Industrie 4.0 Schwachstellen: Basisangriffe und Szenarien

Robert Fischer[1] · Robert Clausing[2] · Jana Dittmann[1] · Yongjian Ding[2]

[1]Otto-von-Guericke University of Magdeburg
Department of Computer Science
robert.fischer@ovgu.de
jana.dittmann@iti.cs.uni-magdeburg

[2]Magdeburg-Stendal University of Applied Sciences
Department of Electrical Engineering
{robert.clausing | yongjian.ding}@hs-magdeburg.de

Zusammenfassung

Mit dem Fortschreiten der vierten industriellen Revolution ergeben sich neue Herausforderungen für die IT-Security hinsichtlich Automationstechnik und eingesetzter IT-Komponenten. Eine wesentliche Herausforderung besteht in der Pauschalisierung und adäquaten Abbildung von komplexen Industrie 4.0 Systemlandschaften, bestehend aus einer Vielzahl von heterogenen Komponenten. Für den Umgang mit diesen sehr komplexen Strukturen wird ein Ansatz vorgeschlagen, der für die Untersuchung von Angriffstechniken auf Umgebungen der Industrie 4.0 erarbeitet wurde. Bestandteile des vorgeschlagenen Ansatzes sind, eine komponentenbasierte Modellierung von Systemlandschaften / Zielinfrastrukturen sowie der Einbezug eines zeitabhängigen Kontexts zur Modellierung von Angriffen und Angreifern. Eine Demonstration der vorgeschlagenen Ansätze erfolgt in Form einer exemplarischen Anwendung unter Verwendung der Basisangriffe. Basierend auf einem adaptierten Praxisvorfall erfolgt die Beschreibung eines komplexen mehrstufigen Angriffsszenarios. Die grundsätzliche Anwendbarkeit der vorgeschlagenen Ansätze kann damit gezeigt werden. Gleichzeitig wurden dabei neue Forschungsfragen sowie die Notwendigkeit weiterer Verfeinerungen identifiziert.

1 Einleitung

Durch gesteigerte politische und gesellschaftliche Anstrengungen im Bereich Industrie 4.0 werden aktuell zwei wichtige Trends beschleunigt und verstärkt. Zum einen, die steigende Anzahl der, mit dem Ziel einer stärkeren Automatisierung von industriellen Umgebungen, eingesetzten IT-basierten Komponenten (Hardware- und Softwaremodule der Automation). Zum anderen, der Trend eines umfassenden Wandels industrieller Strukturen von geschlossenen und weitgehend isolierten Verbünden, hin zu komplexen verteilten Umgebungen [Acat14], bestehend aus untereinander bzw. mit dem Internet vernetzten und interagierenden Anlagen (Anlagenverbünden) [BiVZ15]. Weitere Herausforderungen ergeben sich aus der zunehmenden Komplexität und oftmals ausgeprägten Heterogenität der einzelnen eingesetzten Hard- und Software-Komponenten. Dies führt in vielen Fällen zum Einsatz von nicht standardisierten, maßgeschneiderten Einzellösungen. Neben hohen Kosten sind solche Insellösungen ggf. mit einem negativen Einfluss u.a. auf Wartbarkeit, Zuverlässigkeit, Effizienz und Security der Anlagen verbunden. Der Transformationsprozess in Richtung Industrie 4.0 schließt praktisch alle Industriebereiche

P. Schartner (Hrsg.) · D•A•CH Security 2016 · syssec (2016) 350-362.

ein, hat aber bedingt durch hohe Verfügbarkeits- und Safety-Anforderungen, eine zusätzlich gesteigerte Relevanz für den Bereich kritischer Infrastrukturen [Plat15]. Die Angreifbarkeit vernetzter Industrie 4.0 Umgebungen (hier konkret Energieversorger) wurde im Dezember 2015 in der Ukraine demonstriert [Icsc16]. Dabei wurden mehrere Kraftwerke nahezu zeitgleich attackiert. Als Eintrittspunkt hat der VPN-Fernzugriff gedient. Als Resultat der Attacke wurde die Stromversorgung unterbrochen. Da die Vorgehensweise bei mehreren Kraftwerken angewendet wurde, kam es zu einer Unterbrechung der Versorgung von ca. 225.000 Kunden. Bei diesem Angriff wurden u.a. Trojanische Pferde eingesetzt. Malware stellt nach [MiRo12] oft einen Hauptbestandteil von Cyberangriffen dar. Die Infizierung lässt sich dabei oft auf Social-Engineering in verschiedenen Formen zurückführen. Basierend auf [NcIc16] wird dies mehrheitlich über Spear-Phishing umgesetzt. Außerdem konnten in der Vergangenheit oftmals infizierte USB-Speichermedien, Watering Holes und voreingestellte Zugangsdaten identifiziert werden.

Die Erforschung von Techniken zur adäquaten Schwachstellen- und Angriffsmodellierung sowie Durchführung systematischer Sicherheitsanalysen für komplexe Industrie 4.0 Anlagen stellt daher aktuell ein wichtiges Forschungsfeld in den Bereichen Modellierung von Sicherheit, sichere Steuerung von Industrieprozessen und Schutz kritischer Infrastrukturen dar. In anderen Informatik-Disziplinen, etwa System- und Software Design/Entwicklung, haben sich bei ähnlich stark ausgeprägten Herausforderungen im Umgang mit hoch-komplexen Strukturen modell-getriebene Techniken bewährt [Pric14]. Daher versprechen diese Ansätze auch für die Unterstützung von systematischen Sicherheitsanalysen hohes Potential. Nach derzeitigem Stand der Recherche sind existierende Ansätze zur Sicherheitsanalyse und Modellierung von Sicherheit in unterschiedlicher Art limitiert und eignen sich daher nicht für die angestrebte Realisierung eines ganzheitlichen Ansatzes. Die identifizierten Einschränkungen ergeben sich etwa durch eine Beschränkung auf spezifische Teilfragen (z.B. Netzwerk-, Applikations-Schwachstellen) oder unzureichende Möglichkeiten zur Abbildung von realistischen Angriffsabläufen, unter Berücksichtigung von z.B. Voraussetzungen und Auswirkungen individueller Angriffsschritte, vielfältiger Kombination von Einzelangriffen oder Einbezug zeitabhängiger Aspekte. Die hier vorgestellten Ansätze verfolgen das Ziel der Vorbereitung und Unterstützung von Sicherheitsanalysen, die sowohl den Anforderungen von Industrie 4.0 Umgebungen gerecht werden, als auch die differenzierten Eigenschaften komplexer Angriffsabläufe und individueller Angreifer einbeziehen. Für die weitere Betrachtung werden folgende Forschungsfragen formuliert.

- Erstens, die Erarbeitung von Ansätzen zur anlagen-unabhängigen Modellierung komplexer Systemlandschaften unter Berücksichtigung vielfältiger Netzwerk- und Steuerungslogikeigenschaften.
- Zweitens, die Erarbeitung von Ansätzen zur systematischen Modellierung und Pauschalisierung von Angriffen und Angreifern unter Berücksichtigung komplexer Angriffsabläufe und individueller Angreifereigenschaften.

In Kapitel zwei erfolgt die Darstellung und Zusammenfassung von identifizierten Arbeiten zu Sicherheitsaspekten, Basisangriffen, Angriffs- und Analysezielen in der Schwachstellenanalyse von ICS Umgebungen (Industrial Control Systems) sowie zur Angriffs- und Schwachstellenmodellierung. In Kapitel drei wird ein erster Ansatz zur systematischen, anlagen-unabhängigen Identifikation möglicher Bedrohungsszenarien/Angriffsstrategien vorgestellt. Dies umfasst einen Vorschlag zur strukturierten, anlagen-unabhängigen Abbildung komplexer Systemlandschaften sowie zur Systematisierung der betrachteten Analyse-Scopes und darauf aufbauend

einen Vorschlag zur zeitabhängigen, kontext-basierten Modellierung von Angriffen und Angreifern. In Kapitel vier erfolgt eine exemplarische Anwendung der erarbeiteten Ansätze als Darstellung eines komplexen Angriffsszenarios, abgeleitet von einem aktuellen Praxisvorfall und unter Verwendung der Basisangriffe. Eine Diskussion der eingeführten Ansätze hinsichtlich Stand der Technik und identifizierter Einschränkungen erfolgt in Kapitel fünf. Den Abschluss bildet die Zusammenfassung der wesentlichen Ergebnisse sowie mögliche Fragestellungen für künftige Arbeiten in Kapitel sechs.

2 Stand der Technik

Fokus dieser Arbeit ist die Untersuchung modell-getriebener Ansätze zur Vorbereitung und Unterstützung von Sicherheitsanalysen bzw. zum Testen der Informationssicherheit von IT-Strukturen in Industrie 4.0 Umgebungen. Identifizierte Ansätze in diesem Bereich sind u.a. AutomationML [BeSc15] und die Cyber-Security-Modeling-Language (CySeMoL) [HSBE15]. AutomationML ermöglicht eine XML-basierte Erfassung, Speicherung und Übertragung von Ingenieursdaten. CySeMoL ist ein probabilistisches Tool, das auf Angriffsgraphen basiert und die Abschätzung der Sicherheit von Systemarchitekturen ermöglichen soll. Miteinander verbundene Angriffsschritte besitzen korrespondierende Bayessche Netze, um die Auftrittswahrscheinlichkeit dieser Schritte abzuschätzen. Industrie 4.0 spezifische Eigenschaften (z.B. Impact auf Produktionsprozesse oder strukturelle Effekte) werden durch die identifizierten Ansätze und Werkzeuge aus der Informationssicherheit nicht berücksichtigt.

Domänen-spezifische Vorarbeiten (bspw. [KoTG13]) deuten darauf hin, dass zum einen, bisher in Normen und Empfehlungen wie [Agen12] uneinheitliche Formulierungen und Systematisierungen u.a. für Maßnahmen, Strukturwirkung, Systemlandschaft, Angriffsszenarien, Ziele sowie Analysebereiche genutzt werden. Zum anderen, werden die für Automationsumgebungen spezifischen Eigenschaften losgelöst von bekannten Ansätzen aus der IT-Security betrachtet. Beispielsweise die Einführung von sogenannten Geltungsbereichen (Scopes) in [Agen12], in Form von SCADA-Entwicklungsstationen, SPS-Programmierkonsolen, portablen Geräten, SCADA-Anwendungen und Ingenieursstationen. Wichtige Grundlagen für den vorgestellten Ansatz sind die relevanten Sicherheitsaspekte (Vertraulichkeit, Integrität, Authentizität, Verfügbarkeit, Nachweisbarkeit) [ChHi13], die aus der IT-Security bewährten Basisangriffe (Lesen, Unterbrechen, Modifizieren, Stehlen/Löschen, Erzeugen) [LDKH07] sowie die bekannten Angriffs- und Analyseziele aus der Schwachstellenanalyse [FrGr14, SPL+15] von ICS Umgebungen (Industrial Control Systems). Weitere relevante Arbeiten zur Angriffs- und Schwachstellenmodellierung sind u.a. CNIT [HoLo98] und Kill-Chain [HuCA11]. Zu berücksichtigen sind ferner die zum Zeitpunkt des Beitrages laufenden, nicht abgeschlossenen Arbeiten zur Industrie 4.0 Standardisierung, z.B. das Referenzarchitekturmodell (RAMI 4.0 [ABD+15]).

Die Ergebnisse der Literaturrecherche unterstreichen den Bedarf von Anlagen-unabhängigen Ansätzen zur ganzheitlichen Sicherheitsuntersuchung und Identifikation von Bedrohungsszenarien und Angriffsstrategien für Industrie 4.0 Umgebungen. Solche Ansätze sollten generalisierte Analysebereiche beinhalten, um eine Systematisierung und ein generisches Vorgehen zur Lokalisierung von Schwachstellen für unterschiedliche IT-Komponenten bzw. Automationssysteme (Hardware und Software), Anlagen und Anlagenverbünde sowie Netzwerk-, Kommunikations- und Steuerbeziehungen zu unterstützen.

3 Beschreibung der vorgeschlagenen Ansätze

Als Startpunkt für eine pauschalisierte Untersuchung von Anlagen dient die in Abbildung 5 dargestellte Referenzarchitektur aus [CFDD16]. Die vorgeschlagene Referenzarchitektur setzt sich aus mehreren Ebenen zusammen: einem Unternehmensnetzwerk mit Demilitarisierter Zone (DMZ), eine DMZ für die Leittechnik zur Übergabe von Prozess- und Produktionsdaten, der eigentlichen Leittechnik für Überwachung bzw. Projektierung der Anlage, den Steuerungsnetzwerken für Kommunikation zwischen Speicherprogrammierbaren Steuerungen (SPS) und letztlich den Feldgeräten, bestehend aus unterschiedlichen Sensoren bzw. Aktoren. Es ist zu berücksichtigen, dass mit dem Fortschreiten von Industrie 4.0 ein Wechsel der eingesetzten Kommunikationsprotokolle auf Stufe 1 bis 3 stattfindet. Traditionell eingesetzte Feldbus-Implementierungen (z.B. Profi-Bus) werden zunehmend durch Ethernet-basierte Ansätze ersetzt und die Anwendungen auf den bewährten TCP/IP Protokollstack aufgesetzt.

3.1 Modellierung Systemlandschaft (Ziel-Infrastruktur)

Die systematische Abbildung einer industriellen Anlage wie in Abbildung 5 erfordert die Verwendung von generischen und wiederverwendbaren Bausteinen. In Tabelle 1 werden Basis-Elemente vorgeschlagen, die eine strukturierte Abbildung unterstützen sollen. Der Ansatz basiert auf Vorarbeiten [CFDD16] und wird hier weiter verfeinert und detailliert. Ein zentrales Element des Vorschlags sind Entitäten für die Modellierung von Hardware- (physische Entität *PE*) und Software-Komponenten (logische Entität *LE*). Die Kommunikation zwischen Entitäten erfolgt über Schnittstellen, welche ebenfalls logischer oder physischer Art sein können. Benutzer interagieren über physische Schnittstellen (z.B. Tastatur, Maus, Monitor) mit physischen Entitäten (z.B. Workstation, Terminal, Server). Logische Entitäten (Software-Komponenten) kommunizieren und tauschen Daten über logische Schnittstellen (Programmschnittstellen, Dienste, API). Schnittstellen sind durch Übertragungsmedien miteinander verbunden, physische Schnittstellen z.B. durch eine Netzwerkverkabelung, logische Schnittstellen z.B. durch Shared Memory. Für die Nutzung von Schnittstellen und Übertragungsmedien werden Protokolle zugewiesen. Menschen werden in physischer Ausprägung als Personen abgebildet. Durch Authentifikation an einem entsprechenden System, können physische Personen in logische, interne Repräsentation überführt werden. Dieser Prozess erfordert initial die Anmeldung einer *Person* an einer physischen Entität. Die resultierende logische Repräsentation *Account*, ermöglicht den Zugriff auf logische Schnittstellen wie z.B. Programmschnittstellen (Abbildung 1).

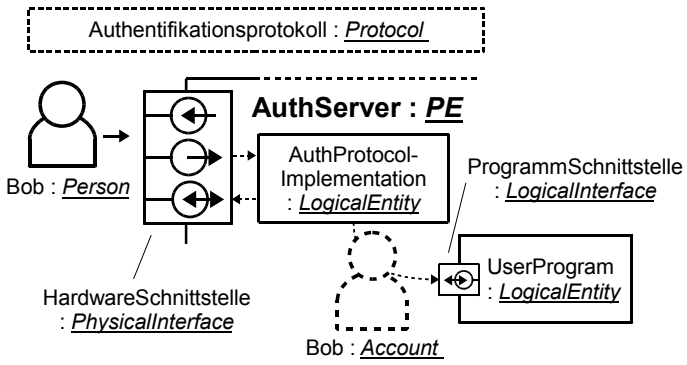


Abb. 1: Authentifikation und Repräsentation von Menschen: physisch (*Person*), logisch (*Account*)

Abzielend auf die Erstellung von hierarchisch strukturierten Modellen werden generalisierte Basis-Elemente definiert und zu Mengen zusammengefasst. Die Basis-Elemente und deren

mögliche Kombinationen werden in Tabelle 1 beschrieben. Die hier vorgestellten ersten Ansätze zielen auf die Identifikation von generalisierten Strukturen. Die Autoren erkennen an, dass die Elemente, abhängig von spezifischen Anwendungsfällen, einer weiteren Verfeinerung und Spezialisierung bedürfen. Logische Entitäten werden mit den zugehörigen logischen Schnittstellen und Daten zu Software-Komponenten zusammengefasst und können weitere logische, aber keine physischen, Entitäten (z.B. Unterprozesse, Dienste) kapseln. Analog dazu werden Hardware-Komponenten als Menge von physischen Entitäten und physischen Schnittstellen abgebildet, die jeweils wieder Software-Komponenten beinhalten können. Eine industrielle Anlage setzt sich zusammen aus einer Menge von Hardware-Komponenten inkl. deren Software-Komponenten, Kommunikationsbeziehungen, Steuer- und Businessprozessen sowie Menschen und Daten. Als Anlagenverbund wird eine Menge von mehreren Anlagen, Steuerprozessen und (Anlagen-)Daten definiert.

Tab. 1: Zusammenfassung der Basis-Elemente und mögliche Kombinationen

Element	Notation	Beschreibung
Entität	PhysicalEntity (PE) LogicalEntity (LE)	Physische Entitäten können physische u. logische Entitäten enthalten, logische Entitäten nur logische Entitäten
Schnittstelle	PhysicalInterface (PIf) LogicalInterface (LIf)	Schnittstellen bilden Ein- und Austrittspunkte von Entitäten
Protokoll	LogicalProtocol (Protocol)	Protokolle sind Verarbeitungsvorschriften zur Nutzung von Schnittstellen/Übertragungsmedien (Spezifikation vs. Implementierung), Protokoll-Impl. kapseln Zugriff auf Schnittstellen
Mensch	Person (Pers) Account (Acc)	Personen interagieren über physische Schnittstellen mit physischen Entitäten, Authentifizierungsprozesse bilden physische Personen auf logische Accounts ab
Übertragungs-medium	PhysicalCarrier (PCa) LogicalCarrier (LCa)	(Netzwerk, Bussystem), (Pipe, Shared Memory), Übertragungsmedien bilden Verbindung zwischen Schnittstellen
Daten	Data (D)	Hardwaredaten (DA1), Rohdateninhalte (DA2), Details über Daten (DA3), Konfigurationsdaten (DA4), Kommunikationsprotokolldaten (DA5), Prozessdaten (DA6), Sitzungsdaten (DA7), Anwenderdaten (DA8)
SW-Komponente	SW-K = Menge logischer Entitäten, Schnittstellen, Daten	
HW-Komponente	HW-K = Menge physischer Entitäten, Schnittstellen, Daten, SW-K	
Anlage	Menge von HW-K, Menschen, Daten	
Anlagenverbund	Menge von Anlagen, Daten	
Kommunikation	Austausch von Daten zwischen Komponenten, Menschen, Anlagen, Infrastrukturen	
Steuerprozess	Menge von Komponenten und Verarbeitungsvorschrift für Interaktion	
Business Prozess	Menge aller Steuerprozesse direkt beteiligt an spezifischem Output einer Anlage	

3.2 Systematisierung Analysebereiche (Analysis-Scopes)

Mit dem Ziel einer ganzheitlichen Erfassung und systematischen Abbildung aller relevanten Einzelbereiche motivieren wir die Berücksichtigung der folgenden fünf Analyse-Scopes. Die Untersuchung zerfällt in Geltungsbereiche für: (1) *Anlagenverbund*, (2) *Anlagen*, (3) *Hardware-Komponenten*, (4) *Software-Komponenten* und (5) *Kommunikationsbeziehungen*. Der Geltungsbereich für *Anlagen* folgt der vorgestellten Referenzarchitektur (Abbildung 5) und der

zugehörigen Beschreibung in Tabelle 1. Ein Vorschlag zur Abbildung von *Anlagenverbünden* kann ebenfalls Tabelle 1 entnommen werden.

Die *Komponenten*-zentrierte Betrachtung (Hard- und Software-Komponenten) erfolgt zusammengefasst als pauschalisiertes Rechnersystem und unter Berücksichtigung von drei wesentlichen Schichten. Die Hardware-Schicht besteht aus physischen Entitäten sowie physischen Schnittstellen und bildet die Grundlage der darauf aufbauenden höheren, logischen Schichten. Die Betriebssystem-Schicht unterteilt sich in Hardware-abhängige und -unabhängige Softwarebestandteile (logische Entitäten). Die obere Anwendungsschicht umfasst Benutzerprogramme und Dienste sowie betriebssystemspezifische Funktionen in Form von Systembibliotheken. Die Darstellung einer pauschalisierten Komponente und Zuordnung zu den forensischen Datenarten findet sich in Abbildung 2.

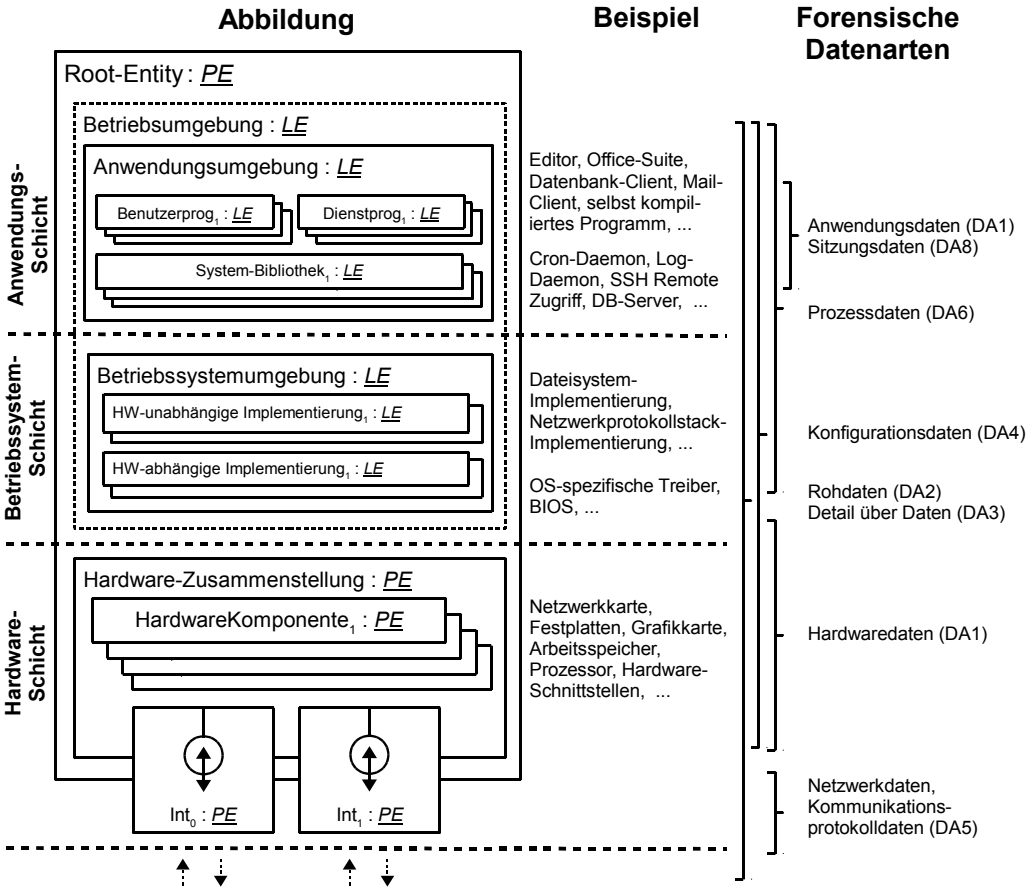


Abb. 2: Komponenten-Scope, pauschalisierte Darstellung Hard- und Softwarekomponenten

Die Betrachtung von Kommunikationsbeziehungen erfolgt als Interaktion von Entitäten (Hard- und Software) oder zwischen Entitäten und Menschen. In Abbildung 3 wird pauschalisiert die Kommunikation zwischen zwei Personen dargestellt. Für eine möglichst generische Beschreibung von Kommunikationsprotokollen wird das ISO/OSI-Schichtenmodell als einheitliche Grundlage genutzt. Zur Modellierung des Angriffskontextes (siehe Abschnitt 3.3) werden die dargestellten Schichten in vier Informationsgrade unterteilt *Full-Informed*, *Meta-Informed*, *Non-Informed*, *External* (vgl. Tabelle 2 und Abbildung 3). Die Systematisierung von Zugriffsmöglichkeiten erfolgt durch kombinierte Betrachtung von logischen und physischen Schnittstellen (uni- oder bidirektional) und Basisoperationen (lesen/schreiben), die ihrerseits wieder

zu Basisangriffen kombiniert werden. Eine Systematisierung der resultierenden Zugriffsmöglichkeiten erfolgt in Form von sogenannten Informed-Operationen (Tabelle 2), die je nach Typ (*In*, *Out*, *In-Out*) auf Schnittstellen ausgeführt werden.

Tab. 2: Systematisierung Zugriffsmöglichkeiten als Informed-Operationen für Schnittstellen

A) "External / physical Operation" (Angriffe direkt auf physikalischen Carrier bzw. Entity)	
A.1) "Physical Read"	z.B. Leitungsabstrahlung, Bildschirmabstrahlung
A.2) "Physical Write"	z.B. Überlagerung, Modulationsänderung, externe Strahlungsquellen / Felder
A.3) "Physical Interrupt"	z.B. Physisches Durchtrennen des Kabels, Zerstörung Monitor
B) "Internal / logical Operation" (Angriffe auf Daten / Übertragungsinhalte Carrier bzw. Entity)	
B.1) "Non-Informed" (Ohne Kontext / Möglichkeit zur Interpretation)	
B.1.1) "NonInformedRead"	"Lesen ohne zu Verstehen", z.B. Unkenntnis Übertragungsprotokoll / Codierung
B.1.2) "NonInformedWrite"	"Schreiben ohne zu Verstehen", z.B. Schreiben zufälliger Sequenzen
B.2) "Meta Informed" (Metadaten interpretierbar: "Wann? Wer? Wie? Wo?")	
B.2.1) "MetaInformedRead"	Metadaten les- und interpretierbar, z.B. IP-Header auslesen, ohne Zugriff Daten bspw. bei Verschlüsselung oder unbekannt Encoding
B.2.2) "MetaInformedWrite"	Metadaten schreibbar durch Vorkenntnisse, ohne Info über aktuellen Zustand des Datenstorms / Sequenz, z.B. auf „Gut Glück“ IP-Header Informationen schreiben, ohne Kenntnis von aktueller Sequenz etc.
B.3) "Full Informed" (Metadaten und Nutzdaten interpretierbar: "Was?")	
B.3.1) "FullInformedRead"	Meta- und Inhaltsdaten les- und interpretierbar, z.B. IP-Header und Paketinhalte les- und interpretierbar
B.3.2) "FullInformedWrite"	Meta- und Inhaltsdaten schreibbar, mit Kenntnis über über aktuellen Zustand Datenstorm / Sequenz, z.B. gezielt vollständige IP-Pakete schreiben

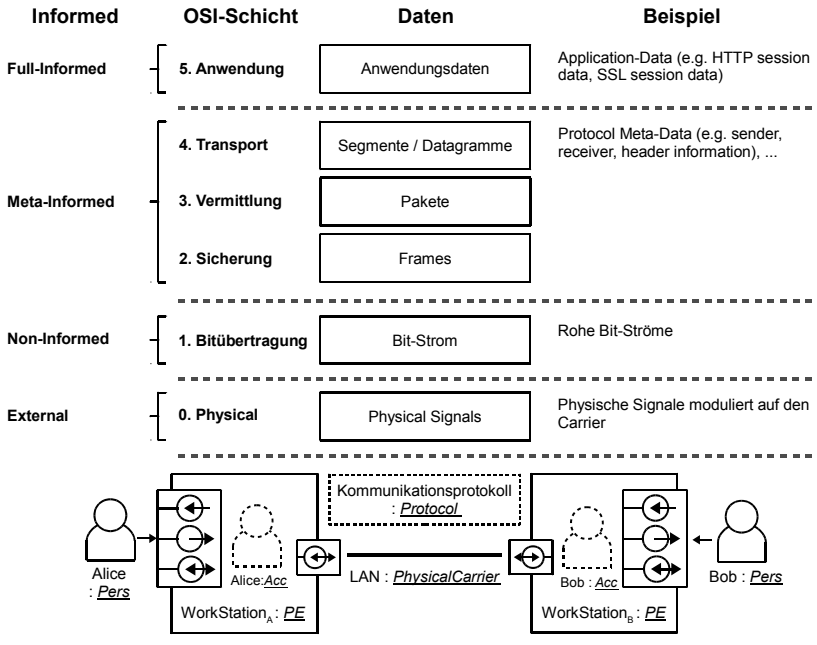


Abb. 3: Kommunikation-Scope, pauschalisierte Darstellung basierend auf OSI-Modell

3.3 Kontext-basierte Modellierung Angriffe und Angreifer

Angreiferkontext: Zur systematischen Modellierung von Angreifern schlagen wir den Angreiferkontext $C_{Angreifer}$ mit folgenden Eigenschaften vor: Berücksichtigung verfügbarer Ressourcen *R* (Zeit, Geld, Rechenzeit, Infrastruktur, Daten, Fähigkeiten, Wissen etc.), Angreifer Motivation *M* (Absicht: Aufmerksamkeit, Herausforderung, Status, Nervenkitzel, Politisch motiviert, Finanziell motiviert, Opportunismus, Patriotismus, Erpressung durch Dritte, Rache, Freude am Schaden, Sicherheitsbeurteilung, Rollen: Planer, Kodierer, Läufer, Hacker, Spione, Terroristen, Angestellte (Insider), Professionelle Kriminelle, Vandalen, Voyeur, Aktivist, Dieb, SecurityScan), verfügbaren Daten (*D*) als Form der Ressource *R* (Hardwaredaten (*DA1*), Rohdateninhalte (*DA2*), Details über Daten (*DA3*), Konfigurationsdaten (*DA4*), Kommunikationsprotokolldaten (*DA5*), Prozessdaten (*DA6*), Sitzungsdaten (*DA7*), Anwenderdaten (*DA8*)), vorhandene Wissensbasis *W* als Form der Ressource *R* (Fachwissen, Schwachstellenwissen, Angriffskontext-Wissen) und vorhandene Fähigkeiten *F* als Form der Ressource *R* (Psychologische Fähigkeiten, kommunikative Fähigkeiten, technische Fertigkeiten, etc.). Der zeitabhängige Angreiferkontext erlaubt somit verschiedene Kontextausprägungen, wie zum Beispiel Änderungen in den Ressourcen, Motivationen, verfügbaren Daten oder Wissen (inkl. Vorwissen und Wissenserwerb im Verlauf des Angriffs) seitens der Angreifer.

Angriffskontext: Um das konkrete Angriffsverhalten eines oder mehrerer Angreifer systematisch abzubilden, schlagen wir die Definition eines Angriffskontexts $C_{Angriff}$ mit folgenden Eigenschaften vor: Angreifer beschrieben durch einen konkreten Angreiferkontext $C_{Angreifer}$, Angriffsbeschreibung durch Nutzung der fünf bekannten Basisangriffe auf Angriffsziele sowie die anvisierten zu störenden Sicherheitsaspekte. Die kombinierte Anwendung von Analyse-Scopes, strukturierten Zugriffsmöglichkeiten und komponenten-basierter Modellierung ermöglicht die Abbildung von zeitabhängigen Änderungen des Angreiferkontexts. Im Verlauf eines komplexen Angriffs können bspw. temporär zusätzliche Ressourcen verfügbar werden oder wegfallen. In Abhängigkeit verfügbarer Daten, Zugriffs- und Interpretationsmöglichkeiten kann sich die ursprüngliche Wissensbasis des Angreifers im Verlauf eines Angriffs erweitern, wenn aus verfügbaren Ressourcen neues Wissen abgeleitet werden kann (Abbildung 4).

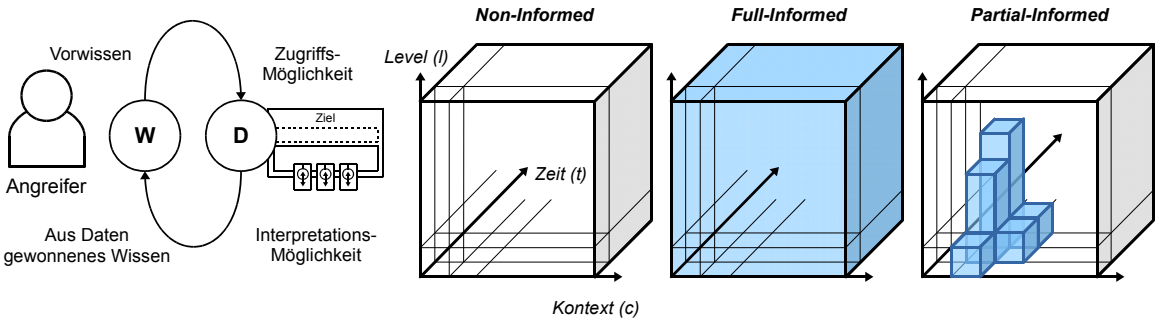


Abb. 4: Wissenserwerb (links) und Angreiferwissen (rechts) (stark vereinfachte Darstellung)

4 Exemplarische Anwendung/Angriffsszenario

Als Grundlage der exemplarischen Anwendung dient der in der Einleitung beschriebene Praxisvorfall [Icsc16]. Fehlende Angriffsaktionen bzw. unvollständige Informationen werden durch denkbares Vorgehen ergänzt. Der gesamte Angriffsverlauf wird in Tabelle 3 schrittweise beschrieben, Zielesysteme und Abfolge der einzelnen Schritte sind in Abbildung 5 dargestellt.

Die Aktionen 1 bis 3 dienen der Vorbereitung/Durchführung einer Spear-Phishing-Kampagne. Durch Auswertung öffentlich verfügbarer Informationen auf der Webseite, erwirbt der Angreifer Wissen über E-Mail Adressen und Corporate Design. Dies ermöglicht die Erstellung/Zustellung von authentisch wirkenden Phishing-Mails mit trojanischen Pferden.

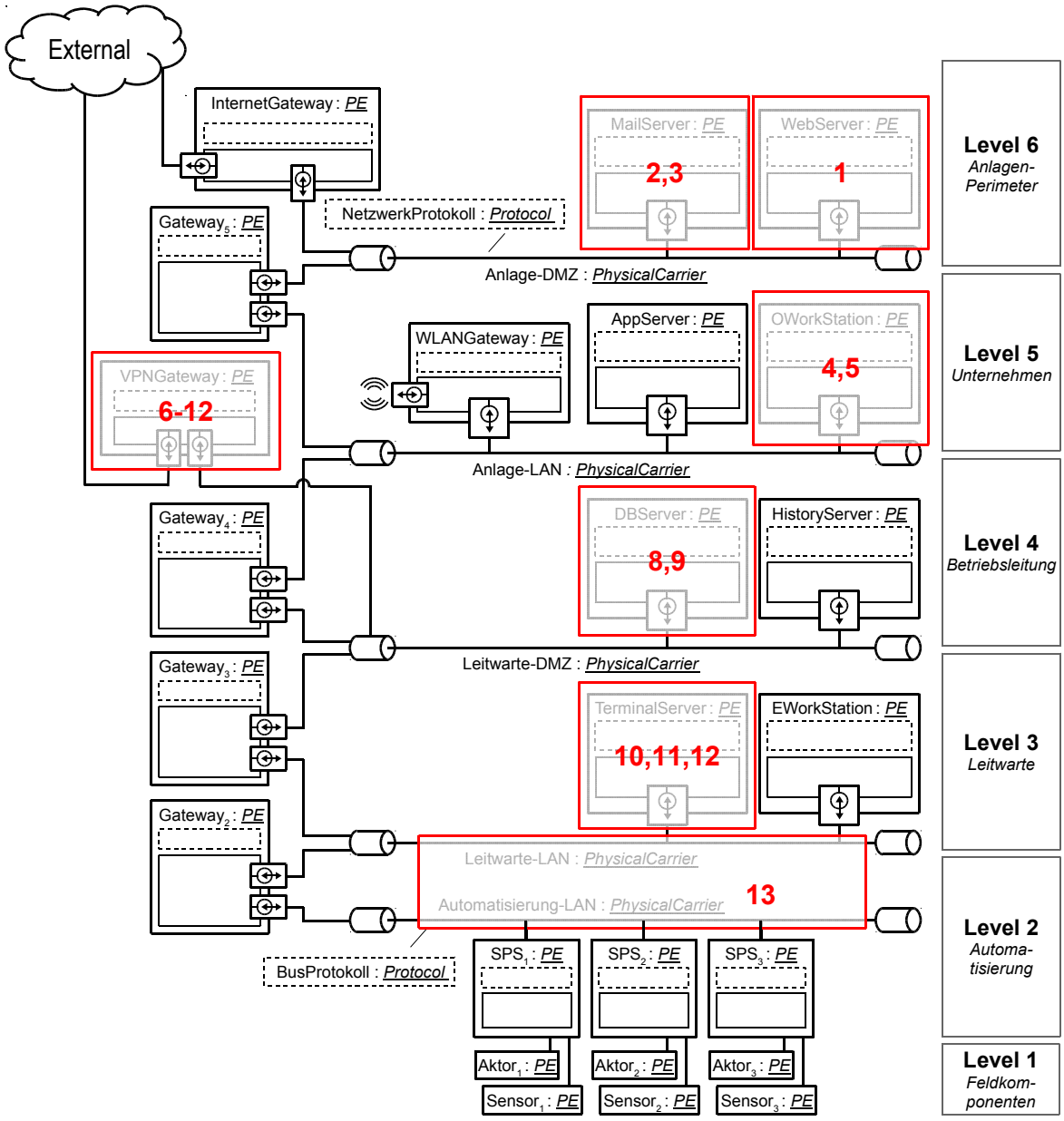
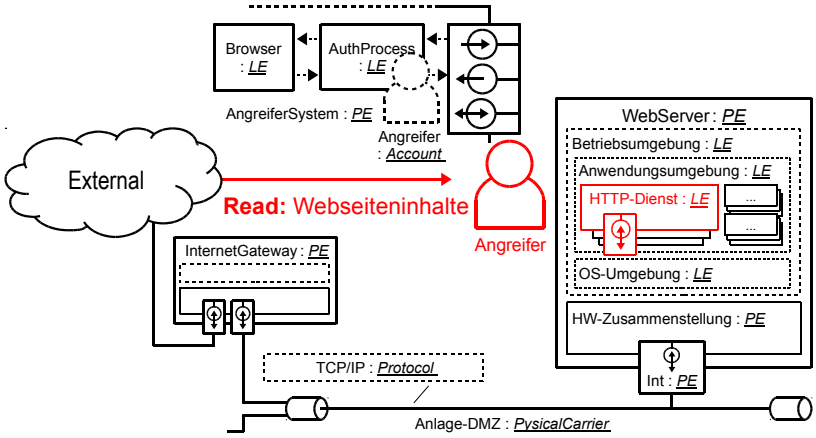


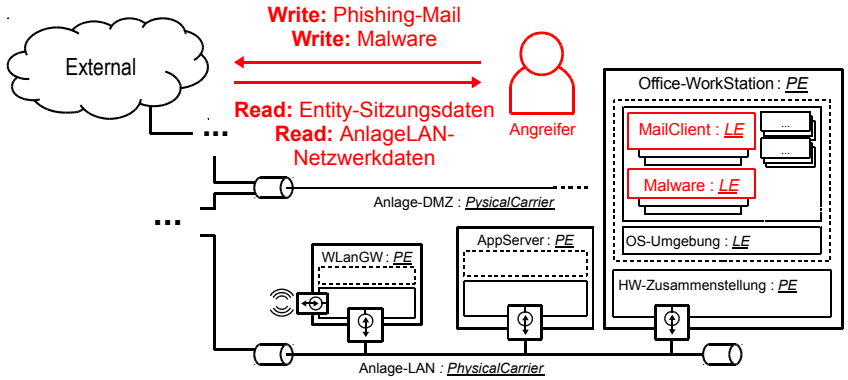
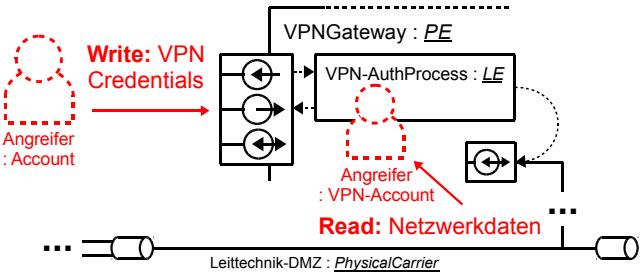
Abb. 5: Referenzarchitektur, pauschalisierte Systemlandschaft Industrie 4.0 (nach [CFDD16])

Nach Installation der Malware erfolgt in den Schritten 4 bis 6 die Beschaffung von Zugangsdaten für den VPN-Fernzugriff und eine legitime Anmeldung am VPN-Gateway unter Verwendung des ausgespähten Accounts. In 7 bis 9 verschafft sich der Angreifer einen Überblick über Level 4 der Anlage und dazugehörige Komponenten, z.B. den dort platzierten Datenbankserver. Die Zugangsdaten für den Terminalserver auf Level 3 werden aus der Datenbank ausgelesen. Mit dem Account erfolgt in 10 die Anmeldung am Terminalserver. In 11 bis 13 erfolgt die

Untersuchung des Servers und dies ermöglicht letztlich das Löschen der Konfiguration für Level 2 Zugriff. Die Verbindung zum Produktionsnetz wird unterbrochen, durch fehlende Steuerbefehle stoppen die Komponenten und damit die Produktion der Anlage.

Tab. 3: Exemplarische Anwendung der Ansätze zur Beschreibung eines komplexen Angriffsvorfalls

#	Aktion	Vorwissen	Daten	Resultat / Ziel
1	Mailadressen und Informationen zu Personen und Erscheinungsbild sammeln *(BA: Normaler Datenfluss)*	Webserveradresse	Webseiteninhalte	Mailadressen, Personennamen, Accountnamen, Positionen im Unternehmen, Corporate Design
	Angreifer : Pers → Angreifer : PE (Browser : LE) → InternetGateway : PE → WebServer : PE (Betriebsumgebung : LE (HTTPdaemon : LE (Webseiteninhalte : Daten)))			
2	Spear-Phishing-Kampagne vorbereiten	Positionen im Unternehmen, Corporate Design		Personalisierte Mails mit authentischer Formatierung Inhalt
3	Spear-Phishing-Mails senden *(BA: Erstellen)*	Mailadressen, Personennamen, Accountnamen		Übertragung Phishing-Mails Mailserver Zielunternehmen, ähnliche Absenderdomain
				
	Angreifer : Pers → Angreifer : PE (PhishingTool : LE) → MailRelay : PE (RelayDaemon : LE) → InternetGateway : PE → MailServer : PE (MailServer : LE)			
4	Infizierung von Desktop-Rechnern im Büro	Nutzer müssen Anhang öffnen und Malware umgeht Schutzmaßnahmen		Platzierte trojanische Pferde auf Systemen mit VPN-Nutzerdaten
5	Nutzer- und Netzwerkinformationen sammeln *(BA: Lesen)*	Bedienung trojanisches Pferd, verdecktes Bewegen auf Zielsystem, Speicherorte von Zieldaten	Entity-Sitzungsdaten, AnlageLAN-Netzwerkdaten	VPN-Zugangsdaten und VPN-Gateway-Adresse
6	Zugriff VPN *(BA: Täuschen)*	VPN-Zugangsdaten und VPN-Gateway-Adresse		Legitime erscheinende Verbindung zur Betriebsleitebene

				
	Angreifer : Pers → Angreifer : PE (VPNclient : LE (ClientAuthProcessVPN : LE (Mitarbeiter : Account))) → VPNGateway : PE (VPNserver : LE (ServerAuthProcessVPN : LE (Benutzerdatenbank : Daten, Mitarbeiter : Account)))			
7	Netzwerkinformationen sammeln *(BA: Lesen)*	Benutzung Sniffer, inkl. unauffällige Anwendung	VPN-Netzwerkdaten	Level 4: Netzwerktopologie, Protokolle, Adresse DBServer
8	Nutzerinformationen für Datenbankserver aus unverschlüsselten Datenstrom extrahieren *(BA: Lesen)*	Adresse des Datenbankservers, Schwachstelle der eingesetzten Datenbanklösung und Protokoll der Datenbankkommunikation	DBServer-Netzwerkdaten	Zugangsdaten Datenbankserver
9	Nutzerinformationen für Terminalserver aus Datenbank lesen *(BA: Erstellen/Täuschen, Lesen)*	Adresse des Datenbankservers, Zugangsdaten für Datenbankanmeldung	DBServer-Anwendungsdaten	Zugangsdaten Terminalserver
				
	Angreifer : Pers → Angreifer : PE (DBMSclient : LE (ClientAuthProcessDBMS : LE (Mitarbeiter : Account)), VPNclient : LE (ClientAuthProcessVPN : LE (Mitarbeiter : Account))) → VPNGateway : PE (VPNserver : LE (ServerAuthProcessVPN : LE (Benutzerdatenbank : Daten, Mitarbeiter : Account))) → DBServer : PE (DBServer : LE (ServerAuthProcessDBMS : LE (Benutzerdatenbank : Daten, Mitarbeiter : Account, TerminalServerCredentials : Daten)))			
10	Zugriff TerminalServer *(BA: Täuschen)*	Adresse Terminalserver, Zugangsdaten Terminalserver		Legitime Anmeldung an TerminalServer mit Berechtigungen Löschen der Konfiguration
11	Systeminformationen sammeln *(BA: Lesen)*	Bedienkenntnisse	Entity-Sitzungsdaten	Systeminformationen, Konfiguration, Speicherorte
12	Konfiguration löschen und TerminalServer Neustart *(BA: Erstellen)*	Speicherort Konfiguration		Unterbrechung der Verbindung zwischen Level 3 und 2
13	Unterbrechung Produktionsprozess			

5 Diskussion, Zusammenfassung und Ausblick

Für die in Abschnitt 1 formulierten Forschungsfragen wurden im Rahmen der Arbeit erste Ansätze vorgeschlagen. Der Komponenten-basierte Ansatz bietet die Möglichkeit zur anlagenunabhängigen Abbildung von Industrie 4.0 Umgebungen unter Berücksichtigung unterschiedlicher Analysebereiche. Die strukturierte Abbildung von Anlagen, Komponenten und Kommunikationsbeziehungen schafft die Grundlage zur systematischen Identifizierung von möglichen Zugriffspunkten und Schwachstellen und damit eine Basis für nachfolgende Sicherheitsanalysen bzw. zum Testen der Informationssicherheit von IT-Strukturen in Industrie 4.0 Umgebungen. Die exemplarische Anwendung deutet auf die Eignung des vorgeschlagenen Vorgehens. Gleichzeitig zeigt sich, dass der Ansatz zum derzeitigen Zeitpunkt in vielen Punkten noch zu abstrakt gestaltet ist und einer weiteren Spezifizierung bedarf. Die ersten Vorschläge zur kontext-basierten Angreifer- und Angriffsmodellierung adressieren den im Stand der Technik identifizierten Bedarf von Ansätzen zur systematischen Beschreibung von komplexen, mehrstufigen Angriffen unter Berücksichtigung von zeitabhängigen Aspekten, bspw. zusätzliche/wegfallende Ressourcen oder schrittweiser Wissensgewinn im Verlauf eines Angriffs. Basierend auf der exemplarischen Anwendung erscheint der Vorschlag zur kontext-basierten Modellierung vielversprechend. Auch hier besteht die Notwendigkeit, die bisher weitgehend abstrakten Vorschläge zu präzisieren. Dies sollte in zukünftigen Arbeiten aufgegriffen und untersucht werden, insbesondere weil bisher keine Ansätze zur Berücksichtigung von temporär verfügbaren Ressourcen oder schrittweisem Wissensgewinn identifiziert werden konnten. Allgemein zeigt sich Bedarf an flexibel anpassbaren Werkzeugen zur Unterstützung und Automatisierung des Vorgehens, insbesondere mit Blick auf eine mögliche Anbindung von existierenden Datenbanken und Katalogen. Diese Fragestellung wird als möglicher Ausgangspunkt für zukünftige Arbeiten empfohlen.

Danksagung

Diese Veröffentlichung wird durch das Bundesministerium für Wirtschaft und Energie (BMWi, SMARTEST, Projekt-Nr. 1501502A, 1501502B), im Rahmen des Deutschen Reaktor-Sicherheits-Forschungsprogramms gefördert. Die Autoren bedanken sich bei den Projektpartnern der Universität Erlangen und AREVA GmbH für die fruchtbaren Diskussionen. Weiterhin geht Dank an Ronny Merkel und das Verbundprojekt INSPECT.

Literatur

[Acat14] Acatech Germany: Recommendations for implementing the strategic initiative INDUSTRIE 4.0, Final report of the Industrie 4.0 Working Group (2014).

[BiVZ15] Bitcom, VDMA, ZVEI: Industrie 4.0 implementation strategy, (2015).

[Plat15] Plattform Industrie 4.0: Industrie 4.0 Whitepaper FuE-Themen, ZVEI (2015).

[Icsc16] ICS-CERT: IR-ALERT-H-16-056-01 Cyber-Attack Against Ukrainian Critical Infrastructure, (2016).

[MiRo12] B. Miller, D. Rowe: A survey SCADA of and critical infrastructure incidents. In: Proceedings of the 1st Annual conf. on Research in information tech, (2002) 51–56.

[NcIc16] NCICC, ICS-CERT: ICS-CERT Monitor Newsletters, (2016).

[Pric14] PricewaterhouseCoopers AG: Industry 4.0 - Opportunities and Challenges of the Industrial Internet, (2014).

[BeSc15] F. Bendik, N. Schmidt: Exchange of engineering data for communication systems based on AutomationML using an EtherNet/IPTM example. In: ODVA Industry Conference & 17th Annual Meeting, (2015).

[HSBE15] H. Holm, K. Shahzad, M. Buschle, M. Ekstedt: CySeMoL Predictive, Probabilistic Cyber Security Modeling Language. In: IEEE Transactions on Dependable and Secure Computing, vol. 12, no. 6 (2015) 626–639.

[KoTG13] P. Kotzanikolaou, M. Theoharidou, D. Gritzalis: Assessing n-order dependencies between critical infrastructures. In: International Journal of Critical Infrastructures, vol. 9, no. 1–2 (2013) 93–110.

[Agen12] Agence nationale de la sécurité des systèmes d'information (ANSSI): Managing Cybersecurity for Industrial Control Systems, (2012).

[ChHi13] Y. Cherdantseva, J. Hilton: A reference model of information assurance & security. In: 8th Int. Conf. on Availability, Reliability and Security (2013) 546–555.

[LDKH07] A. Lang, J. Dittmann, S. Kiltz, T. Hoppe: Future Perspectives – The Car and its IP-Address – A potential safety and security risk assessment. In: Computer Safety, Reliability, and Security (2007) 40–53.

[FrGr14] C. Freckmann, U. Greveler: IT-Sicherheitsaspekte industrieller Steuerungssysteme. In: Sicherheit (2014) 149–156.

[SPL+15] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, A. Hahn: Guide to Industrial Control Systems (ICS) Security, NIST SP 800-82r2 (2015).

[HoLo98] J. D. Howard, T. A. Longstaff: A common language for computer security incidents, Sandia National Laboratories (1998).

[HuCA11] E. M. Hutchins, M. J. Cloppert, R. M. Amin: Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. In: Leading Issues in Information Warfare & Security Research, vol. 1, p. 80 (2011).

[ABD+15] P. Adolphs, H. Bedenbender, D. Dirzus, M. Ehlich, et al.: Status Report - Reference Architecture Model Industrie 4.0, VDI und ZVEI (2015).

[CFDD16] R. Clausing, R. Fischer, J. Dittmann, Y. Ding: Your Industrial Facility and Its IP Address – a First Approach for Cyber-Physical Attack Modeling, erscheint in: 35th Int. Conference on Computer Safety, Reliability and Security (SAFECOMP), 2016.