



„Das Phänomen der Digitalisierung ist kein historisch neues Phänomen. [...] Die große Erzählung der Gegenwart ist jedoch darauf fokussiert, dass die Digitalisierung eine neue Qualität erreicht hat und die Welt der Erwerbsarbeit entscheidend verändern wird.“
Timpf, S. (2017) in: Die historische Dimension der Digitalisierung.

Digitalisierung und CSR II: Akzeptanz und Vertrauen in neue Technologien sicherstellen

Monika Eigenstetter

csr.impuls.papier no. 5.2

CSR Kompetenzzentrum Textil und Bekleidung Niederrhein. 2018

Inhaltsverzeichnis

Akzeptanz und Vertrauen in neue Technologien sicherstellen	2
1 Soziale Verantwortung im Kontext der Digitalisierung	2
2 Zum Verhältnis von Automation und Digitalisierung	2
2.1 Automatisierungslevel in Organisationen.....	2
2.2 Grade und Level der Automatisierung	3
3 Technikvertrauen und Technikakzeptanz	4
3.1 Technikvertrauen	4
3.2 Technikakzeptanz	6
4 „Risiken“ der Automation und Digitalisierung.....	7
4.1 Risikobetrachtungen.....	7
4.2 Klassische Sicherheitsrisiken der Automation: Safety	8
4.3 Risiko Psychische Gefährdungen.....	10
4.4 Risiken der IT-Sicherheit: Datenschutz und Datensicherheit	12
4.5 Weitere Risiken.....	13
5 Handlungsempfehlungen für sichere und akzeptierte Technologien	15
5.1 Ebenen der Gestaltung und das Mensch-Technik-Team berücksichtigen	15
5.2 Kognitive Ergonomie sicherstellen: Usability und User Experience	17
5.3 Kontrolle und Verantwortung ermöglichen.....	18
5.4 Kompetenzerhalt und -aufbau bei den Mitarbeitenden sicherstellen.....	20
5.5 Technikakzeptanz der Mitarbeitenden durch Partizipation und User Centered Design gewährleisten.....	20
6 Checklisten und Handlungshilfen für die Praxis.....	21
6.1 Mittelstand-Digital.....	21
6.2 Offensive Mittelstand: Mittelstand 4.0 – sichere und gesunde Digitalisierung ermöglichen	23
6.3 Bundesamt für Sicherheit in der Informationstechnik.....	24
6.4 Bitkom – vielfache Informationen rund um Digitalisierung	24
6.5 Einfach anfangen: Innovationsgutscheine und Digitalisierungsgutscheine in NRW	25
7 Quellen	26
8 Endnoten	30

Akzeptanz und Vertrauen in neue Technologien sicherstellen

1 Soziale Verantwortung im Kontext der Digitalisierung

Digitalisierung ist ein wichtiger Treiber von innovativen Geschäftsmodellen und gibt neue Impulse für eine gute und sichere Arbeit. Digitalisierung berührt dabei in vielerlei Hinsicht Themen der sozialen Verantwortung, seien es Möglichkeiten der Ressourceneffizienz, der Nachverfolgbarkeit von Produkteigenschaften in der Wertschöpfungskette, Belange der Kommunikation zum Kunden mit Themen des Datenschutzes und der Datensicherheit oder der Gestaltung sicherer und menschengerechter Arbeitsprozesse. Während sich viele Veröffentlichungen vorallem mit den Chancen der Digitalisierung in Bezug auf Ressourceneffizienz und Kundenkommunikation beschäftigen, nimmt die vorliegende eher die Risiken und die nicht-intendierten Nebenwirkungen in den Blick. Warum das? Ganz einfach: Gelingende Digitalisierung braucht Akzeptanz und Vertrauen seitens der Mitarbeitenden und der Kunden. Das vorliegende Papier „Akzeptanz und Vertrauen in neue Technologien sicherstellen“ möchte hierfür wichtige Anregungen geben, damit häufig auftretende Fehler verhindert werden und Verantwortung in automatisierten Systemen „nicht verloren“ geht¹. Denn erst sichere Automatisierung und Digitalisierung führt zu einem Wettbewerbsvorteil.

2 Zum Verhältnis von Automation und Digitalisierung

Automation meint im Allgemeinen ein Agieren von Maschinen, Plattformen oder anderen technischen Systemen unabhängig von einer menschlichen Interaktion. Eine frühe Form der Automation waren mechanische Maschinen¹. Heute umfassen die Techniken der Automatisierung „soft- und hardwaretechnische Konzepte, Methoden, Werkzeuge, Produkte und Lösungen zur Steuerung und Regelung sowie zum selbstablaufenden (automatisierten) oder teilweise selbstablaufenden (teilautomatisierten) Betrieb eines Prozesses einschließlich Planung, Entwurf und Umsetzung“². Digitalisierung ist damit ein bedeutender Teil der Automation.

2.1 Automatisierungslevel in Organisationen

Die neue besondere Qualität der so genannten Industrie 4.0 umfasst die Entwicklungen hin zu einem Produktionsumfeld, welches aus intelligenten, sich selbst steuernden Objekten, besteht: Cyber-Physische Systeme (Cyber-Physical Systems, CPS). Die mit dezentralen Steuerungen ausgestatteten Objekte, nämlich Anlagen, Arbeitsmittel und Produkte, sollen sich – im Idealfall völlig selbstständig – durch die gesamte Wertschöpfungskette von der Auftragsgenerierung beim Kunden über die verschiedenen Prozessschritte der Produktion bis hin zum Kunden selbst organisieren.

¹ Ich bedanke mich bei Leonie Heckmanns und Thomas Langhoff für wertvolle Anmerkungen und Ergänzungen in diesem Text.

Die Automationsprozesse im Organisationskontext werden oft als Pyramide dargestellt, die fünf Ebenen umfasst (Abbildung 1). Die erste Ebene betrachtet die Schnittstellen zum Menschen (Device Level), die zweite Ebene Maschinen- und Computer-Kontrolleinheiten (Control Level), die nächste Ebene betrifft die Produktionssysteme (Fertigungssysteme; MES, Management/Manufacturing Execution System Level), die darüber liegende Ebene beinhaltet die Planung der Unternehmensressourcen (ERP, Enterprise Resource Planning Level), die höchste Ebene vernetzt verschiedene Unternehmen (Multienterprise Network Level). Die beteiligten Akteure reichen, je nach Level, von den Maschinenbedienern (Operateure, Operators) über Vorgesetzte zu Kunden oder Lieferanten³. Da Automation und Digitalisierung im Produktionskontext zunehmend verschmelzen, werden sie bei der folgenden Erläuterung ihrer Wirkungen auf den Menschen nicht weiter unterschieden. Viele dieser Wirkungen werden aktuell unter dem Begriff der Arbeit 4.0 diskutiert.

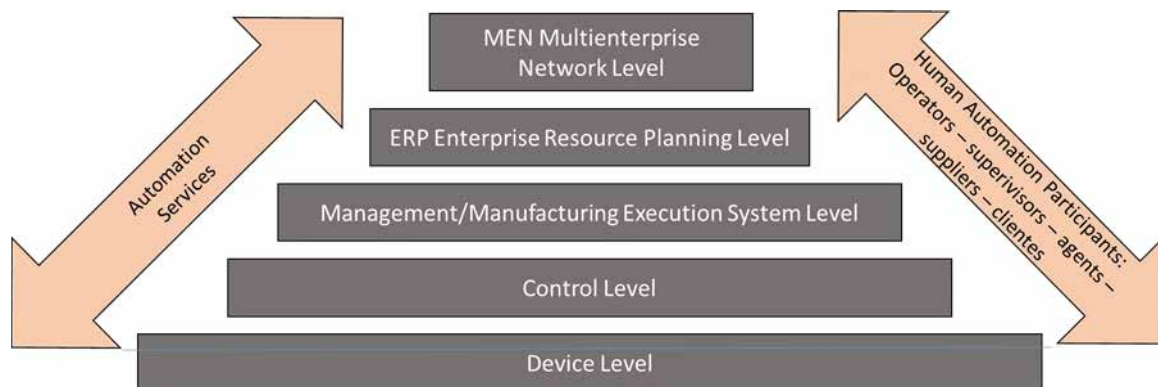


Abbildung 1. Automatisierungspyramide (nach Nof, 2009)

Es kann auch nach Domänen der Automation und Digitalisierung unterschieden werden: Landwirtschaft, Banking, Chemische Industrie, Kommunikation/Presse, Konstruktion, Design, Energieerzeugung, Medizin, Logistik, Haustechnik, Freizeitgestaltung usw.⁴. Es gibt praktisch keinen Bereich, der nicht von Automation und Digitalisierung betroffen wäre.

2.2 Grade und Level der Automatisierung

Im Kontext der Arbeitswissenschaft und Human Factors Forschung werden Ausmaß (Degree) und Level (Level) der Automation unterschieden. DIN IEC 60050-351, das internationale elektrotechnische Wörterbuch für Leittechnik, bezeichnet als Automatisierungsgrad den Anteil, den automatisierte Funktionen an der Gesamtfunktion eines Systems oder einer technischen Anlage haben. Ein vollautomatischer Betrieb liegt erst dann vor, wenn alle Funktionen des betrachteten Systems – ausgenommen Ein- und Ausschaltvorgänge – automatisiert sind. Degrees of Automation (DOA) reichen von „keine Automation“ bzw. manuelle Ausführung über Assistenzsysteme und Teilautomatisierung bis hin zu vollautomatisierten Systemen und werden, je nach Autor oder Branche, in fünf oder mehr Stufen unterschieden. Im Kontext des autonomen Fahrens unterscheidet z.B. BASf (2012) fünf Autonomiegrade der Maschine (resp. des Autos): manuell, assistiert, teilautomatisiert, hochautomatisiert und autonom.⁵

Das Level der Automatisierung (LOA) dagegen wird durch die vier Stufen der menschlichen Handlungsabfolge beschrieben, nämlich (1) Informationsaufnahme, (2) Informationsanalyse, (3) Entscheidungsauswahl und (4) Handlungsausführung⁶ (siehe Abbildung 2). Auf jedem Level der menschlichen Handlungsabfolge (LOA) ist prinzipiell jede Form der Automatisierung (DOA) möglich.

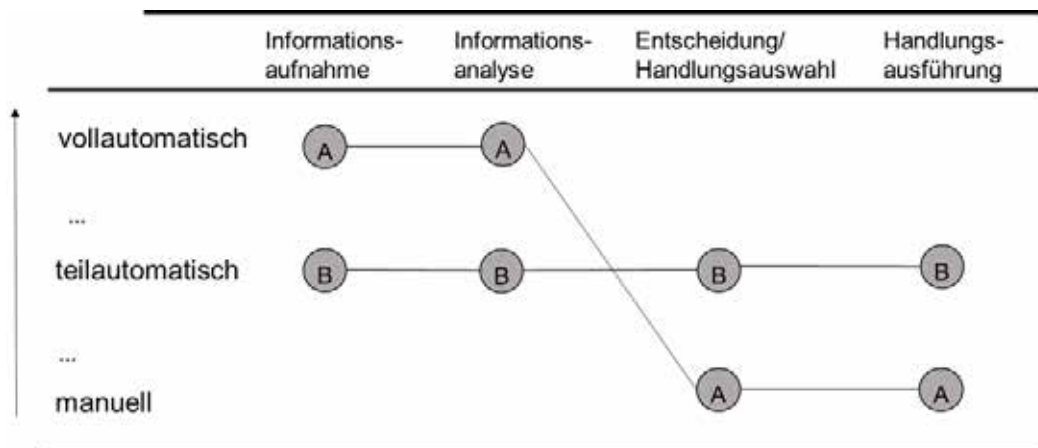


Abbildung 2. Technische Systeme mit unterschiedlicher Kombination aus Grad (DOA) und Level der Automatisierung (LOA) (adaptiert nach Parasuraman et al., 2000). Automat A agiert vollautomatisiert auf den Ebenen der Informationsaufnahme und Verarbeitung. Entscheidung und Auswahl sowie Handlungsausführung verbleibt vollständig beim Menschen. Bei Automat B sind alle Handlungsschritte teilautomatisiert.

3 Technikvertrauen und Technikakzeptanz

Akzeptanz und Vertrauen in Automation und Digitalisierung basieren auf einer Technikgestaltung, die neben psychischen und physiologischen Voraussetzungen die kognitiven Leistungen des Menschen berücksichtigt. Es sind höchste Anforderungen an eine menschengerechte und nutzerfreundliche Technikgestaltung zu stellen, um Vertrauen und Kontrolle im sozio-technischen System aufrecht zu erhalten. Zwei Modelle sollen hier vorgestellt werden, die die Einflussfaktoren von (1) Technikvertrauen und (2) Akzeptanz in die Technik umfassend beschreiben. Allen Modellen gemeinsam ist aber der Verweis auf die „Einfachheit in der Nutzung“, was auf die große Bedeutung von Nutzerfreundlichkeit und User Experience verweist. Diese Faktoren werden im Abschnitt 4.2 eigens betrachtet.

3.1 Technikvertrauen

Technikvertrauen ist in vielen Kontexten von Bedeutung: sei es der Einsatz von automatisierten Kassen im Supermarkt, sei es die Nutzung des Smartphones als Zahlungsmittel oder ein 3D-Scan, der als Vorlage für ein individuell angepasstes Schnittmuster dient. In allen diesen Kontexten geht die Nutzerin bzw. der Nutzer der Technologie in eine riskante Vorleistung, da ggf. nicht bekannt ist, wie die spezielle Technologie funktioniert, und ob die gewünschten Leistungen tatsächlich im erwünschten Sinn erfolgen: Nutzende erlernen die Verlässlichkeit eines Systems erst in der Interaktion mit dem System zu beurteilen.

Hoff und Bashir⁷ erarbeiten ein Modell, das sowohl das Anfangsvertrauen in Technik vor der ersten Interaktion beschreibt (initiales Vertrauen) als auch die weitere Vertrauensentstehung aufgrund der Erfahrungen mit dem jeweiligen System (Abbildung 3). Faktoren des Vertrauens in Technik liegen teilweise in der Person selbst, so durch Alter, Geschlecht und Vorerfahrung mit Technologien der Automation und Digitalisierung allgemein.

Wichtiger aber sind Faktoren der Gestaltung des technischen Systems: Sie werden nach Designmerkmalen und Systemperformanz unterschieden:

- Designmerkmale beschreiben einerseits Aspekte, die sich unter „Anmutungsqualität“ und Nutzerfreundlichkeit fassen lassen: Aussehen, Einfachheit in der Nutzung und Feedback über erfolgte Eingaben, aber auch Höflichkeit in der Kommunikation: Wie werden Nutzer aufgefordert, den nächsten Systemschritt zu unternehmen? Oder: Wie freundlich ist die Fehlermeldung formuliert? Kontrolle dagegen ergibt sich über die Eingriffsmöglichkeiten ins System.
- Systemperformanz umfasst dagegen Faktoren der Systemzuverlässigkeit und Betriebssicherheit oder die Akkuratheit von Fehlermeldungen: Wie häufig treten z.B. Fehlermeldungen auf, obwohl keine Fehler vorhanden sind? Wie viele Fehlzustände des technischen Systems gibt es, obwohl kein Alarm ausgelöst wurde.

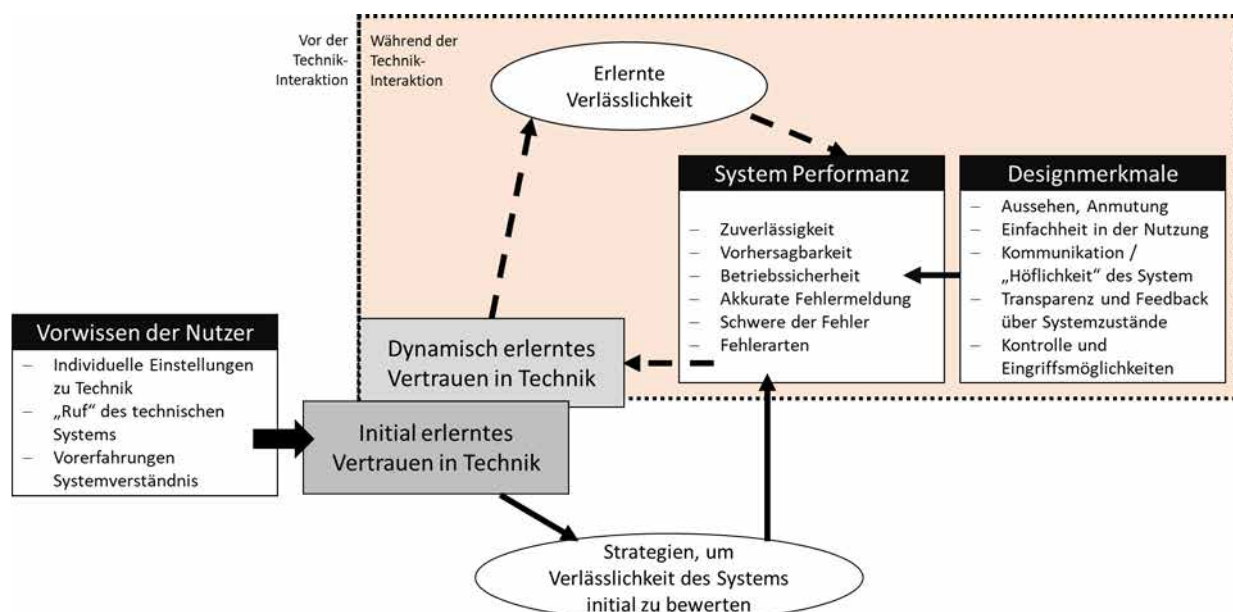


Abbildung 3. Vertrauen in Technik (geringfügig modifiziert nach Hoff und Bashir, 2014)

3.2 Technikakzeptanz

Technikakzeptanz ist von Technikvertrauen zu unterscheiden: Es ist nicht das gleiche. Es kann gut sein, dass man Vertrauen in bestimmte Technologien hat, z.B. in die Zuverlässigkeit eines Webshops einer Firma. Da aber das Produkt der Firma nicht benötigt wird oder andere Alternativen vorhanden sind, die komfortabler und vertrauter sind, wird die Technik nicht genutzt. So sind z.B. Bestellautomaten in Kinos oder Fast-Food-Restaurants, obwohl nutzerfreundlich gestaltet, im Vergleich zu den mit Menschen besetzten Kassen immer noch vergleichsweise wenig akzeptiert. Andere Technologien wie SMS oder WhatsApp haben sich dagegen in Windeseile durchgesetzt, obwohl man weiß, dass gerade Whatsapp wichtige Aspekte der Datensicherheit nicht erfüllt.

Es gibt unterschiedliche Möglichkeiten, Technikakzeptanz zu beschreiben und zu erfassen. So kann Technikakzeptanz z.B. als Grad der Nutzung oder der Marktdurchdringung definiert werden.⁸ Andere Autoren beschreiben Stufenmodelle von aktiver Gegnerschaft bis zustimmendes Wohlwollen und ein Engagement für die Technik. Andere stellen Technikakzeptanz als einen Prozess dar, der neben externen Einflussvariablen über den wahrgenommenen Nutzen und die Einfachheit der Bedienung eine positive Einstellung und die tatsächliche Nutzung beinhaltet (z.B. das TAM- Modell⁹).

Ein etabliertes und mehrfach erweitertes Modell stammt von Venkatesh et al.¹⁰: Unified Theory of Acceptance and Use of Technology (UTAUT). UTAUT ist ein Prozessmodell, das sich durch mehrere Facetten charakterisiert: Haupteinflussfaktoren für eine beabsichtigte und eine darauffolgende tatsächliche Nutzung einer Technologie sind erwarteter Nutzen, Einfachheit der Nutzung, sozialer Einfluss und förderliche Bedingungen. Zudem spielen Merkmale der Nutzenden eine Rolle: Alter, Geschlecht, Erfahrung und Freiwilligkeit der Nutzung eine Rolle (Abbildung 4).

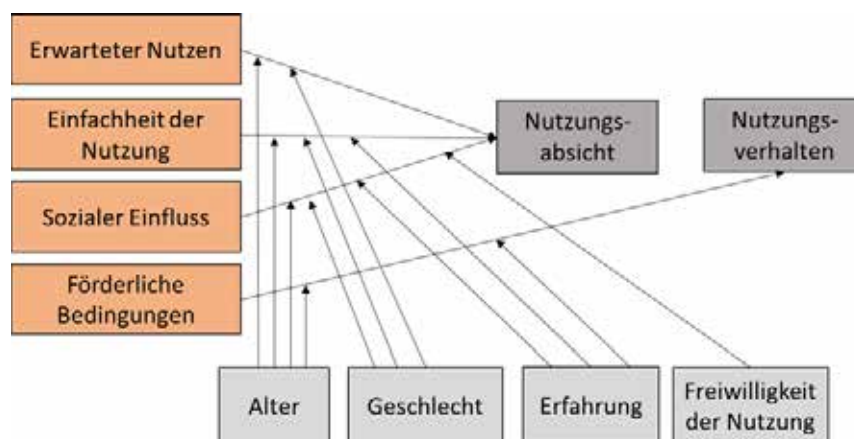


Abbildung 4. Unified Theory of Acceptance and Use of Technology UTAUT (Venkatesh et al., 2003)

Das Modell UTAUT von 2003 wurde um weitere Faktoren erweitert, so z.B. hedonische Motivation, das Preis-Leistungsverhältnis oder Gewohnheiten. Es wurde als UTAUT 2 eingeführt.¹¹

4 „Risiken“ der Automation und Digitalisierung

Automation und Digitalisierung ist für eine hohe Wertschöpfung unabdingbar: Es ist jedoch erforderlich, sich auch mit den Risiken der Digitalisierung auseinander zu setzen, denn Akzeptanz und Vertrauen in Technik lassen sich nur dann sicherstellen, wenn typische Gestaltungsfehler der Automation und Digitalisierung umgangen werden. Es gehört zu einem guten Risikomanagement, sich mit bekannten möglichen negativen Wirkungen der Digitalisierung zu befassen, denn Automation und Digitalisierung erfolgen leider noch zu häufig unter dem Primat des technisch Machbaren, nicht unter dem Primat einer „menschengerechten“ Technikgestaltung. Das heißt konkret: Der Mensch wird häufig als menschlicher Fehler (Human Error) betrachtet und „verkommt zur Restgröße“ im soziotechnischen System. Wenn aber der Mensch im System nicht angemessen mitgedacht wird, drohen Kompetenzverluste und andere Ironien der Automatisierung¹² (Abschnitt 4.2).

Für eine „gute“ Automation und Digitalisierung braucht es also Gestaltungskonzepte, die bewährtes arbeits- und ingenieurwissenschaftliches Knowhow berücksichtigen und Sicherheit gewährleisten. Dabei werden heute mindestens zwei Bereiche der Sicherheit in der vernetzten Produktion berücksichtigt: Safety umfasst die Aspekte der funktionalen und technischen Sicherheit, d.h. Maschinen- und Anlagensicherheit, während Security als „Angriffssicherheit“ IT-Sicherheit und Objektschutz im Visier hat.¹³

4.1 Risikobetrachtungen

Es ist Führungsaufgabe, Risiken an Maschinen zu bewerten und Maßnahmen zur Risikominimierung abzuleiten und durchzuführen. ISO 31000 stellt einen Managementleitfaden bereit, um Risiken zu erkennen, zu vermeiden und sie abzufedern. Zu einem Risikomanagement gehören typischerweise:

- Identifikation der Risiken
- Analyse der identifizierten Risiken hinsichtlich ihrer Auftretenswahrscheinlichkeiten, Schadenspotenziale und Chancen
- Risikobewertung durch Vergleich mit Kriterien der Risiko-Akzeptanz: akzeptables Restrisiko
- Risikobewältigung/Risikobeherrschung durch Maßnahmen, die Gefahren und/oder Eintrittswahrscheinlichkeiten reduzieren oder die Folgen beherrschbar machen
- Risikocontrolling mittels Indikatoren, die eine Beurteilung aktuellen Risiken erlauben
- Dokumentation des Vorgangs

Vier Standardstrategien werden beschrieben, um Risiken zu kontrollieren¹⁴

- Vermeidung bei hoher Schadenshöhe und hoher Eintrittswahrscheinlichkeit
- Verminderung bei hoher Schadenshöhe und niedriger Eintrittswahrscheinlichkeit
- Überwälzung bei niedriger Schadenshöhe und hoher Eintrittswahrscheinlichkeit
- Akzeptanz bei niedriger Schadenshöhe und niedriger Eintrittswahrscheinlichkeit

Ein Problem der Risikobewertung ist, dass Menschen – aufgrund der Besonderheiten der menschlichen Informationsverarbeitung – diese typischerweise falsch einschätzen: z.B. die Vertrautheit mit spezifischen Risiken und Gewohnheiten können die Wahrnehmung und Bewertung verzerren¹⁵: Vorsicht also vor allzu schnellen Entscheidungen!

Vier Risikobereiche der Automation und Digitalisierung werden nachfolgend betrachtet (Abbildung 5), nämlich:

- die klassischen Sicherheitsrisiken (Safety), die durch Ironien der Automatisierung entstehen,
- Risiken durch psychische Belastung und Beanspruchung,
- Risiken der Security, (z.B. Sind die Unternehmensdaten ausreichend gegen Diebstahl geschützt?) und
- weitere Risiken, die z.B. selbstlernenden Maschinen inhärent sind. Technische Lösungen müssen auch daraufhin untersucht werden, ob ihr Einsatz nicht mit grundlegenden gesellschaftlichen Werten kollidiert (z.B. Werden bestimmte Kundengruppen systematisch benachteiligt?)

Mit diesen Fragen werden Aspekte der Menschenrechte berührt, nämlich basale Rechte der Gleichbehandlung (Nichtdiskriminierung) oder der informationellen Selbstbestimmung (Datenschutz).



Abbildung 5. Häufige Risiken der Automatisierung und Digitalisierung

Gefahren durch Automatisierung und Digitalisierung, die z.B. in Luftfahrt, Energiewirtschaft und anderen Hochsicherheitsbranchen hinlänglich bekannt sind, sollten heute in allen Branchen sowie in den KMU zumindest in den Grundzügen klar sein, da sonst Ineffizienz, Qualitätsverluste oder andere weitreichende Schäden drohen. Viele der Probleme sind jeder oder jedem Nutzenden aus der Nutzung von Verkehrsassistenzsystemen zumindest ansatzweise bekannt. Vergleichbare Probleme treten in allen automatisierten Systemen auf.

4.2 Klassische Sicherheitsrisiken der Automation: Safety

Vier Ironien der Automatisierung wurden schon von Brainbridge im Jahr 1983 formuliert¹⁶: oft werden sie auch als Paradoxien von Automation und Digitalisierung bezeichnet. Diese Risiken sind im Betrieb der Technologien, so z.B. in der Produktion von Bedeutung.

1. Die Betrachtung des Menschen als wesentliche Fehlerquelle führt dazu, dass man versucht, ihn weitgehend aus dem soziotechnischen System zu entfernen. Da aber der Entwickler oder die Entwicklerin selbst ein Mensch ist, besteht die große Gefahr, dass die Fehler im Designprozess entstehen: so mag eine fehlende Nutzerfreundlichkeit der Systeme Fehlbedienungen geradetz herausfordern. Eine fehlende Rückmeldung von Systemen führt z.B. dazu, dass man Systemanforderungen mehrfach ausführt, „weil man sich nicht sicher ist“.

2. Die Tätigkeiten, die nicht gut und kosteneffizient automatisierbar sind, werden weiterhin von Menschen übernommen. Es sind dann u.a. die anspruchsvolleren und komplexen Aufgaben, die beim Menschen verbleiben, z.B. visuelle Kontrolltätigkeiten.
3. Man ersetzt den Menschen durch automatisierte Systeme, überträgt ihm aber im Notfall doch wieder die Kontrolle und die Notwendigkeit, um die auftretenden Fehler zu beheben.
4. „Die zuverlässigsten Automatisierungssysteme erfordern den höchsten Aufwand an Trainingsmaßnahmen“¹⁷, weil die aktive Auseinandersetzung mit dem technischen System fehlt: Ohne Training keine Sicherheit!

Auswirkungen unzureichend gestalteter Technik auf effektives Handeln sind hinreichend aus dem Kontext von Hochsicherheitsorganisationen bekannt, die schon lange viele Bereiche automatisiert und digitalisiert haben (so Luftfahrt oder Kerntechnik).¹⁸ Typische Beispiele für diese Probleme sind:

- Durch *Automation erzeugte Fehler* kennen etliche Nutzende von Navigationsgeräten.¹⁹ Manchmal sind die Updates zu spät auf einem Gerät vorhanden, oder das GPS-Signal geht verloren, so dass neue Einbahnstraßen oder Straßenführungen falsch angezeigt werden. Manchmal zeigen Navigationssysteme zu spät einen notwendigen Spurwechsel an, der dann zu manch riskantem Fahrmanöver führt.
- Ein *zu geringes Vertrauen in Automation* kann entstehen, wenn z.B. die Sensoren häufig Fehler melden, aber keine Fehler vorhanden sind. Das kann passieren, wenn die Sensorik daraus aufgelegt ist, alle auftretenden Fehler oder kritischen Zustände zu entdecken und anzuzeigen. Dies führt aber gleichzeitig dazu, dass auch viele Fehlalarme auftreten, ohne dass tatsächlich ein Fehler oder kritischer Zustand vorliegt. Die wiederholte Erfahrung mit Fehlalarmen führt schnell dazu, dass Nutzende die auftretenden Alarme teilweise oder gänzlich ignorieren, auch weil sie nicht verstehen, wie und warum das technische System die Alarme erzeugt.²⁰

Schlägt ein Navigationsgerät zu häufig alternative Routen vor, auch wenn Staus sich schnell auflösen würden, verliert man das Vertrauen in die Zuverlässigkeit des Gerätes. Automaten oder Software stellen oft nicht ausreichend Informationen bereit, die Entscheidungen eines Systemzustandes erkennbar machen. So ist für Nutzende oft nicht nachvollziehbar, warum ein Navigationssystem eine Routenänderung vorschlägt und was diese Routenänderung eigentlich beinhaltet. Dies beeinträchtigt Vertrauen und Akzeptanz der Nutzenden.

- Ein *übersteigertes Vertrauen in Automation* hat einen anderen Effekt. Es gibt unzählige Beispiele, in denen Nutzer dem Navigationsgerät zu sehr vertrauten und vollständig in die Irre geführt wurden. (Suchen Sie nur im Internet: Blindes Vertrauen Navigationsgerät).
- Digitalisierung führt zu einem *Verlust an Kompetenzen*²¹: Junge Erwachsene verlernen zunehmend aufgrund allseits verfügbarer Navigationssysteme, die Fähigkeit, Straßenkarten zu lesen. Fähigkeitsverluste durch Automation und Digitalisierung, im Kontext des Autofahrens oft belächelt und Stoff für Anekdoten, führen im Kontext der Produktion zu ernststen Qualitäts- und Sicherheitsproblemen.
- *Verhaltensänderungen* treten auf, so z.B. Risikokompensation. Wenn ein soziotechnisches System als sehr sicher empfunden wird, neigen Menschen dazu, sich eher riskant zu verhalten.²² Als Beispiel: Vertrauen Menschen in gute Bremsen

und in technische Sicherheitssysteme wie ABS und EPS, neigen sie dazu, risikoreicher zu fahren.

- Automatisierte Systeme können zu einem *Verlust an Situationsbewusstsein* (Situation Awareness) führen, d.h. einem Verlust an Verstehen, was in einer Situation gerade passiert. Situationsbewusstsein ist ein Zustand, den man benötigt, um sich in dynamischen Interaktionen sicher verhalten zu können: sei es Auto zu fahren, mit kollaborierenden Robotern zu arbeiten oder Leitstände zu überwachen. Situationsbewusstsein ist ein Konstrukt, mit dem man die menschliche Fähigkeit beschreibt, (1) Informationen aufzunehmen, (2) diese zu integrieren: „Wie ist die aktuelle Situation zu verstehen?“ und (3) darauf aufbauend zukünftige Systemzustände „Was passiert als nächstes?“ vorherzusagen.²³

Derartige Risiken sind genauso als Bestandteil der Gefährdungsanalysen am Arbeitsplatz nach §5 Arbeitsschutzgesetz zu betrachten wie Risiken durch Lärm, Staub, zu hohe Lasten usw. (vergleiche dazu auch die TRBS 1151, Technische Regeln für Betriebssicherheit für Gefährdungen an der Schnittstelle Mensch - Arbeitsmittel – Ergonomische und menschliche Faktoren, Arbeitssystem) und die Broschüre der Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (siehe dazu die Website der BAUA, Stichwort „Arbeitsgestaltung im Betrieb“).

4.3 Risiko Psychische Gefährdungen

Unter „Belastungen“ versteht man nach DIN EN ISO 10075 die Gesamtheit der Einflüsse, die bei der Arbeit auf den Menschen einwirken, während „Beanspruchungen“ die individuelle und unmittelbare Auswirkung der Belastung auf den Menschen bezeichnet. Beanspruchungen sind demnach die im Menschen auftretenden Reaktionen auf Belastungen. Das bedeutet auch: Gleiche Belastungen können bei verschiedenen Menschen zu unterschiedlichen Beanspruchungen führen. Was das konkret meint? Beanspruchungen durch IT-Programme überfordern einige Mitarbeitende oder Kunden, während andere sich gerne und sofort mit dem System vertraut machen und sich über die Neuerung freuen.

Psychische Belastungen durch technische Systeme können zu einigen negativ bewerteten psychischen Beanspruchungen führen:

- Schon heute gibt es viele vollautomatisierte Systeme, die nur noch von Menschen überwacht werden müssen; z.B. automatisierte Passkontrollen im Flugverkehr oder Anlagenüberwachung im Bereich der chemischen Industrie. Über Kameras, Anzeigetafeln und Leitstände behält der Operator „das Ganze“ im Blick. Hier kann Daueraufmerksamkeit zu einem „Absinken der Wachheit“ und einem Monotonie-Erleben führen.
- Technische Systeme erfordern häufig eine genaue Abfolge von Schritten und wenn fehlerhafte Eingaben resultieren, kommt man nicht zum Ziel. Das erzeugt „Stress“ bei Kunden und Mitarbeitenden. Während sich aber Kunden meist für einen Anbieter mit besser gestalteten Systemen entscheiden können, sieht es im Bereich der Arbeit oft nicht gut für die Beschäftigten aus. Schöpferische Anteile der Arbeit gehen zunehmend verloren und der Mensch sieht sich verstärkt fremdbestimmt und unter technischer Kontrolle.

Psychische Gefährdungen, d.h. negative Auswirkungen auf die Gesundheit der Betroffenen, entstehen z.B. durch ein Zuviel oder ein Zuwenig an Belastungsfaktoren in der Arbeit. Zu wenig anspruchsvolle Tätigkeiten gehen z.B. mit Monotonie und verminderten

Reaktionszeiten einher. Ein Zuviel an informativischer Belastung durch digitalisierte Systeme korrespondiert dagegen mit Ermüdung und Sättigung. Langanhaltender hoher Zeitdruck, häufige Störungen und Unterbrechungen bei der Arbeit, monotone Tätigkeiten oder fehlende Erholungsmöglichkeiten können die Gesundheit beeinträchtigen. Um also Sicherheit, Gesundheit und Wohlbefinden der Arbeitnehmenden am Arbeitsplatz sicherzustellen, müssen technische Systeme an die physischen und psychischen Fähigkeiten des Menschen angepasst werden. Einen umfassenden Überblick über die gesundheitlichen Auswirkungen in Mensch-Maschine-Interaktionen gibt Robelski (2016).

Für einen allgemeinen Überblick zu psychischen Gefährdungen empfiehlt sich z.B. Joiko et al. (2010). GDA Psyche 2017 hat einen Leitfaden mit Kriterien zur Erfassung psychischer Belastungen und Beanspruchungen entwickelt. Psychische Gefährdungsanalysen sind integraler Bestandteil der Gefährdungsanalysen nach §5 Arbeitsschutzgesetz (vergleiche dazu auch die TRBS 1151).

Die Checklisten zur Erfassung der Fehlbeanspruchungsfolgen – ChEF enthalten kurze Fragebögen, um negative Beanspruchungsfolgen zu bewerten.

- https://resilienzforum.net/wp-content/uploads/2017/06/Checklisten_Baua.pdf
- <https://resilienzforum.net/wp-content/uploads/2017/06/Checkliste2-Psychische-Ermuedung.pdf>
- <https://resilienzforum.net/wp-content/uploads/2017/06/Checkliste4-Psychische-Saettigung.pdf>
- <https://resilienzforum.net/wp-content/uploads/2017/06/Checkliste3-Monotonie.pdf>
- <https://resilienzforum.net/wp-content/uploads/2017/06/Checkliste1-Stress.pdf>

Besondere Gefährdungen entstehen auch durch die sogenannte entgrenzte Arbeit, nämlich die permanente Verfügbarkeit von Führungskräften und Mitarbeitenden über die digitalen Medien. Gefährlich ist die Unmöglichkeit, auch mal einfach „abzuschalten“: Digital Detox gilt als eine zu unterstützende neue Fähigkeit.

Die größten psychischen Belastungen werden zukünftig nicht durch Situationen der Unforderung auftreten, sondern durch Situationen der Störungsbeseitigung in digitalisierten und automatisierten Systemen. Arbeitsbedingungen stellen sich dann als fachliche Überforderung in einer Kombination aus nicht angemessener Qualifikation, Zeitdruck, Überkomplexität der Situation etc. dar. Zudem wird auch nicht eine einzelne Person mit Hybridqualifikation Problemlöser sein können, sondern es werden mehrere Personen mit unterschiedlicher Qualifikation in Stresssituationen miteinander kooperieren müssen. Die unterschiedlichen Qualifikationen selbst schon können Stressoren sein, wie jeder weiß, der in interdisziplinären Teams arbeitet. Soziale Fähigkeiten und Konfliktmanagement werden für die Problemlöser essentiell sein ²⁴.

4.4 Risiken der IT-Sicherheit: Datenschutz und Datensicherheit

Ca 70% der deutschen Unternehmen sind jedes Jahr Zielscheibe von Attacken von Datendiebstahl, Industriespionage und Sabotage²⁵. Maßnahmen der Security verhindern, dass ein Unternehmen von Dritten geschädigt wird, sei es durch Wirtschaftsspionage oder Datendiebstahl von Mitarbeitenden innerhalb eines Unternehmens. Auch politisch motivierte Straftaten sind zu verhindern²⁶. Daneben gibt es viele Risiken, die einfach durch Unachtsamkeit und fehlerbehaftete Prozesse entstehen können. Gerade in hochgradig vernetzten Systemen bestehen viele Schwachstellen, die betrachtet werden müssen. Ein Beispiel ist der bekannte Fall eines Neusser Krankenhauses, in dem durch einen Hackerangriff sämtliche Zugänge zu Patentdaten verhindert wurden (Ransomware-Vorfälle). Manchmal ist es auch ein USB-Stick, der Spionage-Software überträgt.

Wenn die funktionale Sicherheit beeinträchtigt werden kann, sollten Security und Safety im Sinne eines Risikomanagements gemeinsam betrachtet, auch um möglicherweise auftretende Zielkonflikte zwischen Safety und Security zu beachten.²⁷

Der Leitfaden der DGUV zu Safety und Security in der vernetzten Produktion²⁸ unterscheidet

- Maschinen mit kontaktbehafteten Steuerungen: Sie benötigen keine besondere Risikobetrachtung in Bezug auf Security.
- Maschinen mit elektronischen Steuerungen: Sie gelten ebenfalls unproblematisch in Bezug auf IT-Sicherheit.
- Maschinen mit programmierbaren Steuerungen (SPS- oder Mikroprozessorsysteme): Hier bestehen Gefahrenpunkte – vor allem dann, wenn die Maschinensteuerungen mit Netzwerkverbindungen zu übergeordneten Rechnersystemen ausgestattet sind. Dann sollten die Risiken bewertet und eine ganze Reihe von Sicherheitsmaßnahmen umgesetzt werden. Die DGUV schlägt z.B. eine Zonenaufteilung, d.h. eine Netzsegmentierung, vor, so dass im Schadensfall nicht alle Produktionsmaschinen gleichzeitig infiziert werden. Authentisierung und Autorisierung, ein permanentes Monitoring und Sicherungen mittels Backups sind einige weitere Forderungen.

Bei IT- oder Cyber-Security ist neben der Informationssicherheit (produktions- oder dienstleistungsbezogene Daten) ein weiteres Themenfeld zu betrachten: der Datenschutz (personenbezogene Daten)²⁹. Digitale Geschäfts- und Produktionsprozesse können langfristig nur auf Basis des Vertrauens in den Datenschutz funktionieren³⁰:

Datensicherheit und Datenschutz erfordern:

- 1) Vertraulichkeit der Daten (Schutz vor Preisgabe der Daten)
- 2) Verfügbarkeit der Daten zum erforderlichen Zeitpunkt
- 3) Datenintegrität: Vollständigkeit und Unveränderlichkeit der Daten

Kunden verlassen sich darauf, dass ihre Daten bei den Unternehmen, bei denen sie einkaufen, sicher sind. Der aktuell bekannt gewordene Fall, in dem tausende Sprachdateien von Alexa in die falschen Hände gerieten, macht einige Probleme deutlich.

Ein Leitfaden zum Risikomanagement der Datensicherheit findet sich auf den Seiten des Bundesamts für Sicherheit in der Informationstechnik. Das Bundesamt bietet mit dem BSI-Standard 200-3: „Risikomanagement. Risikoanalyse auf der Basis von IT-Grundschutz“ eine einfache und doch umfassende Darstellung der risikobezogenen Arbeitsschritte bei der Umsetzung des elementaren IT-Grundschutzes.

Neben den technischen sind nicht-technische Vorkehrungen zu treffen, die die Rechte der Kunden und Mitarbeitenden auf informationelle Selbstbestimmung berühren. Kenntnisse über Verschlüsselung und Pseudonymisierung von Daten oder organisatorische Vorkehrungen, die den Zugang zu Daten beschränken, müssen im Unternehmen vorhanden sein.³¹

Piko und Bertram³² verweisen darauf, dass die größten Sicherheitsprobleme nicht außerhalb der Unternehmen bestehen, sondern durch Ethik- und Verantwortungsmängel verursacht sind. Das innerbetriebliche Klima sollte demnach angemessen gestaltet werden, und Führungskräfte aus Geschäftsführung und Personalentwicklung sollten ein wertschätzendes Arbeitsklima und eine menschengerechte Arbeitsgestaltung im Blick haben. Ein Unternehmensklima, das einseitig auf „Gewinnerzielung um jeden Preis“ setzt, begünstigt schädigende Verhaltensweisen durch Mitarbeitende innerhalb der Unternehmen durch Diebstahl oder Sabotage, wie Eigenstetter et al.³³ zeigen können. Die Mehrzahl der Unternehmen, die „Opfer von Spionage, Sabotage oder Datendiebstahl wurden, haben die Täter im Personenkreis Mitarbeitende identifiziert“³⁴. Racheakte scheinen demnach nicht selten. Erst die nächstgrößere Tätergruppe umfasst „Wettbewerber, Kunden, Lieferanten oder Dienstleister, gefolgt von den Hobbyhackern“³⁵.

So lässt sich festhalten: Ein hoher Risikofaktor für unternehmensschädigende Verhaltensweisen, ist ein Klima, das Egoismen innerhalb einer Organisation fördert. Dies geht einher mit einer fehlenden Fürsorgeorientierung für die Mitarbeitenden sowie erhöhtem Stresserleben. Unternehmen mit einer wertschätzenden Unternehmenskultur sind weit weniger von unternehmensschädigenden Verhaltensweisen betroffen³⁶.

4.5 Weitere Risiken

Die oben genannten Risiken sind nicht abschließend. Wenn ein Unternehmen aufgrund der Digitalisierung viele Stellen abbaut, sollte es sich z.B. im Sinn menschenrechtlicher Due Diligence-Pflichten fragen, wie welche Auswirkungen der Stellenabbau hat und wie er sozial verträglich durchgeführt werden soll³⁷. Da diese Diskussion in den Medien immer wieder aufgegriffen wird, wird hier dieses Thema nicht weiter vertieft.

Ethische Probleme kündigen sich allerdings an, für die noch keine umfassenden Lösungen bereitstehen. Künstliche Intelligenz vermag Entscheidungen zu treffen, die sich nicht mit den Grundsätzen der Gleichbehandlung vertragen. Amazon hat im Oktober 2018 einen Algorithmus vom Netz genommen, da dieser in der Personalauswahl zu einer Benachteiligung von Frauen führte. Das Trainingsmaterial basierte hauptsächlich auf Akten von Männern, weshalb der Algorithmus Männer bevorzugte. Eine Nachkorrektur 2015, als der Fehler entdeckt wurde, führte nicht zu einer wesentlichen Verbesserung³⁸. Ein weiteres Beispiel machte mehr Schlagzeilen. Als Air Berlin insolvent ging, stiegen die Ticketpreise bei Lufthansa. Nach der Aussage von Lufthansa war dies eine autonome Entscheidung der Software³⁹. Die „Fehler“ liegen beide Male in der Entwicklung der Software.

Andere Probleme, die gerade im Kontext der KI auftreten sind, ist fehlende Kontrolle und fehlendes Überblickswissen durch die bedienenden Menschen. Das menschliche Denken ist gut dazu imstande, aus Vergangenen *lineare* Vorhersagen für die Zukunft zu machen. Daten und IT entwickeln sich jedoch *exponentiell*, da sich die Prozessorleistungen alle 12-24 Monate verdoppeln (Moore'sches Gesetz). Für die Menge an Interaktionen von Variablen, die vielfach systemisch vernetzt sind, ist ein „Durchschnittsgehirn“ einfach nicht gemacht. Wer kann letztlich noch verstehen, was in den Algorithmen passiert?

Grote⁴⁰ stellt fest: „Wenn die Auswirkungen von Technologie weder von den Entwicklern noch den Entscheidungsträgern und Nutzern der Technologie in der Organisation vollumfänglich vorhergesehen und gesteuert werden können, kann Verantwortung nicht eindeutig zugeordnet werden.“ Misselhorn verweist auf weitere Schwierigkeiten: Wenn Technik „autonom“ agiert, können viele Probleme möglicherweise von den Entwickelnden gar nicht erkannt werden, weil die Probleme mit einer großen zeitlichen Verzögerung auftreten können, so dass eine kausale Verbindung nicht mehr sichtbar ist⁴¹. Und: Neben der fehlenden Zuschreibung von Verantwortung und Zurechenbarkeit wegen Intransparenz des technischen Systems besteht schon in der Entwicklung das „Problem der vielen Hände“: Wer ist denn – in Entwicklerteams – für auftretende Fehler eigentlich verantwortlich?⁴²

Weiter steht nach Misselhorn⁴³ zu befürchten, dass Moralvorstellungen an das Machbare, also an das, „was sich programmieren lässt“, angepasst werden. Da aber Maschinen letztlich als Hilfsmittel für den Menschen dienen, aus dessen Kreativität geschaffen sind und zu seinem Nutzen eingesetzt werden, sind sie als „Erweiterung des menschlichen Geistes“ einer Person zu betrachten. Und das bedeutet wiederum, der Mensch bleibt moralisch der Verantwortungsträger.

5 Handlungsempfehlungen für sichere und akzeptierte Technologien

Um Automation und Digitalisierung angemessen zu gestalten, müssen mehrere Ebenen der Technik betrachtet werden. Robelski⁴⁴ schlägt drei Ebenen vor:

1. Aufgabenverteilung zwischen Mensch und Technik, nämlich die Mensch-Technik-Funktionsteilung: Wer soll welche Aufgabenanteile übernehmen?
2. Schnittstellengestaltung: Dabei geht es um Fragen des ergonomischen Designs (u.a. Nutzerfreundlichkeit) sowie die Betrachtung von Interaktionskonzepten z.B. in der Display-Gestaltung.
3. Operationale Ebene: Hier geht es um Eingriffsmöglichkeiten, nämlich die Bedienung von Maschinen bzw. die von einem Operateur aktuell durchzuführende Prozesskontrolle und Veränderbarkeiten, die mit psychischen Beanspruchungen wie Monotonie und Sättigung einhergehen können.

Im Folgenden werden die Aufgabenverteilung und Eingriffsmöglichkeiten zwischen Mensch und Technik unter der Idee des Mensch-Technik-Teams betrachtet. Weiter wird der Schnittstellengestaltung ein eigenes Kapitel gewidmet, da der nutzerfreundlichen Schnittstellengestaltung immer noch zu wenig Beachtung geschenkt wird. Sie ist allerdings nur eine Voraussetzung, damit Verantwortung und Kontrolle auch unter den Bedingungen der KI beim Menschen verbleibt. Partizipation und Beteiligung in der Technikentwicklung und -einführung sind wichtige Aspekte, um Akzeptanz und Performanz von soziotechnischen Systemen und Mensch-Maschine-Teams sicher zu stellen.

5.1 Ebenen der Gestaltung und das Mensch-Technik-Team berücksichtigen

Der Idee des Mensch-Technik-Teams liegen u.a. folgende Forderungen zugrunde. Mensch und Technik müssen beidseitig vorhersehbar agieren können, d.h. es muss zu jedem Zeitpunkt erkennbar sein, in welchem Zustand sich die Technik befindet und was als nächstes passieren wird⁴⁵. Technik muss dazu z.B. Aufmerksamkeitsprozesse steuern. Technik muss kontrollierbar und steuerbar sein, wobei die Technik auch Vorschläge zur Zielerreichung machen sollte. Idealerweise sollte bei der Technikgestaltung eine flexible Aufgabenübernahme durch den Menschen ermöglicht werden. Dies sind Überlegungen, die einer adaptiven Technikgestaltung und der Idee der „Teamarbeit zwischen Mensch und Technik“ zugrunde liegen. Je nach Vorwissen und Ermüdung werden vom Operator verschiedene Aufgaben übernommen oder wieder an das technische System zurückgegeben⁴⁶. Schließlich ist bei einer adaptiven Gestaltung von einer hohen Bedeutung, wie die Informationen dargestellt werden und wie die Übergabe von Aufgaben von der Technik an den Menschen und vice versa erfolgen kann.

Lüdtke⁴⁷ betrachtet vier Gestaltungsebenen in einem Mensch-Technik-Team (MTT) (siehe auch Tabelle 1).

1. Komposition: In welcher Umgebung soll das MTT arbeiten und welche Aufgaben soll das MTT durchführen? ...
2. Kooperation: Welche Akteure sollen wie zusammenarbeiten?
3. Interaktion: Welche Informationen sind zu welchem Zeitpunkt für wen relevant?
4. Schnittstelle: Softwareergonomische Anforderungen

MTT	Anforderungsdefinition	Spezifikation	Implementation	Evaluation
Komposition	In welcher Umgebung soll das MTT arbeiten? Welche Aufgaben soll das MTT durchführen? ...	Welche Ressourcen werden für das MTT benötigt? Aus welchen Operateuren (Rollen, Skills, ...) und welcher Technik soll sich das MTT zusammensetzen? ...	Auswahlkriterien und -verfahren sowie Trainingsprogramme für die Operateure festlegen, ...	Abschätzung, ob die Operateure und Technik ausreichen, um die Aufgaben zu bewältigen, ...
Kooperation	Welche Akteure sollen zusammenarbeiten? Welche Akteure sollen welche Aufgaben übernehmen? ...	Definition der Aufgabenallokation, Übergabestrategien, Kooperationsformen, ...	Implementierung der Aufgabenübernahme und -übergabe durch die Technik, Definition von Prozeduren für die Aufgabenübernahme und -übergabe	Abschätzung, ob die Aufgabenübernahme und -übergabe sicher und effizient funktioniert, ...
Interaktion	Welche Informationen sind zu welchem Zeitpunkt für wen relevant? Wieviel muss der Mensch in welcher Situation über die Technik wissen? Wieviel muss die Technik in welcher Situation über den Menschen wissen? ... Welche Bedienaktionen sind notwendig? ...	Definition der zu kommunizierenden Informationen, der Interaktionsmodalitäten (z.B. visuell, akustisch, taktil), der Informationsverteilung, der Bedienstrategien, ... Ggf. Definition der Methoden zur Messung des Zustands der Operateure (z.B. Müdigkeits-, Arbeitslastmessung), ...	Implementierung der Informationsbereitstellung und -verteilung, Realisierung der spezifizierten Interaktionsmodalitäten, der Zustandsmessung, ... Ausarbeitung und Dokumentation der Interaktionsprozeduren, ...	Abschätzung, ob jeder Akteur die notwendigen Informationen zur richtigen Zeit zur Verfügung hat,...
Schnittstelle	Ergonomische Anforderungen laut DIN EN ISO 9241, Berücksichtigung der menschlichen Informationsverarbeitung, (kognitive Ergonomie) ...	Gestaltung der (z.B. grafischen) Informationsdarstellung, der Bedienelemente, ...	Implementation der Ausgabe- (z.B. Displays) und Bedienelemente (z.B.) auf Seiten der Technik, ...	Abschätzung, ob die Schnittstelle eine intuitive, fehlerfreie Mensch-Technik-Interaktion erlaubt, ...

Tabelle 1. Anforderungen an eine gelingende Technikgestaltung (nach Lüdtko, 2015, geringfügig modifiziert)

5.2 Kognitive Ergonomie sicherstellen: Usability und User Experience

Im Bereich der Geschäftsmodelle sollten Nutzerfreundlichkeit (Gebrauchstauglichkeit, Usability) und das positiv bewertete Nutzungserlebnis (User Experience) selbstverständlich sein: Man denke nur an die leichte Bedienbarkeit von Smartphones oder Online-Shops. Doch sieht es leider im Bereich vieler Mensch-Technik-Schnittstellen, z.B. auf Unternehmensseiten oder im Produktionskontext, oft deutlich anders aus. Usability ist nicht zu unterschätzen und wird als Innovationstreiber betrachtet.

Nutzerfreundlichkeit bzw. Gebrauchstauglichkeit definiert sich nach DIN EN ISO 9241-11: Ergonomie der Mensch-System-Interaktion, Teil 110: Grundsätze der Dialoggestaltung anhand von drei Größen der Zielerreichung:

- Effektivität meint die Genauigkeit und Vollständigkeit, mit der Nutzende ein bestimmtes Ziel erreichen.
- Effizienz meint den im Verhältnis zur Genauigkeit und Vollständigkeit eingesetzte Aufwand, mit dem Nutzende ein bestimmtes Ziel erreichen.
- Zufriedenheit wird erzeugt durch die Freiheit von Beeinträchtigungen und positive Einstellungen gegenüber der Nutzung des Produktes.

Entlang von sieben Kriterien der Dialoggestaltung wird die Mensch-Technik-Schnittstelle bewertet (DIN EN ISO 9241-119), d.h. nach

1. **Aufgabenangemessenheit:** Das technische System soll Nutzende unterstützen, die Arbeitsaufgabe zu bewältigen. Das System orientiert sich an den Handlungen und Tätigkeitserfordernissen und stellt dafür geeignete Auswahlmöglichkeiten dar. Die Zahl nötiger Interaktionen wird auf ein Minimum beschränkt (z.B. One-Click-Bestellungen).
2. **Selbstbeschreibungsfähigkeit** bedeutet, dass Nutzende erkennen, an welcher Stelle sie sich in einer Dialogführung befinden. Darstellungen, auf welcher Ebene des Menüs man sich befindet, werden z.B. durch Pfade oder „Reiter“ unterstützt.
3. **Steuerbarkeit des Dialogs** durch Nutzende meint, dass man leicht navigieren kann. So lässt sich bei gängigen Programmen meist entscheiden, ob man über eine Menüführung, kleine Icons bzw. Piktogramme oder über so genannte Shortcuts (Tastenkombinationen) Befehle ausführen möchte.
4. **Erwartungskonformität** besteht, wenn die Bedürfnisse nach Konsistenz beim Benutzer erfüllt sind und wenn allgemeine Standards und Konventionen erfüllt sind. Konsistenz meint z.B. das gleichartige Informationen auch gleichartig angeboten werden. So wird in nahezu allen Programmen das Symbol „Diskette“ oder ein Downloadpfeil zum Speichern angezeigt.
5. **Fehlertoleranz** bedeutet, dass erkannte Fehler nicht das Benutzerziel verhindern, sondern leicht korrigierbar sind. Die „Zurück“-Funktion der Programme ist dafür ein eingängiges Beispiel.
6. **Individualisierbarkeit** meint die Anpassbarkeit an spezifische Aufgabenkontexte. Textverarbeitungsprogramme bieten z.B. die Möglichkeit, die Menü-Leisten so zu verändern, dass häufig gebrauchte Befehle schnell verfügbar sind. Nicht benutzte Leisten können dagegen abgeschaltet werden.
7. **Lernförderlichkeit** heißt, dass man z.B. über Lernprogramme eingeführt wird und das Erlernte auf andere Programme und Systeme übertragen kann.

Von der Bundesanstalt für Arbeitsschutz und Arbeitsmedizin BAUA⁴⁸ wurden zentrale Beurteilungskriterien zusammengefasst:

- Informationsaufnahme Hardware
- Informationsaufnahme Software
- Fehlertolerante, motorisch-unterstützende Software
- Anforderungen an Stellteile
- Störungen vermeiden / Beeinträchtigungen berücksichtigen

Hinzu kommen Verweisungen auf die TRBS 1151, Technische Regeln für Betriebssicherheit für Gefährdungen an der Schnittstelle Mensch - Arbeitsmittel – Ergonomische und menschliche Faktoren, Arbeitssystem sowie auf andere geltende Normen, z.B. DIN EN 894-3 (Sicherheit von Maschinen - Ergonomische Anforderungen an die Gestaltung von Anzeigen und Stellteilen - Teil 3: Stellteile) oder auf barrierefreie Gestaltung von Technik (WCAG). Eine umfassende Zusammenstellung von Qualitätskriterien im Kontext der Arbeitssystemgestaltung bietet die DGUV Information 215-450 - Softwareergonomie.

Ergänzend soll noch ein Instrument genannt werden, das evaluierend zur Prüfung der Gebrauchstauglichkeit eingesetzt werden kann. Prümper hat basierend auf der oben genannten ISO-Norm einen Fragebogen entwickelt, der eine hohe Zuverlässigkeit besitzt und sich einfach auf viele Bereiche anwenden lässt. Er ist als Fragebogen ISONORM 9241/10 frei verfügbar. Eine umfassende Zusammenstellung verschiedener Verfahren zur Erfassung der Gebrauchstauglichkeit bieten Levchuk et al.⁴⁹.

User Experience wiederum ist eine wichtige Domäne des Marketing und der Technikgestaltung für den Kunden. Das Konzept User Experience ist eng verwandt mit Nutzerfreundlichkeit, geht aber darüber hinaus und betont ästhetische und emotionale Qualitäten sowie den Spaß an der Nutzung der spezifischen Technik. Attraktive Oberflächen werden gestaltet, um Kunden anzusprechen und Vertrauenswürdigkeit sicherzustellen⁵⁰. Zudem gilt User Experience (UX) als Innovationstreiber⁵¹. Der Fragebogen AttrakDiff der User Interface Design GmbH, ebenfalls kostenfrei zur Verfügung gestellt, vermag Aspekte der User Experience zu erfassen.

5.3 Kontrolle und Verantwortung ermöglichen

Nach Grote⁵² basiert Kontrolle in technischen Systemen auf drei Dimensionen:

- Durchschaubarkeit: Fähigkeit eines Akteurs, den Zustand eines sozio-technischen Systems festzustellen
- Vorhersehbarkeit: Fähigkeit eines Akteurs, die Funktionsweise eines sozio-technischen Systems zu verstehen
- Beeinflussbarkeit: Fähigkeit eines Akteurs, ein sozio-technisches System zu beeinflussen

Verantwortung in technischen Systemen wiederum umfasst nach Boos et al.⁵³ die Kriterien

- Sichtbarkeit: Anforderung an einen Akteur, seine eigenen Aktivitäten Anderen verständlich zu machen, damit diese ihre eigenen Aktivitäten planen und ausführen können
- Auftragserfüllung: Verteilung von Kompetenzen und Aufgaben, aus denen sich die Anforderungen und Pflichten jedes Akteurs im Hinblick auf die Zielerreichung der Organisation ergeben
- Haftung: Verantwortlichkeit eines Akteurs im Hinblick auf Gesetze, Vorschriften und Verträge

Aus der Kombination dieser Kriterien werden Anforderungen an die Systemgestaltung komplexer technischer Systeme formuliert (Tabelle 2):

Dimension	Durchschaubarkeit	Vorhersehbarkeit	Beeinflussbarkeit
Sichtbarkeit	Wissen über Anforderungen anderer Akteure bzgl. Verständlichkeit der eigenen Handlungen	Vorhersehbarkeit der Folgen des eigenen Handelns für die Informationsanforderungen anderer Akteure	Möglichkeiten, Anderen die eigenen Handlungen verständlich zu machen
Auftragserfüllung	Wissen über eigene Verantwortlichkeiten	Vorhersehbarkeit der Beziehung zwischen eigenen Handlungen und Organisationszielen	Verfügbarkeit aller nötigen Ressourcen für die Auftragserfüllung
Haftung	Wissen über bestehende Haftungsansprüche	Vorhersehbarkeit der Folgen des eigenen Handelns	Entscheidungsgewalt hinsichtlich der (Nicht-) Ausführung bestimmter Handlungen

Tabelle 2. Passung zwischen Kontrolle und Verantwortung (in Anlehnung an Boos et al., 2013, entnommen Grote 2018)

Betrachtet man die genannten Anforderungen in der Tabelle 2, zeigt sich: Die Dimension Durchschaubarkeit gründet im „Wissen“, d.h. vor allem auf den Qualifikationen der Entwickelnden, Entscheidenden und Nutzenden der Technologien. Diese Qualifikationsanforderungen bereitzustellen, ist eine besondere Herausforderung, der man sich im Kontext der Digitalisierung stellen muss.

Die Dimensionen Vorhersehbarkeit und Beeinflussbarkeit verweisen dagegen auf Informationsdarstellung und -verarbeitung sowie Eingriffsmöglichkeiten in der Mensch-Technik-Interaktion: Eingriffsmöglichkeit muss auch heißen, ausreichend Zeit und Reaktionsmöglichkeiten zu geben. Diese Forderung geht über Usability und Nutzerfreundlichkeit hinaus und erfordert ein besonderes Wissen um die Grenzen der menschlichen Informationsverarbeitung.

EEMUA 191⁵⁴ z.B. hat für ein Alarmmanagement in Leitwarten, welche komplexe Anlagen steuern, die erforderlichen Anforderungen definiert. So heißt es z.B. dass ein Alarm pro 10 Minuten effektiv bearbeitbar, ein Alarm pro 5 Minuten noch kontrollierbar sei. Die Realität aber ist häufig ca. ein Alarm pro Minute, was eine systematische Überforderung von Operateuren darstellt und zu Misstrauen in Technik, Überforderung und Stress führt sowie auch oft unsichere Strategien fördert. Wie sich in den aktuellen Erhebungen zeigt, sind die meisten Leitwarten immer noch nicht entsprechend der Empfehlungen gestaltet⁵⁵.

Für die Problematik der „Intransparenz“, d.h. wenn sich Verantwortung nicht mehr eindeutig zuordnen lässt, schlägt Grote⁵⁶ eine umfassende Einbindung von Betroffenen vor: ein erster Schritt einer Lösung sei, das Problem offen und mit allen relevanten Stakeholdern zu diskutieren, anstelle die Nutzenden als letztes Glied in der Kette als „Verantwortungsträger im System“ zu deklarieren und damit wieder als „menschlichen Fehler“ zu klassifizieren.

5.4 Kompetenzerhalt und -aufbau bei den Mitarbeitenden sicherstellen

Mittels Kompetenzstrukturmodellen können aktuelle und zukünftig erforderliche Kompetenzen erhoben und in einem Ist-Soll-Abgleich bewertet werden⁵⁷. Dabei müssen Ausprägungen der jeweiligen Kompetenzen über Merkmale operationalisiert werden⁵⁸. North et al.⁵⁹ unterscheiden die Ausprägungen „Kenner“, „Köner“ und „Experte“, die von Langhoff⁶⁰ um weitere Ausprägungen, nämlich „keine Kompetenz“ und „Lerner“ ergänzt wurden: Merkmale sind Wissenstiefe, Komplexität der Aufgabe, Grad der Selbstständigkeit und Reflexionsfähigkeit⁶¹. Eine erfolgreiche Vermittlung bzw. das Lernen überfachlicher Kompetenzen erfolgt besonders effektiv im Prozess der Arbeit selbst⁶² weshalb systematische Partizipation auch als Prozess der Qualifizierung und der Kompetenzentwicklung gelten kann. Nur eine menschenzentrierte Technikgestaltung vermag die Mitarbeitenden weiter zu qualifizieren, z.B. indem die Technologien als digitale Assistenz gestaltet werden und zur Erweiterung der eigenen Fähigkeiten dienen⁶³.

5.5 Technikakzeptanz der Mitarbeitenden durch Partizipation und User Centered Design gewährleisten

Soule et al.⁶⁴ berichten für digitalisierte Organisationen eine höhere Wertschöpfung und bezeichnen die Fähigkeit der Unternehmen, die digitale Transformation erfolgreich zu gestalten als Digital Dexterity. Die Einbindung neuer Technologien in die Organisation erfordert allerdings die Akzeptanz und Mitarbeit aller Beteiligten, wie auch die Bertelsmannstiftung zur Zukunft der Arbeit feststellt. Es muss u.a. die Einbindung der Techniken in die Organisation betrachtet werden, eine Gestaltungsfrage, die nicht nur die Technik, sondern auch Führung und Zusammenarbeit betrifft: Wie wird sich in flexibilisierten Netzwerksstrukturen Vertrauen zwischen allen Beteiligten, z.B. zwischen Kunden und Organisation oder Mitarbeitenden und Organisation herstellen lassen? Wie wird Akzeptanz für die Veränderungen durch die neu einzuführenden Techniken sichergestellt? Welche Methodenkompetenzen müssen neu aufgebaut werden? Verändern sich Arbeitszeiten und damit ggf. Entgeltsysteme? Digitalisierung erfordert Restrukturierungen, die die psychischen Belastungen und Beanspruchungen weiter erhöhen können. Letztlich geht es um einen umfassenden Change Management Prozess.

Die Komplexität der Herausforderungen verweist darauf, dass erst ein menschenzentriertes Weltbild wertschöpfende Geschäftsideen ermöglicht⁶⁵. Damit ist die aktive Beteiligung der Mitarbeitenden, deren Partizipation, ein zentraler Erfolgsfaktor. Partizipation allerdings ist ein Sammelbegriff und meint sehr unterschiedliche Arten von Beteiligung, die durch Hierarchie, Machtverteilung und Handlungsspielräume charakterisiert werden und sich z.B. durch die Grade der Einflussnahme unterscheiden: z.B. als Informationsrechte, Vorschlagsrechte, Mitbestimmungsrechte, Vetorechte oder Autonomie⁶⁶.

Erfolgsversprechend sind Ansätze, wie sie im partizipativen Design und im Human Centered Design vertreten werden. Partizipatives Design geht über Human Centered Design hinaus, da es emanzipatorisch angelegt ist. Es legitimiert die Nutzenden, ihre Projekt und die

Aufgaben in Zielsetzung und Umsetzung selbst zu bewerten und begleitend zu gestalten⁶⁷. Da Technik die Zukunft von Personen und damit die Lebenswirklichkeit sowie auch die Persönlichkeit beeinflusst, sollte den Einzelnen, die die Technik nutzen (müssen), weitreichende Mitgestaltungsrechte zugesprochen werden.

Dieser Ansatz sollte auch in die Entwicklung hybrider Geschäftsmodelle übertragen werden. Dabei ist von Vorteil, dass partizipatorische Ansätze auch für neue und gerade nicht vorhersagbare Situationen gut passen⁶⁸. Partizipatives Design als User Driven Innovation löst allerdings traditionelle Rollen auf: Die Anwender werden zu Gestaltern. Damit öffnet sich ganz selbstverständlich der Gestaltungsraum neben den Mitarbeitenden auch für die Kunden, so dass gemeinsam robuste Lösungen entwickelt werden können⁶⁹. Wissen und Technik werden gemeinsam im Prozess erzeugt und adaptiert. Damit sollte neben der Entwicklung von umsetzbaren Geschäftsmodellen auch Technikakzeptanz in seinen vielfältigen Facetten gewährleistet werden können⁷⁰. Diese durchaus nicht neuen Ideen werden heute vor allem unter dem Begriff „Design Thinking“ umgesetzt⁷¹.

6 Checklisten und Handlungshilfen für die Praxis

Verschiedene Institutionen stellen umfassende Entscheidungs- und Handlungshilfen für eine gelingende Digitalisierung bereit. Eine Auswahl finden Sie hier:

- *Mittelstand Digital* gibt Impulse, sich mit dem Thema ganz allgemein auseinander zu setzen. Die Seiten sind für „Einsteiger“ gedacht.
- *Offensive Mittelstand*: Mittelstand 4.0 stellt das Thema Arbeit 4.0 in den Mittelpunkt und hat viele Checklisten und Kurzreader zu den verschiedenen Aspekten der Digitalisierung zusammengestellt.
- Das *Bundesamt für Sicherheit in der Informationstechnik* (BSI) gehört zum Geschäftsbereich des Bundesministeriums des Innern. Es bietet Antworten speziell auf Fragen zur IT-Sicherheit.
- Wer vertiefte Studien und Informationen rund um das Thema Digitalisierung benötigt, findet diese auf den Seiten der *BITKOM*.
- Mit dem letzten Abschnitt wird auf die *Fördermöglichkeiten für KMU* verwiesen, die sich dem Thema Digitalisierung annehmen möchten.

6.1 Mittelstand-Digital

Das Bundesministerium für Wirtschaft und Energie will die Digitalisierung im Mittelstand unterstützen und hat daher eine umfangreiche Website www.mittelstand-digital.de aufgebaut. Das BMWi hat darauf Checklisten und Angebote bereitgestellt, um die vielfältigen Möglichkeiten der Digitalisierung, gerade auch für den Mittelstand verfügbar zu machen: Neue Produkte, Geschäftsfelder und Services können schneller entwickelt und an den Markt gebracht werden, Kundenwünsche besser berücksichtigt, neue Geschäftsmodelle angeboten werden. Gerade für kleinere KMU bietet Digitalisierung Möglichkeiten die Interaktion mit Beschäftigten, Kunden und Lieferanten gewinnbringender zu gestalten.

Mit untenstehenden Leitfragen werden die Unternehmen an das Thema Digitalisierung herangeführt: Checklisten und Beratungsangebote sind hinterlegt (Tabelle 3).

<https://www.mittelstand-digital.de/MD/Navigation/DE/Home/home.html>

Leitfragen
Warum soll ich digitalisieren?
Wie erstelle ich einen Fahrplan zur Digitalisierung?
Wie funktioniert Digitalisierung?
Wie optimiere ich meine Prozesse?
Wie funktioniert es sicher?
Wie finanziere ich die Digitalisierung?
Wie überzeuge ich meine Mitarbeiter von der Digitalisierung?
Wie kann ich auf digitalem Weg Fachkräfte gewinnen?
Wie kann ich digital Wissen erhalten?
Wie gewinne ich mehr Kunden?
Wie kann ich mit digitaler Unterstützung den Absatz steigern?
Wie kann ich neue Geschäftsmodelle aufbauen?

Tabelle 3. Angebote des BMWi

6.2 Offensive Mittelstand: Mittelstand 4.0 – sichere und gesunde Digitalisierung ermöglichen

Mittelstand 4.0. bietet Umsetzungs- und Entscheidungshilfen für eine effiziente, sichere und gesunde Digitalisierung an (Tabelle 4):

- Die Entscheidungshilfen sind speziell für den Mittelstand entwickelt und sollen helfen, die Möglichkeiten für den eigenen Betrieb einzuschätzen.
- Die Umsetzungenhilfen ermöglichen, auf KI basierende technische Systeme in die Organisation zu integrieren.

<https://www.offensive-mittelstand.de/serviceangebote/mittelstand-40/>

Entscheidungshilfen	Umsetzungshilfen
Themenfeld "Arbeitswelt 4.0" E 01: Einstiege in die digital-integrierte Wirtschaft – Potenziale der „Arbeit 4.0“ für Mittelstand und Handwerk E 02: Bedeutung von Cyber-Physical Systems (CPS) für KMU und Handwerk E 03: „Arbeit 4.0“: Herausforderung Qualifizierung E 04: Gutes Arbeiten mit der Crowd – Qualität und Standards E 05: Fragen der IT-Sicherheit in der "Arbeitswelt 4.0" E 06: Prävention 4.0 E 07: Führungs- und Kommunikationskompetenz für die "Arbeitswelt 4.0" Themenfeld "Cloud Computing" E 08: Cloud Computing – Orientierungswissen für KMUs E 09: Einstiegshilfe für KMUs – Die ersten Handlungsschritte in Richtung Cloud Computing E 10: Rechtliche Aspekte der Nutzung von Cloud-Lösungen E 11: Qualifizierungsanforderungen für das Cloud Computing u.a.	1. Arbeit 4.0: Führung und Kultur 1.1.1 Externe und interne Strategie in der digitalen Transformation 1.1.3 Unternehmensethik und Software 4.0 1.1.4 Ethische Werte für die Software 4.0 1.3.2 Interaktion zwischen Mensch und Software 4.0 1.3.3 Handlungsträgerschaft im Verhältnis Mensch und Software 4.0 1.3.5 Hersteller- und Unternehmerverantwortung in 4.0 Prozessen 1.4.1 Kompetenzverschiebung zwischen Mensch und Software 4.0 1.5.1 Unternehmenskultur in 4.0-Prozessen 1.5.2 Diversity in 4.0-Prozessen 2. Arbeit 4.0: Organisation 2.1.6 Beschaffung digitaler Produkte 2.2.1 Gefährdungsbeurteilung 4.0 2.2.4 Sicherheitstechnische und arbeitsmedizinische Betreuung 2.3.2 Datenschutz in 4.0 Prozessen 2.3.4 Betriebs- und Dienstvereinbarungen zu 4.0-Prozessen 2.4.1 Prozessplanung mit CPS 2.4.2 Building Information Modeling (BIM) 2.5.1 Anforderungen an eine Cloud 2.5.2 Cloud-Modelle der Bereitstellung und Dienstleistungen 2.6.1 Digitale Planung des Personaleinsatzes 3. Arbeit 4.0: Sicherheit 3.1.1 Betriebssicherheit der CPS 3.2.1 Technische Assistenzsysteme – allgemein 3.2.2 Smartphone, -watch, -glasses (Kognitiv unterstützende technische Assistenzsysteme) 3.2.4 Exoskelette (physisch unterstützende Assistenzsysteme) 3.2.5 Ambient Intelligence, Ambient Assisted Working 3.2.7 Nutzung von Robotern 3.3.1 Personenbezogene digitale Ergonomie 3.6.1 Digitale Persönliche Schutzausrüstung (PSA)

Tabelle 4: Hilfen der Offensive Mittelstand

6.3 Bundesamt für Sicherheit in der Informationstechnik

Das Bundesamt für Sicherheit erarbeitet Standards, die eine grundlegende IT-Grundschutz-Methodik abbilden. Die Standards enthalten Empfehlungen zu Methoden, Prozessen und Verfahren sowie Vorgehensweisen für alle Organisationen.

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards-/ITGrundschutzStandards_node.html

Für KMU wird auf einen Standard gesondert verwiesen: „Leitfaden zur Basis-Absicherung nach IT-Grundschutz: Dieser soll einen einfachen Einstieg zum Aufbau eines Informationssicherheitsmanagementsystems (ISMS) geben. Eine Auswahl der Standards findet sich in Tabelle 5.

Standard	Beschreibung
Leitfaden Basis-Absicherung	Einstieg zum Aufbau eines Informationssicherheitsmanagementsystems (ISMS)
BSI-Standard 200-1: Managementsysteme für Informationssicherheit	Allgemeine Anforderungen an ein Managementsystem für Informationssicherheit (ISMS)
BSI-Standard 200-2: IT-Grundschutz-Methodik	Methodik zum Aufbau eines soliden Informationssicherheitsmanagements (ISMS)
BSI-Standard 200-3: Risikomanagement	Risikobezogene Arbeitsschritte bei der Umsetzung des IT-Grundschutzes

Tabelle 5: Standards des BSI

6.4 Bitkom – vielfache Informationen rund um Digitalisierung

Der größte Digitalverband Deutschlands bietet viele Studien und Hintergrundinformationen zur Digitalisierung an: so zu Nutzungsverhalten oder Qualifizierungserfordernissen, Cyber-Security oder Gestaltungswissen zur Digitalen Transformation. Um einen fundierten und datenbasierten Einblick zu erhalten, sind die Publikationen des Verbandes sehr gut geeignet.

<https://www.bitkom.org>

6.5 Einfach anfangen: Innovationsgutscheine und Digitalisierungsgutscheine in NRW

Das Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen (MWIDE) bietet ein Förderprogramm speziell für den Mittelstand. Unter dem Motto „Mittelstand.innovativ!“ umfasst es die Förderlinien Innovationsassistent und den Innovations- und Digitalisierungsgutschein.

<https://www.ptj.de/projektfoerderung/mittelstand-innovativ>

Die Programmlinie Innovationsassistent(in) unterstützt die Beschäftigung von Hochschulabsolvent(inn)en, um den Wissens- und Technologietransfer von Hochschulen in KMU zu verbessern und damit die Innovationsfähigkeit der Unternehmen.

<https://www.ptj.de/projektfoerderung/mittelstand-innovativ/innovationsassistent>

- Der Projektträger Jülich. „Innovations- und Digitalisierungsgutscheine“ können beim Projektträger der Forschungszentrum Jülich GmbH im Auftrag des MWIDE beantragt werden. *Innovationsgutscheine* sollen die Entwicklung neuer Produkte und Dienstleistungen auf allen Stufen der Wertschöpfungskette voranbringen sowie wesentliche qualitative Verbesserungen bestehender Produkte und Dienstleistungen. Auch Prozesse des Change Managements und der Technikgestaltung können gefördert werden.
- Mit dem *Digitalisierungsgutschein* will man Themen rund um Digitalisierung und IT-Sicherheit in NRW stärken.

<https://www.ptj.de/innovationsgutscheine>

Zielgruppe sind kleine und mittlere Unternehmen in NRW: Die Förderung umfasst bis zu 10.000 Euro für Analysen und bis zu 15.000 Euro für Maßnahmen mit einer maximal 80% Förderquote für Kleinst- und kleine Unternehmen und maximal 50% für mittlere Unternehmen.

Ihre Hochschule ist gerne neben den kommerziellen Anbietern Ansprechpartner, um Sie bei Ihren Herausforderungen zu unterstützen. Über die Forschungstransferstelle der Hochschule Niederrhein werden die entsprechenden Experten angesprochen, um mit den KMU Kontakt aufzunehmen.

7 Quellen

- Antoni, C. H. (1999). Konzepte der Mitarbeiterbeteiligung: Delegation und Partizipation. In C. Graf Hoyos & D. Frey (Hrsg.), *Arbeits- und Organisationspsychologie* (S. 569–583). Weinheim: Psychologische Verlagsunion.
- Arbeitsschutzgesetz vom 7. August 1996 (BGBl. I S. 1246), zuletzt geändert am 19. Oktober 2013
- BASt (2012). Rechtsfolgen zunehmender Fahrzeugautomatisierung. Verfügbar unter https://www.bast.de/BASt_2017/DE/Publikationen/Foko/2013-2012/2012-11.html [23.12.2018]
- BAUA (o.J.) Grenzwerte, Beurteilungskriterien. Verfügbar unter: <https://www.baua.de/DE/Themen/Arbeitsgestaltung-im-Betrieb/Gefahrungsbeurteilung/Expertenwissen/-Arbeitsumgebungsbedingungen/Mensch-Maschine-Rechner-Schnittstelle/grenzwerte.html> [16.12.2018]
- Bertelsmannstiftung: https://www.bertelsmannstiftung.de/fileadmin/files/BSst/Publikationen/GrauePublikationen/Enterprise_for_health_Dokumentation_des_Fachgespraches.pdf
- Berufsverband der Rechtsjournalisten e.V. (o.J.) Datensicherheit: Maßnahmen für den Schutz von Daten. Verfügbar unter: <https://www.datenschutz.org/datensicherheit-massnahmen/> [28.12.2018]
- Bitkom (2018). <https://www.bitkom.org/Presse/Presseinformation/Attacken-auf-deutsche-Industrie-verursachen-43-Milliarden-Euro-Schaden.html>
- Bockelmann, M., Nachreiner, F., Nickel P. (2012). Bildschirmarbeit in Leitwarten. Handlungshilfen zur ergonomischen Gestaltung von Arbeitsplätzen nach der Bildschirmarbeitsverordnung (F 2249). Bundesanstalt für Arbeitsschutz und Arbeitsmedizin. Verfügbar unter: <https://www.baua.de/DE/Angebote/Publikationen/Berichte/F2249.html> [28.12.2018]
- Boos, D., Günter, H., Grote, G. & Kinder, K. (2013b). Controllable accountabilities: The Internet of Things and its challenges for organisations. *Behaviour & Information Technology*, 32, 449-476.
- Brainbridge, L. (1983). Ironies of automation. *Automatica*, 19 (6), 775-779.
- Brynjolfsson, E. & MacAfee, A. (2014). *The second machine age. Work, progress, and prosperity in a time of brilliant technology*. New York: Plassen Verlag.
- BSI-Standard 200-3: Risikomanagement. Risikoanalyse auf der Basis von IT-Grundschutz. Bundesamt für Sicherheit in der Informationstechnik. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/Standard203/ITGStandard203_node.html [23.12.2018]
- Davis, F., Bagozzi, P. and Warshaw, P. (1989). User acceptance of computer technology - a comparison of two theoretical models, *Management Science* 35(8), 982–1003.
- Dehnbostel, P. (2007): *Lernen im Prozess der Arbeit*, Studienreihe Bildungs- und Wissenschaftsmanagement, Bd. 7, Münster
- DGUV Information 215-450 - Softwareergonomie. Verfügbar unter http://regelwerke.vbg.de/vbg_dguvi/di215-450/di215-450_84_.html [28.12.2018].
- DGUV (2018). Fachbereich Holz und Metall. Sachgebiet Mschienen, Robotik und Fertigungsautomation. Safety und Security in der vernetzten Produktion: verfügbar unter: <https://publikationen.dguv.de/dguv/pdf/10002/12761.pdf?src=asp-cu&typ=pdf&cid=6998> [28.01.2019]
- DIN EN 894-3:2010-01: Sicherheit von Maschinen - Ergonomische Anforderungen an die Gestaltung von Anzeigen und Stellteilen - Teil 3: Stellteile. Beuth.
- DIN EN ISO 10075-1 : 2017-01. Ergonomische Grundlagen bezüglich psychischer Arbeitsbelastung -Teil 1: Allgemeine Aspekte und Konzepte und Begriffe. Beuth.
- DIN EN ISO 11064-5 (Ergonomische Gestaltung von Leitzentralen - Teil 5: Anzeigen und Stellteile)
- DIN EN ISO 6385:2004 – Grundsätze der Ergonomie für die Gestaltung von Arbeitssystemen.
- DIN EN ISO 9241-110:2008-09 – Ergonomie der Mensch-System-Interaktion – Grundsätze der Dialoggestaltung. Beuth.
- DIN EN 894-3 (Sicherheit von Maschinen - Ergonomische Anforderungen an die Gestaltung von Anzeigen und Stellteilen - Teil 3: Stellteile)

- DIN ES ISO 26800:2011-11 – Ergonomie – genereller Ansatz, Prinzipien, Konzepte. Beuth.
- DIN IEC 60050-351:2014-09: Internationales Elektrotechnisches Wörterbuch - Teil 351: Leittechnik (IEC 60050-351:2013). Beuth-Verlag.
- Dombrowski, U. & Wagener, T. (2014): Arbeitsbedingungen im Wandel der Industrie 4.0. Mitarbeiterpartizipation als Erfolgsfaktor zur Akzeptanz und Kompetenzentwicklung. In: Zeitschrift für wirtschaftlichen Fabrikbetrieb, 109(5) 351–355.
- EEMUA 191 (1999). Alarm systems - a guide to design, management and procurement. Verfügbar unter: <https://www.eemua.org/Products/Publications/Print/EEMUA-Publication-191.aspx>.
- Eigenstetter (2018). Eine Annäherung an das Konstrukt Verantwortung im Kontext von Sicherheit. In M. Eigenstetter, S. Darlington & F. Klingels (Hrsg.), Verantwortlich Denken und Handeln in komplexen Umwelten. Hintergründe, Herausforderungen, Gestaltungsmöglichkeiten. (S. 13-24). Verlag für Polizeiwissenschaft.
- Eigenstetter, M., Dobiasch, S., Trimpop, R. (2007). Commitment and Counterproductive Work Behavior as Correlates of Ethical Climate in Organizations. Monatschrift für Kriminologie und Strafrechtsreform, 90 (2/3), 224-244.
- Endsley, M. (2017) From Here to Autonomy: Lessons Learned from Human–Automation Research. *Human Factors*, 59 (1), 5-27. DOI: 10.1177/0018720816681350
- Endsley, M.R. (2000). Theoretical underpinnings of situation awareness: A critical review. In M.R. Endsley & D.J. Garland (Eds.), *Situation awareness analysis and measurement*. Mahwah, NJ: LEA.
- GDA, Gemeinsame Deutsche Arbeitsschutzstrategie Arbeitsprogramm Psyche (2017). Arbeitsschutz in der Praxis Empfehlungen zur Umsetzung der Gefährdungsbeurteilung psychischer Belastung https://www.gda-psyche.de/SharedDocs/Downloads/DE/empfehlungen-zur-umsetzung-der-gefaehrdungsbeurteilung-psychischer-belastung.pdf?__blob=publicationFile&v=1 [16.12.2018]
- Gräf, J. (2011), Risikomanagement: Umsetzung und Integration in das Führungssystem, in: *Risikomanagement und Risiko-Controlling*, Der Controlling-Berater, Bd. 16, S. 51-73.
- Grote, (2018). Kontrolle und Verantwortung in automatisierten Systemen. In M. Eigenstetter, S. Darlington & F. Klingels (Hrsg.), *Verantwortlich Denken und Handeln in komplexen Umwelten*. Hintergründe, Herausforderungen, Gestaltungsmöglichkeiten. (S. 117-125). Verlag für Polizeiwissenschaft.
- Grote, S., Kauffeld, S., Billich-Knapp, M., Lauer, L., Frieling, E. (2012): Implementierung eines Kompetenzmanagementsystems: Phasen, Vorgehen und Stolpersteine. In S. Grote, S. Kauffeld und E. Frieling (Hrsg.): *Kompetenzmanagement. Grundlagen und Praxisbeispiele*, 2. Aufl., Stuttgart: Schäffer-Poeschel, S. 35–56.
- Heyse, V. & Erpenbeck, J. (2009): *Kompetenztraining. 64 modulare Informations- und Trainingsprogramme für die betriebliche, pädagogische und psychologische Praxis*. 2. Aufl., Stuttgart
- Hoff, K. & Bashir, M. (2014). Trust in Automation: Integrating Empirical Evidence on Factors That Influence Trust. *Human Factors*, 57, (3), 407-434.
- Informatik aktuell (2018a). Amazon: Algorithmus mit unerwünschten Nebenwirkungen. Verfügbar unter: <https://www.informatik-aktuell.de/aktuelle-meldungen/2018/oktober/amazon-algorithmus-mit-unerwuenschten-nebenwirkungen.html> [28.12.2018]
- Informatik aktuell (2018b). UX als Innovationstreiber von Industrie 4.0 & Digitalisierung. Verfügbar unter: <https://www.informatik-aktuell.de/entwicklung/methoden/ux-als-innovationstreiber-von-industrie-40-digitalisierung.html> [28.12.2018]
- ISO 31000: 2018. Risk management — Risk management – Guidelines, provides principles, framework and a process for managing risk. International Organization for Standardization.
- Joiko, K., Schmauder, M., Wolff, G. (2010). *Psychische Belastung und Beanspruchung im Berufsleben Erkennen – Gestalten*. Herausgeben von Bundesanstalt für Arbeitsschutz und Arbeitsmedizin. Verfügbar unter https://www.baua.de/DE/Angebote/Publikationen/Praxis/A45.pdf?__blob=publicationFile [16.12.2018]
- Kahnemann, D. (2012). *Schnelles Denken, langsames Denken*. Siedler Verlag
- Kirby, T. & Davenport, J. (2015). Beyond Automation. *Harvard Business Review*. Verfügbar unter https://hbr.org/2015/06/beyond-automation?cm_sp=Nav%20Landing_-_Links_-_Featured%20Item [15.04.2017].

- Klein, G., Woods, D., Hoffman, R.R., Feltovich, P.J. (2004). Ten challenges for making automation a "team player" in joint human-agent activity. Verfügbar unter: <https://ieeexplore.ieee.org/document/1363742/figures#figures> [23.12.2018]
- Langhoff, T. (2009): Den demographischen Wandel im Unternehmen erfolgreich gestalten. Eine Zwischenbilanz aus arbeitswissenschaftlicher Sicht. Berlin, Heidelberg: Springer Berlin Heidelberg.
- LANUV (2015) – Leitfaden Alarmmanagement. Verfügbar unter: https://www.lanuv.nrw.de/fileadmin/lanuvpubl/4_arbeitsblaetter/Arbeitsblatt_27.pdf. Landesamt für Natur, Umwelt und Verbraucherschutz Nordrhein Westfalen.
- Lee, J. (2006). Human factors and ergonomics in automation design. In G. Salvendy, (Ed.), Handbook of Human Factors (p. 1570-1596). Wiley.
- Levchuk, I., Klußmann, A., Lang, K-H., & Gebhart, H. (2011): Verfahren der Usability-Evaluation - Methoden und Instrumente zur Prüfung von Gebrauchstauglichkeit von Produkten. Aser.
- Lüdtke, A. (2015). Wege aus der Ironie in Richtung ernsthafter Automatisierung. In A. Bothof, und E. Hartmann (Hrsg.) Zukunft der Arbeit in Industrie 4.0. Springer
- Manzey, D. (2008). Systemgestaltung und Automatisierung. In P. Badke-Schaub, G. Hofinger & K. Lauche (Hrsg.), Human Factors. Psychologie sicheren Handelns in Risikobranchen (S. 308-324). Springer.
- Misselhorn, C. (2018). Grundfragen der Maschinenethik. Reclam.
- Moshagen, M., Thielsch M. T. (2019). Facets of visual aesthetics. In: International Journal of Human-Computer Studies. 68 (10), S. 689–709
- Neuhäuser, C. & Hübscher, M. (2010). Unternehmen, ihre (ethische) Governance und Menschenrechte. In: S. Byrd, J. Hruschka, J. Joerden (Hrsg.), Jahrbuch für Ethik und Recht. Band 18 (S. 349-368). Berlin: Duncker & Humblot.
- Nof, S. Y. (2009). Automation: What it means around the world. In S. Y. Nof (ed.), Springer Handbook of Automation (p.13-52). Springer: Berlin, Heidelberg.
- North, K; Reinhardt, K; Sieber-Suter, B. (2013): Kompetenzmanagement in der Praxis. Mitarbeiterkompetenzen systematisch identifizieren, nutzen und entwickeln. 2. Aufl., Wiesbaden: Springer Gabler.
- Offensive Mittelstand (2018a). Einstieg in die digitale Transformation. Entscheidungshilfen für kleine und mittlere Unternehmen aller Branchen zum Thema Arbeit 4.0. Verfügbar unter: <https://www.inqa.de/DE/Angebote/Publikationen/kmu-entscheidungshilfen.html> [28.12.2018]
- Parasuraman, R. Sheridan, T. & Wickens. C. (2000). A model for types and levels of human interaction with automation. IEEE Systems, Man, and Cybernetics Society, Part A Syst. Hum. 30(3), 286-297
- Piko, T. & Bertram, A. (2018). Current Intelligence: Expertise über Ethik und Sicherheit als nachrichtendienstliches Produkt (S. 201-212). Verlag für Polizeiwissenschaft.
- Plattner, H., Meinel, C. & Weinberg, U. (2009). Design thinking. Innovation lernen. Ideenwelten öffnen. München: Finanzbuch Verlag.
- Prümper (o.J.). Fragebogen ISONORM 9241/10 verfügbar unter: http://www.ergo-online.de/site.aspx?url=html/software/verfahren_zur_beurteilung_der_fragebogen_isonorm_online.htm. [16.12.2018]
- Robelski, S. (2016). Psychische Gesundheit in der Arbeitswelt Mensch-Maschine-Interaktion. Forschung Projekt F 2353. Herausgegeben von der Bundesanstalt für Arbeitsschutz und Arbeitsmedizin. https://www.baua.de/DE/Angebote/Publikationen/Berichte/F2353-4d.pdf?__blob=publicationFile&v=14 [28.12.2018].
- Robertson, T. & Simonson, J. (2013). Participatory Design: an introduction. In J. Simonson und T. Robertson (Hrsg.), Routledge International handbook of participatory design (S. 1-17): New York: Routledge.
- Schäfer, M. & Keppler, D. (2013). Modelle der technikorientierten Akzeptanzforschung Überblick und Reflexion am Beispiel eines Forschungsprojekts zur Implementierung innovativer technischer Energieeffizienz-Maßnahmen. Discussion paper Nr. 34/2013. Zentrum Technik und Gesellschaft. Verfügbar unter: https://www.tu-berlin.de/ztg/menue/publikationen/discussion_papers/ [23.12.2018]

- Soule, D., Puram, A., Westerman, G. & Boennet, D. (2016). Becoming a digital organization. The journey to digital dexterity. MIT Center für Digital Business. Working Paper #301. Verfügbar unter https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2697688 [15.04.2017].
- TRBS 1151, Technische Regeln für Betriebssicherheit für Gefährdungen an der Schnittstelle Mensch - Arbeitsmittel – Ergonomische und menschliche Faktoren, Arbeitssystem. Verfügbar unter: https://www.baua.de/DE/Angebote/Rechtstexte-und-Technische-Regeln/Regelwerk/TRBS/pdf/TRBS-1151.pdf?__blob=publicationFile&v=2 [16.12.2018]
- User Interface Design GmbH (o.J.). Attrakdiff. Verfügbar unter <http://www.attrakdiff.de/> [16.12.2018]
- VDI/VDE Gesellschaft Mess- und Automatisierungstechnik (2009). Automation 2020. Bedeutung und Entwicklung der Automation bis zum Jahre 2020. Verfügbar unter https://www.vdi.de/fileadmin/vdi_de/redakteur_dateien/gma_dateien/AT_2020_INTERNET.pdf [23.12.2018]
- Venkatesh, V., Thong, J. & Xu, X. (2012). Consumer Acceptance and Use of Information Technology: Extending the Unified Theory of Acceptance and Use of Technology, MIS Quarterly, Vol. 36, No. 1, 157-178.
- Venkatesh, V., Morris, M. Davis, G. & Davis, F. (2003). User Acceptance of Information Technology: Toward a Unified View, MIS Quarterly, 27 (3), 425–478
- WCAG (2009). Web Content Accessibility Guidelines (WCAG) 2.0. Verfügbar unter: <https://www.w3.org/Translations/WCAG20-de/> [18.12.2018]
- Weber, A. (2018). Security und Safety: Schnittstellen und Zielkonflikte. In M. Eigenstetter, S. Darlington & F. Klingels (Hrsg.), Verantwortlich Denken und Handeln in komplexen Umwelten. Hintergründe, Herausforderungen, Gestaltungsmöglichkeiten. (S. 102-116). Verlag für Polizeiwissenschaft.
- Wilde G. (1988). Risk homeostasis theory and traffic accidents: propositions, deductions and discussion of dissension in recent reactions. Ergonomics (31), 441–68.

8 Endnoten

- ¹ Nof (2009).
- ² VDI/VDE Gesellschaft Mess- und Automatisierungstechnik (2009).
- ³ Nof (2009).
- ⁴ Nof (2009).
- ⁵ BAST (2012).
- ⁶ Parasuraman et al. (2000).
- ⁷ Hoff und Bashir (2014).
- ⁸ Schäfer und Keppler (2013).
- ⁹ Davies et al. (1989).
- ¹⁰ Venkatesch et al. (2003).
- ¹¹ Venkatesh et al. (2012).
- ¹² Lüdtkke (2015); Lee (2006).
- ¹³ DGUV Fachbereich Holz und Metall (2018).
- ¹⁴ Gräf (2011).
- ¹⁵ dazu z.B. Kahneman (2016).
- ¹⁶ dazu auch Lüdtkke (2015); Wischmann (o.J).
- ¹⁷ Lüdtkke (2015), S.127.
- ¹⁸ Lee (2006).
- ¹⁹ Lee (2006); Manzey (2008).
- ²⁰ Lee (2006); Manzey (2008).
- ²¹ Lee (2006).
- ²² Lee (2006); Wilde (1988).
- ²³ Endsley (2000), (2017).
- ²⁴ Langhoff (2019).
- ²⁵ Bitkom (2018).
- ²⁶ Weber (2018).
- ²⁷ Weber (2018).
- ²⁸ DGUV Fachbereich Holz und Metall (2018).
- ²⁹ Weber (2018); Berufsverband der Rechtsjournalisten e.V. o.J.).
- ³⁰ Offensive Mittelstand (2018a).
- ³¹ Offensive Mittelstand (2018a).
- ³² Piko und Bertram (2018).
- ³³ Eigenstetter et al. (2007).
- ³⁴ Piko & Bertram (2018), S. 205.
- ³⁵ Piko & Bertram (2018), S. 205).

-
- ³⁶ Eigenstetter et al. (2007); Eigenstetter (2018).
³⁷ Neuhäuser und Hübscher (2010).
³⁸ Informatik aktuell (2018a).
³⁹ Misselhorn (2018).
⁴⁰ Grote (2018), S. 124.
⁴¹ Misselhorn (2018).
⁴² Misselhorn (2018).
⁴³ Misselhorn (2018), S. 129.
⁴⁴ Robelski (2016).
⁴⁵ Lüdtke (2015); Klein et al. (2004).
⁴⁶ Parasuraman et al. (2000).
⁴⁷ Lüdtke (2015).
⁴⁸ BAUA (o.J.).
⁴⁹ Levchuk et al. (2009).
⁵⁰ Moshagen & Tielsch (2010).
⁵¹ Informatik aktuell (2018b).
⁵² Grote (2018).
⁵³ Boos et al. (2013), zitiert nach Grote (2018).
⁵⁴ EEMUA 191 (1999).
⁵⁵ Bockelmann et al. (2012); LANUV (2015).
⁵⁶ Grote (2018).
⁵⁷ Dombroski & Wagener (2014); Langhoff (2009); North et al. (2013).
⁵⁸ Grote et al. (2012).
⁵⁹ North et al. (2013).
⁶⁰ Langhoff (2009).
⁶¹ North et al. (2013).
⁶² Heyse & Erpenbeck (2009); Dehnbostel (2007).
⁶³ Kirby & Davenport (2015).
⁶⁴ Soule et al. (2016).
⁶⁵ Brynjolfsson und MacAfee (2014).
⁶⁶ Antoni (1999).
⁶⁷ Plattner et al. (2009).
⁶⁸ Robertson & Simonson (2013), S. 9.
⁶⁹ Beyer & Holtzblatt (1998).
⁷⁰ Venkatesh et al. (2012).
⁷¹ Plattner et al. (2009).

Die Arbeiten aus dem CSR-Kompetenzzentrum Textil & Bekleidung Niederrhein

Der Aufbau des CSR-Kompetenzzentrum Textil & Bekleidung Niederrhein wird im Rahmen des EFRE. NRW 2014-2020 vom Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes NRW gefördert.

Die vorliegenden csr.impuls.booklets wurden in Kooperation von den Projektpartnern und mitwirkenden Unternehmen im Rahmen des Projektes erstellt.

Ein csr.impuls.booklet bietet einen ersten Einstieg in das jeweilige Themenfeld. Die dazugehörigen csr.impuls.papiere geben einen vertiefenden Einblick: Mit einem Selbstcheck, vertiefenden Hintergrundinformationen und empirischen Daten aus dem Projekt erhalten interessierte Unternehmen einen Überblick und können selbst tätig werden.

csr.impuls.booklets und csr. impuls.papiere gibt es zu den CSR-Themen:

- 1 Business Case: Grüne Logistik
- 2 Business Case: Menschenwürdige Arbeitsbedingungen in der Wertschöpfungskette
- 3 Business Case: Veredlung/Färbung und CSR
- 4 Business Case: Arbeitgeberattraktivität und CSR
- 5 Blickpunkt: Digitalisierung und CSR

Die csr.impuls.booklets als auch die dazugehörigen csr.impuls.papiere lassen sich auf den folgenden Webseiten herunterladen:

www.csr-textil-bekleidung.de
www.hs-niederrhein.de/forschung/ethna/

Bildnachweis: Titelbild iStock, weitere Bildnachweise sind den Unterschriften der Abbildungen zu entnehmen.

Impressum

CSR Kompetenzzentrum
Textil & Bekleidung Niederrhein
c/o
WFMG Wirtschaftsförderung Mönchengladbach GmbH
Neuhofstr. 52, 41061 Mönchengladbach

Projektpartner

