3.1.1 Betriebssicherheit der cyber-physischen Systeme (CPS)

Stichwörter: Arbeitsmittel, Anlagen, Beschaffung, Prüfung, Unterweisung

› Warum ist das Thema wichtig?

Smarte Arbeitsmittel, die Bestandteil von cyber-physischen Systemen (CPS)[1] sind und von intelligenter Software[2] mit ihren Modellen der künstlichen Intelligenz (KI) ganz oder teilweise gesteuert werden, stellen in allen Anwendungsbereichen[3] neue Anforderungen an die Betriebssicherheit. Die cyber-physischen Systeme eröffnen einerseits neue Möglichkeiten, die auch der Betriebssicherheit dienen, wie zum Beispiel Zustand und Fehlererkennung beinahe in Echtzeit oder Überprüfung der Schutzeinrichtungen. Andererseits können beim Einsatz dieser 4.0-Technologien[4] in 4.0-Prozessen[5] neue Gefahren und Belastungen entstehen.

Eine zentrale Rolle spielt dabei die intelligente Software (inkl. KI), die durch Sensoren und selbstlernende Systeme in der Lage ist, auf Situationen beinahe in Echtzeit zu reagieren und dadurch beispielsweise die Sicherheit für die Beschäftigten bei der Tätigkeit zu erhöhen. Bei der Anschaffung von smarten Arbeitsmitteln oder der nachträglichen Ausstattung vorhandener Arbeitsmittel mit smarten Technologien sollten daher Aspekte der Betriebssicherheit berücksichtigt werden. Zudem muss gegebenenfalls die europäische Konformität nachträglich geprüft und wieder hergestellt werden.

In dieser Umsetzungshilfe werden überwachungsbedürftige Anlagen nicht behandelt.

› Worum geht es bei dem Thema?

Begriffe: Betriebssicherheit – Arbeitsmittel – Cybersicherheit

Unter **Betriebssicherheit** wird hier verstanden: Betriebssicherheit gewährleistet „die Sicherheit und den Schutz der Gesundheit von Beschäftigten bei der Verwendung von Arbeitsmitteln (...). Dies soll insbesondere erreicht werden durch

1. die Auswahl geeigneter Arbeitsmittel und deren sichere Verwendung,
2. die für den vorgesehenen Verwendungszweck geeignete Gestaltung von Arbeits- und Fertigungsverfahren sowie
3. die Qualifikation und Unterweisung der Beschäftigten.“ [6]

Arbeitsmittel sind „Werkzeuge, Geräte, Maschinen oder Anlagen, die für die Arbeit verwendet werden, sowie überwachungsbedürftige Anlagen.“ [7] Im Folgenden wird auch Software als Arbeitsmittel verstanden. Smarte Arbeitsmittel sind Arbeitsmittel, die mit Sensorik und intelligenter Software (inkl. KI) ausgestattet und Bestandteil von cyber-physischen Systemen sind.

„Die Verwendung von Arbeitsmitteln umfasst jegliche Tätigkeit mit diesen. Hierzu gehören insbesondere das Montieren und Installieren, Bedienen, An- oder Abschalten oder Einstellen, Gebrauchen, Betreiben, Instandhalten, Reinigen, Prüfen, Umbauen, Erproben, Demontieren, Transportieren und Überwachen.“ [8]

Cybersicherheit befasst sich mit allen Aspekten der Sicherheit in der Informations- und Kommunikationstechnik. Das Aktionsfeld der Informationssicherheit wird dabei auf den gesamten Cyberraum ausgeweitet. Dieser umfasst sämtliche mit dem Internet und vergleichbaren Netzen verbundene Informationstechnik und schließt darauf basierende Kommunikation, Anwendungen, Prozesse und verarbeitete Informationen mit ein.[9]

Diese Umsetzungshilfe gibt Experten und Interessierten Anregungen, wie Arbeit 4.0 zu gestalten ist. Die Empfehlungen sollten an die jeweilige konkrete betriebliche Situation angepasst werden.

[1] Cyber-physische Systeme (CPS) verbinden und steuern als autonome technische Systeme Arbeitsmittel, Produkte, Räume, Prozesse und Menschen beinahe in Echtzeit. Die komplette oder teilweise Steuerung übernimmt intelligente Software auf Grundlage von Modellen der künstlichen Intelligenz. Genutzt werden dazu unter anderem auch Sensoren/Aktoren, Verwaltungsschalen, Plattformen/Clouds.

[2] Intelligente Software steuert cyber-physische Systeme (CPS) und andere autonome technische Systeme (wie Messenger-Programme). Intelligente Software nutzt Modelle künstlicher Intelligenz zusammen mit anderen Basistechnologien wie zum Beispiel Algorithmen, semantischen Technologien, Data-Mining. Intelligente Software ist autonom und selbstlernend.

[3] Anwendungsbereiche von CPS können sein: **Insellösungen**, Teilkomponenten und Teilprozesse (zum Beispiel einzelne Arbeitsplätze, Arbeitsmittel, Teile von Anlagen, Räume, Produkte, Assistenzsysteme) und **verkettete Prozesse** und Gesamtsystemlösungen (zum Beispiel verkettete Arbeitsmittel, Wertschöpfungskette). Außerdem **geschlossene Betriebsanwendungen** (autark – zum Beispiel Edge Computing, betriebliche Cloud), **offene Anwendungen** (zum Beispiel Public Clouds, Hersteller-Plattformen).

[4] 4.0-Technologie bezeichnet hier Hardware und technologische Produkte (wie Assistenzmittel/Smartphones, Sensoren/Aktoren in smarten Arbeitsmitteln, Fahrzeugen, Produkten, Räumen usw., smarte Dienstleistungen, Apps), die von intelligenter Software (inkl. KI) ganz oder teilweise gesteuert werden.

[5] Unter 4.0-Prozessen werden hier alle Arbeitsprozesse verstanden, in denen cyber-physische Systeme (CPS) oder andere autonome technische Systeme (wie Plattformen, Messenger-Programme) beteiligt sind. 4.0-Prozesse sind in den Arbeitsprozessen bisher selten vollständig, aber in Ansätzen in allen Betrieben umgesetzt.

[6] § 1 Abs. 1 BetrSichV

[7] § 2 Abs. 1 BetrSichV

[8] § 2 Abs. 2 BetrSichV

[9] BSI 2018

Intelligente Software (inkl. KI) ermöglicht unter anderem folgende neue Funktionen des Arbeitsmittels, die für die Betriebssicherheit[10] relevant sind:

- Autonome Steuerung des Arbeitsmittels durch selbstlernende intelligente Software (inkl. KI) (ganz oder teilweise)
- Eigenständige Interaktion vernetzter Arbeitsmittel untereinander
- Vorausschauendes Erkennen von Fehlern, Verschleiß oder Mängeln im laufenden Betrieb (Predictive Maintenance)
- Automatische Überprüfung der Wirksamkeit von Maßnahmen aus der Gefährdungsbeurteilung
- Personenerkennung, Erstellung von Interaktions-, Bedienungs- und Bewegungsprofilen der Nutzer des jeweiligen Arbeitsmittels
- Position und Bewegungsprofile des Arbeitsmittels und von Personen (Datenschutz vorausgesetzt)
- Erhebung und Auswertung von Daten über Arbeits- und Fertigungsverfahren, Auslastung und Nutzung des Arbeitsmittels und anderer Ressourcen
- Weitergabe durch intelligente Software (inkl. KI) erlernter Optimierungslösungen in der Steuerung des Arbeitsmittels an andere Arbeitsmittel
- Zugriffsmöglichkeiten durch Hersteller und Dritte auf Daten und Steuerung des Arbeitsmittels sowie auf weitergehende Daten des Betriebes, sofern dies vom Betreiber zugelassen ist

Wenn autonome, selbstlernende Software (inkl. KI) in Prozesse eingreift und diese ganz oder teilweise steuert, hat dies Auswirkungen auf die Anschaffung und Verwendung smarter Arbeitsmittel sowie die Organisation der Betriebssicherheit.

Daher ist es wichtig, dass die intelligente Software (inkl. KI) Aspekte der Sicherheit und Gesundheit beim Umgang mit den Arbeitsmitteln berücksichtigt. Dies gilt sowohl für die grundlegenden Funktionen der intelligenten Software (inkl. KI) wie auch für die Kriterien, nach denen sie lernt und entscheidet. Die intelligente Software (inkl. KI) sollte zum Beispiel eine wesentliche Schutzfunktion nicht ausschalten, auch wenn das Arbeiten ohne diese Schutzfunktion effektiver und effizienter ist.

Bei der Veränderung vorhandener Arbeitsmittel muss geprüft werden, ob diese gemäß Maschinenrichtlinie wesentlich ist. Dann wird der Betreiber zum Hersteller und muss die Herstellerpflichten erfüllen (insbesondere Konformitätsbewertungsverfahren). Wesentliche Veränderungen können sich durch das alleinige Aufspielen von Software oder die Durchführung von Updates ergeben. Dann muss die funktionale Sicherheit, die sich als Aufgabe an den Hersteller richtet, wieder hergestellt werden. Diese umfasst:

- Vermeidung systematischer Fehler in der Entwicklung
- Überwachung im laufenden Betrieb zur Erkennung von zufälligen Fehlern
- Sichere Beherrschung von erkannten Fehlern und Übergang in einen vorher als sicher definierten Zustand

Um die Betriebssicherheit in 4.0-Prozessen zu gewährleisten, sollten bei der Anschaffung und Programmierung sowie Verwendung smarter Arbeitsmittel unter anderem folgende Aspekte berücksichtigt werden:

- Aspekte der Sicherheit und Gesundheit müssen durch die intelligente Software (inkl. KI) beim Umgang mit Arbeitsmitteln berücksichtigt werden.
- Einhaltung des Datenschutzes, da die Arbeitsmittel personenbezogene Daten erheben können.
- Datensicherheit, da über die Steuerungsfunktion der intelligenten Software (inkl. KI) die Gefahr vor Fremdzugriffen steigt.
- Datenqualität, um einen zuverlässigen und damit sicheren Einsatz der Arbeitsmittel zu ermöglichen.
- Schnittstellen-Regelungen: Es muss transparent geregelt sein, in welchen Situationen die Handlungsträgerschaft beim Menschen oder bei der intelligenten Software (inkl. KI) liegt und wie die Übergabe zwischen Mensch und intelligenter Software (inkl. KI) erfolgt. › *Siehe Umsetzungshilfe 1.3.3 Handlungsträgerschaft im Verhältnis Mensch und intelligente Software (inkl. KI).*
- Notfallmanagement, da ein Ausfall der intelligenten Software (inkl. KI) den wirtschaftlichen, sicheren und gesundheitsgerechten Einsatz der Arbeitsmittel gefährden kann. › *Siehe Umsetzungshilfen 2.2.1 Risikobetrachtung von 4.0-Prozessen; 2.2.4 Notfallorganisation und 4.0-Prozesse.*

Im Folgenden werden zwei Beispiele dargestellt, die für die Betriebssicherheit der cyber-physischen Systeme relevant sind:

Beispiel: Personenerkennung

Smarte Arbeitsmittel nutzen Sensoren zur Umgebungserfassung inklusive der Personenerkennung. Sie verwenden anschließend die erfassten Daten für unterschiedliche Anwendungen, zum Beispiel für ihre eigene Steuerung, die Steuerung der Interaktion zwischen Mensch und Maschine, die Optimierung der Prozesse (Datenschutz vorausgesetzt). Aus den Daten lassen sich auch Persönlichkeits-, Bewegungs-, Interaktions- sowie Leistungsprofile erstellen, die personenindividuelle Schutzvorkehrungen möglich machen. Dazu zählen beispielsweise skalierbare Warnhinweise, die von der Sehstärke und dem aktuellen Gesundheitszustand des Bedieners abhängen. Möglich ist auch, dass das Bedienen von Arbeitsmitteln an die korrekte Nutzung der Persönlichen Schutzausrüstung gebunden ist. Viele Messverfahren können auch Körperhaltungen aufnehmen, sodass die Möglichkeit eines verbesserten ergonomischen Einsatzes besteht (Sicherheit und Gesundheit).[11]

Bei der Personenerkennung muss stets sichergestellt sein, dass der menschliche Körper zuverlässig analysiert wird (Datenqualität), sodass die Daten für den jeweiligen Verwendungszweck geeignet sind. › *Siehe Umsetzungshilfe 2.3.3 Datenqualität in 4.0-Prozessen.*[12] Der Umgang mit den personenbezogenen Daten ist durch den Unternehmer mit Herstellern und Beschäftigten zu vereinbaren (Datenschutz). › *Siehe Umsetzungshilfe 2.3.2 Datenschutz in 4.0-Prozessen.* Der Schutz der Daten vor Fremdzugriffen ist zu gewährleisten, zum Beispiel durch Auswahl eines verlässlichen Cloud-Dienstleisters (Datensicherheit). › *Siehe Umsetzungshilfen 2.3.1 Datensicherheit in 4.0-Prozessen; 2.5.1 Anforderungen an eine Cloud; 2.5.2 Cloud-Modelle der Bereitstellung und Dienstleistungen.*

[10] Zittlau 2018, S. 269ff.
[11] Schmauder et al. 2016
[12] Schmauder et al. 2016

Beispiel: Wartung, Verschleiß und Fehlererkennung

Die intelligente Software (inkl. KI) kann Verschleiß, Fehler, Mängel sowie kritische Situationen vorausschauend autonom erkennen, Schlussfolgerungen ableiten und reagieren. Sie kann daraufhin Maßnahmen veranlassen, wie beispielsweise die Bereitstellung von Informationen des Herstellers, die rechtzeitige Bestellung von Reparaturmaterial, die Veranlassung von Wartungsprozessen oder die Einleitung von Notfallmaßnahmen. Sind die ergriffenen Maßnahmen für Führungskräfte und Beschäftigte nicht nachvollziehbar, kann das problematisch sein. Deswegen sollte die intelligente Software (inkl. KI) die Beteiligten rechtzeitig über die von ihr eingeleiteten Maßnahmen informieren.

Weiterhin ist ein direkter Zugriff von Herstellern und Dienstleistern beinahe in Echtzeit möglich. Dadurch können die Betriebssicherheit der Arbeitsmittel gewährleistet und vorgeschriebene Prüfungen veranlasst werden. Gleichzeitig können Hersteller auf die Funktionsfähigkeit der Arbeitsmittel einwirken, sofern dies der Betreiber zulässt (der Betrieb sollte dies bei der Beschaffung regeln). Damit kann der Zugriff auf personenbezogene oder sensible betriebliche Daten verbunden sein (zum Beispiel Nutzungsdaten, Daten zu Fehlern und Prozessschritten). › *Siehe Umsetzungshilfe 3.1.6 Smarte Formen der Instandhaltung von Arbeitsmitteln*.

› Welche Chancen und Gefahren gibt es?

Chancen können zum Beispiel sein:

- Zuverlässigere Erfassung, Erhalt und Herstellung des betriebssicheren Zustands von Arbeitsmitteln durch die Nutzung von Echtzeit-Daten
- Zeitnahe, softwaregesteuerte Optimierung der Betriebssicherheit von Arbeitsmitteln auf Grundlage einer breiten Datenbasis aus den vernetzten Arbeitsmitteln in Unternehmen oder unternehmensübergreifend auf Herstellerebene
- Verringerung von Fehlern und Mängeln durch vorausschauende Erfassung und Reaktion beinahe in Echtzeit sowie systematische Auswertung und Verbesserung von Prozessen
- Überwachung der Interaktion von Mensch und Arbeitsmittel und entsprechende Reaktion beinahe in Echtzeit, um Fehler oder Gesundheitsgefahren zu vermeiden (zum Beispiel durch entsprechende Steuerung der Arbeitsmittel oder Hinweisen an die Person)
- Überwachung und Prognose des Verschleißes von technischen Komponenten und damit Reduktion der Ausfallzeiten von Arbeitsmitteln und Senkung der Kosten durch bedarfsgerechten Austausch von Komponenten
- Softwaregesteuerte Absicherung gegen Manipulationen von Arbeitsmitteln (zum Beispiel sensorgesteuerte Zugriffskontrollen)
- Reduktion psychischer und physischer Belastungen, beispielsweise durch Anpassung an körperliche Eigenschaften und Kompetenzen der Beschäftigten (zum Beispiel Informationen, Arbeitsrhythmus, Aufmerksamkeitsanforderungen, Ergonomie)
- Gewährleistung einer fristgerechten Prüfung und bedarfsgerechten Instandhaltung der Arbeitsmittel
- Reduzierung von Unfällen und Störungen durch vorausschauende Sicherheitsvorkehrungen

Gefahren können zum Beispiel sein:

- Fehlende Berücksichtigung von Aspekten der Sicherheit und Gesundheit in der intelligenten Software (inkl. KI) der smarten Arbeitsmittel sowie in den Kriterien, nach denen die Software lernt
- Fehlender Datenschutz in der Verarbeitung und Speicherung personenbezogener Daten aus den Arbeitsmitteln
- Lücken in der Sicherheit können durch die Vernetzung schwerwiegende Auswirkungen haben (zum Beispiel können Hacker nicht nur auf ein Arbeitsmittel, sondern auch auf unternehmensinterne und -übergreifende vernetzte Arbeitsmittel Zugriff haben)
- Fehlende Sicherheit der erzeugten Daten, Zugriffsmöglichkeiten durch Dritte, ungeklärte Besitzverhältnisse der Daten, mangelnder Datenschutz, Angst vor Datenverlust sowie Datenspionage
- Nutzung von Daten für die Betriebssicherheit, die nicht für diese Anwendung geeignet sind (fehlende Datenqualität)
- Intransparente und ungeregelte Schnittstellen zwischen Mensch und intelligenter Software (inkl. KI) des Arbeitsmittels (Handlungsträgerschaft)
- Unvorbereitete Übergabe der Handlungssteuerung von der intelligenten Software (inkl. KI) auf den Menschen
- Ausfall von Steuerungssoftware der Arbeitsmittel durch fehlendes Notfallmanagement
- Fehlende Integrationsfähigkeit von einzelnen Elementen oder Komponenten in das Gesamtsystem (zum Beispiel bei der Verknüpfung von neuen 4.0-Techniken mit alten 3.0-Elementen)
- Fehlende Regelung der Verantwortung (zum Beispiel Hersteller, Unternehmer, Beschäftigte) für Fehler oder Schäden, wenn Arbeitsmittel autonom arbeiten
- Nicht vereinbarte Überwachung des Aufenthalts, des Verhaltens und der Bewegungen von Beschäftigten
- Einschränkung der Autonomie beziehungsweise des Handlungsspielraums als zunehmende Belastung für Beschäftigte

› Welche Maßnahmen sind zu empfehlen?

Anschaffung des smarten Arbeitsmittels

Bei der Anschaffung smarter Arbeitsmittel wird die Empfehlung gegeben, zusätzlich zu den herkömmlichen Maßnahmen der Betriebssicherheit (nach Betriebssicherheitsverordnung) unter anderem folgende Maßnahmen zu beachten:

- Überlegen, in welche Zusammenhänge und Anwendungsbereiche das smarte Arbeitsmittel integriert werden soll (Teilkomponentenprozesse oder Gesamtsystem). Auch schrittweise Eingliederung von bisherigen Arbeitsmitteln in 4.0-Systeme berücksichtigen und deren Sicherheit im Gesamtsystem gewährleisten.
- Überprüfen, wie die Daten des smarten Arbeitsmittels mit weiteren Plattformen und vergleichbaren Netzen verbunden sind und welche weitergehende Kommunikation, weitere Anwendungen und Prozesse in diesem Zusammenhang erfolgen (Cybersicherheit).

- Überprüfen, wie die Daten über den betriebssicheren Zustand des Arbeitsmittels (wie Fehler, Nutzung der Schutzeinrichtungen, Verschleiß, Mängel) für eine wirksame Kontrolle des betriebssicheren Zustands genutzt werden können, und gegebenenfalls entsprechende Maßnahmen einleiten.
- Überprüfen, wie die Daten des smarten Arbeitsmittels für die Unterweisung, Einweisung und für Lernprozesse im Umgang mit dem Arbeitsmittel genutzt werden können, und gegebenenfalls entsprechende Maßnahmen einleiten.
- Überprüfen, wie das smarte Arbeitsmittel die Betriebs- und Datensicherheit in vernetzten Prozessen beeinflusst (zum Beispiel vernetzte Arbeitsmittel im Betrieb und innerhalb der Wertschöpfungskette).
- Informieren, wie das smarte Arbeitsmittel mit den personenbezogenen Daten umgeht, und Datenschutz gewährleisten.
- Informieren, wie das smarte Arbeitsmittel gegen Fremdzugriffe geschützt ist, Datensicherheit gewährleisten.
- Vom Hersteller kurze und verständliche Informationen einfordern, welche Daten das smarte Betriebsmittel erfasst, wie und wo sie gespeichert und verarbeitet werden und wer Zugriff auf die Daten hat. › *Siehe Umsetzungshilfe 1.1.7 Informationsblatt smartes Produkt.*
- Überprüfen, welche Datenqualität für die Arbeitsaufgaben des smarten Arbeitsmittels erforderlich ist und wie das cyber-physische System diese Datenqualität gewährleisten kann, gegebenenfalls Unterstützung durch Fachleute wie Fachkräfte für Arbeitssicherheit oder IT-Experten einholen.
- Vereinbaren, an welchen Stellen die intelligente Software (inkl. KI) des Arbeitsmittels und an welchen der Mensch entscheidet und steuert, wie die Handlungsträgerschaft angezeigt und dokumentiert wird und Übergaberegelungen treffen.
- Prüfen, ob die Kompatibilität der intelligenten Software (inkl. KI) des smarten Arbeitsmittels mit den vorhandenen Systemen im Betrieb und gegebenenfalls innerhalb der Wertschöpfungskette gegeben ist, gegebenenfalls Aufwand für Anpassungen ermitteln.
- Softwaretechnisch sicherstellen, dass Betriebsmittel gegenüber Eingriffen Unbefugter abgeschottet sind.
- Sicherstellen, dass die intelligente Steuerungssoftware der Arbeitsmittel auch in Notfällen funktioniert, zum Beispiel zertifizierte Cloud-Dienstleister beauftragen, Notfallaggregate nutzen.
- Vor der Anschaffung empfiehlt sich die Durchführung einer Gefährdungsbeurteilung, um festzustellen, wo sicherheitstechnische Gefährdungen und gesundheitliche Belastungen auftreten können und welche Maßnahmen erforderlich sind, um den Aufwand für die Integration des smarten Arbeitsmittels abzuschätzen. › *Siehe Umsetzungshilfe 2.2.2 Gefährdungsbeurteilung 4.0.*
- Überprüfen, ob das smarte Arbeitsmittel und dessen intelligente Software (inkl. KI) gebrauchstauglich sind (Usability).
- *Bei neu vernetzten Arbeitsmitteln:* Bei intelligenter Software (inkl. KI) smarter Arbeitsmittel, die durch den Betrieb selbst programmiert oder angepasst wird und die zu wesentlichen Veränderungen führt, wird empfohlen, zusätzlich darauf zu achten, dass die Arbeitsmittel auch nach der Veränderung den Sicherheits- und Gesundheitsanforderungen (nach Maschinenrichtlinie) entsprechen und die Schutz- und Sicherheitseinrichtungen funktionsfähig sind.

Integration des smarten Arbeitsmittels

Bei der Integration des smarten Arbeitsmittels in den Betrieb sind zusätzlich zu den herkömmlichen Maßnahmen der Betriebssicherheit (nach Betriebssicherheitsverordnung) unter anderem folgende Maßnahmen hilfreich:

- Planen, wie das smarte Arbeitsmittel in die betrieblichen Abläufe integriert wird und welche organisatorischen Maßnahmen dazu erforderlich sind (zum Beispiel Arbeitsverfahren festlegen, Handlungsspielräume und Interventionsmöglichkeiten beschließen, Schnittstellenregelungen treffen, Organisationsabläufe und Kompatibilität mit Systemen bestimmen).
- Pilotierung des smarten Arbeitsmittels in begrenzten Bereichen.
- Die betroffenen Führungskräfte und Beschäftigten in die Planung von Maßnahmen und Arbeitsverfahren sowie in den Betrieb der smarten Arbeitsmittel einbinden. Dies ermöglicht die Berücksichtigung ihrer Erfahrungen und fördert ihre Akzeptanz für die neuen Arbeitsmittel .
- Mit Führungskräften und Beschäftigten Vereinbarungen treffen, wie mit personenbezogenen Daten aus dem Arbeitsmittel umgegangen wird (Lagerung, Speicherung, Auswertung, Nutzung, Löschung), gegebenenfalls unter Einbindung der Arbeitnehmervertretungen (Betriebs- und Personalräte).
- Führungskräfte und Beschäftigte in der Nutzung der smarten Arbeitsmittel unterweisen beziehungsweise hierfür qualifizieren.
- Einüben von Notfallprozeduren, um im Notfall geschult reagieren zu können.
- Aufbereitung und Filterung von Informationen für Beschäftigte, um Informationsfluten zu vermeiden und eine schnelle Reaktion sowie qualifizierte Bearbeitung eines Problems zu ermöglichen, entsprechende Programmierung des Systems.

Veränderung von Maschinen und Arbeitsmitteln zu smarten Arbeitsmittel

Bei der Veränderung von Maschinen und Arbeitsmitteln zu smarten Arbeitsmitteln muss geprüft werden, ob eine wesentliche Veränderung nach Maschinenrichtline vorliegt. Demnach muss eine neue Konformitätsbewertung durchgeführt werden, die auch die Überprüfung der funktionalen Sicherheit enthält. Hier sollte mit dem Hersteller zusammengearbeitet werden, auch um zu klären, welche Veränderungen wesentlich sind.[13]

- *Besondere Maßnahmen bei Anlagen nach Störfall-Verordnung:* Bei Anlagen nach Störfall-Verordnung[14] die intern und nach außen informationstechnisch durch 4.0-Technologien vernetzt werden, ist IT-Security Führungsaufgabe und integraler Bestandteil aller Errichtungsphasen von Anlagen und ihrer Integration in den Betriebsbereich bis zur Inbetriebnahme durch den Betreiber. Dies beginnt bei dem Konzept und der Planung der Anlage. Die Maßnahmen sind integraler Bestandteil der Systemfunktionen eines Betriebsbereiches.[15]

[13] ProdSG
[14] § 2 StörfallV
[15] KAS 44 (2017)

Quellen und weitere Informationsmöglichkeiten:

BetrSichV – *Betriebssicherheitsverordnung*, 18.10.2017.

BSI – Bundesamt für Sicherheit in der Informationstechnik (2018). *Glossar der Cyber-Sicherheit*. https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/cyberglossar/cyberglossar_node.html. Zugegriffen: 30.11.2018.

Bundesministerium für Wirtschaft und Energie (2013). *Mensch-Technik-Interaktion. Leitfaden für Hersteller und Anwender.* Berlin.

Deuse, J., Weisner, K., Hengstebeck, A., & Busch, F. (2015). Gestaltung von Produktionssystemen im Kontext von Industrie 4.0. In A. Botthoff, & E. A. Hartmann (Hrsg.), *Zukunft der Arbeit in Industrie 4.0* (S. 99–109). Berlin, Heidelberg: Springer Verlag.

Kagermann, H., Wahlster, W., & Helbig, J. (2013). *Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0. Abschlussbericht des Arbeitskreises Industrie 4.0.* Promotorengruppe Kommunikation der Forschungsunion Wirtschaft – Wissenschaft, acatech – Deutsche Akademie der Technikwissenschaften e. V. https://www.bmbf.de/files/Umsetzungsempfehlungen_Industrie4_0.pdf. Zugegriffen: 23.07.2018.

Kärcher, B. (2015). Alternative Wege in die Industrie 4.0 – Möglichkeiten und Grenzen. In A. Botthoff (Hrsg.), *Zukunft der Arbeit in Industrie 4.0* (S. 47–58). Berlin, Heidelberg: Springer Verlag.

KAS 44 (2017). *Leitsätze der Kommission für Anlagensicherheit zum Schutz vor cyber-physischen Angriffen*. Berlin: Kommission für Anlagensicherheit.

Liggesmeyer, P., & Trapp, M. (2014). Safety: Herausforderungen und Lösungsansätze. In T. Bauernhansl, M. ten Hompel, & B. Vogel-Heuser (Hrsg.), *Industrie 4.0 in Produktion, Automatisierung und Logistik* (S. 433–450). Wiesbaden: Springer Fachmedien.

ProdSG – *Produktsicherheitsgesetz*, 31.08.2015.

Robelski, S. (2016). *Psychische Gesundheit in der Arbeitswelt. Mensch-Maschine-Interaktion.* Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (BAuA). https://www.baua.de/DE/Angebote/Publikationen/Berichte/F2353-4d.pdf?__blob=publicationFile&v=4. Zugegriffen: 23.07.2018.

Schmauder, M., Höhn, K., Jung, P., Lehmann, K., Paritschkow, S., Westfeld, P., & Sardemann, H. (2016). *Sichere Personenerkennung in der Mensch-Maschine-Interaktion*. Dortmund, Berlin, Dresden: Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (BAuA). https://www.baua.de/dok/8480166. Zugegriffen: 21.07.2018.

StörfallV – Zwölfte Verordnung zur Durchführung des Bundes-Immissionsschutzgesetzes (Störfall-Verordnung – 12. BImSchV), 8.12.2017 Zittlau, K. (2018). Sicherheit in der Arbeitswelt 4.0. In O. Cernavin, W. Schröter, & S. Stowasser (Hrsg.), *Prävention 4.0* (S. 269–286). Wiesbaden: Springer Verlag.

Zu diesem Thema könnten Sie auch folgende weitere Umsetzungshilfen interessieren:

- 1.1.7 Informationsblatt smartes Produkt
- 1.3.3 Handlungsträgerschaft im Verhältnis Mensch und intelligente Software (inkl. KI)
- 2.1.5 Beschaffung digitaler Produkte
- 2.2.2 Gefährdungsbeurteilung 4.0
- 2.3.1 Datensicherheit in 4.0-Prozessen
- 2.3.2 Datenschutz in 4.0-Prozessen
- 2.3.3 Datenqualität in 4.0-Prozessen
- 2.5.1 Anforderungen an eine Cloud
- 2.5.2 Cloud-Modelle der Bereitstellung und Dienstleistungen
- 3.1.6 Smarte Formen der Instandhaltung von Arbeitsmitteln
- 3.2.1 Technische Assistenzsysteme – allgemein
- 3.3.2 Gebrauchstauglichkeit der intelligenten Software (inkl. KI)

Herausgeber: „Offensive Mittelstand – Gut für Deutschland" – Stiftung „Mittelstand – Gesellschaft – Verantwortung"
Kurfürsten-Anlage 62, 69115 Heidelberg, E-Mail: info@offensive-mittelstand.de; Heidelberg 2019