Spitzencluster

Technologie-Akzeptanz: Von Maschinenstürmern zu Change Agents

Das Technologie-Netzwerk: Intelligente Technische Systeme OstWestfalenLippe

it's owl

Das Technologie-Netzwerk:
Intelligente Technische Systeme OstWestfalenLippe

it's owl

Von Maschinenstürmern zu Change Agents

Intelligente Technische Systeme im Spiegel von vier Jahrzehnten Technikfolgenabschätzung

DR. MARC MÖLDERS

ANDREAS HEIDENREICH

Stand: 26. November 2013

Servicestelle TA in der Clusternachhaltigkeitsmaßnahme [itsowl-TA]
„Akzeptanz gewährleisten - Technik sozial- und humanverträglich gestalten“

Dr. Marc Mölders
Universität Bielefeld
Fakultät für Soziologie
Postfach 100 131

D-33501 Bielefeld

Tel.: +49-521-106-4674
Fax: +49-521-106-6418
marc.moelders@uni-bielefeld.de
http://www.uni-bielefeld.de/soz/las/TA/itsowl/

Inhalt

Zusammenfassung

Themen im Kontext von „Automatisierung“ standen von Beginn an im Mittelpunkt des Interesses der Technikfolgenabschätzung (TA). Die vorliegende Studie unternimmt den Versuch, die wesentlichen Resultate aus vier Jahrzehnten diesbezüglicher Forschungspraxis für die Clusterthematik intelligenter technischer Systeme (ITS) aufzubereiten, auch um als Grundlage für eine betriebsinterne „TA im Kleinen“ fungieren zu können.

In vier thematischen Blöcken werden die wesentlichen Resultate zusammengefasst: (1) *Partizipatives Change Management*: Die mit der „vierten industriellen Revolution“ einhergehenden Veränderungen der Beschäftigungsstruktur werden unternehmensintern wie -extern besser akzeptiert, wenn die Betroffenen Teil des Umstellungsprozesses werden. (2) *Die Autonomie von Mensch UND Maschine*: In diesem Zusammenhang kommt es darauf an, die Entwicklung von ITS nicht als Nullsummenspiel (Je mehr Autonomie an die Maschine abgegeben wird, desto weniger autonom ist der Mensch), sondern als Verbesserung der Zusammenarbeit von Mensch und Maschine aufzufassen. (3) *Riskantes Vertrauen*: Gerade das reibungslose Funktionieren komplexer Abläufe kann zu Sorglosigkeit und übermäßigem Vertrauen in ITS führen. Insofern gilt es hier, einerseits entlastendes Vertrauen in neue Technologie zu gewinnen, ohne dabei andererseits die Aufmerksamkeit für (seltene) Störungen zu verlieren. (4) *Sicherheit in allen Facetten*: Sicherheit und Schutz (*Safety & Security*) sind für vernetzte Technologien in vielen Hinsichten zentral: Der Schutz der Privatsphäre („gläserner Mitarbeiter“), der Schutz vor Un- oder Ausfällen (Arbeitssicherheit, aber auch neue Technologien zur Verbesserung des Arbeitsschutzes) und vor Angreifern (Datensicherheit), eine zuverlässig funktionierende Vernetzung (Netz(werk)sicherheit) und schließlich Rechtssicherheit (damit allgegenwärtige Technik nicht mit „allgegenwärtiger Unverantwortlichkeit“ einhergeht) sind hier zu nennen.

Jeder dieser Abschnitte schließt mit einem übersichtlichen Frageblock, der eine Anwendung in den Clusterunternehmen erlauben soll. Weitere Hinführungen finden sich im letzten Abschnitt als „Allgemeine Reflexionsanregung und Fazit“.

Einleitung und Rahmung

Die Themen „intelligente technische Systeme“ oder „Industrie 4.0“ sind vergleichsweise jung. Diese Aktualität findet in Studien der Technikfolgenabschätzung (*technology assessment*; TA) durchaus ihren Niederschlag. Die vorliegende Analyse zu laufenden und bereits abgeschlossenen Studien in diesem Feld hat sich dennoch nicht allein auf die o.a. Themen beschränkt. Früh wurde im Zuge erster Recherchen deutlich, dass die in den gegenwärtigen Untersuchungen gezogenen Schlüsse in Entwicklungslinien stehen, die die TA gewissermaßen von ihrem Beginn an begleiten. Als „Geburtsstunde“ institutionalisierter TA gilt gemeinhin die Eröffnung des „Office of Technology Assessment“ (OTA), das 1972 ins Leben gerufen wurde, um den US-Kongress in Fragen wissenschaftlich-technischer Entwicklung zu beraten. Schon in ihren ersten Studien beschäftigt sich das OTA mit Themen wie „automation“, „ambient intelligence“, „(anthropocentric) robotics“ oder „persuasive technology“. So wird verständlich, warum die im Rahmen unserer Auswertung entstandene Datenbank[1] mit einer OTA-Studie aus dem Jahre 1975 beginnt.

Dem Thema „Automation“ kommt dabei, wie sich zeigen wird, eine besondere Bedeutung zu. Das deutet einerseits darauf hin, dass wir es mit einem gut erforschten Thema zu tun haben. Andererseits ist Automatisierung zu einem so dynamischen Feld geworden, dass etwa die aktuellen Entwicklungen zu vernetzten Systemen auch die sie begleitenden TA-Studien vor immer neue Herausforderungen stellen.

Die folgende Darstellung orientiert sich in erster Linie an den in diesen Studien identifizierten zentralen Konfliktlinien. Dabei geht es zunächst darum, die jeweiligen Problematiken nachvollziehbar zu machen. In einem zweiten Schritt soll die Aufbereitung dieser Ergebnisse einen Einstieg zur selbständigen Durchführung erster TA-Prozesse in Unternehmen ermöglichen. Eine solche „TA im Kleinen“ soll in seiner Breite und Tiefe über herkömmliche Methoden des Marketings oder der Meinungsforschung wie der bloßen Identifikation von Zielgruppen, Kundenpräferenzen o.ä. hinausgehen und sowohl die Gestaltungs- als auch Implementierungsphase beglei-

[1] http://www.uni-bielefeld.de/soz/las/TA/itsowl/dokumente.html

ten und bei der Antizipation möglicher Konfliktpunkte behilflich sein.

Die im Rahmen des Spitzenclusters „Intelligente Technische Systeme OstWestfalen-Lippe“ (it’s OWL) angestrebten Produkte und Technologien beziehen sich in aller Regel auf sogenannte b2b-Lösungen („business to business“). Diesem Umstand Rechnung tragend fokussieren wir uns im Folgenden auf mögliche Effekte intelligenter technischer Systeme auf die Arbeitsumgebung und die Beschäftigten. Ausgeklammert bleiben dementsprechend mögliche Konsequenzen beim Endbenutzer in der „außerbetrieblichen Umwelt“. Unsere Anregungen sind so allgemein wie nötig formuliert, um ihre Anwendung auf die zahlreichen unterschiedlichen Projekte im Spitzencluster so konkret wie möglich gestalten zu können.

Anhand vier thematischer Schwerpunkte werden denkbare Herangehensweisen an die Identifikation möglicher krisenhafter Aspekte intelligenter technischer Systeme aufgezeigt. (1) Zunächst steht die Gestaltung von Arbeitsplatzveränderungen im Mittelpunkt. (2) Es folgt eine Auseinandersetzung mit Fragen der Autonomie des Menschen bzw. des Zusammenarbeitens autonomer Maschinen und Menschen unter den Bedingungen zunehmend eigenständiger „Produktionsmittel“. (3) Die Gefahren eines unhinterfragten Vertrauens in automatisierte technische Systeme werden ebenso thematisiert wie (4) Fragen des Datenschutzes und der Privatsphäre bei der Nutzung intelligenter technischer Systeme. Sicherheit und Schutz sind für vernetzte Technologien in weiteren Hinsichten zentral: Arbeitssicherheit und -schutz, Daten-, Netzwerk- und Rechtssicherheit.

In einem abschließenden Schritt wird erörtert, was den Entwicklern im konkreten Gestaltungsprozess intelligenter technischer Systeme eine Hilfestellung hinsichtlich der Identifikation sozial folgenreicher Effekte sein und wie ihnen ggf. begegnet werden könnte.

1. Partizipatives Change Management

Für die generelle Akzeptanz eines technischen Systems im Arbeitsprozess scheint, folgt man den Ergebnissen einiger Studien, die sogenannte „*technological literacy*" ein wesentlicher Faktor zu sein. Hiermit ist eine oftmals implizite und nicht weiter hinterfragte Vertrautheit (im Sinne eines „*tacit knowledge*") mit den Funktionsweisen und dem Gebrauch komplexer technischer Artefakte gemeint. Dies führe zu einer generell wohlwollenderen Haltung gegenüber neuartigen technischen Systemen. So wurde technological literacy auch als Erklärung dafür herangezogen, dass die Computerisierung und Automatisierung der Industrie in Japan eher begrüßt wurde als in anderen westlichen Industrienationen (vgl. OTA 1982, S. 17). Trifft diese These zu, dürften für unseren Fall die Bedingungen für die prinzipielle Akzeptanz intelligenter technischer Systeme geradezu ideal sein. Im Allgemeinen lässt sich eine Selbstverständlichkeit im Umgang mit neuer Technik, etwa PC oder Smartphone, in wohlhabenderen Regionen generationenübergreifend ausmachen. Im Besonderen sind die Arbeitsumgebungen, in denen die zu entwickelnden intelligenten technischen Systeme zum Einsatz kommen werden, ohnehin bereits weitreichend technisiert. Den betreffenden Beschäftigten wird der Einsatz von Technik in ihrem Arbeitsalltag folglich alles andere als fremd sein. Insofern müssten sich die Maßnahmen zur Sicherstellung von Akzeptanz und Nachhaltigkeit vorrangig auf die spezifische Beschaffenheit des konkreten intelligenten technischen Systems und der Arbeitsumgebung, in der es zum Einsatz kommen soll, richten. Die Wahrscheinlichkeit von Akzeptanz lässt sich möglicherweise auch durch Hinweise darauf erhöhen, dass Technik schon vor einer etwaigen Umstellung die Arbeitsbedingungen geprägt hat. Solche Schlussfolgerungen basieren allerdings auf der Annahme, dass sich mit den technischen Entwicklungen *dieselben* Belegschaften auseinanderzusetzen haben.

Die Sorge vor dem Verlust des eigenen Arbeitsplatzes durch effizientere Maschinen dürfte wohl so alt sein wie die Industrialisierung selbst. Wie die sogenannten Maschinenstürmer im 19. Jahrhundert gegen die Mechanisierung ihrer Manufakturen vorgingen, so wurde der Einzug von Computern und Automatisierung in die Produktionsstätten – gewissermaßen die industriellen Revolutionen 1.0 bis 3.0 – seitens

der Beschäftigten generell mit großer Skepsis begleitet (vgl. OTA 1982, S. 14ff.; OTA 1984, S. 101ff.). Dies trifft insbesondere auf das vermittelnde und koordinierende mittlere Management zu (vgl. OTA 1982, S. 37).

In summarischer Rückschau mag diese Sorge angesichts der Beschäftigungszahlen in den entsprechenden Branchen als unberechtigt erscheinen. Für den Einzelnen hat sie sich allerdings häufig bewahrheitet. Einzelfälle dieser Art muss eine Maßnahme, die die Sozialverträglichkeit intelligenter technischer Systeme gewährleisten soll, in den Blick nehmen. Dies gilt im Falle des Spitzenclusters „it's OWL" umso mehr, da eines der strategischen Ziele neben der Sicherung von 80.000 bestehenden Arbeitsplätzen in den entsprechenden Branchen die Schaffung 10.000 neuer Arbeitsplätze ist.[2]

Dass eine Technologie eine Branche um 10.000 Arbeitsplätze wachsen lässt, ist zunächst sicherlich erfreulich. Doch auch eine technologische Entwicklung, die nicht zum Rückgang der absoluten Beschäftigungszahlen („*job loss*") führt oder diese sogar steigen lässt, muss man sich genauer ansehen. Wird etwa im Zuge einer solchen Entwicklung das Personal auf breiter Front ausgewechselt („*job shift*"), stellt sich dieser Erfolg aus der Perspektive der „Verlierer" anders dar. Ganz grundsätzlich bedeutet dies, dass sich anhand der absoluten Beschäftigungszahlen allein eine Veränderung der Beschäftigungsstruktur gar nicht feststellen lässt. Eine auf Nachhaltigkeit ausgelegte Technikbewertung muss auch die Frage stellen, wer in Zukunft überhaupt zur Beschäftigung in Frage kommt, ob die zukünftigen Nutzer noch die Arbeitenden und Angestellten von heute sein sollen.

Im Sinne der Sozialverträglichkeit ist es notwendig, möglichst im Vorfeld klarzustellen, wer von einer technologischen Entwicklung – beispielsweise aufgrund von Qualifikationsniveaus – in welcher Weise voraussichtlich bedroht ist und wie ggf. potentielle „Verlierer" dieser Bedrohung entgehen können. Als zentral in diesem Zusammenhang wird die frühzeitige und breite Partizipation der Belegschaft an Veränderungsprozessen eingeschätzt.

So fasst Michael Decker (2012: 183) in Bezug auf die Zunahme von „Service Robots" zusammen:

---

[2] Vgl. http://www.its-owl.de/technologiecluster/die-vision/ansatz-ziele.php

- Early and continuous cooperation between planners, developers, and users
- Take corporate strategy into consideration
- Worker participation and participatory style of leadership
- Integration of those affected
- Early and comprehensive measures to provide information and training.

Diese aktuelle Studie bezieht sich explizit auf die vom Verein Deutscher Ingenieure (VDI) bzw. der VDI-Hauptgruppe „Der Ingenieur in Beruf und Gesellschaft“ herausgegebene Handlungsempfehlung „Sozialverträgliche Gestaltung von Automatisierungsvorhaben“ aus dem Jahre 1989, die mit Recht in diesem Kontext als Meilenstein gilt. Hierin findet sich auch ein umfangreicher Katalog von Leitfragen, der auf spezifische Automatisierungsvorhaben zugeschnitten werden kann.[3] Aufgrund ihres Umfangs können die zahlreichen wertvollen Hinweise dieser Handlungsempfehlung hier nicht einzeln gewürdigt werden. Grundlegend aber können die u.a. Ausgangsfragen eine sozialverträgliche Gestaltung von Automatisierungsvorhaben anleiten.

Der VDI hat sich auch in neueren Publikationen dem Thema „Automation 2020“ gewidmet (VDI 2009; 2013). In Bezug auf die Veränderung der Beschäftigungsstruktur spricht der Verband von einem Paradigmenwechsel „von der autarken technischen Lösung hin zu einem Problemlöser als ‚Partner des Menschen‘ im Sinne von ‚Technik mit dem Menschen für den Menschen‘“ (VDI 2013, S. 12). Man geht davon aus, dass sich die Zahl der Arbeitsplätze erhöhen wird. Dabei sei aber vor allem an neue Berufsfelder zu denken, die der steigenden Bedeutung von Dienstleistungen und Forschungs- und Entwicklungstätigkeiten im Rahmen von Produktion Rechnung tragen. Dazu sei auch das Berufsbild des Ingenieurs im Allgemeinen nachhaltig zu verbessern, das Studium der Automation im Besonderen attraktiver zu gestalten (vgl. ebd. S. 17). Gerade das in der Entstehung befindliche Feld der „Industrie 4.0“ erfordere die Sicherstellung einer lebenslangen Weiterbildung, um mit dieser Entwicklung

[3] Behandelt werden: Arbeitsbedingungen/Arbeitsorganisation, Entwicklung von Persönlichkeit und Fähigkeiten, Benutzerschutz, Übergreifende Auswirkungen von Automatisierungsvorhaben und Betriebswirtschaftliche Rahmenbedingungen. Vgl. VDI (1989) bzw. unsere Zusammenfassung und den „Leitfragenkatalog“ unter http://www.uni-bielefeld.de/soz/las/TA/itsowl/dokumente.html.

Schritt zu halten (vgl. ebd. S. 22).

Die schon beim VDI (1989) zu findende Betonung eines „*participatory style of leadership*“ ist von TA-Studien vielfach aufgenommen worden. Nicht zuletzt, um innerbetrieblichen Widerständen frühzeitig zu begegnen, ist es ratsam, Veränderungsprozesse gemeinsam mit den Betroffenen zu gestalten. Der Begriff „Betroffene“ wird dabei breit aufgefasst: Wen immer eine Umstellung vor weitreichende Veränderungen stellen wird, sollte beteiligt, informiert und gehört werden. Insofern werden Mitarbeitende selbst zu „*Change Agents*“.

Bei größeren Unternehmen wird aus der Frage der Beteiligung eine der angemessen Repräsentation unterschiedlicher interner Gruppen. Im Clusterkontext geht es oftmals um sogenannte b2b-Lösungen. Das bedeutet in diesem Zusammenhang, dass Veränderungen in der Beschäftigungsstruktur auch und gerade beim abnehmenden Unternehmen zu erwarten sind. Wie weitreichend die Kenntnis dieser Veränderungen jenseits des eigenen Unternehmens ist, kann nicht verallgemeinert und muss im Einzelfall beurteilt werden. Davon unbenommen erscheint es möglich, für entsprechende Veränderungen Interesse zu zeigen und ein partizipatorisches *Change Management* immerhin zu empfehlen bzw. darüber zu informieren, was insbesondere durch eigene diesbezügliche Erfolgsbeispiele („*best practice*“) vereinfacht würde.

- Welche Szenarien, die Gestaltung von Arbeitsplätzen betreffend, sind Gegenstand der Planung?
- Wen betreffen diese Veränderungen?
- Gibt es im Unternehmen Möglichkeiten, gemeinsam mit den Betroffenen die konkreten Veränderungen zu diskutieren?
- Gibt es im Unternehmen Abteilungen („*Change Management*“ o.ä.) oder Zuständige („*Change Agents*“), die solche Prozesse begleiten? Obliegt es den Führungskräften, diesen Wandel zu moderieren? Ist externe Beratung erwünscht?
- Wie kann früh über Veränderungen informiert werden? Wie wird später eine Gewöhnung gewährleistet? (Schulungen)
- Sofern es sich um Produkte handelt, die in anderen Unternehmen verwendet werden: Ist bekannt, wie die Veränderungen dort organisiert werden? Besteht die Möglichkeit, ein partizipatives Change Management zu empfehlen?

2. Die Autonomie von Mensch UND Maschine

Hinter dem Konzept intelligenter technischer Systeme steht der Zielgedanke, ein umfassendes System zu schaffen, dessen Teile auf eine Art und Weise miteinander kommunizieren, die es dem Gesamtsystem insofern autonom zu agieren erlaubt, als es sich die Probleme, die es zu lösen hat, selbsttätig sucht und schafft.[4]

Der oben skizzierte Fall des möglichen Arbeitsplatzverlusts und der vollständigen Ersetzung menschlicher Arbeitskraft ist nur die extreme Ausprägung eines Kontinuums der „Kompetenzübernahme" durch technische Systeme. Doch auch geringere Ausprägungen könnten sich als problematisch erweisen. Eine solche „Ent-Autonomisierung" des Menschen bedeutet demnach eine tendenziell zwingende Anpassung an die durch das technische System vorgegebenen Arbeitsabläufe (vgl. Moniz 2010, S. 4). Dies könnte vor allem dann zu erheblichen Spannungen führen, wenn die „Vorstellung" des intelligenten technischen Systems über einen bestimmten Arbeitsschritt von der des Menschen abweicht.

Ein mit weitreichender „Kontextsensitivität" ausgestattetes System könnte zwar auch in der Lage sein, entsprechend auf den jeweiligen Nutzer, dessen Vorlieben und „Eigenheiten" zu reagieren und sich entsprechend seinerseits anpassen. Allerdings ist hiermit das Problem aufgeworfen, dass ein zu häufiges und möglicherweise zu willkürliches Eingreifen in einen solchen Prozess die „Intelligenz" des technischen Systems und seine Implementierung (und dessen Entwicklung überhaupt) *ad absurdum* führen und dadurch das gesamte Kommunikationsgefüge des Systems in Mitleidenschaft gezogen werden könnte.

Insbesondere der Aspekt der Möglichkeiten und der Grenzen menschlichen Eingriffs – eines „*manual override*" – ist ein interessanter Punkt, an dem sich Fragen der wünschenswerten Grade der Autonomie (sowohl für den Menschen als auch für das technische System), der Zuverlässigkeit und des Vertrauens in „Technik" generell diskutieren lassen. Auf den ersten Blick mag ein nicht umstandslos steuerbares tech-

[4] Vgl. die Definition intelligenter technischer Systeme im Kontext des Spitzenclusters it's OWL: http://www.its-owl.de/technologiecluster/die-vision/intelligente-technische-systeme.php.

nisches System zwar Unbehagen und Ablehnung evozieren, doch ist eine menschliche Entscheidung nicht zwangsläufig der eines technischen Systems überlegen. Dies gilt insbesondere, wenn es auf eine ungleich größere und solidere Informationsbasis zurückgreifen kann (was selbstredend auch erst gewährleistet sein muss). Scheinbar paradoxerweise könnte also insbesondere in Gefahrensituationen die „Indifferenz" des technischen Systems zur besseren Entscheidung führen (vgl. RAE 2009, S. 3).

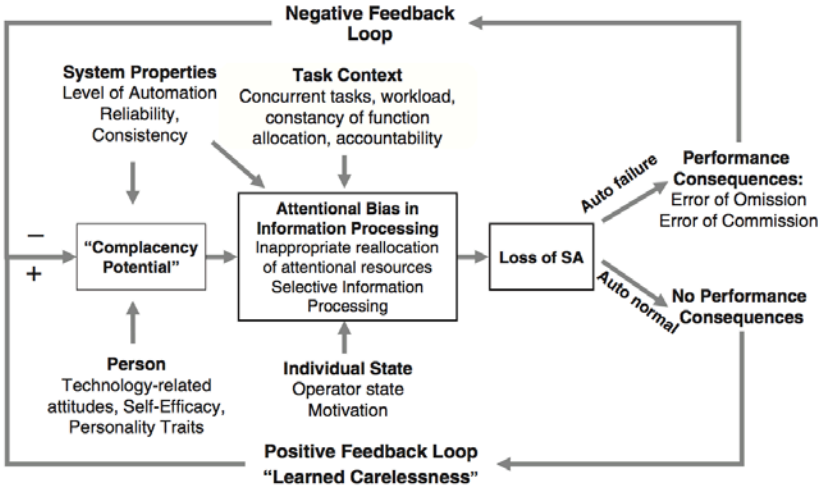
Eine interessante „Zwischenstufe" auf dem Weg zum autonomen technischen System diskutiert Verbeek (2009) am Beispiel der *„persuasive technology"*. Persuasive – also überzeugende, geradezu überredende – Technologie ist als eine Steigerung herkömmlicher Assistenz- und Nutzerinformationssysteme zu verstehen. Sie setzt den Gedanken konsequent fort, dass technische Artefakte mehr sind als Gegenstände, die der Mensch vollständig beherrscht: Setzt man sich etwa auf den Stuhl, weil man den ureigenen Wunsch verspürt, auf diesem zu sitzen, oder legt mir die Anwesenheit des Stuhls erst nahe, dass ich mich setzen könnte? Persuasive Systeme bieten dem Nutzer entsprechend nicht nur Informationen als Entscheidungsgrundlage, sondern versuchen, durch Handlungsempfehlungen eine Kooperation zwischen Mensch und Maschine zu stiften und eine vermittelnde Rolle einzunehmen (vgl. ebd. S. 237).

Die Mensch-Maschine-Interaktion ist ein lange etabliertes Thema in Theorie wie Praxis. Die vielen Arbeiten an technischen Lösungen („Schnittstellen") lassen sich sinnvoll ergänzen, wenn systematisch eruiert wird, wo Mitarbeitende Einschnitte durch Technik erleben. Ob es sich um ein Problem der Eingewöhnung handelt, das durch Schulungen und Training behoben werden kann, oder ob die Technik tatsächlich in einer unproduktiven Art und Weise die Autonomie ihres menschlichen Mitarbeiters beschneidet, lässt sich durch wenig standardisierte Erfahrungsberichte überhaupt erst in Erfahrung bringen.

- Sind die einzelnen Arbeitsschritte und deren Abfolge durchschaubar? Gibt es die Möglichkeit der realen Prozessverfolgung sowie Eingriffsmöglichkeiten?
- Ist allen Beteiligten klar, wann wer (Mensch/Maschine) das „letzte Wort" hat? Sind die entsprechenden Regeln allgemein verständlich?
- Werden Aus(nahme)fälle geprobt und ihre Beherrschung trainiert?
- Existiert eine Fehlertoleranz? Wie werden System- und Bedienungsfehler unterscheidbar?[5]
- Kann Mitarbeitenden die Gelegenheit eingeräumt werden, über ihre Erfahrungen – auch und gerade im Hinblick auf ihre Autonomie – zu berichten?

3. Riskantes Vertrauen

Das Versagen eines technischen Systems kann sich vor allem dann als besonders gravierend erweisen, wenn das Vertrauen in seine „Fähigkeiten" durch bis dato erwiesene Zuverlässigkeit unhinterfragt bleibt. Parasuraman und Manzey (2010) integrieren die Konzepte der „*situation awareness*" (Achtsamkeit), „*automation bias*" (übermäßiges Vertrauen in die Korrektheit eines automatisiert ablaufenden Prozesses) und „*complacency*" (Nachlässigkeit) in einem Modell einer Feedback-Schleife von menschlicher Unachtsamkeit und technischem Versagen:



Aus: Parasuraman/ Manzey (2010), S. 404

[5] Auch hierzu bietet der VDI-Leitfragenkatalog einige Hinweise, insbesondere im ersten Teil zu „Arbeitsbedingungen und Benutzerfreundlichkeit".

Im Wesentlichen sagt dieses Modell aus, dass ein wie gewünscht funktionierendes automatisiertes technisches System zu einer „gelernten Sorglosigkeit" („*learned carelessness*") führt. Diese führe dazu, dass der Anwender des technischen Systems (bzw. eine mit seiner Überwachung betraute Person) im Vertrauen auf die Zuverlässigkeit des automatisierten Prozesses seine Aufmerksamkeit vom technischen System ab- und sich beispielsweise anderen Tätigkeiten zuwendet (vgl. ebd., S. 390) – ebendies ist mit riskantem Vertrauen angesprochen. In diesem Zustand der Nachlässigkeit („*complacency*") ist die Person möglicherweise nicht in der Lage, etwaige Informationen über eine Fehlfunktion des technischen Systems hinreichend wahrzunehmen und unterlässt daraufhin das Ergreifen angemessener Maßnahmen („*error of omission*"). Oder aber sie handelt auf Basis fehlerhafter, allerdings nicht weiter überprüfter Informationen nur *scheinbar* angemessen („*error of commission*").

Bei einem intelligenten technischen System, welches von vornherein auf weitreichende Autonomie hin konzipiert ist, sind solche Effekte umso eher zu erwarten. Mehr noch würden sie ihren Status als *intelligentes* technisches System einbüßen, bedürften sie eines umfangreichen Monitorings im engeren Sinne. Um Probleme dieser Art zu vermeiden, müssen sie bei der Entwicklung des Systems und der Schulung der Mitarbeiter bedacht werden.

Im Kontext der Automatisierung der Luftfahrt sind solche Effekte gut erforscht und ließen sich in der Praxis[6] und in Simulator gestützten Studien mehrfach nachweisen. Konzepte übermäßigen und riskanten Vertrauens sind in der betreffenden Forschung so etabliert, dass sie bereits Einfluss sowohl auf die Technikgestaltung als auch auf Aspekte der Ausbildung hatten. In einer mittlerweile als klassisch geltenden Studie von Parasuraman et al. (1993) wurde festgestellt, dass die Wahrscheinlichkeit, dass ein Nutzer eine simulierte Fehlfunktion in einem automatisierten Fehlererkennungssystem identifiziert, um 149% höher ist, wenn das System *un*zuverlässig arbeitet (ebd., S. 10). Während 82% aller aufgetretenen Fehlfunktionen des unzu-

[6] Die Ursache vieler Flugzeugunfälle wird auf die beschriebenen Effekte zurückgeführt. So beispielsweise auch der Fall der Boeing 747 der Korean Airlines, die 1983 aufgrund eines fehlerhaften Autopiloten in sowjetischen Luftraum eindrang und in der Folge abgeschossen wurde. Die Crew ignorierte dabei alle Hinweise, die auf einen falschen Kurs hindeuteten und vertraute allein der Instrumentenanzeige.

verlässigen Systems erkannt wurden, lag diese Zahl im Falle des zuverlässigen Systems bei gerade einmal 33%. Mosier et al. (1998) fanden unter anderem einen starken *negativen* Zusammenhang zwischen der Fehlererkennung und der Flugerfahrung ihrer Probanden. Je erfahrener die Piloten sind, desto weniger Fehler finden diese in automatisierten Systemen bzw. reagieren auf sie nicht sachgemäß (ebd. S. 58f.).

Ein weiteres, in jüngerer Zeit zunehmend an Relevanz gewinnendes Feld für die Erforschung derartiger Effekte ist die klinische Praxis, da hier insbesondere für die Diagnostik vermehrt auf technische und automatisierte Lösungen, sogenannte „*clinical decision support systems*" (CDSS), zurückgegriffen wird. Unter diesem Begriff firmieren verschiedene Arten von technischen Systemen, beispielsweise sowohl durch den Nutzer anzusteuernde Informationsdatenbanken, die auf Basis zuvor erhobener Symptome eine Diagnose stellen, als auch voll automatisierte Bilddiagnostik. Goddard et al. (2012) stellten jüngst nach Sichtung der für dieses Feld relevanten Studien fest, dass sich der „*automation bias*" und den damit verbundenen Konsequenzen im Kontext der Nutzung von CDSS als robustes Konzept erwiesen hat (vgl. ebd. S. 123).

Eine an mehreren US-amerikanischen Kliniken durchgeführte Feldstudie zum Umgang des Gesundheitspersonals mit computerisierten und automatisierten Systemen (Campbell et al. 2007) kam u.a. zu dem Schluss, dass einige Nutzer dieser Systeme die ihnen bereit gestellten Informationen mitunter höher bewerteten als beispielsweise klinische Zeichen („if it's in a computer it must be accurate and complete", S. 96). Ferner sei die allgemeine Tendenz zu beobachten, dass mit der elektronischen Initiierung eines Prozesses dieser in der klinischen Praxis als faktisch vollzogen betrachtet wurde, so etwa bezüglich einer im System vermerkten Anordnung einer Medikamentengabe (vgl. ebd.).

Cornelius Schubert (2006) macht allerdings darauf aufmerksam, dass die klinische Praxis zu differenzieren ist. Für Anästhesisten etwa weist er nach, dass diese sich geradezu durch einen „methodischen Zweifel" an der Übereinstimmung der biologischen Realität des Patienten mit der technischen Repräsentation der Geräte auszeichnen. Bezogen auf eine intelligent vernetzte Produktionsweise, spricht dies für

die Entwicklung eines methodischen Zweifels, der das kontrollierende Ablesen von Funktionsanzeigen mit einem Blick auf die „Realität der vernetzten Maschinen“ kombiniert. Typisch für hochtechnisierte Bereiche sei, so Schubert, dass mit zunehmender Praxis auch ein Erfahrungswissen entsteht, das die Vereinbarkeit von stetiger Aufmerksamkeit einerseits und entlastender Routine andererseits ermöglicht.

Natürlich ist kehrseitig zu wenig Vertrauen nicht minder riskant als ein allzu sorgloser Umgang. So weisen wiederum Parasuraman et al. (2000) auch auf die Bedeutung des Gewinnens und Bewahrens von Vertrauen in intelligente technische Systeme durch deren Reliabilität hin. Als Beispiel führen die Autoren einen Fall an, in dem ein System aufgrund fehlerhaft erhobener Informationen häufig „falschen Alarm“ geschlagen hatte. Dies führte zu dem Effekt, dass die Nutzer nicht nur diesem einen fehlerhaften System misstrauten und es entsprechend ignorierten, sondern Automatisierung im Allgemeinen in Zweifel zogen und auch in Fällen kritisch prüfend tätig wurden, in denen dies nicht nötig gewesen wäre (vgl. ebd. S. 292).

- Wie wird das intelligente technische System überhaupt überwacht (Monitoring)? Fällt dies in den Kompetenzbereich einzelner, eigens hierfür Zuständiger? Wird diese Aufgabe von ebenso anderen Tätigkeiten nachgehenden Mitarbeiterinnen und Mitarbeitern übernommen?
- Ist den Beteiligten das Problem „riskanten Vertrauens“ bekannt?
- Kann die Routine in der Bedienung und Überwachung des Systems durch Teamarbeit abwechslungsreich gestaltet werden? Welche anderen Mechanismen zur Aufrechterhaltung von Aufmerksamkeit sind in diesem Zusammenhang vorgesehen?
- Wie schnell kann es realistisch möglich sein, Erfahrungswissen im Umgang mit der neuen Produktionsweise und ihrer Überprüfung zu erlangen?
- Kann ein „methodischer Zweifel“ an der Übereinstimmung zwischen einer Anzeige und dem tatsächlichen Funktionieren des Systems ausgebildet werden, ohne damit unzumutbare Effizienzeinbußen zu riskieren?

4. Sicherheit in allen Facetten

Mögliche Konflikte hinsichtlich der Privatsphäre und des Datenschutzes der Nutzer sind für die Sozialverträglichkeit intelligenter technischer Systeme von zentraler Bedeutung. Dies gilt insbesondere, wenn individuelle Nutzerprofile unterstützt werden (vgl. Brey 2005). Einerseits ist dabei natürlich zu bedenken, dass gesetzlichen Vorgaben entsprochen wird, andererseits sollte auch einer möglichen Wahrnehmung als „gläserner Mitarbeiter" vorgebeugt werden. Eine weitreichend vernetzte und Nutzerprofil gestützte Arbeitsumgebung könnte als umfassende Kontrollinfrastruktur gedeutet werden (vgl. OTA 1982, S. 16). Die „Transparenz" des technischen Systems ist in dieser Hinsicht von entscheidender Relevanz. Dem Nutzer muss hinreichend klar sein, wann und in welcher Weise er mit dem technischen System in Verbindung steht, d.h. konkret: welche Daten erfasst werden, wer in diese Einsicht nehmen kann etc. Gesteigert wird diese Problematik, wenn das technische System prinzipiell allgegenwärtig und nicht mehr an ein konkretes technisches Artefakt gebunden ist.

Ein solches „*ambient intelligence system*" (Verbeek 2009; Cook et al. 2007) zeichnet sich unter anderem dadurch aus, dass es möglichst nahtlos in die Umgebung integriert ist (also nicht notwendig über eine grafische Benutzeroberfläche oder dergleichen verfügt), auf seine Umwelt (auch auf die Handlungen des Nutzers) reagiert, personalisierbar ist, lernen und antizipieren kann (Verbeek 2009, S. 233). Die möglichen durch die Barrierefreiheit dieser Systeme geschaffenen Vorteile hinsichtlich ihrer intuitiven Bedienbarkeit könnten von möglichen Bedenken angesichts der eben erwähnten Kontrollierbarkeit durch Vorgesetzte oder sonstigem Missbrauch durch Dritte überwogen werden. Ferner könnte es sich auch als gangbar erweisen, die Schnittstellen als solche kenntlich zu machen, um auf diese Weise das technische System transparent zu gestalten und zumindest die Suggestion von Kontroll- und Steuerbarkeit herzustellen. Wo es sinnvoll ist, könnten Schnittstellen zur Steigerung der Akzeptanz tendenziell anthropomorphisiert werden, wie Erkenntnisse aus der Forschung zu humanoider Robotik nahelegen (vgl. Moniz 2009, S. 95).

In ihrer 2006 veröffentlichten Studie „Technikfolgen-Abschätzung Ubiquitäres Computing und Informationelle Selbstbestimmung“ (TAUCIS) haben das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) und das Institut für Wirtschaftsinformatik der Humboldt-Universität zu Berlin (HU) die Auswirkungen von vernetzten und allgegenwärtigen Technologien umfassend analysiert. Hieraus geht auch hervor, dass die Aspekte Schutz und Sicherheit im Kontext vernetzter Technologien unterschiedliche Bedeutungen annehmen können. Über den bereits beschriebenen Zusammenhang von Datenschutz und Privatsphäre hinaus, benennen die Autoren auch Sicherheit im Sinne von Schutz vor Unfällen oder Ausfällen (*Safety*) und vor Angreifern (*Security*) als relevante Dimensionen (vgl. ULD 2006, S. 71f.).

Einer maßgeblichen Publikation Kumar Ranganathans (2004) folgend, werden diese Fragen als zentrale und die genannten Dimensionen übergreifende identifiziert:

- Mit wem unterhalte ich mich?
- Wird meine Privatsphäre gewahrt bleiben?
- Kann ich dem Gerät trauen, mit dem ich kommuniziere?
- Gibt es eine Regressmöglichkeit?
- Werden die Dienste zuverlässig verfügbar sein?

Die hier unter den Stichworten „Safety & Security“ zusammengefassten Aspekte haben für den Spitzencluster in mehreren Hinsichten besondere Relevanz. Der Schutz vor Unfällen ist selbstredend ein Dauerthema zur Arbeitssicherheit in jeder Form der Produktion. Allerdings sind im Rahmen von it’s OWL auch Technologie geplant, die ihrerseits die Sicherheit am Arbeitsplatz erhöhen sollen. Der Schutz vor Ausfällen weist auf den überaus wichtigen und keineswegs trivialen Umstand hin, dass eine zunehmend vernetzte Produktion ein zuverlässig funktionierendes Netz voraussetzt. Mit der Security-Dimension ist die durch Vernetzung entstehende Form der Verletzlichkeit bezüglich Datensicherheit angesprochen, also nicht zuletzt auch Aspekte wie externe Spionage oder Sabotage. Diesen Zusammenhang illustriert die ursprünglich vom US-Amerikanischen President’s Information Technology Advisory Committee (PITAC) bekannt gemachte Gleichung: „*Ubiquitous Interconnectivity = Widespread Vulnerability*“ (PITAC 2005, S. 7).

Für die TAUCIS-Studie hängt die weitere Entwicklung von einer befriedigenden Lösung der Sicherheitsfragen im Design, der Implementierung und Verwendung vernetzter Systeme maßgeblich ab (ULD 2006, S. 72). Außerdem geben die Autoren zu bedenken, dass nur dann von einer Bereitschaft auszugehen ist, Ubiquitous Computing und verwandte Ansätze zu nutzen, wenn „allgegenwärtige Unverantwortlichkeit" ausgeschlossen werden kann (vgl. ebd.). Die damit hervorgehobene Bedeutung einer Zurechnung für technische Fehler und Missbrauch lässt Rechtssicherheit als eine weitere zu beachtende Facette der Dimensionen „Safety & Security" erkennbar werden.

- Ergeben sich im Zuge der technischen Neuerungen im Unternehmen auch Veränderungen in Hinblick auf den Schutz persönlicher Daten?
- Ist (ggf.) für die Bedienenden transparent, welche (personenbezogenen) Daten erfasst werden und was hiermit im weiteren Verlauf geschieht?
- Ist eine solche Transparenz angesichts der Komplexität der Vernetzung überhaupt möglich? Wie kann ggf. über Datenströme, deren Erfassung und Weiterverarbeitung informiert werden?
- Ist eine personenbezogene Leistungskontrolle vorgesehen? Wird ggf. hierüber vor der Umstellung informiert? Werden mögliche nachteilige Auswirkungen auf das Arbeitsklima erwogen?[7]
- Welche Maßnahmen zur Aufrechterhaltung der Netzsicherheit stehen zur Verfügung? Wie können Ausfälle kompensiert werden?
- Welche Schranken können errichtet werden, um negative externe Einflussnahmen auf die vernetzten Systeme zu verhindern? Ist dieser Zuständigkeitsbereich eindeutig geregelt?

[7] Siehe auch VDI (1989): Teil 3, Benutzerschutz.

Fazit und Ausblick

Nicht selten in ihrer Geschichte wurde die TA als „*technology arrestment*“, als „fortschrittsfeindliches Hemmnis“ kritisiert. Dem kann entgegengehalten werden, dass eine Dämpfung ursprünglicher Ambitionen dem *langfristigen* Erfolg einer Technologie insgesamt zu Gute kommen kann. Konflikte möglichst breit zu antizipieren, kann sich folglich sowohl in der Sozial- als auch in der Handelsbilanz von Unternehmen positiv auswirken.

Parasuraman et al. (2000) verweisen in ihrem grundlegenden Modell[8] darauf, dass Automatisierung in der Anwendung häufig nicht das bedeutet, was alltagsweltlich oder intuitiv vielleicht zu erwarten wäre, nämlich dass zuvor vom Menschen ausgeführte Tätigkeiten „1:1“ an das technische System „übergeben“ würden. Vielmehr hätten sich die Aufgaben selbst im Zuge der Automatisierung verändert (vgl. S. 287). Dies bedeutet hinsichtlich der Planbarkeit des Einsatzes intelligenter technischer Systeme, dass es nicht ausreicht, einen *status quo* zu betrachten, die gegenwärtig durchgeführten Arbeitsprozesse zu identifizieren und ein entsprechendes technisches System auf den Fall maßzuschneidern. Den Autoren zufolge hätte die Implementierung automatisierter Systeme den Operateuren häufig mehr Arbeit (und dem Unternehmen damit Kosten) verursacht, wohingegen ursprünglich erhofft wurde, fortan Einsparungen vornehmen zu können. Der Wirtschaftsinformatiker Arno Rolf (2008: 26) kam in ähnlichem Zusammenhang sogar zu dem Ergebnis, „dass die Kosten von Standardsoftware etwa ein Drittel ausmachen, Anpassungsnotwendigkeiten dagegen zwei Drittel.“ Zu den Kosten für das technische System, seine Installation und die Schulung der Mitarbeiter kommt also noch zu entlohnende Arbeitszeit hinzu. Ein solches Szenario ist sicherlich einem „*worst case*“ nahe. Dies unterstreicht noch einmal die Wichtigkeit, den konkreten Anwendungsfall (auch in Bezug auf die Einbettung anderer Arbeitsprozesse) möglichst erschöpfend zu antizipieren – und dies nicht zuletzt aus ökonomischen Gründen.

8 In diesem Modell finden sich auch die über die TA hinaus bekannt gewordenen „10 Levels of Automation of Decision and Action Selection“, von (1) The computer offers no assistance: human must take all decisions and actions über (5) executes that suggestion if the human approves bis (10) The computer decides everything, acts autonomously, ignoring the human (vgl. Parasuraman et al. 2000, S. 287). Ein in diesem Sinne ebenfalls anwendbares Modell ist das der „anticipatory technology ethics“ (ATE) von Philip Brey (2012).

„Intelligente technische Systeme“ ist ein Oberbegriff, der sehr viele voneinander grundverschiedene technologische Stränge und Entwicklungen in sich vereint. Zu Beginn dieser Handreichung hieß es, ihr Ziel sei die Ermöglichung einer „TA im Kleinen“. Ein konkreter Fall kann aufgrund des beschriebenen Dachcharakters intelligenter technischer Systeme höchst unterschiedliche Feinabstimmungen nach sich ziehen.

Die vorliegende Handreichung hat die wesentlichen in TA-Studien thematisierten Konfliktlinien zu intelligenter, autonomer Technik aus fast vier Jahrzehnten zusammenfassend aufbereitet. Wir hoffen gezeigt zu haben, dass die hier als zentral herauspräparierten Aspekte auch für die Clusterthematik von hoher Aktualität sind. Die die jeweiligen Abschnitte abschließenden Fragen verfolgen das Ziel, für alle im Kontext von it’s OWL entstehenden Systeme anwendbar zu sein. Mehrfach ist darauf hingewiesen worden, dass Fragen dieser Art im Einzelfall genauer zu justieren sein werden. Dass eine solche Spezialisierung gewährleistet ist, hat die Formulierung der Fragen orientiert. Ferner steht die Servicestelle TA für weitere Hilfe zur Verfügung.

Die Angemessenheit und praktische Anwendbarkeit der Frageblöcke lässt sich nur durch eine Erprobung beurteilen und sukzessive verbessern. Insofern laden wir die Partner im Spitzencluster dazu ein, sich diese TA-Fragen kritisch daraufhin anzusehen, ob sie für Prozesse in ihrem Unternehmen sinnvoll sein können. Von entsprechenden Rückmeldungen würde nicht nur unser Leitfaden für eine sozialverträgliche Technikgestaltung, sondern die gesamte TA profitieren. Hiermit verbunden ist unsere Überzeugung, dass diese Zusammenarbeit auch für die Unternehmen und ihre Mitarbeitenden ein Gewinn sein kann.

Allen vorangegangenen Abschnitten ist gemein, dass sie auf Konflikte aufmerksam machen, die entweder bei anderen, verwandten Technologien aufgetreten sind oder bereits im Gestaltungsprozess antizipiert wurden. Diese Konfliktsuche wäre missverständen, fasste man sie als Wecken schlafender Hunde auf. Vielmehr soll sie einen gangbaren Weg zur Bewältigung des sogenannten Collingridge-Dilemmas ebnen. Mit dieser von Beginn der TA an präsenten Figur ist der Umstand angespro-

chen, dass einerseits das Wissen um Folgen umso besser ist, je weiter eine technische Entwicklung vorangeschritten ist. Andererseits ist die Beeinflussung von Technik und ihren möglichen unerwünschten Folgen dann besonders aussichtsreich, wenn sie so früh wie möglich einsetzt, also bevor etwa die Marktreife so fortgeschritten ist, dass Eingriffe kaum noch oder nicht mehr möglich sind (Collingridge 1980).

Selbstverständlich sind nie alle Folgen einer technologischen Entwicklung antizipierbar, nichtsdestotrotz kann aus Erfahrungen gelernt werden. Die Anwendung von Schlüssen aus (teils) abgeschlossenen Entwicklungen auf das höchstaktuelle, im Entstehungsprozess befindliche Thema intelligenter technischer Systeme ist folglich für Theorie und Praxis eine vielversprechende Herausforderung. Die Nachhaltigkeitsmaßnahme „Technik sozialverträglich gestalten" möchte dazu beitragen, dass im Rahmen von it's OWL Widerstände und Konflikte frühestmöglich erkannt und bearbeitet werden können.

Gerade mit Blick auf das Schlagwort „Industrie 4.0" ist eine solche Frühzeitigkeit gegeben. Das ist auch daran erkennbar, dass der VDI in seinen neueren Publikationen darauf verweist, dass auf diesem Gebiet Standardisierungsaktivitäten zu intensivieren seien und auch die „Anwendung einer einheitlichen Begriffswelt" noch ausstehe (VDI 2013, S. 20). Neben diesen unbestreitbar bedeutsamen (technischen) Details legt der VDI in seinen Ausführungen zu Thesen und Handlungsfeldern der „Automation 2020" allergrößten Wert darauf, „Bedeutungen und Chancen der Automatisierungstechnik noch stärker in das Bewusstsein der Öffentlichkeit zu bringen" (ebd. S. 5). Auch gelte es zu verdeutlichen, dass Automation einen wesentlichen Beitrag zur Lösung gesellschaftlicher Herausforderungen leiste – vom Bevölkerungswachstum über Klimaschutz bis zur Verknappung natürlicher Ressourcen (vgl. ebd. S. 11).

Auch und gerade für die öffentliche Bedeutung intelligenter technischer Systeme kann der frühzeitige Einbezug nicht-technischer Aspekte bzw. sozialer Folgen technischer Entwicklungen ausgesprochen hilfreich sein.

Literatur

Brey, Philip (2005): Freedom and Privacy in Ambient Intelligence. In: *Ethics and Information Technology* 7 (3), S. 157–166.

Brey, Philip (2012): Anticipatory Ethics for Emerging Technologies. In: *Nanoethics* 6 (1), S. 1–13.

Campbell, Emily M. et al. (2007): Overdependence on Technology: An Unintended Adverse Consequence of Computerized Provider Order Entry (AMIA 2007 Symposium Proceedings), S. 94-98. http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2710605/pdf/amia-0100-s2007.pdf.

Cook, Diane J. et al. (2009): Ambient intelligence: Technologies, applications, and opportunities. In: *Pervasive and Mobile Computing* 5 (4), S. 277–298.

Collingridge, David (1980): The Social Control of Technology. London: Pinter.

Decker, Michael (2012): Service robots in the mirror of reflective research. In: *Poiesis & Praxis* 9 (3-4), S. 181–200.

Goddard, Kate et al. (2011): Automation bias: a systematic review of frequency, effect mediators, and mitigators. In: *Journal of the American Medical Informatics Association* 19 (1), S. 121–127.

Moniz, António B. (2008): Assessing Scenarios on the future of work. In: *Enterprise and Work Innovation Studies* 4 (4), S. 91–106. http://run.unl.pt/bitstream/10362/1887/1/AMoniz.pdf.

Moniz, António B. (2009): Synthesis about a collaborative project on "Technology Assessment of Autonomous Systems". In: *Enterprise and Work Innovation Studies* 5, S. 83–91. http://run.unl.pt/bitstream/10362/4435/1/Moniz_conf2_83-91.pdf.

Moniz, António B. (2010): Anthropocentric-based robotic and autonomous systems: assessment for new organisational options

Moniz, António B. (2010): Anthropocentric-based robotic and autonomous systems. Assessment for new organisational options. Research Centre on Enterprise and Work Innovation, Lissabon (IET Working Papers Series, No. WPS07/2010). http://run.unl.pt/bitstream/10362/5592/3/WPSeries_07_2010ABMoniz.pdf.

Mosier, Kathleen L. et al. (1998): Automation Bias: Decision Making and Performance in High Tech Cockpits. In: *The International Journal of Aviation Psychology* 8 (1), S. 47–63.

OTA - U.S. Congress Office of Technology Assessment (1982): Exploratory Workshop on the Social Impacts of Robotics: Summary and Issues. http://ota-cdn.fas.org/reports/8209.pdf.

OTA - U.S. Congress Office of Technology Assessment (1984): Computerized Manufacturing Automation: Employment, Education, and the Workplace. http://ota-cdn.fas.org/reports/8408.pdf.

Parasuraman, Raja et al. (1993): Performance Consequences of Automation-Induced 'Compla-

cency'. In: *The International Journal of Aviation Psychology* 3 (1), S. 1–23.

Parasuraman, Raja et al. (2000): A Model for Types and Levels of Human Interaction with Automation. In: *IEEE Transactions on Systems, Man and Cybernetics - Part A: Systems and Humans* 30 (3), S. 286–297.

Parasuraman, Raja/ Manzey, Dietrich H. (2010): Complacency and Bias in Human Use of Automation: An Attentional Integration. In: *Human Factors: The Journal of the Human Factors and Ergonomics Society* 52 (3), S. 381–410.

PITAC - President's Information Technology Advisory Committee: Cyber Security (2005): Cyber Security: A Crisis of Prioritization. Report to the President. http://www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf.

Ranganathan, Kumar (2004): Trustworthy Pervasive Computing: The Hard Security Problems. IEEE Computer Society (Second IEEE Annual Conference on Pervasive Computing and Communications Workshops). http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=01276916.

Rolf, Arno (2008): Mikropolis 2010. Menschen, Computer, Internet in der globalen Gesellschaft. Marburg: Metropolis. http://edoc.sub.uni-hamburg.de/informatik/volltexte/2013/182/pdf/rolf_mikropolis_2010.pdf.

Schubert, Cornelius (2006): Die Praxis der Apparatemedizin. Ärzte und Technik im Operationssaal. Frankfurt a. M., New York: Campus

RAE - The Royal Academy of Engineering (2009): Autonomous Systems: Social, Legal and Ethical Issues. http://www.raeng.org.uk/societygov/engineeringethics/pdf/Autonomous_Systems_Report_09.pdf.

ULD - Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (2006): TAUCIS - Technikfolgenabschätzung ubiquitäres Computing und informationelle Selbstbestimmung. Kiel, Berlin: BMBF. https://www.datenschutzzentrum.de/taucis/ita_taucis.pdf.

VDI - Verein Deutscher Ingenieure (1989): Handlungsempfehlung: Sozialverträgliche Gestaltung von Automatisierungsvorhaben. Düsseldorf.

VDI - Verein Deutscher Ingenieure (2009): Automation 2020. Bedeutung und Entwicklung der Automation bis zum Jahr 2020. Thesen und Handlungsfelder. http://www.vdi.de/fileadmin/vdi_de/redakteur_dateien/gma_dateien/AT_2020_INTERNET.pdf.

VDI - Verein Deutscher Ingenieure (2013): Automation 2020. Bedeutung und Entwicklung der Automation bis zum Jahr 2020. Thesen und Handlungsfelder. http://www.vdi.de/fileadmin/vdi_de/redakteur_dateien/gma_dateien/GMA_Automation_2020_Internet_2Auflage.pdf.

Verbeek, Peter-Paul (2009): Ambient Intelligence and Persuasive Technology: The Blurring Boundaries Between Human and Technology. In: *Nanoethics* 3 (3), S. 231–242.

Kontakt

Servicestelle TA in der Clusternachhaltigkeitsmaßnahme [itsowl-TA]
„Akzeptanz gewährleisten - Technik sozial- und humanverträglich gestalten“

Dr. Marc Mölders
Universität Bielefeld
Fakultät für Soziologie
Postfach 100 131

D-33501 Bielefeld

Tel.: +49-521-106-4674
Fax: +49-521-106-6418
http://www.uni-bielefeld.de/soz/las/TA/itsowl/

BMBF-Spitzencluster Intelligente Technische Systeme (it’s OWL)
http://www.its-owl.de/

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

INVENTED IN GERMANY

BETREUT VOM
PTKA Projektträger Karlsruhe
Karlsruher Institut für Technologie