Olof Leps

Hybride Testumgebungen für Kritische Infrastrukturen

Effiziente Implementierung für IT-Sicherheitsanalysen von KRITIS-Betreibern

Springer Vieweg

Hybride Testumgebungen für Kritische Infrastrukturen

Olof Leps

Hybride Testumgebungen für Kritische Infrastrukturen

Effiziente Implementierung für IT-Sicherheitsanalysen von KRITIS-Betreibern

Springer Vieweg

Olof Leps
Berlin, Deutschland

ISBN 978-3-658-22613-8 ISBN 978-3-658-22614-5 (eBook)
https://doi.org/10.1007/978-3-658-22614-5

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Springer Vieweg

Springer Vieweg ist ein Imprint der eingetragenen Gesellschaft Springer Fachmedien Wiesbaden GmbH und ist ein Teil von Springer Nature
Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

Es gibt keine Sicherheit, nur verschiedene Grade der Unsicherheit.

Anton Pawlowitsch Tschechow

Vorwort

An dieser Stelle möchte ich allen danken, die mich bei der Erstellung dieser Ausarbeitung unterstützt haben. Mein besonderer Dank gilt dabei Herrn Dr. Christof Thim vom Lehrstuhl für Wirtschaftsinformatik, insb. Prozesse und Systeme der Universität Potsdam, der mir bei Fragen zur Seite stand, Problemlagen mit mir diskutierte und mich fachkundig unterstützte. Ebenso möchte ich mich bei den Herren Stephan Arndt und David Kotarski bedanken, die ihre Erfahrungen bei der Modellierung und Implementation von hybriden Simulationen für Testumgebungen mit mir teilten.

Berlin, Februar 2018 *Olof Leps*

Inhaltsverzeichnis

Abkürzungsverzeichnis

ASIC	Application-specific Integrated Circuit, dt.: anwendungsspezifische integrierte Schaltung
BDEW	Bundesverband der Energie- und Wasserwirtschaft e. V.
BIA	Business Impact Analyse, dt.: Schadensfolgeanalyse
BCM	Business Continuity Management, dt.: Geschäftskontinuitätsmanagement
BSI	Bundesamt für Sicherheit in der Informationstechnik
CIF	Control in the Field
CSN	Control Systems Network, dt.: Leitsystemnetzwerk
DCS	Distributed Control System, dt.: Verteiltes Steuersystem
DMZ	Demilitarized Zone, dt.: Demilitarisierte Zone
DVGW	Deutscher Verein des Gas- und Wasserfaches
DWA	Deutsche Vereinigung für Wasserwirtschaft, Abwasser und Abfall
ECN	Enterprise Control (Systems) Network, dt.: Unternehmensnetzwerk
FGPA	Field-programmable Gate Array
FDN	Field Device Network, dt.: Feldgerätenetzwerk
HCS	Hybrid Control System, dt.: Hybrides Steuerungssystem
(H)IDS	(Host-based) Intrusion Detection System
(H)IPS	(Host-based) Intrusion Prevention System
HMI	Human Machine Interface, dt.: Benutzerschnittstelle
ICS	Industrial Control Systems, dt.: industrielle Steuerungssysteme
IDS	Intrusion Detection System, dt.: Einbruchmeldesystem
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
IPS	Intrusion Prevention System, dt.: Einbruchspräventionssystem
ISA	International Society of Automation
ISO	International Standardization Organization, dt.: Internationale Organisation für Normung
IoT	Internet of Things

IT	Informationstechnik
ISMS	Information Security Management System, dt.: Managementsystem für Informationssicherheit
KMU	Kleine und mittelgroße Unternehmen
KRITIS	Kritische Infrastrukturen
MES	Manufacturing Execution System
MON	Manufacturing Operations Network, dt.: Netzwerk für Fertigungsabläufe
MTU	Master Terminal Unit
(N)IDS	(Network) Intrusion Detection System
(N)IPS	(Network) Intrusion Prevention System
NIST	National Institute of Standards and Technology
OT	Operational Technology, dt.: Betriebstechnik
PAT	Process Analytical Technology, dt.: Prozessanalytik
PCN	Process Control (Systems) Network, dt.: Produktionsleitnetzwerk
PDCA	Plan-Do-Check-Act-Zyklus
PLS	Prozessleitsystem
RTU	Remote Terminal Unit, dt.: Fernbedienungsterminal
SCADA	Supervisory Control and Data Acquisition, dt.: Überwachung, Steuerung und Datenerfassung
SIEM	Security Information Event Management-System
SPS	Speicherprogrammierbare Steuerung, engl.: Programmable Logic Controller (PLC)
TCAM	Ternary Content-Addressable Memory

Abbildungsverzeichnis

Tabellenverzeichnis

Management Summary

Automatisierung und Digitalisierung tragen zur Verbesserung der Dienstleistungen vieler Unternehmen bei. Die hierdurch entstehende Vernetztheit geht jedoch auch mit Risiken in der Informationssicherheit einher. Vor allem die Gefährdung von Kritischen Infrastrukturen weist eine für Wirtschaft und Gesellschaft besondere Kritikalität auf. Aufgrund der Kritikalität solcher Infrastrukturen werden für Sicherheitsanalysen nicht Echtanlagen, sondern Testumgebungen genutzt. Jedoch sind klassische Testumgebungen in Form von Modellfabriken entweder zu teuer und unflexibel oder in Form von Simulationen nicht ausreichend realitätsgetreu, um belastbare Sicherheitsanalysen durchzuführen.

Mit der Nutzung einer hybriden Simulation als Testumgebung (kurz: hybride Testumgebung) wird derzeit ein neuerer Ansatz erforscht, der mittels einer speziellen Architektur effiziente Sicherheitsanalysen Kritischer Infrastrukturen ermöglichen soll. Dieser Ansatz kombiniert die Vorteile der klassischen Testumgebungen, indem ein Großteil der Anlage kostengünstig computerbasiert implementiert wird, aber wichtige Anlagenbereiche mit Echtkomponenten physisch in die Testumgebung integriert werden, um eine hohe Realitätsnähe zu erreichen. Eine besondere Herausforderung in der Modellierung und Implementierung ist hierbei die Entscheidung, welche Komponenten in der hybriden Testumgebung am besten physisch integriert und welche eher simuliert, emuliert oder virtualisiert werden sollten.

Die vorliegende Ausarbeitung bietet eine Einführung in das Thema und liefert einen wichtigen Beitrag zur Entwicklung des Ansatzes der hybriden Testumgebung: Es wird ein grundlegendes Vorgehensmodell zur effizienten Modellierung und Implementation einer hybriden Testumgebung vorgeschlagen, das die Vorbereitung, die Konfiguration der Elemente der Testumgebung, die Konfiguration der Testumgebung sowie den eigentlichen Simulationsbetrieb umfasst. Darüber hinaus wird als Teil dieses Vorgehensmodells eine Klassifikation vorgestellt, diskutiert und beispielhaft angewendet, mithilfe derer die Entscheidungsfindung in der Simulationsartbestimmung einer Komponente als entweder physische oder computer-

basierte Komponente erleichtert werden soll. Das Vorgehensmodell und die Klassifikation zielt vorrangig auf kleine und mittelgroße leitungsgebundene KRITIS-Betreiber wie Wasserwerke ab. Konkret soll diese Methodik effiziente Sicherheitsanalysen per Penetrationstest in Form von Communication-Channel-Attacken über das Internet bzw. Netzwerk erleichtern. Darüber hinaus ist ein Einsatz bei der Implementierung von hybriden Testumgebungen auch für andere Anwendungsfälle und Kontexte denkbar. Eine Nutzung durch KMU wird insbesondere dadurch erleichtert, dass das hier beschriebene Vorgehen an die IT-Grundschutz-Methodik anknüpft und vielfach auf bekannte Methoden zurückgegreift.

Kapitel 1
Einleitung

Die zunehmende Automatisierung von Industrieprozessen führt zu einer gesteigerten Effektivität und Effizienz. Doch mit ihr gehen auch neue sicherheitstechnische Risiken einher, die eine Herausforderung für viele Betreiber von kritischen Infrastrukturen und Industrieanlagen darstellen können. Denn Automatisierung erhöht die Abhängigkeit von IT-Systemen wie auch die Anfälligkeit für Angriffe: „Die Netze, der Grad der Vernetztheit nehmen an Größe und Komplexität zu; es entstehen Knotenpunkte, die Angriffsflächen bieten und bei einer Beeinträchtigung nicht nur zu lokalen, sondern wegen der Vernetztheit zu überregionalen oder sogar grenzüberschreitenden Ausfällen führen können."[1] Diese Gefährdungen sind in den letzten Jahren auch einer breiteren Öffentlichkeit durch gezielte Angriffe auf Prozesssteuerungssysteme ins Bewusstsein gerufen worden. Doch obwohl die Verwundbarkeit von Systemen und Komponenten der Automatisierungstechnik seit geraumer Zeit beobachtet und diskutiert werden, zeigte eine Studie jüngst auf, dass es unter Umständen „kinderleicht" sei, im Internet auf ungeschützte oder nicht ausreichend geschützte ICS-/SCADA-Systeme unautorisiert zuzugreifen.[2] Während ein Angreifer nur eine einzige Lücke finden muss, ist die Absicherung eines Informationsverbundes sehr viel komplexer, denn möglichst jede Schwachstelle muss identifiziert werden.

Für besonders kritische Prozesse muss nach einschlägigen Standards der IT-Sicherheit eine vertiefte Sicherheitsanalyse durchgeführt werden, da sie aufgrund ihrer gesellschaftlichen oder betriebswirtschaftlichen Bedeutung einen erhöhten Schutzbedarf aufweisen. Das BSI empfiehlt, für solche Prozesse eine vollumfängliche Sicherheitsanalyse per Penetrationstest oder Schwachstellenanalyse durchzuführen.[3] Diese speziellen Sicherheitsanalysen werden bei kritischen Prozessen

1 Strauß (2015), S. 350.

2 Wilhoit (2013), S. 5-6.

3 BSI-Standard 200-3 (2016), S. 21-32; BSI-Standard 200-2 (2017), S. 124-125; Bundesamt für Sicherheit in der Informationstechnik (2016), M 5.150 Durchführung von Penetrationstests, S. 4669.

O. Leps, *Hybride Testumgebungen für Kritische Infrastrukturen*,
https://doi.org/10.1007/978-3-658-22614-5_1

klassischerweise in besonderen Testumgebungen durchgeführt, welche entweder computerbasiert oder mittels eines identischen physischen Modells der Anlage realisiert werden.[4] Analysen im Echtbetrieb kommen aufgrund der damit verbundenen Ausfallsrisiken nicht in Frage. Simulationen sind hierfür jedoch nur von begrenztem Nutzen, da sie das Originalsystem nicht ausreichend realitätsnah abbilden. Ein physisches Anlagenmodell wiederum ist in der Regel wenig flexibel, mit viel Aufwand und hohen Kosten verbunden, weshalb klassische Testumgebungen für viele Anwendungsfälle und Organisationen bisher nicht in Frage kamen.

Es besteht also ein Bedarf an aufwandsarmen, kostengünstigen und dennoch effektiven Testumgebungen, gerade bei kleinen und mittelgroßen KRITIS-Betreibern: Wie alle anderen Branchen erleben auch Daseinsversorger einen tiefgreifenden Wandel durch Informationstechnik, Digitalisierung und Automatisierung. Der Einsatz von IT hat auch für sie viele Vorteile. So trägt er zu einer Verbesserung der Wirtschaftlichkeit durch effizientere Prozesse bei. Gleichzeitig gehen damit jedoch auch neue Risiken einher.[5] Kritische Infrastrukturen der Daseinsvorsorge sind eine bedeutende Zielgruppe solcher Attacken.[6] Offenkundig ist die Gewährleistung der Sicherheit für viele KRITIS-Betreiber eine Herausforderung. Dies ist darauf zurückzuführen, dass insbesondere KRITIS-KMU oft nicht über die notwendigen finanziellen bzw. personellen Ressourcen oder gar nicht erst über das ausreichende Fachwissen bzw. Problembewusstsein verfügen.[7]

An der Universität Potsdam wird im Rahmen des Projekts Aqua-IT-Lab im Labor des „Anwendungszentrums Industrie 4.0“ eine hybride Simulation als Testumgebung für cyber-physische Sicherheitsanalysen erforscht und in die Praxis umgesetzt.[8] Die hybride Testumgebung kombiniert die Vorteile der klassischen Ansätze, indem ein Großteil der Anlage simuliert wird, aber wichtige Anlagenbereiche mit Echtkomponenten physisch in die Testumgebung integriert werden.[9] Dieser Ansatz ist für KRITIS-Betreiber deshalb interessant, weil hybride Testumgebungen

---

4 National Institute of Standards and Technology (2015), G-24-G-25; Lass und Gronau (2012), S. 2.

5 Strauß (2015), S. 350; vgl. Ver.di (2015), S. 36; Bundesverband der Energie- und Wasserwirtschaft u. a. (2015), S. 51; Bundesamt für Sicherheit in der Informationstechnik (2015), S. 106.

6 Schumacher (2016), S. 676; Association (2014), S. 1; McNabb (2010), S. 24.

7 Bundesamt für Sicherheit in der Informationstechnik (2015), S. 106-108; Detken, Eren und Steiner (2012), S. 1; Brauer und Sturm (2014), S. 15-16; Hulsmann und Smeets (2011), S. 2; EurEau (2011), zitiert nach Castell-Exner (2013), S. 7; Gronau u. a. (2012), S. 2.

8 Lass und Kotarski (2014), S. 398. In dieser Publikation wird im Folgenden der Einfachheit halber meist der Begriff „hybride Testumgebung“ genutzt, um eine Testumgebung zu beschreiben, die mittels einer hybriden Simulation implementiert wurde.

9 Vgl. Lass und Theuer (2011), S. 14; Lass und Gronau (2012), S. 2.

vergleichsweise aufwandsarm und kostengünstig sind und cyber-physische Sicherheitsanalysen mit hoher Realitätsnähe ermöglichen.

Die vorliegende Ausarbeitung bietet eine Einführung und Vorgehensbeschreibung zur Implementierung von hybriden Testumgebungen für IT-Sicherheitsanalysen, mit Schwerpunkt auf die Modellierung und Komponentenauswahl der abzubildenden Anlage. Die Realisierung hybrider Testumgebung unterscheidet sich von anderen Ansätzen. So stellt etwa die Entscheidung, welche Komponenten in der hybriden Testumgebung am besten physisch integriert und welche eher simuliert oder virtualisiert werden sollten, eine besondere Herausforderung in der Modellierung und Implementierung dar. Die Methodik, die in dieser Ausarbeitung vorgeschlagen und diskutiert wird, umfasst einerseits ein Vorgehensmodell, dass die Vorbereitung, die Konfiguration der Elemente der Testumgebung, die Konfiguration der Testumgebung sowie den eigentlichen Simulationsbetrieb beschreibt. Andererseits wird am Beispiel einer kleinen und einer mittelgroßen Anlage der Wasserversorgung eine Klassifikation entwickelt und diskutiert, mithilfe derer die Entscheidungsfindung in der Simulationsartbestimmung einer Komponente als entweder physische oder computerbasierte Komponente erleichtert werden soll. Die Klassifikation ist in das Vorgehensmodell eingebettet, das einen Rahmen bietet und notwendige Vorarbeiten leisten soll. Hierzu gehören etwa in der Vorbereitungsphase die Erfassung und Abgrenzung des Informationsverbunds und der Elemente bzw. Komponenten im Betrachtungsbereich, aber auch Aspekte der Validierung und Verifizierung der Testumgebung.

Insgesamt ist es das Ziel dieser Ausarbeitung, Methoden für Sicherheitsexperten sowie für IT-Verantwortliche bereitzustellen, um die Modellierung und Implementation von hybriden Testumgebungen zu vereinfachen. Die Methodik wird dabei Praxisnah am Beispiel von Industrieanlagen der Wasserversorgung erläutert und zielt vor allem auf kleine und mittlere leitungsgebundene KRITIS-Betreiber ab, die auf diese Weise eine effektive, kostengünstige und aufwandsarme Sicherheitsanalyse durchführen können. Sie soll vorrangig für den Anwendungsfall einer cyber-physischen Sicherheitsanalyse zum Einsatz kommen, mit der Industrieanlagen per Penetrationstest in Form von Control-Channel-Attacken über das Internet bzw. Netzwerk überprüft werden können. Darüber hinaus ist ein Einsatz bei der Implementierung von hybriden Testumgebungen auch für andere Anwendungsfälle denkbar, ggf. mit spezifischen Anpassungen. Eine entsprechende Eignung wird daher kursorisch mitbetrachtet. Hingegen ist der Einsatz aufgrund der stark computerbasierten und simulativen Elemente beispielsweise für jene Analysen nicht ideal, die stark auf physischen bzw. personellen Aspekte basieren. Beispielhaft können hier Social-Engineering-Attacken oder Side-Channel-Attacken über physischen Zugang zur Sensorik genannt werden.

In der Herleitung dieser Methodik wird nach einer kurzen Einführung in das Thema zunächst der Aufbau von Industrieanlagen erläutert, wobei insbesondere auf architektonische Besonderheiten von ICS-Anlagen eingegangen wird und somit wichtige Grundlagen für die Methodik gelegt werden (Kapitel 3). Auch wird in diesem Zusammenhang mit einer Kurzbetrachtung des IT-Grundschutzes an einen bestehenden Standard angeknüpft, der beispielhaft wesentliche Informationen und Vorarbeiten für die Implementierung der hybriden Testumgebung liefern kann (Kapitel 4). Zudem wird an dieser Stelle ein Überblick über klassische Testumgebungen zur Durchführung von ICS-Sicherheitsanalysen geliefert und ihre Vor- und Nachteile beleuchtet, um daraufhin die hybride Testumgebung eingehend zu beschreiben. Auch wird vertieft auf den Forschungsstand und die unterschiedlichen Architekturen und Realisierungsmöglichkeiten von hybriden Testumgebungen eingegangen, bevor Methoden zur Modellierung und Implementierung von hybriden Testumgebungen beschrieben werden (Kapitel 5).

Literaturverzeichnis

Association, A. W. W. (2014), *Process Control System Security Guidance for the Water Sector*, American Water Works Association.

Brauer, F. und S. Sturm (2014), *European Strategic Workshop on Water Safety Planning, 12–13 March 2014, Berlin, Germany – Key Outcomes*, Umweltbundesamt.

BSI-Standard 200-2 (2017), *IT-Grundschutz-Methodik – Community Draft*.

BSI-Standard 200-3 (2016), *Risikoanalyse auf der Basis von IT-Grundschutz – Community Draft*.

Bundesamt für Sicherheit in der Informationstechnik (2015), *KRITIS-Sektorstudie: Ernährung und Wasser*, Bundesamt für Sicherheit in der Informationstechnik.

Bundesamt für Sicherheit in der Informationstechnik (2016), *IT-Grundschutz-Kataloge: 15. Ergänzungslieferung*.

Bundesverband der Energie- und Wasserwirtschaft u. a. (2015), *Branchenbild der deutschen Wasserwirtschaft 2015*, wvgw Wirtschafts- und Verlagsgesellschaft.

Castell-Exner, C. (2013), *Sicherheit in der Trinkwasserversorgung: Risikomanagement im Normalbetrieb – nationale und europäische Ansätze für kleinere Wasserversorger, IWW-Kolloquium "Technisches Risikomanagement – Neue Ansätze für kleine und große WVU", Mülheim*, Präsentation, URL: https://www.dvgw.de/index.php?eID=dumpFile&t=f&f=751&token=595a3d69ad95c090acfb07c49b86673644bbaa69 (besucht am: 20. 12. 2017).

Detken, K.-O., E. Eren und M. Steiner (2012), Erhöhung der IT-Sicherheit durch Konfigurationsunterstützung bei der Virtualisierung, DACH Security, in: P. Schartner und J. Taeger (Hrsg.), *DACH Security 2012: Bestandsaufnahme – Konzepte – Anwendungen – Perspektiven*, Prof. Dr. Patrick Horster.

EurEau (2011), *EurEau Position Paper on the EU Guidance on Developing Water Safety Plans for Small Supplies*, EurEau – European federation of national associations of drinking water suppliers und waste water services.

Gronau, N. u. a. (2012), *Organisation des Schutzes der kritischen Infrastruktur Wasserversorgung: Grundlagen und praktische Anwendung für Betreiber*, GITO mbH Verlag.

Hulsmann, A. und P. Smeets (2011), *Towards a Guidance Document for the implementation of a Risk Assessment for small water supplies in the European Union*, KWR Watercycle Research Institute.

Lass, S. und N. Gronau (2012), Efficient Analysis of Production Processes with a Hybrid Simulation Environment, in: H. Nylund u. a. (Hrsg.), *Proceedings of the FAIM 2012: 22nd International Conference on Flexible Automation and Intelligent Manufacturing, June 10th-13th, 2012, Helsinki, Finland*, Tampere University of Technology.

Lass, S. und D. Kotarski (2014), IT-Sicherheit als besondere Herausforderung von Industrie 4.0, in: W. Kersten, H. Koller und H. Lödding (Hrsg.), *Schriftenreihe der Hochschulgruppe für Arbeits- und Betriebsorganisation e.V. (HAB): Industrie 4.0 – Wie intelligente Vernetzung und kognitive Systeme unsere Arbeit verändern Schriftenreihe der Hochschulgruppe für Arbeits- und Betriebsorganisation*, Gito Verlag Berlin, 397–419.

Lass, S. und H. Theuer (2011), Hybride Simulation – Den besten Grad an dezentraler Produktionssteuerung bestimmen, in: *Productivity Management*, 13–16.

McNabb, J. (2010), *Cyberterrorism & the Security of the National Drinking Water Infrastructure*, Presentation at the DEF CON 18, July 31, 2010.

National Institute of Standards and Technology (2015), *NIST Special Publication 800-82, Revision 2: Guide to industrial control systems (ICS) security – supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as programmable logic controllers (PLC)*.

Schumacher, S. (2016), IT-Sicherheit in der Wasserversorgung: Schutz kritischer Infrastrukturen, in: *Magdeburger Journal zur Sicherheitsforschung*, 11, 667–685.

Strauß, J. (2015), Infrastruktursicherheit, in: T. Jäger (Hrsg.), *Handbuch Sicherheitsgefahren*, SpringerVS.

Ver.di (2015), *Wasserwirtschaft in Deutschland: Branchenanalyse – Trend und Herausforderungen*, Ver.di.

Wilhoit, K. (2013), *Wer steckt tatsächlich hinter den Angriffen auf ICS-Ausrüstung?*, Trend Micro.

Kapitel 2
Informationssicherheit von KRITIS-Betreibern: Eine Übersicht

In diesem Kapitel wird ein Überblick und eine Einführung zur Informationssicherheit von Industrieanlagen im Allgemeinen sowie zur Sicherheitslage von kleinen und mittleren KRITIS-Betreibern im Speziellen gegeben. Relevante Grundlagen und Begriffe zur Informationssicherheit von Industrieanlagen und KRITIS-KMU werden erörtert.

2.1 Informationssicherheit in der Betriebs- und Steuerungstechnik: Begrifflichkeiten und Definitionen

Der Begriff der IT-Sicherheit ist in der Literatur bisher der am meisten genutzte und „beschäftigt sich an erster Stelle mit dem Schutz elektronisch gespeicherter Informationen und deren Verarbeitung". Er lässt dabei semantisch jedoch Aspekte außen vor, die über die Datenverarbeitung hinausgehen, wie beispielsweise menschliche oder organisationale Aspekte.[1] Neben diesem Begriff werden auch weitere Begriffe wie Informationssicherheit, Datensicherheit oder Infrastruktursicherheit in ähnlicher Weise nebeneinander oder synonym genutzt. In dieser Ausarbeitung wird – in Anlehnung an das Begriffsverständnis des BSI – vorrangig der Begriff der Informationssicherheit genutzt, da er umfassender ist und menschliche oder organisationale Faktoren sprachlich miteinbezieht.[2] Der Begriff der Infrastruktursicherheit ist hingegen vergleichsweise ungenau, da er mit Blick auf infrastrukturelle Aspekte der technischen Versorgungssicherheit schwer abzugrenzen ist (also etwa die Frage, ob die Leitungskapazität für eine Anlage ausreichend ist).

1 BSI-Standard 100-1 (2008), S. 12.

2 Vgl. Sowa (2017), S. 8-12; Bundesamt für Sicherheit in der Informationstechnik (2015), S. 98. Dennoch werden sowohl die Begriffe IT-Sicherheit und Informationssicherheit als auch die Begriffe IT-Sicherheitsmanagement und Informationssicherheitsmanagement aufgrund ihrer weiten Verbreitung genutzt.

O. Leps, *Hybride Testumgebungen für Kritische Infrastrukturen*,
https://doi.org/10.1007/978-3-658-22614-5_2

Der Begriff wird auch mit Blick auf die Sicherheit der Anlagen- und Betriebstechnik selten genutzt.[3]

Informationssicherheit im Bereich der (Office-)IT befasst sich vorrangig mit dem Schutz der drei Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit von Informationen. Je nach Anwendungsfall werden auch weitere Werte wie Authentizität, Verbindlichkeit, Zuverlässigkeit und Nichtabstreitbarkeit dazugerechnet.[4] Informationssicherheit kann aber auch – wie im Fall der Kritischen Infrastruktur (auch: KRITIS) der Wasserversorgung – den Schutz technischer Anlagen beinhalten. Hier spielt neben dem Schutz insbesondere des Grundwerts der Verfügbarkeit vor allem auch das Ziel der funktionalen Sicherheit (Safety) eine wichtige Rolle.[5] Das BSI greift im Bereich der Industrietechnik teilweise – je nach branchenüblichem Usus – auf englischsprachige Begriffe zurück, welche in der internationalen Normung definiert wurden, weswegen diese Begriffe auch in der vorliegenden Arbeit vorrangig genutzt werden.[6]

In der IT-Grundschutz-Methodik wird in Bezug auf Anlagensicherheit der Überbegriff der Operation Technology (OT, dt.: Betriebstechnik) verwendet. Dieser umfasst „Hard- und Software, die Änderung durch die direkte Überwachung und / oder Steuerung von physikalischen Geräten, Prozessen und Ereignissen im Unternehmen erfasst und bewirkt."[7] Er deckt bis zur Betriebsleitebene alle Ebenen der Automatisierungspyramide ab (s. Abbildung 1).[8] Mit ERP-Systemen und Manufacturing-Execution-Systemen (MES) bestehen die oberen zwei Ebenen der Pyramide vorrangig aus Komponenten der Office-IT.[9]

Industrial Control Systems (ICS, dt.: Industrielle Steuerungsanlagen[10]) ist der vom BSI genutzte Überbegriff für die eigentliche Automatisierungs- bzw. Steuerungstechnik, welche von der Feldebene bis zur Prozessleitebene in der Automati-

3 Vgl. Strauß (2015), S. 343-344.

4 BSI-Standard 200-2 (2017), S. 14; ISO/IEC 27000:2016(E) (2016), S. 6.

5 Lass und Kotarski (2014), S. 402.

6 Bundesamt für Sicherheit in der Informationstechnik (2013), S. 13. Die Begrifflichkeiten sind jedoch nicht immer einheitlich und unterscheiden sich etwa zwischen ICS-Security-Kompendium und IT-Grundschutz.

7 BSI IT-Grundschutz-Kompendium (2017), S. 1; Gartner (2017).

8 Vgl. Atos (2012), S. 5, wo eine zunehmende Konvergenz von IT und OT diskutiert wird, nach der OT vermehrt auch bis in die Unternehmensebene und ERP-Anwendungen hineinreichen kann.

9 Lass und Fuhr (2013), S. 30.

10 Auch IACS für „Industrial and Automation Control Systems" oder PCS für „Process Control Systems". Vgl. IEC/ISA 62443-2-4:2013 (2013), S. 10; vgl. IEC/ISA 62443-3-3:2013 + Cor.:2014 (2015), S. 27. Allerdings werden in diesem Entwurf auf S. 10 IACS unglücklicherweise als synonym zu SCADA gesehen und in der Konsequenz ggf. nicht als Überbegriff; Association (2014), S. 1.

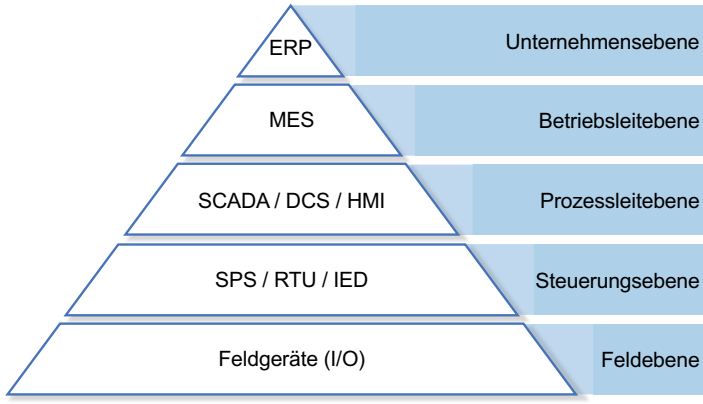

Abb. 1: Automatisierungspyramide. Langmann (2004), S. 335; mit freundlicher Genehmigung von © Carl Hanser Verlag (2004)

sierungspyramide verortet werden kann. „ICS werden überall dort eingesetzt, wo Abläufe automatisiert werden. Sie werden für das Messen, Steuern, Regeln und Bedienen von industriellen Abläufen benutzt."[11] Für cyber-physische Sicherheitsanalysen von ICS können insbesondere hybride Testumgebungen eingesetzt werden, weshalb hier der Schwerpunkt dieser Arbeit liegt, wird jedoch punktuell auch auf die Betriebsleitebene und das Unternehmensnetzwerk eingegangen.

2.2 Gefährdungen und Risiken der Informationssicherheit von Industrieanlagen

Die Gefährdungslage von Industrieanlagen hat sich in den letzten Jahren verschärft.[12] Die Konsequenzen eines Sicherheitsvorfalls in Industrieanlagen können mannigfaltig und gravierend sein: Die Betriebssicherheit kann beeinträchtigt werden, es kann zu Ausfällen in der Versorgung kommen, Betriebsmittel können beschädigt oder zerstört werden. Ebenso kann es zu Umweltverschmutzungen kommen, wichtige Informationen des Unternehmens können kompromittiert werden und/oder es kann in Konsequenz zu Imageschäden oder Haftungsfällen kommen.[13]

[11] Bundesamt für Sicherheit in der Informationstechnik (2013), S. 14-15.
[12] Thim und Kotarski (2015), S. 44; Moss (2012), S. 15.
[13] Floß (2015), S. 17; Assante und Lee (2015), S. 11-12; McNabb (2010), S. 14-15 und S. 26.

Eine Gefährdung wird dabei definiert als die „Möglichkeit, dass [...] aus einer Gefahr ein Ereignis mit einer bestimmten Intensität erwächst, das zu einem Schaden an einem Schutzgut führen kann.“[14] Als Gefahr oder Bedrohung (Threat) können jegliche Ursachen verstanden werden, die einem IT-System, der Organisation oder ihrer Prozesse schaden könnten.[15] Die Bedrohungen können grob in fünf Kategorien unterteilt werden:

- Höhere Gewalt (z. B. Extremwetterereignisse, seismische Ereignisse)
- organisatorische Mängel
- menschliche Fehlhandlungen (z. B. Fahrlässigkeit, Unfälle)
- technisches Versagen sowie
- vorsätzliche Handlungen (Terrorismus, Kriminalität, Cyberwarfare).[16]

Eine Bedrohung wird jedoch erst dann zu einer Gefährdung für eine Organisation, wenn sie auf eine Schwachstelle bzw. vorhandene Verwundbarkeit trifft (Gefährdung = Verwundbarkeit + Bedrohung, s. Abbildung 2).[17] Im Hinblick auf konkrete Bedrohungen hat das BSI eine Liste der aktuellen Bedrohungen mit der höchsten Kritikalität zusammengestellt, denen ICS ausgesetzt sind (s. Tabelle 1).

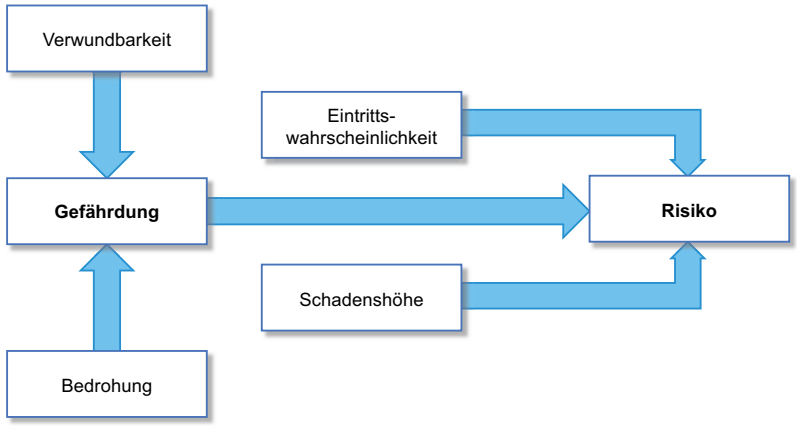

Abb. 2: Gefährdung und Risiko in der Informationssicherheit. Sowa (2017), S. 40; mit freundlicher Genehmigung von © Springer Nature (2017)

14 Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2011), S. 13; Strauß (2015), S. 346.
15 Sowa (2017), S. 41.
16 BSI-Standard 100-1 (2008), S. 61; Strauß (2015), S. 346-347; Luiijf (2016), S. 71.
17 Sowa (2017), S. 42; Lass und Kotarski (2014), S. 403.

Für ein besseres Verständnis der Anlagensicherheit lohnt es sich daher, im Folgenden die Gründe für typische Schwachstellen im Bereich der Betriebs- und Steuerungstechnik zu betrachten. Zunächst können die besonderen Charakteristika untersucht werden, die sich aus dem Anwendungskontext von ICS ergeben und Unterschiede zur Office-IT verdeutlichen: ICS müssen in der Regel eine höchstmögliche Verfügbarkeit und Verlässlichkeit aufweisen, echtzeitfähig sein, dürfen nur eine sehr geringe Latenz aufweisen und müssen garantierte Abarbeitungszeiten leisten können. Die Konsequenzen einer Unterbrechung oder eines Ausfalls Kritischer Infrastrukturen sind groß, da neben der Wirtschaft auch die Umwelt sowie die Sicherung der Existenz der Bürger bedroht sein kann. Hier steht der Schutz von Mensch, Technik und Umwelt im Vordergrund.[18] Insofern sind die Fehler- und Ausfalltoleranzen von ICS sehr viel geringer, als dies bei normalen IT-Systemen der Fall ist, weshalb besondere Anforderungen an die Informationssicherheit von ICS gestellt werden.[19]

Nr.	Top-10-Bedrohungen von ICS 2016
1.	Social Engineering und Phishing
2.	Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware
3.	Infektion mit Schadsoftware über Internet und Intranet
4.	Einbruch über Fernwartungszugänge
5.	Menschliches Fehlverhalten und Sabotage
6.	Zugriff auf Internet-verbundene Steuerungskomponenten
7.	Technisches Fehlverhalten und höhere Gewalt
8.	Kompromittierung von Extranet und Cloud-Komponenten
9.	(D)DoS-Angriffe
10.	Kompromittierung von Smartphones im Produktionsumfeld

Tabelle 1: Top-10-Bedrohungen von ICS in 2016[20]

Als Industrietechnik sind ICS in der Anschaffung vergleichsweise teuer, weisen in der Regel sehr lange Lebenszyklen von mitunter mehr als 20 Jahren auf und sind auf vergleichsweise lange Einsatzzeiten ausgelegt. Entsprechend sind viele Altsysteme im Betrieb, bei denen Sicherheitsbedenken in ihrer Entwicklung noch keine große Rolle spielten. Dies ist auch darauf zurückzuführen, dass viele ICS-/SCADA-Systeme zur Zeit ihrer Einführung über keine Verbindung zum Internet oder zu LANs verfügten, weshalb durch die physische Isolation ein hoher Grad

[18] Bundesamt für Sicherheit in der Informationstechnik (2013), S. 27-28; Lass und Kotarski (2014), S. 397-399.

[19] Christiansson und Luiijf (2008), S. 239; Wilhoit (2013), S. 4.

an Informationssicherheit gewährleistet war.[21] Andere Sicherheitsaspekte werden nun oft erst nachträglich betrachtet und für ältere Komponenten gibt es trotz bekannter Schwachstellen oft keine Sicherheitsupdates mehr. Gleichzeitig können diese Anlagen aufgrund ihrer langen Nutzungsdauer und den hohen Anschaffungskosten auch nicht einfach ausgetauscht werden.[22]

Häufig anzutreffende Schwachstelle sind beispielsweise unsichere Protokolle, über die ICS- und OT-Komponenten miteinander kommunizieren, welche nicht unter Sicherheitsgesichtspunkten entwickelt wurden. Da ICS mittlerweile jedoch oft mit anderen IT-Systemen vernetzt sind, bestehen hier auch Abhängigkeiten zu diesen Systemen, Netzen oder Diensten. Sicherheitsvorfälle oder Ausfälle dieser Systeme können sich auf die OT- bzw. ICS-Komponenten auswirken. Insbesondere bei Zuhilfenahme externer Dienstleister zum Beispiel für Cloud-Lösungen kann dies problematisch sein, denn ein solcher Vorfall kann dann ggf. auch nur durch jene Organisation behoben werden und führt zu Abhängigkeiten. Interdependenzen und Verkettungen von Ereignissen bzw. Kaskadeneffekte werden oft ebenso wenig ausreichend betrachtet, wie die räumliche Verteilung von Infrastrukturen oder fehlende Redundanzen. In diesem Zusammenhang ist auch zu erwähnen, dass es häufig an angemessenen Überwachungs- und Detektionsverfahren im Hinblick auf die unterstützende IT-Infrastruktur fehlt.[23]

Wenn sicherheitsrelevante Updates für OT bzw. ICS vorhanden sind, werden diese dennoch oft nicht durchgeführt und offene oder bekannte Schwachstellen nicht geschlossen.[24] Aber auch das Schaffen von Abhilfe kann eine Herausforderung sein, wenn ICS in betriebliche Abläufe oder Projektierungsprozesse nicht angemessen eingebunden sind. So sind Reboots im produktiven Umfeld nicht ohne Weiteres möglich und Wartungszyklen bedürfen sorgfältiger Planung, denn sicherheitstechnische Eingriffe, etwa zur Durchführung von Sicherheitsupdates, können sonst unerwünschte Folgen nach sich ziehen.[25] Hierzu gehören auch externe Komplikationen, etwa durch das Erfordernis einer erneuten behördlichen Freigabe oder den Verlust des Herstellersupports. Sofern Testkonzepte für Eingriffe an ICS über-

20 Bundesamt für Sicherheit in der Informationstechnik (2016), S. 2.

21 Chabukswar u. a. (2010), S. 1; Wilhoit (2013), S. 4.

22 Bundesamt für Sicherheit in der Informationstechnik (2013), S. 27-28; Lass und Kotarski (2014), S. 399; Bundesamt für Sicherheit in der Informationstechnik (2015), S. 107; BSI-Standard 200-2 (2017), S. 43; BSI IT-Grundschutz-Kompendium (2017), S. 2-4; Bitkom und VKU (2015), S. 78.

23 Strauß (2015), S. 346-350; Bundesamt für Sicherheit in der Informationstechnik (2015), S. 106-110; BSI IT-Grundschutz-Kompendium (2017), S. 5; Assante und Lee (2015), S. 7.

24 Bundesamt für Sicherheit in der Informationstechnik (2015), S. 108.

25 Bundesamt für Sicherheit in der Informationstechnik (2013), S. 27-28.

haupt vorhanden sind, sind diese angesichts der hohen Verfügbarkeitsanforderungen teilweise unzureichend.[26]

Auch die Beschaffung von Ersatzteilen kann bei solchen Altsystemen problematisch sein und das Knowhow in der Pflege und Wartung dieser Systeme liegt bei neuen Mitarbeitern oft nicht vor. Dies ist nicht zuletzt deshalb problematisch, weil Standardkonfigurationen von ICS-Komponenten unsicher sein können und beispielsweise durch Standardpasswörter unbefugte Zugriffe erheblich erleichtert werden. Problematisch können ebenso auch unsichere Administrations- und Fernadministrationskonzepte sein sowie unzureichende Schutzkonzepte gegen Schadprogramme für ICS oder OT.[27] Ganz grundlegend fehlt es vielen Unternehmen an einer geeigneten Einbindung von Operational Technology bzw. Industrial Control Systems in die Sicherheitsorganisation, was darauf zurückzuführen ist, dass bestehende Sicherheitsvorgaben oder klassische Methoden aus dem Bereich der Office-IT nicht ohne Weiteres auf ICS anwendbar sind. Folglich fehlen hier oft Vorgaben, die ICS-spezifische Besonderheiten und Anforderungen berücksichtigen.[28]

2.3 Herausforderungen von KRITIS-Betreibern in der Informationssicherheit am Beispiel der Wasserversorgung

Das Bundesministerium des Innern definiert Kritische Infrastrukturen wie folgt: „Kritische Infrastrukturen sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.“[29] Kritikalität ist demnach ein „relatives Maß für die Bedeutsamkeit einer Infrastruktur in Bezug auf die Konsequenzen, die eine Störung oder ein Funktionsausfall für die Versorgungssicherheit der Gesellschaft mit wichtigen Gütern und Dienstleistungen

[26] BSI IT-Grundschutz-Kompendium (2017), S. 2-3; Bitkom und VKU (2015), S. 78; Lass und Kotarski (2014), S. 399-401.

[27] BSI IT-Grundschutz-Kompendium (2017), S. 2-4; Strauß (2015), S. 346-350; Bundesamt für Sicherheit in der Informationstechnik (2015), S. 106-110; Thim und Kotarski (2015), S. 44; vgl. Christiansson und Luiijf (2008), S. 238.

[28] BSI IT-Grundschutz-Kompendium (2017), S. 2; Lass und Kotarski (2014), S. 397 ff.; Lass und Fuhr (2013), S. 29.

[29] Bundesministerium des Innern (2009), S. 3; zusätzlich zum Begriff der Kritischen Infrastrukturen wird mitunter auch der ähnliche Begriff der „Kritischen Dienstleistungen“ benutzt, die sich in ihrer Bedeutung zum großen Teil überschneiden.

hat."[30] Der Begriff der Kritischen Infrastrukturen als Element der Daseinsvorsorge umfasst beispielsweise Energieanlagen und -netze, Informations- und Kommunikationstechnik, Finanz- und Gesundheitswesen, Abfallentsorgung sowie Transport und Verkehr.[31]

Die Gefährdungslage von Kritischen Infrastrukturen ist aufgrund ihrer Stellung als Teil der Daseinsvorsorge eine Besondere, denn ihre Verfügbarkeit ist für die Wirtschaft und Gesellschaft eines Staates von großer Bedeutung. KRITIS-Betreiber sind als Dienstleistung von allgemeinem (wirtschaftlichem) Interesse[32] unter Umständen besonderen Gefährdungen und können insbesondere für böswillige Angriffe eine attraktive Zielscheibe sein, denn mögliche Unterbrechungen oder Ausfälle im Betrieb können eine große Reichweite haben. Für vorsätzliche Handlungen gegen Organisationen kommen verschiedene Typen von Akteuren in Frage, von Aktivisten über staatliche Akteure bis zu Terroristen, kriminellen Organisationen oder Einzelpersonen, welche sowohl organisationsextern als auch organisationsintern sein können.[33]

Auch die öffentliche Wasserversorgung sowie die Abwasserbeseitigung fallen unter den Begriff der Kritischen Infrastrukturen. Schließlich ist Wasser ein Lebensmittel und ebenso für viele Prozesse in der Landwirtschaft und Industrie unverzichtbar.[34] Der Wassersektor ist ein passendes Beispiel für die Informationssicherheit gerade von kleinen und mittleren KRITIS-Betreibern für die die hybride Testumgebung ein besonders großer Mehrwert darstellen kann, da der Wassersektor in Deutschland durch einen sehr großen Anteil solcher Unternehmen geprägt ist.

Eine Beeinträchtigung oder Unterbrechung der Kritischen Infrastruktur Wasserversorgung hätte mittel- bis langfristig gravierende Auswirkungen für die Gesundheit und Existenz der Menschen. Sie könnte sich auf andere Sektoren und Branchen der Wirtschaft bis hin zur Aufgabenwahrnehmung des Staates auswirken.[35]

---

30 Bundesministerium des Innern (2009), S. 7; Röchert-Voigt, Stein und Weber (2010), S. 8.

31 Europäische Kommission (2004), S. 4; Strauß (2015), S. 344-345; Bundesamt für Sicherheit in der Informationstechnik (2015), S. 37: „Als Daseinsvorsorge wird die Pflicht des Staates verstanden, die Verfügbarkeit von Infrastrukturen und Dienstleistungen zur Versorgung der Bevölkerung mit überlebensnotwendigen Gütern sicherzustellen."

32 Der Begriff der Dienstleistungen von allgemeinem (wirtschaftlichem) Interesse (DAI/DAWI) ist eine unionsrechtliche Perspektive auf den sozialwissenschaftlichen Begriff der Daseinsvorsorge. Der Begriff der Daseinsvorsorge ist kein rechtlich normierter Begriff, wohingegen DAWI bzw. DAI im Unionsrecht definiert werden. Vgl. Kuhnert und Leps (2017), S. 230 ff.

33 Christiansson und Luiijf (2008), S. 241; Davis u. a. (2006), S. 484.

34 Bundesamt für Sicherheit in der Informationstechnik (2015), S. 37.

35 Ebd., S. 37.

Der Stellenwert der Ressource Wasser für unsere Gesellschaft wird am Wasserfußabdruck deutlich, wonach jeder Bundesbürger rechnerisch pro Tag 3.900 Liter Wasser verbraucht.[36] Der tatsächliche Pro-Kopf-Verbrauch von Trinkwasser lag 2010 bei 212 Litern pro Einwohner und Tag.[37] Die Differenz verdeutlicht die Bedeutung der Ressource Wasser für Industrie und Landwirtschaft: Über 130.000 Betriebe in Deutschland haben einen hohen Wasserbedarf.[38]

An diesem Beispiel wird ebenso deutlich, dass Versorgungssicherheit mehr umfasst, als die bloße Zuverlässigkeit der Wasserversorgung für den Endkunden oder die Behebung von Störungen. So liegt der Fokus der Informationssicherheit weniger auf der grundsätzlichen technischen Bereitstellung und Gewährleistung der Wasserversorgung als vielmehr auf dem Schutz dieser Strukturen vor Gefährdungen wie unbefugten Eingriffen, Angriffen, Naturkatastrophen und anderen Krisen. Dies kann sich von der Sicherheitsorganisation und dem Management von Informationssicherheit über technische Informationssicherheit, Detektion, Reaktion und Notfallmanagement bis hin zu Maßnahmen im Bereich Security Awareness erstrecken (s. Abschnitt 2.2).[39] Diese Dimension der Versorgungssicherheit, die sich – verkürzt dargestellt – mit dem Schutz von Komponenten der Betriebs- und Steuerungstechnik sowie ähnlichen zentralen Risikoelementen gegen Ausfälle, Manipulation oder Angriffe beschäftigt, ist für diese Ausarbeitung maßgeblich.

Angesichts der Verbreitung von Gefährdungen und Schwachstellen einerseits und der Bedeutung von Kritischen Infrastrukturen wie der Wasserversorgung andererseits streben Gesetzgeber, Verbände und Unternehmen eine Verbesserung der Sicherheit von Kritischen Infrastrukturen an. Dies äußert sich etwa in verschärften rechtlichen, technischen und verbandlichen Anforderungen und Vorgaben zur Infrastruktur- und Informationssicherheit.[40] Entsprechende Regelwerke, Normen, Leitlinien und ähnliche Hilfestellungen werden derzeit entwickelt oder weiterentwickelt.[41] Spätestens seit den Änderungen am BSI-Gesetz durch das IT-Sicherheitsgesetz muss sich jedes Unternehmen im Bereich der Kritischen Infra-

36 Umweltbundesamt (2014), S. 17. Diese kalkulatorische Angabe ist auf den hohen Verbrauch der Industrie und Landwirtschaft zurückzuführen.

37 Vgl. ebd., S. 74.

38 Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit (2014), S. 3.

39 Fritsch u. a. (2014), S. 5; Bundesamt für Sicherheit in der Informationstechnik (2015), S. 98.

40 Weiblein und Radis (2014), S. 6-8; Ver.di (2015), S. 24-25; Gronau u. a. (2012), S. 6. Vgl. beispielsweise § 1 Abs. 2 Nr. 2 des Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) bzw. § 2 Abs. 10 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG).

41 Ver.di (2015), S. 36; Bundesamt für Sicherheit in der Informationstechnik (2015), S. 106-116. Zu erwähnen sind hier beispielsweise die BSI-Standards zum IT-Grundschutz oder die Umsetzung des IT-Sicherheitsgesetzes. In manchen Bereichen der Informationssicher-

strukturen mit den individuellen Gegebenheiten beschäftigen und für den Umgang mit Risiken entsprechende Maßnahmen treffen.[42]

Das 2015 in Kraft getretene IT-Sicherheitsgesetz hat zum Ziel, digitale Infrastrukturen in Deutschland abzusichern. Es betrifft dabei insbesondere Betreiber Kritischer Infrastrukturen aus den Sektoren Energie, Finanz- und Versicherungswesen, Ernährung, Wasser, Gesundheit, Transport und Verkehr sowie Informationstechnik und Telekommunikation. Diese sind grundsätzlich verpflichtet, allgemeine und branchenspezifische Mindeststandards einzuhalten, regelmäßige Sicherheitsüberprüfungen zum Nachweis der Umsetzung durchzuführen und ggf. Sicherheitsvorfälle zu melden. Es gibt hiervon für kleine und mittlere KRITIS-Betreiber bestimmte Ausnahmeregelungen, wodurch diese vom BSI-Gesetz in deutlich geringerem Ausmaß und somit von einem geringeren Aufwand betroffen sind.[43] Bei Berücksichtigung der weitgehenden Ausnahmen sind mit etwa 230 Anlagen nur knapp 1,4 % der etwa 16.000 Wasserunternehmen in Deutschland von den Verpflichteten nach IT-Sicherheitsgesetz bzw. BSI-Gesetz betroffen.[44]

Jedoch haben kleine und mittelgroße Wasserunternehmen dieselben Infrastrukturen und sind somit denselben Bedrohungen und Gefährdungen ausgesetzt. Dennoch sind sie von Pflichten betroffen, etwa Meldepflichten, welche ggf. sanktionsbewährt sind.[45] Relevant könnten diese Vorschriften für KMU auch im Hinblick auf die Frage nach Sorgfaltspflichten im Fall von deliktischen Haftungsfragen i.S.d. §§ 823 ff. BGB sein. Bei Sicherheitsvorfällen, die zulasten Dritter eine Verletzung eines geschützten Rechtsguts i.S.d. § 823 Abs. 1 BGB – etwa Gesundheit oder Eigentum – zur Folge haben, werden für Haftungsfragen in der Regel die sog. Verkehrspflichten betrachtet, die mit der Sorgfaltspflicht i.S.d. § 276 BGB der Sache nach identisch sind und für welche die Etablierung branchenüblicher Mindeststandards nach IT-Sicherheitsgesetz eine Rolle spielen könnte. In einem solchen Fall könnte sich also auch für kleine und mittlere KRITIS-Betreiber die Frage stellen, ob grundlegende Sicherheitsmaßnahmen etwa gemäß den BSI-Standards durchgeführt wurden.[46]

Durch diese Vorschriften, vor allem aber durch die Gefährdungslage ist also ein Handlungsdruck für KRITIS-Betreiber entstanden, der so manches Wasserunternehmen vor Herausforderungen stellt. Auch wenn sie teilweise von den schärfs-

---

heit existieren hingegen noch keine eigenen Standards für Wasserunternehmen. Stattdessen werden beispielsweise Anforderungen an Prozessleitsysteme teilweise aus dem Energiesektor abgeleitet.

42 Bitkom und VKU (2015), S. 21; Thim und Kotarski (2015).

43 Wegener, Milde und Dolle (2016), S. 164-169.

44 Borchers (2016).

45 Vgl. Kipker und Pfeil (2016), S. 813.

46 Bundesministerium für Wirtschaft und Energie (2016), S. 100 ff.

ten Anforderungen nach BSI-Gesetz ausgenommen sind, stehen hier vor allem kleine und mittelgroße Wasserunternehmen vor Schwierigkeiten:[47] Sie überprüfen die Informationssicherheit bestehender oder zukünftiger IT-Systeme seltener oder es ist überhaupt keine ausreichende Sicherheitskonzeption im Sinne des IT-Grundschutzes vorhanden.[48] Die Gründe hierfür können beispielsweise auf die begrenzten finanziellen Möglichkeiten kleiner und mittelgroßer Wasserversorger zurückgeführt werden.[49] Risikovorsorge kann ressourcen- bzw. kostenintensiv sein, denn auch in kleineren Unternehmen können IT-Infrastrukturen eine hohe Komplexität aufweisen.[50] Gerade eine ergänzende Sicherheitsanalyse für Zielobjekte mit erhöhtem Schutzbedarf kann in der Erstellung eines Sicherheitskonzeptes teuer und aufwendig sein. Deshalb ist der Einsatz von Sicherheitsanalysen wie Penetrationstests oft nicht oder nur begrenzt möglich. Aber auch die Umsetzung grundlegender Sicherheitsmaßnahmen ist ressourcenintensiv und nicht immer selbstverständlich.[51] Zum Beispiel wird bei manchen kleineren Betreibern aus Kostengründen keine Trennung der Netze und Systeme der Office-IT und der Prozess-IT vorgenommen.[52] Dazu kommt, dass kleine und mittlere KRITIS-Betreiber über weniger Personalressourcen verfügen und ihnen deshalb auch oft das notwendige Fachwissen für Informationssicherheit im Bereich ICS fehlt.[53] Dies hat zur Folge, dass manchen KMU im Wassersektor schlicht das Problembewusstsein fehlt, um ausreichende Maßnahmen im Bereich der Informationssicherheit umzusetzen.[54] In den letzten Jahren ist der Personalbestand innerhalb der Netzleittechnik durch Rationalisierungsdruck eher weiter reduziert worden.[55] Ohne an dieser Stelle auf die Hintergründe eingehen zu können, lässt sich ein Teil der Problematik also durch

47 Brauer und Sturm (2014), S. 15-16; Hulsmann und Smeets (2011), S. 2; EurEau (2011), zitiert nach Castell-Exner (2013), S. 7.

48 Bundesamt für Sicherheit in der Informationstechnik (2015), S. 107; Bitkom und VKU (2015), S. 10-14.

49 Bundesamt für Sicherheit in der Informationstechnik (2015), S. 106-108; Detken, Eren und Steiner (2012), S. 1; Hulsmann und Smeets (2011), S. 2; Brauer und Sturm (2014), S. 15-16; Hulsmann und Smeets (2011), S. 2.

50 BSI-Standard 200-2 (2017), S. 15; Schmölzer (2010), S. 30; Detken, Eren und Steiner (2012), S. 1; Thim und Kotarski (2015), S. 44.

51 Lass und Kotarski (2014), S. 401; Christiansson und Luiijf (2008), S. 238; Wilhoit (2013), S. 4; BSI-Standard 200-1 (2017), S. 37-38.

52 Bundesamt für Sicherheit in der Informationstechnik (2015), S. 108; BSI IT-Grundschutz-Kompendium (2017).

53 Thim und Kotarski (2015), S. 44; Detken, Eren und Steiner (2012), S. 1; Brauer und Sturm (2014), S. 15-16; Bundesamt für Sicherheit in der Informationstechnik (2015), S. 106-108.

54 Engler, Haag und Biedermann (2014), S. 6; Bundesamt für Sicherheit in der Informationstechnik (2015), S. 115.

55 Bitkom und VKU (2015), S. 78; Leps (2016), S. 69; vgl. Kuhnert und Leps (2017), S. 322.

Zielkonflikte erklären: Einsparungen zur Verbesserung der Wirtschaftlichkeit können zu Lasten einer hohen Informationssicherheit gehen.[56]

Die besondere Betroffenheit von kleinen und mittleren Wasserversorgern ist für die Daseinsvorsorge in Deutschland von großer Bedeutung, denn KMU machen einen Großteil der deutschen Wasserversorger aus. In der Branche der öffentlichen Wasserwirtschaft sind in Deutschland insgesamt mehr als 16.000 Unternehmen aktiv.[57] Hiervon sind mehr als 6.000 Unternehmen in der Wasserversorgung tätig sowie rund 6.900 in der Abwasserentsorgung.[58] Die Antwort auf die Frage, wie viele kleine und mittlere Wasserversorger es in Deutschland gibt, hängt von der zugrundeliegenden Definition ab. Wesentliche Kriterien sind die Mitarbeiterzahl, der Umsatz bzw. die Bilanzsumme, das Volumen der Wasserbereitstellung sowie die Anzahl der versorgten Einwohner. Eine Erhebung des Statistischen Bundesamtes aus dem Jahr 2005 zeichnet ein differenzierteres Bild: Demnach sind knapp 90 % der Unternehmen im Bereich der Energie- und Wasserversorgung in Deutschland kleine und mittlere Wasserunternehmen. Diese verfügen jedoch nur über 22 % des in diesem Bereich angestellten Personals und erwirtschaften bloß 9 % des Umsatzes. Der Umsatz je Beschäftigtem entsprach bei den KMU mit durchschnittlich 334.878 € nur rund einem Drittel des Wertes der Großunternehmen (943.182 €), obwohl die durchschnittlichen Brutto-Investitionen pro Beschäftigtem mit 48.633 € bei den KMU höher lagen als bei den Großunternehmen (31.344 €).[59] Diese Erhebung wendet die Kriterien der EU-Kommission zu KMU an, stellt also wirtschaftliche Betrachtungen in den Vordergrund, was im Kontext dieser Ausarbeitung angemessen ist, denn Informationssicherheit ist gerade für finanzschwache Unternehmen eine Herausforderung.[60] Auch das BSI-Gesetz beruft sich auf diese Kriterien.[61]

Der dargelegte Handlungsbedarf kleiner und mittlerer Wasserversorger verweist auf die Notwendigkeit der Entwicklung und Anwendung einer effektiven und effizienten Vorgehensweise für Überprüfungen der Informationssicherheit. Ein mögliches Verfahren kann hier die hybride Testumgebung sein.

---

56 IWW Rheinisch-Westfälisches Institut für Wasserforschung (2004), S. 11.

57 Bundesamt für Sicherheit in der Informationstechnik (2015), S. 17.

58 Bundesverband der Energie- und Wasserwirtschaft u. a. (2015), S. 31-33.

59 Kless und Veldhues (2008), S. 231-232.

60 Nach diesen Kriterien haben kleine Unternehmen bis zu 50 Beschäftigte und einen Jahresumsatz von bis zu 50 Mio. €, wogegen mittelgroße Unternehmen bis zu 250 Beschäftigte und einen Jahresumsatz von bis zu 50 Mio. € haben. Vgl. ebd., S. 226; vgl. Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (2003/361/EG), veröffentlicht im Amtsbl. der EU Nr. L 124, S. 36.

61 § 8c BSI-Gesetz i.d.F. 2016.

Literaturverzeichnis

Assante, M. J. und R. M. Lee (2015), *The Industrial Control System Cyber Kill Chain, SANS Institute InfoSec Reading Room*, SANS Institute.

Association, A. W. W. (2014), *Process Control System Security Guidance for the Water Sector*, American Water Works Association.

Atos (2012), *The convergence of IT and Operational Technology – White Paper*, Atos.

Bitkom und VKU (2015), *Praxisleitfaden IT-Sicherheitskatalog – Anforderungen an die IT für den sicheren Betrieb von Energieversorgungsnetzen*, Bitkom und VKU.

Borchers, D. (2016), *IT-Sicherheitsgesetz: Wer was wann zu melden hat*, URL: https://www.heise.de/newsticker/meldung/IT-Sicherheitsgesetz-Wer-was-wann-zu-melden-hat-3096885.html (besucht am: 20. 12. 2017).

Brauer, F. und S. Sturm (2014), *European Strategic Workshop on Water Safety Planning, 12–13 March 2014, Berlin, Germany – Key Outcomes*, Umweltbundesamt.

BSI IT-Grundschutz-Kompendium (2017), *IND.1 Betriebs- und Steuerungstechnik*.

BSI IT-Grundschutz-Kompendium (2017), *Umsetzungshinweise zum Baustein IND.1 Betriebs- und Steuerungstechnik*.

BSI-Standard 100-1 (2008), *Managementsysteme für Informationssicherheit (ISMS)*.

BSI-Standard 200-1 (2017), *Managementsysteme für Informationssicherheit (ISMS) – Community Draft*.

BSI-Standard 200-2 (2017), *IT-Grundschutz-Methodik – Community Draft*.

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2011), *BBK-Glossar Ausgewählte zentrale Begriffe des Bevölkerungsschutzes (Praxis im Bevölkerungsschutz)*, Bd. 8, Bundesamt für Bevölkerungsschutz und Katastrophenhilfe.

Bundesamt für Sicherheit in der Informationstechnik (2013), *ICS-Security-Kompendium*.

Bundesamt für Sicherheit in der Informationstechnik (2015), *KRITIS-Sektorstudie: Ernährung und Wasser*, Bundesamt für Sicherheit in der Informationstechnik.

Bundesamt für Sicherheit in der Informationstechnik (2016), *Industrial Control System Security: Top 10 Bedrohungen und Gegenmaßnahmen 2016 – Empfehlung: IT in der Produktion – BSI-Veröffentlichungen zur Cyber-Sicherheit BSI-CS 005*.

Bundesministerium des Innern (2009), *Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie)*, Bundesministerium des Innern.

Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit (2014), *Wasser ist Leben*, Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit.

Bundesministerium für Wirtschaft und Energie (2016), *Studie im Auftrag des Bundesministeriums für Wirtschaft und Energie: IT-Sicherheit für die Industrie 4.0 – Produktion, Produkte, Dienste von morgen im Zeichen globalisierter Wertschöpfungsketten, Abschlussbericht*, Bundesministerium für Wirtschaft und Energie.

Bundesverband der Energie- und Wasserwirtschaft u. a. (2015), *Branchenbild der deutschen Wasserwirtschaft 2015*, wvgw Wirtschafts- und Verlagsgesellschaft.

Castell-Exner, C. (2013), *Sicherheit in der Trinkwasserversorgung: Risikomanagement im Normalbetrieb – nationale und europäische Ansätze für kleinere Wasserversorger, IWW-Kolloquium "Technisches Risikomanagement – Neue Ansätze für kleine und große WVU", Mülheim*, Präsentation, URL: https://www.dvgw.de/index.php?eID=dumpFile&t=f&f=751&token=595a3d69ad95c090acfb07c49b86673644bbaa69 (besucht am: 20. 12. 2017).

Chabukswar, R. u. a. (2010), Simulation of Network Attacks on SCADA Systems, in: *First Workshop on Secure Control Systems*.

Christiansson, H. und E. Luiijf (2008), Creating a European SCADA security testbed, in: E. Goetz und S. Shenoi (Hrsg.), *International Conference on Critical Infrastructure Protection, 1st IFIP WG 11.10 International Conference, ICCIP 2007, New Hampshire, USA, Revised Selected Papers*, Springer, 237–247.

Davis, C. u. a. (2006), SCADA cyber-security testbed development, in: *Power Symposium, 2006. NAPS 2006. 38th North American*, IEEE, 483–488.

Detken, K.-O., E. Eren und M. Steiner (2012), Erhöhung der IT-Sicherheit durch Konfigurationsunterstützung bei der Virtualisierung, DACH Security, in: P. Schartner und J. Taeger (Hrsg.), *DACH Security 2012: Bestandsaufnahme – Konzepte – Anwendungen – Perspektiven*, Prof. Dr. Patrick Horster.

Engler, J., G. Haag und B. Biedermann (2014), *Erhebung und Bewertung der öffentlichen Wasserversorgung in Bayern – Versorgungssicherheit derzeit und künftig*, Präsentation auf dem DVGW-Forum SSichere Wasserversorgung im Kleinhandel", Mülheim an der Ruhr, (besucht am: 20. 12. 2017).

EurEau (2011), *EurEau Position Paper on the EU Guidance on Developing Water Safety Plans for Small Supplies*, EurEau – European federation of national associations of drinking water suppliers und waste water services.

Europäische Kommission (2004), *Schutz kritischer Infrastrukturen im Rahmen der Terrorismusbekämpfung, Mitteilung der Kommission an den Rat und das Europäische Parlament, KOM(2004) 702 endgültig*.

Floß, A. (2015), *Sicherheit von industriellen Steuerungssystemen: Sicherheitsmanagement mit der BSI IT-Grundschutz-Vorgehensweise*, Präsentation auf dem 14. Deutschen IT-Sicherheitskongress, Bonn.

Fritsch, P. u. a. (2014), *Mutschmann/Stimmelmayr: Taschenbuch der Wasserversorgung*, SpringerVieweg.

Gartner (2017), *Gartner IT Glossary, Operational Technology*, URL: http://www.gartner.com/it-glossary/operational-technology-ot/ (besucht am: 20. 12. 2017).

Gronau, N. u. a. (2012), *Organisation des Schutzes der kritischen Infrastruktur Wasserversorgung: Grundlagen und praktische Anwendung für Betreiber*, GITO mbH Verlag.

Hulsmann, A. und P. Smeets (2011), *Towards a Guidance Document for the implementation of a Risk Assessment for small water supplies in the European Union*, KWR Watercycle Research Institute.

IEC/ISA 62443-2-4:2013 (2013), *Security for industrial automation and control systems – Network and system security – Part 2-4: Security program requirements for IACS service providers*.

IEC/ISA 62443-3-3:2013 + Cor.:2014 (2015), *Industrielle Kommunikationsnetze – IT-Sicherheit für Netze und Systeme – Teil 3-3: Systemanforderungen zur IT-Sicherheit und Security-Level*.

ISO/IEC 27000:2016(E) (2016), *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

IWW Rheinisch-Westfälisches Institut für Wasserforschung (2004), *Kennzahlen für die Wasserversorgung: Feld-Test des Kennzahlensystems der IWA (International Water Association) – Nationales Teilprojekt Deutschland: Abschlussbericht zum Forschungsvorhaben 02 WT 0224*, IWW.

Kipker, D.-K. und D. Pfeil (2016), IT-Sicherheitsgesetz in Theorie und Praxis, in: *Datenschutz und Datensicherheit-DuD*, 40:12, 810–814.

Kless, S. und B. Veldhues (2008), Ausgewählte Ergebnisse für kleine und mittlere Unternehmen in Deutschland 2005, in: *Wirtschaft und Statistik*, 3, 225 ff.

Kuhnert, J. und O. Leps (2017), *Neue Wohnungsgemeinnützigkeit: Wege zu langfristig preiswertem und zukunftsgerechtem Wohnraum*, SpringerVS.

Langmann, R. (2004), *Taschenbuch der Automatisierung*, Hanser Verlag.

Lass, S. und D. Fuhr (2013), IT-Sicherheit in der Fabrik, in: *Productivity Management*, 18:2.

Lass, S. und D. Kotarski (2014), IT-Sicherheit als besondere Herausforderung von Industrie 4.0, in: W. Kersten, H. Koller und H. Lödding (Hrsg.), *Schriften-*

reihe der Hochschulgruppe für Arbeits- und Betriebsorganisation e.V. (HAB): Industrie 4.0 – Wie intelligente Vernetzung und kognitive Systeme unsere Arbeit verändern Schriftenreihe der Hochschulgruppe für Arbeits- und Betriebsorganisation, Gito Verlag Berlin, 397–419.

Leps, O. (2016), *Nutzung und Akzeptanz von E-Government-Fachanwendungen in der öffentlichen Verwaltung: Eine empirische Analyse am Beispiel des europäischen Binnenmarkt-Informationssystems*, Logos Verlag.

Luiijf, E. (2016), Threats in Industrial Control Systems, in: E. J. Colbert und A. Kott (Hrsg.), *Cyber-security of SCADA and Other Industrial Control Systems*, Springer, 15–28.

McNabb, J. (2010), *Cyberterrorism & the Security of the National Drinking Water Infrastructure*, Presentation at the DEF CON 18, July 31, 2010.

Moss, K. T. (2012), *Water treatment and distribution simulation for a SCADA security testbed*, Electronic Theses and Dissertations, Paper 1013, University of Louisville.

Röchert-Voigt, T., M. Stein und E. Weber (2010), *Wandlungsfähige Schutzstrukturen und Folgenabschätzung: Theoretische Grundlagen und praktische Anwendungen; Handlungsleitfaden*, GITO mbH Verlag.

Schmölzer, J. (2010), *IT-Sicherheit von SCADA-Systemen*, Diplomarbeit, Fachbereich Informationstechnik & Elektrotechnik, Hochschule Mittweida (FH).

Sowa, A. (2017), *Management der Informationssicherheit: Kontrolle und Optimierung*, SpringerVieweg.

Strauß, J. (2015), Infrastruktursicherheit, in: T. Jäger (Hrsg.), *Handbuch Sicherheitsgefahren*, SpringerVS.

Thim, C. und D. Kotarski (2015), Herausforderungen der IT-Sicherheit bei kleinen und mittleren Betreibern kritischer Infrastrukturen, in: *DVGW energie | wasser-praxis*, 10, 44–46.

Umweltbundesamt (2014), *Wasserwirtschaft in Deutschland Teil 1 – Grundlage*, Umweltbundesamt.

Ver.di (2015), *Wasserwirtschaft in Deutschland: Branchenanalyse – Trend und Herausforderungen*, Ver.di.

Wegener, C., T. Milde und W. Dolle (2016), *Informationssicherheits-Management: Leitfaden für Praktiker und Begleitbuch zur CISM-Zertifizierung*, Springer-Verlag.

Weiblein, W. und C. Radis (2014), *Tendenzen und Herausforderungen der deutschen Wasserwirtschaft: Zwischen Versorgungssicherheit, Veränderungsprozessen und rechtlichen Rahmenbedingungen*, Baker Tilly Roelfs.

Wilhoit, K. (2013), *Wer steckt tatsächlich hinter den Angriffen auf ICS-Ausrüstung?*, Trend Micro.

Kapitel 3
Der Aufbau von Betriebs- und Steuerungsanlagen

Betriebs- und Steuerungsanlagen sind im Allgemeinen durch eine große Komponentenvielfalt gekennzeichnet und in ihrem Aufbau grundsätzlich sehr heterogen. Es sind Anlagen mit unterschiedlichen Architekturen und Komponenten unterschiedlicher Generationen zu finden, die in Größe, Zweck und Zusammensetzung der Systeme stark variieren können.[1] Innovative Weiterentwicklungen von ICS-Komponenten führen dazu, dass sich dieser Trend noch verstärkt.[2] Die Grenzen zwischen eingesetzten Komponenten wie etwa RTU und SPS verschwimmen bei neueren Geräten, die über mehr und mehr Funktionen verfügen.[3] Die technischen Randbedingungen verändern sich laufend. Dies kann eine klare Einordnung von Komponenten und Gesamtsystemen erschweren.

Trotz dieser Vielfalt können ICS-Komponenten relativ wenigen Klassen zugeordnet werden.[4] Die gängigsten ICS-Komponenten können daher entlang der hierarchischen Gliederung von ICS beschrieben werden (s. Abbildung 1). Wegen der Vielzahl an technischen Lösungen zur Realisierung der Kommunikationsvorgänge und Prozesse in ICS-Systemen wird sich in den folgenden Abschnitten überblicksartig auf die wichtigsten Komponententypen konzentriert.[5] Die Beschreibung wird dabei auf jene Elemente beschränkt, die als ICS zur Betriebs- und Steuerungstechnik im engeren Sinne gehören, was die Ebenen bis zur Prozessführung bzw. Prozessleitebene umfasst.[6]

---

1 Christiansson und Luiijf (2008), S. 237-238; Lass und Kotarski (2014), S. 401.

2 Früh (2009), S. 182; Litz (2013), S. 330.

3 Sosinsky (2009), S. 311. So gibt es etwa Anzeige-, Bedien- und prozessnahe Komponenten, welche Signalverarbeitung, Beobachtung und Bedienung in einem Gerät vereinen und auf allen Ebenen vorkommen können.

4 Sullivan, Luiijf und Colbert (2016), S. 16.

5 Vgl. Bundesamt für Sicherheit in der Informationstechnik (2013), S. 22 ff.

6 Vgl. BSI-Standard 200-2 (2017), S. 72-74; BSI IT-Grundschutz-Kompendium (2017), S. 1; Bundesamt für Sicherheit in der Informationstechnik (2013), S. 14-15; Birkhold und Bauer (2014), S. 13.

O. Leps, *Hybride Testumgebungen für Kritische Infrastrukturen*,
https://doi.org/10.1007/978-3-658-22614-5_3

Zuvor muss jedoch auf die grundlegenden ICS-Architekturen und ihre Unterschiede eingegangen werden. Es gibt verschiedene Architekturansätze von Industrieanlagen, die sich jedoch in ihrem abstrakten Aufbau grundsätzlich ähneln. Dies verdeutlicht sowohl die Automatisierungspyramide als auch die abstraktschematische Darstellung in Abbildung 3.Vgl. Litz (2013), S. 24, für eine ähnliche Darstellung

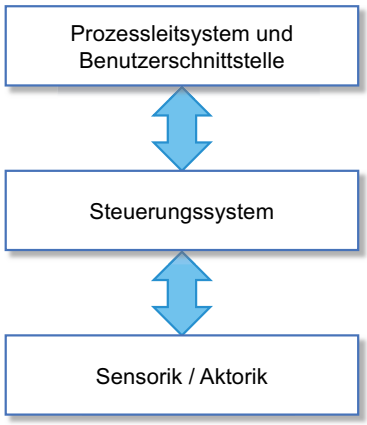

Abb. 3: Schematische Darstellung von der Feldebene zur Prozessleitebene. Adaptiert nach Knapp und Langill (2014), S. 66; mit freundlicher Genehmigung von © Elsevier Books (2015)

Es kann übergreifend zwischen zwei Architekturansätze unterschieden werden, mit denen Prozessleitsysteme (auch Process Control Systems genannt) in Industrieanlagen umgesetzt werden können: SCADA-Systeme (Supervisory Control and Data Acquisition, dt.: Überwachung, Steuerung und Datenerfassung) und DCS (Distributed Control System, dt.: Verteiltes Steuersystem).[7] Beide haben die Überwachung und Steuerung von Produktions- bzw. Industrieprozessen zum Ziel.[8] An dieser Stelle sei gesagt, dass in Literatur und Praxis keine Einigkeit in der Bedeutung und Benutzung dieser Begriffe herrscht.[9] Sowohl DCS als auch SCADA-

[7] Knapp und Langill (2014), S. 15; Greeff und Ghoshal (2004), S. 34. Teilweise werden in Abgrenzung dazu auch noch Safety Instrumented Systems (SIS), Building Automation Systems, Energy Management Systems und Process Control Systems als eigenständige ICS-Typen gesehen. Vgl. Sullivan, Luiijf und Colbert (2016), S. 24-27.

[8] Knapp und Langill (2014), S. 15; Lerch (2012), S. 573; Chabukswar u. a. (2010); Queiroz u. a. (2009), S. 357.

[9] Beispielsweise werden ICS oft pauschal als SCADA bezeichnet, vgl. Knapp und Langill (2014), S. 13. Ebenso werden die Begriffe SCADA und DCS teilweise synonym verwen-

Systeme können grundsätzlich in der Wasserversorgung und Wasserentsorgung zum Einsatz kommen.[10]

SCADA-Systeme werden vorrangig für räumlich verteilte Systeme verwendet, wie sie oft in der Wasserwirtschaft eingesetzt werden.[11] Typischerweise bestehen sie aus einem oder mehreren sog. Master Terminal Units (MTU, auch SCADA-Master oder SCADA-Server genannt), welche als Bedien- und Beobachtungssysteme der Überwachung und Kontrolle des Systems dienen. Des Weiteren bestehen sie aus lokalen steuerungstechnischen Instrumenten wie Remote Terminal Units (RTU), die Signale der lokalen Sensoren verarbeiten bzw. lokale Aktoren ansprechen, sowie der dazugehörigen Netzwerktechnik (s. Abbildung 4 sowie Anlage A.2 als Großdarstellung).[12] Die primäre Bedienung erfolgt in diesem Systemaufbau jeweils über die MTU bzw. die mit dieser verbundene Benutzerschnittstelle, die Echtzeitdaten wiedergibt. Diese dezentrale Prozessleitsoftware kann ggf. durch weitere Anwendungen ergänzt und ausgewertet werden, etwa im Kontrollraum, und kann zu diesem Zweck in größeren Anlagen auch über mehrere MTU-Server- und Sub-MTU-Server verfügen (s. Anlage A.3).[13] SCADA-Systeme gelten vor dem Hintergrund der Nutzung von Fernwirktechniken als datenerfassungsorientiert: Die Feld- und Steuerungsebene muss auch ohne eine Verbindung zur Leitstelle bzw. Prozessleitsoftware den Betrieb aufrechterhalten können, weswegen die relevanten Einstellungen und Prozessdaten dezentral vorgehalten und erfasst werden.[14]

DCS gelten hingegen als prozessorientiert und werden vornehmlich innerhalb kleinteiliger räumlicher Gebiete wie Fabriken oder Gebäuden eingesetzt, denn sie

---

det, vgl. Lewis (2014), S. 223. An anderer Stelle wird der Begriff Prozessleitsystem als Synonym für DCS verwendet, welcher von SCADA-Systemen abgegrenzt wird, vgl. Bundesamt für Sicherheit in der Informationstechnik (2013), S. 13. Nach weiteren Definitionen beschreibt SCADA hingegen die Steuerungssoftware innerhalb eines DCS, vgl. Sosinsky (2009), S. 311, oder wird generell als Synonym für die Benutzerschnittstelle bzw. die dort eingesetzte Hardware und Prozessleitsoftware oder die damit verbundene MTU verwendet, vgl. ebd., S. 301. In dieser Ausarbeitung bezeichnen die Begriffe SCADA-System und DCS unterschiedliche Architekturvarianten von Prozessleitsystemen und die jeweils dazugehörige Software/Hardware, womit sich weitgehend an das Verständnis des BSI angelehnt wird. Die genutzte Software der Prozessleitebene wird im Allgemeinen pauschal als Prozessleitsoftware bezeichnet, wobei sie je nach Architektur (zusätzlich) auf unterschiedlichen Ebenen zum Einsatz kommen kann.

10 National Institute of Standards and Technology (2015), S. 2-5-2-10.

11 Lewis (2014), S. 223; Greeff und Ghoshal (2004), S. 32; Hoeppner u. a. (2006), S. 518.

12 Chabukswar u. a. (2010).

13 Greeff und Ghoshal (2004), S. 35.

14 Macaulay und Singer (2011), S. 43; Bundesamt für Sicherheit in der Informationstechnik (2013), S. 13-21; Greeff und Ghoshal (2004), S. 35.

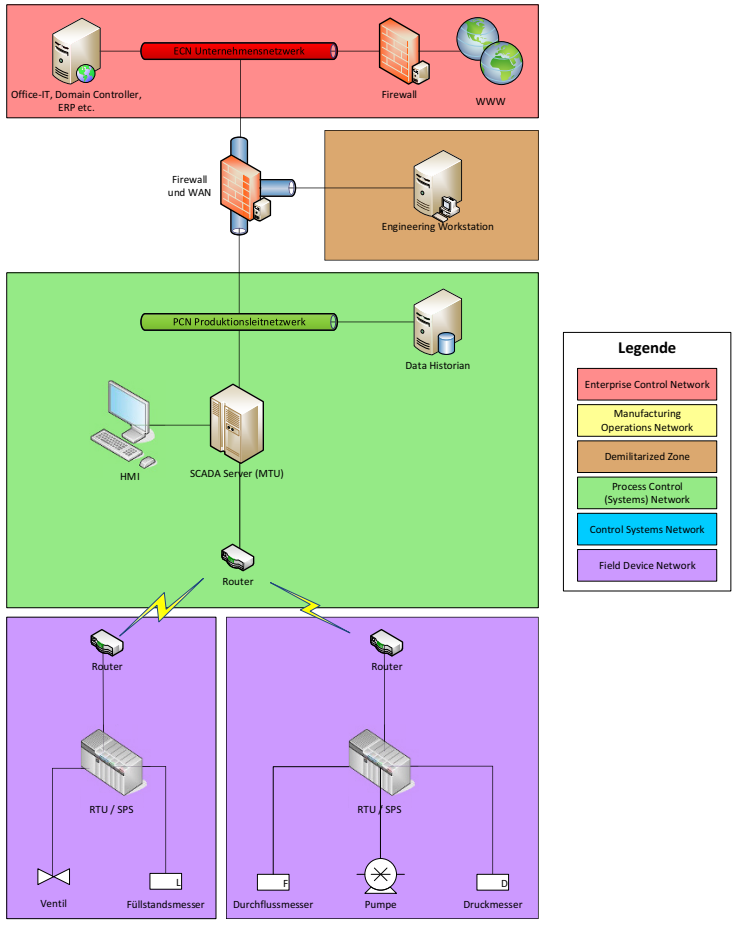

Abb. 4: Aufbau einer idealtypischen und zonierten SCADA-Kleinanlage

werden zentral verwaltet und gesteuert (s. Abbildung 5 sowie Anlage A.1 als Großdarstellung).[15] DCS ermöglichen es dem Anwender, direkt auf die Daten der Feldgeräte zuzugreifen, mit denen das System ständig verbunden ist.[16] DCS verfügen über eine dezentrale Struktur von Steuerungseinheiten wie SPS, in der jeder lokale Prozess von einem oder mehreren solcher Steuerungseinheiten eigenständig gesteuert und kontrolliert wird, die ihre Einstellungen und Anwendungen jedoch

15 Brown (2007), S. 357; Greeff und Ghoshal (2004), S. 35.
16 Greeff und Ghoshal (2004), S. 35.

von einer zentralen Datenbank erhalten und durch eine zentrale Prozessleitsoftware überwacht werden.[17]

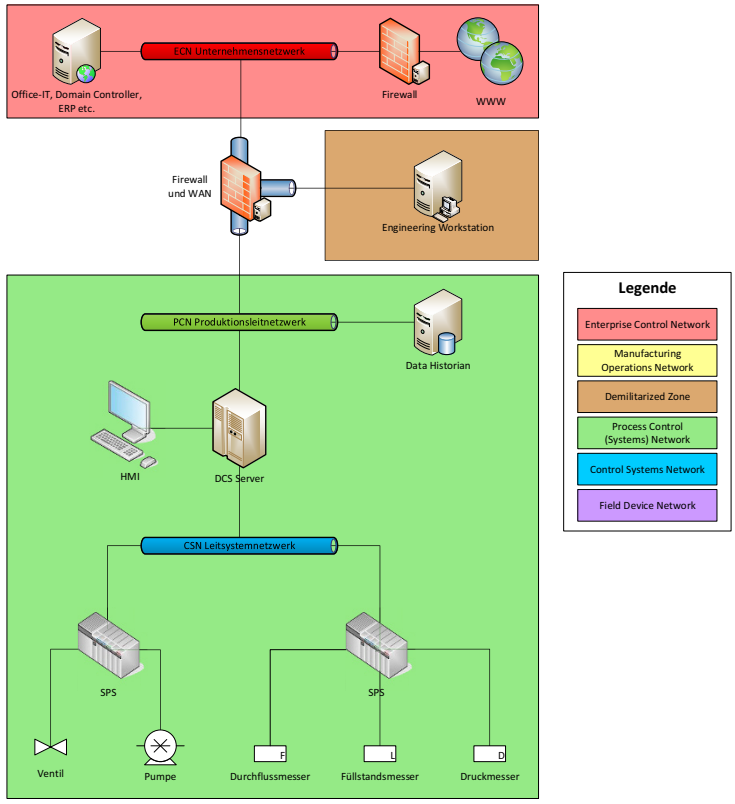

Abb. 5: Aufbau einer idealtypischen und zonierten DCS-Kleinanlage

Es ist grundsätzlich möglich, dass ein System sowohl SCADA- als auch DCS-Funktionalitäten abbildet, auch wenn dies in der Regel nur mit Abstrichen realisiert werden kann. In diesem Sinne werden in den letzten Jahren auch vermehrt hybride Steuerungssysteme (Hybrid Control Systems) entwickelt bzw. unter diesem Begriff geführt.[18] Existierende ICS-Architekturen werden zunehmend offener, integrierter und nach Wunsch erweiterbar, wodurch klare Zuordnungen oft

17 Macaulay und Singer (2011), S. 13-21; Greeff und Ghoshal (2004), S. 31-35.

18 Greeff und Ghoshal (2004), S. 35-36.

nicht leicht sind.[19] Zu dieser Entwicklung gehört auch, dass die Systeme vermehrt mit dem Internet verbunden werden, was als Grund für Sicherheitsbedenken bereits an anderer Stelle diskutiert wurde.[20]

Abgesehen von den unterschiedlichen Architekturen ist ein weiterer architektonischer Gesichtspunkt die Segmentierung und Zonierung von ICS-Netzwerken, womit mittlere oder größere Anlagen in vielfache (ggf. regionale) Netzwerkzellen unterteilt werden können (s. Abbildung 6).

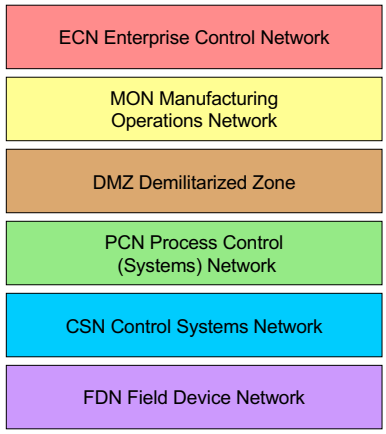

Abb. 6: Typische Netzwerksegmentierung von Industrieanlagen[21]

Bei kleineren Netzwerken sind verschiedene Netzwerkbereiche wie das Feldgerätenetzwerk (FDN), das Leitsystemnetzwerk (CSN) und das Produktionsleitnetzwerk (PCN) oft in einer einzigen Zone zusammengefasst, welche durch eine Accesspoint-Firewall von Unternehmensnetzwerk (ECN) getrennt und geschützt wird. Mittelgroße Anlagen verfügen oft noch über ein Perimeternetzwerk bzw. eine DMZ, die ggf. durch eine weitere Firewall geschützt wird. Es enthält beispielsweise Engineering Workstations oder zusätzliche Data Historians, da diese oft einen Zugang zu Medien oder Drittsystemen benötigen, etwa für das Einspielen von Updates oder das Auslesen der Daten. Anhand einer solchen Trennung zeigt sich auch, dass wichtige (digitale) Angriffskanäle in einer auf diese Weise abgesicherten Anlage entweder im Zugang zur Prozessleitebene oder aber direkt bei der

19 Greeff und Ghoshal (2004), S. 31.
20 Ebd., S. 32. Vgl. Abschnitt 2.2.
21 Vgl. IEC/ISO 62264:2008 (2008); IEC/ISA 62443:2013 (2015).

Sensorik liegen, also am eigentlichen Prozess.[22] Großanlagen verfügen darüber hinaus noch über weitere horizontale und vertikale Netzwerkzonen und -zellen, mit einer feingranularen Aufteilung von Aufgabenbereichen und einem gesonderten Netzwerk für Fertigungsabläufe.[23]

3.1 Ebene 1: Feldebene

Auf der Ebene der Prozessführung im Feld finden sich Komponenten und die dazugehörige Infrastruktur, die das Erfassen und Steuern der Zustände vor Ort zur Aufgabe haben, also des eigentlichen physischen Wertschöpfungsprozesses.[24] Hierzu gehören Sensoren wie Messwertaufnehmer, Endschalter, Grenztaster, Initiatoren oder andere Komponenten zur Erfassung physikalischer Größen ebenso wie Aktuatoren bzw. Aktoren, die Stellgrößen zur Beeinflussung des Prozessgeschehens verändern, wie etwa Pumpensteuerungen oder Antriebe. Darüber hinaus gibt es mit speziellen IEDs und der Analytik (Process Analytical Technology, PAT) auch Feldgeräte, die der Analyse, Kontrolle und Optimierung von Produktionsprozessen dienen, sowie Safetys zur Absicherung der Produktionsprozesse.[25]

Prozessdatensignale werden auf der Feldebene in Echtzeit übertragen, was bedeutet, dass eine Störung der Signalübertragung zu Störungen im Produktionsprozess führt.[26]

3.2 Ebene 2: Steuerungsebene

Auf der Steuerungsebene (auch: „Prozessführung Real Time“[27]) sind jene prozessnahen Komponenten angesiedelt, welche die Signalverarbeitung und -steuerung der Feldebene zur Aufgabe haben. Auch auf dieser Ebene muss eine vordefinierte

22 Die sog. Side-Channel- und Control-Channel-Attacken. Vgl. McLaughlin u. a. (2016), S. 1042 ff. Vgl. IEC/ISA 62443-1-1:2007 (2007), S. 70, wo in diesem Zusammenhang stattdessen von Communication Channels die Rede ist.

23 Siemens (2008), S. 43-53.

24 Hering, Vogt und Bressler (2013), S. 455.

25 Bundesamt für Sicherheit in der Informationstechnik (2013), S. 13-18; vgl. Ghosh (2006), S. 1003. Es gibt jedoch auch Safetys und IEDs, die eher auf der Steuerungsebene anzusiedeln sind.

26 Vgl. Bundesamt für Sicherheit in der Informationstechnik (2013), S. 19.

27 Ebd., S. 19.

Reaktionszeit gewährleistet werden, denn Abweichungen führen zu Störungen im Produktionsprozess.[28]

Die am weitesten verbreitete Steuerungstechnik für diese Zwecke ist die Speicherprogrammierbare Steuerung (SPS, engl.: Programmable Logic Controller).[29] SPSs empfangen Daten der Sensorik und steuern die Aktorik durch empfangene Befehle oder programmierte Automatismen. Informationen werden von den SPS an das eingesetzte Prozessleitsystem weitergeleitet, von wo aus auch auf die SPS zugegriffen werden kann.[30] Typischerweise kommen SPS in DCS zum Einsatz, sind aber auch in SCADA-Systemen keine Seltenheit.[31] Vermehrt werden auch Slot-SPS oder Soft-SPS-Lösungen genutzt, bei denen eine softwarebasierte SPS oder Hardware-Erweiterungskarte auf einem handelsüblichen, dezidierten PC läuft. Diese können über die eigentlichen SPS-Funktionen hinaus noch über weitere Funktionen verfügen.[32] Neuere SPSs verfügen teilweise auch über eine computergestützte Benutzerschnittstelle (HMI), auf welche insbesondere bei SCADA-Architekturen direkt zugegriffen werden kann.[33]

Neben bzw. in Verbindung mit SPS können auch RTUs (Remote Terminal Unit, dt.: Fernbedienungsterminal) in Industrieanlagen zum Einsatz kommen. RTUs werden vor allem in räumlich verteilten Anlagen (z.B. SCADA-Systemen) als Fernwirktechnik genutzt, um Daten und Befehle zwischen einer Verarbeitungseinheit der Feldebene und einer MTU zu übertragen, ggf. nach vorheriger Signalvorverarbeitung. Dabei können sie ggf. auch automatisch agieren (sog. „Intelligent RTUs“).[34] Je nach Systemarchitektur können RTUs jedoch auch mit SPS kommunizieren oder direkt mit der Prozessleitebene verbunden sein.[35] Klassische RTUs sind heutzutage jedoch immer weniger verbreitet, da sie im Gegensatz zu SPS nur schlecht programmierbar sind.[36]

Neuere Komponenten der Steuerungstechnik vereinen oft diese verschiedenen Funktionalitäten, weswegen Abgrenzungen und Zuordnungen von Komponenten schwierig sein können.[37] In diesem Zusammenhang werden auch auf der Steuerungsebene IEDs (Intelligent Electronic Device) teils als eigenständige Kompo-

28 Bundesamt für Sicherheit in der Informationstechnik (2013), S. 19.

29 Plaßmann und Schulz (2016), S. 643.

30 Sosinsky (2009), S. 309.

31 Lewis (2014), S. 223.

32 Wellenreuther und Zastrow (2005), S. 5; Greeff und Ghoshal (2004), S. 30.

33 Totherow (2006), S. 790-791.

34 Bundesamt für Sicherheit in der Informationstechnik (2013), S. 14-19; Moss (2012), S. 9-10; Greeff und Ghoshal (2004), S. 32; Lewis (2014), S. 223.

35 Knapp und Langill (2014), S. 63.

36 Sosinsky (2009), S. 310-311.

37 Sosinsky (2009), S. 311; vgl. Knapp und Langill (2014), S. 91.

nentenklasse beschrieben. Sie sind jedoch nicht eindeutig zu definieren: „[An IED is] any device incorporating one or more processors with the capability to receive or send data/control from or to an external source [...].“[38] IEDs verfügen über unterschiedliche und vielfältige Funktionalitäten, welche auf der Steuerungsebene oft die Eigenschaften von SPS und RTU kombinieren, teilweise in Verbindung mit Funktionen von Feldgeräten oder auch Benutzerschnittstellen. Sie stellen in der Regel eine Teilmenge der fünf Funktionalitäten Absicherung, Steuerung, Überwachung, Messung und Kommunikation zur Verfügung.[39] Je nach Definition fallen unter IED noch weitere Komponentenklassen, welche jedoch teilweise auch als eigenständige Gruppen gesehen werden. So gibt es auch in der Sicherheitstechnik Safety-Komponenten, die nicht (nur) der Feldebene zugeordnet werden, sondern aufgrund ihrer in unterschiedlichen Ausführungen erweiterten Funktionalitäten auch in der Steuerungsebene angesiedelt sein können.[40] Auch können hier CIF-Komponenten (Control in the Field) genannt werden, womit Automatisierungsfunktionen direkt in den Feldgeräten implementiert werden und die insofern sowohl der Feldebene als auch der Steuerungsebene zugeordnet werden können. Sie werden ggf. als IEDs kategorisiert.[41]

3.3 Ebene 3: Prozessleitebene

Auf der Prozessleitebene der Prozessführung befinden sich Komponenten und Anwendungen, mit denen der Anwender vor allem Anzeige- und Bedienfunktionen des Gesamtsystems wahrnehmen und somit auf die Feld- und Steuerungsebene zugreifen kann.[42]

Die zentrale Anwendung für die Anzeige- und Bedienfunktionen des Gesamtsystems ist die Prozessleitsoftware des DCS oder des SCADA-Systems. Sie wird über eine HMI an einer Operator Workstation dargestellt und läuft heutzutage in der Regel auf einem System mit einem üblichen Betriebssystem (s. Abbildung 7).[43] In einem DCS kann eine zentrale HMI bzw. Prozessleitsoftware idealtypisch

38 McDonald (2016), S. 7-2.

39 Sullivan, Luiijf und Colbert (2016), S. 19-20.

40 Strassburger, Schmidgall und Haasis (2003), S. 47 ff.; Campbell, Wendt und Friedmann (2006), S. 971; Beard, Lipták und Girão (2006), S. 1121; Ghosh (2006), S. 1003.

41 Bundesamt für Sicherheit in der Informationstechnik (2013), S. 19.

42 Queiroz u. a. (2009), S. 361; Bundesamt für Sicherheit in der Informationstechnik (2013), S. 14-20.

43 Sosinsky (2009), S. 311; Knapp und Langill (2014), S. 94; Totherow (2006), S. 94. Seltener werden auch Kommandozeilen zu diesem Zweck eingesetzt. Deutlich ältere HMI verfüg-

unmittelbar im Kontrollraum genutzt werden, während ein SCADA-System über einen oder mehrere MTU-(Sub-)Server mit jeweils eigener HMI bzw. Prozessleitsoftware verfügen kann, die durch weitere Anwendungen in ihren Funktionalitäten zusammengeführt oder ergänzt werden können.[44] In moderner HMI bzw. Prozessleitsoftware werden diese unterschiedlichen Architekturen immer mehr kombiniert und selektiv eingesetzt.[45]

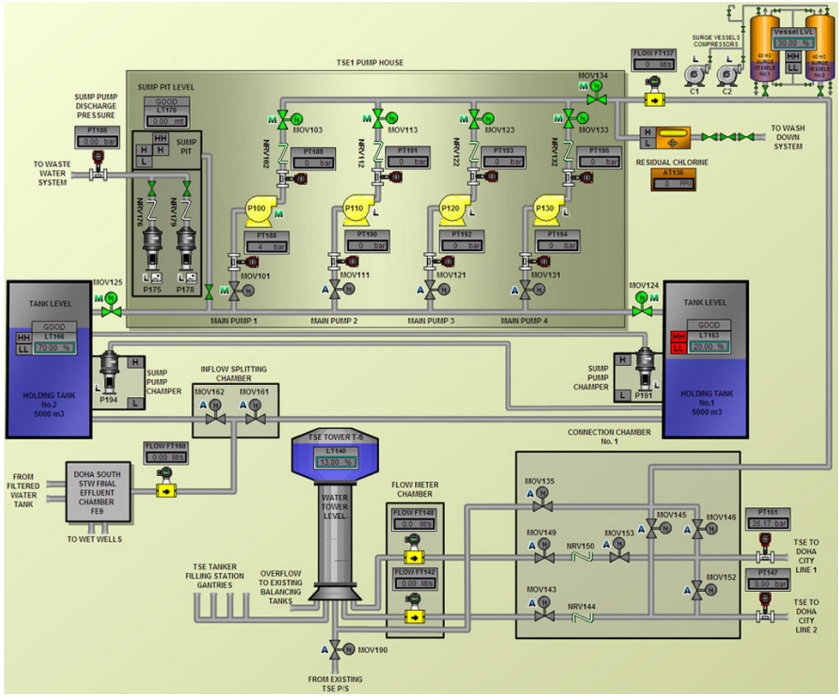

Abb. 7: Beispielhafte Prozessvisualisierung einer Benutzerschnittstelle

Moderne Prozessleitsoftware hat neben der Visualisierung, Steuerung, Überwachung und Auswertung der Anlagenprozesse oft weitere Funktionalitäten, wie Ar-

ten über manuelle Steuerungen und kein Display. Der Begriff des HMI wird in der Regel als Synonym für die jeweils verwendete Steuerungs- und Überwachungs- bzw. Prozessleitsoftware verwendet.

44 Totherow (2006), S. 796-798. Prozessleitsysteme bzw. Prozessleitsoftware und HMI werden SCADA-Systemen nach dem Client-Server-Prinzip aufgebaut und sind auch als „Open HMI“ oder „Offene PLS“ bekannt.

45 Totherow (2006), S. 797-803; Greeff und Ghoshal (2004), S. 35-36.

chivierungsdienste oder Fernwartungsfunktionalitäten.[46] So können sie etwa auch der Automatisierung von Prozessen dienen. Sie ist für die Prozessführung notwendig, verarbeitet Daten jedoch nicht in Echtzeit. Obwohl Verfügbarkeit und Zeitverhalten der Komponenten dieser Ebene daher teilweise weniger kritisch sind, sind Sicherheitsvorfälle mittelbar dennoch auch für die Produktionsprozesse riskant, da sie mit den Feld- und Steuerungsebenen interagieren.[47]

Weitere Komponenten zur Prozessführung, die auf dieser Ebene zu verorten sind und die Prozessleitsoftware ergänzen können, sind beispielsweise Engineering Workstations oder Data Historians.[48] Ein Data Historian läuft typischerweise auf einer Supervisory Workstation oder Application Workstation. Diese Anwendung ist eine Messwert- und Prozessdatenarchivierungssoftware, die die Werte der Feld- und Steuerungsebene sammelt und in einer Historian Database archiviert, einer Datenbank auf einem Archivserver.[49] Eine Engineering Workstation ist typischerweise ein Desktop-System oder ein Server mit einem üblichen Betriebssystem wie Linux oder Windows. Ingenieure bzw. Anwender können die Workstation nutzen, um etwa Änderungen an Steuerungen, Steuerungslogiken und industriellen Anwendungen durchzuführen oder Firmware-Modifikationen auf Speicherkarten zu übertragen. Die hierfür notwendigen Anwendungen und Daten sind auf der Workstation hinterlegt.[50] Da hierfür oft Medien wie USB-Sticks oder Internetzugänge genutzt werden, werden solche Workstations im Idealfall vom Produktionsleitnetzwerk getrennt und sind beispielsweise in einer DMZ zu verorten.

3.4 Ebene 4 und 5: Betriebsebene und Unternehmensebene

In der Betriebsführung und der Produktionsführung auf Unternehmensebene werden Komponenten und Anwendungen eingesetzt, die der Office-IT zuzuordnen und nicht mehr im engeren Sinne Teil der Betriebs- und Steuerungstechnik sind.[51]

Auf der Ebene 4 kommen Komponenten und Anwendungen der Betriebsführung zum Einsatz. Hierzu gehören Manufacturing Execution Systeme (MES), die die Informationen der Produktionsprozesse mit der betriebswirtschaftlichen Datenverarbeitung verbinden. Ebenso dazugezählt werden Anwendungen aus den Be-

46 Totherow (2006), S. 790-791.
47 Bundesamt für Sicherheit in der Informationstechnik (2013), S. 19.
48 Ebd., S. 20.
49 Knapp und Langill (2014), S. 94-95.
50 Sullivan, Luiijf und Colbert (2016), S. 20; Singh und Lipták (2006), S. 869.
51 Lass und Fuhr (2013), S. 30.

reichen Engineering/Planung, mit denen technische Dokumentationen erstellt und gepflegt oder Analysen durchgeführt werden können, sowie die lokale Office-IT.[52]

Anwendungen der Produktionsführung werden auf der Ebene 5 genutzt, um die unternehmensweite Betriebsorganisation zu unterstützen, wozu eine ERP-Anbindung ebenso gehört wie normale Zugänge zum betrieblichen Intranet oder Internet sowie zu betrieblichen Anwendungssystemen.[53]

3.5 Netzwerkkomponenten

Neben der eigentlichen Betriebs- und Steuerungstechnik werden unterschiedliche Netzwerkkomponenten eingesetzt, welche über die Ebenen der Automatisierungspyramide hinweg eingesetzt werden. Sie sind für die Kommunikation und Sicherheit einer Industrieanlage wichtig, weswegen sie an dieser Stelle überblicksartig beschrieben werden.

Neben elektrotechnischer und IT-Verkabelung gehören hierzu vor allem Komponenten wie Hard- oder Software-Firewalls, Hard- oder Software-IDS/IPS, Router, Switches, Modems und andere Komponenten der Fernwirktechnik sowie Domain-Controller.[54] Auch diese Anlagenkomponenten können für die Sicherheit einer Anlage außerordentlich wichtig sein.

Literaturverzeichnis

Beard, C. S., B. Lipták und P. M. B. S. Girão (2006), Actuators: Digital, Electric, Hydraulic, Solenoid, in: B. Lipták (Hrsg.), *Instrument Engineers' Handbook: Process Control and Optimization*, 4. Aufl., Bd. 2, CRC Press.

Birkhold, M. und J. Bauer (2014), *Sicherheit in der Automatisierungstechnik nach BSI IT-Grundschutz, geht das?*, Vortrag, URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Veranstaltungen/Grundschutz/1GS_Tag_2014/02_1_IT-Grund_2014_Birkhold.pdf?__blob=publicationFile (besucht am: 20. 12. 2017).

52 Bundesamt für Sicherheit in der Informationstechnik (2013), S. 20.

53 Ebd., S. 20-21.

54 Liao u. a. (2013), S. 21-2.

Brown, R. (2007), SCADA and DCS Vulnerabilities and Counter-Measures for Engineers, Technicians and IT-Staff, in: B. L. Capehart und L. C. Capehart (Hrsg.), *Web based enterprise energy and building automation systems*, The Fairmont Press, Inc.

BSI IT-Grundschutz-Kompendium (2017), *IND.1 Betriebs- und Steuerungstechnik*.

BSI-Standard 200-2 (2017), *IT-Grundschutz-Methodik – Community Draft*.

Bundesamt für Sicherheit in der Informationstechnik (2013), *ICS-Security-Kompendium*.

Campbell, B. D., C. W. Wendt und P. G. Friedmann (2006), PLC Software Advances, in: B. Lipták (Hrsg.), *Instrument Engineers' Handbook: Process Control and Optimization*, 4. Aufl., Bd. 2, CRC Press.

Chabukswar, R. u. a. (2010), Simulation of Network Attacks on SCADA Systems, in: *First Workshop on Secure Control Systems*.

Christiansson, H. und E. Luiijf (2008), Creating a European SCADA security testbed, in: E. Goetz und S. Shenoi (Hrsg.), *International Conference on Critical Infrastructure Protection, 1st IFIP WG 11.10 International Conference, ICCIP 2007, New Hampshire, USA, Revised Selected Papers*, Springer, 237–247.

Früh, K. F. (2009), *Handbuch der Prozessautomatisierung: Prozessleittechnik für verfahrenstechnische Anlagen*, Oldenbourg Industrieverlag.

Ghosh, A. (2006), Programmable Safety Systems, in: B. Lipták (Hrsg.), *Instrument Engineers' Handbook: Process Control and Optimization*, 4. Aufl., Bd. 2, CRC Press.

Greeff, G. und R. Ghoshal (2004), *Practical E-manufacturing and supply chain management*, Newnes.

Hering, E., A. Vogt und K. Bressler (2013), *Handbuch der elektrischen Anlagen und Maschinen*, Springer-Verlag.

Hoeppner, C. H. u. a. (2006), Telemetering Systems, in: B. Lipták (Hrsg.), *Instrument Engineers' Handbook: Process Control and Optimization*, 4. Aufl., Bd. 2, CRC Press.

IEC/ISA 62443-1-1:2007 (2007), *Security for Industrial Automation and Control Systems – Part 1: Terminology, Concepts, and Models*.

IEC/ISA 62443:2013 (2015), *Industrielle Kommunikationsnetze – IT-Sicherheit für Netze und Systeme*.

IEC/ISO 62264:2008 (2008), *Enterprise-control system integration*.

Knapp, E. D. und J. T. Langill (2014), *Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems*, Syngress.

Lass, S. und D. Fuhr (2013), IT-Sicherheit in der Fabrik, in: *Productivity Management*, 18:2.

Lass, S. und D. Kotarski (2014), IT-Sicherheit als besondere Herausforderung von Industrie 4.0, in: W. Kersten, H. Koller und H. Lödding (Hrsg.), *Schriftenreihe der Hochschulgruppe für Arbeits- und Betriebsorganisation e.V. (HAB): Industrie 4.0 – Wie intelligente Vernetzung und kognitive Systeme unsere Arbeit verändern Schriftenreihe der Hochschulgruppe für Arbeits- und Betriebsorganisation*, Gito Verlag Berlin, 397–419.

Lerch, R. (2012), *Elektrische Messtechnik: Analoge, digitale und computergestützte Verfahren*, 6. Aufl., SpringerVieweg.

Lewis, T. G. (2014), *Critical infrastructure protection in homeland security: defending a networked nation*, John Wiley & Sons.

Liao, H.-J. u. a. (2013), Intrusion detection system: A comprehensive review, in: *Journal of Network and Computer Applications*, 36:1, 16–24.

Litz, L. (2013), *Grundlagen der Automatisierungstechnik: Regelungssysteme – Steuerungssysteme – hybride Systeme*, Walter de Gruyter.

Macaulay, T. und B. L. Singer (2011), *Cybersecurity for industrial control systems: SCADA, DCS, PLC, HMI, and SIS*, CRC Press.

McDonald, J. D. (2016), *Electric Power Substations Engineering*, 2. Aufl., CRC Press.

McLaughlin, S. u. a. (2016), The cybersecurity landscape in industrial control systems, in: *Proceedings of the IEEE*, 104:5, 1039–1057.

Moss, K. T. (2012), *Water treatment and distribution simulation for a SCADA security testbed*, Electronic Theses and Dissertations, Paper 1013, University of Louisville.

National Institute of Standards and Technology (2015), *NIST Special Publication 800-82, Revision 2: Guide to industrial control systems (ICS) security – supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as programmable logic controllers (PLC)*.

Plaßmann, W. und D. Schulz (2016), *Handbuch Elektrotechnik: Grundlagen und Anwendungen für Elektrotechniker*, 6. Aufl., Springer-Verlag.

Queiroz, C. u. a. (2009), Building a SCADA security testbed, in: *Network and System Security, 2009. NSS'09. Third International Conference on*, IEEE, 357–364.

Siemens (2008), *SIMATIC Sicherheitskonzept: PCS 7 und WinCC – Basisdokument – Whitepaper*.

Singh, G. B. und B. G. Lipták (2006), Workstation Designs, in: B. Lipták (Hrsg.), *Instrument Engineers' Handbook: Process Control and Optimization*, 4. Aufl., Bd. 2, CRC Press.

Sosinsky, B. (2009), *Networking bible*, Bd. 567, John Wiley & Sons.

Strassburger, S., G. Schmidgall und S. Haasis (2003), Distributed manufacturing simulation as an enabling technology for the digital factory, in: *Journal of Advanced Manufacturing Systems*, 2:1, 111–126.

Sullivan, D., E. Luiijf und E. J. Colbert (2016), Components of Industrial Control Systems, in: E. J. Colbert und A. Kott (Hrsg.), *Cyber-security of SCADA and Other Industrial Control Systems*, Springer, 15–28.

Totherow, G. K. (2006), Human-Machine Interface Evolution, in: B. Lipták (Hrsg.), *Instrument Engineers' Handbook: Process Control and Optimization*, 4. Aufl., Bd. 2, CRC Press.

Wellenreuther, G. und D. Zastrow (2005), *Automatisieren mit SPS: Theorie und Praxis*, Springer-Verlag.

Kapitel 4
Hybride Testumgebungen in der Informationssicherheit: Effiziente Sicherheitsanalysen für Industrieanlagen

In diesem Kapitel wird die hybride Testumgebung im Kontext des Informationssicherheitsmanagements näher betrachtet. Es wird hierfür zunächst ein Überblick über den Informationssicherheitsprozess nach der IT-Grundschutz-Methodik gegeben, die als effiziente Vorgehensweise insbesondere für KRITIS-Betreiber oder KMU relevant ist und einen Rahmen zur Nutzung von hybriden Testumgebungen bilden kann. Hierauf aufbauend können Testumgebungen in der Sicherheitskonzeption etwa bei der Durchführung von ergänzenden Sicherheitsanalysen in Form von Penetrationstests zum Einsatz kommen. Die hybride Testumgebung wird an dieser Stelle als besonders effiziente Testumgebung eingeordnet und vorgestellt.

4.1 Betriebs- und Steuerungstechnik im Informationssicherheitsmanagement nach IT-Grundschutz

Von internationalen Standards und ausländischen Handreichungen bis hin zu Standards aus dem deutschsprachigen Raum gibt es eine große Vielfalt an Standards oder Quasi-Standards der Informationssicherheit. Sie befassen sich etwa mit der Implementation eines Informationssicherheitssystems und den unterschiedlichen Elementen des Informationssicherheitsmanagements. Die gängigen Best-Practice-Beispiele, Methoden und Standards unterscheiden sich im Hinblick auf den Informationssicherheitsprozess jedoch nur geringfügig.[1] Allerdings sind sie oft nicht ohne Weiteres auf ICS übertragbar bzw. behandeln ICS nur teilweise.[2] In der Einordnung von Betriebs- und Steuerungstechnik in den Informationssicherheitsprozess wird sich im Folgenden an der IT-Grundschutz-Methodik und den entsprechenden Standards des BSI orientiert. Dies hat vor allem zwei Gründe: Zu-

1 Bundesamt für Sicherheit in der Informationstechnik (2013), S. 37-52; Bundesamt für Sicherheit in der Informationstechnik (2015), S. 93 ff.; BSI-Standard 200-2 (2017), S. 37.

2 Lass und Fuhr (2013), S. 30.

O. Leps, *Hybride Testumgebungen für Kritische Infrastrukturen*,
https://doi.org/10.1007/978-3-658-22614-5_4

nächst sind die BSI-Standards sowohl mit Blick auf die rechtlichen und verbandlichen Anforderungen als auch im Kontext des deutschsprachigen Bezugsrahmens von offenkundig großer Bedeutung.[3] Wichtiger jedoch wiegt die Tatsache, dass die Standards des BSI eine praxisnahe Ableitung von Methoden aus der Reihe der IEC-/ISO-Standards der 27xxx-Serie sind, die den Arbeitsaufwand reduzieren sollen. Es werden entsprechend konkrete Methoden beschrieben und geeignete Sicherheitsmaßnahmen vorgeschlagen.[4] Zudem beinhaltet das IT-Grundschutz-Kompendium in seiner neuesten Fassung Bausteine für alle Bereiche einer Institution, eingeschlossen Komponenten aus dem Bereich ICS.[5] Dieser Anspruch passt deshalb zur Zielstellung der vorliegenden Ausarbeitung im Hinblick auf ressourcenschwächere kleine und mittelgroße KRITIS-Betreiber.

Das ISMS in einer Organisation ist der Teil des Managementsystems, der sich mit der Informationssicherheit beschäftigt. Hier werden die Instrumente, Dokumente und Methoden festgelegt, die in den Aufgaben und Aktivitäten der Informationssicherheit zum Tragen kommen. Ein ISMS zielt letztlich darauf ab, mit technischen, organisatorischen und personellen Maßnahmen die Informationssicherheit zu gewährleisten.[6] Die Sicherheitsstrategie zum Erreichen von Sicherheitszielen wird dabei durch die Informationssicherheitsorganisation und das Sicherheitskonzept im Rahmen des kontinuierlichen Informationssicherheitsprozesses umgesetzt. Die Leitungsebene muss diesen Informationssicherheitsprozess initiieren, steuern, unterstützen und kontrollieren.[7] Während in der Informationssicherheitsorganisation Regeln, Anweisungen, Prozesse, Abläufe und Strukturen festgehalten werden, werden im Sicherheitskonzept Risikobewertungen und Sicherheitsmaßnahmen vorgenommen. Alle Elemente des ISMS folgen dem PDCA-Modell und unterliegen nach der initialen Planung und Umsetzung regelmäßigen Überprüfungs- und ggf. Optimierungszyklen (s. Abbildung 8). Informationssicherheit ist ein fortlaufender Prozess.[8]

Ein Teil des ISMS, der für die Anlagensicherheit wichtig ist, ist die Ermittlung von Rahmenbedingungen und Formulierung von allgemeinen Informationssicherheitszielen. Diese leiten sich beispielsweise aus den Geschäftszielen, gesetzlichen Vorgaben und wesentlichen Geschäftsprozessen ab. Auch ist zu ermit-

3 Wegener, Milde und Dolle (2016), S. 192.

4 BSI-Standard 200-1 (2017), S. 11-13; BSI-Standard 200-1 (2017), S. 30; BSI-Standard 200-2 (2017), S. 8.

5 BSI-Standard 200-2 (2017), S. 9.

6 Schmölzer (2010), S. 5.

7 BSI-Standard 200-1 (2017), S. 15-16; ISO/IEC 27000:2016(E) (2016), S. 14; BSI-Standard 200-2 (2017), S. 15-16.

8 BSI-Standard 200-1 (2017), S. 15-16, S. 23; BSI-Standard 200-2 (2017), S. 131-137; BSI-Standard 200-3 (2016), S. 7.

Abb. 8: Phasen des Informationssicherheitsprozesses. Abbildung nach BSI-Standard 200-2 (2017), S. 16; mit freundlicher Genehmigung des © Bundesamtes für Sicherheit in der Informationstechnik (2017)

teln, welche Informationen besonders wichtig und damit besonders schützenswert sind, um im späteren Verlauf ein angemessenes Sicherheitsniveau, Sicherheitsanforderungen und schließlich auch den Schutzbedarf zu bestimmen. Insbesondere für einzelne, besonders hervorgehobene Bereiche einer Institution kann hier das angestrebte Sicherheitsniveau dargestellt werden.[9] Zu den gesetzlich festgelegten Schutz- und Sicherheitszielen gehört in der Wasserversorgung zum Beispiel

[9] BSI-Standard 200-2 (2017), S. 21-24, S. 87-104.

die Gewährleistung der Versorgungssicherheit und der Versorgungsqualität.[10] Für Wasserversorger sind deswegen die Geschäftsprozesse der Wasserversorgung von großer Bedeutung, welche sich in folgende drei Teilprozesse aufteilen lassen: Wassergewinnung, Wasseraufbereitung und Wasserverteilung.[11] Je nach Intensität des IT-Einsatzes können hier keine oder nur geringe Ausfallzeiten toleriert werden.[12] Zwar variieren Anlagen der Wasserversorgung sehr stark in ihrem Aufbau, weswegen allgemeingültige Aussagen zum angemessenen Sicherheitsniveau dieser Geschäftsprozesse nur schwer möglich sind.[13] Dennoch kann grundsätzlich davon ausgegangen werden, dass ein erhöhtes bzw. hohes oder sehr hohes Sicherheitsniveau dieser Geschäftsprozesse angemessen und erstrebenswert ist und diese Geschäftsprozesse im weiteren Verlauf des Informationssicherheitsprozesses auch als kritische Assets („Kronjuwelen“) mit erhöhtem Schutzbedarf besondere Beachtung finden müssen.[14]

Nach der Initiierung des Informationssicherheitsprozesses durch die Leitungsebene sowie der Definition von Sicherheitsleitlinien für die Informationssicherheitsorganisation wird die Sicherheitskonzeption für die Institution erstellt und umgesetzt. Solche Sicherheitskonzepte können für die Modellierung und Implementierung von Testumgebungen von besonderem Nutzen sein. Grundsätzlich wird der Informationssicherheitsprozess auch nach initialer Erstellung der Sicherheitskonzeption im Rahmen des Informationssicherheitsmanagements aufrechterhalten und regelmäßig auf Angemessenheit und Wirksamkeit überprüft, um eine kontinuierliche Absicherung zu gewährleisten.[15]

---

10 Vgl. TrinkwV (2017), *Trinkwasserverordnung in der Fassung der Bekanntmachung vom 10. März 2016 (BGBl. I S. 459), die zuletzt durch Artikel 2 des Gesetzes vom 17. Juli 2017 (BGBl. I S. 2615) geändert worden ist*; vgl. BSI-KritisV (2016), *Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung – BSI-KritisV)*; vgl. BSI-Gesetz (2017), *Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG) vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 1 des Gesetzes vom 23. Juni 2017 (BGBl. I S. 1885) geändert worden ist*.

11 Bundesamt für Sicherheit in der Informationstechnik (2015), S. 34.

12 BSI-Standard 200-2 (2017), S. 24.

13 Karger und Hoffmann (2013), S. 1-3; BSI IT-Grundschutz-Kompendium (2017), S. 2-4.

14 Fritsch u. a. (2014), S. 296, S. 465, S. 758, S. 888-889; BSI-Standard 200-2 (2017), S. 63-67. Auch andere Geschäftsprozesse eines Wasserversorgers können hierunter fallen, zum Beispiel im Bereich des Finanzwesens. Da der Fokus dieser Arbeit jedoch auf dem Einsatz von hybriden Simulationen zum Schutz von ICS liegt, wird sich auf genannte Geschäftsprozesse konzentriert.

15 BSI-Standard 200-2 (2017), S. 17.

4.2 ICS in der Sicherheitskonzeption nach IT-Grundschutz

Die Sicherheitskonzeption ist eine zentrale Aufgabe des Informationssicherheitsmanagements. In der Sicherheitskonzeption wird im Wesentlichen ein Soll-Ist-Vergleich zwischen den Sicherheitsanforderungen und den bereits realisierten Maßnahmen durchgeführt, woraufhin möglichen Sicherheitsdefiziten mit Sicherheitsmaßnahmen begegnet werden kann.[16]

Der Arbeitsaufwand für die Erstellung des Sicherheitskonzeptes hängt entscheidend von der Methodenauswahl ab.[17] Eine vollumfängliche klassische Sicherheitsanalyse kann in der Erstellung eines Sicherheitskonzeptes sehr teuer und aufwendig sein, da viele Szenarien in der schnelllebigen Welt der IT nur schwer fundiert und abschließend analysierbar sind.[18] Insbesondere im Hinblick auf KMU muss auch hier eine Abwägung zwischen den Sicherheitskosten und dem Nutzen bzw. den Risiken stattfinden. Hier kann vorrangig in Maßnahmen investiert werden, welche gegen besonders hohe Risiken schützen oder besonders effektiv sind.[19] Das Vorgehen nach IT-Grundschutz wird als weniger aufwendiges qualitatives Verfahren in der Praxis gerne genutzt, um zu einer allgemeinen Risikoeinschätzung zu kommen, woraufhin selektiv weitergehende Analysen oder Methoden genutzt werden können.[20] Ein Sicherheitskonzept besteht nach IT-Grundschutz-Methodik aus einer Risikobewertung in folgenden Schritten:

- Strukturanalyse
- Schutzbedarfsfeststellung
- Modellierung
- Basis- oder Standard-Sicherheitschecks sowie ggf. einer Kern-Absicherung samt der Auswahl, dem Abgleich und ggf. der Anpassung von Sicherheitsmaßnahmen
- Eine ergänzende Sicherheitsanalyse bei hohem und sehr hohem Schutzbedarf
- Umsetzung des Sicherheitskonzepts mithilfe eines Realisierungsplans[21]

Die im Sicherheitskonzept dokumentierten Erkenntnisse zu Risiken, Schwachstellen oder Optimierungspotential führen zu Konsequenzen im ISMS und fließen

16 Ebd., S. 17.

17 BSI-Standard 200-1 (2017), S. 30.

18 Schmölzer (2010), S. 6; BSI-Standard 200-1 (2017), S. 37-38.

19 BSI-Standard 200-1 (2017), S. 20.

20 ISO/IEC 27005:2008 (2008), S. 14; BSI-Standard 200-1 (2017), S. 30; BSI-Standard 200-2 (2017), S. 64.

21 BSI-Standard 200-2 (2017), S. 17-18; BSI-Standard 200-1 (2017), S. 31-33; BSI-Standard 200-3 (2016), S. 5; ISO/IEC 27000:2016(E) (2016), S. 18.

in die IS-Organisation ein.[22] Auf diese Weise kann angemessen auf Risiken reagiert werden, von der Risiko-Reduktion durch Sicherheits- und Gegenmaßnahmen über Risiko-Vermeidung, Risiko-Transfer bis hin zu Risiko-Akzeptanz.[23] Auch nach dem initialen Aufsetzen eines Sicherheitskonzeptes und Informationssicherheitsprozesses werden diese gemäß dem PDCA-Lebenszyklus überwacht, regelmäßig überprüft und fortlaufend aktualisiert.[24]

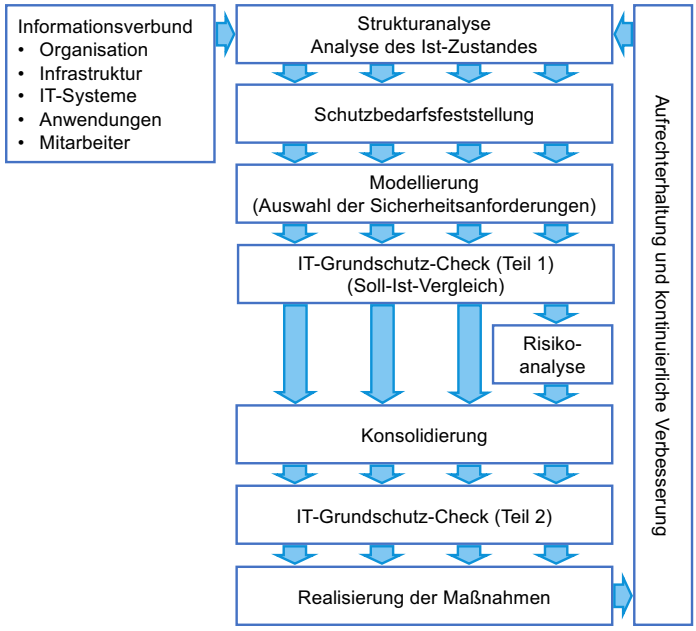

Abb. 9: Vorgehen der Kern- und Standard-Absicherung im Informationssicherheitsprozess nach IT-Grundschutz-Methodik. Abbildung nach BSI-Standard 200-2 (2017), S. 70; mit freundlicher Genehmigung des © Bundesamtes für Sicherheit in der Informationstechnik (2017)

Durch Rückgriff auf die IT-Grundschutz-Methodik kann ein Großteil des Informationssicherheitsprozesses aufwandsarm und zielgerichtet durchgeführt werden, weshalb das Vorgehen gerade für KMU geeignet ist. So werden Bausteine mit typischen Gefährdungen und Sicherheitsmaßnahmen für verschiedene organisationale Bereiche beschrieben, von übergeordneten Themen wie dem IS-Management

22 BSI-Standard 200-2 (2017), S. 131-136.

23 BSI-Standard 200-3 (2016), S. 28-39; BSI-Standard 200-2 (2017), S. 123-126; ISO/IEC 27000:2016(E) (2016), S. 18; Schmölzer (2010), S. 7.

24 BSI-Standard 200-2 (2017), S. 131-134.

bis zu speziellen Komponenten. Ebenso bietet es unterschiedliche Vorgehensweisen je nach gewünschtem Sicherheitsniveau oder Aufwand an, von der genannten „Basis-Absicherung“ als Grundniveau zur Vermeidung von fahrlässigem Sicherheitsgebaren über die „Standard-Absicherung“ für den normalen Schutzbedarf bis zur „Kern-Absicherung“ für besonders schützenswerte Geschäftsprozesse und Informationen (s. Abbildung 9).[25]

Zu Beginn der Erstellung des Sicherheitskonzepts wird eine Ersterfassung durchgeführt, sofern zuvor noch keine Strukturanalyse durchgeführt wurde. Ausgehend von den wesentlichen Geschäftsprozessen werden an dieser Stelle die Anwendungen, IT-Systeme, Netzkomponenten, ICS, Räume und ähnliche Objekte identifiziert und sinnvoll gruppiert.[26] Der Informationsverbund muss klar abgegrenzt sein und sollte kleingehalten werden, um die Komplexität der Absicherung zu reduzieren.[27] Infolge der Strukturanalyse kann der Geschäftsbetrieb bzw. können die Geschäftsprozesse anhand der Bausteine des IT-Grundschutz-Kompendiums modelliert werden und ein Sicherheitskonzept kann aus der Sammlung von Maßnahmenempfehlungen des BSI erstellt werden.[28] Im Rahmen der überarbeiteten IT-Grundschutz-Methodik des BSI-Standards 200-2 sind auch die Bausteine des IT-Grundschutz-Kompendiums überarbeitet und erweitert worden und umfassen nun zum Beispiel auch ICS- und IoT-Komponenten. Sofern Komponenten dennoch nicht über diese Bausteine abbildbar sind, müssen sie durch benutzerdefinierte Bausteine im Sicherheitskonzept erfasst werden.[29] Hierbei kann auch auf das ICS-Security-Kompendium zurückgegriffen werden.[30]

Insgesamt lässt sich sagen, dass die Basis- bzw. Standard-Absicherung ein bewährtes, vergleichbares und vereinfachtes Verfahren darstellt und der Schutz von ICS seit der Einführung von entsprechenden Bausteinen mit der BSI IT-Grundschutz-Methodik machbar ist.[31] Besonders schützenswerte Geschäftsprozesse und Informationen müssen im Sicherheitskonzept nach IT-Grundschutz mittels einer sog. Kern-Absicherung geschützt werden.[32] Bei der Kern-Absicherung wird sich vorrangig auf die besonders schützenswerten Assets („Kronjuwelen“)

25 Ebd., S. 8-9.
26 Ebd., S. 26.
27 Ebd., S. 64-65.
28 BSI-Standard 100-2 (2008), S. 36.
29 Vgl. Birkhold und Bauer (2014), S. 17.
30 Floß (2015), S. 9.
31 Vgl. Floß (2015), S. 29; vgl. Birkhold und Lechler (2014), S. 302-303.
32 BSI-Standard 200-2 (2017), S. 8-9. In der IT-Grundschutz-Methodik nach BSI 200-2 werden diese konsequent mit dem ungeschickten Begriff der „Kronjuwelen“ umschrieben.

einer Institution konzentriert.[33] Darüber hinaus kann mit den neu eingeführten IT-Grundschutz-Profilen ein speziell auf die Anwendergruppe der KRITIS-KMU zugeschnittene Herangehensweise erstellt werden. Für kleine und mittlere KRITIS-Betreiber mit begrenzten Ressourcen ist es einerseits denkbar, die Kern-Absicherung für besonders wichtige Geschäftsprozesse inkrementell, infolge einer vorherigen Standard- oder Basis-Absicherung durchzuführen. Andererseits kann die Kern-Absicherung auch als Einstiegsvorgehensweise genutzt werden, um prioritär zunächst die wichtigsten Versorgungs- und Verwaltungsprozesse abzusichern. Über längere Zeit können dann inkrementell einzelne Szenarien und Prozesse kostenbewusst abgesichert werden, wie es auch die Amerikanische Wasserwerkvereinigung AWWA vorschlägt.[34]

Einen erhöhten Schutzbedarf können insbesondere jene Geschäftsprozesse der Wasserversorgung haben, für die in Abschnitt 4.1 ein erhöhtes Sicherheitsniveau als Sicherheitsziel identifiziert wurde, was auf die gesetzlichen oder untergesetzlichen Vorgaben sowie die gesellschaftliche und betriebswirtschaftliche Bedeutung dieser Prozesse bei Wasserunternehmen zurückzuführen ist: Wassergewinnung, Wasseraufbereitung und Wasserverteilung.[35] Aus diesen Gründen wird auch der Schutzbedarf des Informationsverbunds um die hier zum Einsatz kommenden ICS im Hinblick auf den Grundwert der Verfügbarkeit in der Regel erhöht sein, denn Ausfälle der Wasserversorgung können im Ernstfall erhebliche Verstöße gegen Vorgaben darstellen, die Aufgabenerfüllung stark beeinträchtigen, das Image nachhaltig beschädigen sowie bedeutende finanzielle Verluste nach sich ziehen. Der Schutzbedarf wird durch die schwerwiegendsten Schäden bzw. Auswirkungen bestimmt.[36]

Für Zielobjekte der Kern-Absicherung müssen die Basis- und Standard-Anforderungen des IT-Grundschutz-Kompendiums zunächst komplett umgesetzt werden. Darauf aufbauend muss für diese Zielobjekte unter Beachtung von Kosten- und Wirksamkeitsaspekten des Weiteren geprüft werden, ob zusätzliche oder höherwertige Sicherheitsmaßnahmen erforderlich sind.[37] In solchen Fällen sollte bzw. – bei sehr hohem Schutzbedarf – muss eine ergänzende Sicherheitsanalyse durchgeführt werden, was mit einigem Aufwand verbunden sein kann.[38] Das BSI beschreibt im BSI-Standard 200-3 eine Risikoanalyse als aufwandsarme Methode

33 Vgl. BSI-Standard 200-2 (2017), S. 63-67, insb. für Charakteristika, die bei der Identifikation und Eingrenzung weiterer kritischer Assets helfen können.

34 BSI-Standard 200-2 (2017), S. 122; Thim und Kotarski (2015), S. 31.

35 Vgl. BSI-Standard 200-2 (2017), S. 88.

36 Vgl. BSI-Standard 200-2 (2017), S. 87-98; BSI-Standard 200-3 (2016), S. 4.

37 BSI-Standard 200-2 (2017), S. 63-64.

38 BSI-Standard 200-2 (2017), S. 122; Lass und Fuhr (2013), S. 31.

zur Durchführung einer ergänzenden Sicherheitsanalyse. Hierbei werden grundsätzlich alle elementaren Gefährdungen des IT-Grundschutzes als Ausgangsbasis betrachtet, ggf. weitere realistische und relevante Gefährdungen hinzugefügt und daraufhin qualitativ geprüft, ob sie auf das jeweilige Zielobjekt im Informationsverbund einwirken können.[39] Das BSI hat diese Methode im IT-Grundschutz verankert, da sie kostengünstiger bzw. aufwandsärmer ist als die Durchführung klassischer quantitativer Risikoanalysen. Sie kann diese entweder ersetzen oder kann zunächst durchgeführt werden, um zu entscheiden, ob noch weitergehende Sicherheitsanalysen durchgeführt werden sollen.[40] Je nach Anforderung und Zielstellung kann es zweckmäßig sein, die ergänzende Risikoanalyse durch weitere Verfahren zur Überprüfung der Informationssicherheit zu ergänzen oder diese direkt zu ersetzen.[41] Hierfür kommen, neben besagter Risikoanalyse, in der Regel vor allem Differenz-Sicherheitsanalysen, Schwachstellenanalysen oder Penetrationstests zum Einsatz. Bei der Differenz-Sicherheitsanalyse werden zusätzliche umgesetzte Sicherheitsmaßnahmen der Zielobjekte mit Sicherheitsmaßnahmen für ähnliche Objekte in anderen Organisationen und Umgebungen verglichen, um das Sicherheitsniveau zu überprüfen.[42] Penetrationstests und Schwachstellenanalysen werden meist von externen Experten durchgeführt, die unter Nutzung aller Werkzeuge und Methoden versuchen, die Systeme der jeweiligen Organisation anzugreifen oder Schwachstellen zu identifizieren. Gelingt dies, wird auf die jeweilige Sicherheitslücke reagiert.[43] Laut BSI sollten sicherheitskritische Netze und Systeme regelmäßig beispielsweise mittels Penetrationstests überprüft werden.[44] Gerade bei unterschiedlichen Rahmenbedingungen und technischen Schwerpunkten, wie es bei ICS von Kritischen Infrastrukturen der Fall ist, können weitere Sicherheitsanalysen wie Penetrationstests zum Einsatz kommen.[45] Dafür spricht, dass eine Überprüfung von hochkomplexen Systemen wie ICS aufgrund ihrer speziellen Anforderungen mit gängigen Mitteln wie der Risikoanalyse nach IT-Grundschutz nur eingeschränkt machbar ist.[46]

---

39 BSI-Standard 200-3 (2016), S. 12 ff.

40 Schmölzer (2010), S. 6; BSI-Standard 200-2 (2017), S. 123-124; BSI-Standard 200-1 (2017), S. 37-38.

41 BSI-Standard 200-3 (2016), S. 21 und S. 32; BSI-Standard 200-2 (2017), S. 124-125.

42 Dinger und Hartenstein (2008), S. 223-224.

43 Schumacher (2016), S. 677.

44 Bundesamt für Sicherheit in der Informationstechnik (2016), M 5.150 Durchführung von Penetrationstests, S. 4669.

45 BSI-Standard 200-3 (2016), S. 33; BSI-Standard 200-2 (2017), S. 125.

46 Schaumüller-Bichl und Kolberger (2016), S. 609-611; Kraft und Stöwer (2017), S. 89; Tews und Schlehuber (2014), S. 294; vgl. Kahneman und Tversky (1979).

Abhängig vom Szenario und den eingesetzten Methoden ist der Vorteil von Sicherheitsanalysen wie Schwachstellenanalysen und Penetrationstests, dass mit ihnen eine große Testtiefe erreicht werden kann. Es kann auf die Spezifika der im Einsatz befindlichen ICS-Anlagen eingegangen werden.[47] Klassische Penetrationstests erfolgen entweder per Simulation, was aufwendig und auch teuer sein kann und dennoch oft nur von begrenztem Nutzen ist, oder aber im laufenden Betrieb bzw. am Echtsystem. Letzteres kann jedoch aufgrund möglicher Konsequenzen im Hinblick auf ICS der Wasserversorgung gefährlich sein und sollte daher nur als weniger detailreicher passiver Penetrationstest erfolgen.[48] Die in den folgenden Abschnitten beschriebene hybride Testumgebung und die dazugehörige Vorgehensweise kann hier ein Lösungsansatz sein. Sie führt den Leitgedanken des IT-Grundschutzes fort und ist eine vergleichsweise aufwandsarme und kostengünstige Methode, mit der Sicherheitsanalysen realitätsnah durchgeführt werden können, ohne eine Beeinträchtigung des laufenden Betriebs zu riskieren. Diese Methode kann deshalb auch für kleine und mittelgroße KRITIS-Betreiber wie etwa Wasserversorger attraktiv sein. An dieser Stelle soll jedoch auch betont werden, dass cyber-physische Sicherheitsanalysen und hybride Testumgebungen nicht auf diese Einordnung und Anwendung im Rahmen des IT-Grundschutzes reduziert werden müssen. Sie können auch im Rahmen anderer Ansätze der Informationssicherheit oder für sich genommen genutzt werden, etwa als Reaktionen auf Sicherheitsvorfälle, bei Änderungen oder der Einführung neuer Komponenten oder schlicht, um den Formalismus von aufwendigen Informationssicherheitsstandards zu reduzieren. Cyber-physische Sicherheitsanalysen können in regelmäßigen Überprüfungen im Rahmen periodischer Risikobewertungen, in der Vorbereitung von Audits oder bei internen IS-Revisionen zum Einsatz kommen. Sie können aber auch zur Überprüfung der Effektivität und Effizienz von Sicherheitsmaßnahmen genutzt werden.[49]

---

47 Sowa, Duscha und Schreiber (2015), S. 154-155.

48 Christiansson und Luiijf (2008), S. 242; Queiroz u. a. (2009), S. 358; Bundesamt für Sicherheit in der Informationstechnik (2013), S. 106.

49 BSI-Standard 200-1 (2017), S. 30-35; BSI-Standard 200-2 (2017), S. 131-134; ISO/IEC 27000:2016(E) (2016), S. 53 ff.; Gurschler u. a. (2017), S. 27; vgl. Kersten, Reuter und Schröder (2013), S. 142-143; Sowa, Duscha und Schreiber (2015), S. 151 ff.

4.3 Testumgebungen zur Durchführung von ICS-Sicherheitsanalysen: Die Vorteile der hybriden Testumgebung

Aufgrund des oft besonders hohen Schutzbedarfs von Industrieanlagen können weitergehende Sicherheitsanalysen notwendig sein, etwa in Form von Penetrationstests oder Schwachstellenanalysen.[50] Insbesondere Penetrationstests sind ein beliebtes Mittel, um die Sicherheit von IT-Systemen im Betrieb zu testen und Schwachstellen offenzulegen. Da Angriffe auf ICS jedoch unmittelbare Konsequenzen nach sich ziehen könnten, können in solchen Fällen keine oder nur passive Angriffsmethoden auf das Echtsystem zum Tragen kommen.[51] Oftmals ist sogar die Nutzung von Tools für passive Sicherheitsanalysen nicht ohne Risiko. Beispielsweise sind in einer Studie zur Nutzung von Scanning-Tools in passiven Schwachstellenanalysen 18 % der SPS-Bausteine abgestürzt.[52]

Dennoch sind Sicherheitsanalysen des Gesamtsystems sowohl für die Gewährleistung der Sicherheit von Altsystemen als auch für die Überprüfung von geplanten Anlagen in realitätsnahen Umgebungen wichtig. Denn manche Gefährdungen kommen erst auf der Systemebene zu Tage, etwa wenn verschiedene Schwachstellen kombiniert ausgenutzt werden.[53] Aus diesen Gründen werden die im Folgenden beschriebenen Testumgebungen eingesetzt, um ohne Risiko beispielsweise Sicherheitsanalysen durchzuführen, aber auch für weitergehende Anwendungszwecke wie etwa Schulungsmaßnahmen.[54]

4.3.1 Simulationsansätze in klassischen Testumgebungen

Eine Simulation ist das „Nachbilden eines Systems mit seinen dynamischen Prozessen in einem experimentierfähigen Modell, um zu Erkenntnissen zu gelangen, die auf die Wirklichkeit übertragbar sind.“[55] In einem Simulationssystem werden

---

50 Bundesamt für Sicherheit in der Informationstechnik (2016), M 5.150 Durchführung von Penetrationstests, S. 4669; vgl. National Institute of Standards and Technology (2015), G-25.

51 Christiansson und Luiijf (2008), S. 242.

52 Holm u. a. (2015), S. 12.

53 Chabukswar u. a. (2010), S. 1; Urias und Van Leeuwen (2016), S. 258.

54 Holm u. a. (2015), S. 15.

55 Verein Deutscher Ingenieure (1993), *VDI-Richtlinie 3633, BI. 1: Simulation und Logistik-, Materialfluß- und Produktionssystemen, Beuth*; vgl. Shannon (1998), S. 7.

Elemente abgebildet, die in dem System agieren. Diese Entitäten haben individuelle Eigenschaften (Attribute), wie z.B. der Name, die Priorität oder die CPU-Zeit.[56] Ein Element bzw. Objekt kann durch ein oder mehrere Attribute charakterisiert sein, denen Werte zugeordnet sind. Dies sind entweder indikative Attribute, die das Objekt beschreiben, oder relationale Attribute, welche die Beziehung zwischen Objekten beschreiben.[57]

Simulationen werden in unterschiedlichen Branchen in vielfältigen Anwendungsbereichen genutzt, etwa in der Wissenschaft für die Analyse von komplexen ökologischen Systemen oder im technischen Bereich zur Analyse physikalischer Zusammenhänge im Maschinenbau.[58] In Produktionsprozessen können verschiedene Szenarien und Alternativen überprüft werden, ohne den tatsächlichen Betrieb zu stören.[59] Ebenso werden Testumgebungen zur Durchführung von Sicherheitsanalysen mithilfe von unterschiedlichen Arten von Simulationen realisiert.[60]

Industrieanlagen werden in Testumgebungen klassischerweise auf zwei Arten realisiert: Als physisches Modell (in Form einer Modellfabrik bzw. als prototypische Anlage) oder als computerbasierte Simulation.[61]

Eine Testumgebung auf Basis eines physischen Modells ist eine vereinfachte Abbildung eines tatsächlichen oder geplanten Systems unter Nutzung realer Hardware-Komponenten. Daher ist der Anwendungsbereich einer solchen Testumgebung vergleichsweise eingeschränkt. Die Anpassung der Testumgebung auf andere ähnliche, aber doch unterschiedliche Anlagen kann kosten- und ressourcenintensiv sein, alleine schon aufgrund der großen Anzahl an Elementen in der heterogenen und langlebigen Betriebs- und Steuerungstechnik.[62] IT- und ICS-Infrastrukturen können im KRITIS-Bereich selbst bei kleinen Wasserunternehmen eine hohe Komplexität aufweisen.[63] Insgesamt kann die Implementation einer rein physischen Testumgebung initial mit vergleichsweise wenig Aufwand verbunden sein. Sie kann jedoch aufgrund ihrer mangelnden Flexibilität nur schlecht auf unterschiedliche Anlagen oder Veränderungen des Produktionsprozesses angepasst werden und mit hohen Kosten verbunden sein.[64]

---

56 Shannon (1998), S. 8.

57 Nance (1994), S. 10.

58 Bossel (2004), S. 17; Lass (2011), S. 598; Grube und Theuer (2011); Lass und Theuer (2011).

59 Lass und Fuhr (2013), S. 29.

60 National Institute of Standards and Technology (2015), G-24-G-25.

61 National Institute of Standards and Technology (2015), G-24-G-25; Lass und Gronau (2012), S. 2.

62 Lass (2011), S. 599; Lass und Gronau (2012), S. 3.

63 Detken, Eren und Steiner (2012), S. 1.

64 Lass und Theuer (2011), S. 13; Lass (2011), S. 599.

Hingegen muss bei Testumgebungen mit computerbasierten Simulationen nicht auf teure Hardware-Komponenten zurückgegriffen werden.[65] Deshalb betragen die Kosten solcher Testumgebungen im Allgemeinen nur einen Bruchteil der Einsatzkosten von physischen bzw. realen Modellen. Ein weiterer Vorteil einer softwarebasierten Testumgebung ist, dass sie grundsätzlich eine hohe Anpassungsfähigkeit aufweist und für unterschiedliche Anwendungsfälle genutzt werden kann. Auch kann bei diesem Typus von Testumgebung das Prozess- und Systemverhalten einfach beeinflusst werden und etwa zeitliche Abläufe beliebig beschleunigt oder verlangsamt werden.[66] Bei der computerbasiert Nachbildung der Komponenten für eine Sicherheitssimulation kann grundlegend zwischen drei Arten der Simulation im weiteren Sinne unterschieden werden: der Simulation, der Emulation und der Virtualisierung.

Bei einer Simulation im engeren Sinne werden Komponenten meist vereinfacht oder abstrahiert implementiert.[67] Das System wird mithilfe einer Simulationssoftware abgebildet, wobei Komponenten auf Funktionen der Steuerung sowie der Datenbereitstellung reduziert werden. Simulationen implementieren typischerweise nicht alle Funktionalitäten und Eigenschaften einer Komponente, sondern sind reduzierte Abbildungen.[68] Dabei können auch bestimmte Sicherheitseigenschaften realer Komponenten nachempfunden werden, etwa in Form von Filterregeln oder Zugriffskontrolllisten.[69] So können beispielsweise Netzwerke und Netzgeräte mithilfe von Netzwerksimulationssoftware umfangreich nachgebildet werden und etwa die Netzlast von Protokollen oder Komponenten-Konfigurationen kann getestet werden.[70] Diese Methode hat jedoch auch ihre Nachteile. Weder werden die Betriebssysteme dieser Komponenten, noch die Anwendungen und ihre möglichen Schwachstellen abgebildet. Gerade diese Aspekte sind bei Sicherheitsanalysen jedoch oft von großer Bedeutung.[71] Es kann vorkommen, dass Softwaremodelle für die betreffenden Komponenten oder Systeme nicht existieren und erst aufwendig entwickelt werden müssen. Manche existierende Softwaremodelle bilden die Komponenten und Systeme wiederum nicht ausreichend originalgetreu ab.[72] Eine möglichst vollständige Nachbildung eines Systems ist sehr aufwendig, da die

65 Lass und Gronau (2012), S. 2; vgl. Hellfeld (2012), S. 161-167.

66 Bossel (2004), S. 15.

67 Van Leeuwen u. a. (2009), S. 1.

68 Lass (2011), S. 599; Lass und Gronau (2012), S. 3; Van Leeuwen u. a. (2009), S. 1; Van Leeuwen u. a. (2010), S. 1807.

69 Urias und Van Leeuwen (2016), S. 263-265.

70 Beispielhaft können hier der OPNET Modeler oder NS-3 genannt werden.

71 Van Leeuwen u. a. (2009), S. 1; Van Leeuwen u. a. (2010), S. 1807.

72 Urias und Van Leeuwen (2016), S. 258.

unterschiedlichen Konfigurationen erhoben und ggf. übersetzt werden müssen.[73] Aufgrund der Anzahl der unbekannten Variablen sowie auch der Größe der Gleichungen ist eine umfassende Komponentensimulation nicht mit einem vertretbaren Zeitaufwand durchführbar. Dies führt dazu, dass kleine und mittelgroße Unternehmen oft auf dieses Werkzeug verzichten. Analysen, die ausschließlich softwarebasierte Simulationen nutzen, werden daher normalerweise auf bestimmte Aspekte reduziert, wie zum Beispiel Belastungstests.[74]

Manche dieser Probleme lassen sich durch die kombinierte Nutzung von Emulationen oder Virtualisierungen vermeiden oder abmildern. Hierbei können tatsächlich genutzte Anwendungen oder das Verhalten von Komponenten etwa mithilfe von virtuellen Maschinen oder Emulationssoftware abgebildet werden.[75] Auf diese Weise können im Optimalfall die Anwendungen und Komponenten einer Anlage abgebildet und die jeweiligen Konfigurationen übernommen werden.[76] Einschränkungen können hier jedoch vorliegen, wenn keine exakten oder annähernden (Netzwerk-)Betriebssysteme oder Anwendungen in der richtigen Version vorliegen und stattdessen Ersatzsoftware genutzt werden müsste. Jedoch unterliegen auch emulierte oder virtualisierte Komponenten vielen derselben Nachteile wie simulierte. Aber selbst realitätsnahe Emulationen und Virtualisierungen unterscheiden sich von realen Komponenten in ihrem Verhalten und ihrer Performanz. So sind Aspekte wie etwa die Rate der Paketweiterleitungen anders als bei einer realen Komponente. Auch das Verhalten angesichts von Störungen oder Angriffen wie (D)DoS-Attacken oder Buffer-Overflows ist nicht identisch, was für aussagekräftige Sicherheitsanalysen von Nachteil ist.[77]

4.3.2 Die hybride Testumgebung

Klassische Testumgebungen konzentrieren sich entweder auf Einzelaspekte oder gehen mit einem hohen Aufwand oder hohen Kosten einher, weswegen sie für Sicherheitsanalysen von ICS nur eingeschränkt nutzbar sind. Es gibt deshalb einen Bedarf an Testumgebungen in Verbindung mit aufwandsarmen und kostengünstigen Methoden zur Überprüfung der Informationssicherheit. In der EU sowie in den USA wurden zu diesem Zweck verschiedene ICS-Testumgebungen aufge-

73 Van Leeuwen u. a. (2009), S. 1; Van Leeuwen u. a. (2010), S. 1807.

74 Schumacher (2016), S. 677; Lass (2011), S. 599; Lass und Gronau (2012), S. 2-3.

75 Van Leeuwen u. a. (2010), S. 1806.

76 Urias und Van Leeuwen (2016), S. 254-265.

77 Van Leeuwen u. a. (2009), S. 3-4; Van Leeuwen u. a. (2010), S. 1807-1808.

baut, welche jedoch in der Regel proprietär sind oder nur innerhalb der jeweiligen Institution verwendet werden. Daher ist der Bedarf an solchen aufwandsarmen, kostengünstigen und realitätsnahen Testumgebungen weiterhin vorhanden, gerade auch in Bezug auf spezielle Testumgebungen etwa für kleine und mittlere KRITIS-Betreiber wie Wasserversorger.[78]

Mit hybriden Testumgebungen, die auf dem hybriden Simulationsansatz basieren, steht eine Alternative zur Verfügung, die die Nachteile der klassischen Testumgebungen auszugleichen und die Vorteile zu kombinieren versucht. Sie kann mit wenig Aufwand und niedrigen Kosten belastbare Aussagen zu sicherheitsanalytischen Fragestellungen ermöglichen.[79] Planungsrisiken können vermieden werden und Analysen alternativer bzw. modifizierter Prüfobjekte sind ohne großen Aufwand möglich. Der hybride Ansatz ist dabei realitätsnah und kann auch die Einbindung von menschlichen Aufgabenträgern beinhalten.[80]

In einer hybriden Testumgebung werden simulierte, emulierte oder virtualisierte Komponenten mit physischen (realen) Komponenten zu einem Gesamtsystem verbunden, womit die Vorteile der computerbasierten Testumgebung mit den Vorteilen der hardwarebasierten Testumgebung verbunden werden.[81] Auf diese Weise kann eine Testumgebung geschaffen werden, welche die Anlage des jeweiligen KRITIS-Betreibers realitätsnah, kostengünstig und aufwandsarm darstellt.[82] Für jedes Element der hybriden Testumgebung kann grundsätzlich eine geeignete Simulationsart festgelegt werden, wodurch Sicherheitsanalysen vergleichsweise schnell und flexibel implementiert werden können.[83] Originale Komponenten können an den entscheidenden Stellen verwendet werden, um realitätsnahe Abbildungen zu gewährleisten, während andere Komponenten oder Elemente softwarebasiert abgebildet werden.[84] So ist es möglich, je nach Ziel oder Forschungserfor-

78 Lass und Fuhr (2013), S. 29; Lass und Gronau (2012), S. 2-3; Queiroz u. a. (2009), S. 357-364; Moss (2012), S. 1-3; Christiansson und Luiijf (2008), S. 243; Bundesamt für Sicherheit in der Informationstechnik (2013), S. 118; Lass, Theuer und Gronau (2011), S. 13.

79 Lass und Gronau (2012), S. 3; Lass und Fuhr (2013), S. 29; vgl. Hellfeld (2012), S. 155; Queiroz u. a. (2009), S. 356; Moss (2012), S. 3.

80 Vgl. Hellfeld (2012), S. 167. Der hybride Simulationsansatz wird in der Literatur unter unterschiedlichen Bezeichnungen, Marken- oder Eigennamen geführt, wozu etwa „Live, Virtual, and Contructive“ oder „Simulated, Emulated, and Physical Investigative Analysis (SEPIA)“ gehören. Des Weiteren sind Sicherheitsanalysen mittels hybrider Testumgebung auch als cyber-physische Sicherheitsanalysen (Cyber-Physical Security Analysis) bekannt. Urias, Van Leeuwen und Richardson (2012), S. 254.

81 Lass und Gronau (2012), S. 3; Urias und Van Leeuwen (2016), S. 254.

82 Vgl. Lass (2011), S. 601; Urias, Van Leeuwen und Richardson (2012), S. 4.

83 Lass und Kotarski (2014), S. 601; Lass und Theuer (2011), S. 14; Theuer (2012), S. 586; Lass, Theuer und Gronau (2011), S. 13; Gronau, Fohrholz und Lass (2011), S. 204.

84 Lass und Gronau (2012), S. 3.

dernis eine unterschiedliche Wiedergabetreue in der Testumgebung zu erreichen oder, sofern notwendig, Kosten und Aufwand zu reduzieren (s. Abbildung 10).[85] Die Wiedergabetreue nimmt von realen Komponenten über Virtualisierungen und Emulationen zu Simulationen in der Regel ab, während ebenso der Aufwand bzw. die Kosten abnehmen können. Dies ist jedoch eine pauschale Aussage, die beispielsweise von der Verfügbarkeit passender Software abhängt. Im Einzelfall kann eine Virtualisierung als Image eines Systems oder die Nutzung einer vorhandenen Emulationssoftware deutlich kostengünstiger sein als das aufwendige Aufsetzen einer Simulationssoftware, wenn diese nicht bereits verfügbar ist.

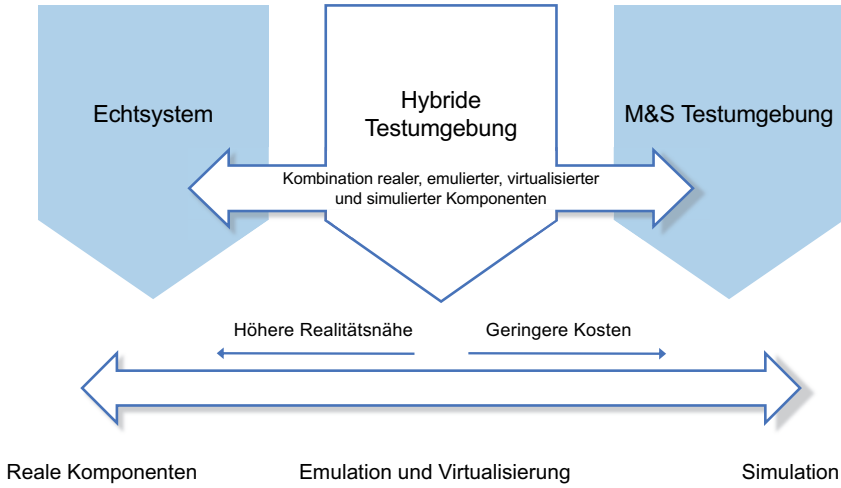

Abb. 10: Einordnung der hybriden Testumgebung in klassische Testumgebungsarten. Adaptiert nach Urias und Van Leeuwen (2016), S. 260; mit freundlicher Genehmigung von © Springer Nature (2016)

Grundsätzlich kann eine hybride Testumgebung für verschiedene Bereiche der Informationssicherheit eingesetzt werden, die unterschiedliche Anforderungen an die Testumgebung stellen können. Sie kann etwa für Sicherheitsanalysen wie Penetrationstests, Schwachstellenanalysen oder die „Relative Risk Assessment"-Methode genutzt werden und ist in diesem Kontext auch als cyber-physische Sicherheitsanalyse bekannt.[86] In dieser Testumgebung können neue Angriffsmöglichkeiten ohne Gefährdung des Betriebs überprüft und auch Effektsimulatio-

[85] Gao u. a. (2014), S. 83; Holm u. a. (2015), S. 21-22.

[86] Christiansson und Luiijf (2008), S. 243; vgl. Urias und Van Leeuwen (2016); Van Leeuwen u. a. (2010), S. 1807; Gurschler u. a. (2017), S. 405.

nen durchgeführt werden, womit sich Auswirkungen auf die Anlage nachvollziehen lassen.[87] Weitere Anwendungsbereiche finden sich in Schadensfolgeanalysen bzw. Folgenabschätzungen, in der Forschung zur Risikominderung (Mitigationsforschung), in der Entwicklung von Modellen für die Sicherheitsforschung, der Sicherheitsvalidierung, für Cyber-Forensics oder in der Schulung von Anwendern, ICS-Verantwortlichen und Sicherheitsexperten.[88] Seltener werden hybride Testumgebungen des Weiteren für Performanzanalysen oder in der Entwicklung von Standardisierungsmaßnahmen genutzt sowie für Bedrohungsanalysen oder Robustheitstests.[89] Auch abseits des Kontexts der Informationssicherheit findet der hybride Simulationsansatz vielfache Anwendungsbereiche. Dies können Geschäftsprozess-, Machbarkeits- und Wirtschaftlichkeitsanalysen sein, aber auch zur Erprobung von Produktionsprozessen wird der hybride Simulationsansatz eingesetzt.[90]

Derzeit wird an der Universität Potsdam eine hybride Testumgebung für cyber-physische Sicherheitsanalysen sowohl als Analysewerkzeug genutzt als auch als Forschungsplattform weiterentwickelt.[91] Die Testumgebung ist sowohl Softwarearchitektur als auch Hardwareplattform und von vornherein darauf ausgerichtet, ausgewählte Hardwarekomponenten über Interfacebausteine und standardisierte Kommunikationsprotokolle aufwandsarm zu integrieren und an die Software anzubinden, mit deren Hilfe andere Komponenten und Anwendungen simuliert, emuliert oder virtualisiert werden können.[92] In dieser Architektur wird eine Unterscheidung zwischen der Anwenderebene einerseits und der Ebene des Simulationsbetriebs andererseits vorgenommen, was sich auch in der Zuordnung von Parametern niederschlägt. Parameter auf der Anwenderseite basieren auf realen Prozessdaten und können über die Oberfläche der Betriebstechnik ausgelesen und ggf. manipuliert werden. Parameter, die dem Simulationsbetrieb zugeordnet werden, dienen der Steuerung der eigentlichen Simulation und können während des Simulationsbetriebs verändert werden, wodurch auch physikalische Phänomene oder Zwischenfälle eingeplant werden können.[93] Diese hybride Testumgebung ist speziell darauf ausgerichtet, aufwandsarme und kostengünstige cyber-physische Sicherheitsanalysen für kleine und mittlere KRITIS-Betreiber insbesondere der

87 Gurschler u. a. (2017), S. 405.

88 Vgl. Hong u. a. (2015), S. 270; Hahn u. a. (2013), S. 848-849.

89 Holm u. a. (2015), S. 17.

90 Vgl. Grambow (2013), S. 130; vgl. Lin, Sedigh und Miller (2009); Lass (2011), S. 602; Lass, Theuer und Gronau (2011), S. 13; BSI-Standard 200-2 (2017), S. 131; vgl. Hellfeld (2012).

91 Lass und Kotarski (2014), S. 398.

92 Vgl. Lass (2011), S. 601; Chabukswar u. a. (2010), S. 1.

93 Lass (2011), S. 601.

Wasserversorgung zu ermöglichen. Einerseits ist dies möglich, da bausteinorientierte Simulationswerkzeuge grundsätzlich mit reduzierten Kosten und Aufwand einhergehen, sowohl in der Implementation als auch im Hinblick auf die Verifikation und Validierung.[94] Andererseits sind zu diesem Zweck auch spezifische Verfahren vorgesehen, wie Sicherheitsschnelltests im Vorfeld oder Objektbibliotheken für eine schnelle Implementation von Simulationsobjekten. In diesen Kontext kann sich auch die in Kapitel 5 vorgeschlagene Vorgehensweise und Klassifikation einfügen, mit der eine Bestimmung der Simulationsart von Simulationsobjekten sowie eine Implementation der jeweiligen Testumgebung erleichtert wird.

Wie auch die Testumgebung des Aqua-IT-Labs verfügt eine typische hybride Testumgebung zunächst über ein Simulationsbetriebsmodul, das die unterschiedlichen Systeme, Komponenten und Anwendungen über Schnittstellen in die Testumgebung integriert (s. Abbildung 11).[95] Verschiedene Netzwerkzonen werden dabei über die Integration und Konfiguration der Systeme, Komponenten und Anwendungen abgebildet, vom Unternehmensnetzwerk bis zum Feldgerätenetzwerk.[96] Im Simulationsbetriebsmodul können darüber hinaus Prozessstörungen in der Simulation oder Auswirkungen von Attacken in der Testumgebung eingestellt werden. Ebenso können Überwachungs- und Analysefunktionalitäten während und infolge der Sicherheitsanalyse für den Simulationsbetreiber bereitgestellt werden.[97] Für Anwender, also etwa Sicherheitsexperten, die einen Penetrationstest durchführen, steht hingegen mit der Anwenderebene eine Darstellung der realen oder computerbasierten Komponenten der hybriden Testumgebung zur Verfügung, die vom Simulationsbetriebsmodul getrennt ist. Auf der Anwenderebene können statt realen Nutzern auch Benutzerinteraktionssimulatoren eingesetzt werden, die das gewünschte Nutzerverhalten abbilden, ohne reale Anwender in Anspruch nehmen zu müssen.

Im Prozessleitmodul werden SCADA-Systeme oder DCS computerbasiert oder real in die Testumgebung eingebunden, ggf. auch in Form von physisch entfernten Kontrollzentren, sowie die dazugehörigen unterstützenden Systeme der Prozessleitebene.[98]

---

94 Vgl. Rabe, Spieckermann und Wenzel (2008), S. 130 ff.

95 Vgl. Urias und Van Leeuwen (2016), S. 263-265.

96 Gao u. a. (2014), S. 88.

97 Vgl. IEC/ISA 62443-2-1:2015 (2015), S. 74 und S. 214. Allerdings muss gerade in Bezug auf besonders kritische Komponenten berücksichtigt werden, dass Überwachungs- und Analysefunktionalitäten der Testumgebung ggf. zu einer verminderten Performanz von Komponenten führen können. Eine fehlende Berücksichtigung dieses Umstands würde Ergebnisse einer Sicherheitsanalyse ggf. verfälschen.

98 Lass (2011), S. 601.

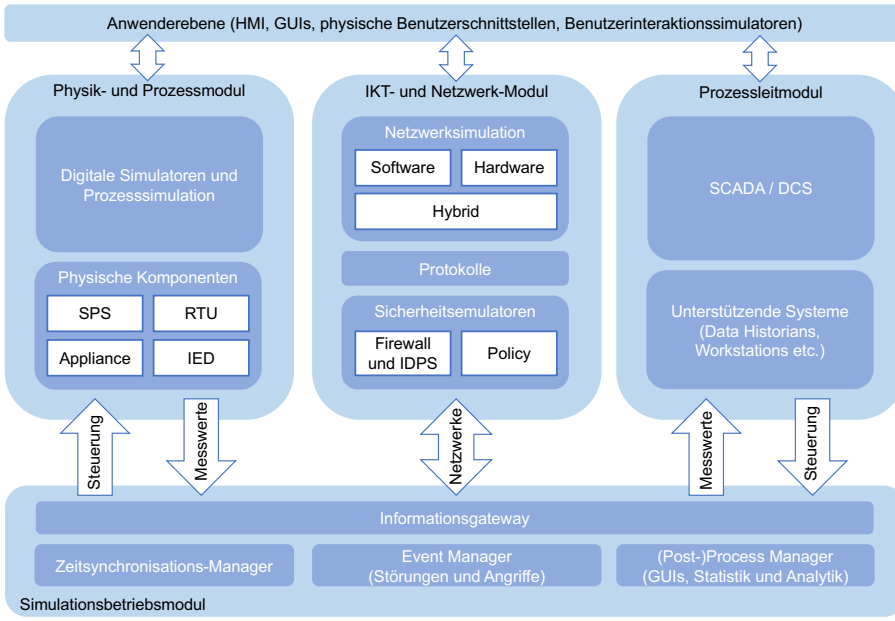

Abb. 11: Logische Struktur einer hybriden ICS-Testumgebung.[99] Adaptiert nach Hong u. a. (2015), S. 267; mit freundlicher Genehmigung von © Springer Nature (2015)

Im Physik- und Prozessmodul kann der Anlagenprozess mithilfe einer Prozesssimulation dargestellt und inkorporiert werden, also die physischen, chemischen oder mechanischen Prozesse der Wertschöpfung, welche üblicherweise über mathematische Modelle abgebildet werden.[100] Auch Prozesse der Wasserversorgung und -entsorgung können auf diese Weise simuliert werden.[101] Für Sicherheitsanalysen werden diese jedoch in der Regel vereinfacht dargestellt, was eine hohe Anpassbarkeit an unterschiedliche Szenarien gewährleistet.[102] Ebenso werden im Prozessmodul die prozessnahen Komponenten der Feld- und Steuerungsebene integriert. Reale Komponenten wie SPS oder RTU können insbesondere bei besonders kritischen oder aus anderen Gründen interessanten Bereichen integriert werden, während andere Komponenten simuliert oder emuliert werden können. Es ist denkbar, dass verschiedene Systeme und Komponenten auf diese Weise konsolidiert und kostengünstig auf einem einzigen mobilen PC abgebildet werden. Durch

99 Vgl. Hahn u. a. (2013), S. 849; Khorrami, Krishnamurthy und Karri (2016), S. 81.
100 Thornton und Morris (2015), S. 123.
101 Adams (2011), S. 17-19.
102 Green u. a. (2017), S. 5.

Instanziierung von Emulationen können auch sehr große und komplexe Anlagen mit vielfachen Redundanzen nachgebildet werden.[103]

Im Netzwerkmodul können Netzwerke und grundsätzlich auch Netzgeräte mithilfe einer entsprechenden Netzwerksimulationssoftware simuliert werden, womit sich etwa auch eine entsprechende Netzlast ggf. erzeugen und messen lässt.[104] Zu diesem Zweck können zumindest die verbreiteteren Kommunikationsprotokolle nutzbar gemacht werden.[105] Darüber hinaus können aktive Netz- und Sicherheitskomponenten auch spezifisch abgebildet werden. Die Integrationsmöglichkeiten dieser Komponenten entsprechen denen der prozessnahen Komponenten im Prozessmodul, sie können also simuliert, emuliert, ggf. virtualisiert oder real in die Testumgebung integriert werden. Virtualisierung ist insbesondere bei jenen Sicherheitskomponenten denkbar, die auf handelsüblichen PCs mit normalen Betriebssystemen wie Windows oder Linux laufen, also etwa Firewalls oder IDS/IPS. Appliances und aktive Netzkomponenten wie Router oder Switches könnten hingegen grundsätzlich emuliert werden, insbesondere wenn hierfür passende Netzwerkbetriebssysteme bzw. Emulatoren zur Verfügung stehen.[106] Die Komponenten in diesem Modul können im Optimalfall durch den Import der tatsächlichen Konfigurationsdateien implementiert werden, um die Anlage realitätsnah abzubilden.[107]

Für die Simulation, Emulation und Virtualisierung wird in unterschiedlichen Testumgebungen eine große Vielfalt an Software eingesetzt. Im Potsdamer „Anwendungszentrums Industrie 4.0“ werden reale Komponenten der Prozessleitebene physisch vorgehalten bzw. in die Testumgebung integriert, während der physische Wertschöpfungsprozess mit IFAK Simba simuliert wird. Ebenso werden Feldgeräte, insbesondere in der dezentralen Peripherie, als Simulation in die Testumgebung integriert, wohingegen Steuerungskomponenten wie SPS-Bausteine vorrangig als reale Hardware abgebildet werden oder zusätzlich per Codesys oder Soft-PLC emuliert werden. Aktive Netzwerk- und Sicherheitskomponenten werden aufgrund ihrer Sicherheitseigenschaften ebenso physisch in die Testumgebung integriert und in größeren Netzwerken mit Emulationen oder Simulationen von Netzkomponenten kombiniert. Das Netzwerk als solches wird per OMNET oder OPNET simuliert, womit sich eine reale Netzlast simulieren lässt. Zuletzt wird AnyLogic als Benutzerinteraktionssimulator eingesetzt, womit Benutzerverhalten auf der Anwenderebene simuliert werden kann.

---

103 Vgl. Urias und Van Leeuwen (2016), S. 260-265; Van Leeuwen u. a. (2010), S. 1807.

104 Urias und Van Leeuwen (2016), S. 165.

105 Wang, Fang und Dai (2010), S. 346.

106 Bekannte Netzwerkbetriebssysteme sind etwa das Open Source VyOS oder auch proprietäre Systeme wie Cisco IOS oder IPOS von Ericsson.

107 Urias und Van Leeuwen (2016), S. 265; Van Leeuwen u. a. (2010), S. 1808.

Da verschiedene Ansätze zur Implementierung von hybriden Testumgebungen existieren und unterschiedliche Vor- und Nachteile haben können, lohnt sich eine vergleichende Betrachtung. Einen Überblick über die Landschaft der Testumgebungen bietet die Metastudie von Holm et al., die 30 verschiedene ICS-Testumgebungen analysiert haben, die in der Regel unterschiedliche Simulationsarten kombinieren.[108]

Komponenten der Prozessleitebene wie Prozessleitsysteme, Server oder Workstations werden in ICS-Testumgebungen meist physisch als originale Hardware und Software eingebunden (37 %) oder aber simuliert (30 %). Letzteres geschieht etwa per LabVIEW, Mathworks Simulink, HoneyD in Verbindung mit IMUNES, dem RINSE-Netzwerksimulator oder mithilfe von Python-Skripten. Seltener werden diese Komponenten auch virtualisiert (13 %), wofür verschiedene Anwendungen zum Einsatz kommen, wie beispielsweise Deter, EmuLab, GENI, PlanetLab oder VirtualBox. Es ist überraschend, dass die Virtualisierung von Komponenten und Anwendung nicht verbreiteter ist, da sich dies aufgrund der verbreiteten Nutzung von üblicher Hardware und üblichen Betriebssystemen anbietet und kostengünstig implementierbar wäre.

Der physische Wertschöpfungsprozess wird in allen betrachteten hybriden Testumgebungen simuliert. Hierfür werden Anwendungen wie Matlab, Mathworks Simulink, Power Hardware-in-the-Loop (OPAL-RT), LabView, PowerWorld, AnyLogic und EZJCOM, ANSYS, EPANET, OMNET oder maßgeschneiderte Anwendungen verwendet, die etwa in Java geschrieben wurden.[109]

Prozessnahe Feld- und Steuerungskomponenten wie SPS-Bausteine und RTU wurden in den betrachteten ICS-Testumgebungen primär physisch abgebildet (47 %), aber auch emuliert oder simuliert (zusammen 47 %).[110] Hierfür kommen Anwendungen wie STEP7, RSEmulate, LabVIEW, Scadapack LP PLC, Modbus Rsim, Soft-PLC, OpenVZ und andere zum Einsatz.[111]

Auch Netzwerke und Netzwerkkomponenten werden primär simuliert (33 %) oder – vor allem die aktiven Netzkomponenten – physisch abgebildet (37 %). Zur Netzwerksimulation werden beispielsweise OPNET, SITL, Iperf, RINSE, OMNET++, PowerWorld Simulator, Mathworks Simulink, das Inet Framework, NS-2 und NS-3, Networksim, IMUNES, das c2windtunnel Framework oder Python-Skripte eingesetzt. Oft werden Komponenten auch virtualisiert (20 %), jedoch nur

108 Vgl. Holm u. a. (2015).

109 Ebd., S. 17-18.

110 Die restlichen Testumgebungen haben Feldgeräte nicht abgebildet. Des Weiteren legen die Autoren den Begriff der Emulation sehr eng aus, wonach etwa RSEmulate oder auch Siemens-Produkte wie STEP7 keine Emulatoren wären. Dies ist diskussionswürdig, weshalb sie in dieser Aufbereitung zusammengefasst wurden.

111 Holm u. a. (2015), S. 17-18.

selten emuliert, etwa mithilfe von CORE und OpenVZ oder RINSE. Von den etwa 150-200 ICS-Protokollen sind die häufigsten im Einsatz befindlichen Protokolle der betrachteten ICS-Testumgebungen Modbus und DNP3. Häufig werden auch OPC, IEC 60870, IEC 61850 und Profibus eingesetzt. Etwas seltener kommen darüber hinaus Fieldbus, FINS, GOOSE, ICCP, IEE C37.118, CIP RJ45, DeviceNet und Genius zum Einsatz.[112]

Die Metastudie verdeutlicht, dass es im Bereich der hybriden Testumgebungen von Industrieanlagen eine große Vielfalt gibt. Laut Holm et al. sind in diesem Feld in den letzten Jahren viele Fortschritte zu verzeichnen gewesen, jedoch werden die verschiedenen Ansätze kaum koordiniert. So gibt es nur in Ansätzen einen einheitlichen Forschungsrahmen, mit dessen Hilfe diese Ansätze eingeordnet und bewertet werden können. Als grundsätzliche Gütekriterien für ICS-Testumgebungen werden von Siaterlis et al. Wiedergabetreue, Wiederholbarkeit, Messgenauigkeit und Safety vorgeschlagen. Insbesondere Wiedergabetreue wird jedoch in der Literatur zu hybriden Testumgebungen meist entweder gar nicht diskutiert oder aber auf Basis von Erfahrungswerten oder auf Grundlage von Architekturen oder Maßgaben von Standards wie etwa ISA-99 gerechtfertigt. Laut Holm et al. sind deshalb eine klare Zielformulierung und die Nutzung von realitätsnahen Methoden zur Abbildung von Komponenten und Anwendungen wichtig. Darüber hinaus schlagen die Autoren vor, in Abwesenheit eines Bewertungsrahmens die Wiedergabetreue durch ein nachvollziehbares und dokumentiertes Vorgehen zu gewährleisten. Genau hier setzt die im folgenden Kapitel beschriebene Vorgehensweise und Klassifikation an.[113]

Literaturverzeichnis

Adams, J. R. (2011), *A water distribution and treatment simulation for testing cyber security enhancements for water sector SCADA systems*, University of Louisville.

Birkhold, M. und J. Bauer (2014), *Sicherheit in der Automatisierungstechnik nach BSI IT-Grundschutz, geht das?*, Vortrag, URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Veranstaltungen/Grundschutz/1GS_Tag_2014/02_1_IT-Grund_2014_Birkhold.pdf?__blob=publicationFile (besucht am: 20. 12. 2017).

112 Holm u. a. (2015), S. 19.

113 Holm u. a. (2015), S. 13-23; Siaterlis, Garcia und Genge (2013), S. 929-942.

Birkhold, M. und A. Lechler (2014), Modellierung von Automatisierungssystemen nach Vorgaben des BSI - Bundesministerium für Sicherheit in der Informationstechnik: Notwendigkeit, Modellkonzept, Vorteile, in: *wt Werkstattstechnik online*, 104:5, 301–306.

Bossel, H. (2004), *Systeme, Dynamik, Simulation – Modellbildung, Analyse und Simulation komplexer Systeme*, BoD.

BSI IT-Grundschutz-Kompendium (2017), *Umsetzungshinweise zum Baustein IND.1 Betriebs- und Steuerungstechnik*.

BSI-Gesetz (2017), *Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG) vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 1 des Gesetzes vom 23. Juni 2017 (BGBl. I S. 1885) geändert worden ist*.

BSI-KritisV (2016), *Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung – BSI-KritisV)*.

BSI-Standard 100-2 (2008), *IT-Grundschutz-Vorgehensweise*.

BSI-Standard 200-1 (2017), *Managementsysteme für Informationssicherheit (ISMS) – Community Draft*.

BSI-Standard 200-2 (2017), *IT-Grundschutz-Methodik – Community Draft*.

BSI-Standard 200-3 (2016), *Risikoanalyse auf der Basis von IT-Grundschutz – Community Draft*.

Bundesamt für Sicherheit in der Informationstechnik (2013), *ICS-Security-Kompendium*.

Bundesamt für Sicherheit in der Informationstechnik (2015), *KRITIS-Sektorstudie: Ernährung und Wasser*, Bundesamt für Sicherheit in der Informationstechnik.

Bundesamt für Sicherheit in der Informationstechnik (2016), *IT-Grundschutz-Kataloge: 15. Ergänzungslieferung*.

Chabukswar, R. u. a. (2010), Simulation of Network Attacks on SCADA Systems, in: *First Workshop on Secure Control Systems*.

Christiansson, H. und E. Luiijf (2008), Creating a European SCADA security testbed, in: E. Goetz und S. Shenoi (Hrsg.), *International Conference on Critical Infrastructure Protection, 1st IFIP WG 11.10 International Conference, ICCIP 2007, New Hampshire, USA, Revised Selected Papers*, Springer, 237–247.

Detken, K.-O., E. Eren und M. Steiner (2012), Erhöhung der IT-Sicherheit durch Konfigurationsunterstützung bei der Virtualisierung, DACH Security, in: P. Schartner und J. Taeger (Hrsg.), *DACH Security 2012: Bestandsaufnahme – Konzepte – Anwendungen – Perspektiven*, Prof. Dr. Patrick Horster.

Dinger, J. und H. Hartenstein (2008), *Netzwerk-und IT-Sicherheitsmanagement: Eine Einführung*, KIT Scientific Publishing.

Floß, A. (2015), *Sicherheit von industriellen Steuerungssystemen: Sicherheitsmanagement mit der BSI IT-Grundschutz-Vorgehensweise*, Präsentation auf dem 14. Deutschen IT-Sicherheitskongress, Bonn.

Fritsch, P. u. a. (2014), *Mutschmann/Stimmelmayr: Taschenbuch der Wasserversorgung*, SpringerVieweg.

Gao, H. u. a. (2014), An Industrial Control System Testbed Based on Emulation, Physical Devices and Simulation, in: *International Conference on Critical Infrastructure Protection VIII, 8th IFIP WG 11.10 International Conference, ICCIP 2014*, Jonathan Butts und Sujeet Hanoi, 79–91.

Grambow, M. (2013), *Nachhaltige Wasserbewirtschaftung: Konzept und Umsetzung eines vernünftigen Umgangs mit dem Gemeingut Wasser*, SpringerVieweg.

Green, B. u. a. (2017), Pains, Gains and PLCs: Ten Lessons from Building an Industrial Control Systems Testbed for Security Research, in: *The 10th USENIX Workshop on Cyber Security Experimentation and Test (CSET '17)*, USENIX Association.

Gronau, N., C. Fohrholz und S. Lass (2011), Hybrider Simulator – Neuer Ansatz zum Produktionsmanagement, in: *ZWF Zeitschrift für wirtschaftlichen Fabrikbetrieb*, 106:4, 204–208.

Grube, G. und H. Theuer (2011), Die Spielarten der Simulation, in: *Computer &Automation*, 2011:9.

Gurschler, T. u. a. (2017), Risikobeurteilung in der IT-Sicherheit Kritischer Infrastrukturen – Eine Analyse der Risikobeurteilung im Förderschwerpunkt ITS|KRITIS, in: *Bundesamt für Sicherheit in der Informationstechnik: Digitale Gesellschaft zwischen Risikobereitschaft und Sicherheitsbedürfnis: Tagungsband des 15. Deutschen IT-Sicherheitskongress 2017*, SecuMedia Verlag.

Hahn, A. u. a. (2013), Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid, in: *IEEE Transactions on Smart Grid*, 4:2, 847–855.

Hellfeld, S. (2012), *Hybride Simulation mobiler Geschäftsprozesse*, KIT Scientific Publishing.

Holm, H. u. a. (2015), A survey of industrial control system testbeds, in: S. Buchegger und M. Dam (Hrsg.), *Secure IT Systems, Lecture Notes in Computer Science*, Springer, 11–26.

Hong, J. u. a. (2015), Cyber-Physical Security Testbed for Substations in a Power Grid, in: C. C. Liu, S. K. Khaitan und J. D. McCalley (Hrsg.), *Cyber Physical Systems Approach to Smart Electric Power Grid*, Springer, 261–301.

IEC/ISA 62443-2-1:2015 (2015), *Security for industrial automation and control systems – Part 2-1: Industrial automation and control system security management system, Draft 7, Edit 5 November 9, 2015*.

ISO/IEC 27000:2016(E) (2016), *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

ISO/IEC 27005:2008 (2008), *Information technology – Security techniques – Information security risk management*.

Kahneman, D. und A. Tversky (1979), Prospect theory: An analysis of decision under risk, in: *Econometrica*, 47:2, 263–292.

Karger, R. und F. Hoffmann (2013), *Wasserversorgung: Gewinnung – Aufbereitung – Speicherung – Verteilung*, Bd. 14, SpringerVieweg.

Kersten, H., J. Reuter und K.-W. Schröder (2013), *IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz*, Springer.

Khorrami, F., P. Krishnamurthy und R. Karri (2016), Cybersecurity for control systems: A process-aware perspective, in: *IEEE Design & Test*, 33:5, 75–83.

Kraft, R. und M. Stöwer (2017), IT-Risikomanagement im Produktionsumfeld – Herausforderungen und Lösungsansätze, in: *HMD Theorie und Praxis der Wirtschaftsinformatik*, 54:1, 84–96.

Lass, S., H. Theuer und N. Gronau (2011), Effiziente Simulation im Produktionsmanagement:Schnelle und belastbare Analyse von Fertigungsprozessen, in: *Industrie Management*, 27:3, 13–15.

Lass, S. (2011), A new Approach to Simulation in Production Management, in: H. El Maraghy (Hrsg.), *Enabling Manufacturing Competitiveness and Economic Sustainability: Proceedings of the 4th International Conference on Changeable, Agile, Reconfigurable and Virtual production (CARV 2011), Montreal, Canada, 2-5 October 2011*, Springer, 598–604.

Lass, S. und D. Fuhr (2013), IT-Sicherheit in der Fabrik, in: *Productivity Management*, 18:2.

Lass, S. und N. Gronau (2012), Efficient Analysis of Production Processes with a Hybrid Simulation Environment, in: H. Nylund u. a. (Hrsg.), *Proceedings of the FAIM 2012: 22nd International Conference on Flexible Automation and Intelligent Manufacturing, June 10th-13th, 2012, Helsinki, Finland*, Tampere University of Technology.

Lass, S. und D. Kotarski (2014), IT-Sicherheit als besondere Herausforderung von Industrie 4.0, in: W. Kersten, H. Koller und H. Lödding (Hrsg.), *Schriftenreihe der Hochschulgruppe für Arbeits- und Betriebsorganisation e.V. (HAB):*

Industrie 4.0 – Wie intelligente Vernetzung und kognitive Systeme unsere Arbeit verändern Schriftenreihe der Hochschulgruppe für Arbeits- und Betriebsorganisation, Gito Verlag Berlin, 397–419.

Lass, S. und H. Theuer (2011), Hybride Simulation – Den besten Grad an dezentraler Produktionssteuerung bestimmen, in: *Productivity Management*, 13–16.

Lin, J., S. Sedigh und A. Miller (2009), Towards integrated simulation of cyber-physical systems: a case study on intelligent water distribution, in: *Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, DASC'09*, IEEE, 690–695.

Moss, K. T. (2012), *Water treatment and distribution simulation for a SCADA security testbed*, Electronic Theses and Dissertations, Paper 1013, University of Louisville.

Nance, R. E. (1994), The conical methodology and the evolution of simulation model development, in: *Annals of Operations Research*, 56, 1–45.

National Institute of Standards and Technology (2015), *NIST Special Publication 800-82, Revision 2: Guide to industrial control systems (ICS) security – supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as programmable logic controllers (PLC)*.

Queiroz, C. u. a. (2009), Building a SCADA security testbed, in: *Network and System Security, 2009. NSS'09. Third International Conference on*, IEEE, 357–364.

Rabe, M., S. Spieckermann und S. Wenzel (2008), *Verifikation und Validierung für die Simulation in Produktion und Logistik: Vorgehensmodelle und Techniken*, Springer Science & Business Media.

Schaumüller-Bichl, I. und A. Kolberger (2016), Information Security Risk Analysis in komplexen Systemen – neue Herausforderungen und Lösungsansätze, in: H. C. Mayr und M. Pinzger (Hrsg.), *GI-Jahrestagung, INFORMATIK 2016, Lecture Notes in Informatics (LNI)*, Gesellschaft für Informatik, 609–617.

Schmölzer, J. (2010), *IT-Sicherheit von SCADA-Systemen*, Diplomarbeit, Fachbereich Informationstechnik & Elektrotechnik, Hochschule Mittweida (FH).

Schumacher, S. (2016), IT-Sicherheit in der Wasserversorgung: Schutz kritischer Infrastrukturen, in: *Magdeburger Journal zur Sicherheitsforschung*, 11, 667–685.

Shannon, R. E. (1998), Introduction to the art and science of simulation, in: *Proceedings of the 30th conference on Winter simulation*, IEEE Computer Society Press, 7–14.

Siaterlis, C., A. P. Garcia und B. Genge (2013), On the use of Emulab testbeds for scientifically rigorous experiments, in: *IEEE Communications Surveys & Tutorials*, 15:2, 929–942.

Sowa, A., P. Duscha und S. Schreiber (2015), *IT-Revision, IT-Audit und IT-Compliance: Neue Ansätze für die IT-Prüfung*, SpringerVieweg.

Tews, E. und C. Schlehuber (2014), Quantitative Ansätze zur IT-Risikoanalyse, in: *Sicherheit*, TU Darmstadt, 293–303.

Theuer, H. (2012), Extension of Value Stream Design for the Simulation of Autonomous Production Systems, in: M. F. Zaeh (Hrsg.), *Enabling Manufacturing Competitiveness and Economic Sustainability: Proceedings of the 5th International Conference on Changeable, Agile, Reconfigurable and Virtual Production (CARV 2013), Munich, Germany, October 6th-9th, 2013*, Springer, 586–591.

Thim, C. und D. Kotarski (2015), Herausforderungen der IT-Sicherheit bei kleinen und mittleren Betreibern kritischer Infrastrukturen, in: *DVGW energie | wasser-praxis*, 10, 44–46.

Thornton, Z. und T. Morris (2015), Enhancing a virtual SCADA laboratory using Simulink, in: M. Rice und S. Shenoi (Hrsg.), *Critical Infrastructure Protection IX, 9th IFIP 11.10 International Conference, ICCIP 2015 Arlington, VA, USA, March 16–18, 2015 Revised Selected Papers*, Springer-Verlag, 119–133.

TrinkwV (2017), *Trinkwasserverordnung in der Fassung der Bekanntmachung vom 10. März 2016 (BGBl. I S. 459), die zuletzt durch Artikel 2 des Gesetzes vom 17. Juli 2017 (BGBl. I S. 2615) geändert worden ist*.

Urias, V. und B. Van Leeuwen (2016), Experimental Methods for Control System Security Research, in: E. J. M. Colbert und A. Kott (Hrsg.), *Cyber-security of SCADA and Other Industrial Control Systems*, Springer, 253–277.

Urias, V., B. Van Leeuwen und B. Richardson (2012), Supervisory Command and Data Acquisition (SCADA) system cyber security analysis using a live, virtual, and constructive (LVC) testbed, in: *Military Communications Conference (MILCOM) 2012*, IEEE, 1–8.

Van Leeuwen, B. u. a. (2009), Simulated, emulated, and physical investigative analysis (SEPIA) of networked systems, in: *Military Communications Conference (MILCOM) 2009*, IEEE, 1–7.

Van Leeuwen, B. u. a. (2010), Performing cyber security analysis using a live, virtual, and constructive (LVC) testbed, in: *Military Communications Conference (MILCOM) 2010*, IEEE, 1806–1811.

Verein Deutscher Ingenieure (1993), *VDI-Richtlinie 3633, BI. 1: Simulation und Logistik-, Materialfluß- und Produktionssystemen, Beuth*.

Wang, C., L. Fang und Y. Dai (2010), A simulation environment for SCADA security analysis and assessment, in: *2010 International Conference on Measuring Technology and Mechatronics Automation (ICMTMA)*, Bd. 1, IEEE, 342–347.

Wegener, C., T. Milde und W. Dolle (2016), *Informationssicherheits-Management: Leitfaden für Praktiker und Begleitbuch zur CISM-Zertifizierung*, Springer-Verlag.

Kapitel 5
Modellierung und Implementierung hybrider Testumgebungen für cyber-physische Sicherheitsanalysen

Mithilfe von unterschiedlichen Ansätzen kann die Modellierung und Implementation einer hybriden Testumgebung strukturiert und beschleunigt werden. In diesem Kapitel wird ein Vorgehensmodell für cyber-physische Sicherheitsanalysen vorgestellt sowie eine Klassifikation beschrieben, womit die jeweils passende Simulationsart von Komponenten mit reduziertem Aufwand bestimmt werden kann. Die Klassifikation kommt in der Vorbereitungsphase des Vorgehensmodells zum Tragen. Das Vorgehen im Allgemeinen sowie die Klassifikation im Speziellen lehnen sich dabei an die IT-Grundschutz-Methodik an und bauen auf Ergebnisse des Informationssicherheitsprozesses nach IT-Grundschutz auf, um eine entsprechende Anknüpfbarkeit zu gewährleisten. Durch eine Anlehnung an diesen in Deutschland anerkannten und insbesondere bei KMU verbreiteten Standard können ebenfalls Aufwände reduziert werden. Dennoch soll betont werden, dass auch andere Standards und Methoden der Informationssicherheit für das Vorgehensmodell und die Klassifikation analog eingesetzt werden können und ebenso Vorarbeiten praxisnaher Methoden wie der Business-Impact-Analyse nachgenutzt werden können.[1]

Das Ziel ist es, mit dem Vorgehensmodell und der Klassifikation ein konsistentes, nachvollziehbares und reproduzierbares Vorgehen bereitzustellen, um die Modellierung und Implementation zu erleichtern. Der Fokus liegt dabei auf dem Schutz vor einem Ausfall der kritischen leitungsgebundenen Wertschöpfung. Entsprechend wird insbesondere bei der Klassifikation von einer Testumgebung für eine cyber-physische Sicherheitsanalyse ausgegangen, bei welcher der Schutz der physischen Wertschöpfungsprozesse gegen Attacken über das Netzwerk bzw. Internet im Vordergrund steht, auch wenn die beschriebenen Vorgehensweisen auch bei anderen Zielstellungen und Anwendungsfällen entsprechend angewendet und angepasst werden können. Sie könnte sich vor allem in jenen Fällen eignen, in denen ein effizientes Vorgehen wichtig ist, wie etwa bei KRITIS-Betreibern und KMU.

[1] IEC/ISA 62443-2-1:2015 (2015), S. 154-155.

O. Leps, *Hybride Testumgebungen für Kritische Infrastrukturen*,
https://doi.org/10.1007/978-3-658-22614-5_5

Im Konkreten liegt der Schwerpunkt dieser Vorgehensweise auf Zielobjekten der Betriebs- und Steuerungstechnik bzw. von Industrieanlagen mit erhöhtem Schutzbedarfe, wobei auch andere IT- und OT-Komponenten mit in die Betrachtung einfließen können, sofern sie Teil einer solchen Anlage sind. So können auch Geräte aus dem Bereich der Telekommunikation oder Büroanwendungen Teil der Analyse sein. Geräte wie Drucker oder Druckserver können Teil des Netzwerks oder direkt mit einem Regelkreislauf verbunden sein.[2] An dieser Stelle soll daher betont werden, dass jedes Gerät und jede Anwendung einer Anlage Sicherheitsimplikationen nach sich ziehen kann, sofern es mit dem Anlagennetzwerk verbunden ist und Daten austauschen kann.[3]

5.1 Vorgehensmodell zur Modellierung und Implementation einer hybriden Testumgebung

In den bisherigen Forschungsarbeiten zum hybriden Simulationsansatz wurde an der Universität Potsdam im Kontext von Produktionsprozessen und Industrie 4.0 neben der eigentlichen Simulation auch ein Vorgehensmodell zur systematischen Aufnahme, Darstellung und Analyse von Fertigungsprozessen entwickelt und validiert, das die Modellierung und Implementation optimieren soll.[4] In diesem Abschnitt wird eine auf cyber-physische Sicherheitsanalysen von Industrieanlagen angepasste Variante des Vorgehensmodells zur Implementation von Testumgebungen beschrieben.

Das Vorgehensmodell besteht aus vier Phasen (s. Abbildung 12): Die Vorbereitung, die Konfiguration der Elemente der Testumgebung, die Konfiguration der Testumgebung sowie der eigentliche Simulationsbetrieb und die Analyse.[5] Die im Folgenden detaillierten Phasen dieses Vorgehensmodells bieten Potentiale zur Reduzierung der Komplexität, um den Aufwand der Modellierung und Simulation zu

---

2 Knapp und Langill (2014), S. 96.

3 Knapp und Langill (2014), S. 96; BSI IT-Grundschutz-Kompendium (2017a). Das BSI beschreibt deshalb in Baustein IND.1.A16 eine Abschottung der ICS- und OT-Komponenten, ggf. per Zonierung.

4 Lass und Gronau (2012), S. 4; Lass, Theuer und Gronau (2011), S. 13. Auch hier war das Ziel, KMU die Möglichkeit zu bieten, „schnell und aufwandsarm“ belastbare Aussagen zu Produktionsszenarien zu erhalten, welche auf das jeweilige Unternehmen ausgelegt sind. Vgl. Lass, Fohrholz und Theuer (2011), S. 205; Lass und Theuer (2011), S. 15; Gurschler u. a. (2017), S. 403.

5 Vgl. Lass und Gronau (2012), S. 4.

verringern.[6] Das Vorgehen folgt dem typischen Aufbau einer Simulationsstudie, wurde jedoch entsprechend angepasst und reduziert.[7]

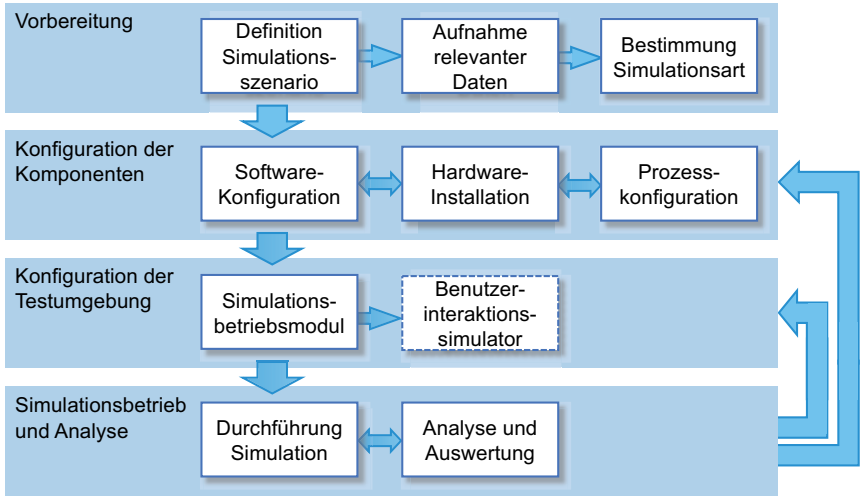

Abb. 12: Vorgehensmodell zur Implementation einer hybriden Testumgebung. Adaptiert nach Lass, Theuer und Gronau (2011), S. 14; mit freundlicher Genehmigung von © GITO mbH Verlag (2011)

Die erste Phase dient der Vorbereitung der Implementation der hybriden Testumgebung, was unmittelbar mit den Vorbereitungen zur Durchführung der Sicherheitsanalyse verknüpft ist. Zur Vorbereitung gehört zunächst, basierend auf den Zielen der jeweiligen Sicherheitsanalyse, die Festlegung des Prüfumfangs, der Prüfobjekte und des Betrachtungsbereichs ebenso wie die Definition des Simulationskonzepts sowie der Simulationsszenarien bzw. Testfälle.[8] Des Weiteren werden die erforderlichen Daten zur Umsetzung des Modellkonzepts erhoben und es wird die Simulationsart der jeweiligen Komponenten bestimmt. Mit dieser Phase wird die Grundlage für das Simulationsmodell und die Systemdefinition geschaffen, was die Systemabgrenzung und das Systemkonzept samt Wirkstruktur beinhaltet.[9] Insgesamt müssen für den Betrachtungsbereich der hybriden Testumgebung infolge der Vorbereitungsphase alle relevanten Informationen über Netz-

6 Vgl. Lass, Theuer und Gronau (2011), S. 14.
7 Law, Kelton und Kelton (1991), S. 106-109; vgl. Shannon (1998).
8 Bundesamt für Sicherheit in der Informationstechnik (2016a), S. 16 ff.
9 Bossel (2004), S. 25 und S. 40-41; Nance (1994), S. 8.

bereiche, Komponenten, Anwendungen etc. der bestehenden oder geplanten Anlage vorliegen.[10] Zum Abschluss der Vorbereitungsphase wird das Konzeptmodell mithilfe der Festlegungen zur Simulationsart der Komponenten in ein formales Modell überführt, welches implementiert werden kann.[11] Diese Schritte sollten wohlüberlegt sein, nachvollziehbar und gut dokumentiert, denn nur wenn die Simulationsart der Komponenten in einer hybriden Testumgebung sinnvoll bestimmt wurde, ist gewährleistet, dass die Sicherheitsanalyse zu realitätsnahen und belastbaren Ergebnissen führen kann.[12] Zur Bestimmung der Simulationsart wird daher in Abschnitt 5.2 eine Klassifikation beschrieben, um den Implementationsaufwand weiter zu reduzieren.[13]

In der zweiten Phase werden einerseits die Hardware-Komponenten entlang des Modellkonzepts installiert und die simulierten, emulierten oder virtualisierten Komponenten konfiguriert.[14] Hierfür kann auf die Informationen aus der Vorbereitungsphase zurückgegriffen werden. Andererseits werden auch die physischen, mechanischen oder chemischen Wertschöpfungsprozesse der Anlage mithilfe einer entsprechend konfigurierten Prozesssimulation abgebildet, wobei reale Prozesse für Sicherheitsanalysen in ihrer Komplexität auch deutlich reduziert dargestellt werden können.[15]

Insbesondere in dieser Phase kann mit der Erstellung einer Bibliothek von Simulationsobjekten ein Vorschlag für eine schnelle und aufwandsarme Implementierung von hybriden Testumgebung zum Tragen kommen. In dieser Bibliothek können die Informationen vergangener Erhebungen etwa hinsichtlich der Konfiguration und der Eigenschaften von simulierten oder emulierten Objekten festgehalten werden, welche in anderen Testumgebungen wiederverwendet werden können und den Implementationsaufwand reduzieren.[16] Sofern also entsprechende Simulationsbausteine vorhanden sind, reduziert dies den Arbeitsaufwand.[17] Solche Bibliotheksobjekte können zur einfacheren Handhabung nach verschiedenen Kriterien klassifiziert werden, womit Abhängigkeiten berücksichtigt werden. Neben der Dokumentation von Eigenschaften kann auch die Zuordnung zur Anwendender- oder Simulationsbetriebsebene dokumentiert werden.[18] Auf diese Weise lassen

10 BSI-Standard 200-2 (2017b), S. 70 ff.

11 Rabe, Spieckermann und Wenzel (2008b), S. 47-48.

12 Holm u. a. (2015), S. 21-23.

13 Lass (2011), S. 601, der die Erstellung eines solchen Maßstabs vorschlägt. Vgl. Lass, Theuer und Gronau (2011), S. 15; vgl. Lass und Gronau (2012), S. 6.

14 Lass, Theuer und Gronau (2011), S. 14; Bossel (2004), S. 25.

15 Green u. a. (2017), S. 5.

16 Vgl. Lass (2011), S. 14-15.

17 Vgl. Rabe, Spieckermann und Wenzel (2008b), S. 130-131.

18 Vgl. Holm u. a. (2015), S. 21-23.

sich Standardsituationen schneller abbilden.[19] Im Beispiel der Prozesssimulation ist etwa für kleine und mittlere Wasserversorger eine vorkonfigurierte Prozesssimulation denkbar, welche je nach Prüfobjekt nur leicht angepasst werden muss.

In der dritten Phase erfolgt daraufhin die Konfiguration der Testumgebung, indem die Wirkbeziehungen der Komponenten für das Betriebsszenario in einen funktionalen Zusammenhang zueinander gestellt werden.[20] Die Teilsysteme werden in dieser Phase zu einem Gesamtsystem zusammengestellt, wozu etwa die Zeitsynchronisation der Systeme oder auch die Konfiguration der Analytik gehören kann. Optional kann an dieser Stelle auch die Anwenderebene mit dem Gesamtsystem verknüpft werden, etwa wenn hier spezielle Systeme zur Bereitstellung von Benutzerschnittstellen oder auch Benutzerinteraktionssimulatoren zum Einsatz kommen sollen.

In der vierten Phase kann die Sicherheitsanalyse mithilfe des ausführbaren Modells durchgeführt und die Testumgebung ggf. angepasst werden. Die dabei anfallenden Daten können ausgewertet und das System kann modifiziert werden.[21] Mittels der verifizierten und validierten Testumgebung können die Assets des Prüfobjekts auf Angriffsvektoren untersucht und mögliche Sicherheitslücken aufgedeckt und mögliche Lösungsansätze überprüft werden.[22] Nach Abschluss der Sicherheitsanalyse können die Sicherheitsmaßnahmen des Unternehmens angepasst werden und die Ergebnisse fließen in den Informationssicherheitsprozess ein.[23] Ebenso müssen die Ergebnisse der Sicherheitsanalyse in der Auswertung ggf. auf die Originalanlagen übertragen werden, wobei der Transferaufwand aufgrund der Realitätsnähe im Regelfall minimal ist.[24] Die Sicherheitsanalyse und alle Teilschritte müssen so wie der Informationssicherheitsprozess kontinuierlich dokumentiert werden, um die Ergebnisse und die daraus resultierenden Entscheidungen qualitätssichern und später nachvollziehen zu können. Auch kann so auf die erhobenen und ausgewerteten Informationen auch an anderer Stelle zurückgegriffen werden.[25]

Das Modell und sein Verhalten müssen während den unterschiedlichen Phasen in Bezug auf das Konzeptmodell, das formale Modell und das ausführbare Modell in Form der hybriden Testumgebung fortlaufend verifiziert und validiert werden. Hierfür werden auch die Ergebnisse des Simulationsbetriebs in der letzten Pha-

19 Lass, Fohrholz und Theuer (2011), S. 14-15.

20 Vgl. Bossel (2004), S. 41-42.

21 Vgl. Lass und Gronau (2012), S. 4; vgl. Lass (2011), S. 600; vgl. Shannon (1998), S. 11.

22 Vgl. Schumacher (2016), S. 677.

23 Bundesamt für Sicherheit in der Informationstechnik (2016a), S. 21-26; BSI-Standard 200-2 (2017b), S. 126.

24 Vgl. Gurschler u. a. (2017), S. 405.

25 BSI-Standard 200-2 (2017b), S. 56 und S. 93.

se herangezogen. In der Verifikation und Validierung wird etwa überprüft, ob die Entitäten und Elemente des Modells vollständig sind, konsistent, plausibel, hinreichend spezifisch und für die Ziel- und Aufgabenstellung angemessen. Das Modell kann ggf. bis auf die Attributebene der Entitäten mit den aufbereiteten Daten abgeglichen werden.[26]

Insgesamt beschreibt das Vorgehensmodell die einzelnen Schritte und Ansätze zur aufwandsarmen Implementation einer hybriden Testumgebung für cyberphysische Sicherheitsanalysen. Es dargelegt, dass hier weiteres Optimierungspotential zur Vereinfachung der Implementation besteht, etwa in der Erarbeitung einer Bibliothek von Simulationsobjekten, in der Dokumentation guter Praxis oder der Detaillierung der Standardisierung des hybriden Simulationsansatzes.[27]

5.2 Klassifikation zur Bestimmung der Simulationsart von Komponenten

Der Ordnungsprozess der Klassifikation zur Bestimmung der Simulationsart von Komponenten für eine hybride Testumgebung besteht aus drei Schritten und kommt in der Vorbereitungsphase des Vorgehensmodells zur effizienten Modellierung einer hybriden Testumgebung zum Einsatz (s. Abbildung 12).[28] Methodisch ist das Ordnungsziel des Klassifikationsschemas eine schrittweise Zuordnung der Ordnungsmenge typischer Anlagenkomponenten entlang von Ordnungsmerkmalen unterschiedlicher Ordnungsdimensionen, um letztlich für den Betrachtungsbereich eines Informationsverbunds die jeweils angemessene Simulationsart der Komponenten festlegen zu können.[29] Im systematisch-hierarchischen Ordnungssystem werden die Komponenten im Verlauf der Klassifikation anhand von Regeln zugeordnet, um diese zueinander in Beziehung zu bringen. Hierfür wird zuerst die Ordnungsmenge bestimmt, woraufhin diese anhand von Ordnungsmerkmalen und Ordnungsdimensionen schrittweise hierarchischen Ordnungsklassen zugeordnet werden, wobei Ordnungsprinzipien die Klassifizierung leiten können.[30] Die hier abstrakt beschriebene Methodik wird in den drei Schritten der Klassifikation

[26] Rabe, Spieckermann und Wenzel (2008b), S. 18 und S. 181-191; Rabe, Spieckermann und Wenzel (2008a), S. 1720.

[27] Bundesministerium für Wirtschaft und Energie (2013), S. 15; Lass (2011), S. 601; Lass, Theuer und Gronau (2011), S. 14-15.

[28] Vgl. Henzler (1992), S. 59.

[29] Vgl. Gronau (2009), S. 42-44; vgl. Henzler (1992), S. 60.

[30] Vgl. Gronau (2009), S. 42; vgl. Laisiepen, Lutterbeck und Meyer-Uhlenried (1972), S. 185-225; vgl. Gronau und Weber (2009), S. 7-10.

im Detail konkretisiert sowie anhand von drei idealtypischen ICS-Architekturen als Fallbeispiele erläutert (s. Abbildung 13).

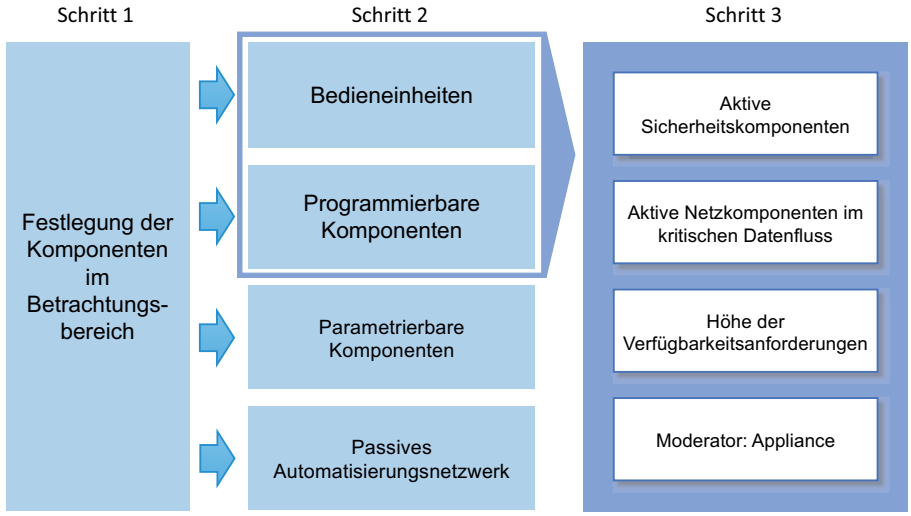

Abb. 13: Klassifikation zur Simulationsartbestimmung

Zunächst soll an dieser Stelle ein Kurzüberblick der einzelnen Schritte vorgenommen werden, bevor diese im Detail beschrieben werden.

In Schritt 1 wird zunächst die Ordnungsmenge festgelegt, was bedeutet, dass die grundsätzlich für die Testumgebung zu betrachtenden Komponenten bestimmt und relevante Daten erfasst werden, nachdem der Betrachtungsbereich der Sicherheitsanalyse festgelegt wurde. Hierfür baut die Klassifikation auf etwaige Vorarbeiten des Informationssicherheitsprozesses auf (s. Abschnitt 5.1).

In Schritt 2 werden die zu betrachtenden Komponenten anhand ihrer logisch-funktionalen Eigenschaften und Merkmalsausprägungen vier übergeordneten Komponentenklassen zugeordnet: Passives Automatisierungsnetzwerk, Parametrierbare Komponenten, Programmierbare Komponenten und Bedieneinheiten.[31] Mit der Zuordnung von Komponenten zu den an jener Stelle erläuterten Klassen Passives Automatisierungsnetzwerk und Parametrierbare Komponenten kann mit der com-

[31] Die Komponentenklassen werden in dieser Ausarbeitung als mehrteiliger Eigenname großgeschrieben, um insbesondere die Klassen Programmierbare Komponenten und Parametrierbare Komponenten von entsprechend adjektivierten Komponenten zu unterscheiden, die als spezifische Komponenten ggf. keine Verbindung zu den Komponentenklassen aufweisen.

puterbasierten Simulation für diese Komponenten bereits eine passende Simulationsart festgelegt werden.[32] Mit den übrigen Komponentenklassen wurden jene Komponenten identifiziert, bei denen eine physische Abbildung im Simulationsmodell möglicherweise angezeigt ist und welche daher im dritten Schritt betrachtet werden.

Das Ergebnis des dritten Schritts ist eine Empfehlung, welche der restlichen Komponenten der Klassen Bedieneinheiten und Programmierbare Komponenten real in die Testumgebung integriert werden sollten. Die Komponenten werden hierfür mithilfe von Ordnungsmerkmalen und Ordnungsprinzipien in Form von drei eigenständigen Kriterien angeordnet: (1) Aktive Sicherheitskomponenten, (2) Aktive Netzkomponenten im kritischen Automatisierungsnetz sowie (3) die Höhe der Verfügbarkeitsanforderungen.[33] Komponenten, welche nicht unter eines der Kriterien fallen, werden computerbasiert abgebildet und dabei bevorzugt realitätsnah emuliert oder virtualisiert. Darüber hinaus gibt es mit dem Moderator „Appliance“ ein weiches Kriterium, das bei der Frage Anwendung finden kann, ob eine wiedergabetreue Emulation oder Virtualisierung etwa aus Ressourcen- oder Aufwandsgründen eine Alternative zur physischen Integration sein kann oder nicht.

Das erste Kriterium basiert auf der Überlegung, dass aktive Sicherheitskomponenten für die Sicherheit einer Anlage offenkundig eine herausgehobene Bedeutung haben. Sie sollten beispielsweise angesichts von Buffer-Overflow- oder (D)DoS-Attacken real in eine Testumgebung integriert werden. Nur auf diese Weise ist ein originalgetreues Verhalten der Hard- und Software angesichts von Attacken gegeben und kann überprüft werden.

Aktive Netzkomponenten im kritischen Automatisierungsnetz sind das zweite Kriterium. Ähnlich wie Sicherheitskomponenten sind Netzkomponenten für eine Industrieanlage von außerordentlicher Wichtigkeit, da sie die einwandfreie Kommunikation und Datenübertragung gewährleisten. Dies gilt allerdings nicht für alle Netzkomponenten in gleichem Maße, weswegen vor allem Komponenten im kritischen Automatisierungsnetz betroffen sind.

Das dritte und letzte Kriterium ist die Höhe der Verfügbarkeitsanforderungen. Von den restlichen Komponenten sind jene Komponenten physisch abzubilden, welche über besonders hohe Verfügbarkeitsanforderungen verfügen, da der kritische Wertschöpfungsprozess von ihnen in höchstem Maße abhängig ist. Hierfür wird, sofern Ergebnisse aus einer vorherigen Schutzbedarfsanalyse nicht vorliegen oder nicht ausreichen, eine Kurzanalyse zur Feststellung der Verfügbarkeitsanforderungen vorgeschlagen.

---

32 Vgl. Gronau (2009), S. 42.

33 Vgl. ebd., S. 42.

Wenn eines der Kriterien auf eine Komponente zutrifft, sollte die jeweilige Komponente real in die Testumgebung eingebunden werden. Den Kriterien – wie auch den Komponentenklassen der Klassifizierung – liegen insgesamt vorrangig Überlegungen zur Gewährleistung der Verfügbarkeit zu Grunde. Für ICS sind vor allem Verfügbarkeit, Integrität und Vertraulichkeit wichtig – in dieser Reihenfolge.[34] Verfügbarkeit ist der wichtigste Grundwert, denn eine Verletzung des Grundwerts bedeutet die Unterbrechung oder den Ausfall von Komponenten oder Prozessen.[35] Die Schäden, die bei einem Verlust der Verfügbarkeit entstehen können, können unterschiedlicher Natur sein und etwa eine Beeinträchtigung der Aufgabenerfüllung oder Verstöße gegen Rechts- oder Verwaltungsvorschriften zur Folge haben.[36] Die Klassifikation basiert insofern im Wesentlichen auf der Prämisse, dass sich bestimmte Attacken und Angriffsarten schon bei kleineren Unterschieden zwischen einer realen und einer computerbasierten Komponente unterschiedlich auswirken können. Deshalb sollten bestimmte Komponenten möglichst real in die Testumgebung integriert werden.

Neben dem Grundwert der Verfügbarkeit liegen der Klassifikation auch Überlegungen zur technischen Möglichkeit bzw. Einfachheit einer wiedergabetreuen computerbasierten Abbildung einer Komponente zu Grunde. Die Komponenten der Klassen Passives Automatisierungsnetzwerk und Parametrierbare Komponenten aus dem zweiten Schritt lassen sich aufgrund ihrer Eigenschaften in der Regel mit hoher Realitätsnähe computerbasiert abbilden, ungeachtet ihrer Relevanz für den Grundwert der Verfügbarkeit. Komponenten der Klassen Bedieneinheiten und Programmierbare Komponenten sind hingegen, sofern sie unter die Kriterien des dritten Schritts fallen, besonders wichtig im Hinblick auf den Grundwert der Verfügbarkeit. Auch lassen sie sich zudem in der Regel nicht so leicht realitätsnah computerbasiert abbilden, weshalb hier eine Integration der realen Komponenten angeraten ist.

Die Flexibilität hybrider Testumgebungen kann auch genutzt werden, um anstelle von möglichst effizienten und gleichzeitig realitätsnahen Testumgebungen andere Schwerpunkte in einer Sicherheitsanalyse zu setzen. Der hybride Ansatz ermöglicht es, Testumgebungen mit unterschiedlicher Wiedergabetreue, aber auch mit unterschiedlichem Aufwand zu erstellen.[37] Es muss dabei sorgfältig eine Balance zwischen Wiedergabetreue, Skalierbarkeit und Komplexitätsreduktion geschaffen werden.[38] Abweichungen von der Klassifikation sind insbesondere

34 IEC/ISA 62443-2-1:2015 (2015), S. 135.
35 Müller (2014), S. 186.
36 Vgl. BSI-Standard 200-2 (2017b), S. 88-90.
37 Vgl. Urias, Van Leeuwen und Richardson (2012), S. 4.
38 Vgl. Green u. a. (2017), S. 1; Holm u. a. (2015), S. 11.

dann möglich, wenn besondere Schwerpunkte, alternative Analyseszenarien oder Sicherheitsziele zu abweichenden Simulationsentscheidungen führen. Dies kann beispielsweise der Fall sein, wenn bestimmte Komponenten(gruppen) aufgrund von vergangenen Sicherheitsvorfällen, Änderungen oder Neueinführungen speziell überprüft werden sollen.[39] Allerdings können auch externe Faktoren wie die verfügbare Bearbeitungszeit, Ressourcen oder Kosten zu einem reduzierten Umfang oder Detaillierungsgrad einer cyber-physischen Sicherheitsanalyse führen.[40] Eine Möglichkeit in diesem Fall ist, die Anzahl der Elemente, den Datenumfang und Anzahl der Beziehungen der Elemente zueinander zu reduzieren oder die Simulationsart der Komponenten zu verändern.[41] Aus fachlicher Sicht kann sich hier aber auch die Frage stellen, ob eine gute Emulation oder Virtualisierung ausgewählter Komponenten bereits eine ausreichende Realitätsnähe bieten kann, wenn Abstriche bei der Implementation einer Wunsch-Testumgebung unvermeidlich sind.[42] Das weiche Kriterium „Appliance“ soll hierfür als Moderator einen Prüfstein bieten, der aufzeigt, wann diese Möglichkeit tendenziell gegeben ist und wann eher nicht. Wenn die Berücksichtigung von sicherheitsrelevanten Eigenschaften – beispielsweise eine identische Performanz, Konfiguration, Firmware, Software und Verhalten – gewährleistet wird, kann eine Emulation oder Virtualisierung unter Umständen ein guter Kompromiss sein. Dies gestaltet sich aber gerade bei Appliances oft schwierig, die aufgrund ihrer applikationsspezifischen Hardware seltener realitätsnahe Abbildungen ermöglichen. Gleichwohl kann mitunter auch ein Kompromiss gefunden werden: Wenn ein bestimmter Anlagenaufbau oder der Schwerpunkt einer Simulation eine größere Anzahl an kritischen Komponenten desselben Typs beinhaltet, ist es denkbar, nur einen kleinen Teil physisch abzubilden, während der Rest simuliert und/oder emuliert wird.[43]

Die Schritte der Klassifikation werden im Folgenden entlang derjenigen Komponententypen näher betrachtet, die in Kapitel 3 vorgestellt wurden. Zu diesem Zweck werden auch drei idealtypische Anlagenarchitekturen als Fallbeispiele für die Anwendung bzw. Überprüfung der jeweiligen Methoden zur Hilfe genommen. Die Klassifikation wird als fortschreitend verstanden, was bedeutet, dass sie auf

---

39 Andere Fälle, in denen von den Ergebnissen dieser Klassifikation abgewichen wird, können beispielsweise Testumgebungen für Sicherheitstrainings oder Schulungen sein, bei denen eine Emulation oder Simulation ggf. ausreichend ist. Urias u. a. (2017), S. 1-6; Jaromin u. a. (2013), S. 38.

40 Vellaithurai, Biswas und Srivastava (2017), S. 2193-2194.

41 Rabe, Spieckermann und Wenzel (2008b), S. 127-130.

42 Für besonders kritische Komponenten sind Simulationen in der Regel nicht als ausreichend realitätsnah anzusehen, wie in Abschnitt 4.3 dargelegt wurde.

43 Van Leeuwen u. a. (2009), S. 6.

sich verändernde Gegebenheiten angepasst werden sollte, etwa hinsichtlich neuer oder weiterentwickelter Komponententypen.

5.2.1 Schritt 1: Bestimmung der Objekte des Betrachtungsbereichs

Im ersten Schritt der Klassifikation werden der Betrachtungsbereich und die zu analysierenden Komponenten der Testumgebung festgelegt. Ziel ist, dass das Simulationsmodell in diesem ersten Schritt auf jene Elemente reduziert wird, welche für die cyber-physische Sicherheitsanalyse als relevant erachtet werden und grundsätzlich in der Testumgebung abgebildet werden sollen.[44] In diesem Schritt wird somit die Ordnungsmenge der Klassifikation bestimmt.[45]

Für die hybride Testumgebung wird ein passendes Modellkonzept des Originalsystems benötigt, das die Risikosituation mit den relevanten Parametern adäquat abbildet, jedoch nach Möglichkeit nicht unnötig komplex ist.[46] Hierbei kann sich grundsätzlich am Informationsverbund des Prüfobjekts orientiert werden. Zur Definition des Informationsverbunds kann also idealerweise an Vorarbeiten des Informationssicherheitsprozesses angeknüpft werden.[47] So ist denkbar, dass mithilfe der Methodik nach IT-Grundschutz bereits Schwachstellen identifiziert, Sicherheitsmaßnahmen überprüft und Sicherheitszonen gemäß Schutzbedarf eingerichtet wurden.[48] Eine zuvor durchgeführte Schutzbedarfsanalyse kann hier eine Priorisierung im Hinblick auf das Prüfobjekt ermöglichen, indem der Geltungsbereich auf Zielobjekte mit einem erhöhten Schutzbedarf beschränkt wird.[49] Der insbesondere infolge der (Kern-)Absicherung definierte Informationsverbund kann auf diese Weise für die cyber-physische Sicherheitsanalyse abgegrenzt und genutzt werden.[50]

---

44 Stachowiak (1973), S. 131 ff.; BSI-Standard 200-3 (2016), S. 9.

45 Gronau (2009), S. 42.

46 Sowa (2017), S. 18; vgl. Gronau, Fohrholz und Lass (2011), S. 207; Lass und Gronau (2012), S. 5.

47 Schumacher (2016), S. 677.

48 BSI-Standard 200-2 (2017b), S. 103 ff. Siehe auch NET.1.1 Netzarchitektur und -design sowie IND.1: Betriebs-und Steuerungstechnik. Auch hier sei betont, dass der IT-Grundschutz nur ein exemplarischer, da für KMU in Deutschland besonders relevanter Standard ist und die entsprechenden Vorarbeiten in den meisten Methoden und Standards in der Informationssicherheit zum Einsatz kommen und genutzt werden können.

49 Dies ist notwendig, wenn der Informationsverbund weiterhin zu groß ist. Bei kleineren Anlagen kann dieser Schritt verzichtbar sein. BSI-Standard 200-3 (2016), S. 9-10.

50 BSI-Standard 200-3 (2016), S. 10; BSI-Standard 200-2 (2017b), S. 64-65.

Grundsätzlich kann der eigentliche Betrachtungsbereich der cyber-physischen Sicherheitsanalyse je nach Zielstellung unterschiedlich ausfallen. Er muss nicht zwangsweise den kompletten Informationsverbund abbilden, etwa wenn mit der hybriden Testumgebung nur ein bestimmter Aspekt des Informationsverbunds überprüft werden soll. So kann der Betrachtungsbereich variieren, je nachdem, ob eine Anlage mit dem Internet verbunden ist oder ob ein Angriff von innen oder von außen analysiert werden soll. Ebenso können Anlagenbereiche, die nicht im näheren Interessensgebiet liegen, abstrahiert dargestellt werden.[51]

Nach der grundsätzlichen Festlegung des Betrachtungsbereichs werden die Informationen zum Anlagennetzwerk sowie zu den Anlagenkomponenten des Betrachtungsbereichs erfasst. Im Optimalfall kann auch für diese Datenerhebung auf Vorarbeiten zurückgegriffen werden, beispielsweise infolge eines Sicherheitskonzeptes mit (Kern-)Absicherung nach IT-Grundschutz, wozu insbesondere die Strukturanalyse gehört.[52] Ein geeigneter Ausgangspunkt für die Erfassung kann der Netzplan sein, der Systeme und Netzverbindungen des betrachteten Bereichs abbildet. Im Ergebnis müssen folgende Elemente inventarisiert werden, welche für die Analyse des Betrachtungsbereichs benötigt werden:

- Geschäftsprozesse
- Prozessverantwortliche Person(en)
- Informationen
- Anwendungen und Datenträger
- IT-Systeme, ICS-Systeme und ähnliche Objekte
- Räume und Gebäude
- Kommunikationsnetze, Kommunikationsschnittstellen und Netzpläne[53]

Es bedarf zu jedem dieser Objekte eines Minimalsatzes an Informationen, wozu eine eindeutige Bezeichnung, Name, Funktion, Typ, Version, Firmware, Anwendungen, die zugrundeliegende Plattform, Standort, vorhandene Kommunikationsschnittstellen sowie die Art der Netzanbindung und Netzadressen gehören. Für die Netzverbindungen sollte des Weiteren zur Art der Kommunikationsanbindung die Datenübertragungsrate, die verwendeten Netzprotokolle sowie Details zu externen Netzen vorliegen. Dies gilt ebenso für virtuelle Systeme und Netze.[54] In Anleh-

51 Vgl. Van Leeuwen u. a. (2010), S. 1809; Bundesamt für Sicherheit in der Informationstechnik (2016a), S. 16-17; Department of Homeland Security (2016), S. 9.

52 BSI-Standard 200-2 (2017b), S. 105-117; BSI-Standard 200-3 (2016), S. 9; Bundesamt für Sicherheit in der Informationstechnik (2016a), S. 20; vgl. Lass (2011), S. 600.

53 BSI-Standard 200-2 (2017b), S. 72 ff.

54 Vgl. BSI-Standard 100-2 (2008), S. 42-46. Grundsätzlich ist hierbei eine Komplexitätsreduktion, wie sie im BSI-Standard 200-2 an verschiedenen Stellen vorgeschlagen wird, denkbar.

nung an die Vollständigkeitsprüfung nach IT-Grundschutz kann etwa anhand des Netzplans überprüft werden, ob das Modellkonzept der Simulation vollständig ist und keine Lücken aufweist.[55]

Häufig reichen die vorhandenen Informationen für Simulationsaufgaben noch nicht aus und müssen vertieft und überprüft werden.[56] Daher kann es notwendig sein, in einem iterativen Prozess mittels Interviews, Systemanalysen und Dokumentenanalysen noch benötigte Eigenschaften und relevante Randbedingungen zur Hard- und Software sowie weitere Prozessdetails zu erheben.[57] Dies ist wichtig, denn veränderte Spezifikationen oder unterschiedliche Ausführungen oder Versionen von Komponenten können das Ergebnis der späteren Sicherheitsanalyse verzerren.[58] Zu diesem Zweck sollten externe Sicherheitsexperten mit den IT- oder ICS-Verantwortlichen in einer iterativen und partizipativen Vorgehensweise zusammenarbeiten.

Neben der qualitativen Erfassung von Informationen zu Netztopologien und den genutzten Komponenten, Anwendungen, Systemen und ähnlichem können darüber hinaus Anwendungen zur Analyse des Netzwerkverkehrs eingesetzt werden. So werden Anwendungen wie Wireshark oder The Open Vulnerability Assessment Language Interpreter genutzt, um Konfigurationen zu erheben oder zu überprüfen. Tools wie Nmap und Antfarm können zur Netzwerkerkennung eingesetzt werden, Firewalk oder NetAPT zur Erfassung von Firewallregeln und Nessus zur Erhebung von Schwachstellen. Während sich diese Tools sehr gut zur Analyse von üblichen Anwendungen und Betriebssystemen eignen, sind sie weniger hilfreich zur Analyse von spezifischen ICS-Komponenten. Für ICS-Komponenten ist stattdessen die Nutzung von agentenbasierten Systemen zur Erfassung von Konfigurationsdateien üblich, aber auch die zuvor beschriebene manuelle Erfassung kann bei kleineren Systemen völlig ausreichend sein.[59]

An dieser Stelle kann die Festlegung und Erfassung des Betrachtungsbereichs der hybriden Testumgebung abgeschlossen sein. Je nach Bedarf kann aber auch eine Komplexitätsreduktion vorgenommen werden. Auf die gleiche Weise, wie der Betrachtungsbereich der Testumgebung je nach Zielstellung angepasst werden kann, kann sich das Simulationsmodell von der Originalanlage unterscheiden, um eine handhabbarere oder aufwandsärmere Testumgebung zu realisieren. Hierbei muss jedoch zwingend darauf geachtet werden, dass die Testumgebung weiter-

55 Bundesamt für Sicherheit in der Informationstechnik (2016b), S. 92.

56 Vgl. Rabe, Spieckermann und Wenzel (2008b), S. 46-92.

57 Vgl. Lass (2011), S. 600-601; vgl. Gronau, Fohrholz und Lass (2011), S. 207; vgl. Lass und Gronau (2012), S. 5.

58 Vgl. Urias und Van Leeuwen (2016), S. 261.

59 Holm u. a. (2015), S. 20-21.

hin von einer hohen Realitätsnähe gekennzeichnet ist. Eine Komplexitätsreduktion sollte daher nur wohlüberlegt vorgenommen werden. Ein wichtiger Aspekt bei der Komplexitätsreduktion von hybriden Testumgebungen ist es, die Homogenität oder Heterogenität von Komponenten und Netzen gebührend zu berücksichtigen.[60] So ist es grundsätzlich denkbar, Netzbereiche mit identischen Komponenten, die redundant ausgelegt sind, verkürzt abzubilden, etwa indem nur eine Teilmenge dieser Komponenten abgebildet wird. Bei identischen kritischen Komponenten, die physisch abgebildet werden sollen, kann eine Teilmenge emuliert oder simuliert werden.[61] Hierbei ist darauf zu achten, dass insbesondere kritische Bereiche nicht oder nur insofern beschränkt abgebildet werden, dass weiterhin eine umfängliche Sicherheitsanalyse möglich ist, etwa was Lasttests angeht. Ebenso kann es vorkommen, dass SCADA-Anlagen mehrfach verteilte lokale Netzbereiche aufweisen, die nahezu identisch sind. In einem solchen Fall kann eine Betrachtung einer Teilmenge der Gesamtanlage reichen, da und sofern von dieser Teilmenge ohne Informationsverlust auf die Informationssicherheit der Gesamtanlage geschlossen werden kann.

Anwendungsbeispiel der Klassifikation: Schritt 1

Wie eingangs angekündigt wurde, sollen zu jedem Schritt bzw. Kriterium der Klassifikation Anwendungsbeispiele kursorisch dargestellt werden. Hierbei sollen unterschiedliche ICS-Architekturen Berücksichtigung finden.

Um die Anwendungsbeispiele möglichst kurz und bündig zu halten, wird in den weiteren Ausführungen im Regelfall eine idealtypische DCS-Kleinanlage beleuchtet, welche aus Abbildung 5 in Kapitel 3 bekannt ist und in Anlage A.1 als Großdarstellung zu finden ist. Der beispielhafte Anwendungsfall ist eine mit dem Internet verbundene DCS-Kleinanlage, die einer Sicherheitsanalyse per Penetrationstest in Form von Control-Channel-Attacken über das Internet bzw. Netzwerk unterzogen werden soll.[a] Das Ziel ist der Schutz der physischen Wertschöpfungsprozesse. An passender Stelle kann ebenfalls kurz auf eine idealtypische SCADA-Kleinanlage eingegangen werden (Abbildung 4 bzw. Anlage A.2). Beim dritten Kriterium des dritten Schritts werden nicht nur Ergebnisse dargestellt, sondern es wird einmalig auch eine größere SCADA-Anlage beispielhaft betrachtet, da Feinheiten der Kurzanalyse von Verfügbarkeitsanforderungen im Hinblick auf den Mehrwert der Abhängigkeitsanalyse aufgezeigt werden können (s. Anlage A.3).

60 Green u. a. (2017), S. 4.

61 Vgl. Van Leeuwen u. a. (2009), S. 6.

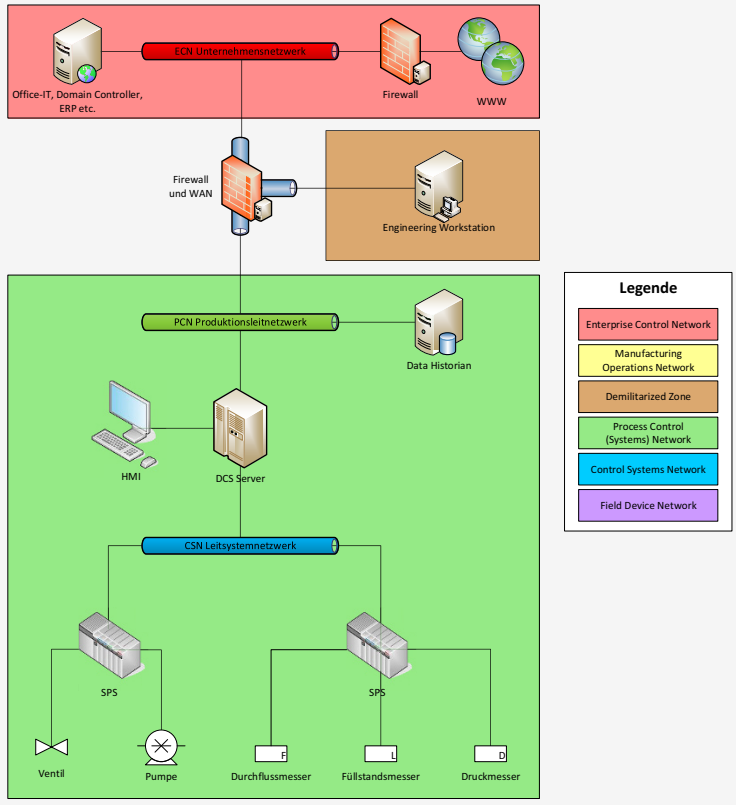

Abb. 14: Aufbau einer idealtypischen und zonierten DCS-Kleinanlage

Im Allgemeinen werden die Anwendungsbeispiele nur kurz erläutert. Für etwaige Grundlagen oder Ergebnisdokumente sind die jeweiligen Abschnitte zurate zu ziehen. Es wird sich anhand der Beispiele zeigen, dass die Anwendung der Klassifikation auf diese Anlagen unkompliziert und einfach sowie schnell und aufwandsarm vonstattengeht. Daran wird deutlich, dass die umfängliche wissenschaftliche Auseinandersetzung innerhalb der jeweiligen Abschnitte einer schmalen, zugänglichen und schnell durchführbaren Klassifikation nicht entgegensteht. Dennoch konnte dadurch gewährleistet werden, dass die Klassifikation auf größere und vor allem auch heterogene Anlagen ebenso gut anwendbar ist. Im Anschluss an die vorliegende Ausarbeitung ist daher die Erarbeitung eines leichtgewichtigen Leitfadens auf dieser Grundlage denkbar.

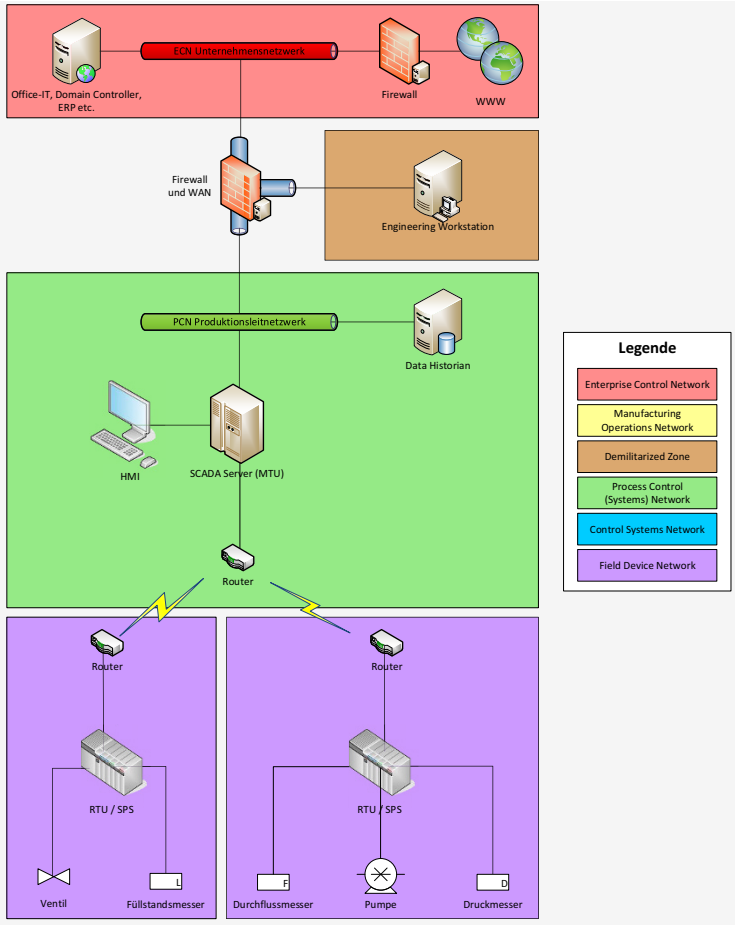

Abb. 15: Aufbau einer idealtypischen und zonierten SCADA-Kleinanlage

In Schritt 1 wird der grundsätzliche Betrachtungsbereich auf Basis einer Strukturanalyse festgelegt, was der Abbildung entspricht. Dazu gehören also die Steuerungs- und Betriebstechnikkomponenten der Feld-, Steuerungs- und Prozessleitebene (grün gefärbte Zone des Produktionsleitnetzwerks). Des Weiteren können relevante Komponenten der demilitarisierten Zone mit einbezogen werden, da diese Zone eine Schutzgrenze zwischen der Fertigungsebene und dem Unternehmensnetzwerk ist. In der demilitarisierten Zone werden oft Anwendungen zur Verfügung gestellt, die mit der Fertigungsebene kommunizieren, wie Remotezugänge, Data Historians oder bestimmte Work-

stations, welche selber Schwachstellen sein können. Als Angriffsvektor kann die Unternehmensebene durch die dargestellte Auswahl wesentlicher Komponenten in den Betrachtungsbereich einbezogen werden[b] In der Unternehmensebene wird die gewöhnliche Office IT vorgehalten, die anfälliger für Angriffe ist, aber auch über die demilitarisierte Zone aggregierte Daten aus dem Fertigungsprozess verarbeitet und somit mittelbar mit der Fertigungsebene verbunden ist.[c]

[a] McLaughlin u. a. (2016), S. 1042 ff.; IEC/ISA 62443-1-1:2007 (2007), S. 70. Diese werden mitunter auch Communication-Channel-Attacken genannt.

[b] Vgl. Bundesamt für Sicherheit in der Informationstechnik (2016a), S. 16-17; Department of Homeland Security (2016), S. 9.

[c] Green u. a. (2017), S. 2.

Im Ergebnis wird im ersten Schritt der Klassifikation der Betrachtungsbereich des Simulationsmodells definiert, was eine Festlegung der grundsätzlich zu betrachtenden Komponenten als Ordnungsmenge der Klassifikation beinhaltet.[62]

5.2.2 Schritt 2: Grobklassifikation und Festlegung der Simulationsart für die Objekte der Klassen Parametrierbare Komponenten und Passives Automatisierungsnetzwerk

Nachdem die Ordnungsmenge mit den zu betrachtenden Komponenten in Schritt 1 festgelegt wurde, werden die Komponenten im zweiten Schritt des Ordnungsprozesses vier übergeordneten Komponentenklassen gemäß ihrer logisch-funktionalen Eigenschaften zugeordnet. Auf diese Weise kann die Simulationsart für einen Teil der Komponenten bereits in diesem Schritt festgelegt werden.

Birkhold und Lechler haben in ihren Arbeiten zur Modellierung von Automatisierungssystemen festgestellt, dass der Komponentenaufbau von Industrieanlagen zwar prozessspezifisch ist, aber grundsätzlich immer ähnliche Gruppen von Komponenten zum Einsatz kommen: „Eine eingehendere Betrachtung zeigt, dass der Anwendungskontext und damit die Parametrierung oder Programmierung abhängig vom Einsatzzweck sind, jedoch der logisch-funktionale Umfang der einzelnen Komponenten [der Komponentengruppen] nicht variiert.“[63] Mithilfe der Vorschläge von Birkhold und Lechler können Komponenten anhand ihrer Merkmalsausprägungen in vier Komponentengruppen unterteilt werden, welche den übergeordneten Komponentenklassen entsprechen: Bedieneinheiten, Programmierbare Kom-

62 Vgl. BSI-Standard 200-3 (2016), S. 9; vgl. Gronau (2009), S. 42.

63 Birkhold und Lechler (2014), S. 303-304; vgl. Birkhold und Bauer (2014), S. 24-26.

ponenten, Parametrierbare Komponenten und Komponenten des Passiven Automatisierungsnetzwerks (s. Tabelle 2).[64]

Komponentenklasse	Beschreibung, Beispiele und Empfehlung
Bedieneinheit	*Beschreibung*: Die Komponente erlaubt die Bedienung der Maschine oder Anlage. Die Komponente verfügt über ein Betriebssystem, das die Ausführung von Programmen erlaubt und/oder logische Schnittstellen. *Beispiele*: Computer mit Bediensoftware wie Prozessleitsoftware (SCADA-MTU/DCS) bzw. Operator Workstations, Engineering Workstations, Supervisory Workstations, Application Workstations, Fernwartungskomponenten oder Data Historians, Bedienterminals, mobile Geräte. *Empfohlene Simulationsart*: Gegebenenfalls als reale Komponente, andernfalls in Form einer Emulation oder Virtualisierung.
Programmierbare Komponente	*Beschreibung*: Die Funktion der Komponenten ist vollständig durch den Anwender veränderbar in Abhängigkeit von einer Programmierung. *Beispiele*: SPS (auch Slot-SPS oder Soft-SPS), programmierbare („intelligent“) RTU, programmierbare IED, CIF, programmierbare Safety-Systeme, aktive Netzwerkkomponenten wie Router, Modems oder Switches, aktive Sicherheitskomponenten wie Firewalls, (N)IDS oder (N)IPS. *Empfohlene Simulationsart*: Gegebenenfalls als reale Komponente, andernfalls in Form einer Emulation oder Virtualisierung.

64 Auch wenn die Merkmalsausprägungen des logisch-funktionalen Umfangs von einem ordinalen Charakter geprägt sind und Komponenten regelmäßig nach der höchstmöglichen Ausprägung gruppiert werden, ist die Komponentengruppierung dennoch als kategoriale Einteilung zu verstehen, die mithilfe der logisch-funktionalen Beschreibung nach Tabelle 2 vorgenommen wird.

Parametrierbare Komponente	*Beschreibung*: Das Verhalten der Komponente kann in Abhängigkeit von einem Parametersatz beeinflusst werden. Die Funktion der Komponenten bleibt dadurch unbeeinflusst. *Beispiele*: Feldgeräte (Sensorik/Aktorik), Sicherheitssysteme mit festgelegtem Verhalten (Safety-Systeme), RTU mit festgelegtem Verhalten, IED mit festgelegtem Verhalten. *Empfohlene Simulationsart*: Simulation oder Emulation.
Passives Automatisierungsnetzwerk	*Beschreibung*: Passive Komponenten des anlagen- oder maschineninternen Netzwerks zum Austausch von Daten ohne Echtzeitanforderung. *Beispiele*: Elektrotechnische Verkabelung, IT-Verkabelung, Feldbus, Steuerungsnetz. *Empfohlene Simulationsart*: Simulation oder Emulation.

Tabelle 2: Komponentenklassen: Merkmale, Beispiele und empfohlene Simulationsart. Adaptiert nach Birkhold und Lechler (2014), S. 304; mit freundlicher Genehmigung von © M. Birkhold (2014)

Komponenten des Passiven Automatisierungsnetzwerks sind Netzwerke zum Austausch von Daten. Parametrierbare Komponenten sind in ihrer Funktion eingeschränkt änderbar und verfügen, in Abhängigkeit von einem Parametersatz, über ein prädefiniertes Verhalten. Programmierbare Komponenten sind dadurch gekennzeichnet, dass sie in der Funktion programmierbar und somit grundsätzlich vollständig veränderbar sind. Bedieneinheiten sind Schnittstellen für den Nutzer zur Bedienung (von Teilen) der Maschine oder Anlage.[65]

Ziel dieses zweiten Schritts der Klassifikation ist nicht nur die Zuordnung aller abzubildenden Komponenten zu den vier Komponentenklassen, sondern ebenso die Festlegung der Simulationsart für einen Teil dieser Komponenten. Im Allgemeinen begründet sich der Unterschied zwischen den Komponentenklassen ei-

[65] Vgl. Birkhold und Bauer (2014), S. 24-26; Birkhold und Lechler (2014), S. 304-305.

nerseits in der Frage, wie einfach und realitätsnah eine Komponente der jeweiligen Klasse in der Testumgebung abgebildet werden kann. Andererseits spielen auch Sicherheitsüberlegungen eine Rolle, also etwa die Frage, inwiefern im Falle einer Kompromittierung von Komponenten einer Klasse größere Teile eines Anlagennetzwerks manipuliert werden können. So hat der Ausfall beispielsweise von parametrierbaren RTUs zwar den Verbindungsverlust zu Feldgeräten zur Folge. Steuerungstechnische Kaskadeneffekte, welche die Sicherheit des SCADA-Systems über das eigentliche Subsystem hinaus betreffen – etwa das Erlangen der Kontrolle über die Anlage durch einen Angreifer –, sind hier jedoch nicht zu erwarten.[66] Vor allem aber können sie leicht computerbasiert abgebildet werden.

Im Folgenden wird zunächst erläutert, wieso die (computerbasierte) Simulationsart der Klassen Passives Automatisierungsnetzwerk und Parametrierbare Komponenten an dieser Stelle bereits festgelegt werden kann. Komponenten der Klassen Bedieneinheiten und Programmierbare Komponenten werden hingegen erst im nächsten Schritt der Klassifikation detailliert betrachtet.

Komponenten des Passiven Automatisierungsnetzwerks haben keinen aktiven Einfluss auf den Netzwerkverkehr in einer Anlage, sondern leiten Signale ohne aktive Beeinflussung lediglich weiter.[67] Aktive Netzwerkkomponenten hingegen verarbeiten oder verstärken Signale und werden daher einer anderen Komponentenklasse zugeordnet.[68] Komponenten des Passiven Automatisierungsnetzwerks sind etwa bloß als Kabel sichtbar, haben jedoch auf logischer Ebene eine hohe Relevanz und dienen beispielsweise als Schnittstelle zwischen regulären Netzwerken und der eigentlichen Anlage oder verbinden Komponenten der Anlage.[69] In Industrieanlagen besteht der Übertragungsweg in der Regel aus mehreren Übertragungsabschnitten, welche aus verschiedenen Übertragungsmedien wie elektrische oder optische Signalübertragung oder Funk bestehen.[70] In diese Komponentenklasse fällt etwa die strukturierte Verkabelung, Rangier- bzw. Spleißverteiler, Patchfelder, Antennen zur Herstellung einer Funkverbindung, Anschlusstechnik, Steuerungsnetze, anlagen- oder maschineninterne Netzwerkwerkverbindungen zum Datenaustausch sowie die elektrotechnische Verkabelung, Verteilung und dazugehörige passive Schutzelemente.[71] Diese Komponenten können in der Regel kostengüns-

66 Nan, Eusgeld und Kröger (2013), S. 260.

67 Metter und Bucher (2012), S. 82.

68 Tiemeyer (2016), S. 271; Pigan und Metter (2015), S. 321.

69 Vgl. Birkhold und Lechler (2014), S. 305.

70 Vgl. Metter und Bucher (2012), S. 82; vgl. Mamzic, Gilbert und Lipták (2006), S. 504 ff.

71 Spitz, Blümle und Wiedel (2015), S. 249; Bundesamt für Sicherheit in der Informationstechnik (2016b), M 5.150 Durchführung von Penetrationstests; Invensys (2004), S. 9-13; BSI IT-Grundschutz-Kompendium (2017b); BSI IT-Grundschutz-Kompendium (2017c); Birkhold und Lechler (2014), S. 304.

tig und ausreichend realitätsnah computerbasiert in einer Testumgebung abgebildet werden. Da sie an der Wirkstruktur des Anlagenmodells nicht aktiv beteiligt sind, ist eine Simulation oder Emulation normalerweise ausreichend.[72] Zu dieser Empfehlung besteht natürlich die Ausnahme, dass Echtkomponenten infolge dieser Klassifikation ggf. auch mittels eines echten (Teil-)Netzwerks in die Gesamtarchitektur der hybriden Testumgebung integriert werden müssen. Die konkrete Entscheidung hierzu hängt vom jeweiligen Testszenario ab, ist jedoch als unkritisch anzusehen: Simulationssoftware für Netzwerke ist weit verbreitet und ressourceneffizient einsetzbar, für bestimmte Systeme des Passiven Automatisierungsnetzwerks aber nicht immer vorhanden. Hier kann eine Emulation ggf. einfacher zu implementieren sein.[73]

Parametrierbare Komponenten sind Komponenten, die ein festgelegtes Verhalten innerhalb bestimmter Wertebereiche haben und dabei in ihrem grundlegenden Funktionsumfang unverändert bleiben. Unter diese Komponentenklasse fallen Feldgeräte (Sensorik/Aktorik), Sicherheitssysteme mit festgelegtem Verhalten (Safety-Systeme) sowie RTUs und IEDs mit festgelegtem Verhalten. Einfache Beispiele für Parametrierbare Komponenten sind Regler wie etwa Servoumrichter oder Servomotoren, da auch sie einen unveränderlichen Funktionsumfang haben und innerhalb festgelegter Parameter agieren.[74] Aufgrund solcher Eigenschaften können Parametrierbare Komponenten mithilfe von entsprechender Software realitätsnah und aufwandsarm simuliert (oder emuliert) werden, da die endlichen Verhaltensweisen von parametrierbaren Komponenten vollumfänglich computerbasiert imitiert werden können. Aus diesen Gründen werden Feldgeräte – ebenso wie die physischen Wertschöpfungsprozesse – in Testumgebungen quasi nie emuliert, sondern meist simuliert.[75] Eine physische Integration in die Testumgebung ist für allgemeine Sicherheitsanalysen von Systemen mit Internetzugang hier nicht angezeigt, obgleich etwa die Sensorik ein lokales Einfallstor für Angriffe

---

72 Genge, Siaterlis und Hohenadel (2012), S. 229; Vellaithurai u. a. (2015), S. 60; Hong u. a. (2015), S. 268.

73 Jaromin u. a. (2013), S. 35.

74 Vgl. Talbot und Lipták (2006). In der Regel setzen Bedieneinheiten oder Programmierbare Komponenten wie SPS die Steuerungssignale für Parametrierbare Komponenten, die daher für eine Kompromittierung der Gesamtanlage ungleich kritischer sein können. Gonzalez und Reed (2016), S. 240.

75 Holm u. a. (2015), S. 17. Feldgeräte werden in vielen Testumgebungen auch physisch abgebildet, was jedoch mit der Zielstellung der jeweiligen Testumgebung zusammenhängt, etwa wenn diese auf die Erprobung von Produktionsmethoden abzielt.

sein kann.[76] Für andere Komponenten ist die Entscheidung zwischen Simulation oder Emulation vor allem vom Vorhandensein passender Software abhängig.

Anwendungsbeispiel der Klassifikation: Schritt 2

Im zweiten Schritt werden Komponenten der Kleinanlage mithilfe von Tabelle 2 aufgrund ihrer Eigenschaften den genannten Klassen zugeordnet. HMI, DCS-Server, Office-IT, Data Historian und Engineering Workstation werden der Klasse Bedieneinheiten zugeordnet. Die SPS-Bausteine und Firewalls sind Programmierbare Komponenten. Diese Komponenten werden in Schritt 3 weiter betrachtet. Hingegen können Ventil, Pumpe, Druckmesser etc. als Parametrierbare Komponenten sowie implizit die Verkabelung, sofern nicht für den Simulationsbetrieb notwendig, als Passives Automatisierungsnetzwerk simuliert werden. Diese Zuordnung ist größtenteils deckungsgleich mit der SCADA-Kleinanlage, wobei die Router als Programmierbare Komponenten eingeordnet werden.

Insgesamt können Anlagenkomponenten mithilfe der Beschreibung und Beispiele nach Tabelle 2 leicht zugeordnet werden.[77] Dies gilt auch für unterschiedliche Varianten eines Komponententyps. Bei Vorhandensein verschiedener Komponententypen in einem System (etwa ein IED mit parametrierbaren und programmierbaren Eigenschaften) vererben sich die kritischeren Eigenschaften der Klassen Programmierbare Komponente oder Bedieneinheit auf das jeweilige System. In diesem Fall ist eine computerbasierte Abbildung jener Komponenten und somit auch des Systems womöglich nicht hinreichend.[78] Aufgrund der heterogenen ICS-Landschaft kann eine Zuordnung im Einzelfall dennoch eine Herausforderung sein.[79] Deshalb werden im verbleibenden Teil dieses Abschnitts typische Varianten Parametrierbarer Komponenten diskutiert, bei denen eine Zuordnung nicht immer einfach ist. Erst danach wird im nächsten Abschnitt das weitere Vorgehen zu Programmierbaren Komponenten sowie Bedieneinheiten beschrieben.

---

76 Obgleich über physischen Zugang jedes System gestört werden kann, ist es im Kontext von Sicherheitsanalysen von Gesamtanlagen mittels Penetrationstests oder Schwachstellenanalysen nicht naheliegend, Aspekte der physischen Zugangskontrolle mittels einer solchen Sicherheitsanalyse prüfen zu wollen. Das reale Equipment, z.B. Pumpen, würden ggf. beschädigt werden. Attacken, bei denen Sensorsignale manipuliert werden, lassen sich jedoch grundsätzlich auch per Simulation darstellen. Vgl. Howser (2015), S. 123; Urbina u. a. (2016), S. 1092-1105.

77 Birkhold und Lechler (2014), S. 304-305.

78 Müller (2014), S. 248; Hafner und Breu (2008), S. 83; Kersten, Reuter und Schröder (2013), S. 139; BSI-Standard 200-2 (2017b), S. 91-92.

79 Vgl. Knapp und Langill (2014), S. 91.

Aus Tabelle 2 wird ersichtlich, dass etwa RTU, IEDs und Safety-Systeme entweder als parametrierbar oder als programmierbar gesehen werden können. Die Sicherheit der Kommunikation zwischen Benutzerschnittstelle und RTU ist für Sicherheitsanalysen von großem Interesse, da RTU eines der wichtigsten Ziele eines Angriffs sein können.[80] Klassischerweise sind RTUs parametrierbare Slave-Komponenten, die auf Anfrage der MTU bzw. des HMI-Servers agieren, und können gut simuliert oder auch emuliert werden.[81] Moderne RTUs sind jedoch oft um Funktionen erweitert, die etwa denen einer SPS entsprechen, um etwa in einem Wasserwerk einen teilautomatisierten Betrieb bei fehlender Netzwerkverbindung aufrecht zu erhalten, in welchem Fall diese als Programmierbare Komponenten ggf. physisch in der Testumgebung abgebildet werden sollten.[82]

Insbesondere bei IEDs kann eine Zuordnung zu Komponentenklassen schwierig sein: Wie in Kapitel 3 beschrieben wurde, sind IEDs nicht klar definiert und können sehr unterschiedliche Funktionalitäten aufweisen. So kann ein IED etwa ein Schutzrelais sein, welches unmittelbar mit der Prozessleitsoftware oder einem lokalen RTU kommuniziert und einen direkten Zugang zur Sensorik und Aktorik bieten kann. Ebenso gibt es IEDs, die ähnlich wie (Kombinationen von) RTU und SPS über „intelligente“ lokale Steuerungs- und Überwachungsmechanismen verfügen und als Standalone-Produkt mit anderen Komponenten kommunizieren.[83] Dabei verfügen sie je nach Ausführung über ein innerhalb eines Parametersatzes festgelegtes Verhalten oder können programmiert werden, um (teil-)autonom zu agieren.[84] So sind intelligente Mess-, Stell-, Kommunikations- und Leiteinrichtungen in der Regel parametrierbar und können gut simuliert oder ggf. emuliert werden. Neuere und komplexere IEDs, die über viele Funktionen und eine sehr hohe Anzahl von Variablen verfügen, sind als programmierbare Komponenten hingegen ggf. schwieriger computerbasiert abzubilden.[85]

Eng verknüpft mit IEDs sind auch Safety-Systeme nicht immer leicht zuzuordnen. Ein Safety-System (Sicherheitssystem) ist eine spezielle Komponente, die gewährleistet, dass der jeweilige Prozess einen potentiellen Gefahrenzustand wieder verlässt, indem Feldgeräte eines Wertschöpfungsprozesses beispielsweise korrigiert oder stillgelegt werden. Safety-Systeme sind deswegen mit Feldgeräten

80 Moss (2012), S. 39.

81 Queiroz u. a. (2009), S. 361; Hahn u. a. (2013), S. 850.

82 Knapp und Langill (2014), S. 90.

83 Strauss (2003), S. 47 ff.; Campbell, Wendt und Friedmann (2006), S. 971; Beard, Lipták und Girão (2006), S. 1121.

84 National Institute of Standards and Technology (2015), S. 2-5-2-6; vgl. Berge (2006), S. 571 ff.; Bastigkeit, Schossig und Steinhauser (2009), S. 55.

85 Schnell und Wiedemann (2008), S. 111; Bastigkeit, Schossig und Steinhauser (2009), S. 54-59.

verbunden und können deren Signale überschreiben. Ein Safety-System kann relaisbasiert sein, wobei die Wahrscheinlichkeit eines Sicherheitsvorfalls infolge einer Cyberattacke gering ist. Alternativ kann es jedoch auch elektronisch und Teil des Anlagennetzes sein, in welchem Fall die Wahrscheinlichkeit und die Konsequenzen eines Angriffs bzw. eines Sicherheitsvorfalls höher sind.[86] Gerade Safety-Systeme wurden um Funktionalitäten von SPS und RTUs ergänzt.[87] Ein solches elektronisches Safety-System ist in der Regel vom jeweiligen Steuerungssystem des Feldgeräts isoliert und wird über eine eigene Steuerungseinheit angesteuert. In der Praxis kommt es jedoch trotz Sicherheitsbedenken ebenso vor, dass dieselben (nicht integrierten) Steuerungseinheiten für das Safety-System und für die Steuerung der Feldgeräte verwendet werden, da sich hierdurch der Aufwand verringert.[88] Je nachdem, ob das Safety-System über ein integriertes Steuerungssystem (SPS) oder eine separate Steuerungseinheit verfügt, kann es im Sinne der Klassifikation als parametrierbar oder programmierbar angesehen werden.[89] Des Weiteren gibt es Safety-Systeme, die über eine integrierte Benutzerschnittstelle konfiguriert werden, um einen schnellen Zugriff auch bei Sicherheitsvorfällen zu gewährleisten, und dementsprechend der Komponentenklasse der Bedieneinheiten zuzuordnen wären.[90] Hierbei ist zu beachten, dass Safety-Systeme oft mehrfach redundant ausgelegt sind. In diesem Fall ist es denkbar, bei Programmierbaren Komponenten oder Bedieneinheiten nur eine Teilmenge der identischen Systeme physisch abzubilden, um mit weniger Aufwand realitätsnahe Ergebnisse für diese Komponenten zu erhalten.[91]

5.2.3 Schritt 3: Festlegung der Simulationsart für die Objekte der Klassen Programmierbare Komponenten und Bedieneinheiten

In Schritt 3 werden die Komponenten der Klassen Programmierbare Komponenten sowie Bedieneinheiten näher betrachtet, um zu entscheiden, welche Komponenten aufgrund ihrer Sicherheitseigenschaft möglichst real in eine Testumgebung integriert werden sollten. Ziel des dritten Schritts der Klassifikation ist die Bestimmung der Simulationsart dieser Komponenten anhand unterschiedlicher

86 IEC/ISA 62443-2-1:2015 (2015), S. 153.
87 Strauss (2003), S. 47.
88 Ghosh (2006), S. 1003.
89 Lipták (2006), S. 667; Birkhold und Lechler (2014), S. 304.
90 Blevins und Nixon (2006), S. 703-705.
91 Clare u. a. (2006), S. 910.

Merkmalsausprägung mithilfe von drei Kriterien: Aktive Sicherheitskomponente, Aktive Netzkomponente im kritischen Automatisierungsnetz sowie die Höhe der Verfügbarkeitsanforderungen. Die Klassifikation wird dabei durch den Moderator „Appliance“ als ergänzendes weiches Kriterium in Grenzfällen unterstützt, in denen eine Komponente bereits als Emulation oder insbesondere als Virtualisierung eine besonders hohe Realitätsnahe aufweist.[92]

Im dritten Schritt werden nur noch jene Komponenten betrachtet, die den vorgenannten zwei Komponentenklassen zugeordnet wurden. Programmierbare Komponenten sind Komponenten, die in ihrer Funktion in Abhängigkeit von einer Programmierung vollständig durch den Anwender veränderbar sind. Idealtypische Beispiele hierfür sind etwa SPS, programmierbare RTU, programmierbare IEDs, CIF, programmierbare Safety-Systeme, aktive Netzwerkkomponenten wie Router, Modems oder Switches sowie aktive Sicherheitskomponenten wie Firewalls, IDS oder IPS. Bedieneinheiten sind Komponenten, welche die Bedienung von (Teilen) einer Maschine oder Anlage erlauben. Sie verfügen in der Regel über ein Betriebssystem, das die Ausführung von Programmen erlaubt und/oder logische Schnittstellen. Hierunter fallen also Computer mit Bediensoftware wie Prozessleitsoftware (SCADA-MTU/DCS) bzw. Operator Workstations sowie Engineering Workstations, Supervisory Workstations und Application Workstations, aber auch Fernwartungskomponenten, Data Historians, Bedienterminals oder mobile Geräte.[93]

Anders als bei Komponenten des Passiven Automatisierungsnetzwerks oder Parametrierbaren Komponenten können diese Komponenten aufgrund ihrer Eigenschaften grundsätzlich quasi unendlich viele Verhaltensweisen aufweisen und somit kaum realitätsnah per Simulation in einer Testumgebung abgebildet werden. Selbst wenn eine identisch konfigurierte Emulation verfügbar ist, kann die Integration einer realen, physischen Komponente in die Testumgebung aufgrund ihrer hervorgehobenen Sicherheitseigenschaften angezeigt sein, um etwa . Dies gilt insbesondere für Appliances, also dedizierte Hardware-Software-Lösungen, wie abschließend zum moderierenden Kriterium erörtert wird. Ist dies nicht der Fall, sollte eine möglichst realitätsnahe Abbildung beispielsweise per Emulation oder Virtualisierung bevorzugt werden, sofern etwa Kostengründe gegen eine Integration der Echtkomponente sprechen.

---

92 Vgl. Gronau und Weber (2009), S. 7-10.

93 Hieb, Graham und Patel (2008), S. 134; Knapp und Langill (2014), S. 94. Ausgenommen hiervon sind grundsätzlich nur HMI-Produkte der 1970er und 1980er Jahre, die über spezielle Mikrorechner betrieben wurden. Vgl. Totherow (2006), S. 795.

5.2.3.1 Kriterium 1: Aktive Sicherheitskomponenten

Das erste Kriterium, wonach Komponenten möglichst physisch und nicht computerbasiert in eine hybride Testumgebung integriert werden sollten, ist das Komponentenmerkmal „aktive Sicherheitskomponente“.

Zu aktiven Sicherheitskomponenten zählen Komponenten, die neben Prävention, Monitoring oder Detektion auch eine Reaktion auf und Beurteilung von Angriffen beinhalten. Dies können sowohl Programmierbare Komponenten als auch Bedieneinheiten sein. Passive Überwachungssysteme, die lediglich über Anomalie-Erkennung verfügen, wie Protokollserver oder manche „Security Information Event Management“-Systeme (SIEM), sind nicht dazuzuzählen.[94] Der Unterschied ist darin begründet, dass eine Manipulation bzw. Kompromittierung durch einen Angreifer bei einer aktiven Sicherheitskomponente weitreichende Folgen nach sich ziehen kann, da sie etwa das Netzwerk lahmlegen kann. Typische aktive Sicherheitskomponenten sind Hard- und Software-Firewalls.[95] Ebenso zählen IPS dazu, welche mit ihrer präventiven Funktionalität als aktive Sicherheitskomponenten anzusehen sind. IDS/IPS werden meist auf handelsüblicher Hardware und üblichen Betriebssystemen eingesetzt, es gibt jedoch auch Varianten mit spezieller Hardware wie ASIC, Netzwerkprozessoren, FPGA oder TCAM.[96] Da sich Unternehmensnetzwerke von ICS-Netzwerken unterscheiden, wurden IDS/IPS lange nicht in Anlagennetzen eingesetzt. Seit einiger Zeit werden sie jedoch auch hier eingesetzt, in der Regel als netzwerkbasierte (N)IDS/(N)IPS, etwa im Übergang vom ICS-Netzwerk zum Unternehmensnetzwerk. Sie können aber auch als hostbasierte (H)IDS/(H)IPS zum Einsatz kommen.[97] Anders als IPS dienen IDS meist nur der Erkennung und Alarmierung, sind also in der Regel als passive Sicherheitskomponenten anzusehen, sofern sie nicht über dynamische Filterregeln verfügen.[98] (N)IPS können bei einem Angriff etwa bestimme Dienste über die Firewall sperren, womit sie unmittelbare Auswirkungen auf andere Komponenten haben können.[99] Unter Umständen sind auch Kommunikationsgateways als aktive Sicherheitskomponenten einzustufen, etwa wenn sie über Virenscanner

94 National Institute of Standards and Technology (2015), S. 5-1; Bundesamt für Sicherheit in der Informationstechnik (2013), S. 65-66.

95 National Institute of Standards and Technology (2015), S. 5-5.

96 Liao u. a. (2013), S. 16-24; National Institute of Standards and Technology (2015), S. 6-40.

97 Colbert und Hutchinson (2016), S. 212-217; vgl. BSI IT-Grundschutz-Kompendium (2017b), S. 22; Invensys (2004), S. 7; Spitzberg (2003), S. 3.

98 Müller (2014), S. 221; Bless u. a. (2006), S. 347.

99 Bundesamt für Sicherheit in der Informationstechnik (2016b), M 5.71 Intrusion Detection und Intrusion Response Systeme, S. 4479.

oder Firewall-artige Filtersysteme verfügen.[100] Bei einer isolierten Industrieanlage spielen Eingangsbarrieren eine geringere Rolle. Dennoch können lokale Schwachstellen auch hier wichtig sein und Schäden zur Konsequenz haben, weswegen aktive Sicherheitskomponenten auch hier relevant sein können.[101] Router oder Layer-3-Switches können ebenso als aktive Sicherheitskomponenten angesehen werden, sofern sie über entsprechende Funktionalitäten verfügen.[102] Sie verfügen teilweise über Sicherheitsfunktionalitäten, die denen einer Firewall ähneln, und werden zum Schutz des Prozessleitnetzwerks eingesetzt. Teilweise wird auch eine Kombination aus Router und Firewall eingesetzt, wobei das Filtersystem des Routers die Firewall entlastet und somit eine hohe Performanz der Firewall gewährleistet wird. Auch die Kombination von Router und Firewall zur Lastreduktion bzw. Sicherung der Performanz der Firewall verdeutlicht noch einmal, dass es wichtig ist, realitätsnahe Sicherheitsanalysen durchzuführen, denn nicht identifizierte Performanzmängel von Sicherheitsgeräten können eine bedeutende Schwachstelle sein.[103]

Anwendungsbeispiel der Klassifikation: Kriterium 1

Mit dem ersten Kriterium fällt die Entscheidung, die Appliance-Firewalls der DCS-Kleinanlage als aktive Sicherheitskomponenten real in die Testumgebung zu integrieren, um diese besonders wichtigen Sicherheitskomponenten vollumfänglich in der späteren Sicherheitsanalyse prüfen zu können. (Würde es sich um Software-Firewalls handeln, hätte gemäß dem Appliance-Moderator ggf. eine Emulation ausgereicht.) In der SCADA-Variante kann dasselbe ggf. für die Router gelten, sofern diese Sicherheitsfunktionalitäten aufweisen – sie werden jedoch ebenso im nächsten Schritt Berücksichtigung finden, mit dem gleichen Ergebnis.

Aktive Sicherheitskomponenten sind für die Sicherstellung der Verfügbarkeit einer Anlage von herausragender Bedeutung. Für eine cyber-physische Sicherheitsanalyse ist eine reale Integration der jeweiligen Komponenten in einer Testumgebung erforderlich, da beispielsweise Buffer-Overflow-, (D)Dos- oder ähnliche Ressourcenüberlastungsattacken nur mit originalgetreuem Verhalten zuverlässig überprüft werden können.[104] Denn vor allem Emulationen, aber auch Vir-

100 Siemens (2008), S. 75.

101 IEC/ISA 62443-2-1:2015 (2015), S. 182.

102 Siemens (2008), S. 26; National Institute of Standards and Technology (2015), S. 5-3; Sullivan, Luiijf und Colbert (2016), S. 22.

103 National Institute of Standards and Technology (2015), S. 5-9.

104 Van Leeuwen u. a. (2010), S. 1811; Bundesamt für Sicherheit in der Informationstechnik (2013), S. 33-34. Buffer Overflow-Angriffe gehören laut Industrial Control System Cyber

tualisierungen dieser Komponenten reagieren selbst bei identischer Konfiguration unter Umständen anders auf Sicherheitsvorfälle. Dies ist beispielsweise in unterschiedlichen Hardwareausführungen begründet, die von einer computerbasierten Darstellung meist nicht vollumfänglich berücksichtigt werden.[105] Selbst bei einem identischen Modelltyp können aufgrund unterschiedlicher Hardwareausführungen solche Unterschiede auftreten. Nur die Integration von aktiven Sicherheitskomponenten aus dem Teilbereich des kritischen Automatisierungsnetzwerks alleine reicht nicht aus, um eine ausreichende Realitätsnähe für eine umfängliche cyberphysische Sicherheitsanalyse zu gewährleisten. Denn auch aktive Sicherheitskomponenten außerhalb dieses Netzbereichs schützen die kritischen Prozesse und kritischen Systeme und sind diesen vorgelagert. Daher sollten möglichst alle aktiven Sicherheitskomponenten des Betrachtungsbereichs einer hybriden Testumgebung real bzw. physisch integriert werden.

5.2.3.2 Kriterium 2: Aktive Netzkomponenten im kritischen Automatisierungsnetz

Gemäß dem zweiten Kriterium wird bei Vorliegen einer aktiven Netzkomponente im kritischen Automatisierungsnetz eine Integration physischer bzw. realer Komponenten in die Testumgebung angeraten.

In modernen ICS-Anlagen können grundsätzlich alle Ebenen, von der Feldebene bis zum Unternehmensnetzwerk, direkt oder indirekt mittels Netzinfrastruktur verbunden werden.[106] Zu aktiven Netzkomponenten zählen Router, Switches, Hubs, Bridges oder Modems, aber auch Komponenten, die Netzwerkdienste bereitstellen, wie etwa DNS-Server.[107] Des Weiteren können auch Kommunikations-

Emergence Response Team (ICS-CERT) des US-amerikanischen Department of Homeland Security zu den häufigsten Angriffsarten bzw. ausnutzbaren Schwachstellen, aber auch andere Schwachstellen oder Angriffe können eine möglichst realitätsnahe Abbildung von Komponenten bedingen. Eine ähnliche Attacke ist die der Ressourcenüberlastung (Resource Exhaustion), wobei der Angreifer mit verschiedenen Methoden – etwa durch Einspielen von Updates – versucht, die Ressourcen einer Komponente voll auszulasten und zu überlasten, womit zwar meist keine Kontrolle über das System gewonnen wird, aber die (Schutz-)Funktionalitäten des Systems teilweise drastisch reduziert werden können. Diese Attacke ähnelt insofern DoS-Attacken. Vgl. Evancich und Li (2016), S. 99-104; National Institute of Standards and Technology (2008), S. 5-4-5-5; Urias, Van Leeuwen und Richardson (2012), S. 4.

105 Urias und Van Leeuwen (2016), S. 272.

106 Mathioudakis u. a. (2013), S. 1; Bundesamt für Sicherheit in der Informationstechnik (2013), S. 18.

107 Invensys (2004), S. 6-8.

Gateways zu den aktiven Netzkomponenten zählen, welche als dedizierte Server Geräten mit unterschiedlichen Protokollen oder Transportmethoden die Kommunikation ermöglichen oder als Schnittstelle zwischen Netzwerken fungieren.[108] Zuletzt gibt es Systeme, die - in Überschneidung zu aktiven Sicherheitskomponenten - der Verwaltung und Überwachung des Netzwerkes durch den Einsatz von rechnerbasierten Managementsystemen dienen. Hierunter fallen Netzwerkmanagement-Tools, Netzwerkmanagement-Agenten oder sonstige Monitoring- oder Netzmanagement-Software.[109] Gemäß der Klassifizierung können als aktive Netzkomponenten nur jene Komponenten eingestuft werden, die entweder als Programmierbare Komponenten oder als Bedieneinheiten eingestuft wurden.

Aktive Netzkomponenten sind für den reibungslosen Betrieb einer Industrieanlage unverzichtbar, denn eine fehlerfreie Kommunikation und Datenübertragung muss zur Sicherstellung der Ressourcenverfügbarkeit der Anlage gewährleistet sein.[110] Hingegen kann eine Kompromittierung oder Störung etwa durch Netzüberlastung oder den Ausfall von Netzkomponenten zu einem Kommunikationsausfall zwischen wichtigen Systemen führen. „Hat ein Angreifer Zugang zu einem Switch, kann er Sicherheitseinstellungen modifizieren und etwa Verbindungen beenden.“[111] Ein solcher Zustand kann ein Einfallstor für weitere Attacken sein oder aber bereits für sich genommen einen Anlagenausfall nach sich ziehen.[112]

Netzkomponenten lassen sich vergleichsweise gut und realitätsnah computerbasiert abbilden.[113] Daher kann ein Großteil der Komponenten eines Anlagennetzwerks in einer Testumgebung einwandfrei simuliert oder emuliert werden, um eine Netzwerkumgebung samt entsprechender Netzbelastung realitätsnah abzubilden. Dennoch sollten jene Netzkomponenten real in die Testumgebung integriert werden, die innerhalb der Sicherheitszone des kritischen Automatisierungsnetzes liegen, denn nicht alle aktiven Netzkomponenten und Netzbereiche sind in einer Gesamtanlage gleich bedeutsam: Nach IT-Grundschutz wird zum Schutz von Industrieanlagen eine Segmentierung sowie eine nach risikobasierten Zonen- und

108 Sullivan, Luiijf und Colbert (2016), S. 22; Singh und Lipták (2006), S. 869.

109 Metter und Bucher (2012), S. 342; Bundesamt für Sicherheit in der Informationstechnik (2016b), B 4.2 Netz- und Systemmanagement, S. 325-330.

110 Bless u. a. (2006), S. 342; Bundesamt für Sicherheit in der Informationstechnik (2016b), B 4.2 Netz- und Systemmanagement, S. 325-330.

111 Bundesamt für Sicherheit in der Informationstechnik (2016b), M 5.150 Durchführung von Penetrationstests, S. 1021.

112 IEC/ISA 62443-3-3:2013 + Cor.:2014 (2015), S. 70.

113 Urias und Van Leeuwen (2016), S. 271.

Conduits-Modellen festgelegte Zonierung von Netzen vorgenommen.[114] Demnach werden etwa ICS-Netze von Nicht-ICS-Netzen sowie kritische ICS-Netze von anderen ICS-Netzen möglichst logisch oder physisch getrennt.[115] Unter anderem ist zudem eine eigene Sicherheitszone für das kritische Automatisierungsnetzwerk vorzusehen, also jenen Teilbereich des Anlagennetzes, der als Hochsicherheitszone die kritischen Prozesse und kritischen Systeme beinhaltet.[116] Durch eine solche Aufteilung soll ein ausreichender Schutz der kritischen Prozesse und der hiermit verbundenen Komponenten gewährleistet werden.[117] Da dieser Teil des Netzwerks besonders sensibel ist, sollten jene Netzkomponenten real in die Testumgebung integriert werden, die zum kritischen Automatisierungsnetz gehören und die Kommunikationskanäle dieses Bereichs bereitstellen. Dies beinhaltet sowohl Komponenten innerhalb dieses Netzbereichs als auch an dessen Grenzen, wie etwa Router mit Ingressfiltern, die einzelne Netzbereiche voneinander trennen.[118] Auf diese Weise wird eine ausgewählte Teilmenge der Netzkomponenten real abgebildet, um eine höchstmögliche Wiedergabetreue der Testumgebung an entscheidender Stelle zu gewährleisten.[119]

Der Netzbereich des kritischen Automatisierungsnetzes umfasst meist Komponenten der Feldebene sowie der Steuerungsebene.[120] Bei kleineren Anlagen kann

114 BSI-Standard 200-2 (2017b), S. 103 ff.; BSI IT-Grundschutz-Kompendium (2017a); IEC/ISA 62443-2-1:2015 (2015), S. 179; IEC/ISA 62443-3-3:2013 + Cor.:2014 (2015), S. 65, SR 5.2 Schutz der Zonengrenzen; vgl. Bless u. a. (2006), S. 148.

115 IEC/ISA 62443-3-3:2013 + Cor.:2014 (2015), S. 64, SR 5.1 Netzaufteilung. Das kritische Automatisierungsnetz entspricht im klassischen Zonenmodell mit sechs Zonen der ersten und ggf. der zweiten Zone, welche die kritischen Automatisierungs- und Steuerungssysteme beinhalten. Vgl. Bitkom und VKU (2015), S. 80-82. Laut Bundesamt für Sicherheit in der Informationstechnik (2013), S. 63 sollten sich alle ICS in der gleichen Sicherheitszone befinden.

116 Das kritische Automatisierungsnetzwerk ist auch bekannt als „Closed-Shop-Betrieb“ nach Müller (2014), S. 236 ff., oder als „kritisches automatisierungstechnisches Netzwerk“ nach IEC/ISA 62443-3-3:2013 + Cor.:2014 (2015). Funktionale Netzwerkebenen und Sicherheitszonen sind hierbei nicht zu verwechseln, auch wenn diese bei kleinen Anlagen deckungsgleich sein können. Eine Sicherheitszone kann auch mehrere Netzwerksegmente umfassen. Aus Platzgründen wird an dieser Stelle nicht näher auf die Modalitäten von Netzwerksegmentierungen und Zonierungen eingegangen. Siehe hierzu auch IEC/ISA 62443-2-1:2015 (2015), S. 179.

117 McLaughlin u. a. (2016), S. 13; ENISA (2016), S. 32-36.

118 Vgl. Mehta und Reddy (2014), S. 362-363; Bless u. a. (2006), S. 339-345.

119 Dieses Vorgehen ähnelt der Schutzbedarfsfeststellung nach IT-Grundschutz, wo der Schutzbedarf des Datenflusses der für kritische Prozesse genutzten Anwendungen und IT-Systeme sich auf die dazwischenliegenden Netzkomponenten vererbt. BSI-Standard 200-2 (2017b), S. 95.

120 Pidikiti u. a. (2013), S. 136.

die Prozessleitebene noch dazukommen, wobei dann das funktionale Netzsegment und die Sicherheitszone deckungsgleich sind.[121] Bei größeren Anlagen sind diese hingegen nicht deckungsgleich und kleinteiliger aufgebaut im Hinblick auf horizontale und vertikale Netzsegmente und Zonierungen.[122]

Anwendungsbeispiel der Klassifikation: Kriterium 2

Nachdem die Simulationsart der aktiven Sicherheitskomponenten bestimmt wurde, wird an dieser Stelle ebenso für die aktiven Netzkomponenten im kritischen Datenfluss die Entscheidung getroffen, diese real in die Testumgebung zu integrieren. Dies betrifft etwa die Router bzw. Modems der SCADA-Anlagen.

Weil nur die aktiven Netzkomponenten des kritischen Automatisierungsnetzes in Form von realen Komponenten in der hybriden Testumgebung integriert werden, lassen sich bei hoher Wiedergabetreue Aufwand und Kosten reduzieren. In diesem Sinne kann an dieser Stelle bei Bedarf eine Komplexitätsreduktion vorgenommen werden: Die Verfügbarkeit und Kontinuität von Anlagenprozessen wird auch bei Netzkomponenten in der Regel durch Redundanzen sichergestellt. Grundsätzlich sollten auch redundant ausgelegte Komponenten Teil einer umfassenden Sicherheitsbetrachtung sein. Nicht nur um die Sicherheit dieser Komponenten zu gewährleisten, sondern auch, weil jene Komponenten grundsätzlich selber ein Sicherheitsrisiko sein könnten, sofern nicht einschlägige Sicherheitsmaßnahmen durchgeführt und überprüft wurden.[123] Doch wenn die Redundanzen durch identische Komponenten ermöglicht werden, ist auch in diesem Fall eine Kombination aus realen und emulierten/simulierten Komponenten denkbar. Wenn eine Teilmenge dieser Komponenten computerbasiert in der hybriden Testumgebung abgebildet wird, können einerseits Sicherheitseigenschaften vollumfänglich abgebildet werden, andererseits kann jedoch auch ein komplexeres Netzwerk schnell und kostengünstig abgebildet werden.[124]

Insgesamt sollten bei der Nachbildung des kritischen Automatisierungsnetzes grundsätzlich echte aktive Netzkomponenten in einer Testumgebung zum Einsatz kommen, da dieser Bereich aus sicherheitstechnischer Sicht besonders wichtig ist. Dennoch kann gerade bei komplexeren Anlagen bzw. aus Kosten- oder Ressourcengründen eine Kombination von realen und emulierten/simulierten Netzkompo-

121 IEC/ISA 62443-2-1:2015 (2015), S. 181 ff.
122 ENISA (2016), S. 19; Ciancamerla u. a. (2010), S. 354.
123 IEC/ISA 62443-2-1:2015 (2015), S. 107.
124 Van Leeuwen u. a. (2009), S. 2.

nenten eine Lösung sein, die eine hohe Aussagefähigkeit der Sicherheitsanalyse ermöglicht.[125]

5.2.3.3 Kriterium 3: Höhe der Verfügbarkeitsanforderungen

Mit den ersten beiden Kriterien wurden sowohl aktive Sicherheitskomponenten als auch aktive Netzkomponenten im kritischen Automatisierungsnetz hinsichtlich ihrer Simulationsart geprüft. Mit dem dritten Kriterium werden die verbleibenden Komponenten der Klassen Programmierbare Komponenten und Bedieneinheiten daraufhin geprüft, ob sie für die Verfügbarkeit der kritischen Prozesse einer Anlage so bedeutsam sind, dass eine reale Integration in die hybride Testumgebung angeraten ist.

Verfügbarkeit ist der wichtigste zu schützende Grundwert eines kritischen Prozesses wie der Wasserversorgung, da eine Verletzung deren Unterbrechung oder Ausfall zur Folge hat.[126] Daher ist es konsequent, vor allem jene verbleibenden Komponenten physisch bzw. real in die Testumgebung zu integrieren, welche für die Gewährleistung der Verfügbarkeit besonders wichtig sind. Diese Überlegung orientiert sich an den möglichen Schäden, die mit einer Beeinträchtigung der Komponenten bzw. Systeme und den ggf. von ihnen abhängigen Komponenten verbunden sind. Denn die Kompromittierung einer besonders wichtigen Komponente kann den Ausfall eines kritischen Prozesses oder weiterer Komponenten zur Folge haben.

Grundsätzlich sollen daher an dieser Stelle jene Komponenten identifiziert werden, deren Verfügbarkeitsanforderung mit denen des eigentlichen Wertschöpfungsprozesses identisch sind, da dieser direkt auf sie angewiesen ist. Zur Feststellung der Verfügbarkeitsanforderungen einzelner Komponenten sind daher vor allem die Abhängigkeitsbeziehungen des Wertschöpfungsprozesses und der Anlagenkomponenten zu berücksichtigen.[127] Auf diese Weise können diejenigen Komponenten herausgefiltert werden, von deren Funktionsfähigkeit der physische Prozess abhängig ist und welche ggf. möglichst real in der Testumgebung abgebildet werden sollten.[128] Der Vorteil dieser Methode ist, dass durch die hierarchische Abhängigkeitsbetrachtung unterschiedliche Verfügbarkeitsanforderungen auch für ansonsten identische Komponenten ermittelt werden können. Dies kann etwa bei Prozessleitkomponenten von verschachtelten SCADA-Architekturen der Fall sein,

125 Urias, Van Leeuwen und Richardson (2012), S. 6.
126 Müller (2014), S. 186.
127 Kersten, Reuter und Schröder (2013), S. 87.
128 Vgl. Scholz und Mörl (2003), S. 6-9.

wie sie in Siemens-WinCC- und PCS-7-Bausteinen für Controlling-, Maintenance- oder Supportprozesse eingesetzt werden.[129] Dieser Aspekt wird im Anwendungsbeispiel erläutert.

Je nach Anlagenausführung kann die Feststellung der Verfügbarkeitsforderungen recht aufwendig sein. Zur Feststellung der Verfügbarkeitsanforderungen wird daher eine Kurzanalyse derselben vorgeschlagen. Die Kurzanalyse orientiert sich an der Schutzbedarfsfeststellung nach IT-Grundschutz-Standard 200-2, legt aber den Fokus auf Verfügbarkeit und Abhängigkeiten zwischen Komponenten in Form eines hierarchischen Bottom-up-Risikomanagements entlang der Wertschöpfungskette. Für die Kurzanalyse wurde die Methodik an die spezifischen Bedürfnisse der Simulationsartbestimmung für hybride Testumgebungen angepasst. Der Vorteil ist, dass eine solche Kurzanalyse im Vergleich zu anderen Analysemethoden besonders aufwandsarm und einfach durchführbar ist. Das Kriterium und die Kurzanalyse fügen sich in die Begriffswelt des IT-Grundschutzes ein und greifen auf bekannte Methoden des BSI zurück. Dies ist der Anwendbarkeit zuträglich, da diese dem KMU bereits bekannt sein sollte. Gleichzeitig unterscheidet sich diese Methode vor allem in der Anwendung von Vererbungsprinzipien.

Wenn bereits eine Schutzbedarfsfeststellung nach BSI-Standard 200-2 durchgeführt und gut dokumentiert wurde, kann es möglich sein, die Ergebnisse zum Schutzziel der Verfügbarkeit von IT- und ICS-Systemen für diesen Schritt nutzbar zu machen. Im Idealfall wurde die Nachnutzung der Ergebnisse bereits in der Schutzbedarfsanalyse mitgedacht. Die Ergebnisse müssen aber ggf. im Hinblick auf redundante Komponenten und die Anwendbarkeit von Vererbungsprinzipien entsprechend der im Folgenden skizzierten Methode überarbeitet werden, da die Kurzanalyse diesbezüglich von der Schutzbedarfsfeststellung nach IT-Grundschutz abweicht. Ebenso kann es passieren, dass die Schutzbedarfskategorien nach IT-Grundschutz zu pauschal festgelegt wurden. Dadurch sind Unterschiede zwischen Komponenten im Grundwert der Verfügbarkeit nicht eindeutig genug, wenn etwa alle Anlagenkomponenten derselben hohen Schutzbedarfskategorie zugeordnet wurden. Für diesen Fall oder wenn keine oder nur eine veraltete Schutzbedarfsanalyse vorliegt, sollte vollständig auf die im Folgenden beschriebene Kurzanalyse zurückgegriffen werden.

Trotz der Ähnlichkeit unterscheidet sich diese Kurzanalyse der Verfügbarkeitsanforderungen von den Methoden und Standards des BSI. In der BIA spielen zwar ebenso vor allem Verfügbarkeitsanforderungen und Abhängigkeiten eine Rolle. Sie spielt sich aber auf einer anderen Ebene ab, denn es werden Schadensszenarien beim Ausfall ganzer (Teil-)Prozesse sowie deren zeitliche Ent-

[129] Vgl. Siemens (2008), S. 26.

wicklung betrachtet.[130] Die Betrachtungsebene der Schutzbedarfsanalyse nach IT-Grundschutz deckt sich mit der Analyse der Verfügbarkeitsanforderungen sehr viel mehr, letztere werden auch im BSI-Standard 200-2 betrachtet. Dieser ist mit der Unterscheidung zwischen IT-Systemen, Anwendungen, ICS-Systemen etc. deutlich differenzierter, was aber keinen Mehrwert für die Analyse der Verfügbarkeitsanforderungen bietet, wo SPS-Bausteine oder Firewalls mal als Appliance, mal softwarebasiert vorliegen. Zudem werden mit der Schutzbedarfsfeststellung andere Ziele verfolgt, die mit der Bestimmung der Simulationsart von Komponenten nicht deckungsgleich sind. Beispielsweise relativiert sich der Schutzbedarf aufgrund des Verteilungseffekts gemäß IT-Grundschutz bei redundanten Steuerungskomponenten.[131] Für eine hybride Testumgebung sind diese Komponenten jedoch weiterhin so zentral, dass bei identischen Komponenten zumindest eine Ausführung dieser Komponenten auch real abgebildet werden sollte. Bei unterschiedlichen Ausführungen sollten im Idealfall alle Komponenten physisch integriert werden, wie in der Kurzanalyse erläutert wird.[132]

Kurzanalyse der Verfügbarkeitsanforderungen

Die Kurzanalyse der Verfügbarkeitsanforderungen verläuft in drei Teilen. Zunächst werden Verfügbarkeitskategorien gebildet, dann werden die Verfügbarkeitsanforderungen der einzelnen Komponenten erfasst und danach werden diese in Abhängigkeit zum Wertschöpfungsprozess gebracht.

1. Definition der Verfügbarkeitskategorien
2. Feststellung der individuellen Verfügbarkeitsanforderungen
3. Berücksichtigung von Abhängigkeiten

Die einzelnen Bestandteile werden im Folgenden beschrieben.

1. Definition der Verfügbarkeitskategorien

Zunächst werden, analog zur Schutzbedarfsfeststellung nach IT-Grundschutz, qualitative Kategorien von Verfügbarkeitsanforderungen gebildet, womit die Verfügbarkeitsanforderungen der Komponenten definiert werden können (s. Tabelle 3). Hierbei genügt es, das Schadensszenario des Prozessausfalls zu betrachten. Wichtig ist in der Festlegung der Kategorien, dass auch bei grundsätzlich erhöhten Verfügbarkeitsanforderungen in der betrachteten Anlage dennoch Unterscheidungen zwischen einzelnen Komponenten in Relation zueinander getroffen werden können: Manche Komponenten sind so wichtig, dass der Prozess womöglich sehr

130 BSI-Standard 100-4 (2008), S. 30-36.

131 Vgl. BSI-Standard 200-2 (2017b), S. 92; Kersten, Reuter und Schröder (2013), S. 139-140.

132 Dies gilt vor allem dann, wenn die redundanten Komponenten identisch sind.

schnell ausfallen könnte, während der Ausfall anderer Komponenten für eine gewisse Zeit keine Auswirkungen haben muss. Die genaue Abgrenzung der jeweiligen Stufen kann eine Organisation selber festlegen.

Verfügbarkeitsanforderungen	
„normal“	Die Auswirkungen eines Ausfalls sind begrenzt und überschaubar.
„hoch“	Die Auswirkungen eines Ausfalls können beträchtlich sein.
„sehr hoch“	Die Auswirkungen eines Ausfalls können ein existentiell bedrohliches, katastrophales Ausmaß erreichen.

Tabelle 3: Kategorien von Verfügbarkeitsanforderungen[133]

Die Bestimmung der richtigen Anforderungskategorie kann in der Praxis manchmal nicht ganz einfach sein, weshalb bei unklaren Fällen im Zweifelsfall eine Einstufung in die höhere Kategorie empfohlen wird. Hierbei gilt, dass so wenig Verfügbarkeitsanforderungskategorien wie möglich, aber so viele wie nötig zu erstellen sind, um eine einfache und eindeutige, aber ausreichend differenzierte Einstufung vornehmen zu können. Es ist dabei darauf zu achten, dass die Kategorien plausibel, vollständig und konsistent sind.

2. Feststellung der individuellen Verfügbarkeitsanforderungen
Wie bei der Schutzbedarfsanalyse nach 200-2 kann zunächst von der Verfügbarkeitsanforderung des jeweiligen Geschäftsprozesses ausgegangen werden, der in der Wasserversorgung erhöht ist, also als „hoch“ oder meistens als „sehr hoch“ anzusehen sein wird.[134]

Daraufhin werden die Verfügbarkeitsanforderungen der einzelnen Komponenten bestimmt. Eine Differenzierung unterschiedlicher Objekte in Anwendungen, ICS- und IT-Systeme muss für den Zweck dieser Kurzanalyse nicht vorgenommen werden, sondern es ist ausreichend, alle zu betrachtenden Komponenten anhand ihrer Funktionalitäten zu unterscheiden und zu bewerten. Aus der Verfügbarkeitsanforderung des Geschäftsprozesses leiten sich die Verfügbarkeitsanforderungen der Komponenten ab, die für die Durchführung des Prozesses eingesetzt werden.

Bei der Bestimmung der Verfügbarkeitsanforderungen der Komponenten kann das Maximumprinzip angewandt werden.[135] Nach dem Maximumprinzip bemisst sich die Verfügbarkeitsanforderung eines Objektes anhand der schwerwiegends-

133 Abbildung nach BSI-Standard 200-2 (2017b), S. 88.
134 Vgl. BSI-Standard 200-2 (2017a), S. 91.
135 Kersten, Reuter und Schröder (2013), S. 139-140; BSI-Standard 200-2 (2017b), S. 91-92.

ten Auswirkungen des Ausfalls eines Teilobjektes, das sich somit auf das gesamte Objekt vererbt. Wenn also beispielsweise eine Komponente über eine Software-Firewall sowie über weitere Anwendungen verfügt, ist die Verfügbarkeitsanforderung der schutzbedürftigsten Anwendung für die Gesamtkomponente maßgeblich.

Aus dem IT-Grundschutz sind weitere Vererbungsprinzipien bekannt, die jedoch nicht angewandt werden. Der Kumulationseffekt spielt keine Rolle, wenn ausschließlich die Gesamtfunktionalität von Komponenten betrachtet wird. Verteilungseffekte kommen aufgrund der unterschiedlichen Zielstellung der Klassifikation nicht zum Einsatz, da auch redundante Komponenten für eine realitätsnahe Sicherheitsüberprüfung mittels hybrider Testumgebung wichtig sein können und sich ihre Verfügbarkeitsanforderung somit nicht relativiert.

3. Berücksichtigung von Abhängigkeiten
Nun werden die Abhängigkeiten zwischen den Komponenten und dem kritischen Wertschöpfungsprozess mit einbezogen und die Verfügbarkeitsanforderung gegebenenfalls korrigiert. Die Korrektur erfolgt dabei auf Basis des Grads der Abhängigkeit. Die Abhängigkeitsgrade sind ausgehend vom Wertschöpfungsprozess bottom up entlang der hierarchischen Wertschöpfungskette zu ermitteln: Komponenten, deren Ergebnisse, Input oder Steuerungsmöglichkeiten für die ständige Aufrechterhaltung des Wertschöpfungsprozesses unabdingbar sind, haben die höchsten Verfügbarkeitsanforderungen.[136] Benötigt eine solche besonders bedeutsame (prozesssteuernde) Komponente Informationen einer weiteren Komponente, ohne die sie ihre Funktionalität nur kurze Zeit aufrechterhalten kann, so wird sich die Verfügbarkeitsanforderung letzterer Komponente ebenfalls erhöhen. Werden von einer Komponente solche Informationen produziert, ist daher zu analysieren, ob die prozessnähere Komponente diesen Output zeitnah benötigt. Hier können also auch Fragen nach tolerierbaren Ausfallzeiten von Komponenten Berücksichtigung finden.

Anwendungsbeispiel der Klassifikation: Kriterium 3

Nachdem die aktiven Sicherheitskomponenten und die aktiven Netzkomponenten im kritischen Datenfluss identifiziert und deren reale Einbindung in die Testumgebung beschlossen wurde, werden mit dem dritten Kriterium nun die restlichen Komponenten dieser Klassen betrachtet.

Die Ergebnisse des dritten Kriteriums sollten identisch sein, unabhängig davon, ob nutzbare Ergebnisse einer Schutzbedarfsanalyse verwendet werden oder aber sich für die Kurzanalyse der Verfügbarkeitsanforderungen entschie-

136 Kersten, Reuter und Schröder (2013), S. 139.

den wird. Im Ergebnis sollte sich herausstellen, dass die RTU bzw. SPS sowie der DCS- bzw. der SCADA-Server (MTU) höhere Verfügbarkeitsanforderungen besitzen als die anderen Anlagenkomponenten, denn der physische Wertschöpfungsprozess ist von diesen unmittelbar Komponenten abhängig. Er lässt sich bei einem Ausfall dieser Komponenten nicht oder nur für kurze Zeit aufrechterhalten. Daher müssen diese Komponenten real in der hybriden Testumgebung abgebildet werden.

An dieser Stelle soll jedoch anhand einer größeren SCADA-Anlage aufgezeigt werden, wieso die Betrachtung der Abhängigkeiten für eine präzise Simulationsartbestimmung wichtig ist. Es wird gezeigt, dass die Klassifikation auch gut auf größere Anlagen angewandt werden kann (s. Abbildung 19 bzw. Anlage A.3 für eine Großdarstellung). Diese SCADA-Anlage verfügt über einen MTU-Server als Masterstation im grün gefärbten Produktionsleitnetzwerk, der eine zentrale Prozessleitsoftware ist, der Auswertung der Anlagen dienen kann und ggf. über zusätzliche Anwendungen verfügt, sowie über zwei Sub-MTU-Server im blau gefärbten Leitsystemnetzwerk, welche die Überwachung und Kontrolle der Prozesse im jeweiligen lokalen Leitsystemnetzwerk bzw. Feldgerätenetzwerk (violett) zur Aufgabe haben. Im Rahmen der Analyse der komponentenindividuellen Verfügbarkeitsanforderungen weisen wahrscheinlich beide Komponenten erhöhte Verfügbarkeitsanforderungen auf. Erst im Rahmen der Abhängigkeitsanalyse wird jedoch klar, dass der lokale Sub-MTU-Server wichtiger für die Gewährleistung des Wertschöpfungsprozesses ist. Während die Masterstation auch für längere Zeiträume ohne Verbindung zu den lokalen Ebenen sein kann, da sie die Wertschöpfungsprozesse nur mittelbar steuert, gilt dies nicht für den prozessnahen Sub-MTU-Server, welcher beim Verbindungsverlust zum Kontrollzentrum dennoch alleinstehend den Prozess unmittelbar steuert.

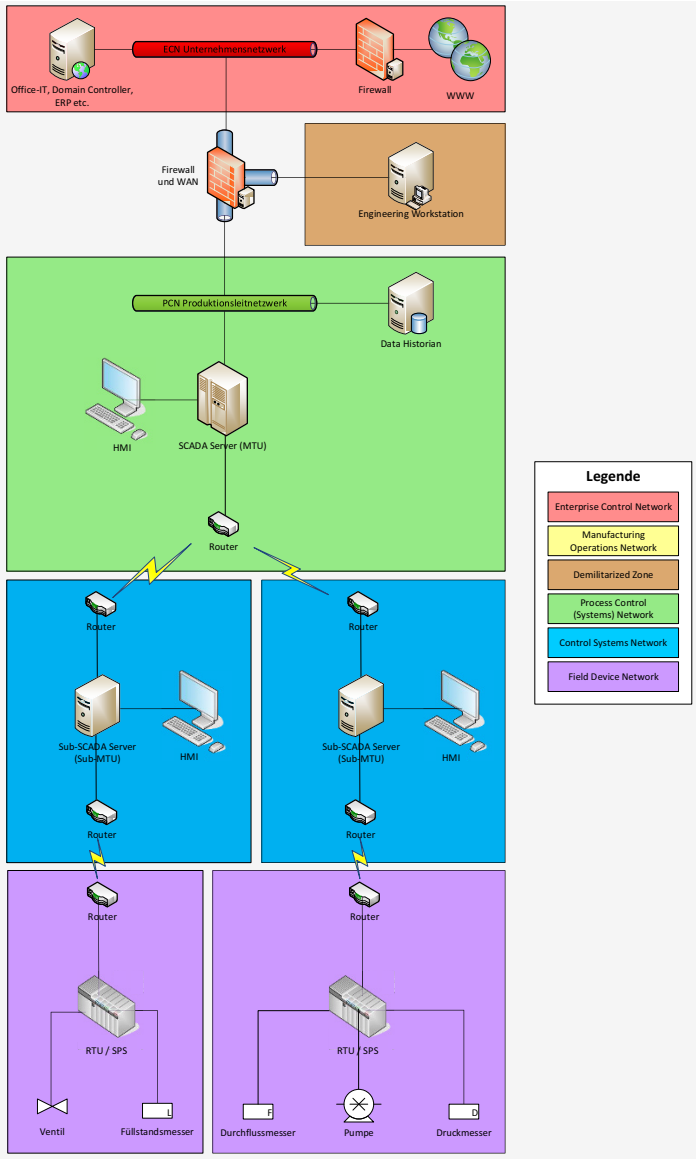

Abb. 16: Aufbau einer idealtypisch verschachtelten und zonierten SCADA-Anlage

Aufgrund dessen sollte der Sub-MTU-Server möglichst real in die hybride Testumgebung eingebunden werden, während die Masterstation auch computerbasiert etwa als Virtualisierung dargestellt werden kann.

Es zeigt sich, dass die Abhängigkeitsbetrachtung wichtig ist, da beispielsweise bei mittelgroßen Industrieanlagen Komponenten mit Prozessleitsoftware aus Benutzerfreundlichkeit oder aus Sicherheitsgründen in unterschiedlichen Netzwerkebenen und Ausführungen mehrfach vorhanden sind und trotz grundsätzlich gleicher Eigenschaften unterschiedliche Verfügbarkeitsanforderungen haben können.[a]

Komponente	**Simulationsart**
Bedieneinheit	
Office-IT	Virtualisiert
Data Historian	Virtualisiert
Engineering Workstation	Virtualisiert
DCS-Server *(bei DCS-Anlage)*	Physisch
SCADA-Server *(bei SCADA-Kleinanlage)*	Physisch
SCADA-Server *(bei SCADA-Großanlage)*	Virtualisiert
SCADA-Sub-Server *(bei SCADA-Großanlage)*	Physisch
Programmierbare Komponente	
Firewall	Physisch
Router/Modem *(bei SCADA-Anlage)*	Physisch
RTU/SPS-Baustein	Physisch
Parametrierbare Komponente	
Felgeräte (Ventil, Pumpe, etc.)	Simuliert
Passives Automatisierungsnetzwerk	
Verkabelung	Simuliert

Tabelle 4: Komponentenzuordnung der Fallbeispiele

Nun stehen alle Komponenten fest, welche real bzw. physisch Teil der hybriden Testumgebung sein sollten (s. Tabelle 4). Übriggebliebene Komponenten aus den Klassen Bedieneinheiten und Programmierbare Komponenten können emuliert bzw. virtualisiert werden. Im konkreten Anlangenbeispiel werden verbleibende Komponenten des Unternehmensnetzwerks und

der DMZ ebenso aufwandsarm wie realitätsnah virtualisiert, wie der Data Historian im Produktionsleitnetzwerk.[b]

[a] Queiroz u. a. (2009), S. 361; Totherow (2006), S. 794.
[b] Green u. a. (2017), S. 3; Bundesamt für Sicherheit in der Informationstechnik (2013), S. 19-20 und S. 114; Urias und Van Leeuwen (2016), S. 270-271.

Im Ergebnis müssen diejenigen Komponenten real in die Testumgebung integriert werden, für die hier eine besonders hohe Verfügbarkeitsanforderung festgestellt werden konnte. In der Regel werden große Teile der prozesssteuernden Komponenten der Steuerungs- und Prozessleitebene durch entsprechend hohe Verfügbarkeitsanforderungen gekennzeichnet sein. Sofern entsprechende Komponenten redundant ausgelegt sind, entscheidet die Redundanzqualität darüber, welche der Komponenten real abgebildet werden müssen: Bei identischen Komponententypen muss nur die primäre Ausführung real integriert werden, da sich jene Komponenten bei prinzipbedingten Fehlern oder bei Schwachstellen identisch verhalten. Bei unterschiedlichen Komponententypen sollten hingegen alle Komponenten physisch in der Testumgebung abgebildet sein, da nur auf diese Weise eine ausreichende Prüfung jedes Komponententyps gewährleistet werden kann.

Um eine solche hierarchische Abhängigkeitsanalyse zu unterstützen, können auch visuelle Hilfsmittel aus der Interdependenz- oder die Pfadanalyse genutzt werden, welche die Abhängigkeit der Verfügbarkeitsanforderungen entlang des Datenflusses der Komponenten abbilden.[137] Die Abhängigkeiten in Form von zuliefernden, steuernden oder abnehmenden Anlagenelementen können hier als horizontale oder vertikale Interdependenzen visualisiert werden. Ein Interdependenznetz kann mit einem Tabellenkalkulationsprogramm, Ursache-Wirkungsdiagrammen oder mithilfe einer Mindmap erstellt werden.[138] Dabei werden die physischen Prozesse bzw. Feldgeräte als das zu betrachtende Ausgangsobjekt in den Mittelpunkt gestellt und alle Pfade davon ausgehend im Hinblick auf Verfügbarkeitsanforderungen analysiert.[139]

137 Vgl. Müller (2014), S. 316; BSI-Standard 200-2 (2017b), S. 95.
138 Vgl. Müller (2014), S. 432-434.
139 Vgl. ebd., S. 232.

5.2.3.4 Das moderierende Kriterium „Appliance“: Abwägungen zwischen einer realen oder computerbasierten Integration angesichts von Ressourcenlimitationen

Eine höchstmögliche Wiedergabetreue ist bei kritischen Komponenten grundsätzlich angezeigt, weshalb Komponenten, die unter eines der drei beschriebenen Kriterien fallen, möglichst real in die Testumgebung integriert werden sollten. Wie in der Einleitung zu Abschnitt 5.2 bereits kursorisch erörtert wurde, kann es je nach Zielstellung oder (z.B. finanziellen) Rahmenbedingungen jedoch attraktiv sein, Komponenten soweit wie möglich zu simulieren, emulieren oder virtualisieren, anstatt sie real in die Testumgebung zu integrieren: Einmal konfiguriert und implementiert können computerbasierte Geräte beliebig instanziiert oder angepasst werden.[140] Insbesondere bei komplexen Anlagen kann dies eine große Rolle spielen.[141] In diesem Abschnitt soll beleuchtet werden, in welchen Fällen und unter welchen Bedingungen die computerbasierte Darstellung einer kritischen Komponente eine ausreichende Wiedergabetreue aufweisen kann, um als zweitbeste Option ohne große Vorbehalte eingesetzt werden zu können. Hierfür soll das weiche Kriterium „Appliance“ einen Prüfstein darstellen, denn applikationsspezifische Hardware ist besonders schwer computerbasiert zu replizieren.[142] Der Prüfstein ist explizit als Empfehlung zu sehen, von der abgewichen werden kann, sofern Rahmenbedingungen dies erfordern.

Grundsätzlich ist es bei guten Emulationen und Virtualisierungen möglich, eine hohe Realitätsnähe zu erreichen. Hierfür werden im Optimalfall originalgetreue Software und Betriebssysteme mit anlagenidentischen Konfigurationen genutzt. Sorgfältige computerbasierte Abbildungen implementieren dabei nicht nur das Verhalten einer Komponente, sondern auch ihre Betriebseigenschaften. Dies kann unter Umständen auch Vorteile gegenüber Hardwarekomponenten haben. So können emulierte SPS robuster sein, was bei bestimmten Sicherheitsanalysen Vorteile haben kann, denn reale Komponenten können unter Umständen dauerhaft beschädigt sein. Hingegen können Emulationen einfach zurückgesetzt werden.[143]

Es spricht jedoch gerade bei sicherheitskritischen Komponenten auch einiges dagegen, realitätsnahe computerbasierte Abbildungen anstelle von realen Komponenten einzusetzen. Hier sind zunächst software- und konfigurationstechnische Gründe zu nennen. Denn bei kritischen Komponenten sollte die Wiedergabetreue von der Oberfläche über die Paketebene bis zur Systeminteraktion und dem Verhal-

140 Jaromin u. a. (2013), S. 35-39; Vellaithurai, Biswas und Srivastava (2017), S. 2-3.
141 Hong u. a. (2015), S. 268.
142 Reuter und Zacher (2014), S. 316.
143 Jaromin u. a. (2013), S. 35-38.

ten in passiven und aktiven Angriffen gegeben sein.[144] Es kann jedoch schwierig sein, insbesondere eine Emulation hinreichend realitätsnah zu implementieren. Es kommt häufig vor, dass innerhalb einer Produktfamilie oder eines Gerätetyps unterschiedliche Architekturen und Plattformen zum Einsatz kommen, es aber nur einen generischen Emulator gibt. Gerade bei ICS-Komponenten der Steuerungs- und Feldebene sind oft nur generische Emulatoren verfügbar, die für kritische Komponenten nicht ausreichend realitätsnah sind. Ebenso kann es vorkommen, dass die Firmware etwa für einen SPS-Emulator nicht in der richtigen Version zur Verfügung steht, was für Sicherheitsanalysen von kritischen Komponenten ein Ausschlusskriterium sein kann.[145] Gerade bei älteren Komponenten oder Komponenten mit proprietären Eigenschaften steht oft kein typengerechter Emulator zur Verfügung. Die Nutzung von benutzerdefinierten Emulationen per Ersatzsoftware wirkt zwar theoretisch vielversprechend, ist aber aufgrund der vielen nicht dokumentierten Eigenschaften mit viel Aufwand verbunden und weicht in der praktischen Nutzung regelmäßig stark von der Originalkomponente ab.[146] Erschwerend wirkt auch, dass Firmware teilweise verschlüsselt oder abgesichert ist, so dass die Konfigurationen nicht ohne Weiteres ausgelesen werden können. Zuletzt können moderne Komponenten wie SPS über verschiedene zusätzliche Dienste auf der Anwendungsebene verfügen, welche samt ihren Konfigurationen ebenso emuliert werden müssen, was in der Praxis oft nicht möglich oder aufwendig sein kann.[147] Kurzum: Wenn eine Emulation bzw. Virtualisierung mit identischen Applikationseigenschaften nicht möglich ist, ist die Wiedergabetreue für eine Sicherheitsanalyse ggf. nicht zufriedenstellend.

Auch wenn Software- oder Konfigurationsfehler mit guten Emulationen oder Virtualisierungen zielgerichtet analysiert werden können, können sicherheitsrelevante Hardwareaspekte trotzdem gegen den Einsatz bestimmter computerbasierter Replikationen zur Überprüfung kritischer Komponenten sprechen.[148] Für eine Sicherheitsanalyse von Komponenten der Betriebs- und Steuerungstechnik ist die Wiedergabetreue der Hardware essentiell: Während erhöhte Latenzzeiten, Performanceschwankungen oder auch kurzzeitige Ausfälle bei normalen IT-Systemen oft akzeptabel sind, sind sie für Anlagenkomponenten inakzeptabel und müssen überprüft werden können.[149] Denn der besonders bedeutsame Grundwert der

144 Vgl. Jaromin u. a. (2013), S. 38 ff., für eine solche Überprüfung.

145 Hong u. a. (2015), S. 268; Jaromin u. a. (2013), S. 35.

146 Holm u. a. (2015), S. 22.

147 Jaromin u. a. (2013), S. 39.

148 Rabe, Spieckermann und Wenzel (2008b), S. 134-136.

149 Collier u. a. (2016), S. 173; IEC/ISA 62443-2-1:2015 (2015), S. 31 und S. 214; IEC/ISA 62443-3-3:2013 + Cor.:2014 (2015), S. 31 und S. 70.

Verfügbarkeit hängt ebenso von den Kapazitätsanforderungen bzw. dem Kapazitätsmanagement einer Komponente ab, welches durch die komponentenspezifische Hardware gewährleistet wird.[150] Beispielsweise kann eine Hardware-Firewall applikationsspezifische Eigenschaften aufweisen, die sich mit einer Emulationssoftware nicht abbilden lassen. Ebenso reagiert eine emulierte SPS bei (D)DoS-Attacken anders als eine Originalkomponente.[151] Denn damit kann die Frage, mit welcher (Netzwerk-)Last die tatsächliche Firewall angesichts von beispielsweise (D)Dos- oder Buffer-Overflow-Attacken umgehen kann, ggf. nicht verlässlich beantwortet werden.[152] Es wird also deutlich, dass diese Problematik vor allem bei dezidierten Hardwarekomponenten („Appliance“) auftritt, da diese über atypische Eigenschaften verfügen können. Bei einer Softwarefirewall, die auf einem handelsüblichen PC läuft, kann eine entsprechend konfigurierte Virtualisierung die Hardwareeigenschaften des Systems in der Regel besser abbilden, als dies bei der Emulation einer Appliance der Fall ist. Neben Firewalls sind Appliances typischerweise bei integral aufgebauten oder sicherheitsgerichteten SPS, RTU, IDS/IPS, Modems, Routern oder Switches anzutreffen.[153]

Das Fazit dieser Überlegungen ist, dass Komponenten, die unter eines der drei Kriterien fallen, grundsätzlich physisch in die Testumgebung integriert werden sollten, da nur dann eine vollumfängliche Sicherheitsanalyse gewährleistet werden kann. Der Moderator bzw. das weiche Kriterium „Appliance“ soll jedoch auch zeigen, dass dies nicht für alle Komponenten in gleichem Maße gilt. Wenn beispielsweise finanzielle Rahmenbedingungen dies erfordern, ist eine realitätsnahe Virtualisierung – also eine computerbasierte Abbildung eines Systems, das auf handelsüblicher PC-Hardware läuft – eher denkbar als die Emulation einer Appliance. Deswegen sollten kritische Komponenten vom Typ Appliance aufgrund ihrer besonderen Eigenschaften real in die Testumgebung integriert werden, da die Wahrscheinlichkeit, dass die besonderen Hardwareeigenschaften realitätsnah emuliert werden können, deutlich geringer ist. Auch wenn der Einsatz von Originalkomponenten mit Kosten behaftet ist, ist Wiedergabetreue an dieser Stelle ein vorrangiger Grundsatz.[154]

---

150 IEC/ISA 62443-2-1:2015 (2015), S. 68.

151 Alves, Das und Morris (2016), S. 11-12.

152 Van Leeuwen u. a. (2010), S. 1811; Bundesamt für Sicherheit in der Informationstechnik (2013), S. 33-34; Evancich und Li (2016), S. 99-104; National Institute of Standards and Technology (2008), S. 5-4-5-5; Kersten, Reuter und Schröder (2013), S. 193.

153 National Institute of Standards and Technology (2007), S. 3-5; Siemens (2008), S. 15; National Institute of Standards and Technology (2015), S. 5-5; Wellenreuther und Zastrow (2005), S. 5; Greeff und Ghoshal (2004), S. 30; Litz (2013), S. 191.

154 Green u. a. (2017), S. 5.

Literaturverzeichnis

Alves, T., R. Das und T. Morris (2016), Virtualization of Industrial Control System Testbeds for Cybersecurity, in: *Proceedings of the 2nd Annual Industrial Control System Security Workshop*, ACM, 10–14.

Bastigkeit, B., T. Schossig und F. Steinhauser (2009), Efficient testing of modern protection IEDs, in: *PAC World*, 3, 54–59.

Beard, C. S., B. Lipták und P. M. B. S. Girão (2006), Actuators: Digital, Electric, Hydraulic, Solenoid, in: B. Lipták (Hrsg.), *Instrument Engineers' Handbook: Process Control and Optimization*, 4. Aufl., Bd. 2, CRC Press.

Berge, J. (2006), Transmitters: Smart, Multivariable, and Fieldbus, in: B. Lipták (Hrsg.), *Instrument Engineers' Handbook: Process Control and Optimization*, 4. Aufl., Bd. 2, CRC Press.

Birkhold, M. und J. Bauer (2014), *Sicherheit in der Automatisierungstechnik nach BSI IT-Grundschutz, geht das?*, Vortrag, URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Veranstaltungen/Grundschutz/1GS_Tag_2014/02_1_IT-Grund_2014_Birkhold.pdf?__blob=publicationFile (besucht am: 20. 12. 2017).

Birkhold, M. und A. Lechler (2014), Modellierung von Automatisierungssystemen nach Vorgaben des BSI - Bundesministerium für Sicherheit in der Informationstechnik: Notwendigkeit, Modellkonzept, Vorteile, in: *wt Werkstattstechnik online*, 104:5, 301–306.

Bitkom und VKU (2015), *Praxisleitfaden IT-Sicherheitskatalog – Anforderungen an die IT für den sicheren Betrieb von Energieversorgungsnetzen*, Bitkom und VKU.

Bless, R. u. a. (2006), *Sichere Netzwerkkommunikation: Grundlagen, Protokolle und Architekturen*, Springer-Verlag.

Blevins, T. L. und M. Nixon (2006), DCS: Integration with Other Systems, in: B. Lipták (Hrsg.), *Instrument Engineers' Handbook: Process Control and Optimization*, 4. Aufl., Bd. 2, CRC Press.

Bossel, H. (2004), *Systeme, Dynamik, Simulation – Modellbildung, Analyse und Simulation komplexer Systeme*, BoD.

BSI IT-Grundschutz-Kompendium (2017a), *Baustein NET.1.1 Netzarchitektur und -design im IT-Grundschutz*.

BSI IT-Grundschutz-Kompendium (2017a), *IND.1 Betriebs- und Steuerungstechnik*.

BSI IT-Grundschutz-Kompendium (2017b), *Umsetzungshinweise zum Baustein IND.1 Betriebs- und Steuerungstechnik*.

BSI IT-Grundschutz-Kompendium (2017b), *Umsetzungshinweise zum Baustein INF.3 Elektrotechnische Verkabelung*.
BSI IT-Grundschutz-Kompendium (2017c), *Umsetzungshinweise zum Baustein INF.4 IT-Verkabelung*.
BSI-Standard 100-2 (2008), *IT-Grundschutz-Vorgehensweise*.
BSI-Standard 100-4 (2008), *Notfallmanagement*.
BSI-Standard 200-2 (2017a), *IT-Grundschutz-Methodik*.
BSI-Standard 200-2 (2017b), *IT-Grundschutz-Methodik – Community Draft*.
BSI-Standard 200-3 (2016), *Risikoanalyse auf der Basis von IT-Grundschutz – Community Draft*.
Bundesamt für Sicherheit in der Informationstechnik (2013), *ICS-Security-Kompendium*.
Bundesamt für Sicherheit in der Informationstechnik (2016a), *Ein Praxis-Leitfaden für IS-Penetrationstests*.
Bundesamt für Sicherheit in der Informationstechnik (2016b), *IT-Grundschutz-Kataloge: 15. Ergänzungslieferung*.
Bundesministerium für Wirtschaft und Energie (2013), *Mensch-Technik-Interaktion: Leitfaden für Hersteller und Anwender*, Bd. 3, Bundesministerium für Wirtschaft und Energie.
Campbell, B. D., C. W. Wendt und P. G. Friedmann (2006), PLC Software Advances, in: B. Lipták (Hrsg.), *Instrument Engineers' Handbook: Process Control and Optimization*, 4. Aufl., Bd. 2, CRC Press.
Ciancamerla, E. u. a. (2010), Discrete event simulation of QoS of a SCADA system interconnecting a Power grid and a Telco network, in: *What Kind of Information Society? Governance, Virtuality, Surveillance, Sustainability, Resilience*, Springer, 350–362.
Clare, W. N. u. a. (2006), PLCs: Programmable Logic Controllers, in: B. Lipták (Hrsg.), *Instrument Engineers' Handbook: Process Control and Optimization*, 4. Aufl., Bd. 2, CRC Press.
Colbert, E. J. M. und S. Hutchinson (2016), Intrusion Detection in Industrial Control Systems, in: E. J. M. Colbert und A. Kott (Hrsg.), *Cyber-security of SCADA and Other Industrial Control Systems*, Springer-Verlag, 239–251.
Collier, Z. A. u. a. (2016), Security Metrics in Industrial Control Systems, in: E. J. M. Colbert und A. Kott (Hrsg.), *Cyber-security of SCADA and Other Industrial Control Systems*, Springer-Verlag, 239–251.
Department of Homeland Security, I. C. S. C. E. R. T. (2016), *Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies*.

ENISA (2016), *Communication network dependencies for ICS/SCADA Systems*, European Union Agency For Network und Information Security.

Evancich, N. und J. Li (2016), Attacks on Industrial Control Systems, in: E. J. M. Colbert und A. Kott (Hrsg.), *Cyber-security of SCADA and Other Industrial Control Systems*, Springer-Verlag, 239–251.

Genge, B., C. Siaterlis und M. Hohenadel (2012), Amici: An assessment platform for multi-domain security experimentation on critical infrastructures, in: B. M. Hämmerli, N. K. Svendsen und J. Lopez (Hrsg.), *Critical Information Infrastructures Security, 7th International Workshop, CRITIS 2012 Lillehammer, Norway, September 2012 Revised Selected Papers*, Springer-Verlag, 228–239.

Ghosh, A. (2006), Programmable Safety Systems, in: B. Lipták (Hrsg.), *Instrument Engineers' Handbook: Process Control and Optimization*, 4. Aufl., Bd. 2, CRC Press.

Gonzalez, C. A. und J. Reed (2016), Cyber Physical Intrusion Detection, in: E. J. M. Colbert und A. Kott (Hrsg.), *Cyber-security of SCADA and Other Industrial Control Systems*, Springer-Verlag, 239–251.

Greeff, G. und R. Ghoshal (2004), *Practical E-manufacturing and supply chain management*, Newnes.

Green, B. u. a. (2017), Pains, Gains and PLCs: Ten Lessons from Building an Industrial Control Systems Testbed for Security Research, in: *The 10th USENIX Workshop on Cyber Security Experimentation and Test (CSET '17)*, USENIX Association.

Gronau, N. (2009), *Wissen prozessorientiert managen: Methode und Werkzeuge für die Nutzung des Wettbewerbsfaktors Wissen in Unternehmen*, Oldenbourg Industrieverlag.

Gronau, N., C. Fohrholz und S. Lass (2011), Hybrider Simulator – Neuer Ansatz zum Produktionsmanagement, in: *ZWF Zeitschrift für wirtschaftlichen Fabrikbetrieb*, 106:4, 204–208.

Gronau, N. und E. Weber (2009), *Wandlungsfähigkeit: Generische Strategien zur Handhabung von Veränderungen in der Umwelt*, Arbeitsbericht, WI–2009–07, Lehrstuhl für Wirtschaftsinformatik und Electronic Government, Universität Potsdam.

Gurschler, T. u. a. (2017), Risikobeurteilung in der IT-Sicherheit Kritischer Infrastrukturen – Eine Analyse der Risikobeurteilung im Förderschwerpunkt ITS|KRITIS, in: *Bundesamt für Sicherheit in der Informationstechnik: Digitale Gesellschaft zwischen Risikobereitschaft und Sicherheitsbedürfnis: Tagungsband des 15. Deutschen IT-Sicherheitskongress 2017*, SecuMedia Verlag.

Hafner, M. und R. Breu (2008), *Security engineering for service-oriented architectures*, Springer Science & Business Media.

Hahn, A. u. a. (2013), Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid, in: *IEEE Transactions on Smart Grid*, 4:2, 847–855.

Henzler, R. G. (1992), *Information und Dokumentation: Sammeln, Speichern und Wiedergewinnen von Fachinformation in Datenbanken*, Springer-Verlag.

Hieb, J., J. Graham und S. Patel (2008), Security Enhancements for Distributed Control Systems, in: E. Goetz und S. Shenoi (Hrsg.), *International Conference on Critical Infrastructure Protection, 1st IFIP WG 11.10 International Conference, ICCIP 2007, New Hampshire, USA, Revised Selected Papers*, Springer, 237–247.

Holm, H. u. a. (2015), A survey of industrial control system testbeds, in: S. Buchegger und M. Dam (Hrsg.), *Secure IT Systems, Lecture Notes in Computer Science*, Springer, 11–26.

Hong, J. u. a. (2015), Cyber-Physical Security Testbed for Substations in a Power Grid, in: C. C. Liu, S. K. Khaitan und J. D. McCalley (Hrsg.), *Cyber Physical Systems Approach to Smart Electric Power Grid*, Springer, 261–301.

Howser, G. (2015), Using information flow methods to secure cyber-physical systems, in: M. Rice und S. Shenoi (Hrsg.), *International Conference on Critical Infrastructure Protection IX, 9th IFIP WG 11.10 International Conference, ICCIP 2015, Arlington, VA, USA, March 16-18, Revised Selected Papers*, Springer-Verlag, 185–205.

IEC/ISA 62443-1-1:2007 (2007), *Security for Industrial Automation and Control Systems – Part 1: Terminology, Concepts, and Models*.

IEC/ISA 62443-2-1:2015 (2015), *Security for industrial automation and control systems – Part 2-1: Industrial automation and control system security management system, Draft 7, Edit 5 November 9, 2015*.

IEC/ISA 62443-3-3:2013 + Cor.:2014 (2015), *Industrielle Kommunikationsnetze – IT-Sicherheit für Netze und Systeme – Teil 3-3: Systemanforderungen zur IT-Sicherheit und Security-Level*.

Invensys (2004), *Process Control Network – Reference Architecture: White Paper*, hrsg. von D. Rath, Invensys.

Jaromin, R. u. a. (2013), Design and implementation of industrial control system emulators, in: J. Butts und S. Shenoi (Hrsg.), *International Conference on Critical Infrastructure Protection VII, 7th IFIP WG 11.10 International Conference, ICCIP 2013, Washington, DC, USA, March 18-20, Revised Selected Papers*, Springer-Verlag, 35–46.

Kersten, H., J. Reuter und K.-W. Schröder (2013), *IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz*, Springer.

Knapp, E. D. und J. T. Langill (2014), *Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems*, Syngress.

Laisiepen, K., E. Lutterbeck und K.-H. Meyer-Uhlenried (1972), *Grundlagen der praktischen Information und Dokumentation*, Verlag Dokumentation.

Lass, S., C. Fohrholz und H. Theuer (2011), Hybride Simulation – Neuer Ansatz zum Produktionsmanagement, in: *Industrie & Management*, 1, 13 ff.

Lass, S., H. Theuer und N. Gronau (2011), Effiziente Simulation im Produktionsmanagement:Schnelle und belastbare Analyse von Fertigungsprozessen, in: *Industrie Management*, 27:3, 13–15.

Lass, S. (2011), A new Approach to Simulation in Production Management, in: H. El Maraghy (Hrsg.), *Enabling Manufacturing Competitiveness and Economic Sustainability: Proceedings of the 4th International Conference on Changeable, Agile, Reconfigurable and Virtual production (CARV 2011), Montreal, Canada, 2-5 October 2011*, Springer, 598–604.

Lass, S. und N. Gronau (2012), Efficient Analysis of Production Processes with a Hybrid Simulation Environment, in: H. Nylund u. a. (Hrsg.), *Proceedings of the FAIM 2012: 22nd International Conference on Flexible Automation and Intelligent Manufacturing, June 10th-13th, 2012, Helsinki, Finland*, Tampere University of Technology.

Lass, S. und H. Theuer (2011), Hybride Simulation – Den besten Grad an dezentraler Produktionssteuerung bestimmen, in: *Productivity Management*, 13–16.

Law, A. M., W. D. Kelton und W. D. Kelton (1991), *Simulation modeling and analysis*, 2. Aufl., McGraw-Hill.

Liao, H.-J. u. a. (2013), Intrusion detection system: A comprehensive review, in: *Journal of Network and Computer Applications*, 36:1, 16–24.

Lipták, B. (2006), DCS: Basic Trends and Advances, in: B. Lipták (Hrsg.), *Instrument Engineers' Handbook: Process Control and Optimization*, 4. Aufl., Bd. 2, CRC Press.

Litz, L. (2013), *Grundlagen der Automatisierungstechnik: Regelungssysteme – Steuerungssysteme – hybride Systeme*, Walter de Gruyter.

Mamzic, C. L., R. Gilbert und B. G. Lipták (2006), Relays for Computing and Programmers, in: B. Lipták (Hrsg.), *Instrument Engineers' Handbook: Process Control and Optimization*, 4. Aufl., Bd. 2, CRC Press.

Mathioudakis, K. u. a. (2013), Towards generic scada simulators: A survey of existing multi-purpose co-simulation platforms, best practices and use-cases,

in: *Scientific Cooperations International Workshops in Electrical-Electronics Engineering*, 33–39.

McLaughlin, S. u. a. (2016), The cybersecurity landscape in industrial control systems, in: *Proceedings of the IEEE*, 104:5, 1039–1057.

Mehta, B. R. und Y. J. Reddy (2014), *Industrial process automation systems: design and implementation*, Butterworth-Heinemann.

Metter, M. und R. Bucher (2012), *Industrial Ethernet in der Automatisierungstechnik: Planung und Einsatz von Ethernet-LAN-Techniken im Umfeld von SIMATIC-Produkten*, John Wiley & Sons.

Moss, K. T. (2012), *Water treatment and distribution simulation for a SCADA security testbed*, Electronic Theses and Dissertations, Paper 1013, University of Louisville.

Müller, K.-R. (2014), *IT-Sicherheit mit System: Integratives IT-Sicherheits-, Kontinuitäts- und Risikomanagement – Sicherheitspyramide – Standards und Practices – SOA und Softwareentwicklung*, 5. Aufl., Springer-Verlag.

Nan, C., I. Eusgeld und W. Kröger (2013), Hidden vulnerabilities due to interdependencies between two systems, in: B. Hämmerli, N. Kalstad Svendsen und J. Lopez (Hrsg.), *International Workshop on Critical Information Infrastructures Security: 7th International Workshop, CRITIS 2012, Lillehammer, Norway, September 17-18, 2012, Revised Selected Papers*, Springer-Verlag, 252–263.

Nance, R. E. (1994), The conical methodology and the evolution of simulation model development, in: *Annals of Operations Research*, 56, 1–45.

National Institute of Standards and Technology (2007), *NIST Special Publication 800-94: Guide to Intrusion Detection and Prevention Systems (IDPS) – Recommendations of the National Institute of Standards and Technology*.

National Institute of Standards and Technology (2008), *NIST Special Publication 800-115: Technical Guide to Information Security Testing and Assessment – Recommendations of the National Institute of Standards and Technology*.

National Institute of Standards and Technology (2015), *NIST Special Publication 800-82, Revision 2: Guide to industrial control systems (ICS) security – supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as programmable logic controllers (PLC)*.

Pidikiti, D. S. u. a. (2013), SCADA communication protocols: vulnerabilities, attacks and possible mitigations, in: *CSI transactions on ICT*, 1:2, 135–141.

Pigan, R. und M. Metter (2015), *Automatisieren mit PROFINET: industrielle Kommunikation auf Basis von Industrial Ethernet*, John Wiley & Sons.

Queiroz, C. u. a. (2009), Building a SCADA security testbed, in: *Network and System Security, 2009. NSS'09. Third International Conference on*, IEEE, 357–364.

Rabe, M., S. Spieckermann und S. Wenzel (2008a), A new procedure model for verification and validation in production and logistics simulation, in: *Proceedings of the 40th Conference on Winter Simulation*, IEEE, 1717–1726.

Rabe, M., S. Spieckermann und S. Wenzel (2008b), *Verifikation und Validierung für die Simulation in Produktion und Logistik: Vorgehensmodelle und Techniken*, Springer Science & Business Media.

Reuter, M. und S. Zacher (2014), *Regelungstechnik für Ingenieure: Analyse, Simulation und Entwurf von Regelkreisen*, 15. Aufl., SpringerVieweg.

Schnell, G. und B. Wiedemann (2008), Bussysteme in der Automatisierungs-und Prozesstechnik, in: *Vieweg+ Teubner, Wiesbaden*.

Scholz, P. und R. Mörl (2003), Risikomanagement entlang von Wertschöpfungsketten, in: *Konferenzband zur Computas, Fachkonferenz für Risikomanagement, Karlsruhe, 19.–20. Mai 2003*.

Schumacher, S. (2016), IT-Sicherheit in der Wasserversorgung: Schutz kritischer Infrastrukturen, in: *Magdeburger Journal zur Sicherheitsforschung*, 11, 667–685.

Shannon, R. E. (1998), Introduction to the art and science of simulation, in: *Proceedings of the 30th conference on Winter simulation*, IEEE Computer Society Press, 7–14.

Siemens (2008), *SIMATIC Sicherheitskonzept: PCS 7 und WinCC – Basisdokument – Whitepaper*.

Singh, G. B. und B. G. Lipták (2006), Workstation Designs, in: B. Lipták (Hrsg.), *Instrument Engineers' Handbook: Process Control and Optimization*, 4. Aufl., Bd. 2, CRC Press.

Sowa, A. (2017), *Management der Informationssicherheit: Kontrolle und Optimierung*, SpringerVieweg.

Spitz, T., M. Blümle und H. Wiedel (2015), *Netzarchitektur – Kompass für die Realisierung: Unternehmensnetzwerke erfolgreich gestalten und erhalten*, Springer-Verlag.

Spitzberg, B. (2003), *Intrusion Prevention – Part of Your Defense in Depth Architecture?*, SANS Institute InfoSec Reading Room.

Stachowiak, H. (1973), *Allgemeine Modelltheorie*, Springer-Verlag.

Strauss, C. (2003), *Practical electrical network automation and communication systems*, Newnes.

Sullivan, D., E. Luiijf und E. J. Colbert (2016), Components of Industrial Control Systems, in: E. J. Colbert und A. Kott (Hrsg.), *Cyber-security of SCADA and Other Industrial Control Systems*, Springer, 15–28.

Talbot, J. E. und B. Lipták (2006), Controllers – Electronic Analog and Digital, in: B. Lipták (Hrsg.), *Instrument Engineers' Handbook: Process Control and Optimization*, 4. Aufl., Bd. 2, CRC Press.

Tiemeyer, E. (2016), *Handbuch IT-Systemmanagement: Handlungsfelder, Prozesse, Managementinstrumente, Good-Practices*, Carl Hanser Verlag.

Totherow, G. K. (2006), Human-Machine Interface Evolution, in: B. Lipták (Hrsg.), *Instrument Engineers' Handbook: Process Control and Optimization*, 4. Aufl., Bd. 2, CRC Press.

Urbina, D. I. u. a. (2016), Limiting the impact of stealthy attacks on industrial control systems, in: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, October 24–28, Vienna, Austria*, ACM, 1092–1105.

Urias, V. E. u. a. (2017), Dynamic cybersecurity training environments for an evolving cyber workforce, in: IEEE (Hrsg.), *2017 IEEE International Symposium on Technologies for Homeland Security (HST)*, IEEE, 1–6.

Urias, V. und B. Van Leeuwen (2016), Experimental Methods for Control System Security Research, in: E. J. M. Colbert und A. Kott (Hrsg.), *Cyber-security of SCADA and Other Industrial Control Systems*, Springer, 253–277.

Urias, V., B. Van Leeuwen und B. Richardson (2012), Supervisory Command and Data Acquisition (SCADA) system cyber security analysis using a live, virtual, and constructive (LVC) testbed, in: *Military Communications Conference (MILCOM) 2012*, IEEE, 1–8.

Van Leeuwen, B. u. a. (2009), Simulated, emulated, and physical investigative analysis (SEPIA) of networked systems, in: *Military Communications Conference (MILCOM) 2009*, IEEE, 1–7.

Van Leeuwen, B. u. a. (2010), Performing cyber security analysis using a live, virtual, and constructive (LVC) testbed, in: *Military Communications Conference (MILCOM) 2010*, IEEE, 1806–1811.

Vellaithurai, C. B., S. S. Biswas und A. K. Srivastava (2017), Development and Application of a Real-Time Test Bed for Cyber – Physical System, in: *IEEE Systems Journal*, 11:4, 2192–2203.

Vellaithurai, C. B. u. a. (2015), Real time modeling and simulation of cyber-power system, in: *Cyber Physical Systems Approach to Smart Electric Power Grid*, 43–74.

Wellenreuther, G. und D. Zastrow (2005), *Automatisieren mit SPS: Theorie und Praxis*, Springer-Verlag.

Kapitel 6
Schlussbetrachtung

Die hybride Testumgebung bietet eine neuartige Infrastruktur für Sicherheitstests wie Penetrationstests oder Schwachstellenanalysen, mit der günstige computerbasierte Abbildungen von Anlagenkomponenten mit realen Komponenten kombiniert werden können, wodurch eine hohe Flexibilität und Realitätsnähe bei niedrigen Kosten erreicht werden kann. Sie ist als effizienter Ansatz gerade für KRITIS-KMU attraktiv, wie sie etwa im Wassersektor oft anzutreffen sind. Denn auch wenn Automatisierung eine Chance für Ressourceneinsparungen sein kann, werden die gestiegenen Anforderungen an die Informationssicherheit gerade von diesen Unternehmen als eine Herausforderung angesehen.

Schwerpunkt dieses Buches war die Vorstellung und Diskussion von Methoden zur Modellierung und Implementierung solcher hybrider Simulationen als Testumgebungen für Sicherheitsanalysen. Hierfür wurden zunächst typische Architekturen von Industrieanlagen beleuchtet und daraufhin die besonderen Sicherheitsanforderungen von Kritischen Infrastrukturen diskutiert. Infolgedessen wurde die hybride Testumgebung in den Informationssicherheitsprozess eingeordnet, vorgestellt und mit klassischen Testumgebungen verglichen.

Im Hauptteil wurde eine Klassifikation vorgeschlagen, beispielhaft angewandt und detailliert, die die Bestimmung der Simulationsart von Komponenten in einer hybriden Testumgebung erleichtert. Anhand von unterschiedlichen Komponentenmerkmalen und Sicherheitseigenschaften kann die passende Simulationsart von Komponenten in einem schrittweisen Ordnungsprozess identifiziert werden. Auf diese Weise wird bei reduziertem Aufwand und reduzierten Kosten eine realitätsnahe Darstellung der verwendeten Betriebs- und Steuerungstechnik möglich, indem Simulationen, Emulationen und Virtualisierungen mit der Integration von realen Komponenten kombiniert werden. Auch ist es möglich, die Wiedergabetreue je nach Anforderung und Zielstellung zu variieren, etwa um Kosten und Aufwand weiter zu reduzieren.

Die Klassifikation wurde in ein Vorgehensmodell eingebettet, das die Modellierung und Implementation von hybriden Testumgebungen für cyber-physische Si-

O. Leps, *Hybride Testumgebungen für Kritische Infrastrukturen*,
https://doi.org/10.1007/978-3-658-22614-5_6

cherheitsanalysen leitet, von der Vorbereitungsphase bis zum Simulationsbetrieb und zur Analyse. Das Vorgehensmodell skizziert dabei wichtige Grundlagen für die Klassifikation und gewährleistet auch, dass die Simulationsartbestimmung in der Modellentwicklung geprüft und ggf. angepasst werden kann.

Insgesamt wurden das Vorgehensmodell und die Klassifikation als konsistente, nachvollziehbare und reproduzierbare Methoden konzipiert. Sie erleichtern die Ausführung einer aufwandsarmen, kostengünstigen und dennoch effektiven hybriden Testumgebung. Eine Nutzung durch KMU wird insbesondere dadurch erleichtert, dass die Ergebnisse an die IT-Grundschutz-Methodik anknüpfen und vielfach auf bekannte Methoden zurückgegriffen wird.

Allerdings zeigte eine kritische Betrachtung der hybriden Testumgebung und der in dieser Arbeit entwickelten bzw. vorgestellten Methoden auch Limitation auf und es zeigte sich, dass in Bezug auf hybride Testumgebungen an einigen Stellen weiterer Handlungs- oder Forschungsbedarf besteht.

So mussten in der Klassifikation unterschiedliche Zielstellungen, Architekturen und Komponentenvarianten berücksichtigt werden, was der Entwicklung eines einfachen und sparsamen (*parsimonious*) Vorgehens entgegenwirkte. Die große Komplexität und Heterogenität von Komponenten der Betriebs- und Steuerungstechnik führt dazu, dass eine Bestimmung der Simulationsart in der Praxis aufwendig sein und zu Ergebnissen schwankender Qualität führen kann. Dies ist gerade für KMU hinderlich, für die die hybride Testumgebung ein Mittel für realitätsnahe und kostengünstige Sicherheitsanalysen sein kann. Dies wird beispielsweise am Spannungsfeld zwischen Wiedergabetreue und Effizienz deutlich, welches in der Simulationsartbestimmung bei bestimmten Komponentenvarianten immer wieder auftritt. So gibt es Komponenten mit Softwarefirewalls oder auch Soft-SPS, die aufgrund ihrer Sicherheitseigenschaft möglichst realitätsnah abgebildet werden sollten, um etwa bei der Analyse von (D)DoS-Attacken belastbare Ergebnisse zu gewährleisten. Diese können manchmal jedoch auch vergleichsweise gut emuliert oder virtualisiert werden. Die Berücksichtigung unterschiedlicher Zielstellungen etwa im Hinblick auf weitere Kostenreduktion oder erhöhte Wiedergabetreue hätte jedoch die Komplexität der Klassifikation deutlich gesteigert. Um diese Problematik aufzufangen, wurde deshalb im dritten Schritt der Klassifikation der Moderator „Appliance“ eingeführt, der als Kunstgriff eine solche Abwägung ermöglicht bzw. beleuchtet und in bestimmten Fällen eine Abweichung von der Klassifikation vorsieht.

Ganz grundsätzlich wurde insbesondere die Klassifikation zwar als kostengünstige und aufwandsarme Methode konzipiert, aber aufgrund der vielfachen Forschungslücken und architektonischen Sonderfälle umfänglich wissenschaftlich beleuchtet, begründet und diskutiert. Somit konnte zunächst als Ergebnis noch kein

leichtgewichtiger Leitfaden konzipiert werden, dies kann jedoch auf Grundlage der Resultate an späterer Stelle folgen. Denn die Fallbeispiele legen die Annahme nahe, dass die Anwendung der Klassifikation unkompliziert und einfach sowie schnell und aufwandsarm sein kann. In der jetzigen Form sind sowohl die Klassifikation als auch das Vorgehensmodell eher als grober Handlungsleitfaden zu verstehen, der dem Modellierer je nach Zielstellung deutliche Ermessensspielräume überlässt. Im Rahmen dieser Diskussion wurde

Der vorgestellte Ansatz zur Implementierung hybrider Testumgebungen zielt in seiner aktuellen Form primär auf Penetrationstests und Schwachstellenanalysen ab. Auch über den Anwendungsfall der cyber-physischen Sicherheitsanalyse für Penetrationstests und Schwachstellenanalysen hinaus sind Weiterentwicklungen und Anpassungen denkbar. Gleichzeitig ist die Anwendung der hybriden Testumgebung für andere Sicherheitstests auszuschliessen, wozu aufgrund der computerbasierten Abbildungen von Komponenten etwa Social-Engineering-Attacken bzw. die Überprüfung personeller Faktoren oder auch Seitenkanalattacken gehören. Für andere Zielstellungen und Use-Cases wie Schadensfolgeanalysen, Performanzanalysen, Bedrohungsanalysen oder Robustheitstests könnten ggf. andere Komponentenmerkmale und Sicherheitseigenschaften relevant sein. Selbiges gilt für den Gegenstand der hybriden Testumgebung: Zwar können Vorgehensmodell und Klassifikation grundsätzlich auch auf andere Organisationen als leitungsgebundene KMU angewandt werden, trotzdem können für andere Organisationskontexte auch Anpassungen notwendig sein. Beispielsweise unterscheiden sich Anlagenarchitekturen von Energieversorgern so stark von leitungsgebundenen Daseinsversorgern, dass eine Anwendung nicht ohne Weiteres möglich ist. Zuletzt werden in Zukunft auch Trends wie Prozessleitanwendungen auf Tablets, Smartphones oder Smartwatches sowie IoT-Geräte, Cloud-Anwendungen oder möglicherweise Distributed Ledger Technologien berücksichtigt werden und Methoden ggf. entsprechend angepasst werden müssen.

Nachdem in dieser Arbeit die Klassifikation und das Vorgehensmodell konzipiert wurden, sind verschiedene Maßnahmen zur spezifischen Weiterentwicklungen empfehlenswert. Ganz grundsätzlich müssen die Methoden über die idealtypischen Fallbeispiele hinaus in Praxistests überprüft und ggf. angepasst werden. Des Weiteren ist eine weitere Schärfung und Komprimierung insbesondere der Klassifikation notwendig, um beispielsweise einen schlankeren Leitfaden zu entwickeln. Fragenkataloge könnten entwickelt werden, welche die Simulationsbestimmung und Modellierungsschritte weiter vereinfachen oder der Validierung der Testumgebung dienen. Als letzter Aspekt ist erwähnenswert, dass zwar den ICS-Testumgebungs-Gütekriterien der Wiedergabetreue, Wiederholbarkeit und Messgenauigkeit in der Klassifikation große Beachtung geschenkt wurde. Das Gütekri-

terium der technischen Sicherheit (Safety) hat aber nur eine geringe Rolle gespielt. Auch hier sind Weiterentwicklungen denkbar.

An dieser Stelle soll auch kurz auf allgemeinen Forschungsbedarf eingegangen werden, welcher in Verbund mit dieser Ausarbeitung identifiziert wurde. Zunächst besteht weiteres Optimierungspotential in dem Anliegen, eine möglichst aufwandsarme und kostengünstige hybride Testumgebung sicherzustellen. Hierzu gehört die Erarbeitung einer Bibliothek von Simulationsobjekten, die Dokumentation guter Praxis oder die Detaillierung der Standardisierung des hybriden Simulationsansatzes. Zudem könnten bestehende Methoden wie das Vorgehensmodell oder die Klassifikation um Erkenntnisse von Threat-Modelling- oder Attack-Tree-Techniken ergänzt werden, um spezifische Untersuchungen zu ermöglichen, Zielstellungen zu verfeinern und überkomplexe Sicherheitsanalysen zu vermeiden. Zuletzt ist erwähnenswert, dass weder für hybride Testumgebungen im Allgemeinen noch für Gütekriterien hybrider Testumgebungen im Speziellen derzeit ein einheitlicher Bewertungsrahmen existiert, der wiederum für die Entwicklung von Qualitätskriterien für hybride Testumgebungen hilfreich sein könnte.

Abschliessend ist zu sagen, dass die Ausarbeitung einer Reihe von Limitationen unterliegt, die dem Analysegegenstand und der eingesetzten Methodik geschuldet sind. Wie schon an anderer Stelle erwähnt wurde, weisen ICS-Architekturen- und Komponenten eine hohe Vielfalt auf. Zwar besteht der Anspruch, dass die Klassifikation mithilfe der identifizierten und abstrakten Sicherheitsmerkmale innerhalb des Betrachtungskontexts universell anwendbar ist, dennoch können Ausnahmen, die zu suboptimalen Modellierungsergebnissen führen, an dieser Stelle (noch) nicht ausgeschlossen werden. Unterschiedliche Architekturen und Varianten der wesentlichen ICS-Komponenten wurden analysiert und anhand von drei idealtypischen Fallbeispielen überprüft. Dennoch muss sich insbesondere die Klassifikation auch in der Praxis bewähren, um ihre Gültigkeit und Anwendbarkeit zu bestätigen.

Des Weiteren gelten dieselben Limitationen, die für Prozesse der Modellierung und Implementierung sowie für Testumgebungen und Sicherheitsanalysen im Allgemeinen gelten. Hier ist beispielsweise anzuführen, dass die Modellierung und Implementation einer hybriden Testumgebung zwar vereinfacht werden kann, die Ergebnisqualität aber dennoch zu einem großen Teil von der Erfahrung und dem Wissen des Modellierenden abhängig ist. Dabei ist der Erklärungsgehalt des Modells aufgrund von Vereinfachungen grundsätzlich reduziert. Ferner müssen die Ergebnisse der Sicherheitsanalyse auf die Originalanlagen rückübertragen werden, wobei der Transferaufwand aufgrund der Realitätsnähe im Regelfall minimal ist, aber insbesondere bei Komplexitätsreduktionen vorhanden sein und mit einem Informationsverlust einhergehen kann.

Literaturverzeichnis

Adams, J. R. (2011), *A water distribution and treatment simulation for testing cyber security enhancements for water sector SCADA systems*, University of Louisville.

Alves, T., R. Das und T. Morris (2016), Virtualization of Industrial Control System Testbeds for Cybersecurity, in: *Proceedings of the 2nd Annual Industrial Control System Security Workshop*, ACM, 10–14.

Assante, M. J. und R. M. Lee (2015), *The Industrial Control System Cyber Kill Chain, SANS Institute InfoSec Reading Room*, SANS Institute.

Association, A. W. W. (2014), *Process Control System Security Guidance for the Water Sector*, American Water Works Association.

Atos (2012), *The convergence of IT and Operational Technology – White Paper*, Atos.

Barnes, K., B. Johnson und R. Nickelson (2004), *Review Of Supervisory Control And Data Acquisition (SCADA) Systems*, Idaho National Engineering und Environmental Laboratory.

Bastigkeit, B., T. Schossig und F. Steinhauser (2009), Efficient testing of modern protection IEDs, in: *PAC World*, 3, 54–59.

Beard, C. S., B. Lipták und P. M. B. S. Girão (2006), Actuators: Digital, Electric, Hydraulic, Solenoid, in: B. Lipták (Hrsg.), *Instrument Engineers' Handbook: Process Control and Optimization*, 4. Aufl., Bd. 2, CRC Press.

Beckereit, M. (2010), Wasserwirtschaft morgen – Zukünftige Herausforderungen, in: *Chemie Ingenieur Technik*, 82:9, 1304–1304.

Berge, J. (2006), Transmitters: Smart, Multivariable, and Fieldbus, in: B. Lipták (Hrsg.), *Instrument Engineers' Handbook: Process Control and Optimization*, 4. Aufl., Bd. 2, CRC Press.

Birkhold, M. und J. Bauer (2014), *Sicherheit in der Automatisierungstechnik nach BSI IT-Grundschutz, geht das?*, Vortrag, URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Veranstaltungen/Grundschutz/1GS_Tag_

2014/02_1_IT-Grund_2014_Birkhold.pdf?__blob=publicationFile (besucht am: 20. 12. 2017).

Birkhold, M. und A. Lechler (2014), Modellierung von Automatisierungssystemen nach Vorgaben des BSI - Bundesministerium für Sicherheit in der Informationstechnik: Notwendigkeit, Modellkonzept, Vorteile, in: *wt Werkstattstechnik online*, 104:5, 301–306.

Bitkom und VKU (2015), *Praxisleitfaden IT-Sicherheitskatalog – Anforderungen an die IT für den sicheren Betrieb von Energieversorgungsnetzen*, Bitkom und VKU.

Bless, R. u. a. (2006), *Sichere Netzwerkkommunikation: Grundlagen, Protokolle und Architekturen*, Springer-Verlag.

Blevins, T. L. und M. Nixon (2006), DCS: Integration with Other Systems, in: B. Lipták (Hrsg.), *Instrument Engineers' Handbook: Process Control and Optimization*, 4. Aufl., Bd. 2, CRC Press.

Borchers, D. (2016), *IT-Sicherheitsgesetz: Wer was wann zu melden hat*, URL: https://www.heise.de/newsticker/meldung/IT-Sicherheitsgesetz-Wer-was-wann-zu-melden-hat-3096885.html (besucht am: 20. 12. 2017).

Bossel, H. (2004), *Systeme, Dynamik, Simulation – Modellbildung, Analyse und Simulation komplexer Systeme*, BoD.

Brauer, F. und S. Sturm (2014), *European Strategic Workshop on Water Safety Planning, 12–13 March 2014, Berlin, Germany – Key Outcomes*, Umweltbundesamt.

Brown, R. (2007), SCADA and DCS Vulnerabilities and Counter-Measures for Engineers, Technicians and IT-Staff, in: B. L. Capehart und L. C. Capehart (Hrsg.), *Web based enterprise energy and building automation systems*, The Fairmont Press, Inc.

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2011), *BBK-Glossar Ausgewählte zentrale Begriffe des Bevölkerungsschutzes (Praxis im Bevölkerungsschutz)*, Bd. 8, Bundesamt für Bevölkerungsschutz und Katastrophenhilfe.

Bundesamt für Sicherheit in der Informationstechnik (2015), *KRITIS-Sektorstudie: Ernährung und Wasser*, Bundesamt für Sicherheit in der Informationstechnik.

Bundesministerium des Innern (2009), *Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie)*, Bundesministerium des Innern.

Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit (2014), *Wasser ist Leben*, Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit.

Bundesministerium für Wirtschaft und Energie (2013), *Mensch-Technik-Interaktion: Leitfaden für Hersteller und Anwender*, Bd. 3, Bundesministerium für Wirtschaft und Energie.

Bundesministerium für Wirtschaft und Energie (2016), *Studie im Auftrag des Bundesministeriums für Wirtschaft und Energie: IT-Sicherheit für die Industrie 4.0 – Produktion, Produkte, Dienste von morgen im Zeichen globalisierter Wertschöpfungsketten, Abschlussbericht*, Bundesministerium für Wirtschaft und Energie.

Bundesverband der Energie- und Wasserwirtschaft (2015), *Wasserkunden sagen ihre Meinung: Ergebnisse des BDEW-Kundenbarometers Wasser / Abwasser 2015*, wvgw Wirtschafts- und Verlagsgesellschaft.

Bundesverband der Energie- und Wasserwirtschaft u. a. (2015), *Branchenbild der deutschen Wasserwirtschaft 2015*, wvgw Wirtschafts- und Verlagsgesellschaft.

Burton, D. P. u. a. (2009), *Simulated, Emulated, and Physical Investigative Analysis (SEPIA) of Networked Systems*, Sandia National Laboratories.

Byres, E. u. a. (2003), Cyber Security: Test Your System Five Ways, in: *InTech Magazine*, 24–27.

Campbell, B. D., C. W. Wendt und P. G. Friedmann (2006), PLC Software Advances, in: B. Lipták (Hrsg.), *Instrument Engineers' Handbook: Process Control and Optimization*, 4. Aufl., Bd. 2, CRC Press.

Capehart, B. L. und L. C. Capehart (2007), *Web based enterprise energy and building automation systems*, The Fairmont Press, Inc.

Castell-Exner, C. (2013), *Sicherheit in der Trinkwasserversorgung: Risikomanagement im Normalbetrieb – nationale und europäische Ansätze für kleinere Wasserversorger, IWW-Kolloquium "Technisches Risikomanagement – Neue Ansätze für kleine und große WVU", Mülheim*, Präsentation, URL: https://www.dvgw.de/index.php?eID=dumpFile&t=f&f=751&token=595a3d69ad95c090acfb07c49b86673644bbaa69 (besucht am: 20. 12. 2017).

Chabukswar, R. u. a. (2010), Simulation of Network Attacks on SCADA Systems, in: *First Workshop on Secure Control Systems*.

Christiansson, H. und E. Luiijf (2008), Creating a European SCADA security testbed, in: E. Goetz und S. Shenoi (Hrsg.), *International Conference on Critical Infrastructure Protection, 1st IFIP WG 11.10 International Conference, ICCIP 2007, New Hampshire, USA, Revised Selected Papers*, Springer, 237–247.

Ciancamerla, E. u. a. (2010), Discrete event simulation of QoS of a SCADA system interconnecting a Power grid and a Telco network, in: *What Kind of Information Society? Governance, Virtuality, Surveillance, Sustainability, Resilience*, Springer, 350–362.

Clare, W. N. u. a. (2006), PLCs: Programmable Logic Controllers, in: B. Lipták (Hrsg.), *Instrument Engineers' Handbook: Process Control and Optimization*, 4. Aufl., Bd. 2, CRC Press.

Colbert, E. J. M. und S. Hutchinson (2016), Intrusion Detection in Industrial Control Systems, in: E. J. M. Colbert und A. Kott (Hrsg.), *Cyber-security of SCADA and Other Industrial Control Systems*, Springer-Verlag, 239–251.

Collier, Z. A. u. a. (2016), Security Metrics in Industrial Control Systems, in: E. J. M. Colbert und A. Kott (Hrsg.), *Cyber-security of SCADA and Other Industrial Control Systems*, Springer-Verlag, 239–251.

Davis, C. u. a. (2006), SCADA cyber-security testbed development, in: *Power Symposium, 2006. NAPS 2006. 38th North American*, IEEE, 483–488.

Detken, K.-O., E. Eren und M. Steiner (2012), Erhöhung der IT-Sicherheit durch Konfigurationsunterstützung bei der Virtualisierung, DACH Security, in: P. Schartner und J. Taeger (Hrsg.), *DACH Security 2012: Bestandsaufnahme – Konzepte – Anwendungen – Perspektiven*, Prof. Dr. Patrick Horster.

Dinger, J. und H. Hartenstein (2008), *Netzwerk-und IT-Sicherheitsmanagement: Eine Einführung*, KIT Scientific Publishing.

Duggan, D. u. a. (2005), Penetration testing of industrial control systems, in: *Sandia National Laboratories*.

Engler, J., G. Haag und B. Biedermann (2014), *Erhebung und Bewertung der öffentlichen Wasserversorgung in Bayern – Versorgungssicherheit derzeit und künftig*, Präsentation auf dem DVGW-Forum SSichere Wasserversorgung im Kleinhandel", Mülheim an der Ruhr, (besucht am: 20. 12. 2017).

ENISA (2016), *Communication network dependencies for ICS/SCADA Systems*, European Union Agency For Network und Information Security.

EurEau (2011), *EurEau Position Paper on the EU Guidance on Developing Water Safety Plans for Small Supplies*, EurEau – European federation of national associations of drinking water suppliers und waste water services.

Evancich, N. und J. Li (2016), Attacks on Industrial Control Systems, in: E. J. M. Colbert und A. Kott (Hrsg.), *Cyber-security of SCADA and Other Industrial Control Systems*, Springer-Verlag, 239–251.

Floß, A. (2015), *Sicherheit von industriellen Steuerungssystemen: Sicherheitsmanagement mit der BSI IT-Grundschutz-Vorgehensweise*, Präsentation auf dem 14. Deutschen IT-Sicherheitskongress, Bonn.

Fritsch, P. u. a. (2014), *Mutschmann/Stimmelmayr: Taschenbuch der Wasserversorgung*, SpringerVieweg.

Früh, K. F. (2009), *Handbuch der Prozessautomatisierung: Prozessleittechnik für verfahrenstechnische Anlagen*, Oldenbourg Industrieverlag.

Gao, H. u. a. (2014), An Industrial Control System Testbed Based on Emulation, Physical Devices and Simulation, in: *International Conference on Critical Infrastructure Protection VIII, 8th IFIP WG 11.10 International Conference, ICCIP 2014*, Jonathan Butts und Sujeet Hanoi, 79–91.

Gartner (2017), *Gartner IT Glossary, Operational Technology*, URL: http://www.gartner.com/it-glossary/operational-technology-ot/ (besucht am: 20. 12. 2017).

Genge, B., C. Siaterlis und M. Hohenadel (2012), Amici: An assessment platform for multi-domain security experimentation on critical infrastructures, in: B. M. Hämmerli, N. K. Svendsen und J. Lopez (Hrsg.), *Critical Information Infrastructures Security, 7th International Workshop, CRITIS 2012 Lillehammer, Norway, September 2012 Revised Selected Papers*, Springer-Verlag, 228–239.

Ghosh, A. (2006), Programmable Safety Systems, in: B. Lipták (Hrsg.), *Instrument Engineers' Handbook: Process Control and Optimization*, 4. Aufl., Bd. 2, CRC Press.

Gonzalez, C. A. und J. Reed (2016), Cyber Physical Intrusion Detection, in: E. J. M. Colbert und A. Kott (Hrsg.), *Cyber-security of SCADA and Other Industrial Control Systems*, Springer-Verlag, 239–251.

Grambow, M. (2013), *Nachhaltige Wasserbewirtschaftung: Konzept und Umsetzung eines vernünftigen Umgangs mit dem Gemeingut Wasser*, SpringerVieweg.

Greeff, G. und R. Ghoshal (2004), *Practical E-manufacturing and supply chain management*, Newnes.

Green, B. u. a. (2017), Pains, Gains and PLCs: Ten Lessons from Building an Industrial Control Systems Testbed for Security Research, in: *The 10th USENIX Workshop on Cyber Security Experimentation and Test (CSET '17)*, USENIX Association.

Gronau, N. (2009), *Wissen prozessorientiert managen: Methode und Werkzeuge für die Nutzung des Wettbewerbsfaktors Wissen in Unternehmen*, Oldenbourg Industrieverlag.

Gronau, N., C. Fohrholz und S. Lass (2011), Hybrider Simulator – Neuer Ansatz zum Produktionsmanagement, in: *ZWF Zeitschrift für wirtschaftlichen Fabrikbetrieb*, 106:4, 204–208.

Gronau, N. und E. Weber (2009), *Wandlungsfähigkeit: Generische Strategien zur Handhabung von Veränderungen in der Umwelt*, Arbeitsbericht, WI–2009–07, Lehrstuhl für Wirtschaftsinformatik und Electronic Government, Universität Potsdam.

Gronau, N. u. a. (2012), *Organisation des Schutzes der kritischen Infrastruktur Wasserversorgung: Grundlagen und praktische Anwendung für Betreiber*, GITO mbH Verlag.

Grube, G. und H. Theuer (2011), Die Spielarten der Simulation, in: *Computer &Automation*, 2011:9.

Gurschler, T. u. a. (2017), Risikobeurteilung in der IT-Sicherheit Kritischer Infrastrukturen – Eine Analyse der Risikobeurteilung im Förderschwerpunkt ITS|KRITIS, in: *Bundesamt für Sicherheit in der Informationstechnik: Digitale Gesellschaft zwischen Risikobereitschaft und Sicherheitsbedürfnis: Tagungsband des 15. Deutschen IT-Sicherheitskongress 2017*, SecuMedia Verlag.

Hafner, M. und R. Breu (2008), *Security engineering for service-oriented architectures*, Springer Science & Business Media.

Hahn, A. u. a. (2013), Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid, in: *IEEE Transactions on Smart Grid*, 4:2, 847–855.

Hellfeld, S. (2012), *Hybride Simulation mobiler Geschäftsprozesse*, KIT Scientific Publishing.

Henzler, R. G. (1992), *Information und Dokumentation: Sammeln, Speichern und Wiedergewinnen von Fachinformation in Datenbanken*, Springer-Verlag.

Hering, E., A. Vogt und K. Bressler (2013), *Handbuch der elektrischen Anlagen und Maschinen*, Springer-Verlag.

Hieb, J., J. Graham und S. Patel (2008), Security Enhancements for Distributed Control Systems, in: E. Goetz und S. Shenoi (Hrsg.), *International Conference on Critical Infrastructure Protection, 1st IFIP WG 11.10 International Conference, ICCIP 2007, New Hampshire, USA, Revised Selected Papers*, Springer, 237–247.

Hillenbrand, T. u. a. (2013), Herausforderungen einer nachhaltigen Wasserwirtschaft: Innovationsreport Arbeitsbericht, in: *Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag*, Arbeitsbericht 158.

Hoeppner, C. H. u. a. (2006), Telemetering Systems, in: B. Lipták (Hrsg.), *Instrument Engineers' Handbook: Process Control and Optimization*, 4. Aufl., Bd. 2, CRC Press.

Holm, H. u. a. (2015), A survey of industrial control system testbeds, in: S. Buchegger und M. Dam (Hrsg.), *Secure IT Systems, Lecture Notes in Computer Science*, Springer, 11–26.

Hong, J. u. a. (2015), Cyber-Physical Security Testbed for Substations in a Power Grid, in: C. C. Liu, S. K. Khaitan und J. D. McCalley (Hrsg.), *Cyber Physical Systems Approach to Smart Electric Power Grid*, Springer, 261–301.

Howser, G. (2015), Using information flow methods to secure cyber-physical systems, in: M. Rice und S. Shenoi (Hrsg.), *International Conference on Critical Infrastructure Protection IX, 9th IFIP WG 11.10 International Conference, ICCIP 2015, Arlington, VA, USA, March 16-18, Revised Selected Papers*, Springer-Verlag, 185–205.

Hulsmann, A. und P. Smeets (2011), *Towards a Guidance Document for the implementation of a Risk Assessment for small water supplies in the European Union*, KWR Watercycle Research Institute.

Invensys (2004), *Process Control Network – Reference Architecture: White Paper*, hrsg. von D. Rath, Invensys.

IWW Rheinisch-Westfälisches Institut für Wasserforschung (2004), *Kennzahlen für die Wasserversorgung: Feld-Test des Kennzahlensystems der IWA (International Water Association) – Nationales Teilprojekt Deutschland: Abschlussbericht zum Forschungsvorhaben 02 WT 0224*, IWW.

Jäger, T. (2015), *Handbuch Sicherheitsgefahren*, SpringerVS.

Jaromin, R. u. a. (2013), Design and implementation of industrial control system emulators, in: J. Butts und S. Shenoi (Hrsg.), *International Conference on Critical Infrastructure Protection VII, 7th IFIP WG 11.10 International Conference, ICCIP 2013, Washington, DC, USA, March 18-20, Revised Selected Papers*, Springer-Verlag, 35–46.

Kahneman, D. und A. Tversky (1979), Prospect theory: An analysis of decision under risk, in: *Econometrica*, 47:2, 263–292.

Karger, R. und F. Hoffmann (2013), *Wasserversorgung: Gewinnung – Aufbereitung – Speicherung – Verteilung*, Bd. 14, SpringerVieweg.

Kersten, H., J. Reuter und K.-W. Schröder (2013), *IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz*, Springer.

Khorrami, F., P. Krishnamurthy und R. Karri (2016), Cybersecurity for control systems: A process-aware perspective, in: *IEEE Design & Test*, 33:5, 75–83.

Kipker, D.-K. und D. Pfeil (2016), IT-Sicherheitsgesetz in Theorie und Praxis, in: *Datenschutz und Datensicherheit-DuD*, 40:12, 810–814.

Kless, S. und B. Veldhues (2008), Ausgewählte Ergebnisse für kleine und mittlere Unternehmen in Deutschland 2005, in: *Wirtschaft und Statistik*, 3, 225 ff.

Knapp, E. D. und J. T. Langill (2014), *Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems*, Syngress.

Kraft, R. und M. Stöwer (2017), IT-Risikomanagement im Produktionsumfeld – Herausforderungen und Lösungsansätze, in: *HMD Theorie und Praxis der Wirtschaftsinformatik*, 54:1, 84–96.

Kuhnert, J. und O. Leps (2015a), *Neue Wohnungsgemeinnützigkeit (NWG): Wege zu langfristig preiswertem und zukunftsgerechtem Wohnraum (Wohnungsgemeinnützigkeit 2.0) – Studie im Auftrag von Bündnis 90/Die Grünen Bundestagsfraktion vom Dezember 2015 (Kurzfassung)*, Bundestagsfraktion Bündnis 90/Die Grünen.

Kuhnert, J. und O. Leps (2015b), *Neue Wohnungsgemeinnützigkeit (NWG): Wege zu langfristig preiswertem und zukunftsgerechtem Wohnraum (Wohnungsgemeinnützigkeit 2.0) – Studie im Auftrag von Bündnis 90/Die Grünen Bundestagsfraktion vom Dezember 2015 (Langfassung)*, Bundestagsfraktion Bündnis 90/Die Grünen.

Kuhnert, J. und O. Leps (2017), *Neue Wohnungsgemeinnützigkeit: Wege zu langfristig preiswertem und zukunftsgerechtem Wohnraum*, SpringerVS.

Laisiepen, K., E. Lutterbeck und K.-H. Meyer-Uhlenried (1972), *Grundlagen der praktischen Information und Dokumentation*, Verlag Dokumentation.

Langmann, R. (2004), *Taschenbuch der Automatisierung*, Hanser Verlag.

Lass, S., C. Fohrholz und H. Theuer (2011), Hybride Simulation – Neuer Ansatz zum Produktionsmanagement, in: *Industrie & Management*, 1, 13 ff.

Lass, S., H. Theuer und N. Gronau (2011), Effiziente Simulation im Produktionsmanagement:Schnelle und belastbare Analyse von Fertigungsprozessen, in: *Industrie Management*, 27:3, 13–15.

Lass, S. (2011), A new Approach to Simulation in Production Management, in: H. El Maraghy (Hrsg.), *Enabling Manufacturing Competitiveness and Economic Sustainability: Proceedings of the 4th International Conference on Changeable, Agile, Reconfigurable and Virtual production (CARV 2011), Montreal, Canada, 2-5 October 2011*, Springer, 598–604.

Lass, S. und D. Fuhr (2013), IT-Sicherheit in der Fabrik, in: *Productivity Management*, 18:2.

Lass, S. und N. Gronau (2012), Efficient Analysis of Production Processes with a Hybrid Simulation Environment, in: H. Nylund u. a. (Hrsg.), *Proceedings of the FAIM 2012: 22nd International Conference on Flexible Automation and Intelligent Manufacturing, June 10th-13th, 2012, Helsinki, Finland*, Tampere University of Technology.

Lass, S. und D. Kotarski (2014), IT-Sicherheit als besondere Herausforderung von Industrie 4.0, in: W. Kersten, H. Koller und H. Lödding (Hrsg.), *Schriftenreihe der Hochschulgruppe für Arbeits- und Betriebsorganisation e.V. (HAB): Industrie 4.0 – Wie intelligente Vernetzung und kognitive Systeme unsere Arbeit verändern Schriftenreihe der Hochschulgruppe für Arbeits- und Betriebsorganisation*, Gito Verlag Berlin, 397–419.

Lass, S. und H. Theuer (2011), Hybride Simulation – Den besten Grad an dezentraler Produktionssteuerung bestimmen, in: *Productivity Management*, 13–16.

Law, A. M., W. D. Kelton und W. D. Kelton (1991), *Simulation modeling and analysis*, 2. Aufl., McGraw-Hill.

Leps, O. (2016), *Nutzung und Akzeptanz von E-Government-Fachanwendungen in der öffentlichen Verwaltung: Eine empirische Analyse am Beispiel des europäischen Binnenmarkt-Informationssystems*, Logos Verlag.

Lerch, R. (2012), *Elektrische Messtechnik: Analoge, digitale und computergestützte Verfahren*, 6. Aufl., SpringerVieweg.

Lewis, T. G. (2014), *Critical infrastructure protection in homeland security: defending a networked nation*, John Wiley & Sons.

Liao, H.-J. u. a. (2013), Intrusion detection system: A comprehensive review, in: *Journal of Network and Computer Applications*, 36:1, 16–24.

Lin, J., S. Sedigh und A. Miller (2009), Towards integrated simulation of cyber-physical systems: a case study on intelligent water distribution, in: *Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, DASC'09*, IEEE, 690–695.

Lipták, B. (2006a), DCS: Basic Trends and Advances, in: B. Lipták (Hrsg.), *Instrument Engineers' Handbook: Process Control and Optimization*, 4. Aufl., Bd. 2, CRC Press.

Lipták, B. (2006b), *Instrument Engineers' Handbook: Process Control and Optimization*, 4. Aufl., Bd. 2, CRC Press.

Litz, L. (2013), *Grundlagen der Automatisierungstechnik: Regelungssysteme – Steuerungssysteme – hybride Systeme*, Walter de Gruyter.

Luiijf, E. (2016), Threats in Industrial Control Systems, in: E. J. Colbert und A. Kott (Hrsg.), *Cyber-security of SCADA and Other Industrial Control Systems*, Springer, 15–28.

Macaulay, T. und B. L. Singer (2011), *Cybersecurity for industrial control systems: SCADA, DCS, PLC, HMI, and SIS*, CRC Press.

Mamzic, C. L., R. Gilbert und B. G. Lipták (2006), Relays for Computing and Programmers, in: B. Lipták (Hrsg.), *Instrument Engineers' Handbook: Process Control and Optimization*, 4. Aufl., Bd. 2, CRC Press.

Mathioudakis, K. u. a. (2013), Towards generic scada simulators: A survey of existing multi-purpose co-simulation platforms, best practices and use-cases, in: *Scientific Cooperations International Workshops in Electrical-Electronics Engineering*, 33–39.

McDonald, J. D. (2016), *Electric Power Substations Engineering*, 2. Aufl., CRC Press.

McLaughlin, S. u. a. (2016), The cybersecurity landscape in industrial control systems, in: *Proceedings of the IEEE*, 104:5, 1039–1057.

McNabb, J. (2010), *Cyberterrorism & the Security of the National Drinking Water Infrastructure*, Presentation at the DEF CON 18, July 31, 2010.

Mehta, B. R. und Y. J. Reddy (2014), *Industrial process automation systems: design and implementation*, Butterworth-Heinemann.

Metter, M. und R. Bucher (2012), *Industrial Ethernet in der Automatisierungstechnik: Planung und Einsatz von Ethernet-LAN-Techniken im Umfeld von SIMATIC-Produkten*, John Wiley & Sons.

Moss, K. T. (2012), *Water treatment and distribution simulation for a SCADA security testbed*, Electronic Theses and Dissertations, Paper 1013, University of Louisville.

Müller, K.-R. (2014), *IT-Sicherheit mit System: Integratives IT-Sicherheits-, Kontinuitäts- und Risikomanagement – Sicherheitspyramide – Standards und Practices – SOA und Softwareentwicklung*, 5. Aufl., Springer-Verlag.

Müller, M. M. (2008), Daseinsvorsorge und die EU: Anmerkungen zu einem alten Streit und jüngeren Entwicklungen, in: E. Bos und J. Dieringer (Hrsg.), *Die Genese einer Union der 27: Die Europäische Union nach der Osterweiterung*, SpringerVS, 205–212.

Nan, C., I. Eusgeld und W. Kröger (2013), Hidden vulnerabilities due to interdependencies between two systems, in: B. Hämmerli, N. Kalstad Svendsen und J. Lopez (Hrsg.), *International Workshop on Critical Information Infrastructures Security: 7th International Workshop, CRITIS 2012, Lillehammer, Norway, September 17-18, 2012, Revised Selected Papers*, Springer-Verlag, 252–263.

Nance, R. E. (1994), The conical methodology and the evolution of simulation model development, in: *Annals of Operations Research*, 56, 1–45.

Otillinger, F. und V. Szymansky (2015), Die deutsche Wasserwirtschaft – leistungsfähig, zuverlässig, nachhaltig, in: *Kommunalwirtschaft*, 2015:7–8, 57–63.

Pidikiti, D. S. u. a. (2013), SCADA communication protocols: vulnerabilities, attacks and possible mitigations, in: *CSI transactions on ICT*, 1:2, 135–141.

Pigan, R. und M. Metter (2015), *Automatisieren mit PROFINET: industrielle Kommunikation auf Basis von Industrial Ethernet*, John Wiley & Sons.

Plaßmann, W. und D. Schulz (2016), *Handbuch Elektrotechnik: Grundlagen und Anwendungen für Elektrotechniker*, 6. Aufl., Springer-Verlag.

Pöhls, U. (2016), *Qualität und Image von Trinkwasser in Deutschland (TWIS) (Erweiterte Fassung), Datenreport 2015/16*, Institut für empirische Sozial- und Kommunikationsforschung.

Queiroz, C. u. a. (2009), Building a SCADA security testbed, in: *Network and System Security, 2009. NSS'09. Third International Conference on*, IEEE, 357–364.

Rabe, M., S. Spieckermann und S. Wenzel (2008a), A new procedure model for verification and validation in production and logistics simulation, in: *Proceedings of the 40th Conference on Winter Simulation*, IEEE, 1717–1726.

Rabe, M., S. Spieckermann und S. Wenzel (2008b), *Verifikation und Validierung für die Simulation in Produktion und Logistik: Vorgehensmodelle und Techniken*, Springer Science & Business Media.

Reuter, M. und S. Zacher (2014), *Regelungstechnik für Ingenieure: Analyse, Simulation und Entwurf von Regelkreisen*, 15. Aufl., SpringerVieweg.

Röchert-Voigt, T., M. Stein und E. Weber (2010), *Wandlungsfähige Schutzstrukturen und Folgenabschätzung: Theoretische Grundlagen und praktische Anwendungen; Handlungsleitfaden*, GITO mbH Verlag.

Schaumüller-Bichl, I. und A. Kolberger (2016), Information Security Risk Analysis in komplexen Systemen – neue Herausforderungen und Lösungsansätze, in: H. C. Mayr und M. Pinzger (Hrsg.), *GI-Jahrestagung, INFORMATIK 2016, Lecture Notes in Informatics (LNI)*, Gesellschaft für Informatik, 609–617.

Schmölzer, J. (2010), *IT-Sicherheit von SCADA-Systemen*, Diplomarbeit, Fachbereich Informationstechnik & Elektrotechnik, Hochschule Mittweida (FH).

Schnell, G. und B. Wiedemann (2008), Bussysteme in der Automatisierungs-und Prozesstechnik, in: *Vieweg+ Teubner, Wiesbaden*.

Scholz, P. und R. Mörl (2003), Risikomanagement entlang von Wertschöpfungsketten, in: *Konferenzband zur Computas, Fachkonferenz für Risikomanagement, Karlsruhe, 19.–20. Mai 2003*.

Schumacher, S. (2016), IT-Sicherheit in der Wasserversorgung: Schutz kritischer Infrastrukturen, in: *Magdeburger Journal zur Sicherheitsforschung*, 11, 667–685.

Schwarting, G. (2001), Kommunale Wirtschaft – Vor großen Herausforderungen, in: *Zeitschrift für öffentliche und gemeinwirtschaftliche Unternehmen*, 24:3, 286–307.

Shannon, R. E. (1998), Introduction to the art and science of simulation, in: *Proceedings of the 30th conference on Winter simulation*, IEEE Computer Society Press, 7–14.

Siaterlis, C., A. P. Garcia und B. Genge (2013), On the use of Emulab testbeds for scientifically rigorous experiments, in: *IEEE Communications Surveys & Tutorials*, 15:2, 929–942.

Singh, G. B. und B. G. Lipták (2006), Workstation Designs, in: B. Lipták (Hrsg.), *Instrument Engineers' Handbook: Process Control and Optimization*, 4. Aufl., Bd. 2, CRC Press.

Sosinsky, B. (2009), *Networking bible*, Bd. 567, John Wiley & Sons.

Sowa, A. (2017), *Management der Informationssicherheit: Kontrolle und Optimierung*, SpringerVieweg.

Sowa, A., P. Duscha und S. Schreiber (2015), *IT-Revision, IT-Audit und IT-Compliance: Neue Ansätze für die IT-Prüfung*, SpringerVieweg.

Spitz, T., M. Blümle und H. Wiedel (2015), *Netzarchitektur – Kompass für die Realisierung: Unternehmensnetzwerke erfolgreich gestalten und erhalten*, Springer-Verlag.

Spitzberg, B. (2003), *Intrusion Prevention – Part of Your Defense in Depth Architecture?*, SANS Institute InfoSec Reading Room.

Stachowiak, H. (1973), *Allgemeine Modelltheorie*, Springer-Verlag.

Strassburger, S., G. Schmidgall und S. Haasis (2003), Distributed manufacturing simulation as an enabling technology for the digital factory, in: *Journal of Advanced Manufacturing Systems*, 2:1, 111–126.

Strauss, C. (2003), *Practical electrical network automation and communication systems*, Newnes.

Strauß, J. (2015), Infrastruktursicherheit, in: T. Jäger (Hrsg.), *Handbuch Sicherheitsgefahren*, SpringerVS.

Sullivan, D., E. Luiijf und E. J. Colbert (2016), Components of Industrial Control Systems, in: E. J. Colbert und A. Kott (Hrsg.), *Cyber-security of SCADA and Other Industrial Control Systems*, Springer, 15–28.

Talbot, J. E. und B. Lipták (2006), Controllers – Electronic Analog and Digital, in: B. Lipták (Hrsg.), *Instrument Engineers' Handbook: Process Control and Optimization*, 4. Aufl., Bd. 2, CRC Press.

Tews, E. und C. Schlehuber (2014), Quantitative Ansätze zur IT-Risikoanalyse, in: *Sicherheit*, TU Darmstadt, 293–303.

Theuer, H. (2012), Extension of Value Stream Design for the Simulation of Autonomous Production Systems, in: M. F. Zaeh (Hrsg.), *Enabling Manufacturing Competitiveness and Economic Sustainability: Proceedings of the 5th International Conference on Changeable, Agile, Reconfigurable and Virtual Production (CARV 2013), Munich, Germany, October 6th-9th, 2013*, Springer, 586–591.

Thim, C. und D. Kotarski (2015), Herausforderungen der IT-Sicherheit bei kleinen und mittleren Betreibern kritischer Infrastrukturen, in: *DVGW energie | wasser-praxis*, 10, 44–46.

Thornton, Z. und T. Morris (2015), Enhancing a virtual SCADA laboratory using Simulink, in: M. Rice und S. Shenoi (Hrsg.), *Critical Infrastructure Protection IX, 9th IFIP 11.10 International Conference, ICCIP 2015 Arlington, VA, USA, March 16–18, 2015 Revised Selected Papers*, Springer-Verlag, 119–133.

Tiemeyer, E. (2016), *Handbuch IT-Systemmanagement: Handlungsfelder, Prozesse, Managementinstrumente, Good-Practices*, Carl Hanser Verlag.

Totherow, G. K. (2006), Human-Machine Interface Evolution, in: B. Lipták (Hrsg.), *Instrument Engineers' Handbook: Process Control and Optimization*, 4. Aufl., Bd. 2, CRC Press.

Umweltbundesamt (2014), *Wasserwirtschaft in Deutschland Teil 1 – Grundlage*, Umweltbundesamt.

Umweltbundesamt (2016), *Rund um das Trinkwasser*, Umweltbundesamt.

Urbina, D. I. u. a. (2016), Limiting the impact of stealthy attacks on industrial control systems, in: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, October 24–28, Vienna, Austria*, ACM, 1092–1105.

Urias, V. E. u. a. (2017), Dynamic cybersecurity training environments for an evolving cyber workforce, in: IEEE (Hrsg.), *2017 IEEE International Symposium on Technologies for Homeland Security (HST)*, IEEE, 1–6.

Urias, V. und B. Van Leeuwen (2016), Experimental Methods for Control System Security Research, in: E. J. M. Colbert und A. Kott (Hrsg.), *Cyber-security of SCADA and Other Industrial Control Systems*, Springer, 253–277.

Urias, V., B. Van Leeuwen und B. Richardson (2012), Supervisory Command and Data Acquisition (SCADA) system cyber security analysis using a live, virtual, and constructive (LVC) testbed, in: *Military Communications Conference (MILCOM) 2012*, IEEE, 1–8.

Van Leeuwen, B. u. a. (2009), Simulated, emulated, and physical investigative analysis (SEPIA) of networked systems, in: *Military Communications Conference (MILCOM) 2009*, IEEE, 1–7.

Van Leeuwen, B. u. a. (2010), Performing cyber security analysis using a live, virtual, and constructive (LVC) testbed, in: *Military Communications Conference (MILCOM) 2010*, IEEE, 1806–1811.

Vellaithurai, C. B., S. S. Biswas und A. K. Srivastava (2017), Development and Application of a Real-Time Test Bed for Cyber – Physical System, in: *IEEE Systems Journal*, 11:4, 2192–2203.

Vellaithurai, C. B. u. a. (2015), Real time modeling and simulation of cyber-power system, in: *Cyber Physical Systems Approach to Smart Electric Power Grid*, 43–74.

Ver.di (2015), *Wasserwirtschaft in Deutschland: Branchenanalyse – Trend und Herausforderungen*, Ver.di.

Waiz, E. (2009), Daseinsvorsorge in der Europäischen Union – Etappen einer Debatte, in: A. Krautscheid (Hrsg.), *Die Daseinsvorsorge im Spannungsfeld von europäischem Wettbewerb und Gemeinwohl*, Springer, 41–76.

Wang, C., L. Fang und Y. Dai (2010), A simulation environment for SCADA security analysis and assessment, in: *2010 International Conference on Measuring Technology and Mechatronics Automation (ICMTMA)*, Bd. 1, IEEE, 342–347.

Wegener, C., T. Milde und W. Dolle (2016), *Informationssicherheits-Management: Leitfaden für Praktiker und Begleitbuch zur CISM-Zertifizierung*, Springer-Verlag.

Weiblein, W. und C. Radis (2014), *Tendenzen und Herausforderungen der deutschen Wasserwirtschaft: Zwischen Versorgungssicherheit, Veränderungsprozessen und rechtlichen Rahmenbedingungen*, Baker Tilly Roelfs.

Wellenreuther, G. und D. Zastrow (2005), *Automatisieren mit SPS: Theorie und Praxis*, Springer-Verlag.

Wilhoit, K. (2013), *Wer steckt tatsächlich hinter den Angriffen auf ICS-Ausrüstung?*, Trend Micro.

Standards und Normen

AVBWasserV (2014), *Verordnung über Allgemeine Bedingungen für die Versorgung mit Wasser vom 20. Juni 1980 (BGBl. I S. 750, 1067), die zuletzt durch Artikel 8 der Verordnung vom 11. Dezember 2014 (BGBl. I S. 2010) geändert worden ist*.

BSI IT-Grundschutz-Kompendium (2017a), *Baustein NET.1.1 Netzarchitektur und -design im IT-Grundschutz*.

BSI IT-Grundschutz-Kompendium (2017a), *IND.1 Betriebs- und Steuerungstechnik*.

BSI IT-Grundschutz-Kompendium (2017b), *IND.2.1 Allgemeine ICS-Komponente*.

BSI IT-Grundschutz-Kompendium (2017c), *IND.2.2 Speicherprogrammierbare Steuerung (SPS)*.

BSI IT-Grundschutz-Kompendium (2017d), *IND.2.3 Sensoren und Aktoren*.

BSI IT-Grundschutz-Kompendium (2017e), *IND.2.4 Maschine*.

BSI IT-Grundschutz-Kompendium (2017b), *Umsetzungshinweise zum Baustein IND.1 Betriebs- und Steuerungstechnik*.

BSI IT-Grundschutz-Kompendium (2017f), *Umsetzungshinweise zum Baustein INF.3 Elektrotechnische Verkabelung*.

BSI IT-Grundschutz-Kompendium (2017g), *Umsetzungshinweise zum Baustein INF.4 IT-Verkabelung*.

BSI-Gesetz (2017), *Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG) vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 1 des Gesetzes vom 23. Juni 2017 (BGBl. I S. 1885) geändert worden ist*.

BSI-KritisV (2016), *Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung – BSI-KritisV)*.

BSI-Standard 100-1 (2008), *Managementsysteme für Informationssicherheit (ISMS)*.

BSI-Standard 100-2 (2008), *IT-Grundschutz-Vorgehensweise*.

BSI-Standard 100-3 (2008), *Risikoanalyse auf der Basis von IT-Grundschutz*.

BSI-Standard 100-4 (2008), *Notfallmanagement*.
BSI-Standard 200-1 (2017a), *Managementsysteme für Informationssicherheit (ISMS)*.
BSI-Standard 200-1 (2017b), *Managementsysteme für Informationssicherheit (ISMS) – Community Draft*.
BSI-Standard 200-2 (2017a), *IT-Grundschutz-Methodik*.
BSI-Standard 200-2 (2017b), *IT-Grundschutz-Methodik – Community Draft*.
BSI-Standard 200-3 (2016), *Risikoanalyse auf der Basis von IT-Grundschutz – Community Draft*.
BSI-Standard 200-3 (2017), *Risikoanalyse auf der Basis von IT-Grundschutz*.
Bundesamt für Sicherheit in der Informationstechnik (2013), *ICS-Security-Kompendium*.
Bundesamt für Sicherheit in der Informationstechnik (2014), *ICS-Security-Kompendium: Testempfehlungen und Anforderungen für Hersteller von Komponenten*.
Bundesamt für Sicherheit in der Informationstechnik (2016a), *Ein Praxis-Leitfaden für IS-Penetrationstests*.
Bundesamt für Sicherheit in der Informationstechnik (2016b), *Industrial Control System Security: Top 10 Bedrohungen und Gegenmaßnahmen 2016 – Empfehlung: IT in der Produktion – BSI-Veröffentlichungen zur Cyber-Sicherheit BSI-CS 005*.
Bundesamt für Sicherheit in der Informationstechnik (2016c), *IT-Grundschutz-Kataloge: 15. Ergänzungslieferung*.
Department of Homeland Security, I. C. S. C. E. R. T. (2016), *Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies*.
Europäische Kommission (2004), *Schutz kritischer Infrastrukturen im Rahmen der Terrorismusbekämpfung, Mitteilung der Kommission an den Rat und das Europäische Parlament, KOM(2004) 702 endgültig*.
IEC/ISA 62443-1-1:2007 (2007), *Security for Industrial Automation and Control Systems – Part 1: Terminology, Concepts, and Models*.
IEC/ISA 62443:2013 (2015), *Industrielle Kommunikationsnetze – IT-Sicherheit für Netze und Systeme*.
IEC/ISA 62443-2-1:2015 (2015), *Security for industrial automation and control systems – Part 2-1: Industrial automation and control system security management system, Draft 7, Edit 5 November 9, 2015*.
IEC/ISA 62443-2-4:2013 (2013), *Security for industrial automation and control systems – Network and system security – Part 2-4: Security program requirements for IACS service providers*.

IEC/ISA 62443-3-3:2013 + Cor.:2014 (2015), *Industrielle Kommunikationsnetze – IT-Sicherheit für Netze und Systeme – Teil 3-3: Systemanforderungen zur IT-Sicherheit und Security-Level*.

IEC/ISO 62264:2008 (2008), *Enterprise-control system integration*.

ISO/IEC 27000:2016(E) (2016), *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

ISO/IEC 27005:2008 (2008), *Information technology – Security techniques – Information security risk management*.

IT-Sicherheitsgesetz (2015), *Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme vom 17. Juli 2015 (BGBl. I S. 1324), das zuletzt durch Artikel 5 Absatz 8 des Gesetzes vom 18. Juli 2016 (BGBl. I S. 1666) geändert worden ist*.

Merkblatt DWA-M 1100 (2008), *Benchmarking in der Wasserversorgung und Abwasserbeseitigung*.

National Institute of Standards and Technology (2007), *NIST Special Publication 800-94: Guide to Intrusion Detection and Prevention Systems (IDPS) – Recommendations of the National Institute of Standards and Technology*.

National Institute of Standards and Technology (2008), *NIST Special Publication 800-115: Technical Guide to Information Security Testing and Assessment – Recommendations of the National Institute of Standards and Technology*.

National Institute of Standards and Technology (2015), *NIST Special Publication 800-82, Revision 2: Guide to industrial control systems (ICS) security – supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as programmable logic controllers (PLC)*.

Siemens (2008), *SIMATIC Sicherheitskonzept: PCS 7 und WinCC – Basisdokument – Whitepaper*.

TrinkwV (2017), *Trinkwasserverordnung in der Fassung der Bekanntmachung vom 10. März 2016 (BGBl. I S. 459), die zuletzt durch Artikel 2 des Gesetzes vom 17. Juli 2017 (BGBl. I S. 2615) geändert worden ist*.

Verein Deutscher Ingenieure (1993), *VDI-Richtlinie 3633, BI. 1: Simulation und Logistik-, Materialfluß- und Produktionssystemen, Beuth*.

Anlage

A.1 Aufbau einer idealtypischen und zonierten DCS-Kleinanlage

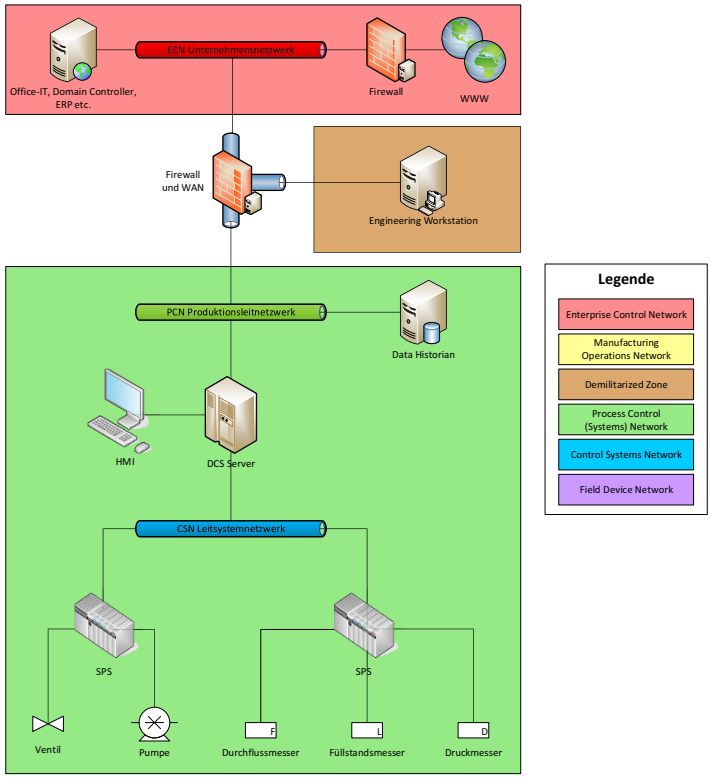

Abb. 17: Aufbau einer idealtypischen und zonierten DCS-Kleinanlage

O. Leps, *Hybride Testumgebungen für Kritische Infrastrukturen*,
https://doi.org/10.1007/978-3-658-22614-5_7

A.2 Aufbau einer idealtypischen und zonierten SCADA-Kleinanlage

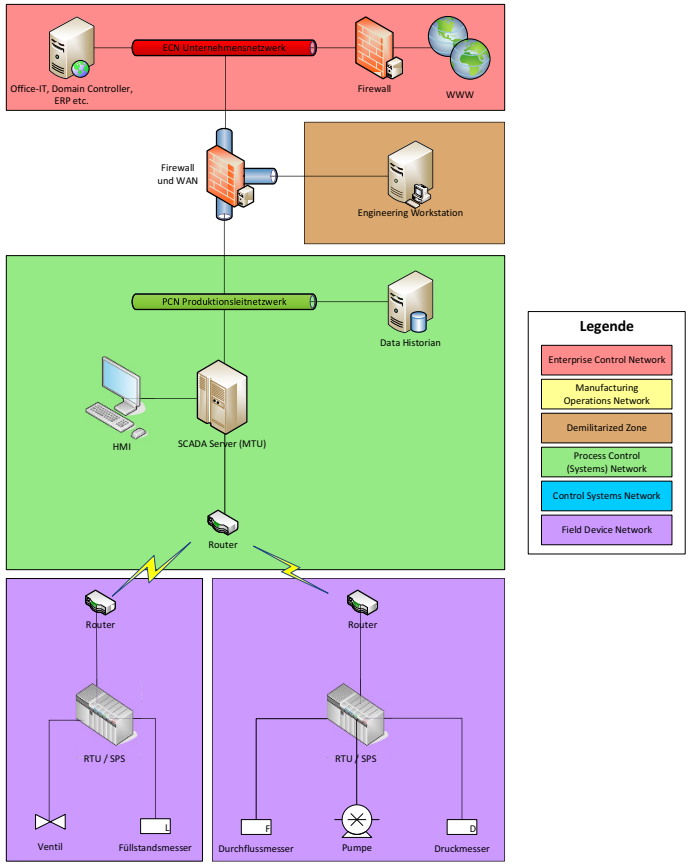

Abb. 18: Aufbau einer idealtypischen und zonierten SCADA-Kleinanlage

A.3 Aufbau einer idealtypisch verschachtelten und zonierten SCADA-Anlage

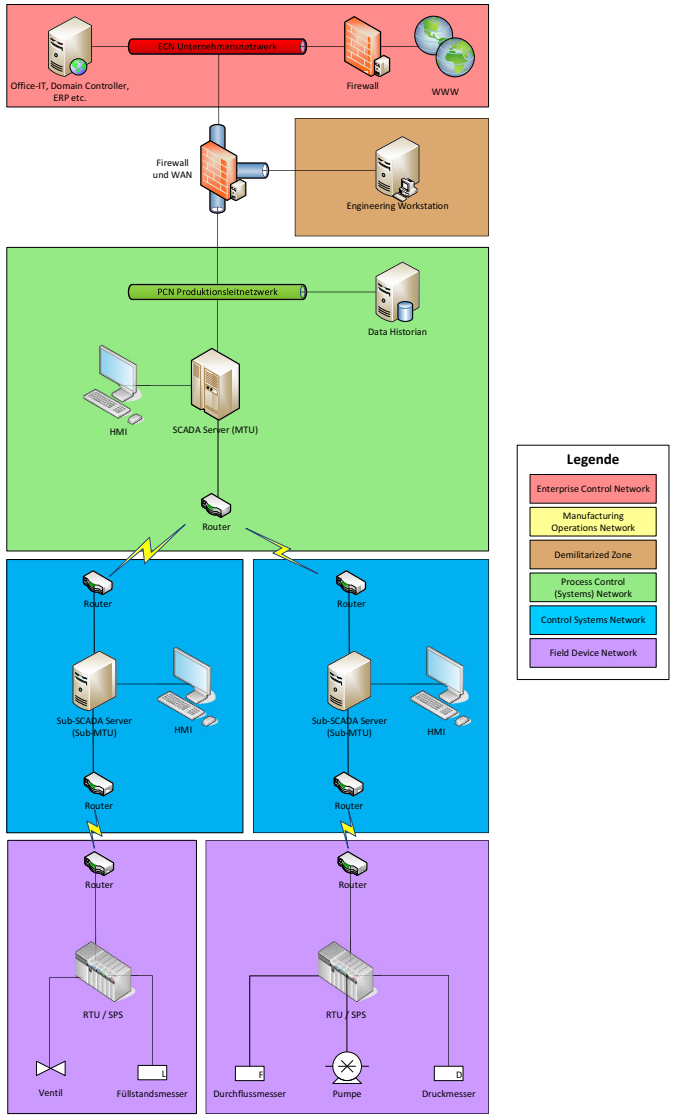

Abb. 19: Aufbau einer idealtypisch verschachtelten und zonierten SCADA-Anlage