AUTONOMIK
INDUSTRIE 4.0

Leitfaden Band 5

Sichere Softwarearchitekturen für Industrie 4.0

Impressum

Herausgeber
Begleitforschung AUTONOMIK für Industrie 4.0
VDI/VDE Innovation + Technik GmbH
Alfons Botthof
Steinplatz 1 | 10623 Berlin
alfons.botthof@vdivde-it.de

www.autonomik40.de

Texte
Inessa Seifert (VDI/VDE Innovation + Technik GmbH)
Peter Gabriel (VDI/VDE Innovation + Technik GmbH)

Gestaltung
Loesch*Hund*Liepold
Kommunikation GmbH
Hauptstraße 28 | 10827 Berlin

Stand
September 2016

Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

Inhalt

Inhalt

1 Einführung 4

2 Checkliste für Anwender 5

3 Allgemeine Vorgaben an funktionale Sicherheit, IT-Sicherheit und Datenschutz 7
3.1 Funktionale Sicherheit 7
3.2 IT-Sicherheit 7
3.3 Datenschutz 8

4 Referenzarchitekturmodelle und grundlegende Standards und Normen 9
4.1 RAMI 4.0 9
4.2 IIRA 10
4.3 RAMI 4.0 und IIRA: ein Vergleich 11
4.4 Standards und Normen für IT-Sicherheit 12
4.5 Standards und Normen für funktionale Sicherheit 13
4.6 Standards und Normen für sichere Identitäten 14
4.7 Kommunikation: OPC Unified Architecture 14
4.8 Entwicklungsprozess für sichere Software: Secure Development Lifecycle 15

5 RAMI 4.0 und IIRA in der Praxis: die Sicht der AUTONOMIK-Projekte 17
5.1 APPsist 17
5.2 CoCoS 17
5.3 GEMINI 18
5.4 InnoCyFer 18
5.5 MANUSERV 18
5.6 motionEAP 19
5.7 OPAK 19
5.8 Fazit 20

6 Literaturverzeichnis 21

1 Einführung

Der Leitfaden umreißt die allgemeinen gesetzlichen Vorgaben für die funktionale Sicherheit, die IT-Sicherheit und den Datenschutz bei Produktionssystemen. Er führt in die beiden aktuellen Referenzarchitekturmodelle für Industrie 4.0 RAMI und IIRA ein und benennt die grundlegenden Standards und Normen für Software-Komponenten in vernetzten Industrieanlagen. Softwarearchitekten und Systementwicklern gibt er damit eine Orientierung für den Umgang mit den heterogenen IT-Technologien in Industrie 4.0 und für die Gestaltung von sicheren Softwarearchitekturen in diesem anspruchsvollen Umfeld. Leser, die an einer weitergehenden, konkreten Bewertung der Referenzarchitekturen RAMI und IIRA interessiert sind, verweisen wir auf die Dokumentation des Workshops „Softwarearchitekturen für Industrie 4.0“, der Anfang 2016 stattgefunden hat (Institut für Innovation und Technik 2016). Beim Workshop haben sieben Verbundprojekte aus „AUTONOMIK für Industrie 4.0“ die Referenzmodelle hinsichtlich der Passfähigkeit für ihre tatsächlichen Software-Architekturen bewertet. Im Anhang findet sich eine Zusammenfassung der Workshop-Ergebnisse.

RAMI ➡ Referenzarchitekturmodell Industrie 4.0
IIRA ➡ Industrial Internet Reference Architecture

2 Checkliste für Anwender

1. Im Vorfeld der Gestaltung von Softwarearchitekturen für Industrie 4.0 sollen die relevanten rechtlichen Rahmenbedingungen für funktionale Sicherheit, IT-Sicherheit und Datenschutz ermittelt werden, die in die Anforderungsanalyse sowie in die funktionale Spezifikation des Systems mit einfließen (siehe Kapitel 3).

2. Aus der Analyse der rechtlichen Rahmenbedingungen sollen die relevanten Normen und Standards zur funktionalen Sicherheit, IT-Sicherheit und Datenschutz abgeleitet werden, um einen rechtlich abgesicherten Einsatz von cyberphysischen Systemen in einer hochkomplexen Produktionsumgebung zu gewährleisten (siehe Kapitel 4.4, 4.5, 4.6).

3. Für die Einordnung und die Spezifikation der Interaktion zwischen den funktionalen Komponenten sollen möglichst aktuelle Referenzarchitekturmodelle verwendet werden, um einerseits die Kommunikation zwischen verschiedenen Akteuren (Systementwickler, Integratoren und Betreiber) in unternehmensübergreifenden Wertschöpfungsnetzten und andererseits die Integration der Komponenten in der heterogenen Technologielandschaft zu erleichtern (siehe Kapitel 4.1, 4.2).

4. Sowohl in der Anforderungsanalyse, bei dem Entwurf, während der Spezifikation als auch in der Implementierung und Tests von cyberphysischen Produktionssystemen sollen Security-, ggf. Data Protection- sowie Privacy by- Design Prinzipien berücksichtigt und angewendet werden.

Weitere Informationen:

Zu 1: Als Einstieg zur Orientierung für die Ermittlung der relevanten Rechtsgebiete bietet sich der in der gleichen Reihe erschienene Leitfaden „Rechtliche Orientierung für digitale Wertschöpfung“ der Begleitforschung „AUTONOMIK für Industrie 4.0“ an.

Zu 2, 3: Zur horizontalen und vertikalen Integration von Komponenten sowie Realisierung der Service-orientierten Architektur-Prinzipien kann das RAMI 4.0 Schichtenmodell genutzt werden. Für die Spezifikation der Interaktion zwischen den Komponenten sowie für die Realisierung der Schlüsseleigenschaften (Safety, Security und Resilienz) kann als Orientierung IIRA (Industrial Internet Refernce Architecture) vom IIC (Industrial Internet Consortium) genutzt werden. (VDI/VDE-GEMA, ZVEI (Hg.): Statusreport. Referenzarchitekturmodell Industrie 4.0 (RAMI4.0), Düsseldorf/Frankfurt am Main 2015. (www.vdi.de/fileadmin/vdi_de/redakteur_dateien/gma_dateien/Statusreport_Referenzmodelle_2015_v10_WEB.pdf), Industrial Internet Consrtium: Industrial Internet Reference Architecture, Version 1.7, 2015. (www.iiconsortium.org/IIRA-1-7-ajs.pdf))

Einen guten Einstieg in die grundlegenden Normen der funktionalen Sicherheit im Maschinen und Anlagenbau bietet der Leitfaden des ZVEI. (ZVEI: Sicherheit von Maschinen. Erläuterungen zur Anwendung der Normen EN 62061 und EN ISO 13849-1, Edition II, Frankfurt am Main 2012 (www.zvei.org/Verband/Publikationen/Seiten/Sicherheit-von-Maschinen.aspx))

Zu 4: Zur Realisierung eines Identitäten-Management-Systems für die vertrauenswürdige und sichere Kommunikation zwischen den Nutzern und Komponenten auch unter Berücksichtigung der unternehmensübergreifenden Kommunikation kann der Leitfaden der Plattform Industrie 4.0 AG 3 „Sichere Identitäten“ genutzt werden. (Plattform Industrie 4.0: Technischer Überblick: Sichere Identitäten, Berlin 2016 (www.plattform-i40.de/I40/Redaktion/DE/Downloads/Publikation/sichere-identitaeten.html))

Zur Betrachtung der datenschutzrelevanten Aspekte können die Leitfäden des BITKOM „Kompass der IT-Sicherheitsstandards“ und der Plattform Industrie 4.0 AG 3, „Sichere Identitäten“ genutzt werden. (Bitkom, DIN (Hg.): Kompass der IT-Sicherheitsstandards. Auszüge zum Thema Elektronische Identitäten, Berlin 2014 (https://www.bitkom.org/Bitkom/Publikationen/Kompass-der-IT-Sicherheitsstandards.html))

Zur Einhaltung von Security-by-Design-Prinzipien bei dem Entwurf, Implementierung und Tests von Sicherheitsarchitekturen kann als Orientierung Microsoft SDL genutzt werden. (Steve Lipner, Michael Howard: Entwicklungszyklus für sichere Software, Microsoft Developer Network, 30.5.2015 (https://msdn.microsoft.com/de-de/library/ms995349.aspx))

Als Überblick über den aktuellen Stand der Technik im Sinne des IT-Sicherheitsgesetztes (ITSiG) eignet sich die Handreichung von Teletrust. (TeleTrust (Hg.): Handreichung zum „Stand der Technik" im Sinne des IT-Sicherheitsgesetzes (ITSiG), Berlin 2016 (www.teletrust.de/fileadmin/docs/fachgruppen/ag-stand-der-technik/TeleTrusT-Handreichung_Stand_der_Technik.pdf))

Für die Betreiber und Hersteller der cyberphysischen Produktionssysteme haben die Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) eine hohe Relevanz:

- Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) zur Überprüfung von Basisschutzmaßnahmen von Industriellen Steuerungssystemen (Industrial Control Systems) „Light and Right Security" ICS (LARS ICS): https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/Tools/LarsICS/LarsICS.html
- Empfehlungen für Hersteller und Integratoren von ICS des Bundesamts für Sicherheit in der Informationstechnik (BSI), Handhabung von Schwachstellen https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/Empfehlungen/ICS-Hersteller/empfehlungen_hersteller_node.

Aktuell sind folgende Netzwerkte, die sich mit sicheren Softwarearchitekturen in Industrie 4.0 befassen, besonders aktiv: Plattform Industrie 4.0 AG 3 (http://www.plattform-i40.de/I40/Navigation/DE/Plattform/Plattform-Industrie-40/plattform-industrie-40.html) „Sicherheit vernetzter Systeme", Industrial Internet Consortium (http://www.iiconsortium.org), Allianz für Cyber-Sicherheit (https://www.allianz-fuer-cybersicherheit.de). Diese Angaben haben keinen Anspruch auf Vollständigkeit!

3 Allgemeine Vorgaben an funktionale Sicherheit, IT-Sicherheit und Datenschutz

Für die Software in Produktionsanlagen gelten zum Teil sehr spezifische gesetzliche Anforderungen, die auch von Industrie-4.0-Systemen erfüllt werden müssen. Die Anforderungen an die funktionale Sicherheit der Produktions- und Automatisierungssysteme fasst die EU-Maschinenrichtlinie zusammen, und das deutsche IT-Sicherheitsgesetz benennt Anforderungen an die IT-Sicherheit von „kritischen Infrastrukturen". Der Umgang mit personenbezogenen Daten wird durch die europäische und deutsche Datenschutzgesetzgebung geregelt. Die gesetzlichen Rahmenbedingen definieren Verantwortlichkeiten, Rechte und Pflichten für die Gestaltung, den Betrieb und die Nutzung der technischen Systeme. Als Voraussetzung für den verantwortungsvollen Umgang mit technischen Systemen gelten technische und organisatorische Maßnahmen, die dem aktuellen „Stand der Technik" entsprechen. Der Stand der Technik wird dabei wesentlich durch aktuelle Normen und Standards von DIN, ISO, DKE oder ISO/IEC und anderen Normungsgremien definiert.

Eine tiefergehende Betrachtung der von Industrie 4.0 berührten Rechtsgebiete findet sich im Leitfaden „Rechtliche Orientierung für digitale Wertschöpfung" der Begleitforschung „AUTONOMIK für Industrie 4.0". Dort werden insbesondere zivil- und strafrechtliche Fragen der Produkthaftung und der Fahrlässigkeit sowie der Umgang mit personenbezogenen Daten im Detail betrachtet.

3.1 Funktionale Sicherheit

Die Funktionale Sicherheit (Safety) von industriellen Anlagen und Maschinen ist durch die Richtlinie 2006/42/EG des europäischen Parlaments gesetzlich verankert. Diese „Maschinenrichtlinie" verlangt die Einhaltung von grundlegenden Sicherheits- und Gesundheitsschutzanforderungen, so dass von Maschinen keine Gefahr für Menschen entstehen darf, die diese Maschinen bedienen oder in Berührung mit ihnen kommen. Dabei muss bei der Konstruktion und Bau der Maschinen berücksichtig werden, dass auch ungeschultes Personal (also Laien) in die unmittelbare Nähe dieser Maschinen gelangen kann.

Durch die wachsende Komplexität der Produktions- und Automatisierungstechnik besteht immer ein Risiko von Funktionsfehlern, die nicht vollständig vorhersehbar sind. Für die Gewährleistung der funktionalen Sicherheit ist es wichtig, die Wahrscheinlichkeit von Funktionsfehlern möglichst gering zu halten. Sollten Funktionsfehler unvermeidbar sein, müssen die entsprechenden Sicherheitsfunktionen implementiert werden (z. B. ein Notfallknopf), die die schlimmsten Verletzungen oder gar Personenschäden verhindern können.

3.2 IT-Sicherheit

Die durchgängige Vernetzung der Produktionssysteme bietet eine wesentlich breitere Fläche für potenzielle Cyberangriffe, Ausspähattacken und Sabotage von Produktionsprozessen. Unter Umständen drohen damit Verletzungs- oder gar Lebensgefahr für die Beschäftigten und hohe Kosten durch Produktionsausfälle oder Verlust vertraulicher Informationen. Daher erhält die IT-Sicherheit in den intelligenten, vernetzten Produktionsanlagen der Zukunft eine besondere Bedeutung.

Auf der europäischen Ebene wurde kürzlich die Richtlinie zur Netz- und Informationssicherheit (NIS) verabschiedet. Die Richtlinie betrifft primär die kritischen Infrastrukturen aber auch Verkehrsknoten, Domain-Registrierungsstellen, Online-Marktplätze wie eBay oder Amazon sowie andere Plattformen in Form von Suchmaschinen wie Google und Cloud-Anbieter fallen unter das Gesetz. Nach zwei Jahren soll die NIS-Richtlinie in das nationale Gesetz umgesetzt werden[1]. Auf der nationalen Ebene wurde als Reaktion auf die zunehmende Bedrohung durch die Cyberangriffe von der Bundesregierung das „Gesetz zur Sicherheit von Kritischen Infrastrukturen" verabschiedet, das bereits vor einem Jahr, in Juli 2015, in Kraft trat.

Das Gesetzt betrifft primäre die Betreiber der kritischen Infrastrukturen aus den Bereichen Energie, IT und

1 http://www.heise.de/security/meldung/EU-Parlament-beschliesst-Cybersicherheitsgesetz-mit-Meldepflicht-3258129.html

Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz und Versicherungswesen, die nun verpflichtet sind, ein Mindestniveau an IT-Sicherheit einzuhalten und erhebliche Störungen an das Bundesamt für Sicherheit in der Informationstechnik (BSI) zu melden. Darüber hinaus sind die IT-Sicherheitsanforderungen für Telekommunikations- und Telemedienanbieter erhört worden, um die Sicherheit im Internet zu steigern.

Die Betreiber der kritischen Infrastrukturen müssen ihre IT-Systeme nach dem Stand der Technik angemessen absichern und dabei die branchenspezifischen Sicherheitsstandards gemäß dem jeweiligen Stand der Technik beachten. Die sofortige Meldepflicht der IT-Sicherheitsvorfälle betrifft zunächst nur die Betreiber von Kernkraftwerken und Telekommunikationsunternehmen. Allerdings wird bereits überlegt, ob nicht durch Industrie 4.0 eine weitere kritische Infrastruktur entsteht, die unter das „Gesetz zur Sicherheit von Kritischen Infrastrukturen" fällt. Der staatliche Regulierungsbedarf, insbesondere die Ausweitung von der Aufsichtspflicht durch das BSI und der Datenschutzbehörde auf die wirtschaftlichen Unternehmen, - oder im Gegensatz dazu - Wege zur Selbstregulierung der IT-Sicherheit z. B. durch Vergabe von IT-Sicherheitszertifikaten werden momentan intensiv in der Öffentlichkeit auf zahlreichen Konferenzen und Foren diskutiert, u. a. auf dem IT-Sicherheitsforum des BMWi.

3.3 Datenschutz

Beispiele für die Erfassung von personenbezogenen Daten findet man auf verschiedenen Ebenen von Industrie 4.0. Wenn private Kunden sich am Produktdesign beteiligen, werden ihre persönliche Wünsche und Präfenzen gespeichert. Bei der Interaktion von Mensch und Roboter oder beim Einsatz von Assistenzsystemen in Produktion und Wartung werden auch Daten zum Verhalten der Arbeitnehmer erfasst. Die entsprechenden Regelungen nach europäischem und deutschem Datenschutzrecht werden im erwähnten Leitfaden „Rechtliche Orientierung für digitale Wertschöpfung" thematisiert. In den internationalen Wertschöpfungsketten von Industrie 4.0 kommt es auch leicht zum Transfer personenbezogener Daten in das Ausland. Für den Datentransfer in die USA wurde dafür vor kurzem das Datenschutzabkommen EU-US Privacy-Shield am 12. Juli 2016 vereinbart[2].

2 http://europa.eu/rapid/press-release_IP-16-2461_en.htm

In der Studie „IT-Sicherheit für die Industrie 4.0. Produktion, Produkte, Dienste von morgen im Zeichen globalisierter Wertschöpfungsketten" hat das BMWi die rechtlichen, organisatorischen und technologischen Aspekte der IT-Sicherheit für die Industrie 4.0 untersuchen lassen (BMWi 2016).

„Zentrale Empfehlungen der Studie, die sich an Unternehmen, insbesondere aus dem Mittelstand, an die Forschungseinrichtungen und die Politik wenden, sind:

- Die konsequente Etablierung eines guten Basisschutzes in Betrieben mit Hilfe heute verfügbarer Sicherheitstechnologien als wichtige Voraussetzung zur Partizipation an Industrie 4.0.
- Die rechtliche Regulierung von IT-Sicherheit, u. a. mangels vorhandener Rechtsprechung, rechtlicher Klarheit zur Bedeutung technischer Standards und anerkannter Vertragspraxis, beispielsweise durch Musterklauseln.
- Die Einführung von Mindeststandards für IT-Sicherheit und die Verwendung von zertifizierten Produkten in digitalen Wertschöpfungsnetzen.
- Die Nutzung von Digitalen Identitäten in Form hardwarebasierter Vertrauensanker zur Absicherung von Kommunikationsbeziehungen.
- Die Schaffung von Konzepten für die integrierte Betrachtung von Safety- und Security-Aspekten, die in produktionstechnischen Umgebungen in engem Zusammenhang stehen."[1]

1 (http://www.bmwi.de/DE/Mediathek/publikationen,did=764200.html)

4 Referenzarchitekturmodelle und grundlegende Standards und Normen

Zurzeit gibt es zwei Referenzarchitekturmodelle, die eine Orientierung in der heterogenen Technologielandschaft für Industrie 4.0 und eine Einordnung der entsprechenden Standards und Normen bieten. Im April 2015 haben die Plattform Industrie 4.0, der ZVEI und die VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik (GMA) die erste Version des „Referenzarchitekturmodells für Industrie 4.0“ (RAMI 4.0) vorgestellt. Fast zeitgleich im Juni 2015 hat das internationale, überwiegend von IKT-Unternehmen getragene Industrial Internet Consortium (IIC) die „Industrial Internet Reference Architecture“ (IIRA 1.7) veröffentlicht. Beide Referenzarchitekturen haben sich zum Ziel gesetzt, einen einheitlichen Rahmen mit einem wohldefinierten Vokabular für die Entwicklung vernetzter IT-Systeme für Industrieanlagen zu definieren, um die Entwicklung solcher Systeme zu vereinfachen und zu beschleunigen.

Daneben existieren eine ganze Reihe weiterer Standards und Normen zu funktionaler Sicherheit, IT-Sicherheit und Datenschutz, die Entwickler von Industrie-4.0-Systemen kennen und berücksichtigen sollten. Auch für ein Kernelement einer industriellen Softwarearchitektur, die sichere Identität von Maschinen, Werkstücken und anderen cyberphysischen Systemen, sind bereits Standards und Normen verfügbar. Für die besonderen Belange der Kommunikationstechnik und der Vorgehensweise bei der Softwareentwicklung in diesen Systemen gibt es sogar schon konkrete technische Spezifikationen, die OPC Unified Architecture (OPC UA) bzw. den Secure Development Lifecycle (SDL).

4.1 RAMI 4.0

Die Hauptmotivation von RAMI 4.0 (Referenzarchitekturmodell für Industrie 4.) ist die Einordnung von bereits existierenden Standards und Normen, um Lücken in den vorhandenen Lösungen zu identifizieren und daraus neuen Bedarf an Standardisierung primär in den Bereichen Automatisierung- und Produktionstechnik abzuleiten (VDI/VDE-GEMA, ZVEI 2016).

Als Grundlage für das Modell wurde das Smart Grid Architecture Model (SGAM) gewählt, das sich als Modell für die Entwicklung moderner IT-basierter Stromnetze bewährt und durchgesetzt hat (CEN-CENELEC-ETSI Smart Grid Coordination Group 2012). SGAM wurde an die Anforderungen von Industrie 4.0 angepasst und erweitert.

RAMI 4.0 realisiert eine einheitliche Sicht auf die für Industrie 4.0 typischen Wertschöpfungsketten, in dem die Betrachtung der Produktions- und Engineeringaspekte in drei verschiedenen Dimensionen aufgeteilt werden.

Die erste Dimension umfasst die gängigen Ebenen der informationstechnischen Modellierung (layers): business layer (Geschäftssicht), functional layer (Funktionsschicht), informational layer (Informationsschicht), communication layer (Kommunikationsschicht), integration layer (Integrationsschicht) und asset layer (Gegenstandssicht). Die zweite Dimension beschreibt den Produktlebenszyklus, wobei zwischen Produkttypen und tatsächlich gefertigten Produktinstanzen unterschieden wird. Für Typen gibt es die Phasen development (Entwicklung) und (Nutzung/Wartung), für Instanzen die Phasen production (Produktion) und wiederum maintenance/usage. Die dritte Dimension beschreibt die funktionale Hierarchie innerhalb einer Anlage bzw. einer Fabrik (hierarchy levels): connected world (externe Partner), enterprise (Unternehmen), work unit (Produktions- oder Prozessumgebung), station (Maschine), control device (Steuersystem), field device (eigenständiges Feldgerät, z. B. ein Sensor) und product (Werkstück).

So lässt sich jeder einzelne Aspekt einer Industrieanlage durch einen RAMI-Würfel aus drei verschiedenen Dimensionen betrachten, welche Akteure mit welchen Aufgaben und Verantwortlichkeiten jeweils auf Ebene der Informationstechnik, des Produktlebenszyklus und der funktionalen Hierarchie berücksichtigt werden sollen.

In der Ausgestaltung der Kommunikationsschicht stützt sich RAMI 4.0 auf den Standard OPC UA, der im Kapitel 4.8 noch ausführlicher behandelt wird.

Datenschutzfragen und funktionale Sicherheit werden in RAMI 4.0 nicht explizit angesprochen. Die Plattform Industrie 4.0 hat aber als Ergänzungen Leitfäden zur IT-Sicherheit und zu sicheren Identitäten in RAMI 4.0 veröffentlicht (Plattform Industrie 4.0 2016a, b). Einen weiteren umfangreichen Leitfaden zur IT-Sicherheit im Sinne des IT-Sicherheitsgesetzes (ITSiG) hat Teletrust vorgelegt (Teletrust 2016). In allen Leitfäden wird die Nutzung der gängigen Standards und Normen für funktionale Sicherheit IT-Sicherheit und Datenschutz empfohlen.

4.2 IIRA

Die „Industrial Internet Reference Architecture“ (IIRA) geht über den Bereich Automatisierung- und Produktionstechnik hinaus und adressiert den breiteren Rahmen eines „Industrial Internet“ (IIC 2015). Anliegen von IIRA ist es, zwei bis jetzt getrennt voneinander betrachtete Welten – die gängige Informationstechnik (informational technologies) und IT-basierte Steuersysteme in der Industrie (operational technologies) – konzeptionell zu beschreiben und zu strukturieren, um daraus die Anforderungen an Technologien und Designprinzipien (design pattern) abzuleiten.

In IIRA werden als erstes eine Reihe von Schlüsseleigenschaften (key system charachteristics der künftigen Industrial Internet Systems (IIS)) eingeführt: Safety (funktionale Sicherheit), Security (IT-Sicherheit) und Resilience (Resilienz, Fehlertoleranz gegenüber internen und externen Störungen). Das Zielverhalten der (teil-)autonomen Industrial Internet Systeme wird durch die Anforderungen an Safety, Security und Resilience sowie die Zusammenhängen in der Interaktion zwischen den genannten Schlüsseleigenschaften definiert. Die Betrachtung von zentralen Eigenschaften eines IIS erfolgt aus den vier verschiedenen Blickwinkeln Business Viewpoint, Usage Viewpoint, Function Viewpoint und Implementation Viewpoint, die es erlauben, die Anforderungen an ein IIS aus den Perspektiven verschiedener Akteure wie Entwickler, Betreiber oder Bediener zu formulieren.

Als Hilfestellung für die Umsetzung der Eigenschaften eines Industrial Internet Systems, wie z. B. Selbstoptimierung, Selbstkonfiguration und auch Selbstheilung der Kommunikationsprozesse, schlägt IIRA eine Reihe von Design-Patterns vor, die als Hilfestellung für die Realisierung der Schlüsseleigenschaften eines IIS dienen. So enthalten die Design-Patterns Empfehlungen an die Softwarearchitekten, die für den Entwurf und Umsetzung von (teil-)autonomen Komponenten in heterogenen Kommunikationsumgebungen genutzt werden können.

Anders als in RAMI werden in IIRA Sicherheit, Datenschutz und Identitätssysteme ausdrücklich behandelt, wenn zum Teil auch auf sehr abstraktem Niveau:

Funktionale Sicherheit. Die Betrachtung der Safety-Aspekte ist in IIRA durchgehend auf einem relativ hohen Abstraktionslevel verankert. So dürfen z. B. die autonomen Komponenten eines Industrial Internet Systems keineswegs die Safety-Anforderungen der sicherheitskritischen Bestandteile der Systeme gefährden, auch wenn übergeordnete Befehle (commands) die funktionalen Sicherheitsanforderungen der Teilkomponenten verletzten. Jede Systemkomponente agiert in einem sogenannten Safety-Framework, das mit den rechtlichen Richtlinien und Rahmenbedingungen im Einklang steht. Konkrete Verknüpfungen zu den aktuellen Gesetzten oder Regelungen werden in IIRA nicht genannt.

IT-Sicherheit. In IIRA wird ein agentenbasierter Ansatz empfohlen, um die verschiedenen Aspekte der IT-Sicherheit möglichst gleichwertig zu gewährleisten. Dazu gehören die Sicherung aller physikalischen „Endpunkte“ (endpoints) wie Maschinen, Werkstücke oder Logistiksysteme (endpoint security), die Sicherung der Kommunikation (communication security), die Einrichtung eines umfassenden Managementsystems (management and monitoring security) sowie die Einrichtung von sicheren und rechtskonformen Systemen für die Speicherung und Verteilung von Daten (data distribution and secure storage). So soll die Verwaltung und Überwachung von

Sicherheitsvorfällen über die Kommunikation zwischen intelligenten Agenten stattfinden, die an verschiedenen verteilten Endpunkten stationiert sind, mit eigenem Entscheidungsspielraum ausgestattet sind, um möglichst autonom agieren zu können. Der Vorteil von den autonomen Agenten ist eine hohe Resilienz des gesamten Systems, das auch im Falle eines erfolgreichen Angriffs auf einen der Endpoints insgesamt stabil bleibt und nicht komplett ausfällt.

Sichere Identitäten. IIRA empfiehlt zur Gewährleistung der IT-Sicherheit für Endpunkte wie Maschinen, Werkstücke oder Logistikträger (endpoint security) die Verwendung von hardwarebasierten Ankern, d.h. Chips mit nicht änderbaren Identitäten (wie sie etwa als Trusted Platform Module [TPM] vom Industriekonsortium Trusted Computing Group definiert sind). Alle Operationen, die für den Aufbau und Aufrechterhaltung von einer verschlüsselten Kommunikation erforderlich sind, sollen auf dem Hardware-Chip stattfinden, um eine mögliche Kompromittierung der Identitäten auszuschließen.

Datenschutz. Die Autoren von IIRA gehen davon aus, dass sowohl personenbezogenen als auch Unternehmensdaten in Industriellen Internetbasierten Systemen permanent erfasst und analysiert und zwischen verschiedenen Anwendungen, aber auch Organisationseinheiten und Unternehmen ausgetauscht werden. IIRA definiert datenzentrierte Grundsätze (data centric policies), die generelle Empfehlungen zum Umgang mit verschiedenen Arten von Daten wie z. B. Finanzdaten oder gesundheitsrelevante Daten beinhalten. IIRA verweist lediglich darauf, dass die aktuellen gesetzlichen Vorschriften zur Speicherung, Analyse und Management sowie die Rechte der Eigentümer der sensiblen und personenbezogenen Daten berücksichtigt werden müssen. Konkrete Hinweise zu den Gesetzen oder Standards und Normen, die diese umsetzen, sind in IIRA 1.7 nicht enthalten.

4.3 RAMI 4.0 und IIRA: ein Vergleich

Wenn man die Ansätze von RAMI 4.0 und IIRA gegenüber stellt, wird deutlich, dass RAMI 4.0 vor allem eine Orientierung am Stand der Technik leistet, während IIRA stärker die Eigenschaften der künftigen Industrial Internet Systeme sowie die methodische Herangehensweise zur Gestaltung von Softwarearchitekturen im Vordergrund stellt.

Das wesentliche Ziel von RAMI 4.0 ist die vertikale und horizontale Integration von heterogenen Technologien mit verschiedenen Hardware- und Softwarekomponenten und Schaffung von einheitlichen Schnittstellen, die eine nahtlose Integration dieser Technologien in der Produktions- und Automatisierungsbranche ermöglichen. Konkrete Betrachtungen und Empfehlungen der Plattform Industrie 4.0 zur funktionalen Sicherheit fehlen zum jetzigen Zeitpunkt. Datenschutzrelevante Aspekte werden in RAMI 4.0 ebenfalls noch nicht explizit behandelt.

IIRA enthält dagegen sehr nützliche architektonische Vorschläge (Design-Patterns) zur Gestaltung von Interaktion und Kommunikation zwischen den einzelnen Komponenten der Industrial Internet Systeme als Orientierung für die Softwarearchitekten, um die Schlüsseleigenschaften funktionale Sicherheit, IT-Sicherheit und Resilienz zu erreichen.

Momentan findet ein intensiver Dialog zwischen der Plattform Industrie 4.0 und dem Industrial Internet Consortium statt, mit den Bestrebungen, IIRA- und RAMI-4.0-Konzepte zu harmonisieren[3]. Ein Workshop der Projekte in „AUTONOMIK für Industrie 4.0“ hat gezeigt, dass die Konzepte von IIRA 1.7 sich viel besser zur Umsetzung der Schlüsseleigenschaften „Safety, Security, Resilienz“ von Softwarearchitekturen eignen. Dagegen ist RAMI 4.0 viel stärker auf die Integration von Automatisierungs- und

3 Plattform Industrie 4.0: First major cooperation meeting between Plattform Industrie 4.0 and Industrial Internet Consortium in Chicago: Implementation of the joint roadmap, Pressemeldung, 20.5.2016 (http://www.plattform-i40.de/SiteGlobals/I40/Forms/Listen/EN/News/News_Formular.html?templateQueryString=Enter+search+term)

Produktionstechnologien und die Standardisierung der Schnittstellen fokussiert (Institut für Innovation und Technik 2016).

4.4 Standards und Normen für IT-Sicherheit

Unter „IT-Sicherheit" wird der „Schutz von Informationen jeglicher Art und Herkunft" verstanden (BSI 2008). Üblich ist die Unterteilung in drei „Schutzziele":

- Integrität: Die Informationen werden nicht ohne Berechtigung und unbemerkt verändert
- Vertraulichkeit: Es gibt keine unberechtigte Einsicht in die Informationen
- Verfügbarkeit: Die Informationen stehen Berechtigten ohne Beeinträchtigungen zur Verfügung.

Die Plattform Industrie 4.0 hat einen allerdings sehr knappen Leitfaden zu „Security in RAMI 4.0" veröffentlicht, der eine Herangehensweise zur Berücksichtigung der IT-Sicherheit bei dem Entwurf und der Realisierung von Automatisierungs- und Produktionssystemen für Industrie 4.0 beschreibt (Plattform Industrie 4.0 2016a). Hervorzuheben ist die holistische Sicht für die IT-Sicherheitsbetrachtungen, die jede Schicht, jede Phase des Produktlebenszyklus sowie jeden Aspekt der Funktionalitäten und Verantwortlichkeiten in der Fabrik/Anlage betrifft. Zur systematischen Betrachtung der IT-Sicherheitsaspekte wird in RAMI 4.0 die Anwendung der Standards IEC 62443 und VDI/VDE 2182 empfohlen:

Die Normenreihe IEC 62443 (Security for Industrial Process Measurement and Control – Network and System Security) wird in enger Kooperation mit der US-amerikanischen International Society of Automation (ISA) erarbeitet. Sowohl die europäische Normungsorganisation CENELEC als auch der VDE wurden die Normen der Reihe IEC 62443 zur IT-Sicherheit in industriellen Automatisierungssystemen und kritischen Infrastrukturen in die europäischen Normen der Reihe EN 62443 und entsprechend in die deutschen Normen der Reihe DIN EN 62443 (VDE 0802) übernommen. Die IEC 62443 lehnt sich in ihrer Struktur eng an die in der Praxis sehr häufig eingesetzte Norm ISO 27001 an, die Anforderungen an ein Managementsystem für Informationssicherheit (information security management systems) definiert, Empfehlungen für Maßnahmen der IT-Sicherheit und des Datenschutzes benennt und ein Schema für die Auditierung vorgibt.

Die Richtlinie VDI/VDE 2182 (Informationssicherheit in der industriellen Automatisierung) der VDI/VDE Gesellschaft für Mess- und Automatisierungstechnik (GMA) definiert ein Vorgehensmodell zur Sicherstellung der Informationstechnik in der Automatisierungstechnik. Bezüge zur ISO 27001 oder zur IEC 62443 werden allerdings nicht hergestellt.

Relevant ist auch das bereits 2013 vom Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlichte ICS-Security-Kompendium (ICS: industrial control system) (BSI 2013). Das Kompendium soll als Leitfaden für die Anwendung des bekannten IT-Grundschutzes des BSI auf heutige industrielle Steuerungsanlagen dienen, auf einen konkreten Bezug zu Konzepten für Industrie 4.0 wurde daher verzichtet. Das Kompendium enthält auch eine Abbildung der empfohlenen IT-Sicherheitsmaßnahmen zu den Maßnahmen, die in ISO/IEC 62443 enthalten sind. Auf diese Art und Weise bleibt die Konformität mit den internationalen Normen und Standards und somit mit dem nach dem IT-Sicherheitsgesetzt erforderlichen „Stand der Technik" erhalten.

Sowohl die Normenreihen 62443 als auch das BSI-Kompendium verfolgen ein Konzept zur hierarchisch strukturierten gestaffelten Verteidigung (defence in depth), die eine Aufteilung der IT-Systeme in Zonen (zones) und gesicherte Kanäle (conduits) voraussetzen. Inwieweit aktuell diskutierte Konzepte für ein Software Defined Networks und die damit einhergehende Abstraktion von den konkreten Netzwerkressourcen mit dem Prinzip der gestaffelten Verteidigung und der Aufteilung des gesamten Netzwerks in „Zonen" und „Kanäle" vereinbar sind, wird sich in der Weiterentwicklung von RAMI 4.0 und von

spezifischen Kommunikationstechnologien für Industrie 4.0 noch zeigen müssen.

4.5 Standards und Normen für funktionale Sicherheit

Funktionale Sicherheit (safety) ist ein zentraler Begriff der Ingenieurwissenschaften. Ziel ist der Schutz des Menschen oder materieller Werte vor Schäden durch ein technisches System bei systematischen oder zufälligen Fehlersituationen wie Systemfehlern, Bedienfehlern und Umwelteinwirkungen. Ziel ist die Minimierung dieses Risikos.

Zentrale und sehr weit verbreitete Norm der funktionalen Sicherheit bei IT-gesteuerten technischen Systemen ist die IEC 61508 (Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme), die mit quantitativen Sicherheitsanforderungsstufen (security integrity level, SIL) das Schadensrisiko quantifiziert. Allerdings ist die IEC 61508 als internationale Norm auf der europäischen Ebene nicht „harmonisiert". Das bedeutet, dass die Anwender dieser Standards ggf. eine zusätzliche Konformitätsprüfung für die Einhaltung der Maschinenrichtlinie benötigen.

Basierend auf der IEC 61508 haben sich Branchennormen entwickelt, wie etwa die DIN EN 61511 für die Prozessindustrie und die DIN EN 62061 für den Maschinenbau. Letztere ist unter der Maschinenrichtlinie harmonisiert. Praxisrelevant ist auch noch die EN ISO 13849-1, die anders als die IEC 61508 und ihre Ableger auch nichtelektronische Maschinensteuerungen abdeckt, z. B. mechanische oder pneumatische Steuerungen (ZVEI 2012).

Für spezielle Fälle wie z. B. der Umgang mit industriellen Robotern, existieren weitere Normen wie DIN EN ISO 10218-1 (Industrieroboter – Sicherheitsanforderungen), die entsprechende Sicherheitsanforderungen wie z. B. inhärent sichere Konstruktion, Schutzmaßnahmen und die Benutzerinformation für Industrieroboter festlegt. Die ISO 10218-Norm ist ebenfalls auf die Einhaltung der Maschinenrichtlinie ausgelegt.

Ein integrierter Standard für die Gewährleistung von IT-Sicherheit und funktionaler Sicherheit existiert zurzeit noch nicht. Herausforderung ist dabei, dass es bei der IT-Sicherheit im Gegensatz zur funktionalen Sicherheit keine etablierten Verfahren der quantitativen Risikoabschätzung gibt. Grundsätzlich ist von einem intelligenten, strategisch vorgehenden Angreifer von außen auszugehen, dessen Erfolgsquote nicht empirisch abgeschätzt werden kann.

4.6 Standards und Normen für Datenschutz

Der Datenschutz ist über das Schutzziel „Vertraulichkeit" Teil der IT-Sicherheit, geht aber wegen der gesetzliche Anforderung an den Umgang mit den persönlichen Daten des Einzelnen darüber hinaus.

Der IKT-Branchenverband Bitkom und der DIN empfehlen in ihrem Leitfaden „Kompass der IT-Sicherheitsstandards" eine Reihe von Normen, die eine systematische Herangehensweise zur Berücksichtigung des Datenschutzes in den IT-basierten Anwendungen und Systemarchitekturen darstellen (Bitkom, DIN 2014).

So beschreibt die Norm ISO/IEC 29100:2011 ein Rahmenwerk zur Wahrung des Datenschutzes. Sie beinhaltet die Definition der Terminologie, beschreibt die Akteure und ihre Rollen, die in der Verarbeitung personenbeziehbarer Daten involviert sind. Die Norm enthält darüber hinaus Verweise auf die wesentlichen Datenschutzgrundsätze, die in der Informationstechnologie zum Schutz der Privatsphäre eingehalten werden müssen.

Die ISO/IEC 29101 spezifiziert technische Aspekte des Datenschutzes, die in der Informations- und in der Kommunikationstechnologie bei der Verarbeitung personenbezogener Daten berücksichtigt werden müssen. Die Norm beschreibt Komponenten für die Implementierung datenschutzfreundlicher Systeme und enthält

Architekturansichten, die diese Komponenten in Kontext zueinander bringen. Darüber hinaus enthält die Norm Leitlinien für Planung, Konzeption und dem Bau von IKT-Systemarchitekturen, die die Privatsphäre der Personen, deren Daten verarbeitet werden, schützen, indem sie die Verarbeitung, von personenbeziehbaren Informationen kontrollierbar machen. Darüber hinaus gibt die Norm Hinweise darüber, wie direkte technische Maßnahmen zur Wahrung des Datenschutzes (privacy enhancing technologies, PET) als Datenschutzkontrollmechanismen eingesetzt werden können.

Da die EU-Datenschutzgrundverordnung erst kürzlich im Mai 2016 verabschiedet wurde, müssen die empfohlenen Normen auf Konformität mit der neuen Regulierung überprüft werden. Zudem sind noch Erweiterungen von RAMI 4.0 um die datenschutzrelevanten Aspekte sowie die Aktualisierung der Standards und Normen in Bezug auf die neue Datenschutzregulierung erforderlich. Entwickler und Anwender von Industrie 4.0 sollten die Entwicklungen in diesem Feld aufmerksam verfolgen.

4.7 Standards und Normen für sichere Identitäten

Sichere digitale Identitäten sind eine wichtige Voraussetzung für Industrie 4.0. Das gilt vor allem, wenn die Kommunikation der cyberphysikalischen Systeme über Unternehmensgrenzen hinweg geht oder zumindest technisch möglich ist.

Ein hohes Schutzniveau verspricht die Verwendung von vertrauenswürdigen hardwarebasierten Ankern (trusted computing), wie etwa in der IIRA vorgeschlagen. Beim Einsatz von Identifikations- und Authentifizierungsverfahren sind aber der gesamte Prozess zur Gewährleistung der sicheren Kommunikation und insbesondere die Aufbewahrung, Verwaltung und Überprüfung der Identitäten ausschlaggebend. In der Praxis werden Public-Key-Infrastruktur-Zertifikate eingesetzt, die auf der Basis von asymmetrischen kryptografischen Verfahren eine sichere Authentifizierung der Kommunikationspartner ermöglichen.

Obwohl Public-Key-Infrastrukturen bereits relativ gut in der „Office-IT“ etabliert sind, besitzen die PKI-Zertifikate einen entscheidenden Nachteil: sie haben nur eine begrenzte Lebensdauer und müssen regelmäßig durch sogenannte „Revocation Lists“ erneuert werden. Die beschränkte Lebensdauer von PKI-Zertifikaten erfordert ein komplexes Identity Management, um immer wieder neue Zertifikate von einer zentralen oder auch lokalen Zertifizierungsstelle anzufordern (z. B. DNS-based Authentication of Named Entities) und an die einzelnen Kommunikationspartner bzw. Komponenten zu verteilen.

Das Ergebnispapier „Technischer Überblick über Sichere Identitäten“ der Plattform Industrie 4.0 erläutert die Anforderungen an sichere Identitäten in Industrie 4.0 und fasst die aktuellen Standards und Normen zum Management von Identitäten zusammen (Plattform Industrie 4.0 2016b):

- ISO/IEC 24760 ist für alle Systeme spezifiziert, die Identitätsinformationen verarbeiten. Der Standard definiert die wesentlichen Begriffe und Konzepte für das Management von Identitäten, auch partielle Identitäten.
- ISO/IEC 29115 umfasst ein Rahmenwerk zur Authentifizierung, das eine Definition von verschiedenen Zuverlässigkeitsstufen, Authentifizierung, Bedrohungen und Gegenmaßnahmen beinhaltet.
- ISO/IEC 29191 gewährleistet Authentifizierung auch unter erhöhten Datenschutzanforderungen.

Konkrete rechtlich anerkannte Mindeststandards und Gütesiegel für IT-Sicherheit, die zur Zertifizierung von unternehmensübergreifenden Kommunikationsschnittstellen genutzt werden könnten, befinden sich momentan aber noch in der Diskussion. Dabei geht es insbesondere um die organisatorischen Prozesse zur Verteilung von kryptografischen Schlüssel sowie deren zuverlässiges Management und Aufbewahrung, um der hohen Dynamik in den zukünftigen Industrie-4.0-Wertschöpfungsnetzen gerecht zu werden.

4.8 Kommunikation: OPC Unified Architecture

Einen zentralen Baustein für die Realisierung von Softwarearchitekturen für Industrie 4.0 stellt die OPC Unified Architecture (OPC: Object Linking and Embedding for Process Control) dar, die als technologischer Ansatz zur Realisierung von Communication Layer im Rahmen von RAMI 4.0 empfohlen wird. OPC Unified Architecture (OPC UA) wird vom internationalen Industriekonsortium OPC Foundation bearbeitet, dessen Mitglieder überwiegend aus der Automatisierungstechnik kommen.

OPC UA ist eine plattformunabhängige Service-Orientierte-Architektur (SOA), die verschiedene Aspekte wie z. B. Discovery-Funktionen für die Suche nach verteilten OPC-Servern im Kommunikationsnetzwerk, Subscription für das Monitoring der Daten und Benachrichtigungen über Änderung von der Client-Seite, Bereitstellung von Methoden und Funktionen vom OPC UA Server als Basisfunktionalitäten spezifiziert und bereitstellt. Weitere anwendungsspezifische Dienste (Services) könnten flexibel über eine wohldefinierte SOA-Schnittstelle in die Gesamtarchitektur integriert werden.

OPC UA bietet über die SOA-Basisfunktionen hinaus auch eine Reihe von Security-Funktionalitäten. So sind die Vertraulichkeit und Integrität der Daten bei der Übertragung (Transport), Verschlüsselung (Session Encryption, Message Signing), Authentizierung auf der Basis von Public-Key-Infrastruktur – Zertifikaten (OpenSSL), Nutzerverwaltung und Zugriffkontrolle im OPC UA Standard bereits enthalten.

Eine Studie zur Analyse von Sicherheitsfunktionen in OPC UA im Auftrag vom BSI hat bestätigt, dass die Spezifikation von OPC UA keine systematischen Sicherheitslücken enthält. Für die Analyse wurde eine bestimmte Referenzimplementierung der OPC Foundation ausgewählt.
Die Ergebnisse der Analyse ergaben Schwachstellen in der Referenzimplementierung, die bei ausgeschalteten Sicherheitsfunktionen ausgenutzt werden können. Diese Schwachstellen sollte von der OPC Foundation mit dem nächsten Update der untersuchten Referenzimplementierung behoben werden (BSI 2016).

4.9 Entwicklungsprozess für sichere Software: Secure Development Lifecycle

Security-by-design ist inzwischen ein häufig verwendeter Begriff bei der Entwicklung von Informationssystemen: Die IT-Sicherheit muss in allen Phasen der Softwareentwicklung betrachtet werden und sollte nicht als Eigenschaft verstanden werden, die nachträglich zu einer fertigen Software ergänzt werden kann. Sowohl die Plattform Industrie 4.0 als auch das IIC und das BSI empfehlen „Security-by-Design“ als geeignete Herangehensweise bei der Entwicklung von IT-basierten Produktionssystemen. Als erster Vorschlag für die Organisation und Umsetzung eines „Security-by-Design“-Prozesses wird sowohl von IIRA als auch von der AG 3 „Sicherheit vernetzter Systeme“ der Plattform Industrie 4.0 der „Secure Development Lifecycle“ (SDL) von Microsoft empfohlen.

Der Secure Development Lyfecycle (SDL) erweitert die klassischen Softwareentwicklungsphasen (Anforderungsanalyse, Entwurf, Implementierung und Test) um weitere Phasen, in denen sicherheitsspezifische Methoden wie Aufstellung von Bedrohungsmodellen, Verwendung von Tools zur statischen Codeanalyse während der Implementierung sowie Durchführung von Codeüberprüfungen und Sicherheitsmängeln zur Anwendung kommen (Lipner, Howard 2015). Darüber hinaus wird eine zusätzliche Phase eingeführt, in der die Ergebnisse von einem externen, vom Entwicklungsteam unabhängigen Expertenteam (Final Security Review) überprüft wird. SDL beruht auf folgenden Grundsätzen:

Secure by Design: Die Software schützt die Informationen, die sie verarbeitet und hält den Angriffen stand.

Secure by Default: Im Standardzustand soll die maximale Sicherheit erreicht werden, z. B. durch die möglichst

niedrige Berechtigungen zum Ausführen der Software, Deaktivierung von Diensten und Features, die im Standardzustand nicht erforderlich sind.

Secure in Deployment: Dokumentation und Gebrauchsanweisungen sollen die sichere Ausführung der Software unterstützen. Die Aktualisierungen (updates) sollen einfach einzuspielen sein.

Communications: Die Softwareentwickler sollen bereit sein, mögliche und entdeckte IT-Sicherheitslücken schnell zu beheben.

Der SDL enthält zusätzliche organisatorische Maßnahmen wie die regelmäßigen Schulungen der Softwareentwickler, die in den Softwareunternehmen eingeführt werden sollen. Größere Unternehmen wie Microsoft sind in der Lage, eigene Teams mit der IT-Sicherheitsexpertise aufzubauen, um sie auf dem aktuellen Stand der neuen Cyber-Attacken oder Schwachstellen auf dem Laufenden zu halten. Kleinere Unternehmen sind dagegen auf externe Beratung angewiesen, um das nötige Know-how über die IT-Sicherheitslücken sowie erforderliche Maßnahmen wie z. B. Berücksichtigung der Schwachstellen wie Pufferüberläufe in Betriebssystemen oder Verwendung von aktualisierten Verschlüsselungsverfahren einzuholen. Auch die Unterstützung durch spezielle Tools, die die aufwendigen, sicherheitsspezifischen Softwaretests wie Fuzzingtools erleichtern, erfordert Kenntnisse des neuesten Stands der Technik wie z. B. neu entdeckte Schwachstellen in der Software der Betriebssysteme.

Die finalen unabhängigen Codeüberprüfungen und -tests (Final Software Review FSR) sollen laut SDL von einem unabhängigen Team durchgeführt werden, das in die Implementierung nicht involviert ist. Gerade für kleine Unternehmen bzw. industrienahen IT-Startups stellt FSR eine Herausforderung dar, den SDL vollständig in ihre Softwareherstellungsprozesse zu übernehmen.

Es ist aber denkbar, dass die neuen Wertschöpfungsnetze, die auf offene Dienstleistungsplattformen ähnlich den Open Innovation-Konzepten setzen, Möglichkeiten bieten, externe Experten für die finale Überprüfung von Softwarecodes einzubinden.

SDL adressiert allerdings nur Aspekte der IT-Sicherheit. Er berücksichtigt weder datenschutzrelevante Aspekte noch die funktionale Sicherheit von Industrie-4.0-Systemen. Ein umfassendes Vorgehensmodell für die Entwicklung sicherer Software für Industrie-4.0-Spezifika muss noch erarbeitet werden.

5 RAMI 4.0 und IIRA in der Praxis: die Sicht der AUTONOMIK-Projekte

Die Begleitforschung des Technologieprogramms „AUTONOMIK für Industrie 4.0“ und das AUTONOMIK-Projekt CoCoS haben am 04. Februar 2016 in Berlin den Workshop „Service-orientierte Architekturen für Industrie 4.0“ veranstaltet, in dem RAMI und IIRA aus Sicht der Projekte im Programm bewertet wurden. Die überwiegende Mehrheit der AUTONOMIK-Projekte – OPAK, CoCoS, MANUSERV, motionEAP, APPsist und InnoCyFer – haben RAMI 4.0 als Referenz zur Einordnung ihrer projektspezifischen Softwarearchitekturen gewählt. Die Projekte CoCoS und MANUSERV haben sich sowohl gegenüber RAMI 4.0 als auch IIRA 1.7 positioniert. Das Projekt GEMINI nahm ausschließlich Bezug zum Business Viewpoint von IIRA 1.7. Die Projekte kamen dabei zu folgenden Empfehlungen und Erkenntnissen (zur vollständigen Dokumentation des Workshops siehe Institut für Innovation + Technik 2016):

5.1 APPsist

Mobile Assistenzsysteme und Internetdienste in der intelligenten Produktion

Projektschwerpunkte: Im Projekt APPsist wird ein KI-basiertes Wissens- und Assistenzsystem entwickelt, das einen Mitarbeiter bei den Tätigkeiten wie Inbetriebnahme, Betrieb, Wartung, Reparatur und vorbeugende Instandhaltung von Anlagen unterstützt. Das Assistenzsystem APPsist setzt dabei auf der Expertise des Mitarbeiters auf, um den Mitarbeiter gezielt bei komplexen bzw. neuen Aufgaben anzuleiten. Die Entwicklung der Wissens- und Assistenzdienste erfordert sowohl ein technisches als auch personales und organisationales Wissen, damit eine adäquate Unterstützung des Mitarbeiters auch unter der Berücksichtigung der arbeitsrechtlichen Aspekte möglich wird.

www.appsist.de

Bewertung: Die Systemarchitektur von APPsist ließ sich im Wesentlichen in RAMI gut einordnen. Allerdings werden im Rahmen von APPsist auch Dienste umgesetzt, die eine Life-Cycle-übergreifende Kommunikation erfordern und sich nicht eindeutig einer bestimmten Phase zuordnen lassen.
Bei der Umsetzung von Security-by-Design Prinzipien in RAMI sollten auch die datenschutzrelevanten Aspekte, wie z. B. das Management und der Zugriff auf personenbezogene Daten berücksichtigt werden.
Die Beschreibung von RAMI 4.0 ist zwar kompakt, aber sehr abstrakt und daher schwer anwendbar. Es sollte ein eingängiges Beispiel angeboten werden, das alle Dimensionen und Ebenen nachvollzierbar und transparent erklärt. Durch die dreidimensionale Darstellung werden bestimmte Teile der projektspezifischen Architektur überdeckt. In APPsist hat sich eine zweidimensionale Darstellung bewährt, in der der RAMI-4.0-Würfel auf mehrere Grafiken aufgeteilt ist.

5.2 CoCoS

Context-Aware Connectivity and Service Infrastructure for Cyber-Physical Production Systems

Projektschwerpunkte: Im Projekt CoCoS wird eine Informations- und Kommunikationsplattform entwickelt, die Maschinen, Transportmittel und Werkstücke in einer Produktionslinie vereint. Durch die durchgängige Vernetzung der CPPS-Komponenten sowie die Vereinheitlichung der Kommunikationstechnologien werden nun alle produktionstechnischen Prozesse mit den betriebswirtschaftlichen Prozessen verzahnt und lassen sich dadurch flexibel steuern und verändern.
CoCoS realisiert keine hierarchische, sondern eine kooperative Netzwerkarchitektur, die es ermöglicht, die Ressourcen durch neuartige Self-X-Fähigkeiten (Selbstheilung, Selbstkonfiguration, Anomaliedetektion und Virtualisierung) optimal zu nutzen.

www.cocos-project.de

Bewertung: RAMI 4.0 eignet sich gut für die Strukturierung der Themen und Kommunikationseigenschaften, die

in CoCoS adressiert werden.
RAMI 4.0 ist mit seinem Ebenenmodell gegenüber IIRA in der Darstellung sehr viel kompakter. IIRA definiert dagegen verschiedene Viewpoints mit unterschiedlichen Detaillierungstiefen.
Für die CoCoS-Kommunikationsplattform hat IIRA 1.7 eine höhere Relevanz, insbesondere weil die „Key System Concerns" der IIRA wie Safety, Security und Connectivity die Schwerpunkte in CoCoS direkt widerspiegeln.
Der Detailierungsgrad der Beschreibung der „Key System Concerns" sollte in IIRA allerdings vereinheitlicht werden.
Die Beschreibung und Anforderungen an Resilienz sollten in IIRA noch konkretisiert werden.
In RAMI sollten die Systemaspekte zur Resilienz an einer Stelle gebündelt dargestellt werden.

5.3 GEMINI

Geschäftsmodelle für Industrie 4.0

Projektschwerpunkte: Ziel des Projektes GEMINI ist die Entwicklung und Bereitstellung von Methoden und Instrumenten zur Entwicklung und Operationalisierung von Geschäftsmodellen in den neuen Wertschöpfungsstrukturen des Bereichs Industrie 4.0. Es werden spezifische Geschäftsmodellmuster, Technologien und Risiken ermittelt und aufbereitet sowie über einen IT-basierten Geschäftsmodell-Konfigurator zur Entwicklung von Geschäftsmodellen verfügbar gemacht. Ein Operationalisierungsplaner unterstützt im Anschluss die Integration des entwickelten Modells in die unternehmerische Wertschöpfung.

www.geschaeftsmodelle-i40.de

Bewertung: Die GEMINI-Methodik stellt eine Grundlage für die im Business Viewpoint anstehenden Überlegungen dar, die wiederum den Ausgangspunkt für die Modellierung von funktionalen Architekturkomponenten darstellen.

5.4 InnoCyFer

Integrierte Gestaltung und Herstellung kundeninnovierter Produkte in Cyber-Physischen Fertigungssystemen.

Projektschwerpunkte: Die Realisierung individueller Gestaltungswünsche der Verbraucher wird zu einer zunehmenden Anforderung für das produzierende Gewerbe. Immer mehr Kunden verlangen einen stärkeren Individualisierungsgrad. Sie wollen direkten Einfluss auf die Gestalt und Funktion des Produktes nehmen. Dafür werden neue Infrastrukturen und hochflexible Fertigungsanlagen benötigt, die es erlauben, die Ideen des Kunden kurzfristig umzusetzen und Änderungen bis in die späten Phasen des Produktentstehungsprozesses zu ermöglichen. Am Beispiel eines individuellen Kaffeevollautomaten wird im Projekt InnoCyFer der Weg von standardisierten hin zu kundenindividuellen Produkten demonstriert.

www.innocyfer.de

Bewertung: Das Projekt InnoCyFer hat genauso wie APPsist den dreidimensionalen RAMI-4.0-Würfel in mehrere zweidimensionale Ansichten aufgeteilt und so die Einordnung der projektspezifischen Architektur in die RAMI-4.0-Schichten vorgenommen.
Bei der Auswahl von Standards und Technologien wären konkrete Beispiele, die auf spezifischen Ebenen von RAMI 4.0 angesiedelt sind, sehr hilfreich.

5.5 MANUSERV

Vom Manuellen Prozess zum industriellen Serviceroboter

Projektschwerpunkte: Im Projekt MANUSERV wird ein System zur Planungs- und Entscheidungsunterstützung entwickelt, das potenziellen Anwendern von industrieller Servicerobotik eine vereinfachte Analyse und Bewertung ihrer Prozesse hinsichtlich möglicher (Teil-) Automatisierungslösungen ermöglicht. Dabei geht es sowohl um die technologische Realisierbarkeit als auch um die

ökonomische Sinnhaftigkeit für die Gestaltung eines hybriden Mensch-Roboter-Arbeitsplatzes.

www.manuserv.de

Bewertung: Die Gestaltung eines hybriden Mensch-Roboter-Arbeitsplatzes lässt sich in RAMI 4.0 angemessen darstellen.
Die Funktionsschicht ist in MANUSERV viel umfangreicher ausgestaltet als die restlichen Schichten von RAMI 4.0. Eine Untergliederung der Funktionsschicht in RAMI 4.0 wäre an dieser Stelle sinnvoll.
In der MANUSERV-Softwarearchitektur wurden bereits Security-by-Design- und Resilienz-Prinzipien berücksichtigt. Beides wird in IIRA 1.7 angemessen berücksichtigt. Sowohl RAMI 4.0 als auch IIRA 1.7 leisten eine sinnvolle Orientierungshilfe in der momentan heterogenen Landschaft der Industrie-4.0-Komponenten.

5.6 motionEAP

Assistenzsystem für die Montage mit Echtzeit-Feedback

Projektschwerpunkte: Im Projekt motionEAP wurde ein neuartiges prozessorientiertes Assistenzsystem für Montageprozesse in der Produktion konzipiert. Das Assistenzsystem gibt dem Mitarbeiter schon während des Arbeitsvorgangs eine Rückmeldung, ob die Arbeitsschritte richtig ausgeführt werden. Ebenso weist es auf ergonomisch ungünstige Bewegungen und Haltungen hin. Die Hinweise werden dem Mitarbeiter über eine Projektion direkt im Arbeitsbereich angezeigt, sei es auf dem Werkstück, dem Arbeitstisch oder der Arbeitsvorrichtung. Ein besonderes Augenmerk legen die Projektpartner auf die Anforderungen älterer und leistungsgeminderter Montagearbeiter, für die ein solches Assistenzsystem besonders nützlich sein kann.

www.motioneap.de

Bewertung: RAMI 4.0 eignet sich gut als Kommunikationswerkzeug („common ground“) für die interessensübergreifende Verständigung zwischen verschiedenen Geschäftsbereichen oder auch firmeninternen Gewerken. Der RAMI 4.0-Würfel kann gut als Klassifizierungstool z. B. zur Funktionsbeschreibung eines Projektprodukts von Projektpartnern, aber auch Endanwendern oder auch zum Vergleich mit den alternativen Lösungen genutzt werden. Referenzarchitekturmodelle leisten eine Hilfestellung im initialen Projektzustand. Weiterhin werden aber die Softwarearchitekturen an die projektspezifischen Anforderungen angepasst. Durch die Anpassungen besteht jedoch die Gefahr, dass der Anschluss an die Referenzarchitekturmodelle verloren geht.

5.7 OPAK

Offene Engineeringplattform für autonome, mechatronische Automatisierungskomponenten in funktionsorientierter Architektur

Projektschwerpunkte: Zunehmend werden einzelne mechatronische Komponenten in der Produktion mit immer mehr Sensorik und Motorik ausgestattet und erhalten dadurch eine eigene Intelligenz, müssen aber über eine zentrale Steuerung mit anderen Komponenten kommunizieren. In OPAK wird eine architekturgestützte und funktionsorientierte Engineeringmethodik entwickelt, die eine nahtlose Integration der Steuerungsarchitektur, der funktionalen Architektur und der mechatronischen Architektur beim Design und der Entwicklung von Produktionsanlagen ermöglicht.

www.opak-projekt.de

Bewertung: Die OPAK-Architektur ließ sich problemlos in RAMI 4.0, insbesondere hinsichtlich Life Cycle & Value Stream, in die Bereiche „Development“ und „Maintainace/Usage“ einordnen.
RAMI 4.0 soll für die praktische Anwendung in Tools für Engineering und im Betrieb der Produktionsanlagen für

spezifische Domänen konkretisiert werden. Zielführend wären daher domänenspezifische Ausprägungen von RAMI 4.0.
Die Hierarchieebenen in RAMI sind sehr stark an die klassische Automatisierungspyramide angelehnt. Anpassungen sind notwendig, um zukünftige, stärker verteilte und weniger hierarchische, Systeme in RAMI abbilden zu können.
Das OPAK-Konsortium begrüßt ausdrücklich die Standardisierungsbemühungen der Plattform Industrie 4.0 für Architektur und die Beschreibung der Automatisierungskomponenten.

5.8 Fazit

Beide Referenzarchitekturen verfolgen ein gemeinsames Ziel: die Schaffung eines einheitlichen Ordnungsschemas mit einer wohldefinierten Terminologie, das eine Grundlage für ein gemeinsames Verständnis zwischen verschiedenen Stakeholdern bei der Entwicklung von komplexen Technologien bietet.

Ein wichtiger Wunsch der AUTONOMIK-Projekte waren eingängige Beispiele für verschiedene Domänen, die die Anwendbarkeit und Nutzerfreundlichkeit beider Referenzarchitekturen enorm steigern würden. Die Aspekte Security-by-Design und Resilience-by-Design werden momentan in RAMI 4.0 nicht berücksichtigt. Beides sollte in der nächsten Version von RAMI 4.0 unbedingt behandelt werden, um Softwarearchitekten und IT-Sicherheitsexperten eine gemeinsame Verständigungsbasis zu geben.

IIRA 1.7 sollte einerseits in der Beschreibung der einzelnen Key Concerns vereinheitlicht werden, andererseits sollte der inhaltliche Rahmen kompakter gehalten werden. RAMI 4.0 schneidet gegenüber IIRA 1.7 hinsichtlich der Klarheit, Transparenz und Kompaktheit der gewählten Struktur deutlich besser ab. Diese klare und transparente Struktur von RAMI 4.0 war bei mehreren Projekten entscheidend bei der Wahl des Referenzarchitekturmodells. Allerdings kann der hohe Grad an Abstraktion hinderlich bei der Einordnung in die jeweiligen Schichten sein, weil konkrete Beispiele und Hinweise zu Technologien fehlen. Der RAMI-4.0-Würfel erlaubt eine eingängige und kompakte Darstellung. Allerdings ist die Einordnung in die einzelnen Ebenen des 3D-Würfels durch gegenseitige Verdeckung oft schwierig. 2D-Visualisierungen wurden von den Projekten sehr begrüßt und in Eigeninitiative bereits für die Darstellung der eigenen Architekturkomponenten verwendet.

Insgesamt waren sich alle Projekte darüber einig, dass eine interaktive, web-basierte Umgebung die Weiterentwicklung der Referenzarchitekturen fördern würde. Eine solche interaktive Umgebung, z. B. im Rahmen der Plattform Industrie 4.0, würde eine Möglichkeit bieten, sich mit ähnlich aufgestellten Projekten zu vernetzen, eine gemeinsame Strukturierung der technologischen Lösungen durch die Einordnung in RAMI 4.0 (bzw. IIRA 1.7) vorzunehmen und voneinander in der Entwicklung und Wiederverwendung von Technologien und bereits bestehenden Konzepten oder auch Geschäftsmodellen zu profitieren.

6 Literaturverzeichnis

Bitkom, DIN (2014) (Hg.): Kompass der IT-Sicherheitsstandards. Auszüge zum Thema Elektronische Identitäten, Berlin 2014 (www.bitkom.org/Bitkom/Publikationen/Kompass-der-IT-Sicherheitsstandards.html)

BSI (2016) (Hg.): Sicherheitsanalyse OPC UA, Bonn (www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2016/Sicherheitsanalyse_OPC_UA_26042016.html)

BSI (2013) (Hg.): ICS-Security-Kompendium, Bonn 2013 (www.bsi.bund.de/DE/Themen/Industrie_KRITIS/Empfehlungen/ICS/empfehlungen_node.html)

BSI (2008) (Hg.): BSI-Standard 100-1, Managementsysteme für Informationssicherheit (ISMS). Version 1.5, Bonn

BMWi (2016) (Hg.): IT-Sicherheit für die Industrie 4.0. Produktion, Produkte, Dienste von morgen im Zeichen globalisierter Wertschöpfungsketten, Berlin (www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/Studien/it-sicherheit-fuer-industrie-4-0-langfassung,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf)

CEN-CENELEC-ETSI Smart Grid Coordination Group (2012): Smart Grid Reference Architecture, November 2012 (www.cencenelec.eu/standards/Sectors/SustainableEnergy/SmartGrids/Pages/default.aspx)

iit (2016): Softwarearchitekturen für Industrie 4.0. RAMI und IIRA aus Sicht der Projekte im Technologieprogramm AUTONOMIK für Industrie 4.0, Berlin

IIC (2015): Industrial Internet Reference Architecture, Version 1.7 (www.iiconsortium.org/IIRA-1-7-ajs.pdf)

Plattform Industrie 4.0 (2016a) (Hg.): Leitfaden Security in RAMI 4.0, Berlin 2016 (www.plattform-i40.de/I40/Redaktion/DE/Downloads/Publikation/security-rami40.html)

Plattform Industrie 4.0 (2016b) (Hg.): Technischer Überblick: Sichere Identitäten, Berlin 2016 (www.plattform-i40.de/I40/Redaktion/DE/Downloads/Publikation/sichere-identitaeten.html)

Lipner, Steve; Howard, Michael (2015): Entwicklungszyklus für sichere Software, Microsoft Developer Network, 30.5.2015 (https://msdn.microsoft.com/de-de/library/ms995349.aspx)

TeleTrust (2016) (Hg.): Handreichung zum „Stand der Technik“ im Sinne des IT-Sicherheitsgesetzes (ITSiG), Berlin 2016 (www.teletrust.de/fileadmin/docs/fachgruppen/ag-stand-der-technik/TeleTrusT-Handreichung_Stand_der_Technik.pdf)

VDI/VDE-GEMA, ZVEI (2015) (Hg.): Statusreport. Referenzarchitekturmodell Industrie 4.0 (RAMI4.0), Düsseldorf/Frankfurt am Main (www.vdi.de/fileadmin/vdi_de/redakteur_dateien/gma_dateien/Statusreport_Referenzmodelle_2015_v10_WEB.pdf)

ZVEI (2012) Sicherheit von Maschinen. Erläuterungen zur Anwendung der Normen EN 62061 und EN ISO 13849-1, Edition II, Frankfurt am Main (www.zvei.org/Verband/Publikationen/Seiten/Sicherheit-von-Maschinen.aspx)

www.autonomik40.de