von Matthias Eckhart

Industrie 4.0 - aber sicher

Das Schlagwort „Industrie 4.0" erzeugt die Vision einer durchwegs digitalen Wertschöpfungskette. Der Begriff beschreibt die Veränderung des traditionellen Produktionsprozesses durch die Vernetzung von Maschinen, Sensoren sowie Aktoren, um ein digitales Abbild der realen Welt zu schaffen. Technische Grundlage sind cyber-physische Systeme (CPS) – also Systeme, die physische mit informationsverarbeitenden, softwarebasierten Komponenten verknüpfen. Mit diesen Verflechtung können intelligente Systeme erschaffen werden, die autonom Prozesse, abhängig von bestimmten Einflussfaktoren, steuern und optimieren können. Dabei beschränkt sich diese Entwicklung nicht nur auf die Automatisierung in der Produktionsindustrie, sondern tangiert auch andere Bereiche wie etwa das Transportwesen oder die Energiewirtschaft. Zusammengefasst wird dies unter dem Begriff „industrielles Internet der Dinge" (engl. Industrial Internet of Things, IIoT), der schon den hohen Grad an Vernetzung von (industriellen) Gegenständen mit dem Internet andeutet.

In diesem Kontext ist die Informationssicherheit als unabdingbare Grundvoraussetzung anzusehen, da nicht nur durch die umfassende Vernetzung weitere Angriffsvektoren entstehen, sondern auch typische Anwendungsszenarien aufgrund ihrer Kritikalität (z.B. Smart Grids) ein attraktives Angriffsziel darstellen. Diese Herausforderung verschärft sich zusätzlich durch den Umstand, dass im Sinne von Industrie 4.0 & IIoT streng isolierte industrielle Steuerungssysteme (engl. Industrial Control System, ICS) nun gewissermaßen dem Internet geöffnet werden. Nicht unbegründet ist daher die Sorge, dass die erfolgreiche Realisierung der „intelligenten Fabrik" an der Implementierung von adäquaten Maßnahmen zur Wahrung der Informationssicherheit scheitert. Dass Cyberangriffe auf ICS längst eine ernstzunehmende Bedrohung darstellen, bestätigt auch der Jahresbericht des US-amerikanischen ICS-CERT, in dem 222 Sicherheitsvorfälle für das Jahr 2016 vermerkt wurden (ICS-CERT, 2017). Dabei dürfte die Dunkelziffer nicht registrierter ICS-bezogener Attacken weit höher liegen und die graduelle Adaptierung von Industrie 4.0- & IIoT-Lösungen IT-Sicherheitsexpertinnen und -experten vor neue Herausforderungen stellen.

DIE ALTLASTEN DER DRITTEN INDUSTRIELLEN REVOLUTION

In Bezug auf die Informationssicherheit kann Industrie 4.0 & IIoT aber nicht nur als Herausforderung, sondern auch als Chance betrachtet werden, um Legacy-Komponenten aus dem ICS zu entfernen. Charakteristisch für eine traditionelle ICS-Architektur ist die Heterogenität des Netzwerkes, sowohl auf der vertikalen, als auch horizontalen Ebene. Die daraus resultierenden Technologiebrüche verursachen vor allem einen hohen Aufwand in der Wartung und Implementierung unterschiedlicher Sicherheitsmaßnahmen. Besonders im Kontrollnetzwerk ist diese Situation problematisch, da neben der Vielzahl an am Markt verfügbaren industriellen Kommunikationsprotokolle auch kaum Sicherheitsmechanismen im Protokoll selbst vorgesehen wurden. Exemplarisch sei hier das Feldbusprotokoll Modbus genannt, das weder Mechanismen zur Authentifizierung, noch zur Verschlüsselung bereitstellt. Ähnlich ist dies auch bei PROFIBUS der Fall, dessen Schwachstellen von Stuxnet ausgenutzt wurden (Abouzakhar, 2013; Karnouskos, 2011). Die Implementierung von Schutzmechanismen innerhalb des Kontrollnetzwerkes gestaltet sich im Vergleich zum Unternehmensnetzwerk schwierig, da weder die Echtzeitkommunikation industrieller Kommunikationsprotokolle eingeschränkt, noch die Zuverlässigkeit des Kommunikationsflusses gefährdet werden darf. Aus diesem Grund werden i.d.R. innerhalb des Kontrollnetzwerkes lediglich passive Schutzmechanismen (IDS) und nur an den Grenzen des Netzwerkes aktiver Schutz (IPS) eingesetzt (Knapp & Langill, 2015). Die dadurch aufgebauten Sicherheitszonen verschwimmen jedoch mit der Annäherung der Bereiche IT und OT (Operational Technology), entsprechend den Prinzipien von Industrie 4.0 & IIoT, ineinander. Dieser Wandel verlangt nach einem standardisierten Kommunikationsprotokoll, das Sicherheitsaspekte gemäß dem Stand der Technik berücksichtigt und eine Integration auf vertikaler und horizontaler Ebene der ICS-Architektur erlaubt. Als Antwort auf diesen Bedarf entwickelte die OPC Foundation den Standard OPC Unified Architecture (UA).

OPC UA IST ENABLER FÜR INDUSTRIE 4.0

Das industrielle Kommunikationsprotokoll OPC UA wird als Schlüsseltechnologie für die Umsetzung von Industrie 4.0 gepriesen, da sich der Standard den Herausforderungen der vierten industriellen Revolution annimmt (OPC Foundation, 2013). Ganz nach den Grundsätzen „Secure by Design" wurde bei der Entwicklung des neuen OPC-Standards die Informationssicherheit miteinbezogen. Demgemäß werden die folgenden Sicherheitsziele spezifiziert (Gallinat, Hausmann, Köster, & Heiss, 2014; Pocock, Kominek, & Hunkar, 2014a, 2014b):

- **Vertraulichkeit** wird erreicht durch das Verschlüsseln der Kommunikation
- **Integrität** wird gewährleistet durch das Signieren der Nachrichten
- **Authentifizierung** sowohl von Benutzerinnen und Benutzer via Benutzername/Passwort, WS-Security Token oder X.509, als auch von Applikationen mittels X.509

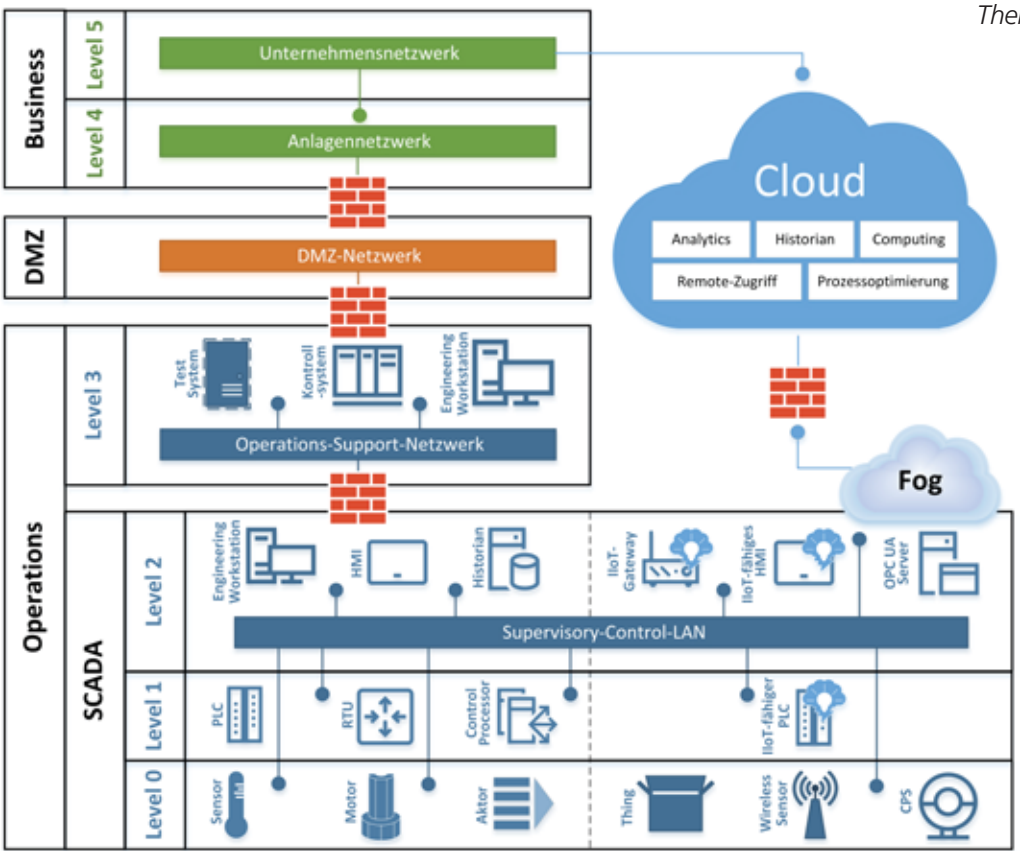

Abbildung 1: IIoT-fähige ICS-Architektur in Anlehnung an das Purdue-Referenzmodell (PERA) (SANS Institute, 2016).

- **Autorisierung** von Benutzerinnen und Benutzern erfolgt mittels granularer Rechtevergabe
- **Verfügbarkeit** des OPC UA Servers wird durch Abwehrmechanismen gegen DoS-Attacken gewährleistet
- **Nachvollziehbarkeit** von Aktionen am OPC UA Server wird dank integrierter Audit-Funktionalität erreicht

Da OPC UA entweder als Binärprotokoll oder über HTTP, optional auch mit SOAP-Anbindung, genutzt werden kann, kommen jeweils unterschiedliche Sicherheitsmechanismen zum Einsatz. Erfolgt die Kommunikation etwa über das Binärprotokoll UA-TCP, so wird der Datenverkehr mittels dem eigens spezifizierten Verfahren UA-SC abgesichert. Dabei kommen je nach eingesetzter Sicherheitsrichtlinie unterschiedliche Varianten der Verschlüsselungsverfahren AES und RSA zur Anwendung. Erfolgt hingegen die Kommunikation über HTTP, so greift der Standard auf das bewährte Protokoll TLS zurück. Eine weitere Option des Standards ermöglicht die Absicherung des SOAP-Datenverkehrs über WS-SC.

Zusammengefasst bietet OPC UA ein umfangreiches Sicherheitskonzept, mit dem die OPC Foundation einen vorbildlichen Schritt in die richtige Richtung macht. Obwohl der Einsatz eines einheitlichen Standards der Protokollvielfalt in der ICS-Landschaft Einhalt gebieten dürfte, ist dies in naher Zukunft aber kaum realistisch.

DIE ICS -ARCHITEKTUR VON MORGEN

Aufgrund der hohen Lebensdauer der ICS-Komponenten von 15 – 30 Jahren (Macaulay & Singer, 2016, S. 16) wird die „intelligente Fabrik" wohl nicht auf der grünen Wiese gebaut. Stattdessen wird primär die vorhandene Infrastruktur erweitert (vgl. Abbildung 1). Dadurch eröffnet sich die neue Produktsparte der sog. IIoT-Gateways, die die Kluft zwischen der dritten und vierten industriellen Revolution überbrücken. Typischerweise werden diese Komponenten nahe am oder im Kontrollnetzwerk platziert und dienen als Anbindung an die Cloud. Dies macht sie zu einem attraktiven Angriffsziel, zumal sie auch eine Rolle in „Fog Computing" einnehmen können. Demzufolge sind potenziell sensible Daten, die nicht, oder nur in aggregierter Form in die Cloud transferiert werden, einem Risiko ausgesetzt.

Veranlasst durch dieses Gefahrenpotenzial erforscht SBA Research Angriffsvektoren im Bereich Industrie 4.0. Derzeit ist eine Modellfabrik in Planung, in der mittels eines Gateways traditionelle und IIoT-spezifische Protokolle verknüpft werden. Basierend auf dieser Grundlage wird neben einer Netzwerkanalyse auch das Sicherheitsrisiko durch BYOD im ICS-Umfeld analysiert. So kommen etwa auch Apps zur Fernwartung von Steuerungssystemen auf den Prüfstand. Wie aktuelle Publikationen von SBA Research aus den verwandten Forschungsbereichen „Sicherheit kritischer Infrastrukturen" (Dabrowski, Ullrich, & Weippl, 2017), „Schutz von IoT-Geräten" (Judmayer, Ullrich, Merzdovnik, Voyiatzis, & Weippl, 2017) und „Hardware-Trojaner" (Kitsos, Sklavos, & Voyiatzis, 2017) zeigen, können wir bereits auf umfangreiches Know-how zurückgreifen.

Dieser OR Code führt Sie zur Online-Literatur-Übersicht:

Matthias Eckhart ist Junior Researcher bei SBA Research und befasst sich mit dem Thema Informationssicherheit in Bezug auf cyber-physische Systeme (CPS), IIoT und Industrie 4.0. Zuvor forschte er als wissenschaftlicher Mitarbeiter am Institut Internet-Technologien & -Anwendungen der FH JOANNEUM in Kapfenberg.