Marit Hansen, Christian Thiel

Cyber-Physical Systems und Privatsphärenschutz

In vielen Produktionsanlagen ist der Einsatz von Sensoren und Aktuatoren selbstverständlich, um ein reibungsloses Zusammenspiel bei der Produktfertigung und beim Anlagenbetrieb zu gewährleisten. Ähnliche Komponenten solcher „Cyber-Physical Systems" werden in jedem neuen Auto verbaut. Eine Forschungsagenda für Deutschland beschreibt die Potenziale und Herausforderungen für diese Systeme, die künftig in vielen Lebensbereichen Einzug halten könnten und aus denen sich bedeutende Datenschutzfragen ergeben.

1 Einleitung

Das ubiquitäre Computing mit allgegenwärtiger Datensammlung und -analyse in beinahe allen Lebensbereichen ist noch nicht Realität, doch die Forschung an derartigen Technologien schreitet voran. In den letzten Jahren haben sich mehrere Studien[1] mit juristischen und gesellschaftlichen Fragen zum Bereich „Ubiquitous Computing" beschäftigt; auch zu einzelnen Anwendungskontexten liegen Ausarbeitungen vor, beispielsweise für die Unterstützung und Versorgung von älteren oder kranken Menschen im sog. „Ambient Assisted Living"[2].

Die Entwicklungen können unter dem Begriff der Cyber-Physical Systems zusammengefasst werden (Abschnitt 2). Entstanden im Rahmen der „Integrierten Forschungsagenda Cyber-Physical Systems" benennt dieser Text mögliche gesellschaftliche Auswirkungen (Abschnitt 3) und wesentliche Akzeptanzfaktoren (Abschnitt 4). Mit dem Fokus auf den Schutz der Privatsphäre werden anschließend Möglichkeiten für „Privacy by Design" erläutert (Abschnitt 5).

2 Cyber-Physical Systems

Cyber-Physical Systems (CPS) sind hoch vernetzte eingebettete Systeme (Embedded Systems), die über Sensoren die Umwelt erfassen und Aktionen auslösen können. Sie fahren beispielsweise bei Sturmwarnung die Rollläden herunter oder übertragen permanent Vitaldaten an einen Arzt, der bei Abweichungen sofort im Patienten implantierte Wirkstoffspritzen aktivieren kann.

Der zentrale Bestandteil von Cyber-Physical Systems sind eingebettete Systeme, also in die Produkte eingebaute, hoch integrierte Rechenkomponenten, wie sie heutzutage in Produktionsanlagen, Autos, Unterhaltungselektronik oder medizinischen Geräten eingesetzt werden. Verbunden mit Sensoren und Aktuatoren können sie unmittelbar physikalische Daten erfassen und auf physikalische Vorgänge einwirken. Sie sind mittels digitaler Netze verbunden, und können weltweit verfügbare Daten und Dienste nutzen. Für den Zugriff der Nutzer auf Cyber-Physical Systems sind verschiedene multi-modale Schnittstellen denkbar, um beispielsweise persönliche Präferenzen zu konfigurieren und zu erreichende Ziele vorzugeben. Aufgrund der möglichen umfassenden Unterstützung der Menschen durch Cyber-Physical Systems in immer mehr Arbeits- und Lebensprozessen ist davon auszugehen, dass der Alltag zunehmend von einer Mensch-Maschine-Kooperation durchdrungen wird.

Die wirtschaftliche Bedeutung von eingebetteten Systemen für Deutschland ist hoch; der Markt wurde für 2007 auf über 18,7

1 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD) / Humboldt-Universität Berlin: Technikfolgen-Abschätzung Ubiquitäres Computing und Informationelle Selbstbestimmung (TAUCIS), 2006, https://www.datenschutzzentrum.de/taucis/; Alexander Roßnagel: Datenschutz in einem informatisierten Alltag, herausgegeben von der Friedrich-Ebert-Stiftung Berlin 2007, http://library.fes.de/pdf-files/stabsabteilung/04548.pdf; Michael Friedewald et al.: Ubiquitäres Computing – Das „Internet der Dinge" – Grundlagen, Anwendungen, Folgen, Studien des Büros für Technikfolgen-Abschätzung beim Deutschen Bundestag – 31, edition sigma, Berlin 2010.

2 ULD: Juristische Fragen im Bereich Altersgerechter Assistenzsysteme, Vorstudie im Auftrag von VDI/VDE-IT im Rahmen des BMBF-Förderschwerpunktes „Altersgerechte Assistenzsysteme für ein gesundes und unabhängiges Leben – AAL", 2011, https://www.datenschutzzentrum.de/aal/2011-ULD-JuristischeFragenAltersgerechteAssistenzsysteme.pdf.

Marit Hansen

Stellvertretende Landesbeauftragte für Datenschutz Schleswig-Holstein, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Kiel

E-Mail: marit.hansen@datenschutzzentrum.de

Dr. Christian Thiel

Bavarian Information and Communication Technology Cluster BICCnet, München; Projektkoordinator und Co-Autor der Forschungsagenda Cyber Physical Systems. Promovierte in Ulm im Bereich Maschinelles Lernen.
E-Mail: christian.thiel@bicc.net.de

Mrd. Euro geschätzt, mit Wachstumsraten von 9-10% pro Jahr.[3] Zudem spielen eingebettete Systeme für wichtige Branchen eine zentrale Rolle: Im Jahr 2005 betrug ihr Wertanteil in Personenfahrzeugen schon 25%,[4] im Maschinen- und Anlagenbau lag der Anteil von Informations- und Automatisierungstechnik (und damit der Embedded Systems) 2007 ebenfalls bei 25%.[5] Mit dem Aufkommen von detaillierter Energieverbrauchsmessung und intelligenten, dezentralen Stromnetzen werden eingebettete Systeme auch im Bereich der Energietechnik verstärkt eingesetzt.

Um die Chancen und Potenziale zu nutzen, die sich mit dem Anwendungsbereiche übergreifenden Einsatz und der globalen Vernetzung von eingebetteten Systemen ergeben, hat das Bundesministerium für Bildung und Forschung die „Integrierte Forschungsagenda Cyber-Physical Systems", kurz AgendaCPS[6], gefördert. Die Agenda spannt anhand von Anwendungsszenarien das Gebiet der Cyber-Physical Systems auf und bestimmt deren technische Merkmale und Fähigkeiten. Nach einer Bestandsaufnahme zum Stand der Technik werden umfassende Maßnahmen und Handlungsempfehlungen für Forschung, Wirtschaft und Politik formuliert.

Für Cyber-Physical Systems identifiziert die AgendaCPS fünf Charakteristika, die mit jeder Stufe eine zunehmende Öffnung, Komplexität, (autonome) „Intelligenz" und Vernetzung aufweisen:

1. Verschmelzung von physikalischer und virtueller Welt
2. System of Systems mit offenen, dynamisch wechselnden Systemgrenzen
3. Kontext-adaptive und (teil-)autonom handelnde Systeme, proaktive Echtzeitsteuerung
4. Kooperative Systeme mit verteilter, wechselnder Kontrolle
5. Umfassende Mensch-System-Kooperation

Die in den Punkten 3 bis 5 genannten Charakteristika beziehen sich darauf, dass die Cyber-Physical Systems die aktuelle Situation und Umgebung inklusive aller Akteure automatisch erfassen. Sofern natürliche Personen unter den Akteuren sind, ist üblicherweise ein unmittelbarer Personenbezug gegeben, und es stellen sich Datenschutzfragen. Betroffene können nicht nur diejenigen sein, die die Cyber-Physical Systems bewusst nutzen, sondern auch andere Personen, deren Daten dadurch erfasst und verarbeitet werden.

3 Gesellschaftliche Auswirkungen

Zum heutigen Zeitpunkt kann weder das volle Potenzial der Cyber-Physical Systems abgeschätzt werden noch lassen sich die damit im Zusammenhang stehenden gesellschaftlichen Entwicklungen genau vorhersagen. Hier wird es stark auf die konkrete Ausgestaltung der Systeme und der Anwendungen sowohl im nationalen als auch im internationalen Kontext ankommen. Jedoch lassen sich bereits jetzt gesellschaftliche Tendenzen identifizieren, die sich aus ähnlichen Diskussionen, beispielsweise in Bezug auf digitale Netze, übertragen lassen und zu einer Spaltung der Gesellschaft führen können. So beispielsweise zwischen den „*Literates*", also denjenigen, die Cyber-Physical Systems und ihre Auswirkungen ausreichend gut kennen, verstehen und für sich selbst wissen, wie sie mit den Systemen umgehen können, und den „*Illiterates*", die nicht im selben Maße ein Bewusstsein für die Funktions- und Konfigurationsmöglichkeiten haben; hier spielen Aspekte der Usability, der Transparenz und der Schulung eine wesentliche Rolle.

Außerdem wird es Gruppen von Menschen geben, die sich dafür entscheiden, Cyber-Physical Systems nicht zu nutzen (auch als „*Drop-outs*", d. h. Aussteiger oder Verweigerer der Technik, bezeichnet). Die Motivation für ein Verweigern kann beispielsweise daher rühren, dass die Menschen bei der Nutzung der Systeme unter Stress leiden (beispielsweise durch Überforderung), oder sich ihnen ausgeliefert fühlen und einen Kontrollverlust wahrnehmen. Je mehr die Cyber-Physical Systems mit allen Bereichen des gesellschaftlichen oder individuellen Lebens verwoben werden, desto größer sind die persönlichen Folgen für etwaige „Drop-outs".

Neben diesen generell für neue Technologien zu untersuchenden Auswirkungen lassen sich Risiken identifizieren, die sich aus etwaigen Missbrauchsmöglichkeiten oder unbeabsichtigten „Nebenwirkungen" ergeben:

- Gerade weil Cyber-Physical Systems darauf basieren, eine Vielzahl von Daten auszuwerten, daraus Entscheidungen abzuleiten und ggf. sogar unmittelbar diese Entscheidungen umzusetzen, können eine Fehlfunktion oder ein Missbrauch wesentliche Folgen nach sich ziehen. Ein offensichtliches Beispiel besteht in der Möglichkeit, dass Entscheidungen manipuliert werden, so dass Personen oder Organisationen wirtschaftliche Schäden erleiden oder dass gar Menschen einer Gefahr für Leib und Leben ausgesetzt sind.
- Die weit reichende Datenverarbeitung durch Cyber-Physical Systems kann außerdem Wirkungen auf die Privatsphäre der Betroffenen haben. Wegen der großen Komplexität dieser Systeme und der Einbindung einer Vielzahl von Akteuren ist es schwierig für Menschen, zu verstehen und nachzuvollziehen, wer wann welche Daten zu welchem Zweck über sie verarbeitet, so wie es das Recht auf informationelle Selbstbestimmung vorsieht. Hinzu kommt, dass allein die Masse an Daten und ihre vielfältigen Auswertungsmöglichkeiten Begehrlichkeiten hervorrufen, die Informationen zu vielfältigen Zwecken zu verwenden. Selbst für den Fall, dass es sich um (zunächst) nicht personenbezogene Daten handelt, können unerwünschte Effekte auf die Privatsphäre von einzelnen Betroffenen oder von Gruppen entstehen – schon durch exakte orts- und zeitbezogene Informationen wird eine recht genau auf eine oder wenige Personen zugeschnittene Interpretation der Daten möglich.
- Ein anderer Effekt ergibt sich daraus, dass die Entscheidungen der Cyber-Physical Systems zu einem normierten Verhalten der Nutzer führen können, wodurch eine freie Fortentwicklung der Gesellschaft gehemmt würde. Das normierte Verhalten entstünde beispielsweise dann, wenn die Cyber-Physical Systems die gleichartigen Entscheidungen direkt umsetzen oder wenn es für die Nutzer zu aufwendig oder (haftungs-)rechtlich ungünstig erschiene, entgegen dem Entscheidungsvorschlag der Systeme zu handeln.
- Hinzu kommt das Risiko einer steigenden Abhängigkeit von den Cyber-Physical Systems, in die sich Einzelne oder die Gesellschaft begibt, wenn diese Systeme in immer mehr Lebens-

3 Studie zur Bedeutung des Sektors Embedded Systems für Deutschland, BITKOM, 2008, http://www.bitkom.org/60376.aspx?url=embedded_systeme_mit_grusswort_kleiner.pdf.

4 Study of Worldwide Trends and R&D Programmes in Embedded Systems in View of Maximising the Impact of a Technology Platform in the Area, FAST GmbH, TU München, 2005, S. 32.

5 VDMA Tendenzbefragung. Bedeutung der IT und Automatisierungstechnik im Maschinenbau, VDMA, 2008.

6 Das Projekt unter der Schirmherrschaft der Deutschen Akademie der Technik-Wissenschaften acatech (in Person von Prof. Dr. Manfred Broy) wird am fortiss-Institut durchgeführt (fachliche Leitung: Dr. Eva Geisberger).

bereichen zum Einsatz kommen. Werden Cyber-Physical Systems in alltäglichen Situationen wie beispielsweise beim Autofahren oder beim Einnehmen von Medikamenten standardmäßig verwendet, kann es sein, dass ihre Nutzer sich ein Leben ohne diese Systeme gar nicht mehr vorstellen können und möglicherweise sogar die Grundfertigkeiten, die sie ohne Cyber-Physical Systems bräuchten, mangels Übung abbauen oder gar einbüßen. Möglicherweise wird künftig der Einsatz von Cyber-Physical Systems in einigen Fällen sogar verpflichtend sein – vergleichbar der Nutzung von Autopiloten in bestimmten Situationen. Die Abhängigkeit bestünde nicht nur in Bezug auf die technische Verfügbarkeit der Cyber-Physical Systems und deren korrektes Funktionieren, sondern auch in der Beziehung zu den Betreibern und Entwicklern der jeweils wesentlichen CPS-Komponenten.

Sofern sich Staat und Gesellschaft immer mehr auf Cyber-Physical Systems verlassen, werden Teile dieser Systeme, beispielsweise im Energie- oder Gesundheitssektor, als kritische Infrastrukturen einzustufen sein, deren korrektes Funktionieren staatlich garantiert werden sollte.

4 Wesentliche Akzeptanzfaktoren

Für eine Akzeptanz neuer Technologien bei denjenigen, die sie einsetzen wollen, ist generell ein ausreichender (hoher) Grad an Beherrschbarkeit wesentlich: Etwaige Risiken und Nebenwirkungen, wie die im vorigen Abschnitt skizzierten, sollten vor einer Einführung in breitem Stil den Akteuren bekannt und bewusst sein, und der geeignete Umgang mit Risiken und Nebenwirkungen sollte im Vorfeld festgelegt sein. Dies folgt nicht nur aus der rechtlichen Verantwortung, beispielsweise aus dem Haftungs- oder Datenschutzrecht, sondern ergibt sich auch aus einem psychologischen Bedürfnis von Menschen. Zu Beherrschbarkeit gehört bei Cyber-Physical Systems auch, dass den Nutzern Informationen und Entscheidungsmöglichkeiten in einer Weise präsentiert werden, die der Situation und ihrem (technischen) Verständnis angepasst ist.

Ein weiteres Bedürfnis besteht nach einer fairen Ausgestaltung der neuen Technologie. Im Sinne der „mehrseitigen Sicherheit“[7] ist es erforderlich, die Interessen aller Beteiligten zu berücksichtigen und in eine faire Balance zu bringen. Bestimmte Regeln für die Ausgestaltung von Marktplätzen, das automatische Verhandeln von Software-Agenten oder den Zugang zu begrenzten Ressourcen müssen mit gesellschaftlichem Konsens festgelegt werden. Auch sollte sich die Gestaltung der Systeme darauf ausrichten, dass, wo immer dies möglich ist, konkrete und nachvollziehbare Zusicherungen gegeben werden, statt Beteiligten blindes Vertrauen abzuverlangen und ihnen das Gefühl des Ausgeliefert-Seins zu vermitteln.

Diese Zusicherungen umfassen den Schutz der Privatsphäre der Betroffenen, gerade weil Cyber-Physical Systems das Potenzial für eine umfangreiche Überwachung bergen: Es wäre gesellschaftlich inakzeptabel und würde zudem das Recht auf informationelle Selbstbestimmung verletzen, wenn ständiges Beobachten, Überwachen und Tracken aller Aktionen einer Person zum Normalfall würden. Stattdessen ist es notwendig, dass alle Beteiligten – also sowohl diejenigen, welche die Systeme betreiben, als auch diejenigen, deren Daten damit verarbeitet werden oder die auf andere Art von durch Cyber-Physical Systems vorbereitete Entscheidungen betroffen sind – in ausreichendem Maße Klarheit und Verständnis über die Datenverarbeitungsprozesse und ihre Auswirkungen haben. Schon ein latent ungutes Gefühl der Betroffenen könnte sich zu einem massiven Akzeptanzproblem entwickeln.

Was für die Privatsphäre der Einzelnen gilt, lässt sich auf den Schutz von Unternehmensinformationen ausdehnen: Werden Mitarbeiter oder Anlagen eines Unternehmens durch Systeme Dritter in ihrem Tun beobachtet, überwacht oder getrackt oder sind anderweitig unberechtigte Zugriffe auf die erfassten und verarbeiteten Daten möglich, kann dies den Schutz von Geschäftsgeheimnissen beeinträchtigen. Hier bedarf es einer differenzierten Lösung, da die Wertschöpfung in CPS-Ökosystemen durch lose Verbünde von Unternehmen erfolgt, die ihre Infrastruktur dazu teilweise öffnen müssen.

5 Privacy by Design

Das einfachste Implementierungskonzept für ein Cyber-Physical System würde darin bestehen, alle anfallenden Daten, die wesentlich sein könnten, an für die Anwendung zentralen Speicherorten für eine gewisse Zeit zu sammeln und gemäß den jeweiligen Vorgaben zu analysieren.[8] Bei einem solchen Konzept handelt es sich in der Regel aber nicht um eine möglichst datensparsame Implementierung, und auch die vom Datenschutzrecht geforderte Zweckbindung wird dadurch technisch nicht unterstützt.

Die Gestaltung der Cyber-Physical Systems sollte daher von Anfang an nicht nur Erfordernisse der Datensicherheit, sondern auch Privacy[9]-Kriterien einbeziehen, um damit den Grundsatz von „Privacy by Design“ umsetzen: Berücksichtigung von Privacy-Anforderungen in allen Phasen des Lebenszyklus der Systeme wie bei der Konzeption, beim Entwurf, bei der Implementierung, bei der Konfiguration und bei der Weiterentwicklung der Systeme. Damit sollen Risiken für die Privatsphäre möglichst vermieden oder zumindest ausreichend minimiert werden; gleichzeitig ist ein Bewusstsein über die verbliebenen Risiken herzustellen.

In jedem konkreten Einsatzbereich müssen bei der Gestaltung von Systemen die Anforderungen aus den jeweils geltenden rechtlichen Normen berücksichtigt werden. Allerdings ist der genaue Einsatzbereich bei Cyber-Physical Systems häufig nicht mehr eingrenzbar, denn die Systeme können sich an neue Anforderungen anpassen und mit anderen Systemen kooperieren. Aus diesem Grund kann für eine erste Annäherung der Gestaltungsanforde-

7 Kai Rannenberg, Andreas Pfitzmann und Günter Müller: Sicherheit, insbesondere mehrseitige IT-Sicherheit, in: Mehrseitige Sicherheit in der Kommunikationstechnik, Addison-Wesley Verlag, 1997.

8 Diese Vorgehensweise ähnelt einem „Data Warehouse“, in dem zunächst alle möglichen Daten gesammelt und anschließend zu vielfältigen Zwecken ausgewertet werden. Dass dadurch u.a. gegen das Erforderlichkeits- und das Zweckbindungsprinzip verstoßen wird, kritisierte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder im Jahr 2000 in einer Entschließung zu „Data Warehouse, Data Mining und Datenschutz“, siehe http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/59DSK-DataWarehouse_DataMiningUndDatenschutz.html.

9 In diesem Text wird unter dem Begriff „Privacy“ ein „Privatsphärenschutz“ für einzelne Individuen oder für Gruppen von Personen verstanden. Damit wird bewusst eine erweiterte Sicht auf den Datenschutz wie er zurzeit gesetzlich in Deutschland normiert ist, gewählt.

rungen auf das bewährte Verfahren aus der Informationssicherheit und dem IT-Grundschutz zurückgegriffen werden, bei dem definierte Schutzziele zur Anwendung kommen: Zunächst wird der Schutzbedarf für die verarbeiteten Informationen und technischen Systeme ermittelt, anschließend werden in Bezug auf die vorgegebenen Schutzziele die geeigneten Maßnahmen zur Umsetzung der Anforderungen ausgewählt. Um neben den drei klassischen Schutzzielen Vertraulichkeit, Integrität und Verfügbarkeit ähnlich prägnant Privacy-Kriterien zu formulieren, wurden spezielle „Privacy-Schutzziele" vorgeschlagen:[10] Transparenz, Intervenierbarkeit und Nichtverkettbarkeit. Diese insgesamt sechs Schutzziele stehen in einem Spannungsverhältnis, das je nach Art der Daten, Zweck der Verarbeitung und Risikoabschätzung auszubalancieren ist.[11]

Im Folgenden werden Beispiele gegeben, wie die drei Privacy-Schutzziele in Cyber-Physical Systems unterstützt werden können.[12]

5.1 Transparenz

Unter dem Schutzziel Transparenz versteht man, dass die Funktionsweise und Wirkung des Systems für Betroffene und Betreiber jederzeit verständlich sein muss. Bei Cyber-Physical Systems läuft ein Großteil der Datenverarbeitung ohne unmittelbare Interaktionen mit Nutzern ab. Damit die Beteiligten die Funktionsweise und tatsächliche Datenverarbeitung (Datenflüsse, Entscheidungen) nachvollziehen können, müssen diese verständlich wahrnehmbar gemacht werden.

Zu den wesentlichen darzustellenden Informationen gehört, welche Teile der Cyber-Physical Systems in wessen Verantwortlichkeit liegen, wie diese Verantwortlichen zu erreichen sind und welches Rechtssystem der Verarbeitung zugrunde liegt. Es ist zu überlegen, inwieweit jeder einzelne der eingesetzten Sensoren und Aktuatoren mit den entsprechenden Informationen ausgestattet werden sollte, das heißt ein Wissen über die für ihn verantwortliche Stelle und die Jurisdiktion hat, das er auch bei Anfragen mitteilt.

Um die Aktionen und Entscheidungen nachvollziehen und zurechnen zu können, ist für jeden Einsatzkontext festzulegen, welche Daten auf welche Weise mitprotokolliert werden sollen und wie der Umgang mit den Protokollierungsdaten gestaltet wird, zum Beispiel durch Definition der Zugriffsrechte für einzelne Personen oder Rollen, durch Implementieren von automatischen Löschroutinen nach spezifizierten Zeiten oder Anlässen und durch ein Absichern der Protokollierungsdaten gegen unberechtigte Zugriffe.

Ein Ansatz zur Wahrnehmbar-Machung wäre das Mitführen eines gesonderten Gerätes, der wahrscheinlichere Weg jedoch die Integration der Privacy-Management-Funktionen in bestehende Smart Devices. Diese Geräte werden unter dem Begriff „nutzergesteuertes Identitätenmanagement" für einige Kontexte diskutiert und prototypisch realisiert.[13] Für Cyber-Physical Systems ist wesentlich, dass Abstufungen im Detaillierungsgrad der Information wählbar sind, damit die Beteiligten den gewünschten Grad und Umfang an Informationen, ggf. mit zusätzlichen Erklärungen, erhalten können.

Aufgrund der komplexen Wechselwirkungen und Datenflüsse wird sich ein Großteil der Nutzer nicht mit den Privacy-Aspekten auseinandersetzen wollen. Eine mögliche Lösung besteht darin, dass Nutzer selbstbestimmt Personen, Organisationen oder Einrichtungen einbeziehen, die Unterstützungsleistungen bieten: Diese können Datenschutz-Interessen im Auftrag der Nutzer wahrnehmen, für sie anschauliche Transparenz herstellen und beispielsweise abgestufte Standard-Datenschutzkonfigurationen entwickeln und pflegen.

Damit Privacy-bezogene Wünsche und Vorgaben automatisch verarbeitet werden können, müssen sie in einer maschinenlesbaren Form vorliegen. Zu diesem Zweck kann auf Policy-Sprachen[14] zurückgegriffen werden, die für den CPS-Kontext angepasst oder erweitert werden sollten. Hier besteht Forschungsbedarf, um Nutzern auf der Basis von Policies einzelner CPS-Komponenten jederzeit ein konsistentes und korrektes Gesamtbild über die Datenverarbeitung vermitteln zu können. Privacy-Policies könnten sowohl für CPS-Komponenten als auch für übertragene Daten definiert werden. Hier ist zu prüfen, wo es sinnvoll ist, „Sticky Policies"[15] einzusetzen, bei denen die Policies mit den Daten untrennbar verbunden werden und auch bei einer Übertragung an den Daten „kleben bleiben".

5.2 Intervenierbarkeit

Das Schutzziel der Intervenierbarkeit fordert, dass die Beteiligten den Cyber-Physical Systems nicht hilflos ausgeliefert sind, sondern aus eigener Souveränität die Möglichkeit des Eingreifens haben, wenn ihnen dies erforderlich scheint.

Für alle Beteiligten und alle Komponenten der Cyber-Physical Systems ist Klarheit über die Eingriffsmöglichkeiten notwendig. Insbesondere muss deutlich werden, wo die jeweiligen Beteiligten Parameter verändern, die Cyber-Physical Systems als Ganzes oder teilweise abschalten oder auch die manuelle Steuerung übernehmen können. Dies hat wiederum Auswirkungen auf die Transparenzanforderungen: Beispielsweise kann ein Intervenieren eine veränderte Haftungssituation nach sich ziehen, dann ist es nötig, dass Eingriffe (ggf. sogar gerichtsfest) mitprotokolliert werden.

Die Datenverarbeitung und Speicherung erfolgt bei Cyber-Physical Systems dezentral. Damit Betroffene das Recht auf Korrektur und Löschung (Sperrung) ihrer personenbezogenen Daten ausüben können, ist hierfür ein „Single Point of Contact" vorzu-

10 Martin Rost, Andreas Pfitzmann: Datenschutz-Schutzziele – revisited, DuD 33(12):353-358, 2009; Martin Rost, Kirsten Bock: Privacy By Design und die Neuen Schutzziele – Grundsätze, Ziele und Anforderungen, DuD 35(1):30-35, 2011.

11 Dieser Ansatz hat sich u.a. in den Bereichen Ambient Assisted Living (Martin Rost: Datenschutz in 3D – Daten, Prozesse und Schutzziele in einem Modell, DuD 35(5):351-355, 2011) und Smart Meter/Smart Grid bewährt.

12 Diese Beispiele sind auch in das Technologie-Kapitel der AgendaCPS aufgenommen worden.

13 Beispielsweise in den EU-Projekten PRIME – Privacy and Identity Management for Europe (http://www.prime-project.eu/) und PrimeLife (http://www.primelife.eu/).

14 Die erste bekanntere Policy-Sprache in Privacy-Bereich war P3P – Platform for Privacy Preferences. Sie dient dazu, die Aussagen von Webseitenanbietern und die Wünsche der Nutzenden maschinell interpretierbar zu machen, hat jedoch keine weite Verbreitung erlangt. Eine Übersicht über Policy-Sprachen, die für Aussagen über Privacy vorgeschlagen wurden, findet sich in: Marit Hansen, Ammar Alkassar (Hrsg.): Study on protocols with respect to identity and identification – an insight on network protocols and privacy-aware communication, Deliverable D3.8, FIDIS – Future of Identity in the Information Society, Frankfurt 2008, http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.8_Study_on_protocols_with_respect_to_identity_and_identification.pdf. In den Jahren 2007 bis 2011 waren solche Sprachen Schwerpunkt der W3C-Arbeitsgruppe „Policy Languages Interest Group – PLING", deren Arbeit in die weiteren Aktivitäten des W3C zu Privacy aufgegangen ist (http://www.w3.org/Privacy/).

15 Marco Casassa Mont, Siani Pearson, Pete Bramhall: Towards Accountable Management of Identity and Privacy: Sticky Policies and Enforceable Tracing Services, Trusted Systems Laboratory, HP Laboratories, Bristol, HPL-2003-49, 2003, http://www.hpl.hp.com/techreports/2003/HPL-2003-49.pdf.

sehen, der die Korrekturen in alle damit zusammenhängenden Cyber-Physical Systems-Teile durchpropagieren kann.

Dieselben Geräte, die zur Herstellung von Transparenz in Cyber-Physical Systems dienen, können auch für Eingriffs- und Konfigurationsmöglichkeiten nutzbar sein. Wünsche oder Vorgaben des Nutzers sollen in standardisierten, maschinenlesbaren Sprachen hinterlegbar sein, so dass nicht in jedem Einzelfall eine Aktion durch den Nutzer nötig ist. Auch hier können Personen, Organisationen oder Einrichtungen eingebunden werden, die den Nutzer unterstützen.

5.3 Nichtverkettbarkeit

Das Schutzziel der Nichtverkettbarkeit umfasst die Anforderungen der größtmöglichen Datensparsamkeit[16] und Trennung von Daten und Prozessen aus unterschiedlichen Kontexten mit dem Ziel, Risiken durch Ansammlungen von umfassend auswertbaren Daten und Auswertungen zu beliebigen Zwecken zu verhindern.

Schon beim Entwurf der Systeme und Dienste muss darauf geachtet werden, nur Daten zu erheben und zu nutzen, die für den beabsichtigten Zweck erforderlich sind. Die Zweckbindung lässt sich technisch durch geeignete Verschlüsselung und Zugriffsbeschränkungen unterstützen.

Die Nichtverkettbarkeit kann realisiert werden durch eine physikalische und logische Trennung der Daten, die zu verschiedenen Zwecken verarbeitet werden, durch ein Verteilen der Daten auf verschiedene, voneinander unabhängigen Instanzen, durch Verfahren der Anonymisierung und Pseudonymisierung oder durch wirkliches Löschen.

Zum Löschen nicht mehr erforderlicher Daten müssen Methoden entwickelt werden, die auch die Protokollierungsdaten (beispielsweise über die Aktivität und Messungen von Sensoren) mit berücksichtigen, da diese häufig Rückschlüsse auf Personen ermöglichen.

Für die Datenminimierung von besonderer Bedeutung sind die kryptografischen Verfahren der attributbasierten Berechtigungsnachweise, auch unter Bezeichnungen wie „private Credentials" oder „Minimal Disclosure Tokens" bekannt:[17] Dabei handelt es sich um gegenüber der prüfenden Stelle anonyme Berechtigungsnachweise, deren Authentizität und berechtigte Verwendung durch einen Nutzer gewährleistet wird und für andere Parteien nachprüfbar ist, ohne dass dessen die Identität offengelegt werden muss. Lediglich die für den jeweiligen Anwendungskontext erforderlichen Attribute werden dabei verwendet. Da die Berechtigungsnachweise bei verschiedenen Verwendungen unterschiedlich aussehen, wird hiermit einer möglichen Verkettung durch andere entgegengewirkt. Beispielsweise könnte ein Nutzer einen digitalen Berechtigungsnachweis zum Führen eines Autos erhalten, der bei jedem Vorzeigen gegenüber anderen Parteien (etwa bei Autovermietungen oder Führerscheinkontrollen) sein Aussehen ändert.

Aufgrund der Massen von bei Cyber-Physical Systems anfallenden Daten – selbst wenn diese zunächst nicht personenbezogen sind, sind statistische Rückschlüsse möglich – und der (oft auch aufgrund der angebotenen Funktionalität so gewollten) Eingriffsmöglichkeiten in das Leben von Menschen bergen Cyber-Physical Systems, die nicht nach datenminimierenden Gesichtspunkten gestaltet sind, ein erhebliches Risiko für die Privatsphäre. Es ist fraglich, ob bei einer derartigen unkontrollierten Konzentration von Daten ein missbräuchliches Nutzen verhindert und Begehrlichkeiten zur weitergehenden Verwendung effektiv zurückgewiesen werden könnten.

5.4 Mehr als Datenschutz

Werden die Privacy-Schutzziele verletzt oder nur unzureichend umgesetzt, entstehen gesellschaftliche Spannungsfelder, die weit über den herkömmlichen Bereich des Datenschutzes hinausreichen. Beispielsweise ist mangelnde Transparenz über die Verantwortung für die einzelnen CPS-Komponenten und ihre Interaktion nicht nur zur Wahrnehmung der Datenschutzrechte relevant, sondern würde bei allen strittigen oder fehlerhaften Funktionsweisen Haftungsfragen aufwerfen.

Bei einem unzureichenden Grad an Intervenierbarkeit könnten die Folgen von automatischen Aktionen oder Entscheidungen der Cyber-Physical Systems nicht oder nur schwer rückgängig gemacht werden. Dies könnten unmittelbare physische Auswirkungen sein oder auch unfaire Diskriminierungen, gegen die sich die Betroffenen kaum effektiv zur Wehr setzen könnten.

Wird das Schutzziel der Unverkettbarkeit nicht ernsthaft verfolgt, bilden sich Machtkonzentrationen bei denjenigen, die Zugriffsmöglichkeiten auf die entstehenden umfassenden Datensammlungen und auf die Funktionsweise der Cyber-Physical Systems haben.

Diese Beispiele für mögliche Technikfolgen zeigen, dass ohne ein ausreichendes Maß an Beherrschbarkeit damit auch die Verfassungskonformität eines solchen Technikeinsatzes in Frage zu stellen wäre.

6 Fazit

Cyber-Physical Systems werden eine zunehmende Rolle in der Entwicklung künftiger Anwendungen und Dienste spielen. Hier ist es notwendig, Einfluss auf die Gestaltung dieser Technologie und der darauf basierenden Anwendungen und Dienste zu nehmen, um zu gesellschaftsverträglichen und von den Nutzern und Betroffenen akzeptierbaren Lösungen zu kommen. Einen Ansatz hierfür bieten die drei Privacy-Schutzziele Transparenz, Intervenierbarkeit und Nichtverkettbarkeit, die es erlauben, weit über den Begriff des Datenschutzes hinaus gehende gesellschaftliche Ziele gegeneinander abzuwägen und im gewünschten Maße umzusetzen.

Neue Konzepte sind nötig – sowohl in der technischen und organisatorischen Gestaltung als auch im regulativen Bereich. Der Veröffentlichung der Forschungsagenda zu Cyber-Physical Systems sollten zu diesen Themen Ausarbeitungen folgen.

16 Datensparsamkeit betrifft nicht nur die Verringerung des Umfangs der (personenbezogenen) Daten, sondern auch die Unmöglichkeit oder das Erschweren, einen Personenbezug herzustellen. Anders formuliert handelt es sich um eine Nichtverkettbarkeit von Daten zu einer Person, s.a. ULD / Technische Universität Dresden: Verkettung digitaler Identitäten, 2007, https://www.datenschutzzentrum.de/projekte/verkettung/.

17 Jan Camenisch, Anna Lysyanskaya: An efficient system for non-transferable anonymous credentials with optional anonymity revocation, in: Advances in Cryptology – EUROCRYPT 2001, Lecture Notes in Computer Science Vol. 2045, Springer, 2001, S. 93-118, doi:10.1007/3-540-44987-6_7; Stefan A. Brands: Rethinking public key infrastructures and digital certificates, MIT Press, 2000.

Das von der EU geförderte Projekt ABC4Trust (https://www.abc4trust.eu/) erarbeitet aktuell Konzepte und Implementierungen für solche attributbasierten Berechtigungsnachweise in mehreren Anwendungsbereichen.