Department of Computer Science

Seminar IT-Sicherheit im Wintersemester 2017/2018

IT-Sicherheit in Industrie 4.0

Eingereicht am:

22. Februar 2018

Eingereicht von:

Frauke Jörgens

minf101207@fh-wedel.de

Betreut von:

Prof. Dr. Gerd Beuster

gb@fh-wedel.de

Inhaltsverzeichnis

1 Einleitung **1**

2 Der Begriff Industrie 4.0 **2**

2.1 Definition . . . 2

2.2 Vernetzung und Cyber-Physical Systems . . . 2

3 Problematik aus Sicht der IT-Sicherheit **4**

3.1 IT-Schutzziele . . . 4

3.2 Anforderungen an die Sicherheitsarchitektur . . . 5

3.2.1 Integrität der Daten . . . 5

3.2.2 Verfügbarkeit von Informationen . . . 5

3.2.3 Schützen von Wissen und sicherer Datenaustausch . . . 6

3.2.4 Vernetzung aller an der Produktion beteiligten Komponenten . . . 6

3.2.5 Verwaltbarkeit . . . 7

3.3 Angriffsvektoren . . . 9

4 Handlungsempfehlungen **12**

4.1 Auf kurze Sicht . . . 12

4.2 Auf lange Sicht . . . 15

4.2.1 Security by Design . . . 15

4.2.2 OPC UA . . . 15

5 Zusammenfassung **19**

Literaturverzeichnis **20**

1

Einleitung

Industrielle Produktionsanlagen sind ein Kernstück der deutschen Wirtschaft und basieren auf Effizienz, Wirtschaftlichkeit und Optimierung. Durch die Digitalisierung werden neue Herangehensweisen für die Wertschöpfungsketten angestoßen. Eine Initiative, die 2013 ins Leben gerufen wurde, nennt sich Industrie 4.0 und sieht eine allgegenwärtige und allumfassende Vernetzung von allen an der Produktion beteiligten Komponenten – auch über Unternehmensgrenzen hinaus – vor [KWH13]. Diese Vision birgt viele Gefahren aus Sicht der IT-Sicherheit, die in dieser Seminararbeit thematisiert werden. Werden diese Gefahren nicht erkannt, können Angriffe auf Produktionsnetze trivial sein und häufig auftreten. Ohne ein hohes IT-Sicherheitsniveau hat die Industrie 4.0 keine Chance, sich zu etablieren, da das Vertrauen in diese Herangehensweise verletzt würde.

Diese Seminararbeit definiert zunächst den Begriff Industrie 4.0, erläutert anschließend die Problematik, die sich aus Sicht der IT-Sicherheit aufgrund der Ausgangslage von Produktionsanlagen und der Anforderungen der Industrie 4.0 ergibt und zeigt anschließend Handlungsvorschläge auf, die als wirksame Mittel eingesetzt werden können, um Industrie 4.0 sicherer zu gestalten.

2

Der Begriff Industrie 4.0

2.1 Definition

Industrie 4.0 ist eine Initiative der Branchenverbände Bitkom, VDMA und ZVEI, die sich 2013 zur Arbeitsgruppe „Plattform Industrie 4.0“ [KWH13] zusammengeschlossen haben. Unterstützt wird das Projekt vom Bundesministerium für Wirtschaft und Energie (BMWi). Ziel ist die Stärkung der Wettbewerbsfähigkeit der deutschen Wirtschaft in Zeiten der Digitalisierung. In dieser Vision sind Produktionsprozesse in der Industrie so automatisiert, dass Maschinen anhand von Algorithmen und Daten eigenständige Entscheidungen treffen können und der Mensch in nur wenigen Fällen eingreifen muss, an vielen Stellen jedoch auch eingreifen darf. Dies soll über eine großflächige und allgegenwärtige Vernetzung von Menschen, Maschinen, Sensoren, Aktoren und Controllern – mobil sowie stationär – und über Unternehmensgrenzen hinaus, ermöglicht werden.

Der Begriff Industrie 4.0 soll den Beginn einer vierten industriellen Revolution verdeutlichen. Im englischen Sprachraum wird dieser Begriff entweder direkt übernommen („Industrie 4.0“), übersetzt („Industry 4.0“) oder mit ähnlichen Begriffen, wie „Smart Factory“ oder „Industrial Internet of Things“ (IIoT) beschrieben.

2.2 Vernetzung und Cyber-Physical Systems

Informationstechnische Prozesse werden in Produktionsumgebungen als hierarchisch angesehen. So entsteht eine Automatisierungspyramide, die diese Prozesse als Stufenordnung darstellt. Auf den unteren Ebenen dieser Automatisierungspyramide befinden sich prozessnahe Komponenten auf der echtzeitkritischen Feld- und Steuerungsebene. Die Abstraktion der Prozesse nimmt Ebene um Ebene zu, sodass auf der obersten Ebene (Unternehmensleitebene) abstrakte Entscheidungen getroffen werden können. Diese abstrakte Entscheidungen werden widerrum abwärts der Automatisierungspyramide in primitive Steuerbefehle übersetzt. Diese Art der Kommunikation wird *vertikale Vernetzung* genannt, da die Abläufe in der Automatisierungspyramide vertikal und in den meisten Fällen in nur einem Unternehmen vorgehen.

Ein besonderes Merkmal der Industrie 4.0 ist, dass Unternehmen zusätzlich untereinander kommunizieren, sodass die Automatisierungspyramiden auch horizontal vernetzt werden. Auch die

direkte Kommunikation unter beliebigen Ebenen zwischen Unternehmen (*horizontale Vernetzung*) ist zentraler Bestandteil der Industrie 4.0 und sorgt dafür, dass sich der klassische hierarchische Aufbau der Automatisierungspyramide zunehmend auflöst und durch dezentrale und autonom agierende Komponenten ersetzt wird (siehe [VDI13]).

Diese neue Art von vernetzten Produktionssystemen werden *Cyber-Physical Systems* (CPS)[1] genannt. *Cyber-Physical Systems* sind die Basis für das industrielle Internet der Dinge und verknüpfen Komponenten der physischen Welt (Anlage, Maschine, Roboter, Sensoren, ...) mit virtuellen informationsverarbeitenden Systemen über das Internet oder über Cloud-Systeme. Automatisch erfasste Daten und Prognosen steuern die Produktion und Kommunikation komplett autonom (siehe Abbildung 2.1) [LBK14].

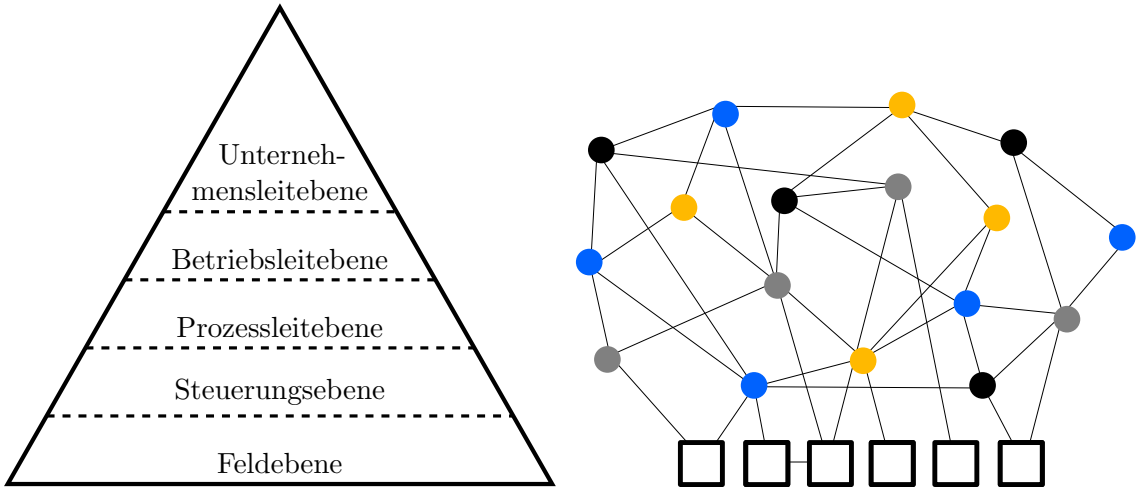

Abbildung 2.1: In Industrie 4.0 wird die klassische Automatisierungspyramide (links) zunehmends durch eine Netzstruktur (rechts) ersetzt. Grafik nach [VDI13].

Durch die vollkommen automatisierte und unternehmensübergreifende Vernetzung ergeben sich folgende Vorteile für Produktionsstätten: [Jes+17; VDI13]

- Automatische Selbstdiagnose und Fehlerdetektion: Anhand von gewonnenen Daten der verschiedenen Ebenen der Automatisierungspyramide können mithilfe von Algorithmen „smarte Entscheidungen“ getroffen werden, um Fehler präventiv und reaktiv zu bekämpfen.
- Intelligente Produktionsplanung und Automatisierung: Die Produktion von individualisierten Produkten von geringen Stückzahlen ist durch die intelligente Automatisierung möglich und wirtschaftlich sinnvoll. Die Produktion eines Produkts kann automatisch auf verschiedene Maschinen aufgeteilt werden. Des Weiteren ist es durch die weltweite Vernetzung über das Internet möglich, Arbeitsschritte der Produktion auszulagern.
- Vorhersagbarkeit der Produktion und Transparenz: Die automatisch getroffenen Entscheidungen werden protokolliert und begründet, sodass sie stets nachvollziehbar sind.
- Effizienz in der Produktion und Effektivitätssteigerung durch wenig Abfall und minimale Ressourcennutzung

[1] Im Bezug auf Produktionsumgebungen werden *Cyber-Physical Systems* auch *Cyber-Physical Production Systems* (CPPS) genannt.

3

Problematik aus Sicht der IT-Sicherheit

Ein generelles Problem ist, dass die IT-Sicherheit von Produktionssystemen schlecht oder gar nicht gewahrt wurde, da viele Anlagenbetreiber schlichtweg keine Kenntnis ihrer Sicherheitslücken hatten: Es werden auch heute noch oft *Default*-Nutzernamen und -Passwörter für z.B. VPN-Zugänge genutzt und die Zugriffskontrolle wurde oft grob vernachlässigt [Ull+16]. Dies muss sich grundlegend für Industrie 4.0 ändern. Im folgenden Abschnitt werden die IT-Sicherheits-Anforderungen an Industrie 4.0 diskutiert und mit den Anforderungen aus der Office-IT verglichen.

3.1 IT-Schutzziele

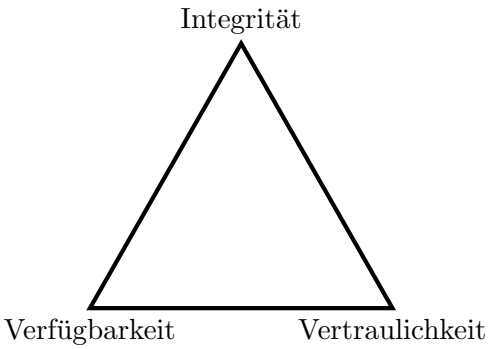

Abbildung 3.1: Drei Grundsätze der IT-Sicherheit: Integriät, Verfügbarkeit und Vertraulichkeit

Drei Grundsätze der IT-Sicherheit sind die Verfügbarkeit, die Vertraulichkeit und die Integrität von ausgetauschten Daten und Informationen. Obwohl sich in der klassischen Office-IT bereits Sicherheitslösungen und *Best Practices* für den Schutz dieser Grundsätze erfolgreich etabliert haben, können sie nicht direkt für den Anwendungsfall der Industrie 4.0 übernommen werden, da sie in der Vergangenheit andere Schwerpunkte gesetzt haben: In der klassischen Office-IT sind die Vertraulichkeit und Integrität der Daten die höchsten Güter, sodass ein Systemausfall bei einem erfolgreichem Angriff zwar unschön, aber vertretbar ist. Der Schutz der *Intellectual Property* nimmt in der Office-IT eine wichtigere Rolle ein.

In industriellen Anlagen ist die Situation eine andere: Die operative Sicherheit und Verfügbarkeit der Produktion sind unabdingbar [Dzu+05; Wai+13]. Der Fokus liegt daher auf der Integrität und Verfügbarkeit der Daten, während die Vertraulichkeit von Daten kein primäres Ziel ist. In der Vergangenheit

waren zudem industrielle Anlagen nicht miteinander vernetzt, sodass Angriffe aus dem Internet als potenzielles Risiko ausgeschlossen wurden. Somit kann ein industrielles Netz möglicherweise viele Sicherheitslücken aufweisen, da sie über Jahre hinweg nicht erkannt und behandelt wurden. Weitere Schutzziele der IT-Sicherheit sind die Authentizität – also die Echtheit, Überprüfbarkeit und Vertrauenswürdigkeit von Daten –, die Nichtabstreitbarkeit von durchgeführten Handlungen, sowie die eindeutige Zurechenbarkeit von Handlungen zu einem Kommunikationspartner.

3.2 Anforderungen an die Sicherheitsarchitektur

In *Cyber-Physical Systems* müssen insbesondere folgende Anforderungen gegeben sein:

- Integrität der Daten
- Verfügbarkeit von Informationen
- Schützen von Wissen und sicherer Datenaustausch
- Vernetzung aller an der Produktion beteiligten Komponenten
- Verwaltbarkeit

Im Folgenden werden die Anforderungen genauer beschrieben. Tabelle 3.1 vergleicht die IT-Sicherheitsanforderungen der klassischen Office-IT mit denen der Produktions-IT.

3.2.1 Integrität der Daten

Daten, die zwischen Industrie 4.0-Komponenten ausgetauscht werden, dürfen nicht unbemerkt von Dritten verändert werden können. Ist die Integrität verletzt, können beispielsweise Maschinenbefehle so manipuliert werden, dass andere als vom ursprünglichen Sender beabsichtigte Bewegungen der Maschine ausgeführt werden, ohne dass dieser Umstand bemerkt wird. Dies kann von minimalen Schäden an einem Produkt bis zur Gefährdung von Menschenleben reichen [Mag+17]. In kritischen Infrastrukturen, wie der Gas-, Atom- oder Elektroindustrie, können viele Menschen und sogar ganze Städte betroffen sein und gefährdet werden. Hier verbinden sich folglich *Security* und *Safety* (funktionale Sicherheit), sodass *Safety* nur dann gegeben ist, wenn auch eine ausreichende *Security* gegeben ist [SWW15; SN13].

3.2.2 Verfügbarkeit von Informationen

Systeme, auf denen der Datenaustausch basiert, müssen autorisierten Nutzern zu beabsichtigten Zeitpunkten verfügbar sein, insbesondere auch dann, wenn Aktualisierungen oder Wartungsarbeiten vorgenommen werden müssen oder das System durch einen *(Distributed) Denial-of-Service*-Angriff ((D)DoS-Angriff) unbenutzbar wird. Hinzu kommt, dass in solchen echtzeitkritischen Produktionssystemen nur geringe Latenzzeiten im Bereich von Millisekunden toleriert werden. Übliche kryptografisch sichere Protokolle wie TLS/SSL können bei Komponenten mit wenig Rechenleistung Verzögerungen

in der Übertragung auslösen [Ull+16; Dzu+05]. Der Ausfall einer Maschine oder Anlage, aber auch vermeidbare Verzögerungen in der Kommunikation zwischen den Komponenten, hemmen die Produktionseffizienz und können schwere wirtschaftliche Folgen haben. Übliche Vorgehensweisen aus der Office-IT, wie der Neustart des Systems für Aktualisierungs- oder Fehlerbehebungsmaßnahmen, müssen daher komplett ausgeschlossen und vermieden werden.

3.2.3 Schützen von Wissen und sicherer Datenaustausch

Daten, die zwischen Maschinen, Sensoren, Menschen und Informationsverarbeitungssystemen zwischen und innerhalb von Unternehmen ausgetauscht werden, dürfen von Dritten nicht mitgelesen werden können (Vertraulichkeit), da andernfalls die Gefahr der Industriespionage und Produktpiraterie besteht. Produktionsaufträge eines Kunden können sensible Daten beinhalten, die Rückschlüsse auf das Design eines Produktes zulassen können. Daher müssen die an diesem Prozess teilnehmenden Komponenten Mechanismen aufweisen, die eine Verschlüsselung der Daten zulassen (z.B. Public-Key-Verschlüsselung oder symmetrische Verschlüsselungsverfahren).

Unternehmen müssen externen Parteien zusätzlich vertrauen können, dass auch diese mit ihren vertraulichen Daten richtig umgehen können. Sie müssen daher a) davon ausgehen können, dass es sich bei dem vermeintlichen Kommunikationspartner auch um denjenigen handelt (Authentizität), und b), dass dieser ein vertrauenswürdiger Kommunikationspartner ist. Im Idealfall sollte nur dann eine Verbindung aufgebaut werden, wenn diese beiden Punkte gegeben sind, um einen Datenabfluss zu verhindern. Dies gilt auch insbesondere für die direkte Kommunikation zwischen zwei Maschinen (Maschine-zu-Maschine-Kommunikation). Hier bedarf es sicherer Identitäten. Es wird zurzeit geforscht, inwiefern Smart Contracts und die Blockchain-Technologie hier zum Einsatz kommen könnten [Eck17].

Der Zugriff auf Daten in der Cloud beispielsweise kann ebenfalls anhand der Identitäten erfolgen und muss feinkörnig gestaltet sein, um einen unerlaubten Zugriff zu verhindern. Auch hier besteht Handlungsbedarf, da eine Zugriffskontrolle in Produktionsumgebungen in der Vergangenheit nicht ernst genommen wurde, sodass sie nur grobkörnig oder gar nicht umgesetzt wurde [Ull+16].

3.2.4 Vernetzung aller an der Produktion beteiligten Komponenten

Anlagen und Maschinen haben naturgemäß eine hohe Lebenserwartung – oftmals von mehreren Jahrzenten –, während der sie in industriellen Produktionsstätten in Betrieb sind. Da viele Maschinen in den nächsten Jahren dementsprechend nicht ersetzt werden dürften, müssen sich auch diese zu sicheren Kommunikationspartnern über ihren ganzen Lebenszyklus hinweg etablieren lassen. Hinzu kommt, dass alte industrielle Anlagen zum Konstruktionszeitpunkt noch nicht für die Kommunikation über das Internet bestimmt waren und somit Aspekte der IT-Sicherheit für die großflächige Vernetzung komplett außer Acht gelassen wurden [Ull+16]. Viele dieser Anlagen waren

„air-gapped“[1], sodass dadurch bereits eine Reihe von möglichen Angriffsvektoren umgangen wurden. Da die großflächige Vernetzung von Maschinen, auch über das Internet, ein Kernthema der Vision Industrie 4.0 ist, besteht hier enormer Handlungsbedarf. Auch für neue Komponenten bedeutet der lange Lebenszyklus von Anlagen, dass sie für die Zukunft gewappnet sein müssen, indem die Sicherheitsmechanismen einfach wart- und austauschbar sind.

Eine weitere Folge der physischen Trennung von Industrienetzwerken ist die hohe Homogenität des Systems sowie die Entstehung von „Insellösungen“, die oftmals durch die proprietäre Software und Protokolle der Maschinenhersteller bedingt ist. Die Tatsache, dass proprietäre Protokolle für einen Außenstehenden schwer verständlich und kompliziert sind, ließ den Glauben entstehen, dass diese ohne Weiteres nicht – oder nur schwer – angreifbar sind. Dieses Konzept der „Security by Obscurity“[2] umgeht die eigentliche Anforderung einer gut geschützten Infrastruktur, anstatt ein vernünftiges Sicherheitskonzept aufzubauen. Weit verbreitete Industrieprotokolle wie Modbus und Profibus, die eine herstellerneutrale Schnittstelle zwischen Hardwarekomponenten anbieten, wurden ohne Rücksicht auf IT-Sicherheit entwickelt, da dies zu der Zeit aufgrund der Isolation von Industrienetzwerken noch kein thematisiertes Problem war. Diese Protokolle bieten zudem keine Industrie 4.0-freundliche Schnittstelle [Joh16].

Auch innerhalb einer Produktionsanlage gibt es oft eine heterogene Mischung von Schnittstellen. Damit Komponenten von verschiedenen Herstellern auf allen Ebenen der Automatisierungspyramide entsprechend der Vision von Industrie 4.0 miteinander kommunizieren können, müssen proprietäre Lösungen abgeschafft und durch einheitliche, standardisierte und sichere Kommunikationsverfahren, die von Komponenten verschiedener Hersteller interpretiert werden können, abgelöst werden.

Besonders problematisch sind die hardwarenahen Komponenten, denn sie weisen mitunter wenig Arbeitsspeicher und Rechenkapazität auf, da sie minimal für ihre spezifische Aufgabe designt wurden. Sie unterstützen in den meisten Fällen keine Sicherheitsmechanismen wie Authentisierung, Zugriffskontrolle oder die Isolierung des Arbeitsspeichers für verschiedene Prozesse [Dzu+05] aufgrund der reduzierten Rechenkapazität.

3.2.5 Verwaltbarkeit

Durch die extrem hohe Vernetzung entsteht zwangsläufig eine hohe Zahl an Kommunikationsteilnehmern und Identitäten mit verschiedenen Rechten. Diese Teilnehmerzahl muss übersichtlich und verwaltbar gehalten sein, damit das System sicher bleibt.

[1] Zu deutsch: „Getrennt durch Luft“, im übertragenen Sinne: Physisch von anderen Netzwerken isoliert.
[2] Zu deutsch: „Sicherheit durch Unklarheit“.

Kategorie	Klassische Unternehmens-IT	Produktions-IT
Performance	• keine garantierten Abarbeitungszeiten • hohe Latenz akzeptabel	• garantierte Abarbeitungszeiten • Latenz ist zum Teil hart begrenzt
Verfügbarkeit	• Rebooten nicht ungewöhnlich • Kurzfristige Wartungsvorgänge (z.B. Patch) • geringe Kosten für Wartungsausfälle	• Rebooten im produktiven Umfeld nicht akzeptabel • Wartungszyklen nur mit langem Vorlauf • Wartungsausfälle verursachen hohe Kosten
Beurteilung von Risiken	• Vertraulichkeit und Integrität von Daten stehen im Vordergrund • bei Nichtbeachtung: Nachhaltige Störung von Geschäftsprozessen	• Schutz von Mensch und Umwelt stehen im Vordergrund • Bei Nichtbeachtung: Gefahr für Mensch und Umwelt; Zerstörung von Produktionskapazitäten
Lebenszeit der Komponenten	• wenige Jahre	• bis zu 25 Jahre

Tabelle 3.1: Vergleich der IT-Sicherheitsanforderungen in Office-IT und Produktions-IT [BSI13].

3.3 Angriffsvektoren

Durch die geplante weltweite Vernetzung von Maschinen und Anlagen, die womöglich in sich selbst nicht sicher sind, entsteht eine enorme Angriffsfläche für Angreifer. Bei einem erfolgreichen Angriff auf ein System müssen Folgeangriffe auf weitere, vernetzte Systeme unbedingt verhindert werden, um die Ausbreitungsgeschwindigkeit und das Ausmaß des Angriffs so klein wie möglich zu halten. Denn durch die allumfassende Vernetzung von Komponenten steigt der Risikofaktor eines Angriffs: Ist nur eine Komponente hinreichend unsicher, besteht eine Infektionsgefahr für alle vernetzten Komponenten.

Das BSI [BSI16a] identifiziert regelmäßig die Top 10 Bedrohungen für ICS (Industrial Control Systems, Industrielle Kontrollsysteme) mitsamt ihrer Folgen und Gegenmaßnahmen. Die Auflistung erfolgt anhand der Kritikalität einer Bedrohung, die sich aus Verbreitungspotenzial, Lokalisierbarkeit und Ausnutzbarkeit der Schwachstelle, sowie Detektion der Kompromittierung ergibt. Dabei werden ausschließlich Primärangriffe (Infektionsvektoren) benannt, aus denen Folgeangriffe abgeleitet werden können. Jene werden von Angreifern zur Rechteerweiterung, Außerkraftsetzung von Sicherheitsmechanismen und Ausbreitung im System genutzt. Die Auflistung der Top 10 Bedrohungen für ICS-Security des Jahres 2016 ist in Tabelle 3.2 wiedergegeben.

Nr.	Bedrohung	Kategorie
1	Social Engineering und Phishing	Menschliches Fehlverhalten
2	Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware	Ausnutzung von vorhandenen Schwachstellen (tendenziell interner Täter)
3	Infektion mit Schadsoftware über Internet und Intranet	Ausnutzung von vorhandenen Schwachstellen (tendenziell Täter von außerhalb)
4	Einbruch über Fernwartungszugänge	Schlechte Praxis
5	Menschliches Fehlverhalten und Sabotage	Menschliches Fehlverhalten
6	Internet-verbundene Steuerungskomponenten	Schlechte Praxis
7	Technisches Fehlverhalten und höhere Gewalt	Technisches Fehlverhalten
8	Kompromittierung von Extranet und Cloud-Komponenten	Ausnutzung von vorhandenen Schwachstellen
9	(D)DoS-Angriffe	–
10	Kompromittierung von Smartphones im Produktionsumfeld	Ausnutzung von vorhandenen Schwachstellen, Schlechte Praxis

Tabelle 3.2: Top 10 Bedrohungen für Industrial Control System Security [BSI16a] und abgeleitete Kategorien.

Aus den Bedrohungen wurden Kategorien abgeleitet, die im Folgenden genauer aufgeführt sind:

Menschliches Fehlverhalten In diese Kategorie fallen die Bedrohungen Social Engineering und Phishing sowie menschliches Fehlverhalten und Sabotage. Aus technischer Sicht ist es hier wichtig,

die Identitäten mitsamt ihrer Berechtigungen mit Bedacht zu wählen, sodass nur die für die Person relevanten Aktionen zulässig sind, um das Fehler- oder Missbrauchspotenzial so klein wie möglich zu halten. So sollten beispielsweise Benutzerkonten, die von mehreren Nutzern benutzt werden können, unbedingt vermieden werden. Darüber hinaus sollten Mitarbeiter regelmäßig über IT-Sicherheitsrisiken geschult werden.

Ausnutzung von vorhandenen Schwachstellen Durch vorhandene Sicherheitslücken können Systeme über das Internet oder über externe Medien wie Wechseldatenträger infiziert werden. Durch die Vernetzung von Produktions-IT und Office-IT besteht die Möglichkeit, dass Produktionskomponenten von Schwachstellen im Bereich der Office-IT betroffen sind. Eine vernünftige Segmentierung in Subnetze ähnlicher Schutzbedarfe ist daher notwendig, um die Ausbreitung von Infektionen einzudämmen.

Bereits heute werden mobile Endgeräte wie Smartphones genutzt, um Parameter in Produktionsumgebungen anzeigen, oder verändern zu können. Auch diese Geräte müssen als potenziell unsichere Kommunikationsteilnehmer betrachtet werden. Andernfalls können sie beispielsweise ein Einfallstor für das Einschleusen von Malware sein.

Eine weitere Bedrohung dieser Kategorie ist die Kompromittierung von Extranet und Cloud-Komponenten. In der Industrie 4.0 werden für die Optimierung der Geschäftsprozesse Daten großzügig verarbeitet and analysiert (Stichwort „Big Data“). Diese Verarbeitung kann aufgrund der Datenmenge sehr rechenaufwendig sein, weshalb solche Prozesse mitunter in die Cloud ausgelagert werden. Auch rechenintensive Aufgaben, die zur Steuerung von Maschinen benötigt werden, können durch die Bereitstellung von Rechenleistung von der Cloud übernommen werden (*Automation as a Service*). Die Datensicherheit der ausgelagerten Komponenten und Daten liegt damit nicht mehr in den Händen des Anlagenbetreibers, sondern in denen des Cloud-Anbieters, sodass eine gewisse Vertrauensbeziehung bestehen muss. Treten bei diesen ausgelagerten Komponenten Sicherheitsrisiken auf, sind also auch die Mandantendaten gefährdet. Auch Angriffe auf ein Cloud-System können sich auf verbundene Systeme ausbreiten. Hier muss sichergestellt werden, dass die Cloud-Anbieter vertrauenswürdig sind.

Schlechte Praxis Besonders in Produktionsumgebungen hat sich ein vernünftiges Sicherheitsniveau noch nicht etablieren können, weshalb in der Praxis viele vermeidbare Sicherheitslücken existieren. Zur Fernwartung werden oftmals Tunneling-Verfahren wie VPN verwendet, welche nach einer Authentisierung mit Benutzername und Passwort einen verschlüsselten Kommunikationskanal herstellen. Leider werden in der Praxis oft Standard-Nutzernamen und -Passwörter genutzt, was einen Fremdeingriff ungemein einfach machen kann.

Viele ICS-Komponenten sind darüber hinaus direkt mit dem Internet verbunden (d.h. sie haben keine private, sondern eine global eindeutige IP-Adresse). Mit Suchmaschinen und Datenbanken wie

der Google Hacking Database und Shodan können die zugehörigen IP-Adressen dieser Komponenten herausgefunden werden. Über weitere Sicherheitslücken können anschließend andere Angriffe folgen, um größeren Schaden anzurichten. In einer Studie von TrendMicro ([Mag+17]) gelang es Sicherheitsexperten, über dieses Einfallstor direkt aus dem Internet auf industrielle Roboter zuzugreifen.

Technisches Fehlverhalten Leider sind Software-Fehler, die zu unvorhergesehenem Fehlverhalten führen können, sowie Hardwaredefekte und Stromausfälle, nicht auszuschließen. Um Software-Fehler weitestgehend zu vermeiden, sollten standardisierte und für sicher befundene Schnittstellen, Protokolle und Bibliotheken bei der eigenen Softwareentwicklung genutzt werden.

(D)DoS-Angriffe Wenngleich (D)DoS-Angriffe schon in der Office-IT eine echte Gefahr sind, ist das Gefahrenpotenzial für Industrie 4.0 noch größer, da solche Angriffe den Betrieb und somit die komplette Produktion zum Stillstand bringen können. Vor allem (D)DoS-Angriffe auf Industrieanlagen wie Industroyer (2015) haben in den vergangenen Jahren für Aufsehen gesorgt.

4

Handlungsempfehlungen

Grundkonzepte der IT-Sicherheit wie Verschlüsselung, Firewalls und Segmentierung der Netze haben sich bereits in der Office-IT etabliert und können konzeptionell auch für die Komponenten der Industrie 4.0 genutzt werden. Wie in Abschnitt 3.2 bereits angesprochen, gibt es zusätzliche Anforderungen an etablierte Sicherheitslösungen (z.B. die Echtzeitfähigkeit), sodass diese nicht direkt umgesetzt werden können. Die Industrie sieht sich zudem mit dem Problem des Retrofitting – der Anpassung alter Komponenten an aktuelle Architekturen – konfrontiert. Um Sicherheit zu ermöglichen, wird daher empfohlen, zunächst kurz- und mittelfristige[1] Sicherheitslösungen zu implementieren, um in der Übergangsphase Langzeitlösungen bereitstellen zu können.

4.1 Auf kurze Sicht

Das Bundesamt für Wirtschaft und Energie [BMW16b] und die Plattform Industrie 4.0 [BMW16a] haben Handlungsempfehlungen und *Best Practices* für industrielle Produktionsanlagen veröffentlicht, um Industrie 4.0 sicherer zu gestalten. In der folgenden Aufzählung werden die wichtigsten und übereinstimmenden Punkte wiedergegeben:

Netzsegmentierung Wie auch in der klassischen Office-IT sollte die Unterteilung in Subnetze erfolgen, da so in einem Angriffsfall die Ausbreitung an den Zonenübergängen (Firewalls) gehemmt werden kann. Insbesondere sollte das Office-IT-Netz von dem Produktionsnetz logisch getrennt sein, da andernfalls beide Teilnetze durch Schwachstellen des jeweils anderen Teilnetzes gefährdet sind. Durch die Unterteilung in Subnetze ist es möglich, Störfalle in einem Subnetz zu isolieren, sodass sie in anderen Subnetzen keinen Schaden anrichten können. Komponenten mit ähnlichem Schutzbedarf können in einer Zone zusammengefasst werden. An den Zonenübergängen können Firewalls oder Datendioden benutzt werden, um eine Filterung bzw. Kommunikation in nur eine Richtung zuzulassen.

Im Hinblick auf die allgegenwärtige Vernetzung ist es auch von großer Wichtigkeit, diese Zonierung auch für Funktechnologien (Wireless Communication) umzusetzen. Sie sollten beispielsweise durch Abschirmung des Signals so konfiguriert sein, dass das Signal jeweils nur in einer Zone gültig ist und der Sender klar einer Zone zugeordnet werden kann.

[1] In einem Zeitraum von 1–2 Jahren umsetzbar. [BMW16b]

Starke Authentisierung, feingranulare Zugriffskontrolle und sichere Identitäten Für die sichere Kommunikation ist es unerlässlich, dass beide Kommunikationspartner korrekt identifiziert und authentisiert werden, da andernfalls die Integrität der Daten verletzt ist (siehe Abschnitt 3.2). Das Vortäuschen einer Identität wie bei einem *Man-in-the-Middle*-Angriff darf schlichtweg nicht möglich sein. Durch eine feingranulare Zugriffskontrolle werden die Berechtigungen von Nutzer (Menschen, aber auch Maschinen) in einen Rahmen gefasst, in dem nur die für ihn relevanten Aktionen erlaubt sind. Hier lässt sich die Zugriffspolitik der *Attribute-Based Access Control (ABAC)* oder der *Context-Based Acces Control (CBAC)* gut einsetzen, wobei weiterhin beachtet werden muss, dass die Anzahl der Regeln überschaubar bleibt. Eine Feingranulare Zugriffskontrolle kann zusätzlich die Schwere eines Angriffs hemmen, da die Handlungsmöglichkeiten eines Angreifers eingeschränkt werden.

Auch innerhalb eines Unternehmens kann es potenzielle Angreifer geben, die möglicherweise ihre Berechtigungen missbrauchen, um Schaden zu stiften. Durch Logging-Verfahren können Authentifizierungen aufgezeichnet werden und Anomalien im Anmeldeverfahren erkannt werden (z.B. wenn ein Nutzer versucht, sich innerhalb kurzer Zeit als ein anderer Nutzer zu authentisieren). Zur zentralen Verwaltung von zugriffgeschützten Logs werden Standardformate wie Syslog, LEEF und CEF vorgeschlagen. Privilegierte Nutzer wie Instandhalter von Maschinen und Systemen benötigen oft breite Zugriffsrechte, um Anpassungen vornehmen zu können. Hier besteht folglich wiederum die Gefahr des Berechtigungsmissbrauchs, die Aufgrund der gegebenen Privilegien umso gravierender sein kann. Um diesem Problem zumindest leicht entgegenzuwirken, wird die Nutzung einer *Privileged Identity Management*-Lösung empfohlen.

Es wird vorgeschlagen, kein rein wissensbasiertes System (z.B. Benutzername & Passwort), sondern ein Mehrfaktorverfahren für die Authentisierung eines Nutzers zu verwenden. Besonders im Produktionsbereich findet sich die sicherheitskritische Praxis, dass die gleichen Standardpasswörter zur Authentisierung (z.B. bei der Tunnelung über VPN) auch über verschiedene Systeme hinweg genutzt werden. Für Mehrfaktorverfahren eignet sich zusätzlich die Authentisierung mit Tokens, also Gegenständen, die mit RFID- oder NFC-Technik ausgestattet sind, und die somit Identität sowie Zugriffsrechte eines Nutzers speichern. Im Sinne der Authentisierung in der Maschine-zu-Maschine-Kommunikation wird das in mobilen Anwendungen bereits häufig verwendete OAuth 2.0-Verfahren, welches den Zugriff auf fremde Ressourcen regelt, empfohlen.

Verschlüsselter Datenaustausch Um dem IT-Sicherheits-Grundsatz der Vertraulichkeit nachzugehen, müssen die Daten verschlüsselt übertragen werden. Für langzeitige Fernzugriffe wird der Einsatz von kryptografisch abgesicherten VPN-Tunneln (IPSec oder SSL VPN) oder die Kapselung mit OPC UA (siehe Unterabschnitt 4.2.2) empfohlen. In prozessnahen Komponenten wie Maschinen kann aufgrund der hohen Echtzeitanforderung nicht immer eine Verschlüsselung gewährleistet werden. Hier wird wieder eine Kapselung über einen sicheren Kommunikationskanal, z.B. OPC UA nahe gelegt. Als Verschlüsselungsverfahren sollen ausschließlich standardisierte und für sicher befundene Verfahren benutzt werden, die in etablierten Crypto-Libraries überlicherweise bereits

implementiert und so einfach zugreifbar sind. Aufgrund der langen Einsatzdauer von Maschinen im Betrieb sollte darauf geachtet werden, dass die genutzten kryptografischen Verfahren gegen modernere austauschbar sind.

Für die Verwaltung der Schlüssel muss die Public-Key-Infrastruktur (PKI) der Office-IT um die Identitäten der neu hinzukommenden Komponenten (Maschinen, Mikrocontroller, usw.) ergänzt werden. Für die leichte Verwaltung der Zertifikate wird empfohlen, ein Certificate Lifecycle Management (CLM) Tool zu verwenden. Damit sich auch Kommunikationsteilnehmer wie eingebette Systeme, die aufgrund von begrenztem Arbeitsspeicher nicht für die Nutzung von Zertifikaten geeignet sind, authentifizieren können, wird die Nutzung eines Validierungsdiensts, dem Online Certificate Status Protocol (OCSP) empfohlen, obwohl auch bei diesem bereits Sicherheitsprobleme gefunden wurden. Dennoch kann es aufgrund der erheblichen Menge von Kommunikationsteilnehmern, wie es bei der Industrie 4.0 der Fall ist, sehr umständlich werden, die zugehörigen Schlüssel, Identitäten und Zertifikate des gesamten Unternehmens übersichtlich zu verwalten. Hier bedarf es weiterhin einer skalierbaren Verwaltungslösung.

Monitoring der Netzkommunikation Um auffälliges Verhalten innerhalb eines Subnetzes identifizieren zu können, muss die Kommunikation überwacht werden. Die zur Netzwerksegmentierung genutzten Zonenübergänge sind als Einsatzort für Intrusion Detection Systeme (IDS) und Intrusion Prevention Systeme (IPS) gut geeignet, um dort Anomalien zu erkennen und die Ausbreitung möglicher Schadsoftware zu unterbinden. Die bereits erwähnten Logs können durch Security Information and Event Management (SIEM)-Lösungen, welche die zentrale Überwachung und Verwaltung von Auffälligkeiten und Störfällen erlauben, kontrolliert werden. Das Monitoring kann jedoch möglicherweise nur für nicht-echtzeitkritische Komponenten genutzt werden, da durch die Netzwerküberwachung Latenzen entstehen können.

Softwaresicherheit Hier greifen im Grunde die selben Prinzipien wie im Office-IT-Bereich. Gemeint sind vor allem die Prüfung der Daten, die Wahl einer sicheren Programmiersprache, die Nutzung gängiger Kryptografie-Bibliotheken, und die digitale Signierung herausgegebener Updates. Die genutzte Software sollte stets auf dem neuesten Stand sein, damit entstandene Sicherheitslücken geschlossen und IDS/IPS über neue Angriffsarten informiert werden. Auch beim Einkauf von Maschinen und Anlagen sollte darauf geachtet werden, dass diese ein aktuelles Sicherheitsniveau erfüllen können, sodass die besprochenen Handlungsvorschläge umgesetzt und die Anlage gut in die Sicherheitsarchitektur der Produktion integriert werden können.

4.2 Auf lange Sicht

4.2.1 Security by Design

Viele der Probleme, die nun zu bewältigen sind, rühren daher, dass industrielle Kontrollanlagen und ihre Komponenten nur für die betriebsinterne Benutzung vorgesehen waren und Sicherheitsaspekte – *Safety* ausgenommen – in den meisten Fällen gar nicht beachtet wurden. Oft werden zuerst die funktionalen Anforderungen an Software implementiert und erst anschließend eine Sicherheitsbetrachtung durchgeführt. Da hier die IT-Sicherheit erst im zweiten Schritt betrachtet wurde, muss das Design der Komponente häufig neu durchdacht werden, um den Sicherheitsanforderungen gerecht zu werden. Neben dem höheren Arbeits- und Kostenaufwand schafft diese Herangehensweise einen längeren Zeitraum, in dem das System angreifbar sein kann, da das Aussetzen der Komponente keine wirkliche Alternative ist und den hohen Verfügbarkeitsanforderungen widerspricht [WK16]. IT-Sicherheit sollte stattdessen bereits beim Entwurf in die Architektur jeder Komponente bereits beim Entwurf eingebettet werden. Das Konzept der *Security by Design* sollte nicht nur im Sinne der Industrie 4.0 genutzt werden, sondern in der Soft- und Hardware-Entwicklung insgesamt.

4.2.2 OPC UA

OPC UA (Open Platform Communications - Unified Architecture)[2] ist ein plattformunabhängiges, offenes und freies Protokoll, das eine verschlüsselte vertikale (innerhalb der Automatisierungspyramide eines Unternehmens) sowie horizontale Kommunikation (über Unternehmen hinweg) zwischen verschiedenen Produktionskomponenten erlaubt. Dazu wird zurzeit eine Service-orientierte Architektur (SOA) genutzt, welche auf dem *Client-Server*-Prinzip beruht: *Clients* können Anfragen (*requests*) an den *Server* senden und erhalten nach Bearbeitung eine Antwort (*response*). Eine Besonderheit des Protokolls ist, dass IT-Security direkt in das Design eingeflossen und ein Kernthema der Spezifikation ist. Folgende etablierte Sicherheitsmechanismen umfasst OPC UA [Bur13]:

- Verschlüsselung von Sessions: Verbindungen von *Client* zu *Server* werden mit gängigen Verschlüsselungsverfahren wie RSA und AES verschlüsselt. Die Verschlüsselungsverfahren sind auch austauschbar, sodass neue und bessere Verschlüsselungsverfahren leicht integrierbar sind. Digitale Signaturen mit RSA und SHA werden ebenfalls unterstützt.
- Authentisierung von Anwendungen und Nutzern: Jeder OPC UA-*Client* und -*Server* sowie jeder Nutzer ist mit Zertifikaten ausgestattet, die deren Identität bestätigen. Dadurch wird ebenfalls die Autorisierung geregelt.
- Prüffähigkeit: Jegliche Aktivitäten von Nutzern und Kommunikation werden aufgezeichnet (*Logging*), sodass sie ständig evaluiert werden können.

[2] siehe `http://opcfoundation.org`

- Firewall-freundlich: Dadurch, dass OPC UA nur einen Port verwendet (TCP Port 4840), ist es ein Leichtes, entsprechende Firewall-Regeln zu erstellen und zu verwalten.

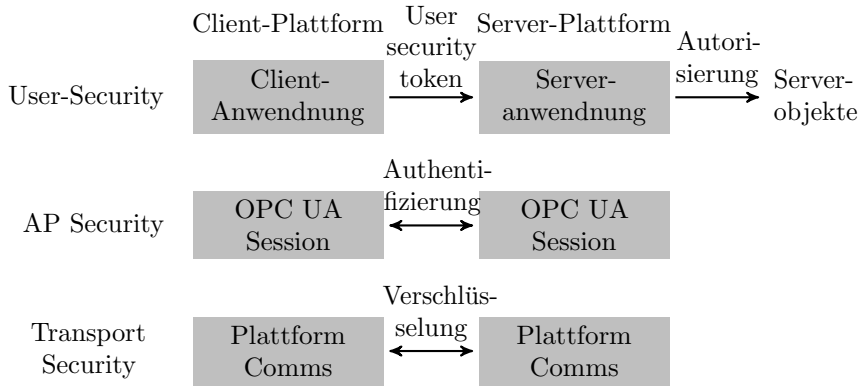

Abbildung 4.1: Das grundlegende Sicherheitsmodell von OPC UA. Grafik nach [Bur13].

Basis für die Verwaltung von kryptografischen Schlüsseln und die Authentisierung über Zertifikate ist der etablierte *X.509*-Standard. Zusätzlich enthält jedes Zertifikat einen privaten Schlüssel, mit dem eine verschlüsselte Verbindung aufgebaut werden kann, wenn die Identifikation beider Kommunikationspartner bestätigt und für gültig erklärt wurde. Abbildung 4.1 beschreibt das Sicherheitsmodell von OPC UA auf drei Ebenen der *User Security, Application (AP) Security* und der *Plattform Communications*.

Auf der Ebene der *User-Security* identifiziert sich ein User einmalig bei einem Sitzungsaufbau mit einem *Security-Token* bei einer Server-Anwendung. Die Server-Plattform kann den Nutzer anhand des *Security-Tokens* identifizieren und beispielsweise für den Zugriff auf Server-Objekte autorisieren. Die Ebene der *Application Layer (AP) Security* wird ebenfalls beim Sitzungsaufbau zum Austausch digital signierter Software-Zertifikate durchlaufen. Diese Zertifikate identifizieren die genutzte Software auf *Client*- sowie *Server*-Seite und gleichen deren OPC UA-Profile ab. Für die Verschlüsselung von Nachrichten kann die Ebene der *Transport-Security* genutzt werden.

Darüber hinaus ist OPC UA plattformunabhängig (sowohl in Hard-, als auch in Software) und kann somit sowohl auf der Feldebene als auch Cloud-basiert und über verschiedene Hersteller und Unternehmen hinweg eingesetzt werden. Somit bringt OPC UA automatisch die Voraussetzung für die vertikale und horizontale Vernetzung mit. Durch die vielschichtige Architektur wird Skalierbarkeit erreicht, sodass OPC UA auch für die Zukunft relevant bleibt. OPC UA kann in C/C++, .NET und Java implementiert werden.

In einer Studie des Bundesamtes für Sicherheit in der Informationstechnik (BSI) [BSI16b] wurde eine Sicherheitsanalyse von OPC UA durchgeführt. Dabei konnten bei der Spezifikationsanalyse keine systematischen Schwachstellen gefunden werden; lediglich in der Referenzimplementierung wurden einige Probleme festgestellt. Die generell positiv ausgefallene Bilanz jedoch spricht für einen Einsatz von OPC UA innerhalb von Industrie 4.0-Umgebungen, zumal die Alternativen sich als deutlich unsicherer herausgestellt haben.

Industrie 4.0-Anforderung	OPC-UA-Lösung
Sicherer Datenaustausch (Vertraulichkeit, Integrität, Authentizität, Nichtabstreitbarkeit & Zurechenbarkeit)	Gegeben durch Zertifikate (Authentifizierung, Zurechenbarkeit), welche die signierte und verschlüsselte Datenübertragung erlauben (Integrität, Nichtabstreitbarkeit, Vertraulichkeit). Für die Verschlüsselung und die Signierung von Nachrichten werden standardisierte und etablierte Verschlüsselungsverfahren genutzt (TLS/SSL mit RSA).
Verfügbarkeit von Informationen	Gegeben im Sinne der Authentisierung, sowie durch Redundanzfunktionen, Timeouts und automatischer Fehlererkennung bei Übertragungen zum Erreichen von hoher Verfügbarkeit. Allerdings wurde auf die Echtzeitanforderungen keine besondere Rücksicht gelegt.
Vernetzung aller an der Produktion beteiligten Komponenten	Gegeben durch die Betriebssystem- und Herstellerunabhängigkeit sowie herstellerneutrale Schnittstellen. Darüber hinaus gibt es OPC UA Embedded, was die Funktionalität von OPC UA auf Chipebene und ohne Betriebssystem realisiert. Durch das skalierbare Sicherheitskonzept wird auch der lange Lebenszyklus von Maschinen beachtet.
Verwaltbarkeit	Die Verwaltbarkeit liegt in der gewählten Struktur des Anlagenbetreibers und wird aufgrund der hohen Menge von Kommunikationsteilnehmern weiterhin ein Problem sein.

Tabelle 4.1: Vergleich von Industrie 4.0-Anforderungen und Lösungsmöglichkeiten durch OPC UA.

In Tabelle 4.1 werden Anforderungen der Industrie 4.0 mit den Möglichkeiten von OPC UA gegenübergestellt. Sie zeigt, dass OPC UA bereits viele Anforderungen erfüllen kann (vgl. Abschnitt 3.2 und [Bur13]).

Wie die Tabelle auch aufzeigt, gibt es eine Anforderung, die OPC UA zur Zeit noch nicht bedienen kann: Die Echtzeitfähigkeit auf der Feldebene. In einer aktuellen Studie [PBS16] wurde geprüft, inwiefern der TSN[3]-Standard innerhalb von OPC UA zum Einsatz kommen kann. Für die erfolgreiche Umsetzung muss zumindest auf der echtzeitkritischen Ebene das *Client-Server*-Modell durch ein *Publish-Subscribe*-Modell ersetzt werden. In letzterem gibt es statt *Client* und *Server* *Subscriber*, die ein Thema (*Topic*) abonnieren und bei neuen Ereignissen über dieses Thema informiert werden, und *Publisher*, die zu definierten Themen neue Nachrichten via Broadcast an die *Subscriber* verschicken. Dieses Modell wird auch in vielen *IoT*-Anwendungen verwendet und zeichnet sich durch einen leichtgewichtigen und schnellen Datenaustausch aus, der in vielen Fällen echtzeitfähig ist.

[3]Time-Sensitive Networking, ein Standard der IEEE 802 Ethernet-Spezifizierung.

Die Ergebnisse, die bisher mit OPC UA TSN erzielt wurden, sind vielversprechend: In einem *Proof-of-Concept* ([PBS16]) konnten Latenzzeiten von wenigen Millisekunden erreicht werden, was, je nach Anwendung, die Echtzeitfähigkeit bestätigt. Die OPC-Foundation plant, TSN zukünftig in die Architektur von OPC UA zu integrieren. Harte Echtzeitanforderungen kann OPC UA TSN bisher nicht bedienen. Um diesen trotzdem gerecht werden zu können, müssen in den betroffenen Bereichen weiterhin Feldbusse benutzt werden.

5

Zusammenfassung

Gesamt betrachtet fällt auf, dass die Office-IT und die Produktions-IT viele Gemeinsamkeiten haben und somit Sicherheitsprobleme der Produktions-IT in vielen Fällen wie in der Office-IT behandelt werden können. Dennoch haben sie auch viele Unterschiede, die eine neue Problematik ergeben. Die Designfehler und Sicherheitslücken, die aus einer Zeit stammen, in der die Vernetzung von Produktionsanlagen nicht in Betracht gezogen wurde, müssen zunächst direkt beseitigt werden.

Da die IT-Sicherheit von Produktionsanlagen der der Office-IT stark hinterher hinkt, besteht hier großer Aufholbedarf. Office- und Produktions-IT müssen weiter zusammenwachsen und einheitliche Standards und Normen für die IT-Sicherheit von Produktionsanlagen verfasst werden. Optimal wäre es, wenn schlussendlich die Office-IT zusammen mit der Produktions-IT genormt wird, sodass es einen allgemeingültigen, übergreifenden IT-Sicherheitsstandard gibt.

OPC UA eignet sich wunderbar für die Kommunikation in Industrie 4.0. Weiche Echtzeitanforderungen können mit OPC UA TSN bedient werden; für harte Echtzeitanforderungen müssen allerdings weiterhin Feldbusse genutzt werden. Ein bleibendes Problem ist die Verwaltung der enormen Anzahl von Identitäten der Kommunikationsteilnehmer.

Literaturverzeichnis

[BMW16a] BMWi - Bundesministerium für Wirtschaft und Energie (Hrsg.) *IT-Security in der Industrie 4.0: Handlungsfelder für Betreiber*. Techn. Ber. Berlin: Plattform Industrie 4.0, 2016, S. 1–49. URL: http://www.plattform-i40.de/I40/Redaktion/DE/Downloads/Publikation/leitfaden-it-security-i40.pdf.

[BMW16b] BMWi - Bundesministerium für Wirtschaft und Energie (Hrsg.) *IT-Sicherheit für Industrie 4.0, Abschlussbericht - Kurzfassung*. Techn. Ber. Berlin: Bundesministerium für Wirtschaft und Energie (BMWi), 2016, S. 1–37. URL: http://www.bmwi.de/Redaktion/DE/Downloads/I/studie-it-sicherheit-fuer-industrie-4-0-kurzfassung.pdf.

[BSI13] BSI. *ICS-Security-Kompendium*. 2013. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security_kompendium_pdf.pdf (besucht am 21. 02. 2018).

[BSI16a] BSI. *Industrial Control System Security Top 10 – Bedrohungen und Gegenmaßnahmen 2016*. BSI-Veröffentlichungen zur Cyber-Sicherheit. Bundesamt für Sicherheit in der Informationstechnik, 2016. URL: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_005.pdf?__blob=publicationFile (besucht am 21. 02. 2018).

[BSI16b] BSI. *Sicherheitsanalyse OPC UA*. Bundesamt für Sicherheit in der Informationstechnik, 2016. URL: https://www.bsi.bund.de/DE/Publikationen/Studien/OPCUA/opcua.html (besucht am 21. 02. 2018).

[Bur13] T. J. Burke. *OPC Unified Architecture – Wegbereiter der 4. industriellen (R)Evolution*. OPC Foundation, 2013. URL: https://www.iosb.fraunhofer.de/servlet/is/21752/OPC-UA-Wegbereiter-der-I40.pdf?command=downloadContent&filename=OPC-UA-Wegbereiter-der-I40.pdf (besucht am 21. 02. 2018).

[Dzu+05] D. Dzung u. a. "Security for Industrial Communication Systems". In: *Proceedings of the IEEE*. Bd. 93. 6. IEEE, Juni 2005. URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.332.5162&rep=rep1&type=pdf.

[Eck17] C. Eckert. *Handbuch Industrie 4.0 – Geschäftsmodelle, Prozesse, Technik*. Hrsg. von G. Reinhart. München: Carl Hanser Verlag, 2017. Kap. 5: Cyber-Sicherheit in Industrie 4.0, S. 111–136. ISBN: 978-3-446-44642-7.

[Jes+17] S. Jeschke u. a. "Industrial Internet of Things and Cyber Manufacturing Systems". In: *Industrial Internet of Things: Cybermanufacturing Systems*. Hrsg. von S. Jeschke u. a. Cham: Springer International Publishing, 2017, S. 3–19. ISBN: 978-3-319-42559-7. DOI: 10.1007/978-3-319-42559-7_1. URL: https://doi.org/10.1007/978-3-319-42559-7_1.

[Joh16] C. Johnson. "Securing Safety-Critical SCADA in the Internet of Things". 2016. URL: http://www.dcs.gla.ac.uk/~johnson/papers/IET2016/SCADA_IoT.pdf (besucht am 21. 02. 2018).

[KWH13] H. Kagermann, W. Wahlster und J. Helbig. *Recommendations for implementing the strategic initiative INDUSTRIE 4.0*. Techn. Ber. Frankfurt/Main: INDUSTRIE 4.0 Workgroup, 2013, S. 1–78. URL: http://www.acatech.de/fileadmin/user_upload/Baumstruktur_nach_Website/Acatech/root/de/Material_fuer_Sonderseiten/Industrie_4.0/Final_report__Industrie_4.0_accessible.pdf.

[LBK14] J. Lee, B. Bagheri und H.-A. Kao. "A Cyber-Physical Systems architecure for Industry 4.0-based manufacturing systems". In: *SME Manufacturing Letters*. Bd. 3. 12. Cincinnati: Elsevier Ltd., 2014, S. 18–23. DOI: 10.1016. URL: https://www.researchgate.net/profile/Jay_Lee10/publication/269709304.

[Mag+17] F. Maggi u. a. "Rogue Robots: Testing the Limits of an Industrial Robot's Security". 2017. URL: https://documents.trendmicro.com/assets/wp/wp-industrial-robot-security.pdf (besucht am 21. 02. 2018).

[PBS16] C. Pogacean, S. Broschei und G. Süss. *Implementing Deterministic OPC UA Communication*. Haar: Softing Industrial Automation GmbH, 2016, S. 1–19. URL: https://www.automation.com/pdf_articles/softingna/OPCUAPublisherSubscriber_W_EN_160407_100.pdf.

[SN13] R. von Solms und J. van Niekerk. "From information security to cyber security". In: *Computers & Security*. Bd. 38. 10. Elsevier Ltd., 2013, S. 97–102. DOI: 10.1016/j.cose.2013.04.004. URL: https://www.researchgate.net/profile/Johan_Van_Niekerk2/publication/278325582.

[SWW15] A.-R. Sadeghi, C. Wachsmann und M. Waidner. "Security and privacy challenges in industrial internet of things". In: *Proceedings of the 52nd Annual Design Automation Conference - DAC*. San Francisco: ACM, 2015, S. 1–6. DOI: 10.1145/2744769.2747942. URL: https://www.academia.edu/23878296/Security_and_Privacy_Challenges_in_Industrial_Internet_of_Things.

[Ull+16] N. Ulltveit-Moe u. a. "Secure Information Sharing in an Industrial Internet of Things". 2016. URL: https://arxiv.org/pdf/1601.04301.pdf.

[VDI13] VDI - Verein Deutscher Ingenieure e.V. (Hrsg.) *Cyber-Physical Systems: Chancen und Nutzen aus Sicht der Automation*. Techn. Ber. Düsseldorf: VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik (GMA), 2013, S. 1–12. URL: https://www.vdi.de/uploads/media/Stellungnahme_Cyber-Physical_Systems.pdf.

[Wai+13] M. Waidner u. a. *Eberbacher Gespräch zu „Sicherheit in der Industrie 4.0"*. Okt. 2013. URL: https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Eberbach-Industrie4.0_FraunhoferSIT.pdf (besucht am 21. 02. 2018).

[WK16] M. Waidner und M. Kasper. “Security in industrie 4.0 - challenges and solutions for the fourth industrial revolution”. In: *2016 Design, Automation & Test in Europe Conference & Exhibition (DATE)* (2016), S. 1303–1308.