Sicherheitsnachweisführung von digital vernetzten Maschinen und Anlagen der Industrie 4.0

Björn KASPER, Stefan VOSS

Gruppe Arbeitsstätten, Maschinen- und Betriebssicherheit
Bundesanstalt für Arbeitsschutz und Arbeitsmedizin, D-01099 Dresden

Kurzfassung: Auch bei Industrie 4.0-Anwendungsszenarien ist die Sicherheit der Beschäftigten zu gewährleisten. Dazu müssen auf Grund des hohen Vernetzungsgrades neben den bisher berücksichtigten sicherheitstechnischen Aspekten der funktionalen Sicherheit (Safety) in verstärktem Maße die industrielle Angriffssicherheit (Security) sowie deren Wechselwirkungen untereinander betrachtet werden. Aus Sicht des Arbeitsschutzes sind insbesondere Security-Aspekte mit Auswirkungen auf die funktionale Sicherheit zu betrachten.

Schlüsselwörter: Industrie 4.0, Sicherheitsnachweisführung, funktionale Maschinensicherheit, Safety, Angriffssicherheit, Security

1. Selbstorganisierende Produktionssysteme der Industrie 4.0

Der Begriff „Industrie 4.0“ steht als Synonym für die „vierte industrielle Revolution“. Basierend auf der rasant zunehmenden Digitalisierung von Wirtschaft und Gesellschaft und der Verschmelzung der industriellen Produktion und Fertigung mit modernster Informations- und Kommunikationstechnik (IKT) wird eine intelligente Organisation und Steuerung der Wertschöpfungskette über alle Phasen des Lebenszyklusses eines Produktes möglich. Dadurch lassen sich Kundenwünsche von der Produktidee bis hin zum Recycling einschließlich der damit verbundenen Dienstleistungen mitdenken. Darüber hinaus könnten leichter als bisher maßgeschneiderte Produkte nach individuellen Kundenwünschen produziert werden (vgl. Plattform Industrie 4.0 2017). Nach der Dampfmaschine (1. Industrielle Revolution), dem Fließband (2. Industrielle Revolution), der Elektronik und der Informationstechnik (3. Industrielle Revolution) bestimmen nun intelligente Fabriken (sogenannte „Smart Factories“) die Entwicklung (vgl. Plattform Industrie 4.0 2017).

Wesentliche technische Grundlagen der Industrie 4.0 sind intelligente, digital vernetzte Systeme, sog. cyber-physische Systeme (CPS). Mit ihrer Hilfe soll eine weitestgehend selbstorganisierte Produktion möglich werden: Menschen, Maschinen, Anlagen, Logistik und Produkte kommunizieren und kooperieren in der Industrie 4.0 direkt miteinander. Produktions- und Logistikprozesse zwischen Unternehmen im selben Produktionsprozess können intelligent miteinander verzahnt werden, um die Produktion effizienter und flexibler zu gestalten (vgl. Plattform Industrie 4.0 2017). Hieraus ergeben sich für die Industrie neuartige Möglichkeiten der Flexibilisierung sowie die Chance einer weitergehenden Qualitäts- und Effizienzsteigerung.

2. Sicherheitstechnische Aspekte von Maschinen und Anlagen

Jede Maschine oder Anlage besitzt Betriebsfunktionen, die zur eigentlichen Wertschöpfung beitragen. Dies soll am Beispiel der in Abbildung 1 dargestellten Gesenk-Presse gezeigt werden. Zur Ausübung ihrer wesentlichen Betriebsfunktion „Umformen eines Halbzeuges (Rohling)“ werden die beteiligten Werkzeuge (Ober- und Untergesenk), der Hauptantriebsmotor mit dem Frequenzumrichter für die Strom- und Momentenregelung sowie die Pressensteuerung mit dem Bearbeitungsprogramm benötigt.

Mit dem Umformvorgang und den dafür notwendigen Schließbewegungen der Presse unter Anwendung großer Kräfte oder Drücke sind erhebliche Risiken für den Maschinenbediener verbunden. Um diese zu reduzieren, werden neben klassischen Sicherheitsmaßnahmen wie z. B. trennenden Schutzeinrichtungen Maßnahmen der funktionalen Sicherheit wie z. B. Sicherheitsfunktionen eingesetzt. Eine typische Sicherheitsfunktion an Pressen ist die Maßnahme „Sicheres Stillsetzen der Pressenbewegung“ (vgl. Abbildung 1).

Sicherheitsfunktionen bestehen stets aus sicherheitsgerichteten Sensoren (bspw. Lichtgitter, Laserscanner), der sicherheitsgerichteten Logik (Sicherheitsprogramm auf der Maschinensteuerung) sowie der sicherheitsgerichteten Aktorik (schnelles Stillsetzen gefahrbringender Maschinenbewegungen mit definierten und überwachten Bremsrampen). Damit wird gewährleistet, dass Fehlerzustände im Bearbeitungsprozess erkannt werden können und die vorgesehene Schutzwirkung für den Menschen eintritt (vgl. Kasper und Voß 2018).

Für alle sicherheitstechnischen Betrachtungen ist entscheidend, zwischen den Betriebs- und Sicherheitsfunktionen einer Maschine zu unterscheiden (siehe Abbildung 1). Sicherheitsfunktionen zur Erreichung der funktionalen Sicherheit werden oft als Safety-Funktionen bezeichnet. Die sicherheitsgerichtete Logik wertet die Signale der Sensorik (z. B. Lichtgitter) aus und veranlasst im Fehler- bzw. Gefahrenfall den Aktor (Maschinenantrieb), in einen sicheren Zustand (Stillstand) zu gehen. Wenn diese sicherheitsgerichteten Signale über weite Strecken oder besonders im Kontext der Industrie 4.0-Konzepte über ungesicherte Medien (z. B. funkbasierte Netzwerke) übertragen werden, müssen geeignete Security-Maßnahmen zur Manipulationsvermeidung ergriffen werden. Entsprechende Security-Maßnahmen sind z. B. eine Ende-zu-Ende-Verschlüsselung der Kommunikation oder die anwendungsspezifisch gezielte Reduktion von Funk-Reichweiten (Kasper und Voß 2018).

3. Neue Anforderungen an sicherheitstechnische Analyse- und Bewertungs-Methoden

Hinsichtlich der Sicherheit heutiger Maschinen und Anlagen und besonders im Kontext der Industrie 4.0 sind zwei Aspekte zu berücksichtigen: Zum einen die Produkt- und Betriebssicherheit (engl. Safety) sowie zum anderen die Angriffs- und Manipulations-sicherheit der verwendeten Informations- und Netzwerk-Technologie (engl. Security). Beide Aspekte können sich gegenseitig beeinflussen. Aus Sicht des Arbeitsschutzes gilt es, diese Zusammenhänge zu betrachten (Kasper und Voß 2018).

So kann mangelhafte Angriffssicherheit durch Manipulation der Maschinensteuerung(en) beispielsweise über deren Vernetzungen untereinander zum Ausfall von

Schutzfunktionen führen und damit zur Gefahr für die Beschäftigten werden. Diese beiden Sicherheits-Aspekte werden bislang methodisch einzeln betrachtet, indem Risikobeurteilungen getrennt für die Aspekte Safety und Security durchgeführt werden (Kasper und Voß 2018).

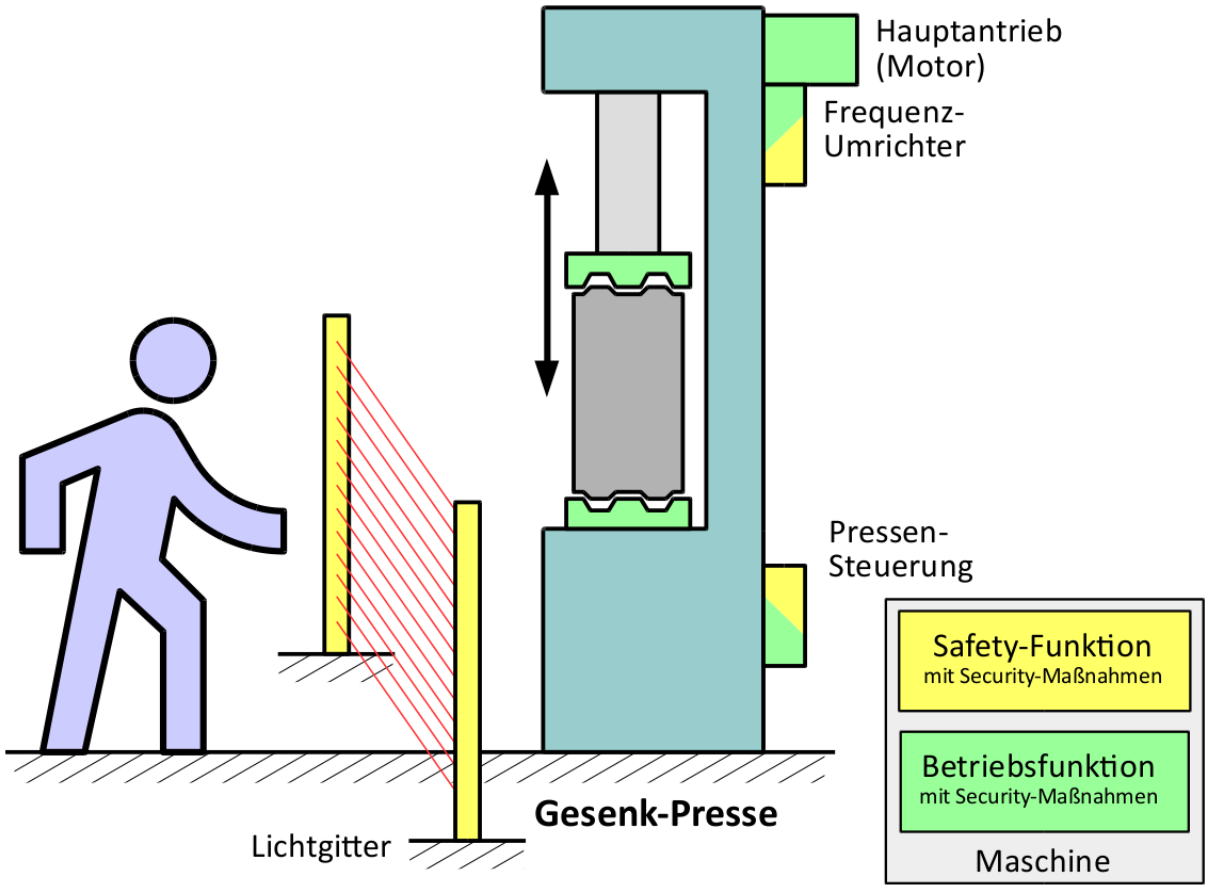

Abbildung 1: *Betriebsfunktionen und Sicherheitsfunktionen von Maschinen*

In heutigen Produktionsanlagen werden marktbedingte Absatz- und Variantenschwankungen meist mit einem Ressourcenvorhalt berücksichtigt. Die damit erreichbare Flexibilität einer Anlage umfasst die Änderungsmöglichkeiten, die eine Anlage von sich aus mitbringt, um auf zum jeweiligen Planungszeitpunkt bekannte Änderungen reagieren zu können. Innerhalb zuvor vereinbarter Grenzen kann die flexible Anlage sehr schnell und mit geringem Aufwand auf die geänderten Randbedingungen angepasst werden (Steegmüller und Zürn 2016).

Zukünftig werden deutlich dynamischere und volatilere Märkte erwartet, wodurch der dafür erforderliche Flexibilitätsvorhalt nicht mehr wirtschaftlich wäre. Aus diesem Grund werden im Kontext von Industrie 4.0 wandlungsfähige Fertigungsanlagen durch auftragsbezogene Rekombination von Fertigungsmodulen diskutiert. Die Wandlungs-fähigkeit einer Anlage beschreibt dabei ihr Vermögen und Potenzial, mit minimalem Aufwand beliebig umgestaltet zu werden (Steegmüller und Zürn 2016). Diese Wandlungsfähigkeit wird erreicht, indem einzelne Fertigungsmodule auftragsbezogen zu Fertigungsinseln rekombiniert, vernetzt und automatisch konfiguriert werden. Einzelmodule (sog. Industrie 4.0-Komponenten) werden dazu flexibel und zumeist funkbasiert miteinander vernetzt.

Dadurch ergeben sich zur Laufzeit der Anlage Systeme aus (Teil-)Systemen, die

zu einer grundlegenden Steigerung der kombinatorischen Komplexität des Gesamtsystems führen. Die Struktur und das Gesamtverhalten sowie die Abhängigkeiten der Systemkomponenten untereinander können zur Entwicklungszeit der Einzelsysteme nicht oder nur schwer vorhergesagt werden.

Diese Eigenschaften führen zu Unsicherheiten in der Aussage über das zu erwartende Gesamtsystemverhalten. Dadurch kommen die heute verfügbaren Methoden zur Analyse und Bewertung der funktionalen Sicherheit an ihre Grenzen, da solche dynamischen Systeme und Szenarien von den aktuellen Sicherheitsnormen nicht erfasst bzw. in deren Anwendungsbereich explizit ausgeschlossen werden (vgl. Kasper und Voß 2018).

Die heutigen sicherheitstechnischen Konzepte (vor allem bezüglich Safety) sowie die Methoden zur Sicherheitsnachweisführung beruhen bislang zentral auf der Annahme eines deterministischen, vorhersagbaren Systemverhaltens (vgl. Liggesmeyer und Trapp 2016). Von diesem deterministischen Verhalten konnte bisher ausgegangen werden, wenn in der Konstruktions- und Designphase definierte Anlagen zugrunde gelegt werden, in denen zwar variable aber vorab klar definierte Prozesse ablaufen. Die sicherheitstechnischen Standards gehen heute davon aus, dass ein System vor seiner sicherheitstechnischen Abnahme und Zulassung vollständig entwickelt und konfiguriert ist (vgl. insbes. DIN EN 61508-3:2011-02, VDE 0803-3:2011-02). Danach dürfen keine sicherheitsrelevanten Veränderungen (auch Reparaturen) vorgenommen werden, ohne dass eine erneute sicherheitstechnische Überprüfung und Abnahme zumindest der betroffenen Teilsysteme erfolgt (vgl. Kasper und Voß 2018; vgl. Kasper 2018).

Wie im vorigen Abschnitt dargestellt, folgt der bisherige Stand der Sicherheitstechnik dem deterministischen Sensor-Logik-Aktor-Prinzip. Es steht allerdings zu erwarten, dass in der stärksten Ausprägung von Industrie 4.0 Algorithmen aus dem Bereich des Maschinellen Lernens zukünftig auch bei Betriebsfunktionen im Maschinen- und Anlagenbau Verwendung finden werden, um die Produktionsprozesse flexibel und intelligent miteinander zu verknüpfen (vgl. Wickert 2017).

Damit sind die in der Fachwelt diskutierten Industrie 4.0-Anwendungsszenarien mit den heutigen Methoden zur Analyse und Bewertung der funktionalen Sicherheit nicht oder nur mit erheblichen Einschränkungen hinsichtlich der zur Laufzeit zulässigen Dynamik, Variabilität, Wandelbarkeit und Lernfähigkeit der Maschinen bzw. der verfahrenstechnischen Anlagen validierbar. Daher ergibt sich der Bedarf, die heutigen sicherheitstechnischen Methoden an die neuen bzw. geänderten Anforderungen wandlungsfähiger Fertigungsanlagen anzupassen oder weiterzuentwickeln (Kasper und Voß 2018; vgl. Kasper 2018).

4. Industrie 4.0-Anwendungsszenarien und ihre sicherheitstechnischen Aspekte

Zur Beurteilung des aktuellen Standes der Technologieentwicklung im Kontext von Industrie 4.0 wurde durch die Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (BAuA) eine Literaturstudie erarbeitet. Dabei war der Fokus, einen Überblick über wesentliche Grundlagen und Zusammenhänge von Industrie 4.0-Konzepten sowie ausgewählte Anwendungsszenarien zu erhalten. Die untersuchten Anwendungsszenarien betrachteten jeweils verschiedene Facetten der Industrie 4.0-Konzepte mit unterschiedlichen Wichtungen. Keines der Anwendungsszenarien beleuchtete alle

Aspekte der Industrie 4.0-Konzepte in gleichem Maße (Kasper und Voß 2018; vgl. Kasper 2018).

Um die Sicherheit der Beschäftigten zu gewährleisten, müssen bei Anwendungsszenarien im Kontext von Industrie 4.0 durch den hohen Grad der Vernetzung dezentraler Teilsysteme mit Hilfe von IKT neben den bisher vorwiegend berücksichtigten sicherheitstechnischen Aspekten der funktionalen Sicherheit (Safety) in verstärktem Maße die industrielle Angriffssicherheit (Security) sowie deren Wechselwirkungen untereinander betrachtet bzw. berücksichtigt werden. Bei der sicherheitstechnischen Bewertung der ausgewerteten Anwendungsszenarien hat sich gezeigt, dass nur einige der in der Literatur beschriebenen Anwendungsszenarien die Aspekte der funktionalen Sicherheit betrachtet haben. Jedoch adressierte keines der untersuchten Anwendungsszenarien inhaltlich die industrielle Angriffssicherheit. Demzufolge wird auch in keinem der betrachteten Anwendungsszenarien ein Zusammenhang zwischen funktionaler Sicherheit (Safety) und industrieller Angriffssicherheit (Security) hergestellt bzw. mögliche Wechselwirkungen zwischen beiden Sicherheitsaspekten dargestellt oder näher untersucht. In den zur Verfügung stehenden Literaturquellen der betrachteten Anwendungsszenarien werden keine Risikoanalysen und -bewertungen durchgeführt oder Maßnahmen zur Risikominderung aufgezeigt.

Abschließend wurde in der Studie eine fachliche Einschätzung dahingehend gegeben, ob die im Kontext von Industrie 4.0 z. T. neuen sicherheitstechnischen Anforderungen an derartige Systeme, Anlagen oder Maschinen mit den heutigen Mitteln des technischen Arbeitsschutzes erfüllt werden können bzw. inwieweit Methoden der Sicherheitsnachweisführung zur Verfügung stehen.

5. Ausblick

Zusammenfassend ist festzustellen, dass die sicherheitstechnische Bewertung von Industrie 4.0-Prozessen und -Systemen eine Reihe offener Fragestellungen aufwirft und aufgrund der facettenreichen Aspekte eine hohe Interdisziplinarität vorliegt. Dabei stehen u. a. Fragen im Raum, inwieweit die Sicherheit von Maschinen und Anlagen im Kontext von Industrie 4.0 aufgrund ihrer Wandlungsfähigkeit oder sogar Lernfähigkeit ihrer Betriebsfunktionen sowie möglicherweise auch ihrer Sicherheitsfunktionen gewährleistet werden kann. Insbesondere sollte zukünftig untersucht werden, wie die Wechselwirkungen von funktionaler Sicherheit und industrieller Angriffssicherheit zu bewerten sind bzw. ob diese über heute verfügbare sicherheitstechnische Bewertungsmethoden erfasst werden und identifizierte Risiken mit angemessenen Maßnahmen reduziert werden können (Kasper 2018).

6. Literatur

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. DIN Deutsches Institut für Normung e. V.

Kasper, Björn. 2018. Maschinen und Anlagen in der digitalen Produktion – Neue Anforderungen an die Sicherheitsnachweisführung. baua:Aktuell – Amtliche Mitteilungen der Bundesanstalt für Arbeitsschutz und Arbeitsmedizin 3/18 (11. September): Seite 6.

Kasper, Björn und Stefan Voß. 2018. Neue Anforderungen an die Sicherheitsnachweisführung von Maschinen und Anlagen im Kontext von Industrie 4.0. sicher ist sicher 69, Nr. 9 (7. September):

Seiten 368–371.
Liggesmeyer, Peter und Mario Trapp. 2016. Safety in der Industrie 4.0: Herausforderungen und Lösungsansätze. In: Handbuch Industrie 4.0 Bd.1: Produktion, 107–123. Springer-Verlag GmbH, 7. Dezember.
Plattform Industrie 4.0. 2017. Was ist Industrie 4.0? Die vierte industrielle Revolution: Auf dem Weg zur intelligenten und flexiblen Produktion.
Steegmüller, Dieter und Michael Zürn. 2016. Wandlungsfähige Produktionssysteme für den Automobilbau der Zukunft. In: Handbuch Industrie 4.0 Bd.1: Produktion, hg. von Birgit Vogel-Heuser, Thomas Bauernhansl, und Michael ten Hompel, 27–44. Springer-Verlag GmbH, 7. Dezember.
Wickert, Karl. 2017. Algorithmen: Chance und Herausforderung für die Maschinensicherheit. sicher ist sicher, Nr. 12/2017: 531–533.

Gesellschaft für
Arbeitswissenschaft e.V.

Arbeit interdisziplinär
analysieren – bewerten – gestalten

65. Kongress der
Gesellschaft für Arbeitswissenschaft

Professur Arbeitswissenschaft
Institut für Technische Logistik und Arbeitssysteme
Technische Universität Dresden

Institut für Arbeit und Gesundheit
Deutsche Gesetzliche Unfallversicherung

27. Februar – 1. März 2019

GfA-Press

Bericht zum 65. Arbeitswissenschaftlichen Kongress vom 27. Februar – 1. März 2019

Professur Arbeitswissenschaft, Institut für Technische Logistik und Arbeitssysteme, Technische Universität Dresden;
Institut für Arbeit und Gesundheit, Deutsche Gesetzliche Unfallversicherung, Dresden

Herausgegeben von der Gesellschaft für Arbeitswissenschaft e.V.
Dortmund: GfA-Press, 2019
ISBN 978-3-936804-25-6

NE: Gesellschaft für Arbeitswissenschaft: Jahresdokumentation

Als Manuskript zusammengestellt. Diese Jahresdokumentation ist nur in der Geschäftsstelle erhältlich.

Schriftleitung: Matthias Jäger
im Auftrag der Gesellschaft für Arbeitswissenschaft e.V.

Screen design und Umsetzung
© 2019 fröse multimedia, Frank Fröse
office@internetkundenservice.de · www.internetkundenservice.de