Schlusswort

Die Bewertungsmethode wurde mit der Idee entwickelt, nicht nur Risiken aufzuzeigen, sondern durch die hohe Transparenz und Verknüpfung zu potenziellen Maßnahmen, dabei zu unterstützen, die Risiken durch die Vernetzung in der Produktion nachhaltig zu minimieren und im Idealfall zu eliminieren. Voraussetzung für die Ergreifung von Maßnahmen ist, dass die Risiken für verschiedene Adressatenkreise – im Besonderen für die Entscheidungsträger – transparent gemacht werden. So war es das primäre Ziel der Arbeit, eine Bewertungsmethode zu kreieren, die technische und operative IT-Risiken aufzeigt und diese in Hinblick auf die unternehmerischen Ziele bewertet. Rechtliche Anforderungen an die Methode hinsichtlich der Aussage ‚Fähigkeit über den Zustand der EDV-Systeme' mussten dabei genauso berücksichtigt werden, wie eine gute Anwendbarkeit in der Praxis. Entstanden ist die VIP-Bewertungsmethode, der die Automatisierungspyramide als mehrstufiges Modell zugrunde liegt, um die vielen Facetten der Risiken in der Produktion exakt bewerten zu können. Die Bewertung der einzelnen Automatisierungsebenen erfolgt stets nach demselben Schema und greift dabei auf die bereits etablierten und für die Praxis hochrelevanten Bewertungsmethoden der IT-Grundschutz-Kataloge zurück. Der dahinter liegende Gedanke war es, eine Bewertungsmethode zu schaffen, die von der Praxisrelevanz der zugrundeliegenden Methoden und deren Reifegrade profitiert, letztlich also selbst eine hohe Ausgereiftheit vorweist. Die Notwendigkeit, eine ausgereifte Bewertungsmethode zu entwickeln, die eine durchgängige Bewertung ermöglicht, kommt daher, dass insbesondere der letzte Punkt ein großes Manko der in der Theorie beschriebenen Modelle ist. Das größte Problem, das sich in der Theorie ergibt, ist die mangelnde Durchgängigkeit der Risikobewertung. Rechtlich verbindlich und konkret beschrieben ist hauptsächlich die Bewertung der finanziellen Risiken, wie sie im Finanz- und Bankensektor vorkommen. Die Regulierung ist für diesen Sektor sehr greifbar und beschreibt eindeutig, bis zu und ab welcher Summe finanzielle Risiken zu bewerten sind. Im Zusammenhang mit diesen Regelungen wird auch darauf eingegangen, dass EDV-Systeme bzw. IT-Risiken zu bewerten sind. Die zuvor beschriebene

G. Schlingermann, *IT-Risiken in der vernetzten Produktion*,
DOI 10.1007/978-3-658-18346-2

Greifbarkeit der Regelungen ist für die IT-Risikobewertung hingegen nicht gegeben. Das verschärft das grundlegende Problem, dass durch die unkonkreten Regelungen es jedem Unternehmen freisteht, die IT-Risiken anders zu bewerten. Und das stellt letztendlich ein Problem für die Stake- und Shareholder dar, denen bei diesen Regelungen die einzelnen Bewertungen nicht transparent ersichtlich sind. Bei produzierenden Betrieben kommt die Komplexität des Produktionsprozesses hinzu. Nahezu alle Produktionsprozesse werden heutzutage von IT-Systemen gestützt oder gesteuert. Das bedingt eine komplexe prozessuale und auch technische Vernetzung in der Produktion. Genau diese Komplexität muss durch eine geeignete Bewertungsmethode reduziert werden, um eine durchgängige und transparente IT-Risikobewertung zu ermöglichen. Aus Sicht des Autors ist dies mit der VIP-Bewertungsmethode gegeben. Es wurden die wesentlichen, in der Theorie beschriebenen Probleme ausgiebig betrachtet und erkannt, dass sie für die entwickelte VIP-Bewertungsmethode nicht zutreffen. Es schließt sich die Frage an, welche wesentlichen Probleme in der Praxis entstehen können. Das größte zu erwartende Problem ist vermutlich organisatorischer Natur. Die treibende Idee hinter der VIP-Bewertungsmethode ist es, die IT-Risiken einzelner Anlagen-PCs und Systeme über alle Automatisierungsebenen hinweg zu aggregieren und schlussendlich das gesamte Informations- und IT-Risiko der Produktion aufzuzeigen. Es ist davon auszugehen, dass gerade in größeren Unternehmen klare organisatorische Trennungen zwischen IT-Risikomanagement und dem unternehmensweiten Risikomanagement bestehen. Genau hier kann ein wesentliches Problem liegen. Eine durchgängige Betrachtung setzt voraus, dass es möglich ist, eine ganzheitliche Betrachtung durchzuführen und dass die Ergebnisse von allen Seiten akzeptiert werden. Der letzte Punkt ist absolut essenziell. Neben den organisatorischen Herausforderungen gilt es, auch die quantitativen und qualitativen Herausforderungen zu bewältigen. Um ein aussagekräftiges Ergebnis zu bekommen, müssen alle IT-Systeme und Anlagen bewertet werden. Neben der Fehleranfälligkeit bei einer manuellen Erhebung wäre auch der enorme zeitliche Aufwand als Problem zu sehen. Ebenfalls ist es wichtig, dass der Betrachtungszeitraum relativ klein ist,

da gerade im IT-Bereich häufig neue IT-Risiken auftreten, die dann ebenfalls bewertet werden müssten. Aus den genannten Gründen ist es notwendig, dass die Erfassung bzw. Bewertung der IT-Risiken technisch unterstützt wird. Hierbei kann es zu ungenauen Auswertungen kommen, wenn im Vorfeld nicht detailliert festgelegt wird, welche Parameter ausgelesen und welche Systemereignisse wie bewertet werden. Analog zu anderen technisch unterstützten Erhebungen muss im Vorfeld analysiert werden, wie die Erhebung manuell, stichprobenartig überprüft werden kann. Zusammengefasst wird das in der Praxis hauptsächlich bestehende Problem darin liegen, dass die Bewertungsmethode die Komplexität der IT-Risikobewertung zwar reduziert, dass IT-Umfeld als solches aber nicht weniger komplex macht.

Abschließend stellt sich die Frage, wie man Theorie und Praxis sinnvoll zusammenführen kann. Im Zusammenhang mit der Einführung eines Managementsystems für Informationssicherheit wurde der PDCA-Zyklus samt seiner vier Phasen Plan, Do, Check und Act ausführlich diskutiert. Daraus ließ sich folgern, dass Theorie und Praxis dann sinnvoll zusammengeführt werden können, wenn die vier Phasen des PDCA-Zyklus berücksichtigt werden. Bei der Entwicklung einer Bewertungsmethode für das IT-Risikomanagement zur Bewertung der Risiken durch die Vernetzung in der Produktion wurden verschiedene Modelle zur Diskussion gestellt und Probleme, die sich in der Theorie ergeben, analysiert, um schließlich als Ergebnis der gesammelten Erkenntnisse die VIP-Bewertungsmethode hervorzubringen. Im Anschluss an die abgeschlossene Planungs- und Konzeptionsphase gilt es nun, die entwickelte Methode in der Praxis anzuwenden. Es ist wünschenswert, dass sich die Methode als praxistauglich erweist. Das bedeutet v. a., dass die IT-Risikobewertungen sich als transparent und aussagefähig erweisen. Ob dies zutrifft, kann nur durch die Interaktion sowohl mit den für die Risikobewertung zuständigen Abteilungen erfolgen als auch mit den Shareholdern, die abschließend bewerten müssen, ob die IT-Risiken für sie transparenter geworden sind. Gemäß des PDCA-Zyklus gilt es daher, eine Erfolgskontrolle durchzuführen, um als abschließenden Schritt die Optimierung und Verbesserung der VIP-Bewertungsme-

thode zu bewirken. Es lässt sich resümieren, dass das Ziel der Arbeit, eine praxistaugliche Bewertungsmethode zu schaffen, in dem Moment erreicht ist, in dem die VIP-Bewertungsmethode in der Praxis zur Anwendung kommt und durch das stetige Durchlaufen des PDCA-Zyklus die Interaktion zwischen Theorie und Praxis fordert.

Literaturverzeichnis

absatzwirtschaft.de. (2013). Was die Autobauer pro Fahrzeug verdienen: Profitabilität in der Automobilindustrie. Abgerufen am 05.12.2015 von http://www.uni-due.de/~hk0378/publikationen/2013/Absatzwirtschaft-21%2011%202013.pdf

Abts, D., & Mülder, W. (2009). *Grundkurs Wirtschaftsinformatik* (6., überarb. und erw. Aufl.). Wiesbaden: Vieweg + Teubner.

Audi AG. (2014). *Geschäftsbericht 2013*. (Audi AG, Hrsg.) Abgerufen am 05.12.2015 von http://www.audi.com/content/dam/com/DE/investor-relations/financial_reports/annual-reports/audi_gb_2013_de.pdf

Audi AG. (2015). *Geschäftsbericht 2014*. (Audi AG, Hrsg.) Abgerufen am 30.11.2015 von http://www.audi.com/content/dam/com/DE/investor-relations/financial_reports/annual-reports/audi_gb_2014_de.pdf

Bartsch, M. (2013). Service Level Agreements – rechtliche Aspekte. *Informatik-Spektrum, 36*(5), 449–454.

Bauernhansl, T. (2014). Die Vierte Industrielle Revolution. Der Weg in ein wertschaffendes Produktionsparadigma. In T. Bauernhansl, M. ten Hompel & B. Vogel-Heuser (Hrsg.), *Industrie 4.0 in Produktion, Automatisierung und Logistik. Anwendung, Technologien und Migration* (S. 5–35). Wiesbaden: Springer Vieweg.

Bauernhansl, T., Hompel, M. ten & Vogel-Heuser, B. (Hrsg.). (2014). *Industrie 4.0 in Produktion, Automatisierung und Logistik. Anwendung, Technologien und Migration*. Wiesbaden: Springer Vieweg.

Bayer AG. (2015). *Geschäftsbericht 2014*. (Bayer AG, Hrsg.) Abgerufen am 30.11.2015 von http://www.geschaeftsbericht2014.bayer.de/de/bayer-geschaeftsbericht-2014.pdfx?forced=true

Bayrische Motoren Werke AG. (2014). *Geschäftsbericht 2013*. (Bayrische Motoren Werke AG, Hrsg.) Abgerufen am 05.12.2015 von https://www.bmwgroup.com/content/dam/bmw-group-websites/ bmwgroup_com/ir/downloads/de/2013/geschaeftsbericht2013.pdf

G. Schlingermann, *IT-Risiken in der vernetzten Produktion*,
DOI 10.1007/978-3-658-18346-2

Bayrische Motoren Werke AG. (2015). *Geschäftsbericht 2014*. (Bayrische Motoren Werke AG, Hrsg.) Abgerufen am 30.11.2015 von http://geschaeftsbericht2014.bmwgroup.com/bmwgroup/annual/2014/gb/German/pdf/bericht2014.pdf

Brünger, C. (2009). *Erfolgreiches Risikomanagement mit COSO ERM Empfehlungen für die Gestaltung und Umsetzung in der Praxis.* Berlin: Erich Schmidt Verlag.

Bundesamt für Sicherheit in der Informationstechnik. (2008). *Anerkennung der ISO 27001-Zertifizierung*. (Bundesamt für Sicherheit in der Informationstechnik, Hrsg.) Abgerufen am 15.02.2014 von https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzZertifikat/ISO27001Zertifizierung/Anerkennung/anerkennung_27001.html

Bundesamt für Sicherheit in der Informationstechnik. (2008). *BSI-Standard 100-1*. (Bundesamt für Sicherheit in der Informationstechnik, Hrsg.) Abgerufen am 06.06.2014 von https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1001_pdf.pdf?__blob=publicationFile

Bundesamt für Sicherheit in der Informationstechnik. (2008). *BSI-Standard 100-2*. (Bundesamt für Sicherheit in der Informationstechnik, Hrsg.) Abgerufen am 06.06.2014 von https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1002_pdf.pdf?__blob=publicationFile

Bundesamt für Sicherheit in der Informationstechnik. (2008). *BSI-Standard 100-3*. (Bundesamt für Sicherheit in der Informationstechnik, Hrsg.) Abgerufen am 06.06.2014 von https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1003_pdf.pdf?__blob=publicationFile

Bundesamt für Sicherheit in der Informationstechnik. (2008). *BSI-Standard 100-4*. (Bundesamt für Sicherheit in der Informationstechnik, Hrsg.) Abgerufen am 06.06.2014 von https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1004_pdf.pdf?__blob=publicationFile

Bundesamt für Sicherheit in der Informationstechnik. (2013). *IT-Grundschutz-Kataloge*. (Bundesamt für Sicherheit in der Informationstechnik, Hrsg.) Abgerufen am 06.06.2014 von https://gsb.download.bva.bund.de/BSI/ITGSK/IT-Grundschutz-Kataloge_2013_EL13_DE.pdf

Bundesamt für Sicherheit in der Informationstechnik. (2014). *ISO 27001 Zertifizierung auf Basis von IT-Grundschutz*. (Bundesamt für Sicherheit in der Informationstechnik, Hrsg.) Abgerufen am 12.09.2014 von https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzZertifikat/itgrundschutzzertifikat_node.html

Bundesamt für Sicherheit in der Informationstechnik. (2014). *Kreuzreferenztabellen der IT-Grundschutz-Kataloge*. (Bundesamt für Sicherheit in der Informationstechnik, Hrsg.) Abgerufen am 20.11.2015 von https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Check/kreuzreferenz_tabellen_zip.zip?__blob=publicationFile&v=1

Bundesamt für Sicherheit in der Informationstechnik. (25.04.2014). *Welche Gefahren begegnen mir im Netz?* (Bundesamt für Sicherheit in der Informationstechnik, Hrsg.) Abgerufen am 25.04.2014 von https://www.bsi-fuer-buerger.de/BSIFB/DE/GefahrenImNetz/gefahren_node.html

CCN. (26.09.2007). *Sources: Staged cyber attack reveals vulnerability in power grid*. (CCN, Hrsg.) Abgerufen am 23.05.2015 von http://edition.cnn.com/2007/US/09/26/power.at.risk/index.html?_s=PM:US#cnnSTCVideo

Chair of Statistics, University of Würzburg. (01.08.2012). *Lehrstuhl für Mathematik VIII - Statistik*. (University of Würzburg, Chair of Statistics, Hrsg.) Abgerufen am 24.04.2015 von http://www.statistik-mathematik.uni-wuerzburg.de/fileadmin/10040800/user_upload/time_series/the_book/2012-August-01-times.pdf

Chalmers, A. F. (2013). *Wege der Wissenschaft* (6. Aufl.). Berlin: Springer Verlag.

Claus, T., Herrmann, F., & Manitz, M. (Hrsg.) (2015). *Produktionsplanung und -steuerung.* Berlin: Springer-Verlag.

Daimler AG. (2014). *Geschäftsbericht 2013*. (Daimler AG, Hrsg.) Abgerufen am 05.12.2015 von https://www.daimler.com/dokumente/investoren/berichte/geschaeftsberichte/daimler/daimler-ir-geschaeftsbericht-2013.pdf

Daimler AG. (2015). *Geschäftsbericht 2014*. (Daimler AG , Hrsg.) Abgerufen am 30.11.2015 von http://www.daimler.com/Projects/c2c/channel/documents/2590211_Daimler_FY_2014_Geschaeftsbericht.pdf

DaimlerChrysler AG. (2006). *Geschäftsbericht 2005*. (DaimlerChrysler AG, Hrsg.) Abgerufen am 10.04.2013 von http://www.daimler.com/Projects/c2c/channel/documents/829809_DCX_2005_Gesch__ftsbericht.pdf

DaimlerChrysler AG. (2007). *Geschäftsbericht 2006*. (DaimlerChrysler AG, Hrsg.) Abgerufen am 10.04.2013 von http://www.daimler.com/Projects/c2c/channel/documents/1003904_DCX_2006_Gesch__ftsbericht.pdf

Deutsches Rechnungslegungs Standards Committee. (14.09.2012). *Deutscher Rechnungslegungs Standard Nr. 20*. (D. R. Committee, Hrsg.) Abgerufen am 30.10.2015 von http://www.drsc.de/docs/press_releases/2012/120928_DRS20_nearfinal.pdf

Dörner, D., & Doleczik, G. (2000). Corporate Governance. In D. Dörner, P. Horváth, & H. Kagermann (Hrsg.), *Praxis des Risikomanagement* (S. 193–224). Stuttgart: Schäffer-Poeschel Verlag.

Dörner, D., Horváth, P., & Kagermann, H. (Hrsg.) (2000). *Praxis des Risikomanagement.* Stuttgart: Schäffer-Poeschel Verlag.

Eller, R., Heinrich, M., Perrot, R., & Reif, M. (Hrsg.) (2010). *Kompaktwissen Risikomanagement.* Wiesbaden: Gabler Verlag.

Europäische Union. (1993). *Verordnung (EWG) Nr. 1836/93 des Rates vom 29. Juni 1993 über die freiwillige Beteiligung gewerblicher Unternehmen an einem Gemeinschaftssystem für das Umweltmanagement und die Umweltbetriebsprüfung*. (E. Union, Hrsg.) Abgerufen am 06.12.2013 von http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1993:168:0001:0018:DE:PDF

Fallenbeck, N. D., & Eckert, C. P. (2014). IT-Sicherheit und Cloud Computing. In T. Bauernhansl, M. ten Hompel & B. Vogel-Heuser (Hrsg.), *Industrie 4.0 in Produktion, Automatisierung und Logistik* (S. 398–430). Wiesbaden: Springer Vieweg.

Franz, K.-P. (2000). Corporate Governance. In D. Dörner, P. Horváth, & H. Kagermann (Hrsg.), *Praxis des Risikomanagement* (S. 41–72). Stuttgart: Schäffer-Poeschel Verlag.

Funk, W., & Rossmanith, J. (Hrsg.) (2008). *Internationale Rechnungslegung und Internationales Controlling*. Wiesbaden: GWV Fachverlage.

Gleißner, W. (2001). Quantitative Verfahren im Risikomanagement: Risikoaggregation, Risikomaße und Performancemaße. In A. Klein (Hrsg.), *Risikomanagement und Risiko-Controlling* (S. 179–204). Freiburg: Haufe Verlag.

Graf von Brühl, R. (2011). *Interdependenzen von Ökologie und Betriebswirtschaftslehre.* Frankfurt am Main: R. G. Fischer Verlag.

Grünendahl, R.-T., Steinbacher, A. F., & Will, P. H. (2009). *Das IT-Gesetz: Compliance in der IT-Sicherheit.* Wiesbaden: Vieweg + Teubner.

Handelsblatt. (09.01.2015). *Daimler kommt näher*. (Handelsblatt, Hrsg.) Abgerufen am 30.11.2015 von http://www.handelsblatt.com/unternehmen/industrie/abstand-zu-bmw-und-audi-daimler-kommt-naeher/11206322.html

Heinrich, B., Linke, P., & Glöckler, M. (2015). *Grundlagen Automatisierung.* Wiesbaden: Springer Vieweg.

heise. (20.03.2013). *Wurm im Werk*. (H. Z. KG, Hrsg.) Abgerufen am 12.04.2013 von http://www.heise.de/tr/artikel/Wurm-im-Werk-1818812.html

heise. (31.12.2014). *31C3: Wie man ein Chemiewerk hackt*. (H. Z. KG, Hrsg.) Abgerufen am 22.05.2015 von http://www.heise.de/newsticker/meldung/31C3-Wie-man-ein-Chemiewerk-hackt-2507259.html

Heitmann, M. (2007). *IT-Sicherheit in vertikalen F&E-Kooperationen der Automobilindustrie.* Wiesbaden: GWV Fachverlage.

Henkel, K., Kühne, J., Storch, D., & Waitz, D. (2010) MaRisk: Mindestanforderungen an das Risikomanagement in Kreditinstituten. In R. Eller, M. Heinrich, R. Perrot, & M. Reif (Hrsg.), *Kompaktwissen Risikomanagement* (S. 13–26). Wiesbaden: Gabler Verlag.

Internationale Organisation für Normung. (1996). *ISO 14001:1996 Environmental management.*

Internationale Organisation für Normung. (2009). *ISO 31000:2009 Risk management – Principles and guidelines.*

Internationale Organisation für Normung. (2012). *ISO 27005:2010 Information technology – Security techniques – Information security management systems – Overview and vocabulary.*

Iteem school. (31.08.2012). *International – Internship – Iteem – #interteem*. Abgerufen am 08.05.2015 von http://international.iteem.ec-lille.fr/wp-content/uploads/2012/07/AssemblyCarPlantProcess-1024x386.png

Kiefer, J. (2007). *Mechatronikorientierte Planung automatisierter Fertigungszellen im Bereich Karosserierohbau.* Saarbrücken: Universität des Saarlandes.

Klein, A. (Hrsg.) (2011). *Risikomanagement und Risiko-Controlling.* Freiburg: Haufe Verlag.

Klipper, S. (2011). *Information Security Risk Management.* Wiesbaden: Vieweg + Teubner Verlag.

Klug, F. (2010). *Logistikmanagement in der Automobilindustrie* (3. Aufl.). Heidelberg: Springer Verlag.

Köhler, P. T. (2007). *ITIL* (2. Aufl.). Berlin: Springer-Verlag.

Königs, H.-P. (2013). *IT-Risikomanagement mit System.* Wiesbaden: Springer Vieweg.

Kramer, A., & Ekkenga, J. (2001). Compliance-Risikoanalyse: Nutzen, Umsetzung, und Integrationin das RM System. In A. Klein (Hrsg.), *Risikomanagement und Risiko-Controlling* (S. 113–134). Freiburg: Haufe Verlag.

Kropik, M. (2009). *Produktionsleitsysteme in der Automobilfertigung.* Berlin: Springer-Verlag.

Kühnapfel, J. B. (2014). *Nutzwertanalysen in Marketing und Vertrieb.* Wiesbaden: Springer Gabler.

Lück, W. (2000). Managementrisiken. In D. Dörner, P. Horváth, & H. Kagermann (Hrsg.), *Praxis des Risikomanagement* (S. 311–344). Stuttgart: Schäffer-Poeschel Verlag.

März, L. (2015). Dynamische Austaktung in sequenzierten Produktionslinien der Automobilindustrie. In T. Claus, F. Herrmann, & M. Manitz (Hrsg.), *Produktionsplanung- und steuerung* (S. 241–255). Berlin: Springer-Verlag.

Müller, K.-R. (2014). *IT-Sicherheit mit System* (6. Aufl.). Wiesbaden: Springer Vieweg.

Ossadnik, W., & Langer, O. (2008). Risikomanagement internation agierender Unternehmen. In W. Funk, & J. Rossmanith (Hrsg.), *Internationale Rechnungslegung und Internationales Controlling* (S. 319–342). Wiesbaden: GWV Fachverlage.

Paulus, S. (2000). Risiken beim Einsatz von Informationstechnologie. In D. Dörner, P. Horváth, & H. Kagermann (Hrsg.), *Praxis des Risikomanagement* (S. 379–414). Stuttgart: Schäffer-Poeschel Verlag.

Popper, K. (2007). *Logik der Forschung.* Berlin: Akademie Verlag.

Prokein, O. (2008). *Markt- und Unternehmensentwicklung*. Wiesbaden: GWV Fachverlage.

Rieger, F. (2015). Jeder ist angreifbar. *Der Spiegel* (39/2015), S. 68–69.

Schäl, I. (2011). *Management von operationellen Risiken*. Wiesbaden: Gabler Verlag.

Scharpf, P. (2000). Finanzrisiken. In D. Dörner, P. Horváth, & H. Kagermann (Hrsg.), *Praxis des Risikomanagement* (S. 253–282). Stuttgart: Schäffer-Poeschel Verlag.

Schneck, O. (2001). Compliance-Risikoanalyse: Nutzen, Umsetzung, und Integration in das RM System. In A. Klein (Hrsg.), *Risikomanagement und Risiko-Controlling* (S. 87–110). Freiburg: Haufe Verlag.

SecuMedia Verlags-GmbH. (2012). Lagebericht zur Informationssicherheit. *<kes> Die Zeitschrift für Informations-Sicherheit* (Sonderdruck).

Strohmeier, G. (2007). *Ganzheitliches Risikomanagement in Industriebetrieben*. Wiesbaden: GWV Fachverlage GmbH.

Swales, J. (1990). *Genre Analysis: English in Academic and Research Settings (Cambridge Applied Linguistics).* Cambridge: Cambridge University Press.

Thies, K. H. (2008). *Management operationaler IT- und Prozess-Risiken.* Heidelberg: Springer Verlag.

Töpfer, A., & Heymann, A. (2000). Marktrisiken. In D. Dörner, P. Horváth, & H. Kagermann (Hrsg.), *Praxis des Risikomanagement* (S. 225–252). Stuttgart: Schäffer-Poeschel Verlag.

Verbund Deutscher Ingenieure. (07.12.2012). *Industrie-4.0-Konzepte rütteln an der Automatisierungspyramide*. (Verbund Deutscher Ingenieure, Hrsg.) Abgerufen am 15.01.2013 von http://www.vdi-nachrichten.com/Technik-Wirtschaft/Industrie-40-Konzepte-ruetteln-an-Automatisierungspyramide

Witt, B. C. (2006). *IT-Sicherheit kompakt und verständlich*. Wiesbaden: GWV Fachverlage GmbH.

Wöhe, G. (2010). *Einführung in die Allgemeine Betriebswirschaftslehre* (24. Aufl.). München: Verlag Franz Vahlen GmbH.

Anhang

Tabelle 22: Zuordnung IT-Grundschutz-Risiken ausgewählter Bausteine zu IT-Risiken[225]

		Verfügbarkeit	Vertraulichkeit	Integrität	B 3.101 Allgemeiner Server	B 3.201 Allgemeiner Client	B 3.202 Allgemeines nicht vernetztes IT-System	B 3.405 Smartphones, Tablets und PDAs	B 3.406 Drucker, Kopierer und Multifunktionsgeräte	B 5.21 Webanwendungen	B 5.25 Allgemeine Anwendungen	B 4.1 Heterogene Netze	B 4.6 WLAN
G 3.1	Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten		x						x		x		
G 3.2	Fahrlässige Zerstörung von Gerät oder Daten	x									x		
G 3.5	Unbeabsichtigte Leitungsbeschädigung	x										x	
G 3.86	Ungeregelte und sorglose Nutzung von Druckern, Kopierern und Multifunktionsgeräten	x							x				

[225] Eigene Darstellung

G. Schlingermann, *IT-Risiken in der vernetzten Produktion*,
DOI 10.1007/978-3-658-18346-2

G 4.1	Ausfall der Stromver-sorgung	x			x		x					x	
G 4.13	Verlust ge-speicherter Daten	x			x	x					x		
G 4.31	Ausfall oder Störung von Netz-komponenten	x										x	
G 4.42	Ausfall des Mobiltelefons, Smartphones, Tablets oder PDAs	x						x					
G 4.7	Defekte Datenträger	x					x						
G 4.84	Unzureichende Validierung von Ein- und Aus-gabedaten bei Webanwendung en und Web-Services			x						x			
G 4.87	Offenlegung vertraulicher Informationen bei Web-anwendungen und Web-Services		x							x			
G 5.1	Manipulation oder Zerstörung von Geräten oder Zubehör	x	x	x	x	x	x	x	x			x	
G 5.125	Datendiebstahl mithilfe mobiler Endgeräte		x					x					

G 5.138	Angriffe auf WLAN-Komponenten	x	x	x									x
G 5.139	Abhören der WLAN-Kommunikation		x										x
G 5.165	Unberechtigter Zugriff auf oder Manipulation von Daten bei Webanwendungen und Web-Services		x	x						x			
G 5.2	Manipulation an Informationen oder Software	x	x	x	x	x	x	x	x		x	x	
G 5.7	Abhören von Leitungen		x			x						x	
G 5.71	Vertraulichkeitsverlust schützenswerter Informationen		x		x	x			x				x
G 5.85	Integritätsverlust schützenswerter Informationen			x	x	x							