „Deadline“) verknüpft.

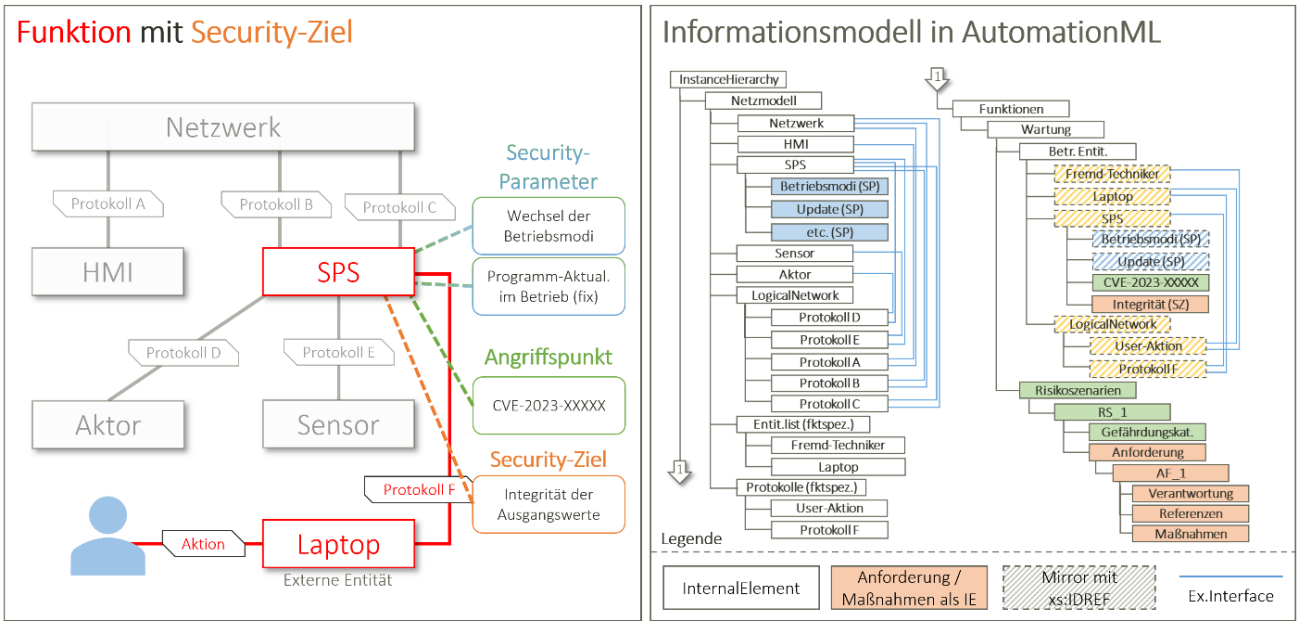

Abbildung 2-13: Links – Erweiterung der Funktion mit einem Security-Ziel; Rechts – Vereinfachte Struktur des Informationsmodells (mit Anforderung sowie Maßnahamen)

2.3.4.5 Bibliothek in AutomationML für Automation-Security-Engineering-Prozesse

Um die Wiederverwendung von Informationen und Funktionen im Rahmen von "Security by Design" zu erleichtern, empfiehlt sich der Aufbau zusätzlicher Bibliotheken. Diese Bibliotheken werden vom Software-Demonstrator abgeleitet und enthalten dieselben Inhalte. Diese Bibliotheken können abstrakte Entitäten, Security-Parameter, Security-Ziele und andere relevante Informationen als Vorlagen in AutomationML speichern. Zudem können sie bereits etablierte Funktionsvorschläge enthalten, um die Entwicklung zu beschleunigen. Die Bibliothek kann kontinuierlich durch den Export eines JSON-Objektes

(siehe Kapitel 2.3.5.2) von der Datenbank aktualisiert werden, um die neuesten Entwicklungen und Standards zu reflektieren. Weitere Details und Inhalte der Bibliothek sind in der Arbeit [10] zu finden.

2.3.4.6 Zusammenfassung

Der entwickelte Leitfaden bietet eine schrittweise Anleitung zur Integration von Security-Eigenschaften in das Informationsmodell, wodurch eine praxisorientierte Methode zur Verbesserung der Security in der Automatisierungstechnik entsteht. Durch die Modellierung von Security-Parametern wird eine systematische Analyse der security-relevanten Aspekte ermöglicht, was als Basis für die Entwicklung passender Maßnahmen dient. Zudem schafft das Informationsmodell einen algorithmischen Zugang zu den Daten und eröffnet damit vielfältige Anwendungsmöglichkeiten für verarbeitende Software (Demonstrator) als Backend: digitaler Datenfluss, Änderungsmanagement, automatische Konflikterkennung und Konsistenzprüfung, moderne Assistenzsysteme für das Security-Engineering, Impact-Analysen, Mustererkennung und vorgefertigte Lösungen.

2.3.5 Entwicklung eines Demonstrators für ein Software-Werkzeug (AP 6)

2.3.5.1 Umsetzung des Demonstrators

Zur Unterstützung der Integration von Security in den Automation-Engineering-Prozess wurde ein Software-Demonstrator entwickelt, der auf den Prinzipien von „Security by Design Decisions“ basiert. Der Demonstrator ist auf einer Architektur aufgebaut, die ein Frontend und ein Backend umfasst. Das Backend nutzt das Python-basierte Flask-Framework, während das Frontend auf dem JavaScript-Framework React basiert. Die Daten werden in einer graphbasierten Neo4j-Datenbank gespeichert, die ideal für das zugrunde liegende Datenmodell geeignet ist. Die Abbildungen aus Kapitel 2.3.3 zeigen Ausschnitte aus dem Demonstrator. Der Software-Demonstrator bietet folgende Implementierungen:

- Umsetzung des gesamten entwickelten Automation-Security-Engineering-Workflows.
- Umsetzung aller in der Security-Merkmalsbibliothek entwickelten Konzepte (Funktionen, Entitäten, Protokolle, High Consequence Events, Security-Parameter, Angriffspunkten, Security-Ziele und Standardanforderungen)
- Bereitstellung erster Bibliotheksinhalte für Funktionen (einschließlich Entitäten und Protokollen) sowie Security-Parameter (einschließlich Angriffspunkten).
- Interaktive und bearbeitbare Darstellung der entwickelten Security-Diagramme.

2.3.5.2 AutomationML-Export/Import

Das Backend des Demonstrators ermöglicht die Erzeugung eines JSON-Objekts anhand eines vorgegeben „Gerüsts“, das für die Export- und Importschnittstelle verwendet werden kann, um eine Verbindung zu AutomationML herzustellen. Python wurde als Entwicklungsumgebung genutzt. Die AML.Engine-Dateien [4], [7] aus der C#-Bibliothek wurden übernommen und in die Python-Umgebung integriert. Dabei wurde eine detaillierte Anleitung erstellt, die beschreibt, wie die Integration genutzt werden kann. Diese Anleitung ermöglicht es, dass auch Studierende auf dieser Basis Forschungsarbeiten durchführen können, da nun auch die Autocompletion-Funktionalität in Entwicklungsumgebungen zur Verfügung stehen.
Zur Sicherstellung der Zuverlässigkeit des Exporters wurde eine AutomationML-Datei aus dem JSON-Objekt generiert. Praxisorientierte Beispielsdaten kamen zum Einsatz, um die Funktionalität des Exporters zu überprüfen und sicherzustellen, dass er den Anforderungen und Erwartungen der definierten Anwendungsfälle entspricht. Dabei umfasst das Informationsmodell alle relevanten Informationen aus dem Demonstrator sowie deren Verbindungen und Referenzen. Ebenso wird der Import der AML-Datei ermöglicht, wobei die Struktur des JSON-Gerüsts abgebildet wird, sodass diese Daten vom Software-Demonstrator eingelesen und weiterverarbeitet werden können.

Der Export und Import der Daten wurden manuell überprüft, da eine Testung am Software-Demonstrator aufgrund sicherheitsrelevanter Maßnahmen nicht möglich war.

2.3.6 Evaluation unter realen Bedingungen (AP 7)

Die Validierung erfolgte in drei Runden (Workshops) mit den assoziierten Partnern INEOS und HIMA. Reale Engineering-Projekte der Anwendungspartner wurden unter Verwendung der im Forschungsprojekt entwickelten Methodik erneut durchgeführt. Zur Messung des Erfolgs der Validierung wurden, wenn möglich, quantitative, sonst qualitative Validierungsfragen formuliert (Tabelle 2-3).

Tabelle 2-3: Validierungsfragen

Validierungsfrage	Metrik (# / % = quantitativ / → = qualitativ)
Entscheidungen identifizieren: Identifizieren die Entscheidungsträger mehr Security-Entscheidungen?	# Identifizierte Entscheidungen[3] # Zusätzlich[1] identifizierte Entscheidungen[3] # / % Übersehene Entscheidungen[1, 3]
Entscheidungen ins Engineering integrieren: Können die Entscheidungsträger festlegen, wann eine Entscheidung spätestens getroffen werden muss?	# Entscheidungspunkte[3] # / % Anders zugeschnittene / überarbeitete Entscheidungspunkte[3] # / % Entscheidungspunkte[3] ohne Zuweisung zu einem Deliverable → Waren die Entscheidungen sinnvoll zu Entscheidungspunkten gebündelt? Warum / warum nicht? → Wahrscheinlichkeit, dass Sie die Security-Entscheidungen zukünftig tatsächlich bei Erstellung dieses Deliverables treffen werden?
Entscheidungen treffen: Können die Entscheidungsträger die Security-Entscheidungen selbstständig basierend auf den dargebotenen Informationen treffen?	# Getroffene Entscheidungen[3] # Zusätzlich[1] getroffene Entscheidungen[3] # Veränderte Entscheidungen[1, 3] % Entscheidungen, die nicht getroffen werden konnten[3] → Waren Sie die richtige Person, um die Entscheidung zu treffen? → Warum konnten Sie die Entscheidungen nicht treffen / welche Informationen haben gefehlt?
Entscheidungen begründen / nachvollziehen: Können Dritte für jede Security-Entscheidung nachvollziehen, warum sie so getroffen wurde?	# / % Zielbasierte Entscheidungen[3] # / % Risikobasierte Entscheidungen[3] # / % Compliance-basierte Entscheidungen[3] # / % Auf einer funktionalen Anforderung / Restriktion basierte Entscheidungen[3] # / % Entscheidungen ohne Begründung[3] → Wahrscheinlichkeit, dass Sie die Ergebnisse in der Betriebsphase verwenden? → Wahrscheinlichkeit, dass Sie die Ergebnisse für die Management-Kommunikation verwenden?
Entscheidungen wiederverwenden: Können Artefakte, die während der Entscheidungsfindung genutzt bzw. erstellt wurden, für zukünftige Projekte wiederverwendet werden?	# / % Anwendbare Bibliotheksfunktionen # / % Veränderte Bibliotheksfunktionen[2] # / % Neu erstellte Bibliotheksfunktionen # / % Anwendbare Security-Parameter # Veränderte Security-Parameter[2] # Neu erstellte Security-Parameter →Wahrscheinlichkeit, dass Sie die Ergebnisse in zukünftigen Projekten wiederverwenden?

[1] Verglichen mit dem Originalprojekt, das ohne die neue Methodik durchgeführt wurde
[2] im Vergleich zur Bibliothek. (Bei Security-Parametern: Beinhaltet auch zusätzliche / entfernte Zuordnungen zu Entitäten.)
[3] ausgewertet je Entscheidungstyp: Funktion (eliminieren, Protokolle, Security-Parameter), Architektur, Lebenszyklus

Alle Validierungsfragen konnten positiv beantwortet werden, mit Einschränkungen bei der Frage nach der Integration in den Engineering-Workflow. Diese Einschränkungen lagen im Setup der Validierung begründet: Da die Anwendungspartner ein bestehendes Projekt erneut durchführten, waren von Anfang an alle Security-Entscheidungen bekannt; sie wurden nicht erst im Laufe des Projektes offenbar. Drei besonders herausstechende Ergebnisse zeigen die folgenden Abbildungen.

Abbildung 2-14 zeigt die Anzahl der zusätzlich getroffenen Security-Entscheidungen mit der neuen Methode: Zwischen 25 % und 49 % der in den Validierungsprojekten getroffenen Security-Entscheidungen wurden aufgrund der neuen Methode erstmals bewusst getroffen; sie waren vorher entweder gar nicht getroffen worden oder die Ingenieure waren sich der Security-Implikationen nicht bewusst. Das wurde sowohl vom Projektteam als auch den Anwendungspartnern als großer Erfolg gewertet.

Abbildung 2-15 zeigt die Verteilung der Entscheidungstypen über die drei Validierungsrunden. Die häufigsten Entscheidungen waren Entitätseigenschaften. Dies ist einerseits einleuchtend, da dieser Entscheidungstyp die detailliertesten und damit auch die zahlreichsten Entscheidungen beinhaltet. Zusätzlich ist es aber auch der Entscheidungstyp, für den es im Demonstrator bereits eine Bibliothek gab, das heißt den Testpersonen wurde vorgeschlagen, sich mit diesen Entscheidungen zu befassen. Die Existenz der Bibliothek hat also maßgeblich dazu beigetragen, dass zusätzliche Entscheidungen getroffen

werden konnten. Daher ist eine Erkenntnis für zukünftige Forschung, dass die Bibliotheken auch auf andere Entscheidungstypen (also zum Beispiel Entscheidungen über die Systemarchitektur oder über die Veränderungen von Funktionen) ausgeweitet werden sollten.

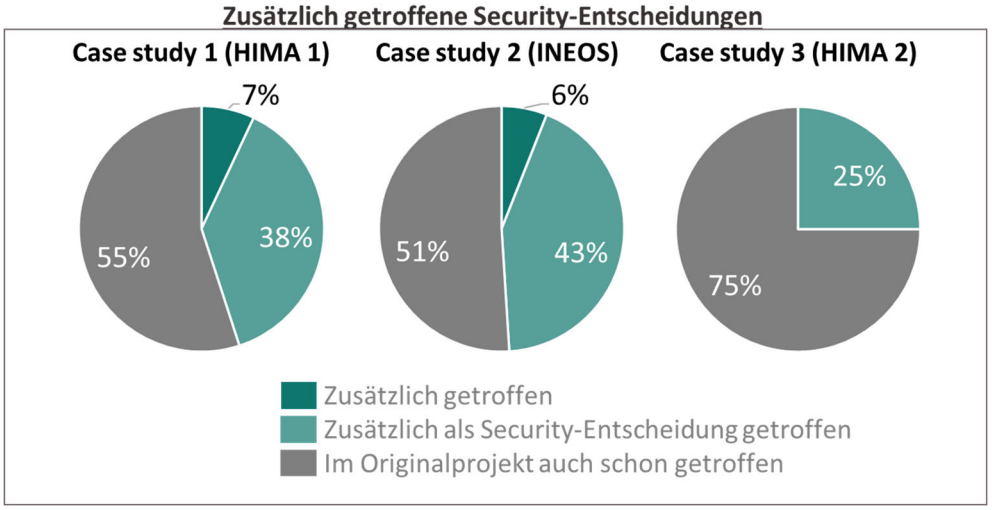

Abbildung 2-14: Zusätzliche Security-Entscheidungen aufgrund der neu entwickelten Methode in den drei Validierungsrunden

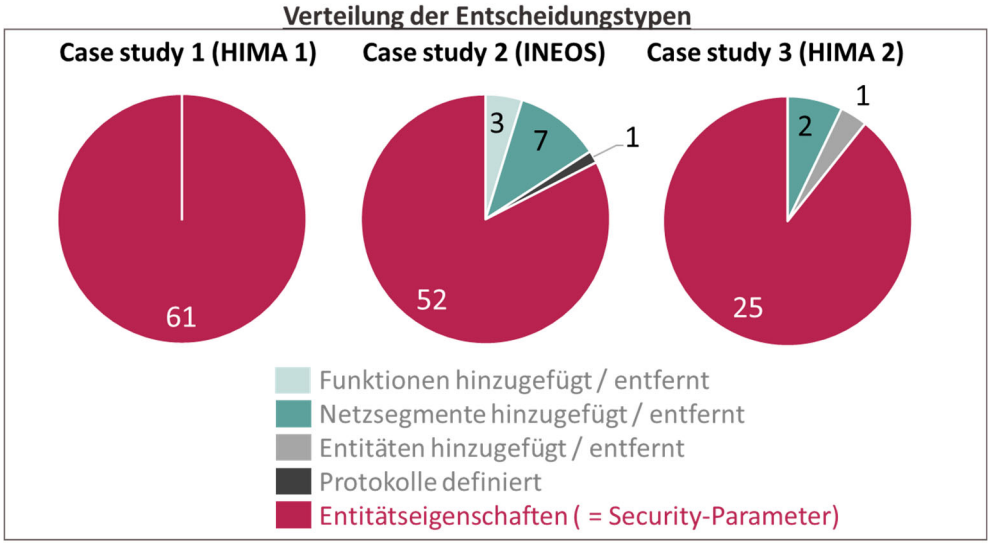

Abbildung 2-15: Verteilung der Entscheidungstypen der mit der neuen Methode getroffenen Security-Entscheidungen in den drei Validierungsrunden

Die Ergebnisse der Validierung wurden den Anwendungspartnern INEOS und HIMA präsentiert und mit ihnen diskutiert. Die Ergebnisse der Validierung sind in [7], [13], [6], [14] ausführlich beschrieben.

3 Veröffentlichungen und Kommunikation der Ergebnisse

1. **AALE 2022, Pforzheim (11.03.2022):** Taştan, Fluchs, Drath: „Warum wir ein Security-Engineering-Informationsmodell brauchen - Motivation, Anwendungsfälle und Konzept für ein neues Domänenmodell für Security-Engineering“, https://doi.org/10.33968/2022.25
2. **Entwurf komplexer Automatisierungssysteme (EKA) 2022, Magdeburg (23.06.2022):** Fluchs, Drath, Fay: “A Security Decision Base: How to Prepare Security by Design Decisions for Industrial Control Systems - Analysis of concepts for organizing security-relevant information from software engineering, requirements engineering, and systems engineering”, https://openhsu.ub.hsu-hh.de/entities/publication/14723

3. **Automation 2022, Baden-Baden (28.06.2022):** Fluchs, Taştan, Mertens, Horch, Ritter, Drath, Fay: „Security-Entscheidungen „by Design“ in das Engineering prozesstechnischer Anlagen integrieren. Konzept der „Automation Security by Design Decisions“, https://openhsu.ub.hsu-hh.de/entities/publication/14735
4. **Automation 2022, Baden-Baden (28.06.2022):** Taştan, Fluchs, Drath: „AutomationML-basierte Modellierungsansätze für ein Security-Engineering-Informationsmodel“, https://www.researchgate.net/publication/361741141_AutomationML-basierte_Modellierungsansatze_fur_ein_Security-Engineering-Informationsmodell
5. **atp-magazin (26.09.2022):** Fluchs, Taştan, Mertens, Ritter, Horch, Drath, Fay: Security by Design für Automatisierungssysteme. Teil 1: Begriffsklärung und Analyse existierender Ansätze, https://doi.org/10.17560/atp.v63i9.2620
6. **atp-magazin (26.09.2022):** Taştan, Fluchs, Drath: „AutomationML: Ansätze für ein Security-Engineering Informationsmodell“, https://atpinfo.de/produkte/atp-magazin-9-2022/
7. **IEEE IECON 2022, Brüssel (17.10.2022):** Fluchs, Taştan, Mertens, Horch, Drath, Fay: “Security by Design Integration Mechanisms for Industrial Control Systems”, https://doi.org/10.1109/IECON49645.2022.9968406
8. **NAMUR-Hauptsitzung, Neuss (10.11.2022):** Fluchs: Ein Informationsmodell für Security Engineering und warum wir das brauchen
9. **atp magazin (06.12.2022):** Fluchs, Taştan, Mertens, Ritter, Horch, Drath, Fay: „Security by Design Decisions für Automatisierungssysteme. Teil 2: Konzept für die Integration von Security-Entscheidungen“, https://doi.org/10.17560/atp.v63i11-12.2643
10. **IEEE Access (19.01.2023):** Fluchs, Drath, Fay: “Evaluation of visual notations as a basis for ICS security design decisions” (https://doi.org/10.1109/ACCESS.2023.3238326)
11. **S4x23 Conference, Miami, FL, USA (14.02.2023):** Sarah Fluchs: Security by Design Decisions, https://www.youtube.com/watch?v=qlvYe_UXIpo
12. **Sensors (13.06.2023)**: Fluchs, Taştan, Trumpf, Horch, Drath, Fay: “Traceable Security-by-Design Decisions for Cyber-Physical Systems (CPSs) by Means of Function-Based Diagrams and Security Libraries” https://doi.org/10.3390/s23125547
13. **AUTOMATION 2023, Baden-Baden (29.06.2023):** Taştan, Fluchs, Drath: „Security-Engineering mit AutomationML – Methodik zur Modellierung von Security-Entscheidungen, -Zielen, -Risiken und -Anforderungen“, https://www.researchgate.net/publication/372049746_Security-Engineering_mit_AutomationML_-_Methodik_zur_Modellierung_von_Security-Entscheidungen_-Zielen_-Risiken_und_-Anforderungen
14. **OT Cybersecurity Expert Panel Forum, Singapore (22.08.2023):** Fluchs**: “**Turning Security by Design from Myth to Reality”, https://www.youtube.com/watch?v=Wlkk8OMYvGc
15. **at - Automatisierungstechnik (08.09.2023):** Fluchs, Taştan, Trumpf, Horch, Drath, Fay: „Nachvollziehbare Security by Design-Entscheidungen für Automatisierungssysteme mittels funktionsbasierter Diagramme und Security-Bibliotheken, https://doi.org/10.1515/auto-2023-0084 (at - Automatisierungstechnik, vol. 71, no. 9, pp. 759–778)
16. **ZPT - Cyber Security für die produzierende Industrie 2023, Pforzheim (28.09.2023):** Taştan: Präsentation - „Security-by-Design Entscheidungen für Ingenieure ohne Security-Expertise“
17. **Industrial Security Conference 2023, Kopenhagen (13.11.2023):** Halmans: Präsentation – “Library-Based Security-by-Design“
18. **NAMUR-Empfehlung (02.07.2024):** Schüller, Fluchs, Höper, Reuter, Taştan, Ehrlich: NE 193 – Ein Informationsmodell für das Automation Security Engineering, https://www.dinmedia.de/de/technische-regel/namur-ne-193/382244840
19. **Dissertation (09.08.2024):** Fluchs: „A visual, model-based concept for making, documenting, and communicating cybersecurity decisions during and after the (re-)design of industrial cyber-physical systems”, https://openhsu.ub.hsu-hh.de/entities/publication/16760
20. **IEEE Transactions on Dependable and Secure Computing (im Peer Review seit 18.12.2023):** Fluchs, Tastan, Mertens, Horch, Matraxia, Drath, Fay: Communicating cybersecurity decisions and their rationales explicitly during and after CPS design

4 Finanzieller Nachweis

4.1 Wichtigste Positionen des zahlenmäßigen Nachweises

4.1.1 admeritia GmbH

Tabelle 4-1: Finanzieller Nachweis – admeritia GmbH

ID	Kostenposition	Bewilligt	Gesamtkosten 2021 - 06.2024
837	Personalkosten	1.048.705,20 €	1.188.898,87 €
838	Reisekosten	14.300,00 €	11.893,73 €
847	vorhabenspezifische Abschreibungen	15.478,00 €	18.924,37 €
850	sonstige unmittelbare Vorhabenkosten	16.390,00 €	20.326,22 €
	Summe	**1.094.873,20 €**	**1.240.043,19 €**

Pandemiebedingt wurden fast alle Projekttreffen in der gesamten Projektlaufzeit auf virtuelle Treffen umgestellt, was wodurch die Projekt-internen Reisekosten admeritia-seitig vollständig entfallen sind. Die Reisen zu Vorträgen auf Kongressen wurden nach der Pandemie ähnlich wie geplant durchgeführt. So sind die Reisekosten zwar weitestgehend angefallen, blieben aber etwas über 15% unterhalb der bewilligten Kosten.

Alle anderen Kostenpositionen sind vollständig angefallen und landeten am Ende auch leicht über dem im Jahr 2020 kalkulierten Umfang. Dies hatte insbesondere bei den Positionen der Abschreibungen und unmittelbaren Vorhabenkosten, den Ursprung in den Preissteigerungen für IT-Komponenten durch Lieferengpässe im Jahr 2021 und durch die hohe Inflation im Jahr 2022.

Die Personalkosten liegen etwas über dem Planungsstand, auch hier sind die Steigerungen der branchenüblichen Personalkosten in den letzten Jahren etwas höher gewesen, als im Jahr 2020 einkalkuliert.

Die über die bewilligten Förderbeträge hinausgehenden angefallenen Kosten trägt selbstverständlich die admeritia vollständig.

4.1.2 Hochschule Pforzheim

Tabelle 4-5: Finanzieller Nachweis - Hochschule Pforzheim

Nr.	Bezeichnung	Gesamt-bewilligt	2021	2022	2023	2024	
812	Beschäftigte E12-E15	274.037,44 €	61.019,89 €	71.774,88 €	72.643,31 €	65.282,03 €	
817	Beschäftigte E1-E11	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	
820	Lohnempfänger / Mitarbeiter	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	
822	Beschäftigungsentgelte (HiWis/LBA)	5.757,96 €	0,00 €	1.098,00 €	3.436,20 €	2.301,00 €	
831	Gegenstände bis zu 800 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	
834	Mieten und Rechnerkosten	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	
835	Vergabe von Aufträgen	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	
843	Sonstige allg. Verwaltungsausgaben	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	
846	Dienstreisen (ohne Reisekosten LBA)	3.600,28 €	0,00 €	1.255,68 €	2.616,70 €	0,00 €	
850	Gegenstände und Investitionen > 800 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	
Gesamtausgaben (ohne P-Pauschale)		283.395,68 €	61.019,89 €	74.128,56 €	78.696,21 €	67.583,03 €	
Bundesmittel (einschl. Projektpauschale)		**340.074,81 €**	80.292,23 €	88.696,65 €	96.011,40 €	72.712,95 €	
BMBF-Projektpauschale (20%)		56.679,14 €	12.203,98 €	14.825,71 €	15.739,24 €	13.516,61 €	
Bundesmittel laut Bescheid vom ...			25.10.21	14.11.22	17.11.23	17.11.23	**Summe**
Bundesmittel einschl. Projektpauschale		Jahres-scheiben	80.292,23 €	88.696,65 €	96.011,40 €	75.074,53 €	**340.074,81 €**
Kassenbestand			**5.890,30 €**	**5.675,62 €**	**6.988,91 €**	**0,00 €**	

In 2023 wurde eine kostenneutrale Projektverlängerung beantragt und genehmigt. Die Kostenneutralität wurde vorrangig durch die Auswirkungen der Corona-Pandemie und die damit verbundenen nicht ausgegebenen Mittel für studentische und wissenschaftliche Hilfskräfte (Beschäftigungsentgelte) sowie für Dienstreisen erreicht. Die im Projektplan vorgesehenen Treffen mit dem Konsortialführer und den assoziierten Partnern wurden unter den gegebenen Umständen virtuell durchgeführt, da geplante Präsenztreffen nicht realisiert werden konnten. Im Rahmen dieser kostenneutralen Projektverlängerung wurden die Mittel verwendet, um die notwendigen abschließenden Arbeiten im Jahr 2024 durch Einstellung von Frau Anastasiia Riabova als weitere Projektmitarbeiterin erfolgreich zu erledigen.
In 2024 wurden nur noch diejenigen Mittel abgerufen, die auch verbraucht wurden, so dass der Kassenbestand zum Ende des Projektes vollständig ausgeglichen ist.

5 Notwendigkeit und Angemessenheit der Projektarbeiten

5.1 admeritia GmbH

Die Entwicklung einer neuen Methode für die Integration von Security in die Automation-Engineering-Workflow ist eine risikobehaftete Aufgabe und wäre für die admeritia GmbH im normalen Projektgeschäft außerhalb des IDEAS-Projekts nicht möglich gewesen.
Einen Großteil der Zeit nahm die initiale Anforderungsanalyse sowie die anschließende Validierung der Projektergebnisse mit den Anwendungspartnern ein. Dies war essenziell, um sicherzustellen, dass die

entwickelte Methode für die Zielgruppe, Ingenieure bei Herstellern, Integratoren und Betreibern von Automatisierungssystemen, praktisch anwendbar und nützlich sein würde.
Weiterhin war die Programmierung und Optimierung des Demonstrators eine zeitintensive, aber absolut notwendige Arbeit, da der modell- und bibliotheksbasierten sowie sehr visuelle Ansatz ohne die Entwicklung einer Software nicht umsetzbar und somit auch nicht validierbar gewesen wäre. Als ein wesentlicher Akzeptanzfaktor für die entwickelte Methode wurde von Anfang an die Effizienz und Integrierbarkeit in den Alltag der Zielgruppe identifiziert. Mit manuell erstellten Modellen und Grafiken wäre dies kaum möglich gewesen.
Die durch die kostenneutrale Projektverlängerung möglich gewordene zusätzliche Validierung hat ermöglicht, dass beide Aspekte, die Praktikabilität der Methode für die Zielgruppe und ihre effiziente Umsetzung im Demonstrator, nach Umsetzung der Erkenntnisse aus den ersten Validierungsrunden erneut getestet und zusätzliche Erkenntnisse gewonnen werden konnten.

5.2 Hochschule Pforzheim

Die Hochschule Pforzheim hat das Projekt wissenschaftlich begleitet, die Vernetzung mit dem aktuellen und Stand der Forschung gefördert. Die HSPF hat neuartige Verfahren zur Integration von Security-Informationen in AutomationML über Python entwickelt. Insbesondere wurden Methoden zur systematischen Modellierung von Security-Analysen entwickelt. Die entstandenen Modelle sind maschinenlesbar und standardisierbar und ermöglichen die Entwicklung von Software-Schnittstellen für den automatisierten Datenaustausch.
Der Austausch mit der admeritia bzw. den assoziierten Industriepartnern im Projekt hat dazu beigetragen, ein tiefes Verständnis für die in der Praxis bzw. in Unternehmen vorliegenden Daten zu erhalten. Durch die enge Zusammenarbeit konnten die entwickelten Verfahren verifiziert und weiter verfeinert werden. Ohne den Einbezug der admeritia hätte die Hochschule Pforzheim in diesem Bereich keine wesentliche wissenschaftliche Forschung betreiben bzw. diese nicht angemessen evaluieren können.

6 Voraussichtlicher Nutzen, insbesondere Verwertbarkeit

6.1 admeritia GmbH

Die wirtschaftliche Verwertung der Projektergebnisse erfolgt durch admeritia über das Projektgeschäft sowie durch eine optimierte Beratung im Bereich der OT-Security innerhalb der Automatisierungstechnik. Zielkunden für die angestrebte Lösung sind zunächst größere Mittelständler und Großunternehmen mit komplexen industriellen Automatisierungssystemen und Produktions-anlagen. Seit Beginn des Projekts hat die Notwendigkeit, Security effizient in den Engineering-Prozess sowohl bestehender als auch neuer Anlagen zu integrieren, zugenommen. Ein Beispiel hierfür ist die steigende Aufmerksamkeit der Genehmigungsbehörden auf Sicherheitsaspekte bei der Genehmigung von Anlagen, die unter die Störfallverordnung (12. BImschV, „StörfallV“) oder die Betriebssicherheitsverordnung fallen. Für Hersteller von Automatisierungstechnik sind die zusätzlichen regulatorischen Anforderungen durch das IT-Sicherheitskennzeichen des BSI und den Cyber Resilience Act (CRA) ein weiteres Beispiel. Mit dem Abschluss des Projekts plant admeritia eine etwa 6- bis 9-monatige Phase der Markteinführung. In dieser Phase sollen die Projektergebnisse, einschließlich der entwickelten Methodik und des Software-Werkzeugs, zur Marktreife gebracht werden. Dies umfasst die Schulung der Methodik für admeritia-eigene Berater und später auch für Kunden. Mit Blick auf die wirtschaftliche Verwertung sowie Pflege und Weiterentwicklung der Projektergebnisse wurden bei der admeritia bestehende Entwicklerstellen verstetigt sowie weitere Stellen neu geschaffen. Dies ermöglicht es dem Unternehmen, die gewonnenen Erkenntnisse und Technologien langfristig in die Praxis umzusetzen und kontinuierlich weiterzuentwickeln, um den wachsenden Anforderungen an Security in der Automatisierungstechnik gerecht zu werden.

6.2 Hochschule Pforzheim

Für die Hochschule Pforzheim umfasst die wissenschaftliche und technische Verwertung ebenfalls mehrere Aspekte. Die Ergebnisse wurden auf Konferenzen veröffentlicht. Durch diese Publikationen wurde angestrebt, die Ergebnisse einer breiten Leserschaft zugänglich zu machen und deren Bedeutung in relevanten Leitmedien hervorzuheben. Darüber hinaus wird die Hochschule Pforzheim durch die Teilnahme an Projekten und die Nutzung neuer Methoden ihre Fachkompetenz weiter ausbauen und den wissenschaftlichen Nachwuchs fördern. Die Beteiligung an innovativen Projekten bietet eine wertvolle Gelegenheit zur Erweiterung der Kenntnisse und Fähigkeiten der beteiligten Professoren und Nachwuchskräfte. Ein weiterer wichtiger Aspekt ist der Ausbau des Netzwerks zu Experten und Institutionen. Der intensive Wissensaustausch und die Zusammenarbeit mit anderen Fachleuten ermöglichen es, neue Erkenntnisse zu gewinnen und Synergien zu nutzen. Schließlich wird die Hochschule Pforzheim auch Impulse zur Weiterentwicklung des AutomationML Editors geben. Die Projektergebnisse werden verwendet, um die Funktionalität und Effizienz des Editors zu verbessern, indem Feedback und Anregungen aus der Praxis integriert werden. Die Hochschule Pforzheim verfolgt hingegen keine wirtschaftlichen Verwertungsinteressen in Bezug auf die Projektergebnisse.

7 Fazit

Das Projekt IDEAS hat sein Forschungsziel erreicht: Automatisierungsingenieuren, die bereits während der Entwicklung die Security ihrer Systeme berücksichtigen wollen, stehen nun eine Methode und ein Software-Demonstrator inklusive Schnittstellen für die Integration in die bestehende Engineering-Toollandschaft zur Verfügung.

Die Anwendung der entwickelten Methode kann außerdem die Entscheidungsfindung und -kommunikation während und nach der Designphase von Automatisierungssystemen verbessern. Für Hersteller bietet dies die Chance, Security-Merkmale ihrer Produkte explizit zu machen und Kunden besser zu erklären. Betreiber profitieren, indem sie ihre eigenen Security-Prioritäten klarer an die Hersteller kommunizieren und nachvollziehen können, inwiefern diese berücksichtigt wurden.
Während des Projekts ergaben sich vielversprechende Anknüpfungspunkte für zukünftige Forschung:

- Weiterentwicklung des Bibliotheks-Ansatzes zur Identifikation und Wiederverwendung von Security-Entscheidungen. Dieser war ursprünglich im Projekt gar nicht geplant, erwies sich aber in der Validierung als großer Erfolgsfaktor.
- Weiterentwicklung der bislang auf Integratoren und Betreiber ausgelegten Methode für die Bedürfnisse von Komponentenherstellern. Dies gewinnt nicht zuletzt aufgrund mittlerweile entstandener Regularien für die Cybersecurity von Komponentenherstellern (Cyber Resilience Act der EU für digitale Produkte, R 155 / R 156 der UNECE für die Automobilindustrie, PSTI Act in UK für Consumer IoT) an Bedeutung.

Quellen

[1] NAMUR NA 35, „Engineering and execution of PCT projects in process industry“. 2019.
[2] M. Hollender, *Collaborative process automation systems*. Research Triangle Park, NC: ISA, 2010.
[3] S. Fluchs *u. a.*, „Security-Entscheidungen ‚by Design‘ in das Engineering prozesstechnischer Anlagen integrieren. Konzept der ‚Automation Security by Design Decisions‘“, gehalten auf der AUTOMATION 2022 (23. Leitkongress der Mess- und Automatisierungstechnik), Baden-Baden, Germany, Juni 2022. [Online]. Verfügbar unter: https://www.researchgate.net/publication/361650012_Security-Entscheidungen_by_Design_in_das_Engineering_prozesstechnischer_Anlagen_integrieren_-_Konzept_der_Automation_Security_by_Design_Decisions
[4] R. Drath, *AutomationML: das Lehrbuch für Studium und Praxis*. in De Gruyter Studium. Berlin Boston: De Gruyter Oldenbourg, 2022. doi: 10.1515/9783110782998.
[5] E. Taştan, S. Fluchs, und D. Rainer, „Warum wir ein Security-Engineering-Informationsmodell brauchen“, in *Wissenstransfer im Spannungsfeld von Autonomisierung und Fachkräftemangel*, Hochschule für Technik, Wirtschaft und Kultur Leipzig, Jan. 2022. doi: 10.33968/2022.25.
[6] S. Fluchs, „Cybersecurity Decision Diagrams: A visual, model-based concept for making, documenting, and communicating cybersecurity decisions during and after the (re-)design of industrial cyber-physical systems“, Helmut Schmidt Universität / Universität der Bundeswehr Hamburg, Hamburg, 2024. [Online]. Verfügbar unter: https://doi.org/10.24405/16760
[7] S. Fluchs, E. Taştan, T. Trumpf, A. Horch, R. Drath, und A. Fay, „Traceable Security-by-Design Decisions for Cyber-Physical Systems (CPSs) by Means of Function-Based Diagrams and Security Libraries“, *Sensors*, Bd. 23, Nr. 12, S. 5547, 2023, doi: 10.3390/s23125547.
[8] A. A. Bochman und S. G. Freeman, *Countering Cyber Sabotage. Introducing Consequence-Driven, Cyber-Informed Engineering (CCE)*, First edition Published 2021. Boca Raton, Florida: CRC Press, Taylor & Francis Group, 2021.
[9] U.S. Department of Energy, Hrsg., „National Cyber-Informed Engineering Strategy“. 2022. [Online]. Verfügbar unter: https://www.energy.gov/sites/default/files/2022-06/FINAL%20DOE%20National%20CIE%20Strategy%20-%20June%202022_0.pdf
[10] E. Taştan, R. Drath, und S. Fluchs, „Security-Engineering mit AutomationML – Methodik zur Modellierung von Security-Entscheidungen, -Zielen, -Risiken und -Anforderungen“, in *Automation 2023*, VDI Wissensforum GmbH, Hrsg., VDI Verlag, 2023, S. 413–428. doi: 10.51202/9783181024195-413.
[11] AutomationML consortium, „AutomationML Whitepaper Communication, Version 1.0“. September 2014. Zugegriffen: 11. Dezember 2018. [Online]. Verfügbar unter: https://www.automationml.org/o.red/uploads/dateien/1459418220-AutomationML%20Whitepaper%20-%20AutomationML%20Communication%20v1_Sept2014.pdf
[12] E. Taştan, S. Fluchs, und R. Drath, „AutomationML-basierte Modellierungsansätze für ein Security-Engineering-Informationsmodell“, gehalten auf der AUTOMATION 2022 (23. Leitkongress der Mess- und Automatisierungstechnik), Baden-Baden, Germany, Juni 2022. [Online]. Verfügbar unter: https://www.researchgate.net/publication/361741141_AutomationML-basierte_Modellierungsansatze_fur_ein_Security-Engineering-Informationsmodell
[13] S. Fluchs, E. Taştan, T. Trumpf, A. Horch, R. Drath, und A. Fay, „Nachvollziehbare Security by Design-Entscheidungen für Automatisierungssysteme mittels funktionsbasierter Diagramme und Security-Bibliotheken“, *at - Automatisierungstechnik*, Bd. 71, Nr. 9, S. 759–778, Sep. 2023, doi: 10.1515/auto-2023-0084.
[14] S. Fluchs *u. a.*, „Communicating cybersecurity decisions and their rationales explicitly during and after CPS design (to be published)“, *IEEE Transactions on Dependable and Secure Computing*, 2024.

Bundesministerium
für Bildung
und Forschung

admeritia

HS PF

Kurzbericht zum BMBF-Forschungsprojekt

Vorhabenbeschreibung	IDEAS - Integrated Data Models for the engineering of Automation Security
Förderkennzeichen	16KIS1269K
Projektkonsortium	**admeritia GmbH** (KMU + Konsortialführer) **Hochschule Pforzheim** (Forschungseinrichtung) **INEOS Manufacturing Deutschland GmbH** (assoziierter Anwendungspartner) **HIMA Paul Hildebrandt GmbH** (assoziierter Anwendungspartner)
Laufzeit des Vorhabens	01.01.21-30.06.24
Autoren	Sarah Fluchs (admeritia GmbH) Emre Tastan (Hochschule Pforzheim) Prof. Dr.-Ing. Rainer Drath (Hochschule Pforzheim)
Datum	05.12.2024

1 Kurze Darstellung zum Projekt

1.1 Motivation und Aufgabenstellung

Abbildung 1-1: IDEAS-Logo

Mit der zunehmenden Vernetzung von Industrie 4.0-Komponenten werden automatisierte Anlagen anfälliger für IT-Angriffe und Schadsoftware.
Während funktionale Sicherheit streng reguliert ist, fehlten bislang vergleichbare Vorschriften für die Cybersecurity für die Entwicklung von Anlagen. Die Implementierung von Security-Maßnahmen kann die Produktionsleistung beeinträchtigen, etwa durch reduzierte Reaktionszeiten aufgrund von Verschlüsselung. Um das zu vermeiden, ist es wichtig, frühzeitig im Engineering-Prozess Security-Anforderungen zu definieren, um mit den funktionalen Anforderungen verträgliche Security-Maßnahmen zu finden. Security-Engineering muss also wie die funktionale Sicherheit in den Automatisierungsprozess integriert werden. Security-Maßnahmen müssen bereits in der Entwicklungsphase integriert werden, anstatt sie nachträglich hinzuzufügen. Um breite Akzeptanz zu erreichen, müssen die Security-Methoden effizient und praktikabel für Ingenieure umsetzbar sein.
Im Projekt „Integrated Data Models for the Engineering of Automation Security“ (IDEAS) wurde untersucht, wie der Security-Engineering-Prozess effektiv in den bestehenden Automatisierungs-Engineering-Prozess integriert werden kann. Die Forschungsfragen lauteten:

- Forschungsfrage 1 (Analyse): Wie kann sich Security-Engineering künftig frühestmöglich in den Engineering-Prozess einer automatisierten Anlage eingliedern?
- Forschungsfrage 2 (Datenmodellierung): Wie und in welchen Phasen des Automatisierungs-Engineerings können security-relevante Informationen in einem elektronischen Datenmodell systematisch abgebildet werden?
- Forschungsfrage 3 (Wertschöpfung): Wie kann auf Basis des Datenmodells mittels eines Engineering-Werkzeugs der Security-Engineering-Prozess effizient unterstützt werden?

Die Zielgruppe waren Automatisierungs- bzw. Leittechnikingenieure, die im Ergebnis befähigt werden sollen, Security bei der Entwicklung und Pflege ihrer Systeme im Sinne von „Security by Design“ direkt zu berücksichtigen.
Das Projekt wurde von einem Automatisierungstechnik-Hersteller und einem -Betreiber unterstützt, um die praktische Anwendbarkeit der Ergebnisse sicherzustellen.

1.2 Wissenschaftlicher und technischer Stand, an den angeknüpft wurde

Im Projekt wurde auf existierende Methoden für das Threat Modeling und die Security-Risikoanalyse aufgebaut: auf die ISA/IEC 62443-Reihe, das Threat Modeling Framework MITRE ATT&CK sowie anlagennahe OT-Security-Methoden wie das Consequence-Based, Cyber-informed Engineering und das Security PHA Review, mit dem Ergebnisse der funktionalen Sicherheit für die Cybersecurity nutzbar gemacht werden können. Im Bereich der Datenmodelle entwickelt der AutomationML e.V. Empfehlungen für Automatisierungskomponenten und Kommunikationsnetzwerke, die als Basis verwendet wurden, um zusätzlich Security-Aspekte abzubilden.

1.3 Planung und Ablauf des Vorhabens

Das Projekt IDEAS war ursprünglich für den Zeitraum vom 01.01.2021 bis zum 31.12.2023 geplant. Aufgrund der pandemiebedingten Herausforderungen wurde eine kostenneutrale Verlängerung bis zum 30.06.2024 gewährt. Das Gesamtvolumen des Vorhabens betrug 1,43 Millionen Euro, wovon 69% durch das Bundesministerium für Bildung und Forschung (BMBF) finanziert wurden. Die admeritia GmbH leitete das Projekt als Konsortialführer. Zusätzlich haben als assoziierte Anwendungspartner INEOS Manufacturing Deutschland GmbH (Betreiber) sowie die HIMA Paul Hildebrandt GmbH (Hersteller) Anforderungen und Beispieldatensätze aus der Praxis beigetragen und dem Forschungsteam ermöglicht, die Ergebnisse anhand realer Engineering-Projekte zu validieren. Ein dritter assoziierter Anwendungspartner war die NAMUR – Interessengemeinschaft Automatisierungstechnik der Prozessindustrie e.V. Gemeinsam mit dem NAMUR-Arbeitskreis AK 1.3 Informationsmodelle hat das Forschungsteam ein UML-Datenmodell für das Security-Engineering entwickelt.

admeritia GmbH

Gesamtmittel: 1.094.873,20 €
BMBF [60 % FÖRDERQUOTE]: 656.923,92 €
EIGENANTEIL: 437.949,28 €

Hochschule Pforzheim – Gestaltung, Technik, Wirtschaft und Recht
Gesamtmittel: 340.074,81 €
BMBF [100 % FÖRDERQUOTE]: 340.074,81 €

1.4 Wesentliche Ergebnisse aus IDEAS

Forschungsfrage 1 (Analyse): Wie kann sich Security-Engineering künftig frühestmöglich in den Engineering-Prozess einer automatisierten Anlage eingliedern?
Nach eingehender Analyse der bestehenden Automation-Security-Engineering-Prozesse wurde die ursprüngliche Idee eines festen Phasenmodells, in das Security integriert wird, verworfen. Stattdessen wurde ein modellbasiertes Konzept entwickelt: Ein Anlagenmodell, das nur security-relevante Informationen enthält, wird als zusätzliche Lieferleistung von Anfang an im Engineering mitgepflegt.
Es wird im Vorhinein in Form von „Security-Entscheidungspunkten“ definiert, welche Änderungen am Modell security-relevant sind – zum Beispiel Netzwerkarchitekturentscheidungen, Entscheidungen über die Funktionen von Feldgeräten oder Entscheidungen über die Detailkonfigurationen von Steuerungen. Sobald diese Entscheidungen während des Engineerings getroffen werden, werden ihre Security-Implikationen mitberücksichtigt, sie werden als Security-Entscheidungen dokumentiert und mit einer Begründung versehen.
Forschungsfrage 2 (Datenmodellierung): Wie und in welchen Phasen des Automatisierungs-Engineerings können security-relevante Informationen in einem elektronischen Datenmodell systematisch abgebildet werden?
Es wurde sowohl ein UML-Modell als auch ein AutomationML-Modell entwickelt, um security-relevante Anlageninformationen systematisch abbilden zu können.
Forschungsfrage 3 (Wertschöpfung): Wie kann auf Basis des Datenmodells mittels eines Engineering-Werkzeugs der Security-Engineering-Prozess effizient unterstützt werden?
Die Effizienz in der Security-Entscheidungsfindung kann vor allem durch Bibliotheken erhöht werden. Diese Bibliotheken ermöglichen eine schnellere Modellierung der security-relevanten Aspekte einer Anlage sowie die Wiederverwendbarkeit von Bedrohungsmodellen und Security-Entscheidungen (mitsamt Begründungen) für bestimmte Anlagenmodelle.