Weiterentwicklung sicherheitstechnischer Analyse- und Bewertungsmethoden für die Industrie 4.0
Development of safety related security methods in the field of Industry 4.0

Dipl.-Ing. Björn Kasper
Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (BAuA), Dresden, kasper.bjoern@baua.bund.de

Kurzfassung

Die Konzepte von Industrie 4.0 sehen vor, dass die Produktion auf Kundenanforderungen in weit größerem Maße individuell und flexibel reagieren kann. Dies hat zur Folge, dass sich technische Produktionsanlagen selbsttätig und auftragsbezogen konfigurieren müssen, um eine Individualisierung des Produktes umsetzen zu können. Allerdings gehen heutige sicherheitstechnische Konzepte in der Konstruktions- und Designphase von definierten Anlagen aus, in denen zwar variable aber vorab klar definierte Prozesse ablaufen. Die sicherheitstechnischen Beurteilungsmethoden legen die Annahme zugrunde, dass die Maschine oder Anlage nach der Inbetriebnahme und der sicherheitstechnischen Abnahme nicht mehr verändert wird, ohne dass eine erneute sicherheitstechnische Überprüfung erfolgt. Sich selbst konfigurierende Anlagen der Industrie 4.0 würden diese Voraussetzungen verletzen. Der folgende Beitrag stellt Ansätze vor, wie heute verfügbare sicherheitstechnische Analyse- und Bewertungsmethoden weiterentwickelt werden können. Dies erfolgt mit dem Ziel, dass jede konkrete Betriebsfunktion einer Maschine oder Anlage nach deren auftragsbezogener Rekombination mit der jeweils geforderten Sicherheitsstufe zur Laufzeit abgeglichen (validiert) werden kann. Es wird diskutiert, wie sich das heutige Sicherheitsniveau für die Beschäftigten auch im Kontext von Industrie 4.0 aufrechterhalten oder weiter verbessern lässt.

Abstract

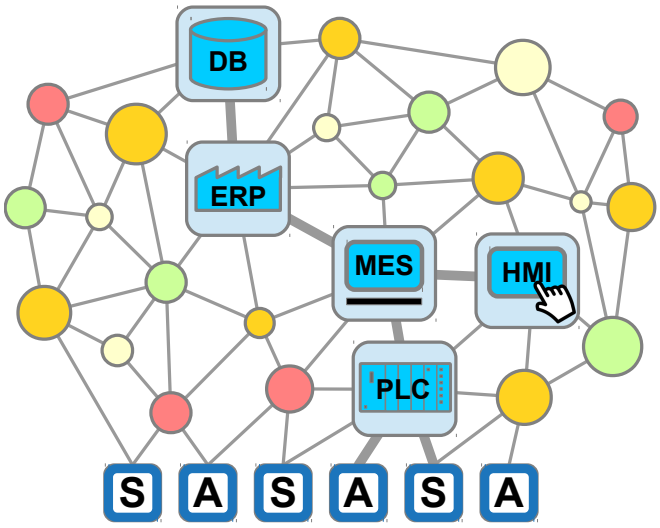
The concepts of industry 4.0 provide that the industrial production will be able to react much more individually and more flexibly to customer requirements when compared to the current state. This means that technical production facilities must be able to configure themselves automatically and order-related to realize an individualization of the product. Currently, the engineering and design phases of safety and industrial security concepts are based on automation systems with clearly pre-defined processes, although these processes may run dynamically. The safety and security assessment methods are based on the assumption that the machinery or automation system remains unchanged after commissioning and the safety/security approval, without requiring a renewal of safety/security inspection. Self-configuring automation systems as envisioned for industry 4.0 would violate these requirements. The following article presents approaches for the further development of safety/security analysis and assessment methods available today. With the help of this it will be possible to align (validate) every specific operating function of the machinery or automation system after order-related recombination with the required safety/security level at runtime. It is discussed how the current safety/security level for employees can be maintained or further improved in the context of industry 4.0.

1 Flexible Automatisierungsstrukturen der Industrie 4.0

Die Konzepte von Industrie 4.0 sehen vor, dass die Produktion auf Kundenanforderungen in weit größerem Maße individuell und flexibel reagieren kann. Dies hat zur Folge, dass sich technische Produktionsanlagen selbsttätig und auftragsbezogen konfigurieren müssen, um eine Individualisierung des Produktes umsetzen zu können. Damit gehen auch ein deutlich höherer Vernetzungsgrad der Maschinen- und Anlagen-Komponenten sowie eine auftragsbezogene Ankopplung an das Internet einher.

Wesentliche Elemente der Industrie 4.0 sind sog. Cyber-Physische Systeme (CPS). Diese umfassen eingebettete Systeme, Produktions-, Logistik-, Engineering-, Koordinations- und Managementprozesse sowie Internetdienste, die mittels Sensoren unmittelbar physikalische Daten erfassen und mittels Aktoren auf physikalische Vorgänge einwirken. Mit Hilfe offener, teilweise globaler und jederzeit miteinander verbundener Informationsnetze kommunizieren sie untereinander, nutzen weltweit verfügbare Daten und Dienste und realisieren multimodale Mensch-Maschine-Schnittstellen (vgl. [8, 15, 1, 9]).

Insbesondere im Kontext von Industrie 4.0 geht es um die Anwendung von CPS in der produzierenden Industrie, diese werden daher als Cyber-Physische Produktions-Systeme (CPPS) bezeichnet. In CPPS werden Daten, Dienste und Funktionen dort gehalten, abgerufen und ausgeführt, wo es im Sinne einer flexiblen, effizienten Entwicklung (inklusive Entwurf und Engineering) und Produktion den größten



Legende:
A / S … intelligenter Aktor / Sensor
PLC … Programmable Logical Control (Speicherprogrammierbare Steuerung)
HMI … Human Machine Interface
MES … Manufacturing Execution System
ERP … Enterprise Ressource Planning
DB … Datenbank

Abbildung 1 CPPS-basierte industrielle Cloud (basierend auf [15])

Vorteil bringt. Dienste, Daten und Hardwarekomponenten können auf beliebige CPS-Knoten des entstehenden Automatisierungsnetzes dezentral verteilt werden. Diese dezentralen Netze aus CPS-Knoten werden als (industrielle) Clouds bezeichnet (siehe Abbildung 1).

2 Sicherheitstechnische Aspekte von Maschinen und Anlagen

Bei der Sicherheit von Maschinen und Anlagen der Industrie 4.0 werden zwei Aspekte unterschieden: die Produkt- und Betriebssicherheit (engl. *Safety*) sowie die Angriffs- und Manipulationssicherheit der verwendeten Informations- und Netzwerk-Technologie (engl. *Security*). Beide Aspekte können sich gegenseitig beeinflussen. So kann beispielsweise mangelhafte Angriffssicherheit durch Manipulation der Maschinensteuerung(en) zum Ausfall von Schutzfunktionen führen und damit zur Gefahr für die Beschäftigten werden. Allerdings wurden diese beiden Aspekte bislang von verschiedenen Fachdisziplinen mit unterschiedlichen Herangehensweisen einzeln bearbeitet. So hat man die Risikobeurteilungen bisher getrennt für die Aspekte Safety und Security durchgeführt.

Heutige sicherheitstechnische Konzepte (vor allem bezüglich Safety) gehen in der Konstruktions- und Designphase von definierten Anlagen aus, in denen zwar variable aber vorab klar definierte Prozesse ablaufen. Die sicherheitstechnischen Beurteilungsmethoden legen die Annahme zugrunde, dass die Maschine oder Anlage nach der Inbetriebnahme und der sicherheitstechnischen Abnahme nicht mehr verändert wird, ohne dass eine erneute sicherheitstechnische Überprüfung erfolgt.

Sich selbst konfigurierende Anlagen der Industrie 4.0 ergeben allerdings durch ihre flexible Vernetzung zur Laufzeit Systeme von Systemen, deren Struktur und Gesamtverhalten zur Entwicklungszeit der Einzelsysteme nicht oder nur schwer vorhergesagt werden können. All diese Eigenschaften führen zu Unsicherheiten in der Aussage über das zu erwartende Gesamt-Systemverhalten. Damit stehen sie im Widerspruch zur heutigen Sicherheitsnachweisführung, die zentral auf der Annahme eines deterministischen, vorhersagbaren Systemverhaltens beruht (vgl. [11]).

Dies wird auch durch die hierfür zur Anwendung kommenden aktuellen Sicherheitsnormen reflektiert, die eine dynamische Rekonfiguration der Systeme zur Laufzeit explizit verbieten (vgl. vor allem DIN EN 61508-3 [2]). Besonders dieser für Software relevante Teil 3 der Norm macht deutlich, dass der Standard davon ausgeht, dass ein System vor seiner Zulassung vollständig entwickelt und konfiguriert ist. Jegliche Mechanismen, die das System zur Laufzeit noch einmal ändern, würden zu einer Invalidierung der Zulassung führen und sind daher nicht erlaubt [11].

Darüber hinaus kommt es bereits heute allzu oft vor, dass erst bei der Inbetriebnahme von Maschinen und Anlagen die Aspekte der Angriffssicherheit (Security) „nachgebessert“ werden. Innerhalb der analytischen, methodischen und nicht zuletzt auch normativen Betrachtungsweisen ist deshalb eine Definition von Schnittmengen und Schnittstellen zwischen Safety und Security erforderlich.

3 Neue Anforderungen an sicherheitstechnische Analyse- und Bewertungsmethoden

Vor dem Hintergrund der Konzepte von Industrie 4.0 ist es erforderlich, die Sichtweisen hinsichtlich der betrachteten Steuerungs-Strukturen einerseits sowie der für ihre sicherheitstechnische Analyse und Bewertung angewendeten Methoden andererseits, zu differenzieren (siehe Abbildung 2).

Maschinen und Anlagen der Industrie 4.0 sowie deren Steuerungsstrukturen müssen zur Laufzeit veränderlich (dynamisch) sein. Nur dadurch wird eine auftragsbezogene Rekombination der Anlagen erst ermöglicht.

Heutige Sicherheitsfunktionen zur Erreichung der funktionalen Sicherheit (einschließlich der Angriffssicherheit) werden meist durch eine zentralisierte Steuerungsstruk-

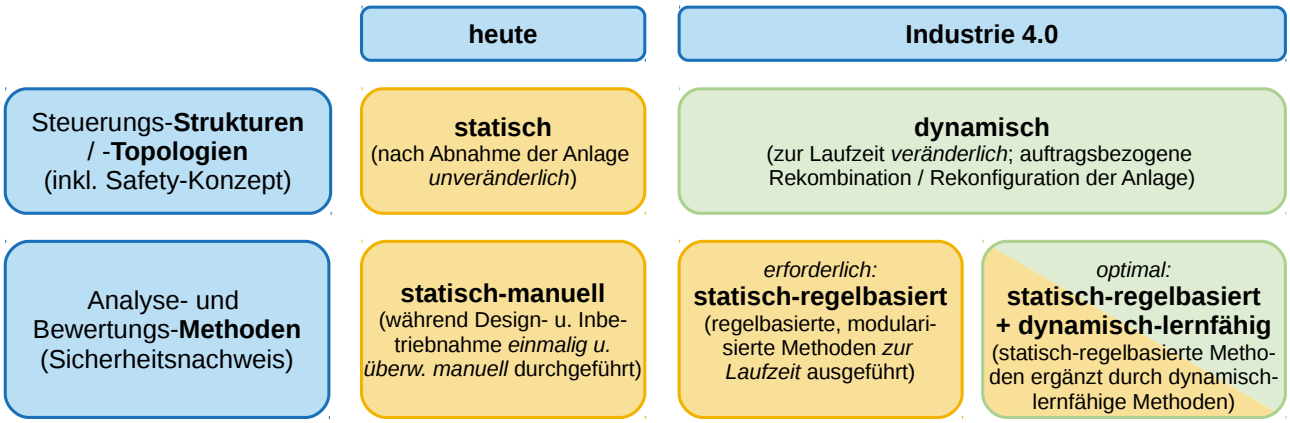


Abbildung 2 Gegenüberstellung statischer und dynamischer Steuerungsstrukturen sowie der entsprechenden Analyse- und Bewertungsmethoden

tur realisiert. Sicherheitsfunktionen setzen sich dabei immer aus den sicherheitsgerichteten Teilfunktionen *Sensorik* (z. B. Lichtvorhang, Laserscanner), *Logik* (z. B. Safety-SPS) sowie *Aktorik* (z. B. Abbremsen und Stillsetzen eines Antriebssystems) zusammen. Damit lassen sich Sicherheitsfunktionen wie z. B. „Sicherer Betriebshalt (SOS)“ oder „Sicherer Stopp (SS1/2)“ nach DIN EN 61800-5-2 [4] umsetzen.

Mit der auftragsbezogenen Rekombination der Maschinen und Anlagen geht eine Dezentralisierung der Steuerungsstrukturen und damit notwendigerweise auch der Sicherheitsfunktionen einher. Diese werden in Zukunft dezentralisiert (verteilt über viele Steuerungs-Komponenten) als modulare, zur Laufzeit und situationsbezogen vernetzbare Sicherheitsmodule vorliegen müssen. Sicherheitsmodule bestehen in diesem Kontext aus vernetzbarer, sicherheitsgerichteter Hardware und Software, welche die sicherheitsgerichteten Teilfunktionen Sensorik, Logik oder Aktorik erfüllen können.

Damit ergeben sich die für den sicheren Betrieb der Maschine bzw. Anlage erforderlichen Sicherheitsfunktionen durch situationsbezogene Vernetzung zur Laufzeit. Nach der Vernetzung muss die mit der neuen Kombination *erreichbare* Sicherheitsstufe (vgl. z. B. *Safety Integrity Level (SIL)* nach DIN EN 61508-4 [3] bzw. *Perfomance Level (PL)* nach DIN EN ISO 13849-1 [5]) mit der für die konkrete Betriebsfunktion der Maschine bzw. Anlage *geforderten* Sicherheitsstufe abgeglichen werden. Dieser Prozess wird als *Validierung* bezeichnet und muss in Zukunft zur Laufzeit durchgeführt werden können. Damit geht einher, dass die heute weitgehend als manuelle Abläufe vorliegenden Methoden zur Risikoanalyse und -bewertung steuerungstechnisch automatisierbar und vernetzbar werden müssen. Nur so kann das heutige Sicherheitsniveau bzgl. der Aspekte Safety und Security für die Beschäftigten aufrecht erhalten oder verbessert werden.

Daher ist es zunächst notwendig, heute verfügbare *manuelle* Analyse- und Bewertungsmethoden durch Implementierung in Software grundlegend zu *automatisieren*. Damit die Software-Methoden später auf die einzelnen CPPS-Komponenten eines Gesamtsystems verteilt werden können, müssen sie gleichzeitig *modularisiert* werden (vgl. Abbildung 2). Hierzu werden aktuell in den entsprechenden Fachgremien Ansätze und theoretische Modelle diskutiert, wie sich die so entstehenden kleinen Software-Bausteine mit Hilfe *statischer* Entscheidungs-Regeln (Boolesche Logik) und deren Grenzen (sog. „regelbasierte Systeme“) realisieren lassen (vgl. „Deutsche Normungs-Roadmap Industrie 4.0, Version 2“ [7]).

Die statischen Entscheidungs-Regeln könnten hierbei Teil-Fehlerbäume des jeweiligen CPPS beschreiben und sich innerhalb der sog. *Verwaltungsschale (Administration Shell)* der Industrie 4.0-Komponente befinden (vgl. DIN SPEC 91345 „Referenzarchitekturmodell Industrie 4.0 (RAMI4.0)“, Abschnitt 6.2 „Verwaltungsschale der I4.0-Komponente (Administration Shell)“ [6]).

In der Fachwelt wird weiterhin diskutiert, dass sich nach der Rekombination der Anlage (Neuvernetzung vieler CPPS zu einem Gesamtsystem) die einzelnen Teil-Fehlerbäume zu einem Gesamt-Fehlerbaum des Gesamtsystems verbinden lassen könnten. Damit ließe sich die Sicherheit des Gesamtsystems *zur Laufzeit* trotz dynamisch veränderlicher Steuerungs-Topologien validieren (vgl. [10, 13, 14]). Diese Verknüpfung von Teilsystemen (hier Teil-Fehlerbäumen) basiert auf dem Ansatz der Schachtelbarkeit von Industrie 4.0-Komponenten unter Anwendung von Industrie 4.0-konformen Kommunikationsschnittstellen (vgl. DIN SPEC 91345, Abschnitt 6.1.7 „I4.0-System (I4.0 System) aus I4.0-Komponenten“ sowie Abschnitt 6.1.8 „Schachtelbarkeit“ [6]).

Vorteil der *statisch-regelbasierten Methoden* ist, dass zu jedem Zeitpunkt (besonders nach System-/Anlagenstart) das Systemverhalten (z. B. sicherheitsgerichtete Reaktion auf erkannte Fehler) durch die Deterministik (es treten nur definierte und reproduzierbare Zustände auf) und die bekannten Ausfallwahrscheinlichkeiten einzelner Komponenten weitgehend vorhersagbar ist. Allerdings ist eine sicherheitsgerichtete Reaktion auf zum Zeitpunkt des System-Entwurfs unbekannte Fehler nicht möglich.

Daneben gibt es Ansätze für *dynamisch-lernfähige Methoden* (z. B. Heuristiken, Anomalieerkennungen, Künstliche Intelligenz, Künstliche Neuronale Netzwerke, Maschinelles Lernen (vgl. [12]). Um diese zur sicherheitsgerichteten Analyse und Bewertung verwenden zu können, müs-

sen sie zunächst auf ihre prinzipielle Eignung untersucht und bewertet werden. Da die dynamischen Methoden das „richtige“ Verhalten (gemeint ist eine angemessene sicherheitsgerichtete Reaktion auf erkannte Fehler) zur Laufzeit des Gesamtsystems zunächst *erlernen* müssen, unterliegen diese Verhaltensmuster einer stetigen Veränderung. Im Idealfall konvergiert das Systemverhalten. Das heißt, es gibt zunächst eine *unruhige* Trainings- bzw. Lernphase mit *fehlenden Alarmen* (Fehler werden nicht erkannt) sowie *Fehl-Alarmen* (Auslösen von Fehlerreaktionen ohne objektive Ursache). Erst nach einer hinreichend langen Lernphase werden stabile sicherheitsgerichtete Entscheidungen ermöglicht.

Vorteilhaft der *dynamisch-lernfähigen Methoden* ist, dass sicherheitsgerichtete Reaktionen auf zum Zeitpunkt des System-Entwurfs unbekannte Fehler durch Erlernen möglich werden. Allerdings steht zu erwarten, dass besonders in der Trainings- bzw. Lernphase die sicherheitsgerichteten Reaktionen auf (vermeintlich) erkannte Fehler unzuverlässig sein werden.

Aus heutiger Sicht werden die *dynamisch-lernfähigen* die *statisch-regelbasierten* Methoden wahrscheinlich nicht *ersetzen* sondern eher *ergänzen* können. Dazu muss durch weitere Untersuchungen eine Methode zur lernzustandsabhängigen Wichtung der Entscheidungsergebnisse beider Methoden-Gattungen (statisch/dynamisch) gefunden werden, um so deren jeweilige Vorteile kombinieren zu können.

4 Ausblick

Die Weiterentwicklung und Modularisierung der heute verfügbaren (manuellen) *statisch-regelbasierten* sowie *dynamisch-lernfähigen* Analyse- und Bewertungsmethoden wird durch einschlägige Forschung erfolgen müssen. Die daraus ableitbaren Ergebnisse sollten anschließend geeigneten Normungsgremien vorgestellt werden mit dem Ziel, dass die weiterentwickelten Methoden in die strategische und inhaltliche Normungsarbeit einfließen.

Damit sich möglichst viele Interessensgruppen aktiv an dem Weiterentwicklungs- und Normungsprozess beteiligen können, sollte die Forschung von Beginn an als *Open Source*-Prozess etabliert werden.

Entsprechend (quell-)offen sollten die Ergebnisse in Form von Prinziplösungen publiziert werden. Dadurch werden unterschiedliche Steuerungs-Hersteller in die Lage versetzt, die in Form von Open Source Software vorliegenden weiterentwickelten und modularisierten Methoden in eigener Verantwortung auf ihre konkrete Steuerungs-Architektur zu portieren und zu einem industriell einsetzbaren und sicheren Produkt weiterzuentwickeln.

In diesem spannenden und anspruchsvollen Themenfeld wird sich die Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (BAuA) in Zukunft engagieren.

Literatur

[1] BMBF, Bundesministerium für Bildung und Forschung. „Intelligente Vernetzung in der Produktion - Ein Beitrag zum Zukunftsprojekt ‚Industrie 4.0‘“. In: *Bundesanzeiger Nr. 197 vom 30. Dezember 2011* (19. Dez. 2011). URL: http://www.produktionsforschung.de/national/archiv/UCM01_000913 (besucht am 27. 01. 2015) (siehe S. 1).

[2] DIN EN 61508-3:2011-02, VDE 0803-3:2011-02. *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme - Teil 3: Anforderungen an Software (IEC 61508-3:2010); Deutsche Fassung EN 61508-3:2010*. deutsch. Techn. Ber. DIN Deutsches Institut für Normung e. V. URL: http://www.beuth.de/de/norm/din-en-61508-3-vde-0803-3-2011-02/135505701 (besucht am 10. 02. 2017) (siehe S. 2).

[3] DIN EN 61508-4:2011-02, VDE 0803-4:2011-02. *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme - Teil 4: Begriffe und Abkürzungen (IEC 61508-4:2010); Deutsche Fassung EN 61508-4:2010*. deutsch. Techn. Ber. DIN Deutsches Institut für Normung e. V. URL: http://www.beuth.de/de/norm/din-en-61508-4-vde-0803-4-2011-02/135405992 (besucht am 10. 02. 2017) (siehe S. 3).

[4] DIN EN 61800-5-2:2008-04, VDE 0160-105-2:2008-04. *Elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl - Teil 5-2: Anforderungen an die Sicherheit - Funktionale Sicherheit (IEC 61800-5-2:2007); Deutsche Fassung EN 61800-5-2:2007*. deutsch. Techn. Ber. DIN Deutsches Institut für Normung e. V. URL: http://www.beuth.de/de/norm/din-en-61800-5-2/105745905 (besucht am 23. 01. 2017) (siehe S. 3).

[5] DIN EN ISO 13849-1:2016-06. *Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen - Teil 1: Allgemeine Gestaltungsleitsätze (ISO 13849-1:2015); Deutsche Fassung EN ISO 13849-1:2015*. deutsch. Techn. Ber. DIN Deutsches Institut für Normung e. V. URL: http://www.beuth.de/de/norm/din-en-iso-13849-1/230387878 (besucht am 23. 01. 2017) (siehe S. 3).

[6] DIN SPEC 91345:2016-04. *Referenzarchitekturmodell Industrie 4.0 (RAMI4.0)*. deutsch. Techn. Ber. DIN Deutsches Institut für Normung e. V. URL: http://www.beuth.de/de/technische-regel/din-spec-91345/250940128 (besucht am 17. 02. 2017) (siehe S. 3).

[7] DKE und VDE. *DKE Normungs-Roadmap - Deutsche Normungs-Roadmap Industrie 4.0, Version 2*. Normungs-Roadmap. DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE, Okt. 2015. URL: https://www.

dke.de/de/std/Documents/NR_Industrie%204.0_V2_DE.pdf (besucht am 30. 03. 2016) (siehe S. 3).

[8] Henning Kagermann, Wolfgang Wahlster und Johannes Helbig. *Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0 - Abschlussbericht des Arbeitskreises Industrie 4.0*. Techn. Ber. acatech - Deutsche Akademie der Technikwissenschaften e. V., Apr. 2013. URL: https://www.bmbf.de/files/Umsetzungsempfehlungen_Industrie4_0.pdf (besucht am 18. 01. 2017) (siehe S. 1).

[9] Edward A. Lee. *Cyber Physical Systems: Design Challenges*. Techn. Ber. UCB/EECS-2008-8. EECS Department, University of California, Berkeley, 23. Jan. 2008. URL: http://www.eecs.berkeley.edu/Pubs/TechRpts/2008/EECS-2008-8.html (besucht am 29. 01. 2015) (siehe S. 1).

[10] Peter Liggesmeyer und Mario Trapp. „Safety: Herausforderungen und Lösungsansätze“. In: *Industrie 4.0 in Produktion, Automatisierung und Logistik*. Hrsg. von Thomas Bauernhansl, Michael ten Hompel und Birgit Vogel-Heuser. Springer Fachmedien Wiesbaden, 2014, S. 433–450. ISBN: 978-3-658-04681-1. DOI: 10.1007/978-3-658-04682-8. URL: http://link.springer.com/chapter/10.1007/978-3-658-04682-8_21 (besucht am 10. 02. 2017) (siehe S. 3).

[11] Peter Liggesmeyer und Mario Trapp. „Safety in der Industrie 4.0. Herausforderungen und Lösungsansätze“. In: *Handbuch Industrie 4.0 Bd.1: Produktion*. Springer-Verlag GmbH, 7. Dez. 2016, S. 107–123. ISBN: 978-3-662-45279-0. DOI: 10.1007/978-3-662-45279-0_34. URL: http://link.springer.com/chapter/10.1007/978-3-662-45279-0_34 (besucht am 10. 02. 2017) (siehe S. 2).

[12] Sebastian Nusser. „Robust learning in safety-related domains: machine learning methods for solving safety-related application problems“. Englisch. Dokument. Universität Magdeburg, Fakultät für Informatik, 10. Juli 2009, S. 140. URL: http://nbn-resolving.de/urn:nbn:de:101:1-201012104420 (besucht am 30. 03. 2016) (siehe S. 3).

[13] Michael Roth und Peter Liggesmeyer. „Modeling and Analysis of Safety-Critical Cyber Physical Systems using State/Event Fault Trees“. In: *SAFECOMP 2013 - Workshop DECS (ERCIM/EWICS Workshop on Dependable Embedded and Cyber-physical Systems) of the 32nd International Conference on Computer Safety, Reliability and Security, France (2013)*. Hrsg. von Matthieu ROY. Toulouse, France, 26. Juli 2013, S. 11. URL: https://hal.archives-ouvertes.fr/hal-00848640 (besucht am 31. 03. 2016) (siehe S. 3).

[14] Max Steiner und Peter Liggesmeyer. „Combination of Safety and Security Analysis - Finding Security Problems That Threaten The Safety of a System“. In: *SAFECOMP 2013 - Workshop DECS (ERCIM/EWICS Workshop on Dependable Embedded and Cyber-physical Systems) of the 32nd International Conference on Computer Safety, Reliability and Security, France (2013)*. Hrsg. von Matthieu ROY. Toulouse, France, 26. Juli 2013, S. 8. URL: https://hal.archives-ouvertes.fr/hal-00848604 (besucht am 18. 04. 2016) (siehe S. 3).

[15] VDI / VDE-GMA. *Thesen und Handlungsfelder - Cyber-Physical Systems: Chancen und Nutzen aus Sicht der Automation*. Techn. Ber. VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik, Apr. 2013. URL: http://www.vdi.de/uploads/media/Stellungnahme_Cyber-Physical_Systems.pdf (besucht am 27. 01. 2015) (siehe S. 1, 2).