

Endbericht

Selbstorganisierende adaptive Systeme - Analyse der Chancen und Risiken sowie der Gestaltungsansätze neuer IKT Ansätze

FKZ: 16/1571

Förderung von „Innovations- und Technikanalyse“ des Bundesministeriums für Bildung und Forschung

vorgelegt dem Projektträger

VDI/VDE/IT

Steinplatz 1

10623 Berlin

Berlin, März 2010



i | ö | w

Institut für ökologische Wirtschaftsforschung (IÖW)

Potsdamer Straße 105

D-10785 Berlin

Tel. +49 – 30 – 884 594-0

E-mail: mailbox@ioew.de

In Kooperation mit:



Leibniz
Universität
Hannover



Leibniz Universität Hannover

Institut für Systems Engineering

Fachgebiet System- und Rechnerarchitektur (SRA)

Appelstraße 4

30167 Hannover



FU Berlin

Institut für Philosophie

Habelschwerdter Allee 30

14195 Berlin

und



KANZLEI DR. ERBEN

Neuenheimer Landstraße 36

D-69120 Heidelberg

BearbeiterInnen:

Institut für ökologische Wirtschaftsforschung (IÖW)

Dr. Jobst Conrad (Hauptautor des Endberichtes)
Ulrich Petschow
Eugen Pissarskoi
Angelika Müller: Fallstudie adaptive Kameras
Jakob Höhne: Fallstudie Logistik
Enrico Pisko: Fallstudie Verkehrssteuerung

Leibniz Universität Hannover

Yvonne Bernard
Prof. Dr. Jörg Hähner

Freie Universität Berlin

Argumentanalyse

Juniorprof. Dr. Gregor Betz
Christian Voigt

Kanzlei Dr. Erben

Rechtsexpertise

Dr. Meinhard Erben
Dr. Wolf Günther

Inhaltsverzeichnis

0	Zusammenfassung	8
1	Aufbau, methodisches Vorgehen, Ziele und Grenzen der Studie.....	11
2	Neue Ansätze bei Informations- und Kommunikationstechnologien: zentrale Konzepte und Merkmale	15
2.1	Entwicklungstrends	15
2.2	Konzepte und Merkmale smarter IT-Systeme	17
2.3	Spezifikation von Organic Computing	20
2.4	Klärung zentraler Begriffe wie Autonomie, Selbstorganisation, Emergenz	26
3	Entwicklungslinien und Marktperspektiven von Organic Computing und smarten IT-Systemen.....	47
3.1	Zur Geschichte und Entwicklung von Organic Computing	47
3.2	Übersicht über laufende OC Projekte	54
3.3	Marktanalyse und Bedingungen der Markteinführung	57
3.4	Entwicklungs- und Marktperspektiven von Organic Computing	60
4	Chancen und Risiken selbstorganisierender adaptiver Systeme.....	65
4.1	Analyseraster	65
4.2	Probleme und Issues von smarten adaptiven Systemen.....	70
4.3	Chancen und Risiken von Organic Computing: Kontext und Spezifikation	76
5	Fallstudien zu Organic Computing.....	80
5.1	Ampel- und Verkehrssteuerung	80
5.2	Adaptive Kamerasysteme	82
5.3	Logistik	84
5.4	Vergleichende Zusammenfassung	87
6	Debatten über Chancen und Risiken von Organic Computing: Soziale Diskurse und Argumentationsanalyse.....	90
6.1	Charakteristika sozialer Diskurse.....	90
6.2	IT- und OC-Diskurse	92
6.3	Charakteristika von Argumentationsanalysen	93

7	Rechtliche Problemstellungen bei Organic Computing	100
8	Zusammenfassender Überblick	109
9	Ergebnisse und Schlussfolgerungen	113
9.1	Validität und Generalisierbarkeit	113
9.2	Zentrale Ergebnisse	114
9.3	Roadmap und (politische) Gestaltungsmöglichkeiten	116
10	Literatur.....	123
A-I	ANHANG I: Liste der interviewten Personen.....	I-1
A-II	ANHANG II: Argumentationsanalyse für und wider den Einsatz von Organic Computing ...	II-1
A-III	ANHANG III: Rechtsexpertise zu selbstorganisierenden adaptiven IT Systemen.....	III-1

Abbildungsverzeichnis

Abbildung 2.1: Entwicklung der Autonomie über die Zeit am Beispiel ausgewählter Architekturmuster	29
Abbildung 2.2: Konzeptionelles Modell der fundamentalen Begriffe.....	29
Abbildung 2.3: Taxonomie der Systemeigenschaften	32
Abbildung 2.4: Konzeptionelles Modell von Autonomie	34
Abbildung 3.1: DFG-Schwerpunktprogramm „Organic Computing“	52
Abbildung 4.1: Erweiterte Gliederung der Soziosphäre	68
Abbildung 6.1: Argumentlandkarte: Entwicklung der Autonomie über die Zeit am Beispiel ausgewählter Architekturmuster.....	95
Abbildung 6.2: Argumentlandkarte: Diskussion um die Verhältnismäßigkeit, Ausschnitt 1	97
Abbildung 6.3: Argumentlandkarte: Diskussion um die Verhältnismäßigkeit, Ausschnitt 2	98
Abbildung 9.1: Herausforderungen von OC	118

Tabellenverzeichnis

Tabelle 4.1: Analytisches Modell der Chancen und Risiken von OC	66
Tabelle 4.2: Dimensionen technischer Chancen und Risiken.....	66
Tabelle 4.3: Dimensionen sozialer Chancen und Risiken	69
Tabelle 5.1: Evolution der Planungs- und Steuerungsprozesse logistischer Objekte.....	86
Tabelle 6.1: Ausschnitt aus dem Fragenkatalog: Fragen zur Verhältnismäßigkeit des OC Systems im Anwendungskontext.....	99

Abkürzungsverzeichnis

AC(I)	autonomic computing (initiative)
ACM	association for computing machinery
AI	artificial intelligence
AIS	Fraunhofer Institut Autonome Intelligente Systeme, St. Augustin
Aml	ambient intelligence
ARCS	(International Conference on) Architecture of Computer Systems
ATC	(International Conference on) Autonomic and Trusted Computing
Az	Aktenzeichen
BICC	Biologically Inspired Cooperative Computing
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BMBF	Bundesministerium für Bildung und Forschung
BMWi	Bundesministerium für Wirtschaft
BSI	Bundesamt für Sicherheit in der Informationstechnik
CEC	Congress on Evolutionary Computation
CEBIT	Centrum der Büro- und Informationstechnik
CCS	carbon capture and storage
DFG	Deutsche Forschungsgemeinschaft
DNA	desoxyribonucleic acid
DoS	denial of service
EU	Europäische Union
FE	Forschung und Entwicklung
FU	Freie Universität (Berlin)
GI	Gesellschaft für Informatik
GPSG	Geräte- und Produktsicherheitsgesetz
IBM	International Business Machines
IBV	intelligente Bildverarbeitung
ICT	information and communication technologies
IDATE	Institut de l'Audiovisuel et des Télécommunications en Europe
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IÖW	Institut für ökologische Wirtschaftsforschung
ISTAG	Information and Communication Technologies Advisory Group
IT	Informationstechnologie
ITG	Informationstechnische Gesellschaft
IuK	Information und Kommunikation
KIT	Karlsruhe Institute of Technology
KKW	Kernkraftwerk
LFGB	Lebensmittel- und Futtermittel-Gesetzbuch
MAS	Multiagenten-System
MDA	model-driven architecture
NASA	National Aeronautics and Space Administration
NC	natural computing
OC	Organic Computing
OECD	Organisation for Economic Cooperation and Development
PC	personal computer

PC	pervasive computing
P2P	peer-to-peer
ProdHG	Produkthaftungsgesetz
RFID	Radio Frequency Identification (Radiofrequenz Identifikation)
SAP	Systems Applications and Products in Data Processing
SaSo	selbstadaptiv selbstorganisierend (self-adaptive self-organising)
SFB	Sonderforschungsbereich (der DFG)
SOA	service-oriented architecture
SRA	(Fachgruppe) System- und Rechnerarchitektur (im Institut für Systems Engineering)
SuOC	system under observance and control
TA	technology assessment
TNO	Toegepast Natuurwetenschappelijk Onderzoek
TU	Technische Universität
TWEL	Trustworthiness Enforcement Layer
UBA	Umweltbundesamt
UC	ubiquitous computing
VDE	Verband der Elektrotechnik Elektronik Informationstechnik
VDI	Verein Deutscher Ingenieure

0 Zusammenfassung

Diese Studie befasst sich mit der Spezifikation und den Chancen, Risiken und Gestaltungsmöglichkeiten von Organic Computing als einem auf technische Umsetzung abhebenden Programm von selbstadaptiven selbstorganisierenden (SaSo-)Systemen. Organic Computing (OC) stellt ein zielorientiertes, vielfältige Anwendungen erlaubendes und anstrebendes Konzept dar, das ein die verschiedenen Ebenen von ubiquitous computing umfassendes (visionäres) Leitbild mit auf technische Umsetzung orientierten Ziel(vorstellung)en – wie Selbstorganisation, kontrollierte Emergenz, Observer/Controller-Architektur – verknüpft.

Dabei basieren die im Laufe des eineinhalbjährigen Untersuchungszeitraums von den drei beteiligten Projektgruppen (IÖW Berlin, SRA Hannover und Institut für Philosophie, FU Berlin) und über ein externes Rechtsgutachten zusammengetragenen Informationen und durchgeführten Analysen im Wesentlichen auf umfangreichen Literatur- und Internet-Recherchen, 15 halb- bis einstündigen Interviews mit IT- und OC-Experten, der Teilnahme an dem zweitägigen 8. Organic Computing Kolloquium, Interviews auf der CEBIT in Hannover, sowie zwei Workshops an der Universität Hannover (Möglichkeiten von OC und Rechtsaspekte).

In dem Vorhaben ging es um die Bestandsaufnahme von Forschungsansätzen im Bereich selbstorganisierender adaptiver Systeme, um exemplarische Fallstudien, und um die integrierende Zusammenführung und mögliche Verallgemeinerbarkeit der Untersuchungsergebnisse. Von daher will die Studie einen konsistenten systematischen Überblick über die verschiedenen für die Entwicklung und Nutzung von OC relevanten Aspekte geben. Demgegenüber entfielen angesichts der Begrenztheit der projektbezogen verfügbaren personellen Ressourcen ins Detail gehende, mögliche Dilemmata und Kontroversen in *einzelnen* OC-Projekten in den Blick nehmende Untersuchungen.

Als wesentliche Ergebnisse der Untersuchung lassen sich festhalten:

- 1) Infolge der zunehmenden, sozial zwar kritisch beleuchteten, aber nicht in Frage gestellten Informatisierung (ambient intelligence, Vernetzung, Digitalisierung) der Gesellschaft, der damit einhergehenden Komplexitätszunahme technischer Systeme sowie der Überforderung und dem Versagen konventioneller Formen der Programmierung und Fehlerkontrolle von Software wird (in sich mit IT befassenden Diskursen) ein gesellschaftlicher Bedarf nach selbstadaptiven selbstorganisierten Systemen wahrgenommen und formuliert, die diesen Megatrend technisch zu bewältigen erlauben sollen.
- 2) In Rahmen der generellen Diskussion und modellhaften Konzeptualisierung solcher selbstadaptiver selbstorganisierender Systeme entwickelte sich seit den 2000er Jahren die Organic Computing Initiative als auf technische Anwendungen orientiertes deutsches Spezifikum, das als DFG-Schwerpunktprogramm unterschiedliche Forschungsvorhaben koordiniert und eine gewisse Eigendynamik gewonnen hat.
- 3) Sein Ziel ist es, die wachsende Komplexität der uns umgebenden Systeme durch Mechanismen der Selbstorganisation zu beherrschen, indem kontrolliertes emergentes Verhalten in technischen Systemen theoretisch verstanden und ermöglicht wird und aufeinander abgestimmte (Basis-)Technologien für Organic Computing entwickelt werden.
- 4) Faktisch dient(e) OC dabei als ein auf technische Umsetzung des allgemeinen Konzepts von SaSo-Systemen orientiertes Leitbild, das zu vermehrter Kommunikation und Austausch zwischen in diesem Forschungsfeld engagierten Wissenschaftlern und zur formell-

organisatorischen Integration ansonsten separater Forschungsaktivitäten mit der Folge stärkerer gemeinsamer Forschungsziele und -linien führt(e).

- 5) Als eine Querschnittstechnologie kann Organic Computing grundsätzlich in vielen Bereichen zum Einsatz kommen, wie industrielle Produktion, Energiesysteme, Logistik, Handel, Wartung hochwertiger technischer Produkte, Mobilität/Transport, Telekommunikation, Sicherheits- und Kontrollsysteme, Gesundheitswesen, intelligentes Büro, oder Produktintelligenz. Dabei geht es vorrangig um die verstärkte Einbettung großer Hardware- und Software-Komplexe in technische Systeme und nicht allein um größere, komplexere und vernetztere IT-Systeme, die sowohl die Verbesserung bereits in der Praxis eingesetzter technischer Systeme als auch die Realisierung neuartiger technischer Systeme betrifft.
- 6) Bislang ist allerdings noch offen, ob das Ziel von Organic Computing von weitgehend autonomer Selbstorganisation mit kontrollierter Emergenz und Selbst-X-Eigenschaften sowohl in technischer als auch in wirtschaftlicher Hinsicht (Einführungsprobleme, wirksame Lernkurven, Kosten, Wettbewerbsfähigkeit) auch erreicht werden wird.
- 7) Insofern OC-Systeme eine substantielle Alternative zu und – im Falle ihrer erfolgreichen Anwendung – zumeist einen wirklichen Fortschritt gegenüber bislang eher dominierenden zentral gesteuerten smarten IT-Systemen darstellen, stehen sie in Konkurrenz zu diesen und könnten sie – bei gelingender Selbstorganisation, kontrollierter Emergenz und preislicher Wettbewerbsfähigkeit – vielfach mittelfristig ersetzen. Demgegenüber werden zum gegenwärtigen Zeitpunkt Forschungskonzepte, die sich primär um ein besseres Verständnis und die Modellierung dezentraler SaSo-Systeme bemühen, eher als einander ergänzend denn als miteinander konkurrierend wahrgenommen.
- 8) Es geht bisher im Wesentlichen um (anwendungsorientierte) Grundlagenforschung mit zwar in ihrem Zeithorizont differierenden, aber durchweg mittel- bis längerfristigen Marktperspektiven von 5 bis 25 Jahren.
- 9) Bis zum gegenwärtigen Zeitpunkt handelt es sich bei Organic Computing im Wesentlichen um eine wissenschafts- und technikgetriebene Trajektorie, deren konkrete Gestaltung von einer aus Wissenschaftlern bestehenden Akteurkonstellation bestimmt wird, was sich in den verfolgten Projekten und Untersuchungsdesigns niederschlägt und durch das Fehlen relevanter Kontroversen über Forschungsziele, -methoden und -ergebnisse auszeichnet.
- 10) Wirtschaftsunternehmen verhalten sich bislang gegenüber Organic Computing eher zögernd und sind hierin trotz Aufforderungen zur Kooperation nicht involviert, beobachten aber teils diese Entwicklung und verfolgen teilweise selbst ähnliche, weniger breit angelegte, auf Selbstorganisation hinauslaufende FE-Vorhaben.
- 11) Das generische Grundproblem von Organic Computing besteht in der Möglichkeit und Realisierbarkeit kontrollierter Emergenz und notwendiger Selbsterklärung, sodass eine erfolgreiche Balance zwischen Autonomie und Begrenzung von OC-Systemen erreicht werden kann.
- 12) Von daher sind Fragen der Sicherheit von OC-Systemen und des Haftungsrechts für ihre praktische Nutzung zentral und stehen Anwendungen in technisch weniger sicherheitsrelevanten Bereichen bzw. in Bereichen, in denen sicherheitsrelevante Risiken ausgeschlossen werden können, im Vordergrund (wie z.B. adaptive Kamerasysteme oder Logistiksysteme).

Was den angestrebten Entwicklungspfad von Organic Computing anbelangt, so geht es auf technischer und organisatorischer Ebene im Wesentlichen um

- die genaue theoretisch-konzeptionelle Analyse von OC und den Design komplexerer OC-Systeme,
- die technische Verbesserung und Optimierung von OC ermöglichenden Architekturen,
- die systemtechnische Realisierung der Balance in OC-Systemen zwischen Autonomie qua Selbstorganisation und Kontrolle qua kontrollierter Emergenz,
- die Vernetzung und Koordination von unterschiedlichen Dimensionen und Erfordernissen der OC-Forschung,
- konkrete Anwendungen von OC und deren praktische Erprobung,
- die Einbettung von OC-Systemen in technische Anwendungssysteme in Kooperation mit den diese herstellenden oder nutzenden Unternehmen und den zuständigen Behörden,
- die Nutzung von Zeitfenstern mit für OC-Entwicklung und -Anwendungen geeigneten Rahmenbedingungen,
- die Abschätzung und das Management möglicher (spezifischer) Risiken von OC-Systemen
- und um die durch diese Aktivitäten induzierte Eigendynamik, um eine breitenwirksame Durchsetzung von OC zu erreichen.

1 Aufbau, methodisches Vorgehen, Ziele und Grenzen der Studie

Dieser Abschlussbericht des vom BMBF geförderten Vorhabens „Selbstorganisierende adaptive Systeme: Analyse der Chancen und Risiken sowie der Gestaltungsansätze neuer IKT-Ansätze“ befasst sich mit einem durchgängig zu beobachtenden Entwicklungstrend bei Informations- und Kommunikationstechnologien in Richtung von „integrated systems of advanced computing devices, intelligent interface design, anytime, anywhere data communication“ (Weiser 1991), der unter Oberbegriffen wie ubiquitous computing (UC), ambient intelligence (AI), pervasive computing, autonomous computing (AC), self-adaptive self-organizing systems (SaSo) – und in diesem Zusammenhang speziell Organic Computing (OC) – in fast allen Bereichen des Lebens Einzug halten und dieses im Wesentlichen durch effektivere, effizientere und komplexere Informationsverarbeitung erleichtern soll. Damit sind allerdings zugleich zusätzliche (neuartige) technische und soziale Risiken, insbesondere etwa ein verstärktes Risiko des unentdeckten Missbrauchs verbunden.¹ Ein maßgeblicher Hintergrund dieser Entwicklung beruht auf der zunehmenden Komplexität neuer IT-Systeme, die einerseits möglichst individuell maßgeschneiderte Anwendungsoptionen bieten sollen, aber andererseits mit der tendenziellen Überforderung von Software-Entwicklern, steigender Fehleranfälligkeit der Software und personalaufwändigen Lokalisierungsprozessen auftretender Fehler einhergeht.² Mainzer (2008:105) fasst diese Aussichten und Problematik folgendermaßen

¹ “Billions of devices that are always on and always connected ... increase the complexity of our systems to the point where it is not possible to comprehend all of what we are using... We need to resolve issues of identity and authority when these devices conduct activities for people without human intervention, when no one is around to notice.” (Accenture/CERIAS 2001:11)

² Von der Malsburg (2008:9ff) beschreibt diese Schwierigkeiten wie folgt: “To realize broad application of systems composed of large numbers of limited complexity processing elements a new style of programming will be necessary, able to implement heterogeneous domains of data and processes in massively parallel systems, able to sustain faults in the system, and, above all, able to deal with complexity beyond the imagination of systems designers. Random faults may be an inevitable consequence of pushing electronic technology down to molecular dimensions (although error-correction techniques may be able to shield us from that problem), but, more importantly, none of the assumptions made at system design time about an application domain and its data structures may be reliably met at execution time. The combinatorics of violated assumptions create complexity that grows exponentially with system size (and what is to be called a system has to span all the subsystems to be integrated with each other!), forcing the system designer to give up explicit consideration of modes of fault and to handle the problem in a generic way. The way to go may be to give up deterministic control altogether and formulate systems as probabilistic processes, such as modeled in belief propagation networks, for instance...”

The computing power worldwide that is installed now or will be soon is arousing expectations as to what to do with it, creating tremendous market pull for complex software. Historically, the number of command lines in any large software venture, such as space programs, telephone exchanges, enterprise software, search engines etc., has been growing exponentially. New software projects often set themselves tasks that evidently are too complex to manage, leading to project failures, such as the American FAA Air Control project, the Denver Airport luggage handling system, the US's IRS or German Federal Tax software projects, which all failed without any tangible result. It is easy (and probably correct) to blame these failures on human management insufficiencies. But that only hides the fact that our computing paradigm is no longer adequate in view of the demands we put on it. The pool of available relevant human talent is already stretched to its limit... (In line with the classical programming paradigm) software can still be designed for programmers to keep track of this relocation, in order to keep up detailed communication, but this will make the system even more complex and difficult to work with. The only natural way to solve this difficulty is to let the system autonomously organize its internal structure, give up detailed communication and accept loss of insight. In order to do that, we will have to endow systems with their own creative infrastructure enabling them to autonomously organize themselves, effectively creating their own programs... The principles with which programmers formulate programs in

zusammen: „Complex computing systems begin to overwhelm the capacities of software developers and administrators. Self-organization has been a successful strategy of evolution to handle the increasing complexity of organisms with the emergence of novel structures and behavior. Thus, self-organization and emergence are fundamental concepts of organic computing. But these concepts are often used in a more or less intuitive manner. In the theory of complex systems and nonlinear dynamics, self-organization and emergence can be mathematically defined... In technology, the emergence of order and structures displays desired and undesired synergetic effects. Thus, controlled emergence is a challenge of computational systems simulating self-organizing organic systems of evolution. The question arises how far can we go in simulating high dimensional complex systems and avoiding uncontrolled risks.” (Mainzer 2008:105)

Wie durchweg bei der Einführung und Diffusion neuer Technologien in modernen Gesellschaften hängt deren Durchsetzung von den seitens ihrer Promotoren, Nutzer (und Betroffenen) perzipierten Chancen und Risiken ab. Diese resultieren insbesondere aus der technischen Reife und Zuverlässigkeit, den relativen Kostenvorteilen, der Sicherheit für Hersteller, Nutzer und Drittparteien, der Bandbreite der möglichen Anwendungen, der Machtposition der Promotoren und Implementatoren, der Umweltverträglichkeit und schließlich auch der gesellschaftlichen Akzeptanz einer (neuen) Technologie (vgl. Bauer 1995, Bauer 2004, Braun 1992, Conrad 1990, Freeman 1974, 1991, 1992, Huber 2004, Porter 1986). Diese ihre Durchsetzung begünstigenden Merkmale einer Technologie ergeben sich letztlich aus dem sich in ihrer Entwicklung und sie betreffenden sozialen Auseinandersetzungen faktisch herauskristallisierenden, in dieser Form von den Akteuren kaum so intendierten Technologiepfad, wie diverse Untersuchungen zur Technikgenese und technologischen Trajektorien herausgearbeitet haben (vgl. Dierkes 1997, Haniel/Stübinger 1999, Nelson/Winter 1982). Damit hängt die bewusste oder implizite Abwägung der Chancen und Risiken von selbstorganisierenden adaptiven Systemen deutlich von ihrer konkreten Gestaltung ab, für die sowohl in technischer als auch in sozialer Hinsicht zumeist eine beachtliche Bandbreite möglicher Entwicklungspfade existiert und für die infolgedessen Leitplanken zugunsten eines sozial erwünschten Entwicklungspfades entwickelt werden können. Ob diese Gestaltungschancen in der gesellschaftlichen Praxis wahrgenommen werden, lässt sich typischerweise nur im Einzelfall und vielfach erst ex post feststellen.

Dieser Bericht fasst nun die hierzu speziell für OC im Rahmen des Vorhabens recherchierten und diskutierten Informationen zusammen, die teils in den im Zwischenbericht (Petschow et al. 2009) und in den Anlagen des Endberichts wiedergegebenen Einzelstudien ausführlicher dargestellt und erörtert werden.

Dabei werden in diesem Kapitel 1 zunächst Aufbau, methodisches Vorgehen und Grenzen der Studie vorgestellt. In Kapitel 2 geht es um zentrale Begriffe, Konzepte und Problemlagen von selbstorganisierenden adaptiven Systemen, speziell von OC. Kapitel 3 zeigt dann Entwicklungslinien und Marktperspektiven von OC und smarten adaptiven Systeme auf, während Kapitel 4 ihre Chancen und Risiken systematisch diskutiert. Kapitel 5 resümiert die im Rahmen des Projekts durchgeführten Fallstudien zur (möglichen) Anwendung von OC bei Ampelsteuerung, adaptiven Kamerasystemen und in der Logistik. Kapitel 6 rekonstruiert die Logik der Argumentation im OC-Diskurs, ob und wie sich der Einsatz von OC in Abhängigkeit von seinen Chancen und Risiken hinreichend begründen lässt, während Kapitel 7 die rechtlichen Problemstellungen und möglichen

Regelungserfordernisse des Einsatzes von OC zusammenfasst. Auf dieser Grundlage gibt Kapitel 8 einen Überblick über Akteurkonstellationen, institutionelle Settings, Innovationsdynamik, Entwicklungsperspektiven und Folgewirkungen von OC. Abschließend fasst Kapitel 9 die wesentlichen Ergebnisse und Schlussfolgerungen der Studie nochmals zusammen, erörtert ihre Validität und Generalisierbarkeit, und versucht entsprechende (politische) Gestaltungsmöglichkeiten aufzuzeigen.

Die im Laufe des eineinhalbjährigen Untersuchungszeitraums von den drei beteiligten Projektgruppen (IÖW Berlin, SRA Hannover und Institut für Philosophie, FU Berlin) und über ein externes Rechtsgutachten zusammengetragenen Informationen und durchgeführten Analysen basieren im Wesentlichen einerseits auf umfangreichen Literatur- und Internet-Recherchen, über 15 halb- bis einstündige Interviews mit IT- und OC-Experten, (vgl. Anhang I) der Teilnahme an dem zweitägigen 8. Organic Computing Kolloquium, dem Besuch der CEBIT in Hannover (einschl. Fachgespräche und Interviews) sowie Workshops zu Chancen und zu rechtlichen Aspekten und internen Projekttreffen und Workshops, und andererseits auf der Ausarbeitung von Diskussionspapieren und Fallstudien und deren kritischer Kommentierung, Erörterung und Überarbeitung.

Die dabei (teils mehrfach) diskutierten Fragen betrafen im Wesentlichen:

- 1) die begriffliche Bestimmung, Eindeutigkeit und Abgrenzbarkeit von OC (vgl. Kapitel 2),
- 2) die Spezifika von OC gegenüber IT-Systemen allgemein und speziell smarten IT-Systemen (vgl. Kapitel 2.3),
- 3) Stand der Entwicklung, tatsächliche Anwendungen und Marktperspektiven von smarten IT-Systemen und speziell von OC (vgl. Kapitel 3),
- 4) die Taxonomie und Bestimmung von OC-Risiken (vgl. Kapitel 4),
- 5) die genuin mit OC verbundenen Chancen und Anwendungsmöglichkeiten (vgl. Kapitel 3, 4 und 5),
- 6) die Genese, zeitliche Entwicklungs- und Innovationsdynamiken, maßgebliche Akteure von OC, sowie deren Vorgehensweisen, Interessenlagen und -konflikte (vgl. Kapitel 4 und 8),
- 7) rechtliche Schwierigkeiten und Regulierungserfordernisse des Einsatzes von OC (vgl. Kapitel 7),
- 8) Auswahl und Durchführung geeigneter exemplarischer Anwendungsfallstudien (vgl. Kapitel 5),
- 9) die Entwicklung von OC prägenden und legitimierenden Argumentationsfiguren und Diskursmustern (vgl. Kapitel 6),
- 10) und die Eindeutigkeit der letztlich selektiv gewonnenen Befunde. (vgl. Kapitel 9)

Entsprechend sind die Ziele dieser Studie in folgenden Punkten zu sehen:

- 1) Herausarbeitung des Kontexts von OC: Informatisierung aller Lebensbereiche, smarte IT-Systeme und SaSo-Systeme
- 2) Erörterung der Ziele und Spezifik von OC und begriffliche Bestimmung seiner maßgeblichen Merkmale
- 3) Untersuchung der Entstehung, zeitlichen Entwicklung, Anwendungsmöglichkeiten und Marktpotenziale von OC

- 4) Benennung konkreter mit OC befasster Forschungsprogramme und -projekte und Darstellung der in ihnen untersuchten Inhalte, Probleme und Fragestellungen
- 5) Untersuchung der Rolle und Struktur von OC in exemplarischen Anwendungsgebieten
- 6) Diskussion der die Entwicklung von OC bestimmenden Akteurkonstellationen, Alleinstellungsmerkmale und konkurrierenden IT-Systeme
- 7) Diskussion und Unterscheidung der spezifischen und generellen, nicht spezifischen Chancen und Risiken von OC
- 8) Untersuchung der Argumentationsmuster in OC-Diskursen
- 9) Darstellung der insbesondere haftungsrechtlichen Problemstellungen bei OC
- 10) Schlussfolgerungen und Gestaltungsmöglichkeiten der Entwicklung und Nutzung von OC-Systemen.

Reichweite und Grenzen der Studie sind im Wesentlichen durch folgende Tatbestände bestimmt:

- 1) Das Vorhaben fokussiert eindeutig auf Organic Computing, während selbstorganisierende adaptive Systeme generell als maßgeblicher Kontext bestimmt, jedoch nicht im Detail untersucht wurden.
- 2) Angesichts der Begrenztheit der projektbezogen verfügbaren personellen Ressourcen wurden die einzelnen Bausteine des Projekts zwar auf eher allgemeiner Ebene systematisch behandelt, aber ins Detail gehende, mögliche Dilemmata und Kontroversen in einzelnen OC-Projekten in den Blick nehmende Untersuchungen entfielen.
- 3) Da sich OC noch weitgehend in der Forschungs- und Entwicklungsphase befindet und seine praktische Nutzung in den meisten Anwendungsfällen bestenfalls in einem Jahrzehnt zu erwarten ist, lassen sich viele der oben angesprochenen Fragestellungen lediglich auf Plausibilitätsebene und nicht empirisch eindeutig beantworten, sodass die Ergebnisse der Studie auch von daher zwar durchaus Evidenz und Stichhaltigkeit beanspruchen können, aber sich erst zukünftig als zutreffend erweisen müssen.
- 4) Entsprechend vermochten die Interviewpartner bei aller Auskunftsbereitschaft kaum eindeutige Aussagen zu weitergehenden Fragen nach konkreten Chancen und Risiken zu machen, da diese eben auch erst mittelfristig erwartete Nutzungsformen von OC betrafen.
- 5) Schließlich ging es in dem Vorhaben um die Bestandsaufnahme von Forschungsansätzen im Bereich selbstorganisierender adaptiver Systeme, um exemplarische Fallstudien, und um die integrierende Zusammenführung und mögliche Verallgemeinerbarkeit der Untersuchungsergebnisse. Von daher will die Studie einen konsistenten systematischen Überblick über die verschiedenen für die Entwicklung und Nutzung von OC relevanten Aspekten geben. Dabei nutzt sie zwar theoretische Ansätze, etwa aus der Innovations- und Technikgeneseforschung, um die Entwicklungspfade von OC angemessen zu interpretieren und zu kontextualisieren. Sie prüft jedoch weder diese Ansätze (im Sinne von Theorietests) auf ihre Richtigkeit noch entwickelt sie – abgesehen von deren eklektischer Kombination – solche selbst.

2 Neue Ansätze bei Informations- und Kommunikationstechnologien: zentrale Konzepte und Merkmale

Ehe Entwicklungslinien, Chancen und Risiken von OC näher betrachtet werden, sind zunächst zentrale Merkmale von smarten IT-Systemen und die Spezifikationen von OC genauer herauszuarbeiten und diesbezügliche begriffliche Klarstellungen und Definitionen vorzunehmen. Dies geschieht, indem signifikante Entwicklungstrends aufgezeigt (2.1), diesbezügliche Ansätze unter Bezugnahme auf die ausgewertete Literatur begrifflich genauer bestimmt (2.2), die Kennzeichen von OC herausgearbeitet (2.3) und die hierbei zum Tragen kommenden Konzepte erörtert werden (2.4).

2.1 Entwicklungstrends

Aus soziologischer Sicht spricht viel für die Vermutung, „dass die gesellschaftliche Komplexität durch die Entwicklung neuer Technik ständig größer wird und dass dieser Prozess mit der zunehmenden Durchdringung sozialer Systeme mit Informations- und Kommunikationstechnologien eine nochmalige Steigerung erfahren wird. Denn die Komplexität der Strukturen und Prozesse auf der Sach- und Beziehungsebene wird durch ihre informationstechnische Abbildung insofern gesteigert, als die Modelle der sekundären Ebene zur Steuerung der primären Prozesse verwendet werden (und insofern mehr sind als ein bloßes Abbild). Smarte, autonome Technik treibt diese Entwicklung weiter voran und steigert sie nochmals in eine neue Dimension.“ (Weyer 2009:6) In einer Dezennienperspektive lässt sich jedenfalls (in Ländern der 1. Welt) generell eine zunehmende Informatisierung fast aller Lebensbereiche beobachten, die mit verstärkter Vernetzung, individuellem Zugriff auf möglichst bedienungsfreundliche (persönliche) Computer und wachsender Komplexität der genutzten IT-Systeme einhergeht (vgl. Coenen 2008, ISTAG 2004, Lieshout et al. 2006, TNO/IDATE 2006).³ „Im IuK-Bereich kann quer durch alle betrachteten Studien die Verbreitung intelligenter, (auch drahtlos) vernetzter Objekte als ein wesentlicher Trend identifiziert werden. Diese neuartigen alles durchdringenden (Computer-)Netze können dabei alle Arten von Bestandteilen vom Supercomputer bis zu mobilen Kleinrechnern und intelligenten, eingebetteten Geräten sowie Mikrosystemen, Sensoren, RFID-Chips usw. umfassen.“ (Holtmannspötter et al. 2006:195) Demgemäß sind (künftige) technische Systeme computerisiert, komplex, stark vernetzt und sicherheitskritisch.⁴ Entscheidend ist hierbei, dass es um eine *verstärkte Einbettung* großer Hardware- und

³ Im Zwischenbericht wurde dieser Prozess wie folgt charakterisiert: „Unsere Welt ist – speziell im Technikbereich – in den letzten drei Jahrzehnten zunehmend komplexer geworden. Ein Fahrzeug besteht beispielsweise schon längst nicht mehr aus Motor, Bremse und ein paar Sensoren, sondern vereinigt eine Vielzahl eingebetteter Systeme in sich, die miteinander interagieren, um dem Fahrer ein optimales, komfortables und sicheres Gesamtsystem zu liefern. Ausgehend von ‚Moore’s Law‘, das eine jährliche Kapazitätssteigerungsrate mikro- und nanoelektronischer Schaltungen von ca. 66% besagt, werden Prozessoren auch in Zukunft immer komplexer werden. Auch die Bandbreiten der Kommunikationskanäle sind in der Vergangenheit gestiegen und ermöglichen eine wesentlich höhere Anbindung von eingebetteten Systemen untereinander als noch vor wenigen Jahren. Auch eine Anbindung noch leistungsfähigerer Server wäre möglich. Zudem sind die Entwicklungszyklen für neue Systeme immer kürzer geworden, so dass die Entwickler vor der Problematik stehen, immer komplexere Systeme immer kleiner in immer kürzerer Zeit zu schaffen.“ (Petschow et al. 2009:11)

⁴ Mit dem Begriff „sicherheitskritisch“ wird der Zusammenhang bezeichnet, dass im konkreten Fall grundsätzlich vorgehene und erwünschte Entscheidungen und Verhaltensweisen eines Systems dessen Funktionsfähigkeit oder auch

Software-Komplexe in technische Systeme wie Flugzeuge, Fahrzeuge, Telekommunikationsnetze und Fabrikationsanlagen geht (vgl. Müller-Schloer et al. 2004) und nicht allein um größere, komplexere und vernetztere IT-Systeme. Dieser Megatrend setzt allerdings die Entwicklung entsprechend smarter IT-Systeme voraus, wobei es sich durchaus um den Ausbau und die Weiterentwicklung bestehender Ansätze und Betriebssysteme handeln kann und grundlegende Umbrüche in der Gestaltung und Nutzung von IT-Systemen teils erst im nachhinein als solche deutlich werden, auch wenn solche komplexen IT-Systeme neue Organisationskonzepte und Architekturmuster⁵ erfordern, um sie handhabbar zu halten. Entsprechend fassen Heiß et al. (2008:2) Gründe für, die Grundidee von und die Ambivalenz der Autonomie smarter IT-Systeme wie folgt zusammen: „Rechnersysteme durchdringen unser Leben immer mehr. Lange schon sind Computer nicht nur in ‚klassischen‘ Bereichen wie in Rechenzentren oder in der Büroautomatisierung zu finden, sondern auch in Dingen des täglichen Lebens wie in Autos, Telefonen oder selbst in Kleidung, so dass das verlässliche Funktionieren der Informations- und Kommunikationssysteme immer essentieller wird. Dabei ist die für menschliche Administratoren kaum noch zu überschauende und folglich auch nur noch schwer zu beherrschende Komplexität heutiger IT-Infrastrukturen mittlerweile eine erhebliche Schwachstelle geworden. Es müssen daher neue Ansätze für Systemarchitekturen und Entwicklungsmethodiken gefunden werden, die das Ziel realisieren, das begründete Vertrauen in die Verlässlichkeit der Systeme zu erhöhen. Insbesondere muss die Komplexität durch zunehmende *Autonomie* der Systeme handhabbarer gemacht werden, damit IT-Sicherheitskonzeption, Revision und Zertifizierung weiterhin realisierbar sind. Das Potenzial autonomer Systeme für die effiziente Handhabung komplexer IT-Infrastrukturen wurde erkannt und ist auch von Herstellern in der Computerindustrie bereits aufgegriffen worden... Die Grundidee besteht darin, ein System mit Algorithmen und Verfahren derart zu erweitern, dass dieses die Sicherstellung bestimmter, in einer abstrakteren Zielstellung beschriebener Eigenschaften selbständig verfolgt. Für die Durchsetzung dieser Eigenschaften soll kein Nutzer oder Administrator dedizierte Maßnahmen ergreifen müssen. Systeme, die die Einhaltung einer Zielstellung selbständig verfolgen, werden auch selbstmanagend genannt. Mechanismen zur Realisierung von autonomem Verhalten bergen ein immenses Potenzial für die Umsetzung sowie für den Betrieb komplexer und dynamischer Systeme. Allerdings kann die Autonomie eines Systems ein bedarfsgerechtes Sicherheitsniveau gefährden (vgl. Kephart/Chess 2003, VDE/ITG/GI 2003): Durch das Zusammenspiel mit anderen Systemen bzw. Systemteilen können ungewollte emergente Effekte auftreten, die die Verlässlichkeit des betrachteten Systems verringern. Autonomes Verhalten kann also die Einhaltung von Sicherheitszielen negativ beeinflussen. Dies trifft umso mehr zu, da auch unerwünscht Autonomie auftreten kann, also ein beim Systementwurf nicht beabsichtigtes autonomes Verhalten.“

In der Wahrnehmung des benannten Megatrends unter den involvierten Akteuren wird denn auch die (laufende) Entwicklung selbstorganisierender adaptiver Systeme als mehr oder weniger zwangsläufiger Prozess dargestellt, der lediglich in seiner konkreten Form und Geschwindigkeit nicht festgelegt und damit von maßgeblichen Akteuren durchaus beeinflussbar und steuerbar ist. Dabei werden die Chancen solcher Systeme im Wesentlichen in der effektiveren, effizienteren und komplexeren Informationsverarbeitung gesehen, die zum einen mit Zeitgewinn und der Einsparung

infolge seiner Einbettung diejenige seines (IT-)Umfelds gefährden oder auch zum Systemzusammenbruch führen kann. Für autonome Systeme im Allgemeinen ergibt sich daraus die Forderung, dass – trotz der erwünschten Autonomie – noch eine manuelle Eingriffsmöglichkeit vorhanden sein sollte, mit der der Mensch das System in Bezug auf sicherheitskritische Entscheidungen beeinflussen kann und es z. B. in einen sicheren Zustand überführen kann.“ (Heiß et al. 2008:228)

⁵ „Ein Architekturmuster abstrahiert von einer Klasse von Architekturen und gibt mindestens eine wesentliche Charakteristik der betreffenden Architekturen wieder“ (Heiß et al. 2008:11), wobei eine Architektur Regeln bezüglich der Struktur eines Systems und den Zusammenhängen zwischen seinen Elementen definiert.

von Material- und Personalressourcen bei in anderer Form bereits praktizierten Prozessen, z.B. Ampelsteuerung, Kamerasysteme, Logistik, Service-Roboter u.a., und zum anderen mit der Realisierbarkeit neuer, bislang technisch nicht (effizient) durchführbarer Optionen, z.B. ambient assisted living, ambient assisted working/smart factory, smart mobility u.a. einhergeht (vgl. Schmeck 2009a; als frühzeitige Vision Weiser 1991). Dies geschieht vor allem dadurch, dass smarte IT-Systeme eigenständig (Gesamt-)Aufgaben übernehmen und optimieren, die sonst (bislang) menschlicher Arbeit und Kontrolle oder aufwändigerer Informationsverarbeitungsprozesse bedürfen. Als typische Anwendungsfelder werden industrielle Produktion, Energiesysteme, Logistik, Handel, Wartung hochwertiger technischer Produkte, Mobilität/Transport, Telekommunikation, Sicherheits- und Kontrollsysteme, Gesundheitswesen, intelligentes Büro, oder Produktintelligenz für den Endverbraucher genannt, in denen diverse Facetten smarterer Systeme wie digitales Produktgedächtnis, Internet der Dinge, Multi-Agenten-Systeme und ambient intelligence zum Tragen kommen (vgl. Nafz et al. 2006, Schmeck 2009a).

Auf den Punkt gebracht handelt es sich bei diesen smarten IT-Systemen und ihren Anwendungen vor allem um

- (eine Vielzahl von) intelligente(n) eingebettete(n) Systeme(n)
- in potenziell unlimitierten Netzwerken
- mit spontanen lokalen Interaktionen, die mit aus ihrer Selbstorganisation resultierenden emergenten Effekten einhergehen können,
- mit robusten Service-Leistungen in sich (dynamisch) verändernden Umwelten
- und mit flexiblen Verhaltensmustern als Reaktion auf variierende externe Beschränkungen (vgl. Schmeck 2009a).

2.2 Konzepte und Merkmale smarterer IT-Systeme

In diesem Abschnitt werden nochmals wesentliche Grundkonzepte smarterer selbstorganisierender adaptiver Systeme zusammenfassend präsentiert, um danach die sie mehr oder minder kennzeichnenden Merkmale und Problemstellungen deutlich zu machen. Auch wenn es sich (in der Praxis) um gleitende Übergänge handelt, werden als smarte Systeme hier nur solche IT-Systeme verstanden, die als selbstadaptive selbstorganisierende Systeme (SaSo) zumindest ansatzweise über Elemente von Selbstorganisation und der Anpassungsfähigkeit an sich verändernde Umwelten verfügen (vgl. Schmeck et al. 2009).⁶

Betrachtet werden, wie eingangs aufgelistet, ubiquitous computing (UC), pervasive computing (PC), ambient intelligence (Aml), autonomous computing (AC), self-adaptive self-organizing systems (SaSo).⁷

6 Beispielsweise sind ein handelsüblicher PC oder typische Computerspiele noch keine smarten Systeme.

7 In Bezug auf weitere Konzepte wie affective, invisible, ubisafe, calm, natural, grid oder cloud computing sei auf die entsprechende Literatur verwiesen (vgl. Bernard 2008, Pissarskoi 2008).

Ubiquitous computing stellt keinen eigenständigen Computing-Ansatz dar, sondern geht auf die eingangs zitierte Vision von Weiser (1991) zurück, um allgegenwärtige Datenverarbeitung als dritte Generation von IT-Systemen zu charakterisieren, die durch ortsunabhängige Datenverarbeitung, die Vernetzung datenverarbeitender Aggregate, die Ausstattung der meisten Geräte mit datenverarbeitenden Technologien, die kontextsensitive Verarbeitung von Informationen und zunehmende Selbstorganisation gekennzeichnet ist. Insofern bezeichnet UC als Überbegriff einfach ganz allgemein die mit der mehr oder weniger durchgängigen Informatisierung aller Lebensbereiche einhergehende Präsenz von in technische Geräte integrierten und (global) vernetzten IT-Systemen.⁸

Auch *pervasive computing* bezeichnet primär die Vision einer alles durchdringenden Computertechnologie, welche durch die stetige Miniaturisierung von Computerchips und -speichern sowie Fortschritte der Sensortechnik und der drahtlosen Kommunikation ermöglicht wird. „Zusammen mit stetig fallenden Preisen lassen es diese Fortschritte zu, dass derartige elektronische Komponenten in immer mehr alltägliche Dinge eingebaut werden können, sodass diese letztlich über die Sensoren ‚fühlen‘, mit Hilfe des Chips ‚denken‘, vermöge des Speichers ‚sich erinnern‘ sowie dank der drahtlosen Kommunikationsmodule ‚reden‘ können.“ (Coroama 2006:106) Ziel des pervasive computing ist es, Technologien möglichst weitgehend in den Alltag zu integrieren, sie immer und überall verfügbar zu machen, wobei die genutzten Gegenstände aufgrund entsprechender Sensoren im vorgegebenen Rahmen intelligent, zunehmend autonom und untereinander vernetzt agieren (sollen), um sie für den Menschen so unauffällig wie möglich zu gestalten (vgl. BSI 2006). „Der Mensch soll zwar von den vielen Möglichkeiten seiner vernetzten Umwelt profitieren, sich aber nicht mit den Zugangsschwierigkeiten über verschiedenste Nutzerinterfaces befassen müssen. Dafür ist es nötig, sowohl Sensoren als auch Aktuatoren kontextsensitiv auf den Nutzer und die aktuelle Aufgabe auszurichten.“ (Petschow et al. 2009:16) Bei pervasive computing geht es somit um die zwanglose, selbstverständliche Nutzung von mit vernetzter IT-Technik ausgestatteten, qua ihrer ‚Intelligenz‘ und Kontextsensitivität begrenzt selbstorganisiert adaptiv agierenden technischen Geräten wie z.B. in der häuslichen und mobilen medizinischen Versorgung. Festzuhalten ist hierbei, „dass sich Pervasive Computing noch in den ‚Kinderschuhen‘ befindet, da nur ein geringer Teil der identifizierten Systeme bis dato klinisch Tests durchlaufen hat oder sich bereits im regulären Einsatz befindet (vgl. Graefe et al. 2008, Orwat et al. 2008).“⁹

In ähnlicher Form zielt *ambient intelligence* (Umgebungsintelligenz) darauf ab, Sensoren, Funkmodule und Computerprozessoren massiv zu vernetzen, um so den Alltag des Menschen zu verbessern. Mit Hilfe von Sensornetzen können zahllose Überwachungs- und Komfortaufgaben übernommen werden. So hat *ambient assisted working* das Ziel, eine smart factory unter effektiver Ausnutzung vernetzter Sensoren zu realisieren. Und *ambient assisted living* steht für Assistenzsysteme im Gesundheits- und Lebensbereich, indem durch den Einsatz neuer (unauffälliger, unsichtbarer und leicht bedienbarer) Technologien die Umgebung, in der sich etwa ältere Menschen aufhalten, so gestaltet wird, dass für die betroffenen Personen ein hoher Grad an Selbständigkeit erhalten werden kann, ihre Sicherheit erhöht wird und die Kommunikation mit ihrem sozialen Umfeld

⁸ „Ubiquitous computing enables people to live, work, use, and enjoy things directly without being aware of their computing devices.“ (Mainzer 2008:119)

⁹ Die sozialen, ökonomischen, ökologischen oder ethischen Implikationen von Pervasive Computing (oder ambient intelligence oder ubiquitous computing) wurden bereits früh diskutiert und in TA-ähnlichen Projekten untersucht (vgl. Alahuhta et al. 2006, Bizer et al. 2006, Bohn et al. 2005, Friedewald et al. 2007, Gabriel et al. 2006, Heesen et al. 2005, Hilty et al. 2003, 2004, Meier/Stiftung Risikodialog 2006, Orwat et al. 2008, Wright et al. 2008)

verbessert wird.¹⁰ Ambient intelligence nutzt die Vernetzung verschiedenster Elemente, um einen neuen Zugang zu Technologien zu ermöglichen.

Autonomic computing lässt sich zwar ebenso wie die bislang beschriebenen Konzepte durch das Arrangement von IT-Systemen für einen generellen Zweck charakterisieren, jedoch stehen bei ihm deren rechnerbezogene Optimierung im Vordergrund. Das Paradigma Autonomic Computing geht auf eine Initiative der Firma IBM zurück (IBM Research 2009, Kephart/Chess 2003), die von dieser inzwischen aber – anders als jetzt cloud computing – nicht mehr ernsthaft verfolgt wird (vgl. Hähner/Müller-Schloer 2009). Ziel ist es, Möglichkeiten der Selbstkonfiguration, Selbstheilung, Selbstschutz und Selbstoptimierung in technische Produkte einzubauen, wobei auf die gesamte IT-Infrastruktur abgestellt wird. Diese Aspekte werden hauptsächlich aus Unternehmenssicht betrachtet, wobei speziell der Kostenfaktor berücksichtigt wird. Darauf aufbauend werden fünf Reifegrade der Unternehmens-IT unterschieden (vgl. Petschow et al. 2009:14):

- *Grundlegend*: Die einzelnen Bestandteile der IT-Infrastruktur werden getrennt betrieben und gewartet.
- *Geleitet*: System-Management Werkzeuge werden verwendet, um Information zentral zu sammeln.
- *Vorhersagend*: Analysemethoden und -Werkzeugen werden genutzt, um mögliche Szenarien vorab zu simulieren.
- *Adaptiv*: Computersysteme können automatisiert Aktionen aufgrund von Informationssystemen und extrahiertem „Wissen“ starten.
- *Autonom*: Vollständig von Anforderungsbeschreibungen und definierten Zielen getriebene IT-Infrastruktur.

Schließlich sind als allgemeines Konzept *self-adaptive self-organizing systems* (SaSo) zu nennen. Der Bezeichnung gemäß geht es allgemein um die (formalen) Strukturen, die Entwicklung und Gestaltung von smarten IT-Systemen, die in der Lage sind, ihre Dienstleistungen in Anpassung an die jeweiligen, sich verändernden Umweltgegebenheiten und Nutzerbedürfnisse selbst zu organisieren. Wie diese Anpassungs- und Selbstorganisationsfähigkeit im Einzelnen jeweils computer- und netzwerktechnisch gewährleistet wird, ist damit nicht festgelegt. Bei Aml oder AC dürfte es sich in der Tendenz, aber nicht zwingend um SaSo-Systeme handeln. Jedenfalls stellt die Entwicklung und (kommerzielle) Realisierung von selbstadaptiven und selbstorganisierenden IT-Systemen einen Fokus der Informatik und Computer Science mit entsprechenden internationalen Tagungen wie der IEEE¹¹ International Conference on Self-Adaptive and Self-Organizing Systems (SASO) dar. OC-Systeme sind in diesem Zusammenhang eindeutig als auf technische Umsetzung ausgegerichtete SaSo-Systeme zu klassifizieren.¹²

¹⁰ „Dazu gehören auch die Unterstützung bei alltäglichen Verrichtungen, die Gesundheits- und Aktivitätsüberwachung, der Zugang zu sozialen, medizinischen und Notfallsystemen und die Erleichterung sozialer Kontakte.“ (Gesellschaft für Informatik/Informationstechnische Gesellschaft 2008:9)

¹¹ genealogisch 1884 als Akronym für Institute of Electrical and Electronics Engineers entstanden

¹² Sie weisen deshalb in der Tendenz eine etwas größere Marktnähe als SaSo-Systeme im Allgemeinen auf.

Zusammenfassend lässt sich der angesprochene Megatrend zu einer allgegenwärtigen Datenverarbeitung (UC) mit Müller et al. (2006) in drei (qualitative zeitliche) Schritte aufteilen:

Im ersten Schritt (mobile computing) werden um 2000 folgende Eigenschaften realisiert: (1) Ortsunabhängigkeit der Datenverarbeitung, (2) Ausstattung von so vielen Dingen wie möglich mit datenverarbeitenden Technologien, (3) Vernetzung der datenverarbeitenden Dinge untereinander.

Im zweiten Schritt werden technische Geräte bis ca. 2010 dazu gebracht, kontextsensitive Informationen zu verarbeiten (pervasive computing).

Im dritten Schritt wird bis ca. 2020 ihre Selbstorganisation verwirklicht (self-adaptive self-organizing systems, organic computing, autonomic computing).

Die skizzierten Grundkonzepte smarter IT-Systeme lassen sich auch als Leitbilder verstehen, die sich mithilfe ebendieser propagierten (Computing-)Technologien in absehbarer Zeit verwirklichen lassen sollen.

2.3 Spezifikation von Organic Computing

Auf der Basis des vorangehenden Abschnitts können nun Essenz und maßgebliche Charakteristika von OC gemäß den Spezifikationen in der Literatur genauer bestimmt werden (vgl. Gesellschaft für Informatik et al. 2008, Würtz 2008; Conrad 2008b, 2008c, Petschow et al. 2009).

Gemäß der Bionik als dem Versuch, von der Natur zu lernen, um die Technik zu verbessern (vgl. Gleich et al. 2007, Rossmann/Tropea 2005) ist die Grundidee von OC, „Ideen und Konzepte aus der Natur auf komplexe technische Systeme zu übertragen, um diese beherrschbar und robuster gestalten zu können.“¹³ (Bernard 2008:2) „Ziel des Organic Computing ist es, die wachsende Komplexität der uns umgebenden Systeme durch Mechanismen der Selbstorganisation zu beherrschen und an den Bedürfnissen der Menschen zu orientieren.“ (Gesellschaft für Informatik et al. 2008:31) “A central assumption of Organic Computing is that it is scientifically fruitful to interpret complex systems of interacting processes as computational systems and to study them as such. Consequently, they can in principle be reduced to or simulated by Boolean operations, but the study of their organizational structure should be carried out on a higher level. The second assumption, which is the computer science point of view, states that it is technically useful to apply the lessons learned from the study of natural systems to build computational systems with desired properties – complex in their inner structure, but relatively straightforward to interact with. It is very clear that no magic is to be expected from Organic Computing in solving computational problems... Perhaps the most striking feature of these processes is that the systems show organized behavior by themselves, without any obvious planning or external control. Central to Organic Computing research are therefore phenomena of self-organization, accompanied by a set of effects known under the name self-x properties.” (Würtz 2008:3f) “From a methodological point of view, the introduction of order parameters for modeling self-organization and the emergence of new structures is a giant reduction of complexity. The study of, perhaps, billions of equations, characterizing the behavior of the elements on the microlevel, is replaced by some few equations of order parameters, characte-

¹³ “Organic Computer Systems consist of autonomous cooperative subsystems and act – as far as possible – self-organized.” (Hähner/Müller-Schloer 2009:5)

riking the macrodynamics of the whole system. Complex dynamical systems and their phase transitions deliver a successful formalism to model self-organization and emergence.¹⁴ Further on, the knowledge of characteristic order parameters and critical values of control parameters open a chance to influence the whole dynamics and to create desired states of technical systems by self-organization. The formalism does not depend on special, for example, physical laws, but must be appropriately interpreted for biological and technical applications.” (Mainzer 2008:111) Im Vordergrund von OC steht also das Selbstmanagement der Systeme; dies bedingt Eigenschaften der Selbstkonfiguration, der Selbstoptimierung, der Selbstheilung, des Selbstschutzes.¹⁵ Ein „organischer Computer“ sei damit nach Müller-Schloer et al. (2004:332) definiert als ein selbstorganisierendes (technisches) System, das sich den jeweiligen Umgebungsanforderungen dynamisch anpasst. Selbstorganisation und Adaptivität mit all ihren Facetten werden nicht nur das System insgesamt, sondern das Verhalten sämtlicher Komponenten eines künftigen organischen Informationsverarbeitungssystems bestimmen.¹⁶ Sie haben (strukturimmanente) Vor- und Nachteile: flexibel, robust, selbstoptimierend, sinkender Entwurfsaufwand¹⁷; nicht tolerable Fehler und unproduktiver Aufwand lernender Systeme, lange Reaktionszeiten, gezielte unerlaubte Beeinflussungen.¹⁸ OC baut somit auf dem Zusammenspiel einer großen Anzahl von Einzel-Elementen auf. Dabei wird von den Elementen erwartet, dass sie sich nicht starr an einprogrammierte Vorgaben halten, sondern adaptiv auf Anforderungen von außen reagieren. Das Verhalten des Gesamtsystems ergibt sich dann wieder aus dem Zusammenspiel der Elemente (Emergenz).¹⁹ Die Nutzung des Emergenzverhaltens organischer eingebetteter Systeme qua seiner Gestaltung und Beschränkung (kontrollierte Emergenz) wird ausschlaggebend für deren technischen Einsatz sein.²⁰ „Um die Chancen solcher Systeme zu nutzen und ihre Risiken zu beherrschen, sind ein tieferes Verständ-

14 “According to the principle of computational equivalence (Mainzer 2004), any dynamical system can be simulated by an appropriate computational system. But, contrary to Turing’s AI-thesis, that does not mean computability in every case... Limitations of computability are characteristic features of complex systems. In a complex dynamical world, decision making and acting is only possible under conditions of bounded rationality.” (Mainzer 2008:118)

15 Diese Eigenschaften werden als unausweichliche Forderung angesehen, ohne die zukünftige komplexe Systeme nicht mehr zu managen bzw. nicht mehr beherrschbar sein werden. Selbstbewusstsein wird damit noch nicht unterstellt, jedoch nicht ausgeschlossen.

16 „For self-organization to be possible, the systems must contain ways of assessing themselves and modify their behavior or parameters, according to *metrics*, which measure the desirability or utility of a certain state... In the long run, these metrics must be also subject to evolution and learning. The hope here is to be able to find rather general meta-algorithms that can pick up even these evaluation metrics from the environment in a useful way.” (Würtz 2008:4)

17 Entsprechend benennen Hähner/Müller-Schloer (2009:8) als Vorteile von OC: (1) Scalability: Decentralization enables building of large networks. (2) Robustness: Self-healing properties make systems robust to failures. (3) Self-control: OC systems have less management overhead.

18 Emergenz und Selbstorganisation sind Schlüsselthemen im Bereich intelligenter technischer Systeme. Selbstorganisation ist ein Prozess, der durch das kooperative Wirken von Teilsystemen zu komplexen Strukturen des Gesamtsystems führt. Emergenz bezeichnet das Phänomen, dass sich bestimmte Eigenschaften eines Ganzen nicht aus seinen Teilen erklären lassen. Etwas präziser kann Emergenz auch als die Zunahme der Ordnung aufgrund selbstorganisierter Prozesse zwischen den Systemelementen bezeichnet werden.

19 Von zentraler Bedeutung für den technischen Einsatz der Prinzipien des Organic Computing wird daher ein tieferes Verständnis organischer Systemarchitekturen sein. Es geht dabei sowohl um ein Verständnis natürlicher emergenter Systeme als auch um die Frage der Beherrschbarkeit von Selbstorganisation und Emergenz in technischen Systemen (vgl. Mainzer 2008, Müller-Schloer/Sick 2008, Wolf/Holvoet 2005). „From the view point of systems science, the challenge of organic computing is controlled emergence.“ (Mainzer 2008:116)

20 Trotz vieler interessanter Forschungsansätze sind zentrale Fragen des Organic Computing ungelöst und bedürfen einer übergreifenden Analyse und Kooperation. Hierzu gehören die folgenden Themen: Theorie komplexer Systeme, zielgerichtete emergente Prozesse, System-Architekturen, eingebettetes Lernen, Lerneffizienz und A-priori-Wissen, Sicherheit und Beschränkung, Selbsterklärung, Hardware-Basis.

nis solcher Systeme, die Kontrolle des kollektiven Verhaltens ihrer Komponenten, die Beherrschung von Nicht-Determinismus und die praktische Umsetzung komplexer, technischer Systeme durch Architekturen, Werkzeuge und Entwurfsverfahren notwendig.“ (Gesellschaft für Informatik et al. 2008:31)

“Our goal in the context of organic computing is to define an architecture of data elements and their interactions, to be implemented in arrays of digital processors, so that iteration of the interactions lets the system gravitate towards (sequences of) globally ordered states. The challenge is to define this architecture on a very general level, without explicit reference to specific problems and applications. The latter is then to be achieved by installation in the system of appropriate initial states, an endowment of useful algorithms, and exposure to specific input patterns. The architecture, initial state and library of algorithms constitute the innate structure, based on which the exposure to specific input in education and learning prepares for specific tasks to be performed. Self-organization is particularly important in noise-prone systems, such as the living cell or human brain or, in fact, the analog computer. The latter was brought down by the difficulty that when many elementary steps are chained up, each one subject to some level of inaccuracy, the end result of a long computation is totally dominated by noise and useless. How does (a system like) the cell or the brain avoid this error catastrophe? It all depends on the nature of the system dynamics realized by the interactions. If this dynamics is of the chaotic type, where small differences in initial state lead to large differences in final state, the system will be drowned in noise. If, on the other hand, the dynamics is of attractor type, such that sets of similar initial states lead to the same final state, then the error catastrophe is averted. The globally ordered states of self-organizing systems are attractor states. The task ahead of us in the present context is to define an architecture, a set of fundamental rules of interaction of active data elements, that turn functionally desirable system states into attractor states.“ (Malsburg 2008:15f)

Die entsprechenden ingenieurwissenschaftlichen Herausforderungen beschreiben Bellman et al. (2008:27f) folgendermaßen: “We examine the systems engineering challenges of developing the above capabilities, focusing on five specific challenges. The first of these challenges is to create generative processes. That is, although traditional design methods include tools for adjusting an operating point within a known parameter space, we will also need to develop processes for our OC systems that can efficiently create new and very different possibilities for the system. Secondly, because OC systems will adapt and change, the instrumentation that provides information about the system’s current internal state will also need to rapidly adjust in a number of ways to the system’s increasing complexity. This challenge also implies that we will also need to develop tools for creating evaluative processes that express the results of measurements in ways that are useful and understandable to both the system and its engineers, developers and users. The next challenge that we address is how to build the capabilities for reflection and direction that enable an OC system to identify and assess possible responses, and choose, implement, and adjust them as its context and understanding shift. Our fourth challenge is to enable our OC systems to utilize a portion of their resources to “actively experiment”, discovering properties, relationships, attributes, and limitations of both their own capabilities and their ability to operate within different environments. The final engineering challenge is to combine the capabilities resulting from the previous four challenges to enable our OC systems to build models of their changing environment, and to use those models to identify unusual features of their situation. That is, we suggest that an OC system must achieve a situational awareness capability that directs its resources toward the aspects of its envi-

ronment and internal state that present, at the current time, the most important threats or opportunities.“²¹ (Bellman et al. 2008:27f)

Auch wenn OC somit eine bestimmte Perspektive und mögliche Charakteristik smarter Systeme in den Vordergrund stellt, nämlich die bessere Beherrschung und Reduktion der Komplexität datenverarbeitender Systeme qua Selbstorganisation und Adaptivität, ist es deshalb aber noch nicht als eine genuin eigene Fallgruppe smarter Systeme einzustufen, da es zum einen bislang vor allem ein im Entstehen begriffenes interdisziplinäres Forschungsfeld im Rahmen des gleichnamigen DFG-Schwerpunktprogramms bezeichnet und zum andern konzeptionell und technisch nicht eindeutig von verwandten, auf SaSo-Systeme ausgerichteten Forschungsaktivitäten abgrenzbar ist (vgl. Bernard 2008, Pissarskoi 2008).²² Von daher dürften sich Chancen und Risiken von OC zwar in manchen Facetten, nicht jedoch strukturell von denjenigen smarter (selbstorganisierender) adaptiver Systeme unterscheiden.²³

„Da es sich bei Organic Computing zunächst um Paradigmen und abstrakte Konzepte handelt, ist die Menge der möglichen Anwendungen für Organic Computing denkbar vielfältig.“ (Bernard 2008:9) Anwendungen werden etwa in den folgenden Bereichen angestrebt (vgl. Gesellschaft für Informatik et al. 2008, Nafz et al. 2006, Petschow et al. 2007): Automobiltechnik, Verkehrstechnik,

²¹ Hierbei soll das System seine Entwickler in der Generierung der passenden Operationen und Sprache seiner Programmierung unterstützen: “We intend that the system will help the designers create the language, by operating for a while, so that the system can know enough to make some good choices, and that it can present enough information to the designers so that they can make other good choices.

In the most general terms, we can describe the operation of such a system as follows:

- system observes external and internal behavior
 - developers must provide initial languages
 - system use languages to record these observations
 - system assesses the adequacy of its own languages
 - system changes the languages or invents new ones as necessary
 - the process cycles back to the system’s use of languages
- system creates models
 - developers must provide initial notations
 - system uses notations to record these models
 - system assesses the adequacy of the notations
 - system changes the notations or invents new ones as necessary
 - the process cycles back to the system’s use of notations
- system inherits or creates goals
 - developers must provide initial goals
 - system reasons about the models in pursuit of its goals
 - system assesses the adequacy and consistency of the goals
 - system changes or replaces the goals as necessary, according to the results of negotiations with developers
the process cycles back to the system’s use of goals.” (Bellman et al. 2008:67)

²² „Während die Ziele des Organic Computing stark auf die Untersuchung selbstorganisierender und insbesondere eingebetteter oder ubiquitärer Systeme ausgerichtet sind, steht beim Autonomic Computing mehr das Selbstmanagement der Serversysteme und großer verteilter Rechnersysteme im Vordergrund.“ (Gesellschaft für Informatik et al. 2008:32)

²³ „Jedenfalls ist es nicht augenscheinlich und nicht leicht herauszuarbeiten, welche Chancen und welche Risiken auf allgemeinerer Ebene OC-spezifisch sind bzw. im Prinzip die gleichen wie a) andere analoge konkurrierende IT-Systeme (autonomous computing und ähnliche) und b) andere smarte IT-Systeme wie ambient intelligence oder ubiquitous computing.“ (Conrad 2008a:4)

Fabrikautomatisierung, Mechatronik, Gebäudetechnik, Sicherheitstechnik, adaptive Energieversorgung, Sensornetzwerke, Smart-Office, Roboteranwendungen, Chipdesign, biologische Systeme und medizinische Ausstattung, Bildverarbeitung und Computer-Sehen.

Allerdings ist OC noch in der Forschungs- und Entwicklungsphase. Zur Zeit existieren „noch keine fertigen, marktreifen Produkte nach Organic Computing-Kriterien.“ (Bernard 2008:9) “Organic computing may or may not be able to get off the ground in direct competition with solidly established software applications such as operating systems or enterprise software, and it may have to prove itself in novel fields that are too expensive to develop in classical programming style.”²⁴ (Malsburg 2008:23)

Mit Blick auf die Autonomie von IT-Architekturen kennzeichnen Heiß et al. (2008:45) OC zusammenfassend folgendermaßen: „Die OC-Initiative verfolgt drei wesentliche Ziele:

- Systeme mit lebensähnlichen Eigenschaften erschaffen. Zu den angestrebten Eigenschaften zählen unter anderem Autonomie, Adaptivität, Lernfähigkeit, Skalierbarkeit, Fehlertoleranz sowie die Selbst-X-Eigenschaften.
- Vorgehensweisen aus der belebten Natur auf IT-Systeme übertragen. Beispiele hierfür sind Redundanz, Observer/Controller-Muster, Schwarmverhalten, Immunabwehr und pheromonbasierte Algorithmen;
- Hinwendung auf die Wünsche und Belange des Benutzers, um die Benutzbarkeit zu steigern sowie ein Kontextbewusstsein zu schaffen.“²⁵

Für das auf Observer/Controller-Architekturen²⁶ abhebende technische Design von OC halten Müller-Schloer/Sick (2008:97) fest: “The Observer/Controller/Productive-system loop constitutes a basic building block of OC systems. This building block has all four characteristic properties of a holon ..., i.e., it is (1) a self-contained autonomous unit, (2) communicates with other holons on the same level of order (3) to build higher level ‘organs’, which in turn have the properties of a holon. Their constituent holons can stop cooperating which (4) leads to their decay.“ Dabei gilt: “The goal of OC is to build systems that perform their tasks by using (controlled) self-organization. However, this is independent of using centralized or decentralized observer/controller architectures, since the elements of the system work autonomously and the controller affects some local control parameters only and does not control single elements in detail.” (Müller-Schloer/Sick 2008:89)

²⁴ Vision is such a field. Four decades of frustration made it clear that replicating vision on the computer is a very complicated thing, both in terms of processes and data. Mankind will never muster the resources to generate it while programming line-by-line. Full-fledged computer vision will only be realized with the help of organic growth, learning and instruction, that is, by organic computing.” (Malsburg 2008:23)

²⁵ „Nicht direkt im Fokus von Organic Computing stehen DNA-Computer, genetische Algorithmen und künstliche Intelligenz. Stattdessen wird vor allem die Selbstorganisation in den Vordergrund gerückt. Das Verbesserungspotenzial selbstorganisierender Systeme wird hierbei insbesondere bei Handhabung komplexer Situationen und bei der Energieeinsparung gesehen. Gleichzeitig stellt diese Vision klar, dass Sicherheitskonzepte erforderlich sind, die zu einem vertrauenswürdigen Computersystem führen. Insgesamt ist Organic Computing daher eher im Bereich Pervasive Computing und Ubiquitous Computing angesiedelt und nicht wie die Autonomic Computing Initiative im Bereich der Unternehmensanwendungen.“ (Heiß et al. 2008:45)

²⁶ Diese werden in Kapitel 2.4 erläutert.

Bei allen Unterschieden im Detail und ihren Anwendungen zeichnen sich OC-Vorhaben, wie sie etwa im DFG-Schwerpunktprogramm „Organic Computing“ verfolgt werden, durch gemeinsame Fragestellungen und Zielsetzungen aus wie die Organisation großer Systeme, die Realisierung von Selbst-X-Eigenschaften, kontrollierte Selbstorganisation, kontrollierte Emergenz. Es geht nicht um bzw. um mehr als die Übertragung biologischer Regulierungsmuster²⁷ oder bestimmte (zukünftige) Computer-Techniken wie Quanten- oder DNA-Computing, sondern um die (gelingende) Anstrengung, Systeme, die sich an verändernde Umwelten selbstorganisiert anpassen und sich dabei unvorhergesehen verhalten können, in ihrer technischen Realisierung soweit unter Kontrolle zu behalten, dass nichts Ungewolltes passiert.²⁸ OC betrifft – anders als das auf große Serversysteme gerichtete AC – zum einen grundsätzlich beliebige Anwendungsbereiche, indem es in die jeweiligen technischen Systeme eingebettet ist, und zum anderen zugleich die Ebenen der Modellierung, der Software, des Betriebssystems und (im Falle der Rekonfiguration) auch der Hardware.

Von daher stellt OC ein zielorientiertes, vielfältige Anwendungen erlaubendes und anstrebendes Konzept dar, das ein die verschiedenen Ebenen von Computing (wie mobile, pervasive, autonomous computing) umfassendes (visionäres) Leitbild mit auf technische Umsetzung orientierten Ziel(vorstellung)en (wie Selbstorganisation, kontrollierte Emergenz, Observer/Controller-Architektur) verknüpft und damit das allgemeine Konzept der SaSo-Systeme ein wenig substantiiert und auf seine technische Umsetzung ausrichtet. Analytisch-kategorial gehört OC somit zur Klasse der SaSo-Systeme, die tendenziell als eigener, abgrenzbarer Computing-Ansatz eingestuft werden kann. OC kann daher in seinen konkreten operativen Formen als eigenständiger Typus eines smarten IT-Systems betrachtet werden, jedoch nicht als ein kategorial eigenständiges Computing-System.²⁹

Zusammenfassend geht es mit Schmeck (2009:4) bei OC um

- “collections of intelligent (embedded) systems (scenarios like smart house, car, office, factory, shop, healthcare,ubiquitous, pervasive computing),
- potentially unlimited networks (large number, mobility),

²⁷ “There are two driving differences between the needs of biological systems in general and OC systems. The first is a result of the essentially ‘alien’ nature of the OC system... Biological systems are not only somewhat continuous with their environment, but are also part of a complete ecosystem; that is, in collaboration and competition with other systems, all of which are linked to and part of a larger whole. In contrast, the very concept of engineering a system leads it to be disconnected and ‘alien’; it is developed by us, usually with materials very different from those in its operational environment, doing functions that may have little to do with those of any other system in the operational environment... Thus, unlike a biological organism, an OC system will always retain a special type of differentiation from its surroundings in that it is deployed into an operational context to achieve purposes other than its own survival... But in addition to creating analogies to existing biological processes, we also discussed some unique challenges for OC systems; the greatest of which is that these systems must always be accessible, monitorable and coordinated with our goals and intentions for the systems. This implied to us that OC systems require sophisticated instrumentation, self-monitoring and reflection capabilities as well as the ability to represent their states to us, communicate and negotiate with us, and hence share the development of its control and organization with us.” (Bellman et al. 2008:43ff)

²⁸ Analoge einfachere Beispiele sind der Autopilot in Flugzeugen oder der Tempomat in Autos, in deren Funktionsablauf sehr wohl eingegriffen werden kann, was bei OC schwieriger und mit tendenziell gravierenderen Folgen verbunden ist.

²⁹ Bildhaft gesprochen steht OC zu Konzepten wie AC, PC oder Aml eher oblique als orthogonal, da es mit ihnen kompatibel ist, teils deren Elemente enthält und in ihnen im Prinzip auch genutzt werden kann, weshalb sie zumeist als einander überlappende Konzepte mit fließenden Übergängen angesehen werden. “It is no surprise that Organic Computing is not monolithic and clearly separated from other fields but has significant overlap with many of them.” (Würtz 2008:5)

- spontaneous local interaction, leading to unexpected global behavior (emergent phenomena as a result of self-organisation),
- robust services in dynamically changing environments (e.g. mobile communication).
- flexible behaviour as a reaction to varying external constraints (e.g. traffic light control),
- design, management and acceptance problems with increasingly complex systems”, insbesondere hinsichtlich ihrer Kontrollierbarkeit und Vertrauenswürdigkeit.

Deshalb “we have to come up with good ideas for designing, managing, and controlling unlimited, dynamical networks of intelligent devices, utilising the available technology for the utmost benefit to humans.”

2.4 Klärung zentraler Begriffe wie Autonomie, Selbstorganisation, Emergenz

Wie beschrieben zielt Organic Computing darauf ab, durch geeignete technische Arrangements die wachsende Komplexität uns umgebender Systeme (vgl. Richter/Rost 2004) durch Mechanismen der Selbstorganisation zu beherrschen und jene dabei anwendungs- und nutzerorientiert zu gestalten. Die für OC-Systeme relevanten (teils aus dem Verständnis biologischer Systeme entwickelten) Begriffe, Konzepte und Problemlagen sind insbesondere System, Eigenschaft, Modell und Modellierung, Architekturmuster, Observer/Controller-Architekturen, Komplexität, Autonomie, Selbstorganisation, Selbst-X-Eigenschaften, Emergenz, Vertrauen, Verlässlichkeit und Sicherheit, Steuerbarkeit, autonomieinduzierte Schwachstellen und Maßnahmen zur Schwachstellenbekämpfung. Diese teils bereits mehrfach genutzten und für die Analyse der Struktur, Entwicklung, Perspektiven und Gestaltungsansätze von OC-Systemen oder allgemeiner von SaSo-Systemen zentralen Begriffe werden deshalb nachfolgend in dieser Reihenfolge vor allem mithilfe diesbezüglicher Zitate aus der Fachliteratur, insbesondere der Studie von Heiß et al. (2008) genauer bestimmt und definiert³⁰, um so zum einen Bandbreiten und Ausrichtung der Konstruktion von sowie der Schwachstellenbekämpfung in OC-Systemen auf technischer Ebene aufzuzeigen und zum anderen die für die (zukünftige) Einführung und Nutzung von OC relevante Struktur von OC-Systemen deutlich zu machen, selbst wenn in der anschließenden Darlegung von Geschichte, Entwicklung und Marktperspektiven, Chancen und Risiken, rechtlichen Problemstellungen und politischen Gestaltungsmöglichkeiten von OC deren Auswirkungen auf ebendiese Strukturmerkmale konkreter OC-Systeme nicht näher ausgeführt werden (können).

System, Eigenschaft, Modell

„Ein *System* ist eine Menge von Elementen, die in einer bestimmten Umgebung oder in einem bestimmten Kontext als Einheit aufgefasst werden. Die Elemente dieser Einheit interagieren, stehen miteinander in Beziehung und können ihrerseits wiederum als System aufgefasst werden. Diese

³⁰ Die Begriffsbestimmung und -differenzierung erfolgt überwiegend mithilfe entsprechender Zitate, weil sie dadurch als besonders präzise, prägnant und fachlich abgesichert gelten kann.

Definition macht deutlich, dass ein System das Ergebnis einer Interpretation ist und nicht per se existiert.“³¹ (Heiß et al. 2008:7)

„Eine *Eigenschaft* ist das, was eine Entität (im hier interessierendem Fall: ein System) von einer anderen Entität (oder von sich selbst zu einem anderen Zeitpunkt) unterscheidbar machen kann.“ (Heiß et al. 2008:8)

Mahr (2007) stellt unterschiedliche Ansätze des Modellbegriffs vor und diskutiert, woran ein Modell als ein solches erkannt werden kann. Für Systeme der Informatik passt der Ansatz von Stachowiak (1973), der ein Modell anhand von drei Merkmalen beschreibt:

- 1) „Abbildungsmerkmal. Modelle sind stets Abbildungen, Repräsentationen natürlicher oder künstlicher Originale, die selbst wieder Modelle sein können.
- 2) Verkürzungsmerkmal. Modelle erfassen im Allgemeinen nicht alle Attribute des durch sie repräsentierten Originals, sondern nur solche, die den jeweiligen Modellerschaffern und/oder Modellbenutzern relevant scheinen.
- 3) Pragmatisches Merkmal. Modelle sind ihren Originalen nicht per se eindeutig zugeordnet. Sie erfüllen ihre Ersetzungsfunktion:
 - für bestimmte – erkennende und/oder handelnde modellbenutzende – Subjekte;
 - innerhalb bestimmter Zeitintervalle und
 - unter Einschränkung auf bestimmte gedankliche oder tatsächliche Operationen.“³² (Heiß et al. 2008:12)

„Prinzipiell gibt es zwei Klassen von *Grundeigenschaften*, die ein Modell abbilden kann: die Struktur eines Systems und das Verhalten eines Systems. Jede andere Eigenschaft lässt sich auf eine dieser beiden Kategorien reduzieren. Verhalten beschreibt dabei die Aktionen eines Systems, die entweder autonom oder eine Reaktion auf Interaktionen (mit) der Umwelt sind. Struktur beschreibt dagegen die Verknüpfungen zwischen Systemelementen. Eine Modellierungstechnik kann beide Elemente in unterschiedlicher Gewichtung enthalten.“ (Heiß et al. 2008:103)

Modellierung – einschließlich Modellprüfung (vgl. Clarke et al. 1999) – bezeichnet dann den Vorgang, „der zur Erschaffung eines Modells führt. Bestandteil dieses Vorgangs ist eine Analyse, um beispielsweise relevante und irrelevante Eigenschaften zu bestimmen, die im Modell hervorgehoben bzw. vernachlässigt werden sollen.“ (Heiß et al. 2008:12)

³¹ „Aufgrund ihres rekursiven Charakters können des Weiteren die Begriffe System und Element weitgehend synonym verwendet werden. Aus Sicht des Nutzers gibt es jedoch einen Unterschied: Ein [technisches] System hat einen bestimmten Zweck bzw. bietet dem Nutzer eine bestimmte Funktion an. Dagegen ist es die wichtigste Funktion von Elementen, dass sie zu einem System zusammengesetzt werden können.“ (Heiß et al. 2008:7)

³² Modelle können sowohl als Abbild von existierenden Systemen geschaffen werden als auch als Vorbild für neu zu erstellende Systeme dienen.

Architekturmuster und Architekturen

Bei der Betrachtung von *Architekturmustern* und *Architekturen*³³ sowie der Analyse von Eigenschaften werden je nach Intention des Entwicklers und/oder des Betrachters verschiedene Ebenen der Abstraktion und unterschiedliche Zeitpunkte in den Mittelpunkt gestellt. Deshalb lassen sich Architekturmuster nach ihrem jeweiligen Skalenwert in Bezug auf grundlegende Eigenschaften einordnen. Mit Blick auf die Förderung von – für OC-Systeme zentral – Autonomie sind hier zu nennen (Heiß et al. 2008:60ff):

Homogenität: Mit zunehmender Homogenität ist mit abnehmender Spezialisierung (und damit zunehmender grundsätzlicher Austauschbarkeit) der Komponenten zu rechnen, so dass damit Autonomie begünstigt wird.

Synchronität: Je loser die Kopplung ist, desto schärfer sind die Grenzen der Teile und desto stärker wird folglich der Informationsgradient, was Autonomie fördert.

*Bindung*³⁴: Späte Bindungen führen in ein System zusätzlichen Freiheiten ein: Die Menge der möglichen Interaktionspartner wächst, so dass einerseits Komponenten Interaktionspartner werden können, die zur Entwurfszeit noch gar nicht bekannt waren, andererseits auch im Falle der Bindung zur Laufzeit eventuell sogar verschiedene Interaktionspartner für die gleiche Art von Interaktion innerhalb einer Anwendungsinstanz genutzt werden können. Solche zusätzlichen Freiheiten (begünstigen) ein autonomes Verhalten.

Koordination: Eines der Ziele autonomer Systeme liegt in der Selbststabilisierung (Selbstheilung), was durch das Vorhandensein eines *Single Point of Failure* gefährdet ist. Somit sind dezentral koordinierte Steuerungen für autonome Systeme besser geeignet.

Interaktion: Die Teile eines Systems können auf unterschiedliche Weise miteinander interagieren, sodass sich in Abhängigkeit von der Angabe des Interaktionspartners und des Informationsflusses vier Interaktionsmuster unterscheiden lassen: request/reply, anonymous request/reply, callback, ereignisbasiert. Hierbei erlaubt die ereignisbasierte Interaktion eine dynamische Anpassung der in eine Interaktion involvierten Komponenten zur Laufzeit. Sie eignet sich daher für autonome Systeme besonders gut.

Dynamik: Ein autonomes Verhalten, insbesondere Selbstkonfiguration, Selbstorganisation und Emergenz, wird von dynamischem Verhalten begünstigt.

³³ Wie oben bereits angesprochen, abstrahiert ein Architekturmuster von einer Klasse von Architekturen und gibt mindestens eine wesentliche Charakteristik der betreffenden Architekturen wieder, während eine Architektur Regeln bezüglich der Struktur eines Systems und den Zusammenhängen zwischen seinen Elementen definiert.

³⁴ Die Eigenschaft der Bindung bezieht sich auf das Auffinden der entsprechenden Interaktionspartner.

Abbildung 2.1 ordnet in einer stark vereinfachten Illustration verschiedene Architekturmuster sowohl zeitlich als auch hinsichtlich ihrer Unterstützung von Autonomie ein (vgl. Heiß et al. 2008).

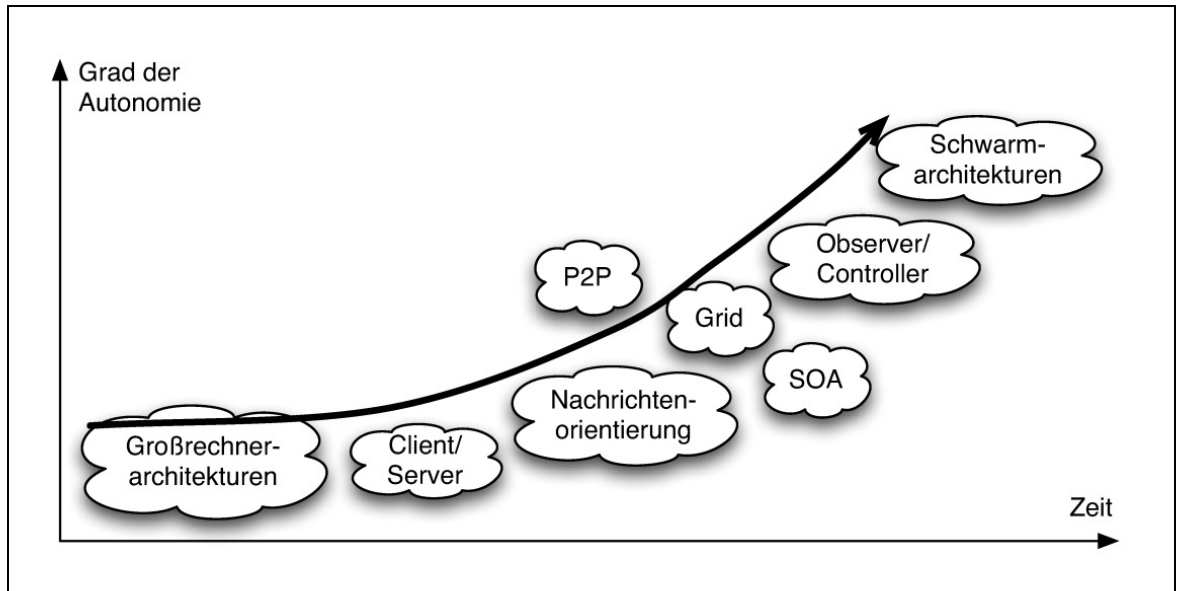


Abbildung 2.1: Entwicklung der Autonomie über die Zeit am Beispiel ausgewählter Architekturmuster

Quelle: Heiß et al. 2008:100

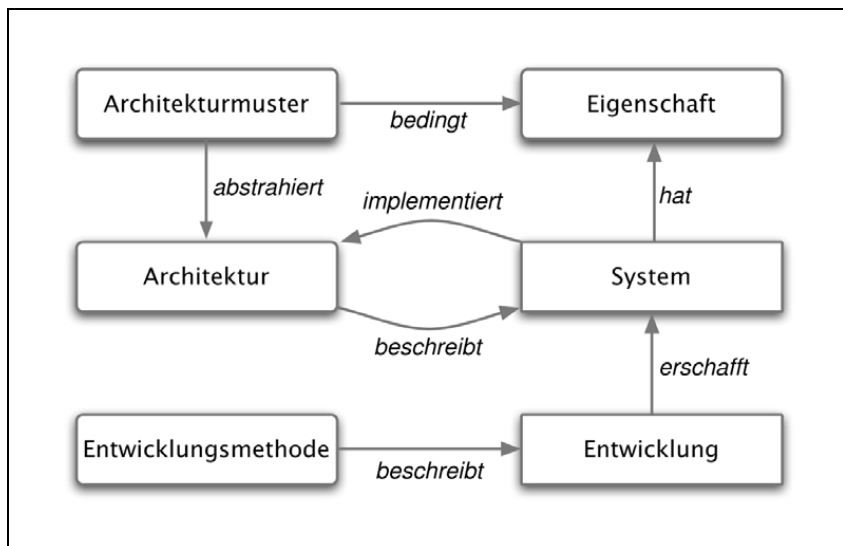


Abbildung 2.2: Konzeptionelles Modell der fundamentalen Begriffe

Quelle: Heiß et al. 2008:54

Zwischen diesen eingeführten Begriffen bestehen im Übrigen folgende Zusammenhänge: „(1) Ein System implementiert eine Architektur. (2) Eine Architektur folgt einem oder auch mehreren Architekturmustern. (3) Ein Architekturmuster ermöglicht oder verhindert bzw. verstärkt oder vermindert bestimmte Eigenschaften des Systems.“ (Heiß et al. 2008:11) Darauf basierend setzt das in Abbildung 2.2 wiedergegebene konzeptionelle Modell die relevanten Konzepte in einen gemeinsamen Zusammenhang, wobei Pfeile die Richtung einer Relation zwischen zwei Konzepten markieren und die Bedeutung einer Relation durch dessen Bezeichnung gegeben wird.

Observer/Controller-Architektur

Die bei OC präferierten *Observer/Controller*-Architekturen, gegebenenfalls durch die Integration modellgetriebener Architektur erweitert (mit dem Ziel der Trennung der Spezifikation der Systemfunktionalität von spezifischen, plattformabhängigen Technologien und Architekturen), zeichnen sich durch eine in der Tendenz zentralisierte Koordination aus, während schwarmbasierte Architekturen mit genetischen (Ameisen-)Algorithmen keinerlei zentrales Element aufweisen und dezentral gesteuert werden (vgl. Heiß et al. 2008:89ff). „Das grundlegende Observer/Controller-Muster ist eine Einheit aus Mess- und Stellort eines Systems und seinem Controller. Diese Einheit stellt auch im Gebiet der Regelungstechnik ein grundlegendes Muster dar.“ (Heiß et al. 2008:89) Mithilfe von Observer/Controller-Architekturen soll die mit autonomer Selbstorganisation zwangsläufig gegebene Möglichkeit unerwünschter emergenter Effekte beherrschbar gemacht werden, indem das selbstorganisierende (Produktiv)System (SuOC: system under observation and control) durch ein darüber liegendes, aus Observer und Controller bestehendes System geregelt wird (vgl. Branke et al. 2006, Cakar et al. 2007). Die Observer/Controller-Architektur beobachtet, analysiert und bewertet bezüglich vorgegebener Zielkriterien in einer Art Regelkreis das Verhalten der zu überwachen- den Systeme. Dies führt zur Auswahl geeigneter Maßnahmen, um das zukünftige Verhalten in der gewünschten Richtung zu beeinflussen. Die Architektur besteht aus einem Netzwerk autonomer Einheiten, ergänzt durch jeweils eine oder mehrere Observer- und Controller-Einheiten. Für den Observer muss eine angemessene Methodik entwickelt werden, um das (globale) Systemverhalten zu beobachten und hinsichtlich des Auftretens von Emergenzeffekten zu analysieren und zu bewerten. Der Controller soll aufgrund der Ergebnisse des Observers entscheiden, in welcher Form das Produktivsystem beeinflusst werden muss, um ein kontrolliertes, selbst organisiertes, globales Verhalten innerhalb der Grenzen und Ziele zu ermöglichen, die von einer externen Einheit (der Umgebung) als Ziel vorgegeben sind. Der Controller soll somit in der Lage sein, sein Verhalten lernend zu verbessern, d.h. insbesondere aufgrund von Erfahrungen bezüglich der Wirkung früherer Aktionen sein Verhalten anzupassen. Dabei können sich Observer/Controller-Architekturen deutlich unterscheiden, je nachdem ob sie zentral, mehrschichtig, hierarchisch oder verteilt aufgebaut sind. Der Entwicklungstrend für OC-Systeme geht in Richtung zunehmender Selbstorganisation und wachsender Variabilität des (Produktions)Systems unter zentraler, dezentraler oder Mehrebenenbeobachtung und -kontrolle. Je nach Systemtyp und -erfordernissen sind daher unterschiedliche Observer/Controller-Architekturen optimal.

Komplexität

„Es gibt in der Informatik keine allgemeine Definition des Begriffs ‚Komplexität‘, aber zahlreiche spezifische Definitionen und Maße. Insgesamt kann aber beobachtet werden, dass ein System als komplexer als ein anderes gilt, wenn in ihm mehr Beziehungen (räumliche, zeitliche, funktionelle etc.) existieren, als im zweiten. Dabei sind Systeme mit vielen Komponenten meist automatisch komplexer, weil bei gleichem Konstruktionsschema zwischen mehreren Elementen auch mehr Beziehungen existieren. Die bekannteste Klasse von Maßen zu Komplexität in der Informatik beschreibt die *Berechnungskomplexität*, die den algorithmischen Aufwand eines Programmes bewert-

tet. Teilweise wird zwischen ‚Kompliziertheit‘ und ‚Komplexität‘ eines Systems unterschieden. In diesem Fall betont Kompliziertheit die Anzahl der Komponenten und deren Beziehungen, während Komplexität zusätzlich die Art der Beziehungen berücksichtigt. So impliziert beispielsweise die Nichtlinearität von Beziehungen häufig, dass kleine Änderungen zu großen und oft unvorhersagbaren Auswirkungen führen können.“³⁵ (Heiß et al. 2008:52) Komplexität ist somit zunächst primär als formale (technische) Größe zu verstehen.

Die Komplexitätsforschung zeichnet sich im Übrigen durch Konzepte und Theorien aus, die auf unterschiedliche Dimensionen von Komplexität fokussieren: (1) Komplexität als *strukturelles*, systemimmanentes Faktum oder als ein *subjektives* Konstrukt des – möglicherweise nicht hinreichend kompetenten – Beobachters, (2) Komplexität als *quantitativ* (unüberschaubar) große Zahl von Komponenten (Kompliziertheit) oder als *Qualität* ihrer Interaktion und der sich daraus ergebenden (nicht-linearen) Eigendynamiken (Komplexität) (vgl. Weyer 2009:8).

Autonomie

„*Autonomie* in der Informatik bezieht sich auf das beobachtbare Verhalten eines Systems. Ob ein System autonom ist, wird also daran festgemacht, ob es seine Funktion autonom – also ohne äußere Kontrolleingriffe – erbringt... Autonomes Verhalten ist eine nichtfunktionale Eigenschaft, die im Zusammenhang zu anderen nicht-funktionalen Eigenschaften steht. Aufgrund dieser Betrachtung kann ein konzeptuelles Netzwerk aufgestellt werden, um diese Begriffe miteinander in Relation zu bringen (siehe Abbildung 2.3)... Autonomes Verhalten an sich kann nicht innerhalb eines isolierten Systems beobachtet werden, da autonomes Verhalten immer an eine Funktion gebunden ist, die autonom erbracht wird, das heißt dieses System in Beziehung zu anderen Systemen setzt. So verhält sich die Autonomie eines Systems bei dieser Betrachtung wie beispielsweise die örtliche Verfügbarkeit: Auch sie stellt keine Funktionalität eines Systems dar und ist auch nicht durch eine Funktion zu repräsentieren. Stattdessen kann Autonomie (wie auch lokale Verfügbarkeit) durch Entwurfsmuster bzw. Architekturmuster realisiert werden... Die Grundidee, Computersysteme mit autonomem Verhalten zu entwickeln, besteht darin, ein System mit Algorithmen und Verfahren derart anzureichern, dass die Einhaltung bestimmter Eigenschaften, ausgedrückt in einer Zielstellung, selbständig verfolgt wird. Das Ziel ist die Schaffung von Systemen, die die notwendigen steuernden Interaktionen mit dem Menschen minimieren.“ (Heiß et al. 2008:42ff)

Dabei gibt es bei Betrachtung existierender autonomer Architekturmuster (insbesondere Observer/Controller- und schwarmbasierte Architekturen) zwei grundsätzliche Kennzeichen von Autonomie:

- *„Informationsgradient“*: Innerhalb eines Systems werden wesentlich größere Mengen an Information verarbeitet, als über die Systemgrenzen hinweg ausgetauscht werden.
- *Emergentes Verhalten*: Das System zeigt Verhaltensweisen, die nicht unmittelbar auf Komponenten- bzw. Subsystemebene angelegt sind.

35 Selbst ein sehr einfaches – und damit eher nicht komplexes – System kann übrigens autonom sein. Und umgekehrt können komplexe Systeme als wenig autonom eingestuft werden, da viele ihrer das Verhalten betreffenden Beziehungen an Steuerinformationen gekoppelt sind. (vgl. Heiß et al. 2008:52f)

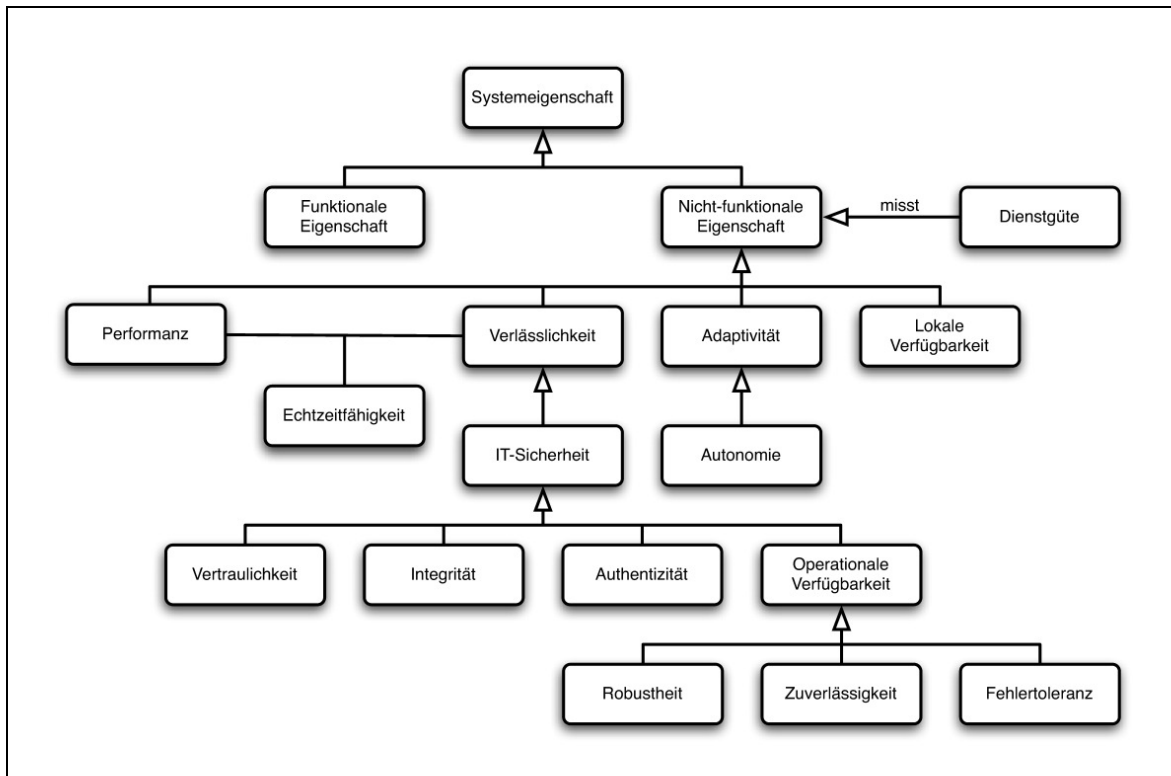


Abbildung 2.3: Taxonomie der Systemeigenschaften

Quelle: Heiß et al. 2008:43

Beide Kennzeichen sind nicht eindeutig – in einem stärkeren oder schwächeren Maß kommen sie praktisch in jedem System vor.“³⁶ (Heiß et al. 2008:49)

„Autonomie kann sich sowohl positiv als auch negativ auf die Verlässlichkeit eines Systems auswirken.

Positive Auswirkungen: Die Erhöhung der Verlässlichkeit ist in der Regel ein Hauptziel beim Entwurf von Systemen mit erhöhter Autonomie. Die Auswirkungen von Störungen sollen besser ohne äußeren Eingriff behandelt werden können. Dadurch kann erreicht werden, dass Fehlerzustände zu keiner oder keiner langfristigen Beeinträchtigung des Systemdienstes führen. Dies wirkt sich positiv auf Metriken wie Zuverlässigkeit oder Verfügbarkeit aus.

Negative Auswirkungen: Autonomie kann sich auch negativ auswirken. Prinzipiell muss hier zwischen zwei Fällen unterschieden werden:

- *Erwünschte Autonomie:* Autonomie führt in der Regel zu einer höheren Komplexität. Dies steigert die Wahrscheinlichkeit, dass im Laufe des Entwurfszyklus Fehler auftreten bzw. auftretende Fehler nicht behoben werden. Während dies ein Problem ist, das allgemein bei Komplexi-

³⁶ Dies stimmt im Übrigen mit der Beobachtung überein, dass Autonomie – wenn auch in unterschiedlicher Ausprägung – prinzipiell in jedem System zu finden ist.

tätserhöhung auftritt (z. B. allgemein bei Einführung von Fehlertoleranzmaßnahmen), gibt es eine Reihe von autonomietypischen Beeinträchtigungen... Allgemein gilt: Jedem Mehr an Autonomie für das System steht ein Weniger an Autonomie für Systemnutzer gegenüber. Je nach potentieller Fähigkeit eines Nutzers, Störungen zu erkennen und korrekt darauf zu reagieren, kann dies zu einer Verringerung der Systemverlässlichkeit (bezüglich einer durch den Nutzer erreichbaren Verlässlichkeit) führen.

- *Unerwünschte Autonomie*: Autonomie kann auch auftreten, wenn dies im Systementwurf nicht explizit vorgesehen ist. Prinzipiell gelten hier auch die evtl. negativen Auswirkungen, die bei erwünschter Autonomie auftreten. Zusätzlich kann – insbesondere durch die mit Autonomie verbundene Verhaltensemergenz – die Korrektheit des Systems leiden. Dabei widerspricht das Systemverhalten unter Umständen nicht der geschriebenen Spezifikation, aber dem intendierten Systemverhalten.“ (Heiß et al. 2008:53)

Die Autonomie eines IT-Systems korreliert typischerweise mit dem Maß seiner Selbstorganisation. Hähner/Müller-Schloer (2009) unterscheiden 5 Autonomiegrade (0-4), denen Selbstorganisations-typen mit folgenden charakteristischen Eigenschaften korrespondieren: Bei vorgegebenen *starr*en Relationen ohne Selbstorganisation hat das System keine Adaptivität und keine externe Kontrolle. *Multimodale* Selbstorganisation geht mit einfachen Zuständen, isolierten Funktionen und einem kleinen Konfigurationsraum einher. Ein *rekonfigurierbarer, parametrisierbarer* Selbstorganisations-typ besitzt einen großen Konfigurationsraum und vernetzte Komponenten. Ein *brokered* System (aus semi-autonomen Elementen) verfügt über aktive Agenten und vermittelt Kooperationen.³⁷ Und *verteilte kooperative* Selbstorganisation ist durch autonome Agenten und fehlende zentrale Kontrolle gekennzeichnet.

Abbildung 2.4 verdeutlicht das dem als nicht-funktionale Eigenschaft skizzierten Autonomiebegriff zugrunde liegende konzeptionelle Modell, dessen Elemente von Heiß et al. (2008:46ff) wie folgt definiert werden.

„*Adaptivität*: Ein System ist adaptiv bezüglich einer Menge von Eingabefunktionen und einer Zielstellung, wenn es in der Lage ist, für diese Eingabefunktionen die Zielstellung zu erfüllen.“³⁸

Selbstmanagement, Autonomie: Ein System ist selbstmanagend, wenn es adaptiv ist, ohne von außen kontrolliert zu werden.³⁹

Selbstkonfiguration: Ein System ist selbstkonfigurierend, wenn es seine Konfiguration (innerhalb gegebener Grenzen) ohne externen Kontrolleingriff anpasst, um seine Adaptivität sicherzustellen.

³⁷ „The broker plays the role of a central matching and assessment service enabling a marketplace mechanism... It monitors the agents, aggregates their states and predicts future demands.“ (Müller-Schloer/Sick 2008:99)

³⁸ Organic Computing-Systeme zeichnen sich durch eine hohe Adaptivität aus. „Bei Informations- und Kommunikationstechnologien und Anwendungssystemen bedeutet Adaptivität u.a. die Möglichkeit der Personalisierung und damit der Orientierung an Aufgaben und Bedürfnissen des Benutzers. Auch die automatische Einstellung auf Netzwerkverbindungen oder Stromquellen fällt unter den Begriff der Adaptivität.“ (Bendel/Hauske 2004)

³⁹ Autonomie und Selbstmanagement sind aus dieser Sicht Synonyme.

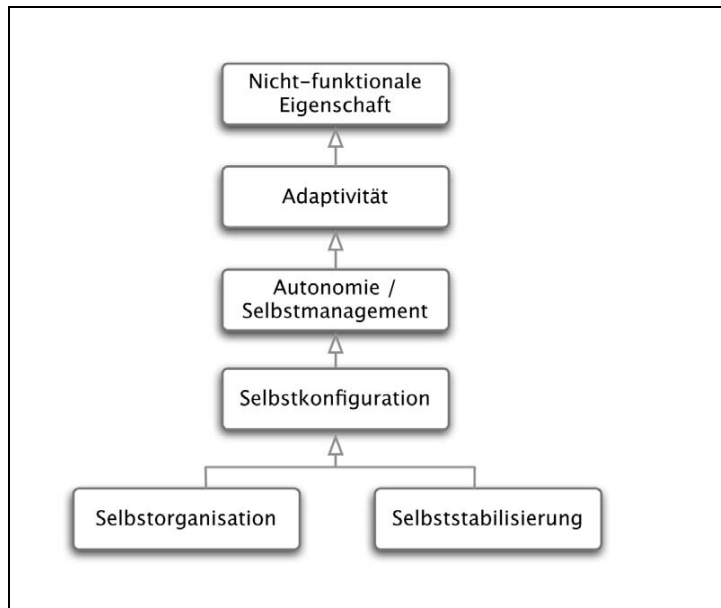


Abbildung 2.4: Konzeptionelles Modell von Autonomie

Quelle: Heiß et al. 2008:48

Selbststabilisierung: Ein System ist selbststabilisierend, wenn es im fehlerfreien Fall (1) ausgehend von einem beliebigen Zustand einen legalen Zustand in beschränkter Zeit erreicht und (2) ausgehend von einem legalen Zustand seinen Zustand in der Menge der legalen Zustände hält.

Selbstorganisation: Ein selbstorganisierendes System ist ein selbstmanagendes System, welches zusätzlich strukturadaptiv ist und eine dezentrale Kontrolle hat.⁴²

Da Autonomie keine auf Komponentenebene zu identifizierende Eigenschaft ist, ist zu untersuchen, ob und wie Autonomie *indirekt* beschrieben werden kann. „Da sich Autonomie explizit auf *Verhalten* bezieht, sind alle Modellierungsansätze, die den Verhaltensaspekt nicht

oder nur schwach beinhalten, nur bedingt für die Beschreibung von Autonomie geeignet.

Möglicherweise können allerdings auch in Strukturbeschreibungen Anzeichen für Autonomie gefunden werden... Für das Autonomieindiz ‚emergentes Verhalten‘ ist (noch mehr als bei ‚Informationsgradient‘) eine Ausprägung des Verhaltensaspektes notwendig. Diese ist jedoch nicht hinreichend: Vielmehr muss der Modellierungsansatz die Möglichkeit des Wechsels der Beschreibungsebene geben, um emergente Eigenschaften überhaupt *ausdrücken* zu können.“ (Heiß et al. 2008:147ff) Die gängigen Modelle insbesondere des Softwareengineering sind eher eingeschränkt zur Modellierung von Autonomie geeignet. „Dies ist nicht verwunderlich, da es in der Informatik bisher meist kein unmittelbares Ziel war, Autonomie analytisch zu finden oder konstruktiv herzustellen. Es empfiehlt sich daher, auch Modellierungsansätze zu betrachten, die in der Informatik

42 Ein System ist hierbei strukturadaptiv, wenn es adaptiv ist, weil es seine Struktur ändert. Das heißt, wenn es seine Struktur nicht ändern würde, so wäre es nicht adaptiv.“ (Heiß et al. 2008:48)

eher am Rand stehen oder vollständig aus anderen Bereichen kommen. Solche Modellierungssätze sollten folgende Eigenschaften aufweisen:

- Sie sollten auf Systeme der Informatik anwendbar sein.
- Sie sollten verhaltensorientiert sein.
- Die Autonomiemerkmale sollten beschreibbar sein.
- Innerhalb des Ansatzes sollten Übergänge von Abstraktionen möglich sein.“ (Heiß et al. 2008:153f)

Diese Merkmale sehen Heiß et al. (2008) am ehesten in der Systemtheorie gewährleistet.⁴³

Selbstorganisation

Selbstorganisation gilt als grundlegende Eigenschaft von OC-Systemen, die ihnen ein adaptives und kontextsensitives Verhalten erlaubt.⁴⁴ Auf der Grundlage einer sauberen und klärenden Darstellung des Konzepts der *controlled self-organisation* in Organic Computing und verschiedener konzeptioneller Fassungen der Selbstorganisation technischer Systeme machen Cakar et al. (2007) deutlich, dass Selbstorganisation von der vom Beobachter gewählten Systemgrenze abhängt, insbesondere ob der observer/controller loop als ihm zugehörig oder extern definiert wird. Der Grad der Selbstorganisation hängt ab vom Ausmaß erforderlicher externer Kontrolle, um die Struktur und/oder das Verhalten eines Systems⁴⁵ zu verändern („ultimately zero for a completely self-organising or autonomous system“).⁴⁶ Das aus Selbstorganisation resultierende Selbstmanagement und Autonomie geht mehr oder minder (gezielt) einher mit den erwarteten und angestrebten *Selbst-X-Eigenschaften*⁴⁷ wie Selbstkonfiguration, Selbstoptimierung, Selbstheilung, Selbstschutz und Selbsterklärung.⁴⁸

Durch selbsttätige Rekonfiguration kann auch das Ziel der *Selbstoptimierung*, des eigenständigen Findens eines optimalen Systemzustands, erreicht werden.

⁴³ Auch in der Soziologie gibt es den Begriff der Systemtheorie, z. B. bei Luhmann und Parsons. Allerdings unterliegen hier die Begrifflichkeiten einer in vielen Geisteswissenschaften anzutreffenden Unschärfe, so dass ein Vergleich mit den natur- und ingenieurwissenschaftlichen Varianten der Systemtheorie nur schwer möglich ist und nur bedingt sinnvoll ist.

⁴⁴ Allgemein versteht man unter Selbstorganisation „ das Auftreten systemübergreifender („langreichweitiger“) zusammenhängender, in irgendeinem Sinne geordneter („kohärenter“) Strukturen in einem Ensemble vieler lokal interagierender Elemente. Häufig treten die kohärenten Strukturen spontan auf, sobald ein kritischer Wert eines Kontrollparameters überschritten wird. Man bezeichnet Selbstorganisation daher auch als Phasenübergang hin zu höherer räumlicher Ordnung.“ (Hütt 2006:93)

⁴⁵ Struktur und Verhalten eines Systems werden als Konfiguration bezeichnet.

⁴⁶ Dabei muss es ein Maß für die Qualität der Selbstorganisation geben, und die Zusatzkosten selbstorganisierender Systeme sind gegenüber ihrem Nutzen abzuwägen.

⁴⁷ „Dabei steht das X als Platzhalter für unterschiedliche Funktionen wie Konfigurations- oder Schutzmaßnahmen, die ein Computersystem selbstständig durchführen soll. Durch diese Vorgehensweise soll die mit dem Betrieb des Systems verbundene Komplexität reduziert werden.“ (Heiß et al. 2008:2)

⁴⁸ Durch Selbstkonfiguration und Selbstoptimierungsstrategien sind OC-Systeme wesentlich flexibler als viele herkömmliche Systeme. Neue Knoten können zur Laufzeit des Systems integriert werden und die Selbstheilung ermöglicht die Weiterarbeit trotz ausfallender Knoten, so dass das System sehr dynamisch ist.

Selbsteilung bezeichnet die Fähigkeit eines Systems, sich selbständig ohne Eingriffe von außerhalb des Systems von Fehlern und (Teil-)Ausfällen zu erholen. Störungen werden sowohl selbst entdeckt als auch selbst beseitigt.

Selbstschutz ist die Selbstkonfiguration mit dem Ziel der Sicherstellung von Sicherheitseigenschaften und bezeichnet die Fähigkeit eines Systems, Angriffen von außen entgegenzutreten und deren interne Auswirkungen vermeiden oder begrenzen zu können.

Selbsterklärung meint die Fähigkeit eines Systems, dem Nutzer sein Verhalten und die komplexe dynamische Organisation eines selbstorganisierenden adaptiven Systems von selbst (leicht und rasch) verständlich machen zu können⁴⁹; denn ein solches stellt eine besondere Herausforderung an die Nutzerschnittstelle dar. Interessanterweise ist Selbsterklärung von den Selbst-X-Eigenschaften bislang am wenigsten untersucht und gewährleistet, obgleich sie maßgeblich für die Gewährleistung des Nutzervertrauens ist.

Selbststeuerung kann ebenfalls als Form der Selbstorganisation aufgefasst werden, da auch hier ebenso wie in der Selbstkonfiguration dezentral autonome Entscheidungen die Funktionsweise des Gesamtsystems definieren. „Kern der Idee der *Selbststeuerung* ist, im Unterschied zu bestehenden zentral und hierarchisch ausgerichteten Planungs- und Steuerungsansätzen, dezentrale und heterarchische Steuerungsmethoden zu entwickeln, die es erlauben, zeitnah und effizienter auf Veränderungen im komplexen Umfeld zu reagieren.“ (Windt 2006:271) Kennzeichnende Merkmale von Selbststeuerung sind nach Windt (2006) Fähigkeit zur autonomen Entscheidung, autonomes zielorientiertes Verhalten, Fähigkeit zur Messung, Rückkopplung und Bewertung von Ereignissen, Interaktionsfähigkeit, Nichtdeterminismus (emergentes Verhalten) und Heterarchie.⁵⁰

Emergenz

Emergenz bezeichnet, vereinfacht ausgedrückt, das Auftauchen von Systemzuständen, die nicht durch die Eigenschaften der beteiligten Systemelemente erklärt werden können (vgl. Stein 2004). Der Begriff der *Emergenz* ist jedoch stark umstritten (vgl. Werner 2007). „Dies liegt vor allem daran, dass es sich bei Emergenz einerseits um ein sehr altes Konzept handelt, dass aber andererseits dieses Konzept nicht eindeutig definiert und z. T. auch nicht vollständig durchdrungen scheint. Hinzu kommt, dass der Emergenz-Begriff in einer Vielzahl von Wissenschaftsbereichen vorkommt, von der Soziologie über die Biologie bis eben in die Informatik.“ (Heiß et al. 2008:50) Werden von Bedau (1997) lediglich *starke* und *schwache* Emergenz unterschieden, gibt es bei Bar-Yam (2004) bereits fünf und bei Fromm (2005a) sieben verschiedene Arten der Emergenz. Einen guten Überblick über verschiedene Ansätze zum Emergenz-Begriff in Philosophie und Systemdesign geben Johnson (2001) und Johnson (2005).⁵¹ Somit ist bei der Nutzung des Emergenzkonzepts Vorsicht

⁴⁹ So muss ein OC-System dem Nutzer beispielsweise (ausfallbedingte) Umkonfigurationen erklären.

⁵⁰ Aus ingenieurwissenschaftlicher Sicht ergänzt der Begriff der Selbststeuerung das (transdisziplinäre) Verständnis von Selbstorganisation, wobei sich kaum signifikante Unterschiede identifizieren lassen. Am Beispiel typischer Strukturmerkmale (wie dezentrale Entscheidungsfindung, Emergenz, Skalierbarkeit) und Fähigkeiten (wie Kooperationsfähigkeit, Interaktionsfähigkeit, Selbstveränderungsfähigkeit) oder bezogen auf System- versus Objektbezug wird deutlich, „dass bei dem Ansatz der Selbstorganisation die Merkmale auf der Management- und Organisationsebene stärker ausgeprägt sind, hingegen für Selbststeuerung die Merkmale für das Ausführungssystem relevanter sind... Selbststeuerung ist eher am einzelnen Objekt orientiert, während der Ansatz der Selbstorganisation eher das System als Ganzes betrachtet.“ (Windt 2006:296)

⁵¹ Die Zeitschrift „Emergence“ gibt regelmäßig neue Forschungsergebnisse im Bereich der Emergenz heraus.

geboten. Solange sich Emergenz im Effekt von einer stets auf der Mikroebene nicht darzustellenden Systemeigenschaft nicht grundsätzlich unterscheidet, sollte man von ihr nicht sprechen und ist sie kein Argument, dass es sich bei Emergenz um nicht auf der Mikroebene der Systemelemente und ihrer Wechselwirkungen kausal erzeugte und beschreibbare Phänomene handelt (vgl. Stephan 1999).

Müller-Schloer/Sick (2008) thematisieren die für OC erforderliche gesteuerte Emergenz und Selbstorganisation und resümieren: "Although the concepts of self-organization and emergence have been subject to extensive investigations and discussions for more than 100 years, soon it became clear that we lack a quantitative assessment of these concepts as a basis for an implementation in technical systems. The main questions to be answered in this context are: Can we define emergence and self-organization (or sub-concepts thereof) compatible with a quantitative, experimental, and objectifiable method as required in natural science? Can we control self-organization and emergence without forcing their meaning? Are there generic architectures generally applicable to technical systems serving this purpose?... We have to investigate how emergence and self-organization can be fostered or even designed in a technical system while, at the same time, they are kept under control. We want to allow a maximum of 'freedom' and 'creativity' of the system itself, but only within a certain, well-defined area. For this purpose we have to define architectural superstructures that are able to keep emergent systems under control and guide them towards the desired objectives."⁵² (Müller-Schloer/Sick 2008:81f)

"In philosophy of mind, the emergent behavior of more or less complex 'systems' (being either natural, supernatural, or artificial) has been investigated for more than a hundred years and definitions of 'weak emergentism' and 'strong emergentism', for instance, have been provided (see Stephan 2006 for a comprehensive review). Weak emergentism is based on the three theses of (1) physical monism, (2) systemic (collective) properties, and (3) synchronous determinism. From a viewpoint of technical (i.e., artificial) systems, only the thesis of systemic (collective) properties is relevant. Basically, it says: 'Emergent properties are collective (systemic), i.e., the system as a whole has this property but single components do not have properties of this type.'... From the viewpoint of OC, weak emergence is certainly a necessary pre-condition, but not a sufficient one. There are many OC systems that are emergent in a weak sense but their emergent properties are not interesting. A notion of emergence that adds very stringent requirements to weak emergence is strong emergence. Strong emergentism is based on the thesis of irreducibility that addresses the question why a system has a certain property. Basically, it says: 'The macro-behavior of a system can in principle not be explained knowing the micro-behavior of components, their interaction rules, etc.'... Altogether, from the viewpoint of OC, historical, philosophical definitions of emergence are either too weak or too strong. The former means that too many systems are termed emergent, the latter implies that no artificial (technical) systems are emergent. We need a technology-oriented notion of emergence (more than weak emergence) possibly depending on the type of OC systems we investigate and the type of questions we ask. In this sense, a system may be regarded as being emergent concerning one (objective) aspect and being non-emergent with respect to another."⁵³ (Müller-Schloer/Sick 83f)

⁵² Ausführlich befassen sich manche Beiträge in Vlec et al. (2006) mit dem Zusammenwirken von Selbstorganisation, Komplexität und Emergenz.

⁵³ Intelligenz als emergentes Phänomen wird in Hillis (1988) diskutiert.

„In contrast to Stephan’s cause-oriented approach, Fromm sees emergence from a largely modeling-oriented viewpoint (focusing on multi-agent systems; cf. Fromm 2005a, 2005b). The following – somehow recursive – definition is used as a starting point: ‘A property of a system is emergent, if it is not a property of any fundamental element, and emergence is the appearance of emergent properties and structures on a higher level of organization or complexity.’ The four ordered types or classes of emergence are nominal, weak, multiple, and strong emergence (where ‘weak’ and ‘strong’ are not equivalent to the corresponding terms used in philosophy of mind!). The four classes differ mainly in the type of the system (e.g., closed with passive components, open with active or multiple levels, or new levels), the roles of the components (e.g., fixed, flexible, or fluctuating), and the feedback mechanisms between components or levels (e.g., top-down feedback or multiple feedback). In particular the classes of weak and multiple emergence definitely can be found in many OC systems. In the opinion of Gabbai et al. (2005) – who study emergence in the context of multi-agent systems – ‘emergence is a sometimes negative phenomenon found in complex systems, which can also be positively exploited to varying degrees. The full, or ultimate, positive exploitation of emergence is self-organization; a system aligns itself to a problem and is self-sustaining, even when the environment changes.’... While all these cause-oriented, process-oriented, or modeling-oriented concepts are valuable from the OC viewpoint, one important aspect has been neglected until recently: the measurement-oriented view. In our opinion, it is a must to reconceive emergence considering the analysis of OC systems. It must be shown, for example, how the following types of emergence could be quantified: emergence due to interactive complexity (Stephan), multiple emergence (Fromm), or stigmergic dynamic emergence (Abbott). In OC systems, we want to ‘do’ (design or allow) emergence but must, at the same time, keep it under control. That is, the emergent behavior of OC systems must be achieved by a balanced approach where the emergent processes are kept within pre-defined boundaries by certain control mechanisms. However, the other viewpoints have certainly to be considered when appropriate measures are defined, selected, or combined. A measurement-oriented notion of emergence may coexist with most of the existing definitions of emergence (in particular the definitions of ‘weak’ and ‘strong’ emergence used in philosophy of mind). It must be technically realizable and allow to determine a ‘degree’ of emergence. Finally, it must definitely be objective, i.e., independent from the knowledge of the observer or the measurement techniques. We expect that there will be a variety of measures for different emergent phenomena and different system objectives, resulting in a collection of emergence ‘detectors’. For each application we must determine the appropriate attributes that characterize emergence, e.g., measures for order, complexity, information flow, etc.” (Müller-Schloer/Sick 2008:85ff)

Vertrauen

Vertrauen (trust), verstanden als Annahme, dass Entwicklungen einen positiven oder erwarteten Verlauf nehmen, und nach Luhmann (2000) ein Mechanismus zur Reduktion sozialer Komplexität und zudem eine riskante Vorleistung, beschreibt „die Erwartung an Bezugspersonen oder Organisationen, dass deren künftige Handlungen sich im Rahmen von angenommenen Verhaltensmustern, gemeinsamen Werten oder moralischen Vorstellungen bewegen werden. Vertrauen wird durch Glaubwürdigkeit, Verlässlichkeit und Authentizität begründet, wirkt sich in der Gegenwart aus, ist aber auf künftige Ereignisse gerichtet.“ (<http://de.wikipedia.org/wiki/Vertrauen>) Dabei ist die Verwendung des Begriffs in verschiedenen wissenschaftlichen Disziplinen eher unterschiedlich und auch innerhalb einer Disziplin oft umstritten. Man kann ihn – als eine anthropogen bestimmte Größe und bezogen auf technische Systeme – auf eine Menge klar definierbarer Aspekte von Vertrauen zurückführen, die je nach Anwendung unterschiedlich stark ausgeprägt sein können: Funktionalität (functionality), Ausfallsicherheit (safety), Zuverlässigkeit (reliability), Sicherheit (security), Glaubwürdigkeit (credibility) und Benutzerfreundlichkeit (usability) (vgl. Bonabeau et al. 1999, Chu

et al. 1997, EATMP 2003, Eddon/Eddon 1998, Jameson 2003). „Für jeden Aspekt existieren Methoden und Techniken, um ihn für konventionelle (IT-)Systeme zu gewährleisten.“ (André et al. 2009:6) Um ein System als vertrauenswürdig einstufen zu können, sind im Allgemeinen alle aufgeführten Aspekte notwendig. OC-Systeme können und werden nun trotz der durch sie bewirkten Effizienzsteigerung, leichteren Wartbarkeit und größeren Anpassungsfähigkeit in vielen Bereichen nur dann eingesetzt, wenn sie vertrauenswürdig sind. In sicherheitskritischen Anwendungen ist z.B. das Einhalten bestimmter Verhaltensgarantien eine absolut notwendige Voraussetzung, weshalb emergentes Verhalten faktisch nicht toleriert werden kann. Für Anwendungen, die personalisierte Dienstleistungen anbieten, sind dagegen Datenschutz und Integrität von Daten unabdingbar. Derzeit sind die Anwendbarkeit bestehender Methoden zur Gewährleistung von Vertrauenseigenschaften bei OC-Systemen bei praktisch allen Vertrauensaspekten nicht oder nur sehr eingeschränkt gegeben, sodass die Entwicklung von Techniken, „die es erlauben, Systeme so zu konstruieren, dass einerseits die Vorteile von Organic Computing spürbar werden und andererseits parallel dazu Trust gewährleistet werden kann“ (André et al. 2009:3) eine notwendige Herausforderung und Aufgabe für die (kommerziellen) Einsatz von OC darstellt.⁵⁴

Verlässlichkeit

Eine zentrale nicht-funktionale Eigenschaft ist die *Verlässlichkeit* eines Systems. Die Verlässlichkeit eines Systems ist zu sehen in dem begründeten Vertrauen, dass das System genau seine spezifizierte Funktionalität erbringt. In der Informatik deckt dieser Begriff einen Teilbereich der nicht-funktionalen Eigenschaften ab. Mit Blick auf smarte Systeme und OC ist dabei zu fragen, ob autonomes Verhalten eines Systems dessen Verlässlichkeit erhöhen kann oder sie umgekehrt einschränkt. Verlässlichkeit stellt eine Art Überbegriff dar, der sich in verschiedene Aspekte aufteilt.

Im Zentrum steht dabei die *Sicherheit* eines Systems, wobei das Konzept der (IT-)Sicherheit ein eher generisches Qualitätsmerkmal eines Systems beschreibt. „Der BSI Standard 100-1 zum Beispiel definiert die Aspekte Vertraulichkeit, Integrität und Authentizität als Grundwerte der Sicherheit in der IT (vgl. BSI 2005).

- *Vertraulichkeit*: Die Vertraulichkeit ist die Eigenschaft eines Systems, Daten vor dem Zugriff durch unbefugte Dritte zu schützen.
- *Integrität*: Die Integrität bezeichnet die Fähigkeit eines Systems, Daten unverfälscht und in gültiger Weise zu verarbeiten.
- *Authentizität*: Die Authentizität eines Objektes besagt, dass aufgestellte Behauptungen über das Objekt wahr sind.

Darüber hinaus wird mit dem Begriff der Sicherheit auch die *Betriebssicherheit* abgedeckt, die auch *technische Sicherheit* genannt wird. Gängige Konzepte der Betriebssicherheit sind:

- *Verfügbarkeit*: Die (operationale) Verfügbarkeit ist die Fähigkeit des Systems, zu einem gegebenen Zeitpunkt seinen Dienst erbringen zu können.

⁵⁴

Im Hinblick auf die Sicherstellung der Funktionalität eines IT-Systems kann wegen der Unvorhersagbarkeit von OC ein Ziel z.B. „für formale Verifikation sein, dass anstelle von festen Verhaltensgarantien (wie bei der Programmverifikation üblich) der Nachweis des Verweilens in einem bestimmten Verhaltenskorridor gezeigt wird.“ (André et al. 2009:10)

- *Zuverlässigkeit*: Die Zuverlässigkeit ist die Fähigkeit eines Systems, seinen Dienst über einen gegebenen Zeitraum hinweg zu erbringen.
- *Fehlertoleranz*: Die Fehlertoleranz ist die Eigenschaft eines Systems, trotz des fehlerhaften Verhaltens von Systemkomponenten, wie z.B. deren Ausfall, die operationale Verfügbarkeit zu gewährleisten (*maskierende Fehlertoleranz*) bzw. wiederherzustellen (*nicht-maskierende Fehlertoleranz*), d.h. die spezifizierte Funktion zu erbringen.
- *Robustheit*: Die Robustheit ist die Eigenschaft eines Systems, seine operationale Verfügbarkeit auch bei einem Betrieb in einem Bereich außerhalb seiner eigentlichen Spezifikation zu gewährleisten. Im Unterschied zur Fehlertoleranz geht es hier daher nicht – oder zumindest nicht ausschließlich – um Fehler innerhalb des Systems, sondern um eine widrige Einwirkung der Umwelt (inklusive der Eingaben) auf das System.⁵⁵
- *Performanz*: Die Performanz ist die Eigenschaft eines Systems, eine vorgegebene Funktion ausreichend schnell ausführen zu können. Häufig wird nur die durchschnittliche Performanz betrachtet.
- *Echtzeitfähigkeit*: Die Echtzeitfähigkeit ist die Eigenschaft eines Systems, unter vorgegebenen zeitlichen Bedingungen die geforderte Funktion zu erbringen.“ (Heiß et al. 2008:25)

In diesem Zusammenhang kann das Verhalten eines Systems in drei verschiedene Klassen eingeteilt werden:

- *Korrektes Verhalten*: Das Verhalten des Systems entspricht der Erwartung.
- *Inkorrektes Verhalten*: Das Verhalten des Systems entspricht nicht der Erwartung.
- *Schädliches Verhalten*: Ein inkorrektes Verhalten, das einem oder mehreren Systemen der Umwelt Schaden zufügt.

Es ist zu beachten, dass schädliches Verhalten entsprechend dieser Einteilung stets inkorrektes Verhalten impliziert. Die Umkehrung gilt aber nicht.“ (Heiß et al. 2008:26)

Der Unterschied zwischen Zuverlässigkeit und Sicherheit eines Systems liegt im zulässigen Systemverhalten. „Während Zuverlässigkeit die Erbringung eines Dienstes fordert (also ein gewisses Verhaltensmuster an der Systemgrenze), erwartet technische Sicherheit⁵⁶ die Nichtgefährdung der Umwelt (was auch gegebenenfalls die Einstellung jeglicher Kommunikation bedeuten kann).“ (Heiß et al. 2008:34)

Weil es sich als äußerst schwierig herausgestellt hat, Metriken für Sicherheit (security) anzugeben, „werden zur Beschreibung von Sicherheit häufig Metriken oder Modelle benutzt, die nicht die Sicherheit (also die Gewährleistung) von Schutzzielen beschreiben, sondern die Effektivität von Schutzmaßnahmen. In Menezes et al. (1996) werden z. B. fünf Sicherheitsklassen unterschieden:

⁵⁵ Robustheit ist ein Vorteil von Organic Computing-Systemen, insofern sie prinzipiell in der Lage sind, sich von Fehlern selbständig zu erholen und sich ihrer Umgebung optimal anzupassen.

⁵⁶ „Das Maß der (technischen) Sicherheit $S(t)$ eines Systems ist die Wahrscheinlichkeit, dass das System über einen Zeitraum $t_0 + t$ seine Umgebung nicht gefährdet.“ (Heiß et al. 2008:34)

Ad hoc-Sicherheit (ad hoc security): Ein Abwehrmechanismus ist ad hoc sicher (häufig auch heuristisch sicher genannt), wenn es überzeugende Argumente dafür gibt, dass er mit einem bestimmten Aufwand nicht zu überwinden ist.

Aufwandsabhängige Sicherheit (computational security): Ein Abwehrmechanismus ist aufwandsabhängig sicher (mitunter auch praktisch sicher genannt), wenn der angenommene (Rechen-)Aufwand zur Überwindung (unter Annahme des effektivsten bekannten Angriffs) einen gewissen (großen) Rechenaufwand benötigt.

Beweisbare Sicherheit (provable security): Ein Abwehrmechanismus wird als beweisbar sicher gegenüber einem Angriff bezeichnet, wenn gezeigt werden kann, dass die Überwindung des Mechanismus im Wesentlichen so schwierig ist wie die Lösung eines wohlbekanntes und als schwierig vermuteten Problems.

Komplexitätstheoretische Sicherheit (complexity-theoretic security): Es wird angenommen, dass ein Angreifer sich jeden Aufwand einer bestimmten Komplexitätsklasse leisten kann. Ein Abwehrmechanismus ist komplexitätstheoretisch sicher, wenn bewiesen werden kann, dass der Mechanismus gegen jeden Angriff, den der Angreifer sich leisten kann, unüberwindlich ist.

Unbedingte Sicherheit (unconditional security): Ein Abwehrmechanismus ist unbedingte (auch: unbeschränkt) sicher, wenn er bewiesenermaßen nicht von einem Angreifer mit beliebigen Ressourcen überwunden werden kann.“ (Heiß et al. 2008:36)

Steuerbarkeit

„Die Steuerbarkeit eines Systems wird informell folgendermaßen definiert: Ein System ist steuerbar (controllable), wenn das Verhalten des Systems durch Kontrolleingaben in allen Situationen von außen geeignet beeinflusst werden kann.“⁵⁷ (Heiß et al. 2008:184) Steuerung ist auch bei konventionellen IT-Systemen eine zu lösende Aufgabe. SaSo-Systeme wie OC kennzeichnen jedoch gerade ihre Autonomie und (kontrollierte) Selbststeuerung, und damit ein negativer Informationsgradient.⁵⁸ „Eine mögliche Folge einer Einschränkung des Informationsflusses über die Schnittstellen eines Systems ist, dass es eventuell nicht mehr möglich ist, so auf das System von außen einzuwirken, dass ungewolltes Verhalten vermieden oder zumindest abgestellt wird. In solch einem Szenario kann von einer mangelnden Steuerbarkeit des Systems gesprochen werden. In der Regelungstechnik ist die Steuerbarkeit eine essentielle Eigenschaft eines Systems, welche z.B. eine wichtige Rolle bei der Stabilisierung instabiler Systeme oder bei der Realisierung optimaler Regelungen spielt.“ (Heiß et al. 2008:184)

⁵⁷ „Ein Beispiel für mangelnde (Ausgabe)Steuerbarkeit ist der Absturz einer Boeing 767 der Lauda-Air in Thailand im Jahr 1991. Hier schaltete sich während des Steigfluges unter anderem durch einen Softwarefehler die Schubumkehr der Triebwerke ein. Die überraschten Piloten hatten keine Möglichkeit mehr, den Absturz zu vermeiden. Die Schubumkehr wird normalerweise bei einer erfolgten Landung des Flugzeuges von den Piloten aktiviert und muss während des Fluges abgeschaltet bleiben. Nach dem Unglück wurde eine Schubumkehrsicherung in diesen Flugzeugtyp eingebaut, die eine Aktivierung der Schubumkehr in der Luft verhindert.“ (Heiß et al. 2008:185)

⁵⁸ „Dieser besagt insbesondere für Steuer- bzw. Kontrollinformationen, dass im System mehr Informationen verarbeitet werden, als über seine Grenzen transportiert werden und damit an den Schnittstellen des Systems abgreifbar sind.“ (Heiß et al. 2008:184)

Beachtet werden muss dabei auch, „dass in einem System aus vielen Komponenten die Steuerbarkeit nicht nur dahingehend relevant ist, dass ein Mensch etwas steuern kann, sondern sich auch (bei entsprechend gewählter Betrachtungsebene) darauf bezieht, dass ein Teil des Systems von einem anderen Teil des Systems gesteuert werden kann, ersterer also entsprechende Möglichkeiten der Steuerung bieten muss.“ (Heiß et al. 2008:227)

Jedes (rigide) komplexe System sieht sich unabhängig vom gewählten Modellansatz mit (meist von außen kommenden) Problemen seiner Steuerbarkeit und Kontrollierbarkeit konfrontiert. Die OC-Spezifika besteht in der (angestrebten) kontrollierten Emergenz, um aus Selbstorganisation resultierende Emergenz in einem vorgegebenen Rahmen halten zu können. Daher sind lernende Systeme von besonderem Interesse. In der OC-Forschung geht es dann darum, ihnen vorzuschreiben, in welche Richtung sie aus vorgegebenen Beispielen in sinnvoller Art verallgemeinern können. Wünschenswert ist, die Verallgemeinerungsrichtungen vom Benutzer vorgeben zu können.

Insgesamt wird deutlich, dass Selbstorganisation keineswegs als gänzlich autonom angesehen werden kann, die Grenzen der Steuerbarkeit solcher Systeme jedoch insbesondere von ihrer Eindeutigkeit, Komplexität und der Begrenzbarkeit und Beeinflussbarkeit ihrer Aktionen und Entscheidungen abhängen (vgl. Vec et al. 2006).

Autonomieinduzierte Schwachstellen

Neben den offensichtlichen Vorteilen autonomer Systeme bergen diese Systeme auch spezifische Risiken, die durch die Architektureigenschaften des jeweiligen Systems verursacht werden können und auch durch die unter Umständen fehlende Beobachtbarkeit und Steuerbarkeit aufgrund des Informationsgradienten auftreten können. Natürlich kann ein autonomes System neben solchen *autonomieinduzierten Schwachstellen* auch alle Schwachstellen aufweisen, die ein System ohne die Eigenschaft ‚Autonomie‘ haben (vgl. Merlin 1974). Der für Schwachstellen relevante Kontext sind Sicherheitsstrategien für IT-Systeme, mit deren Hilfe bestimmte, nachfolgend definierte Schutzziele erreicht werden sollen (vgl. Heiß et al. 2008:168f).

„*Authentizität*: Unter Authentizität eines Objektes wird die Echtheit und Glaubwürdigkeit des Objektes verstanden, die anhand einer eindeutigen Identität und charakteristischen Eigenschaften überprüfbar ist.

Datenintegrität: Die Datenintegrität eines Systems ist gewährleistet, wenn es nicht möglich ist, die zu schützenden Daten unautorisiert und unbemerkt zu manipulieren.

Informationsvertraulichkeit: Die Informationsvertraulichkeit ist gewährleistet, wenn das System keine unautorisierte Informationsgewinnung ermöglicht.

Verfügbarkeit: Die Verfügbarkeit eines Systems ist gewährleistet, wenn authentifizierte und autorisierte Nutzer in der Wahrnehmung ihrer Berechtigung nicht unautorisiert beeinträchtigt werden können. Zu beachten ist, dass diese Begriffsbestimmung ... neben dem Aspekt der Security auch Aspekte der Verlässlichkeit umfasst, da eine Beeinträchtigung der Wahrnehmung der Berechtigung neben Angriffen auch durch technische Fehlfunktionen erfolgen kann.

Verbindlichkeit: Verbindlichkeit bedeutet in diesem Kontext, dass durchgeführte Aktionen dem entsprechenden Subjekt (z. B. dem Nutzer, der sie ausgeführt hat) so zugeordnet sind, dass sie nicht abgestritten werden können.

Anonymisierung und Pseudonymisierung: Unter Anonymisierung wird das Verändern personenbezogener Daten solchermaßen verstanden, dass es nicht mehr möglich ist (oder nur mit unverhältnismäßig hohem Aufwand), Einzeldaten den dazugehörigen Personen zuzuordnen. Pseudonymisierung hat das gleiche Ziel, allerdings in der abgeschwächten Form, dass die Zuordnung ohne Kenntnis der Zuordnungsvorschrift nicht möglich ist.

In Eckert (2001) werden diese Schutzziele allgemein betrachtet, also nicht mit Fokus auf autonome Systeme. Es ist an obigen Beschreibungen jedoch leicht zu sehen, dass diese Ziele für ein autonomes System in gleicher Weise gelten wie für jedes andere System. Wird zudem berücksichtigt, dass ein autonomes System weitgehend ohne Nutzereingriffe seine Funktion erfüllen soll, so unterstreicht das die Bedeutung dieser Schutzziele zusätzlich... In autonomen Systemen können (z.B. durch Selbstorganisation) fortlaufend Eigenschaften erscheinen, verschwinden, verstärkt oder auch abgeschwächt werden. Die dadurch auftretenden Effekte können dabei sowohl beabsichtigt (erwünschte Autonomie) als auch unbeabsichtigt sein (unerwünschte Autonomie). Ziel ist es, erwünschte Autonomie zu fördern und unerwünschte Autonomie soweit wie möglich zu vermeiden.“ (Heiß et al. 2008:169ff) Dementsprechend sind autonomieinduzierte Schwachstellen danach zu unterscheiden, ob sie eine Folge erwünschter bzw. beabsichtigter Autonomie sind oder ob sie durch unbeabsichtigte Autonomie verursacht werden.

Schwachstellen durch erwünschte Autonomie resultieren entweder aus der autonomiefördernden Auslegung der dem System zugrunde liegenden Architektur oder aus dem Einsatz von autonomen Techniken. Erstere beziehen sich auf die erwähnten, von unterschiedlichen Architekturmustern verschieden ausgeprägten Grundeigenschaften (Homogenität, Synchronität, Bindung, Koordination, Interaktion, Dynamik), letztere auf ineffektive Selbstoptimierung, mangelnde Selbstkenntnis, mangelnde Fehlertoleranz und Verklemmungen⁵⁹ (deadlocks) (vgl. Heiß et al. 2008:172ff).

Das Auftreten von emergentem Verhalten und das Vorhandensein eines Informationsgradienten sind wie gesagt Indizien von Autonomie, und zwar unabhängig davon, ob das autonome Verhalten beabsichtigt ist. Somit kann das unerwünschte Vorhandensein dieser Indizien als Hinweis auf unerwünschte Autonomie gesehen werden. Von daher resultieren Schwachstellen durch unerwünschte Autonomie insbesondere aus dem Auftreten unerwünschter Emergenz oder aus einem unerwünschten Informationsgradienten. Unerwünschte Effekte emergenten Verhaltens können sich aus unerwünschter Dynamik (z.B. einem sich Aufschaukeln) oder aus unerwünschten Wechselwirkungen (z.B. infolge unberücksichtigter Abhängigkeiten) ergeben. Ein aus der Autonomie eines Systems resultierender negativer Informationsgradient geht wie gesagt mit einem beschränkten Informationsfluss über die Schnittstellen des Systems einher, sodass es zu mangelnder Steuerbarkeit (controllability) oder mangelnder Beobachtbarkeit⁶⁰ kommen kann (vgl. Heiß et al. 2008:181ff). Insgesamt benennen Heiß et al. (2008:198) folgende autonomieinduzierte Schwachstellen: common mode failure, mangelnde Rückmeldungen vom Interaktionspartner, Manipulierbarkeit von Bindungen, manipulierbare Entscheidungsfindung, Ereignisschauer⁶¹, man in the middle⁶², uner-

⁵⁹ „Verklemmungen können dazu führen, dass das System dauerhaft versagt, da es die gewünschten Aktionen nicht ausführen kann. Daher ist es für autonome Systeme essentiell, dass in ihnen das Auftreten von Verklemmungen vermieden wird oder wenigstens beim Auftreten dafür gesorgt wird, dass diese geeignet aufgelöst werden.“ (Heiß et al. 2008:179)

⁶⁰ Problematisch kann in diesem Fall auch werden, wenn das autonome System falsche Rückschlüsse aus seiner Beobachtung zieht.

⁶¹ Überlastung des Monitoring durch gleichzeitige Sensorenbeobachtungen und -meldungen bei Katastrophen

wünschte Komponenten im System, ineffektive Optimierungen, lokale statt globaler Optimierungen, unzureichendes Wissen im System über das System, unzureichende Laufzeitinformationen im System über das System, fehlendes Fehlermodell, mangelnde Fehlertoleranz, Verklemmungen, unerwünschte Emergenz, unerwünschte Dynamik, unerwünschte Wechselwirkungen, unerwünschter Informationsgradient, mangelnde Steuerbarkeit, mangelnde Beobachtbarkeit.

Zusammenfassend kann mit Heiß et al. (2008:202f) festgehalten werden: „Durch Autonomie – egal, ob sie beabsichtigt oder unbeabsichtigt in ein System eingebracht wurde – können zusätzliche Schwachstellen auftreten. Dabei fällt es schwer, diese Schwachstellen *direkt* der Autonomie zuzuordnen. Vielmehr werden Schwachstellen, die auch anderweitig auftreten können, begünstigt, d. h. die Wahrscheinlichkeit ihres Auftretens steigt. Dies sind aber in der Regel mittelbare Effekte, die ihren Grund in den Eigenschaften der Architekturmuster haben, die in Systemen mit Autonomie anzutreffen sind. Eigenschaften wie Asynchronität, späte Bindungen oder dezentrale Koordination, die zwar autonomie-typisch, aber nicht autonomie-implizierend sind, bringen eine Anfälligkeit für die diskutierten Schwachstellen mit sich. Diese Eigenschaften erschweren bei gewünschter Autonomie auch die Gegenmaßnahmen: typische Teile-und-herrsche-Ansätze zur Erhöhung der Beherrschbarkeit von Schwachstellen, die meist mit Hierarchisierung, Reduzierung von Schnittstellen, Einschränkung des Verhaltens und/oder des Zustandsraums verbunden sind, schränken die Freiheitsgrade eines Systems ein und vernichten damit gewünschte Autonomie oder behindern sie mindestens. Falls jedoch Fälle von unerwünschter Autonomie auftreten, können diese klassischen Ansätze natürlich hilfreich sein. In diesen Fällen liegt das Problem eher bei der *Erkennung*: Fehlerhaftes autonomes Verhalten tendiert dazu, sich als *Heisen-Bug* darzustellen, also als ein Fehler, der bei näherer Untersuchung verschwindet. Auch bei erwünschter Autonomie ist die Schwachstellenerkennung schwierig. Sie vereinfacht sich, wenn autonomes Verhalten formalisiert werden kann... Jedoch zeigt es sich in der Praxis oft, dass selbst bei existierender *Möglichkeit der* Modellierbarkeit eines Systems (die eine Grundlage der formalen Behandlung bildet) diese häufig nicht genutzt wird. Dies liegt meist daran, dass sich die Systementwickler entweder nicht des Risikos bewusst sind, oder dass sie den Aufwand als zu hoch im Verhältnis zum Risiko einschätzen oder dass sie sich einfach nicht in der Lage sehen, entsprechende Methoden anzuwenden. Aber insbesondere beim Auftreten emergenten Verhaltens, das ja typisch für Systeme mit Autonomie ist, gibt es auch vielfach noch keine stringenten Methoden der Modellierung oder gar der Analyse. Hier sind Systementwickler auf naturgemäß weniger zuverlässige Adhoc-Ansätze angewiesen. Eine noch allgemeinere Quelle für autonomie-induzierte Schwachstellen wurde bisher noch gar nicht angesprochen: Die Komplexität. Natürlich ist eine steigende Komplexität ein allgemeines Phänomen der modernen Systementwicklung. Jedoch gilt, ... dass Autonomie in der Praxis stets die Systemkomplexität und damit die Gefahr von Schwachstellen erhöht. Alle anderen ... Schwachstellen gewinnen dadurch zusätzliches Gefährdungspotenzial: Nicht nur, dass ihr Auftreten durch die systemeigene Autonomie wahrscheinlicher ist, sie sind auch noch durch die autonomie-induzierte Komplexität schwerer zu identifizieren und zu beheben. Dies tritt insbesondere bei Systemen mit beabsichtigter Autonomie auf. Dadurch verschärft sich das bereits diskutierte Problem der Erkennung autonomieinduzierter Schwachstellen noch zusätzlich.“

Maßnahmen zur (autonomieinduzierten) Schwachstellenbekämpfung

Maßnahmen zur (autonomieinduzierten) Schwachstellenbekämpfung müssen berücksichtigen, dass Autonomie einerseits häufig dafür eingesetzt wird, die Verlässlichkeit von IT-Systemen zu erhöhen, und andererseits genuine (zusätzliche) Gefährdungen bewirken kann, egal ob die Autono-

mie beabsichtigt eingebracht wurde, oder ob es sich um unbeabsichtigte Autonomie handelt. „Bei IT-Systemen geht es also darum, korrektes autonomes Verhalten zu erzielen, also Autonomie in den Grenzssetzungen der Systemintentionen. Daher müssen bei Maßnahmen, die der Verbesserung der Verlässlichkeit autonomer Systeme dienen, stets zwei Aspekte berücksichtigt werden: die Sicherstellung korrekten autonomen Verhaltens und die Unterdrückung inkorrekten autonomen Verhaltens. Zum letzteren gehört insbesondere unerwünschte Autonomie... Es ist zu beachten, dass beide Aspekte bei der Behandlung eines einzigen Systems eine Rolle spielen können: Es kann gleichzeitig darum gehen, sowohl gewünschte Autonomie zu fördern und ihre Korrektheit zu gewährleisten, als auch unerwünschte Autonomie zu vermeiden.“ (Heiß et al. 2008:204)

Maßnahmen zur Sicherstellung erwünschter Autonomie betreffen die Auswahl geeigneter Architekturmuster in der Designphase, die Bekämpfung architekturinduzierter Schwachstellen durch Abschwächung etwa der autonomiefördernden Auslegung von Eigenschaften, Selbststabilisierung⁶³ und Superstabilisierung⁶⁴, Fehlereindämmung⁶⁵, und Sicherstellung der Lebendigkeit.⁶⁶ (vgl. Heiß et al. 2008).

Maßnahmen zur Vermeidung unerwünschter Autonomie betreffen die Vermeidung unerwünschter Dynamik (eines autonomen Systems), die Vermeidung unerwünschter (Auswirkungen von) Wechselwirkungen, die Sicherstellung ausreichender Beobachtbarkeit, und die Sicherstellung ausreichender Steuerbarkeit (vgl. Heiß et al. 2008:220ff)

Schwachstellenbekämpfung hat auch *Konsequenzen für die Modellierung*, was etwa die Auswahl geeigneter Modellierungstechniken, die besondere Rolle modellgetriebener Architektur (Model-Driven Architecture (MDA)), Reflexion und Adaption, Komponierbarkeit und vereinfachte Verifikation anbelangt (vgl. Heiß et al. 2008:230ff).

Zusammengefasst betreffen Maßnahmen zur Schwachstellenbekämpfung sowohl Maßnahmen zur Sicherstellung erwünschter Autonomie als auch solche zur Vermeidung des unerwünschten Auftretens von Autonomie. „Als essentiell hat sich herausgestellt, dass das Wissen im System über das System selbst (Selbstkenntnis) möglichst detailliert und präzise sein muss. Das betrifft sowohl statisches Wissen über die beteiligten Komponenten, ihre Konfiguration und ihre Zusammenhänge, als auch dynamisches Wissen über den aktuellen Systemzustand. Die Akkumulation des Wissens

⁶³ „Selbststabilisierung ist ein Konzept der Fehlertoleranz in verteilten Systemen. Ein System wird als selbststabilisierend bezeichnet, wenn garantiert ist, dass es sich eigenständig von beliebigen transienten Fehlern in beschränkter Zeit erholt und wieder einen legalen Betriebszustand erreicht.“ (Heiß et al. 2008:212)

⁶⁴ „Superstabilisierung erweitert ... das Konzept der Selbststabilisierung um ein sogenanntes Passagenprädikat, das auch während einer Rekonfiguration aufgrund einer Topologieänderung erfüllt bleibt. Passagenprädikate sind üblicherweise schwächer als Korrektheitsprädikate, jedoch stark genug, um zusätzlichen Nutzen zu bieten.“ (Heiß et al. 2008:214)

⁶⁵ „Fehlereindämmung (fault containment) ist eine Maßnahme aus dem Gebiet der Fehlertoleranz, die dazu dient, die Auswirkungen von Fehlern lokal zu begrenzen, indem beispielsweise dafür gesorgt wird, dass das Versagen eines Teilsystems nicht zum Versagen des gesamten Systems führt... Für selbststabilisierende Systeme ist Fehlereindämmung essentiell, da die Selbststabilisierung ein beliebiges Verhalten des Systems während der Stabilisierung, unabhängig von der Schwere des aufgetretenen Fehlers, erlaubt. Selbststabilisierung legt damit als nicht-maskierender Fehlertoleranzmechanismus zunächst mehr Wert auf die Lebendigkeit als auf die Betriebssicherheit eines Systems.“ (Heiß et al. 2008:214ff)

⁶⁶ Lebendigkeit ist für autonome Systeme eine essentielle (originär aus der Informatik stammende) Eigenschaft. Es geht ihr um den Umgang mit Verklemmungen, wobei Verklemmungsfreiheit schwache Lebendigkeit bedeutet.

sowie die Integration der Mechanismen zur Realisierung der Selbstkenntnis sollten dabei nicht nachträglich zum System ergänzt oder erst bei der Implementierung berücksichtigt werden, sondern von Beginn des Designs an berücksichtigt werden. Jegliches Wissen sollte explizit gemacht werden und nicht implizit in der Implementierung verborgen sein. Eine vielversprechende Vorgehensweise ist dabei eine durchgängige Modellierung, wie sie beispielsweise im Rahmen der modellgetriebenen Entwicklung realisiert werden kann. Wichtig ist dabei, dass die im Rahmen eines solchen Ansatzes zur Verfügung stehenden Modelle so weitreichend sind, dass sie die Modellierung allen relevanten Wissens auf geeignete Weise ermöglichen. Dies umfasst insbesondere die weitgehend automatische Überführung eines Modells in eine Implementierung (Codegenerierung) als auch den umgekehrten Weg von einer angepassten Implementation zurück zum Modell. Die durchgängige Modellierung umfasst auch den Betrieb des Systems, wo die benutzten Modelle beispielsweise im Rahmen einer reflektiven Middleware Verwendung finden. Mit diesem Ansatz ist eine fundierte Basis vorhanden, um in jeder Phase des Lebenszyklus eines autonomen Systems die geeigneten Maßnahmen zur Sicherstellung der Verlässlichkeit anwenden zu können. In der Entwicklungsphase umfasst dies unter anderem den Entwurf von Schnittstellen mit Berücksichtigung sämtlicher relevanten funktionalen und nicht-funktionalen Eigenschaften, in der Integrationsphase eine hinsichtlich ihrer Eigenschaften vorhersagbare Komposition der einzelnen Subsysteme und im Betrieb beispielsweise die Selbstoptimierung und Fehlereindämmung. Die aktuelle Praxis der Software-Entwicklung autonomer Systeme ist von diesem Idealziel allerdings noch weit entfernt. Es bedarf damit weitergehender Anstrengungen sowohl im Bereich der Bereitstellung geeigneter Softwarewerkzeuge (beispielsweise integrierte Modellierungs- und Entwicklungsumgebungen), aber auch im Bereich der Forschung hinsichtlich beispielsweise entsprechender Algorithmen, die die skizzierten Maßnahmen durchgehend umsetzen.“ (Heiß et al. 2008:241)

3 Entwicklungslinien und Marktperspektiven von Organic Computing und smarten IT-Systemen

Nachdem im vorangehenden Kapitel zentrale Konzepte und Merkmale von OC auf primär begrifflich-analytischer Ebene vorgestellt wurden, geht es in diesem Kapitel um die historische und ökonomische Dimension von OC: Wie ist es entstanden? Welche Entwicklungslinien und Marktperspektiven lassen sich aufzeigen? Dafür wird zuerst die bisherige Herausbildung und Entwicklung von OC in Kapitel 3.1 resümiert, um anschließend in Kapitel 3.2 die im Rahmen des DFG-Schwerpunktprogramms „Organic Computing“ (<http://www.aifb.uni-karlsruhe.de/Forschungsgruppen/EffAlg/projekte/oc/inhalte>) laufenden OC-Projekte aufzuführen. Der anschließende Überblick über die gegenwärtige und voraussichtliche zukünftige wirtschaftliche Bedeutung von smarten IT-Systemen und befähigenden (IT-)Technologien benennt in Kapitel 3.3 typische Voraussetzungen einer erfolgreichen Marktpenetration von OC und fasst auf dieser Basis seine Entwicklungs- und Marktperspektiven in Kapitel 3.4 zusammen.

3.1 Zur Geschichte und Entwicklung von Organic Computing

Entstehungsgeschichte

Wie im Sinne der Ausführungen in Kapitel 2 führt Schmeck (2006:14) als OC den Weg bereitende Marksteine an: ubiquitous computing (Weiser 1991), intelligent autonomous systems (Siemens, ~1994), pervasive computing (~1996), neuro sciences and molecular biology as basis for organic computing (von der Malsburg 2001), autonomic computing (IBM, ~2001), evo-architecture for cars (DaimlerChrysler, ~2001), organic IT for enterprise server architectures (Forrester Research, April 2002).

Würtz (2008:V) markiert sodann die bisherige Entwicklung von OC auf der Ebene sozialer Bemühungen und Ereignisse prägnant wie folgt: “As an idea whose time simply has come, Organic Computing is growing from multiple roots. In November 2001, a Symposium “Organic Computing – Towards Structured Design of Processes” was held at the Heinz Nixdorf Museum in Paderborn, Germany, bringing together computer scientists and biologists to pursue the idea. Independently, the Technical Informatics Branch of the German Computer Science Society (GI) developed the concept in a series of workshops in 2002. The scope was broadened by the Organic Computing Initiative of GI at a workshop in Hannover in 2003, which outlined the scope of today’s Organic Computing research. As a third root on the industrial side, Forrester Research presented a study in 2002, which proposed Organic IT as a strategy for information systems infrastructure. In the meantime, Organic Computing is a powerful driving force for a whole spectrum of research. Most visibly in terms of academic funding, in fall 2004, the DFG issued a call for proposals for a priority program on Organic Computing, which started with 18 projects in August 2005 and is currently in its second phase. In January 2006, there was a first Dagstuhl seminar, which also attracted participants from overseas, a second one is scheduled for the spring of 2008.”

Kennzeichnende Merkmale

Im Kern geht es aus Sicht der OC-Proponenten bei OC darum, große Gruppen von Forschungseinheiten zu organisieren. Auf dieser nicht bloß technischen Ebene sind außer Informatik/Informationstechnik auch andere Disziplinen (Ökonomie, Biologie, Soziologie) als Organisationswissenschaften involviert. Frühere derartige Versuche wie Kybernetik oder Systemwissenschaften versandeten meist.⁶⁷ Gemeinsamer Bezugspunkt von auf OC ausgerichteten Forschungs- und Entwicklungsvorhaben ist Selbstorganisation; von daher ist das Observer/Controller-Arrangement mit Organisation beschäftigt. Bei allen OC-Systemen geht es zumeist um Lernen, genetische und evolutionäre Algorithmen, Learning-Classifer-Systeme. Das Ziel angemessener Beherrschung von Komplexität strebt kontrollierte Emergenz an.⁶⁸ Auf der Ebene der Betriebssysteme geht es hierbei darum, erst einmal für kleine Systeme Selbstorganisationsprinzipien in entsprechende Software zu übersetzen. In diesem Zusammenhang stellt sich dann das Skalierungsproblem, ob eine bei kleinen Systemen funktionierende Software-Selbstorganisation auch nach denselben Prinzipien in großen Systemen (mit z.B. 100.000 Elementen) funktioniert. Abhängig hiervon läuft die Selbstorganisation (und Virtualisierung) auf höherer Ebene erfolgreich oder gelingt nicht.

Von daher ist OC „keine etablierte Technologie, sondern ein aktuelles, im Entstehen begriffenes interdisziplinäres Forschungsfeld, das erste Erfolge vorweisen kann... Langfristig bietet Organic Computing die Chance, die bereits heute sichtbar werdenden Probleme der Beherrschung komplexer technischer Systeme besser in den Griff zu bekommen... Es ist nicht die Frage, *ob* adaptive und selbstorganisierende Systeme entstehen – erste Ansätze sind vielfach zu beobachten – sondern *wie* wir sie gestalten. Dem Albtraum eines autonomen Systems, das seinen eigenen ‚Willen‘ durchsetzt, steht die Vision von freundlichen Systemen gegenüber, welche nicht bedient werden sondern dem Menschen dienen.“⁶⁹ (Müller-Schloer et al. 2004:336)

Relevante Aspekte von OC sind bereits (in Form spezifischer Anwendungen) ausgeübte Praxis, z.B. bei ambient assisted living. Zumeist geht es um die sukzessive Ausweitung adaptiver Systeme, wie z.B. die Regelung und Steuerung von Flugzeugen, Anti-Virus-Programmen oder Spam-Filtern.

Gerade bei Organic Computing Techniken stellt kontrollierte Emergenz das Ziel neuer Methoden zur Beherrschung von Komplexität dar (vgl. Weyer 2009). Das Potenzial an neuartigen Systemen, das sie erschließen könnte, ist im Erfolgsfall enorm groß, auch wenn zur Zeit noch keine fertigen, marktreifen Produkte nach Organic Computing Kriterien existieren, da sich OC-Systeme noch in der (fallspezifisch unterschiedlich weit fortgeschrittenen) Forschungs- und Entwicklungsphase be-

⁶⁷ Auf abstrakter Ebene gab es all dies (Selbstorganisation, Feedback-Schleifen) (implizit) schon lange, aber als eigener Bereich und expliziter Umgang mit ebendiesen Parametern ist dies neu. Es handelt sich um bewusste Eingriffe und kontrollierte Emergenz. Gegenüber traditionellen Differentialgleichungen in der Regelungstechnik für je spezifische Systeme geht es bei OC um den Umgang mit diskreten (nur begrenzt berechenbaren) IT-Systemen; hierbei stellt die Regelungstechnik sehr wohl ein nützliches Instrument dar.

⁶⁸ Kontrollierte Emergenz ist von gesteuerter Emergenz zu unterscheiden, insofern es um einen Sicherheitskorridor geht, während Steuerung (in der Regelungstechnik) ein klar definierter Begriff ist.

⁶⁹ Von daher geht es „im Forschungsgebiet Organic Computing zunächst darum, die natürlichen Phänomene besser und vor allem quantitativ zu verstehen, welche zu Emergenz, Selbstorganisation und autonomem Verhalten führen. Darüber hinaus muss das Ziel aber in einer ingenieurtechnischen Beherrschung solcher Systeme liegen.“ (Müller-Schloer et al. 2004:334)

finden (vgl. Gesellschaft für Informatik et al. 2008, Bernard 2008). Zur Realisierung solcher (neuar- tiger) OC-Systeme werden folgende Herausforderungen an die Informatikforschung gesehen: Kontrolle von Selbstorganisation und Emergenz⁷⁰, OC-Architekturen⁷¹, Selbst-X-Eigenschaften⁷², Si- cherheit, Robustheit und Vertrauenswürdigkeit⁷³, Entwurfsverfahren, Entwurfswerkzeuge und Ent- wurfsmethodik⁷⁴, Verständlichkeit für den Menschen⁷⁵, Lernverfahren⁷⁶, Inspiration aus der Gehirn- forschung und Bionik: Aktivität, Motivation und Emotionen⁷⁷, Komplexitätsreduktion⁷⁸, Organisati- onswissenschaften⁷⁹, Anwendungsgebiete.⁸⁰

-
- 70 „Es fehlen das systematische Verständnis und theoretische Beschreibungsmöglichkeiten der Konfigurierbarkeit von Systemen. Vielversprechende Ansätze sind Konfigurationsraummodelle, welche die Gesamtheit aller möglichen Zu- stände und die zugelassenen vs. verbotenen Konfigurationen beschreiben.“ (Gesellschaft für Informatik et al. 2008:32)
- 71 „Die Überwachungs- und Steuerungsebene könnte dabei langfristig ebenfalls aufwändiger werden als die Produktiv- ebene. Zu den in dieser Überwachungsebene zu lösenden Aufgaben gehören die Beobachtung und Beurteilung so- wie die Koordination dynamischer und adaptiver Subsysteme, die Bewertung von Alternativkonfigurationen, Koopera- tions- und Konfliktlösungsverfahren und die Durchführung von Rekonfigurationen.“ (Gesellschaft für Informatik et al. 2008:32f)
- 72 „Die Selbst-X-Anforderungen ... sollen in einer ganzheitlichen Architektur umgesetzt werden, um Selbstmanagement komplexer Systeme zu erreichen. Vorgänge innerhalb des Systems werden erfasst, analysiert, Maßnahmen zur An- passung, Verbesserung oder Reparatur ausgewählt und vom System weitgehend ohne Eingriff des Menschen durch- geführt. Eine solche ganzheitliche Architektur ist durch eine Observer/Controller-Architektur gegeben, bei der Observer ... und Controller ... zu Rückkopplungsschleifen zusammengefasst sind. Das System organisiert und wartet sich auf diese Weise selbst. Zudem wird ein System durch diese zusätzlichen Eigenschaften komplexer und teurer. Dort, wo Bedienbarkeit und Wartbarkeit die Komplexität eines Systems beschränken, ist die Erweiterung aber sehr sinnvoll. Performanzsteigerungen durch Adaptivität und Kosteneinsparungen beim Support rechtfertigen hier diese Vorgehensweise.“ (Gesellschaft für Informatik et al. 2008:33)
- 73 „So ist beispielsweise in sicherheitskritischen Anwendungen das Einhalten bestimmter Verhaltensgarantien eine ab- solut notwendige Voraussetzung. Für Anwendungen, die personalisierte Dienstleistungen anbieten, sind dagegen Da- tenschutz und Integrität von Daten unabdingbar.“ (Gesellschaft für Informatik et al. 2008:33)
- 74 „Durch die fortlaufende Evaluation ist Emergenz bei diesem Entwurstil kein Problem, sondern sogar wünschenswert. Problematisch ist hier, dass unsere vorhandenen Methoden nicht ausreichen, solch einen Entwurstil umzusetzen. Man braucht geeignete Basiselemente für das Anpassen und die Feinabstimmung. Man braucht Vorstrukturierungsmethoden und auf Aufgabenstellungen und Basiselemente abgestimmte Algorithmen, um den (Selbst-)Entwurfsprozess zu beschleunigen. Auch bedarf es Strategien, um das System mit einfachen Aufgabenstellungen zu beginnen und mit komplexeren Aufgaben wachsen zu lassen. Solche Vorgehensweisen sind für den selbstorganisie- renden Entwurf bisher noch nicht ausreichend untersucht. Wenn Systeme sich selbst entwerfen, so dürfen sie dies nur innerhalb vorgegebener Grenzen. Also muss die formale Spezifikation einerseits Vorgaben (Soll-Ziele), ander- seits zusätzliche Freiheitsgrade enthalten. Es entsteht so eine „Fuzzy“-Spezifikation. Ein anderer Ansatz zur Be- schränkung der Freiheitsgrade ist ein Constraint-based-Design. Analog zu Software-Systemen, welche zunächst nur über Testfälle beschrieben werden, könnte man im Systementwurf vorgehen. Es werden nur Constraints beschrieben: Das System darf alles, was nicht verboten ist.“ (Gesellschaft für Informatik et al. 2008:34)
- 75 „Ein selbstorganisierendes adaptives System stellt eine besondere Herausforderung an die Nutzerschnittstelle dar... Einerseits kann man dem Nutzer immer die interne Aufgabenverteilung darstellen ..., oder man stellt dem Benutzer nur die Ergebnisse dar... Im ersten Fall müssen Mechanismen der Selbsterklärung erdacht werden, um die komplexe dynamische Organisation des organischen Systems nach außen verstehbar zu machen. Zum anderen müssen ge- eignete Techniken entwickelt werden, die mit den OC-Algorithmen interagieren und geeignete Abstraktionen finden, um die Aspekte Benutzerfreundlichkeit und Vertrauenswürdigkeit abzudecken.“ (Gesellschaft für Informatik et al. 2008:34)
- 76 „Adaptive und selbstorganisierende Systeme müssen lernfähig sein. Lernverfahren ermöglichen während des Be- triebs eines organischen Rechnersystems dessen Optimierung sowie die Vorhersage von Ausfällen... Lernen ist grundsätzlich zeitaufwändig und erfordert viele (Fehl-)Versuche. Mithilfe modellbasierter Ansätze kann das Lernen simulativ und damit schneller sowie ohne unmittelbare Auswirkung auf die Umgebung erfolgen. Erst überprüfte Lö- sungen werden freigegeben.“ (Gesellschaft für Informatik et al. 2008:34)
- 77 „Damit Systeme sich selbst konfigurieren, optimieren, heilen und schützen können, müssen zumindest einige Kompo- nenten aktiv werden, d.h. sie verfolgen eigene Ziele. Dieses Verhalten lässt sich mit Eigenschaften wie Motivation, Trieben oder Selbstbewusstsein beschreiben... Es gibt Grundprinzipien im Gehirn, die möglicherweise auch für tech-

Mit Blick auf die laufende und zukünftige Entwicklung von OC-Systemen können und werden diese in vielen Bereichen nur dann eingesetzt werden, „wenn sie vertrauenswürdig sind. Vielversprechende Ansätze dazu sind wiederum Observer/Controller-Architekturen, die Zustandsraumüberwachung mittels Guarding und Assertions, Stabilitätskontrolle, die Unterscheidung von Selbst- und Fremdkomponenten (Immunsystem) sowie Erkennung und Schutz vor Angriffen.“ (Gesellschaft für Informatik et al. 2008:33) Mit der Zunahme der Autonomiestufen von OC-Systemen, d.h. der Größe des Konfigurationsraumes, in dem es Parameter selbst bestimmen kann⁸¹, wachsen deren Möglichkeiten der Selbstorganisation und die Wahrscheinlichkeit (erwünschter) emergenter Effekte. Wenn „gerade größere, komplexere Systeme vom verstärkten Einsatz von Organic Computing-Prinzipien profitieren werden, ist die Einführung von überwachenden und vertrauensfördernden Strukturen wie Observer/Controller oder TWEL [Trustworthiness Enforcement Layer; vgl. Brancovici 2008] ein entscheidendes Kriterium für die wirtschaftliche Vermarktung von Organic Computing-Systemen. Gerade hier ist das große Potenzial von Organic Computing spürbar. Jedoch werden diese komplexen Organic Computing-Systeme der höheren Autonomiestufen erst marktreif produziert werden können, wenn man auch in der Lage ist, ihre Autonomie so zu überwachen, dass die Systeme vertrauenswürdig sind.“⁸² Diese Tatsache wird in mehreren Organic Computing-Forschungsprojekten bereits berücksichtigt. In der Entwicklung bedeutet dies, dass die Konfigurationsräume nur so groß geöffnet werden, wie sie auch von Kontrollinstanzen beherrscht werden können. Zukünftige Organic Computing-Systeme werden also zunehmend mehr Möglichkeiten zur Konfiguration besitzen und somit immer komplexere Aufgaben erledigen können. Ein Wachsen des Autonomiegrades wird einhergehen mit einer Vergrößerung der Kontrollmechanismen, um die Systeme abzusichern.“ (Bernard 2009:3; Schmeck et al. 2009) Die Simulation als Element der Risikominimierung, die Wahl einer geeigneten Struktur und Architektur, sowie Prozessverbesserungs- und Analysetechniken können bei OC ebenso angewandt werden wie bei herkömmlicher Software. Demgegenüber sind herkömmliche Testverfahren des Software Engineerings zwar anwendbar, aber nicht ausreichend, da sich OC-Systeme zur Laufzeit verändern können. So ist es Gegenstand aktueller Forschung, inwieweit die gewollte Lernfähigkeit eines Systems in der Praxis genutzt werden kann, ohne das System in unerwünschte Zustände zu bringen. Auch ist es fraglich,

nische Systeme interessant sind... Ähnlich der Bionik kann die Natur als Inspiration für weitere Algorithmen und Verfahren der Informatik dienen.“ (Gesellschaft für Informatik et al. 2008:34f)

- 78 „Ein alternativer Ansatz verfolgt die *Komplexitätsreduktion* als Entwurfskriterium. Man geht beim Entwurf der Basiselemente nicht an die Grenzen des Machbaren, sondern reduziert das System auf das Nötigste zur Erfüllung der vorgesehenen Aufgaben, um es einfach und wartbar zu halten... Der derzeitige Trend zur Integration vieler Prozessoren auf einem Chip und die Vernetzung vieler Rechensysteme erfordern diese Methode der Komplexitätsbeherrschung.“ (Gesellschaft für Informatik et al. 2008:35)
- 79 „Können die Observer-/Controller-Prinzipien auch auf Organisationen, Firmen oder Gesellschaften angewandt werden?“ (Gesellschaft für Informatik et al. 2008:35)
- 80 „Insbesondere muss die Überführung relevanter Ergebnisse aus der OC-Grundlagenforschung in die industrielle Praxis gefördert werden. Lücken bestehen u.a. auf den Gebieten der Architekturen, der Sicherheit, der Entwurfsverfahren und -werkzeuge und der Anwendungen für selbstorganisierende adaptive Systeme. Gesucht werden anwendungsspezifische Lösungen möglichst mit Demonstratoren aus den Bereichen der Automobiltechnik, Verkehrstechnik, Fabrikautomatisierung, Mechatronik, Gebäudetechnik, Sicherheitstechnik und der adaptiven Energieversorgung.“ (Gesellschaft für Informatik et al. 2008:36)
- 81 „Die Zunahme der Autonomie inkludiert letztlich das Potenzial von Organic Computing, je mehr Parameter vom System selbst eingestellt und optimiert werden können, desto stärker ist das System in der Lage, sich selbst schnell in den optimalen Zustand zu bringen.“ (Bernard 2009:1)
- 82 In der mehrfach zitierten Studie von Heiß et al. (2008) wird die Frage der Autonomie komplexer Computersysteme unter verschiedenen, teils wiedergegebenen Gesichtspunkten systematisch behandelt, um Sicherheitsrisiken autonomen Verhaltens und angemessene Schutzvorkehrungen zu identifizieren, was entsprechende Schlussfolgerungen für die Risiken selbstorganisierender OC-Systeme erlaubt.

ob OC sich aufgrund seiner Grundarchitektur an umfassende Standards halten kann, wie sie z.B. in der Automobilbranche üblich sind (Bernard 2009).⁸³

DFG-Schwerpunktprogramm und Entwicklungsperspektiven

Ohne die DFG als Geldgeber und Förderer des von 2005 bis 2011 laufenden Schwerpunktprogramms „Organic Computing“ gäbe es mit an Sicherheit grenzender Wahrscheinlichkeit kein OC mit rund 20 Projekten über insgesamt 6 Jahre, sondern es würden nur diesbezügliche Einzelprojekte durchgeführt. OC wurde anfangs in technischen Kreisen ziemlich emotional diskutiert und erhielt durch die DFG-Förderung quasi ein Gütesiegel. Entsprechende Ideen kursierten zwar schon lange, die aber teils eher etwa als unrealistisch oder unausgegoren belächelt wurden. Die gezielte Förderung induzierte einen Kristallisationseffekt und inzwischen eine beachtliche Eigendynamik.

Das DFG-Schwerpunktprogramm „Organic Computing“ umfasst breite Grundlagenforschung und konkrete Anwendungen, wie Abbildung 3.1 verdeutlicht, und ist darum nur begrenzt top-down steuerbar. Sein Fördervolumen beträgt über die sechsjährige Laufzeit 12 Mio. €.

Bei darüber hinausgehenden konkreten, auf Marktfähigkeit abzielenden Anwendungen dürften die (von BMBF und Industrie aufzubringenden) jährlichen Entwicklungskosten für z.B. drei erfolgversprechende Anwendungsoptionen jeweils ca. 50 Mio. € betragen, sodass für einen Anwendungsbereich (bei 10 Jahren Entwicklungszeit) mit 500 Mio. € Kosten zu rechnen ist. Dabei stellt OC jedoch meist nur eine Komponente innerhalb solcher FE-Projekte dar. Allerdings zeigte die Industrie über die partielle Beobachtung dieses neuen Forschungsfeldes hinaus bislang wenig Interesse, in (gemeinsame) OC-Vorhaben zu investieren. Entsprechende Kontakte und Bemühungen waren im Wesentlichen vergeblich. So wurde auch keine gemeinsame Architektur für OC-Systeme, z.B. eine Server/Controller Architektur identifiziert.

Terminologisch ist ‚Organic Computing‘ im Grunde die Bezeichnung für den DFG-Forschungsschwerpunkt und damit ein in Deutschland (auf einem Workshop über Zukunftsthemen der Technischen Informatik und einem Symposium „Organic Computing – Towards Structured Design of Processes“) um 2001/2002 generierter Begriff. Dieser Forschungsschwerpunkt befasst sich mit der Untersuchung und Entwicklung von SaSo-Systemen, wobei es von vornherein um seine Ausrichtung auf gesteuerte Autonomie ging. Durch auf OC bezogene Präsentationen und Veranstaltungen auf Computer- und IT-Tagungen (ARCS, ACM, BICC, ATC, CEC, SASO)⁸⁴ ist dabei die Sichtbarkeit von OC durchaus gegeben.

⁸³ Wesentliche Unterschiede zwischen herkömmlichen Systemen und Systemen, die nach dem Organic Computing-Paradigma erstellt wurden, bestehen in folgenden Punkten: „Durch die Fähigkeit zur Selbstheilung können Organic Computing-Systeme flexibel auf Systemteilausfälle reagieren. Die Gesamtfunktion des Systems bleibt also trotz ausfallender Komponenten erhalten, was bei herkömmlichen Systemen nicht der Fall ist. Organic Computing-Systeme sind in der Lage, defekte Komponenten selbsttätig zu erkennen und zu isolieren. Auch die Erweiterung um neue Komponenten ist durch die dynamische Struktur der Organic Computing-Systeme, speziell durch die Selbstorganisation, wesentlich besser realisierbar als bei herkömmlichen Systemen. Ebenso können Organic Computing-Systeme sich im Gegensatz zu bisherigen Systemen schnell geänderten Umweltbedingungen anpassen, wie in den Fallstudien verdeutlicht wurde. Ein wesentlicher Punkt zur Unterscheidung von herkömmlichen Systemen und Organic Computing-Systemen ist die Lernfähigkeit: Organic Computing-Systeme können nicht nur adaptiv auf Veränderungen der Umwelt reagieren, sondern auch sowohl zur Laufzeit als auch a posteriori aus ihrem Verhalten lernen.“ (Bernard 2009:4)

⁸⁴ International Conference on Architecture of Computer Systems, ACM International Conference on Computing Frontiers, IFIP Conference on Biologically Inspired Cooperative Computing, International Conference on Autonomic and

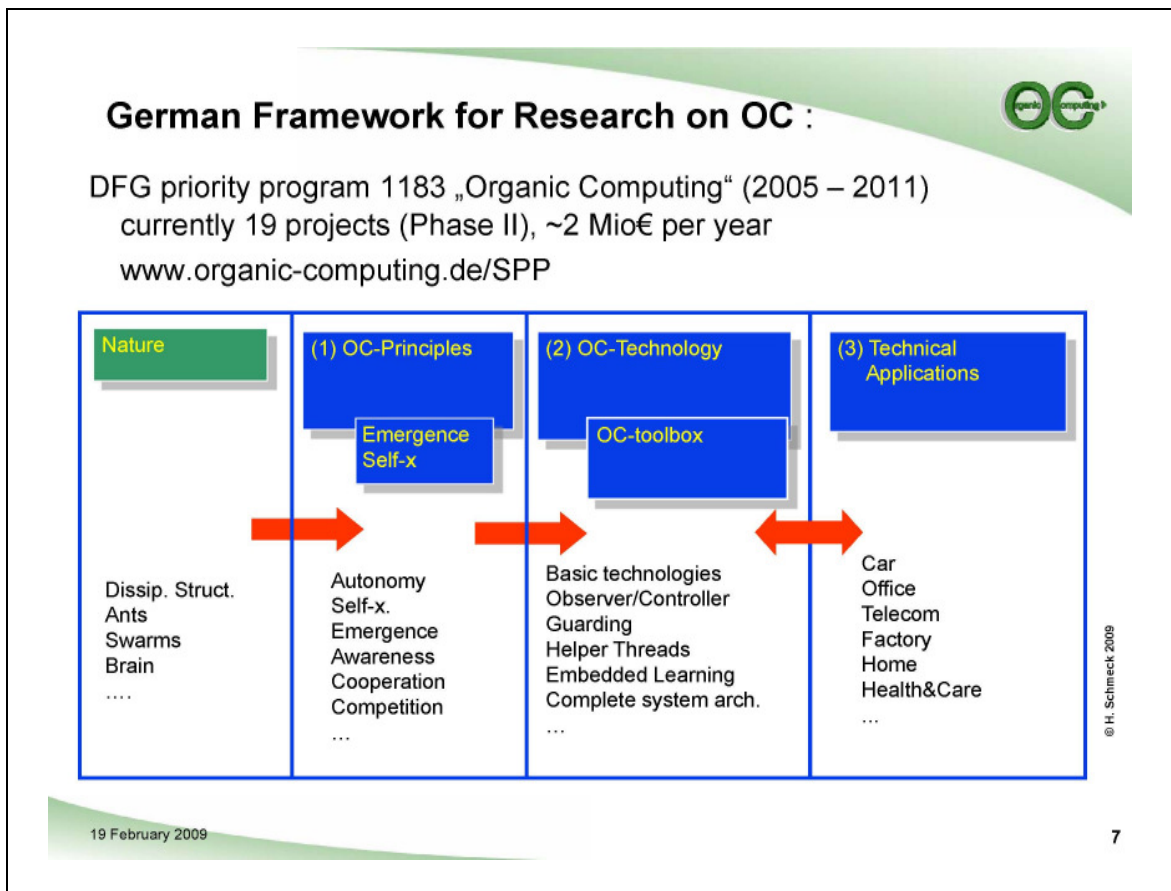


Abbildung 3.1: DFG-Schwerpunktprogramm „Organic Computing“

Quelle: Schmeck 2009a:7

Weltweit gibt es laut Aussage verschiedener Interviewpartner in Form der Entwicklung und Nutzung von smarten IT-Technologien oder von SaSo-Systemen ähnliche (exemplarische Anwendungen avisierende) Anstrengungen und Vorhaben, die aber (im Sinne alternativer Technologieentwicklungspfade) kaum in Konkurrenz zu OC stehen, sondern alle verschiedene Facetten und Themen im Bereich UC bearbeiten. Auch die Industrie ist – in zumeist eigenen FE-Projekten – in die Entwicklung von SaSo-Systemen involviert. Gleiches gilt für die NASA, z.B. bei der Entwicklung von den Asteroidengürtel erforschenden Satelliten, die zu Ausweichmanövern fähig sein müssen.

Was (noch) weitgehend fehlt, ist eine ausreichende Vernetzung mit diversen analogen Aktivitäten, die sich im Rahmen eigener technischer Fach- und Problemgemeinschaften etwa mit lernenden Systemen, Selbststeuerung und -reparatur, Systemarchitekturen, Maschinenlernen, AC, Multi-Agenten-Systemen (MAS), neuronalen Netzwerken, evolutionären Algorithmen (vgl. Branke/Schmeck 2002) oder klassischer Regelungstechnik befassen. Wie bereits das Beispiel des DFG Schwerpunktprogramms „Organic Computing“ zeigt, ist eine solche Vernetzung allerdings

schon aus Gründen begrenzter Informations- und Kommunikationskapazitäten der jeweils involvierten Forschergruppen nur eingeschränkt und selektiv realisierbar und zu erwarten.

Anwendungen und Akteurkonstellationen

Als Querschnittstechnologie hat OC (nach Einschätzung seiner Proponenten) Potenzial in vielen Bereichen. Wie bereits erwähnt betreffen Anwendungsszenarien etwa Verkehr, Energie, Netzwerke, Produktionssysteme, Logistik.

In seiner derzeitigen frühen Entwicklungsphase stellen sich den beteiligten Akteuren durchaus auch grundsätzliche substanzielle Fragen wie:

- OC soll das Leben für die Menschen leichter machen. Dafür gibt es bisher aber nur vorläufige Indizien. Kann OC diesbezüglich wirklich etwas erreichen?
- Kann OC für konkrete Anwendungen entsprechend designt werden?
- Ist OC konventionellen Lösungen überlegen?
- Lässt sich das bei OC gegebene doppelte Mikro-Makro-Problem lösen? Das Format von Emergenz stellt ein Mikro→Makro-Problem dar, während es sich bei der Umsetzung von OC (in geeigneten Rechnerarchitekturen und Software) um ein Makro→Mikro-Problem handelt.

Ebenso sind die für frühe Phasen der Technikgenese typischen Probleme der Gewinnung überzeugender und durchsetzungsfähiger Fach- und Machtpromotoren offenkundig. So gibt es einen technikinternen, aber keinen öffentlichen Diskurs um OC, in dem neben Design- und Methodenfragen auch die Überzeugung von Entscheidungsträgern in Unternehmen eine wichtige Rolle spielt, während mögliche (öffentliche) Akzeptanzprobleme und Technikskepsis insbesondere das mögliche (unzureichend kontrollierbare) Eigenleben von IT-Systemen betreffen könnten, aber vorerst nicht virulent sind. Aus Sicht der OC-Proponenten geht es also (in den kommenden Jahren) wesentlich darum, Entscheidungsträger in Unternehmen vom enormen Potenzial von OC zu überzeugen. Wenn OC substanziell verstanden würde, würde es auch akzeptiert und umgesetzt werden. Es werde aber wohl noch eine Entwicklergeneration brauchen, bis OC sich bestenfalls in 10-15 Jahren durchsetzen könne, weil die heutigen technikrelevanten Entscheidungsträger noch dem alten Paradigma der klassischen Automatisierungstechnik verhaftet seien und daher entsprechende Abwehrmechanismen aufwiesen.

In jedem Fall sei exemplarisch zu zeigen, dass OC bei konkreten Anwendungen in der Praxis funktioniert. Universitätsinstitute verfügten aber nicht über die hierfür erforderlichen Ressourcen. Die Forschungs- und Technologiepolitik könnte durch ein entsprechendes weiteres OC-Forschungsprogramm (wie bei jeder neuen Technologie) den Anstoß geben, dass sich die Akzeptanz potenzieller OC-Anwender erhöht. Wenn etwa das BMWi OC in großem Maßstab wollte und förderte, dann könnte es sich durchsetzen. So könnten z.B. OC-Systeme dann an einem realen praxisrelevanten Demonstrator getestet und Fragen bis hin zur Produkthaftung geklärt werden, so dass eine raschere Umsetzung möglich wäre; denn OC-Methoden und -Verfahren müssten prinzipiell TÜV-abnahmefähig sein, um beispielsweise für die Kfz-Industrie akzeptabel zu sein. Bisher gibt es für OC als ein junges Feld erwartungsgemäß noch keine Normen und Standards. Es exis-

tieren nur domänenbezogene Standards. – Ein Schlüsselproblem ist das Haftungsrecht.⁸⁵ Da hier eine bidirektionale Verfolgbarkeit⁸⁶ (traceability) notwendig ist, scheiden viele konventionelle Methoden aus.

Falls OC etwa in der Autoindustrie und in der Medizintechnik anerkannt und eingesetzt würde, dann würde sein Durchbruch voraussichtlich rascher und in vielen weiteren Anwendungsbereichen stattfinden. Klein- und Mittelunternehmen könnten dann auch leichter problembezogene Forschungsk Kooperationen eingehen.

3.2 Übersicht über laufende OC Projekte

In der derzeit laufenden Phase II des DFG-Schwerpunktprogramms ‚Organic Computing‘ (2005-2011) werden (neben seiner notwendigen Koordination und diesbezüglichen Tagungsorganisation) nachfolgende 20 Projekte mit insgesamt 12 Mio. € gefördert (vgl. DFG 2009, Schmeck 2009a):

- 1) Model-driven Development of Self-organizing Control Applications (TU Berlin, Universität Duisburg-Essen)
- 2) Organic Fault-Tolerant Control Architecture for Robotic Applications (Universität Lübeck, Universität Osnabrück, Fraunhofer Institut Autonome Intelligente Systeme (AIS) St. Augustin)
- 3) Smart Teams: Local Distributed Strategies for Self-Organizing Robotic Exploration Teams (Universität Paderborn)
- 4) Formal Modeling, Safety Analysis, and Verification of Organic Computing Applications (SAVE ORCA) (Universität Augsburg)
- 5) Embedded Performance Analysis for Organic Computing (TU Braunschweig)
- 6) Observation and Control of Collaborative Systems (OCCS) (Universität Hannover, Universität Karlsruhe)
- 7) Organic Traffic Control Collaborative (OTC²) (Universität Hannover, Universität Karlsruhe)
- 8) A Distributed and Self-Regulating Approach for Organizing a Large System of Mobile Objects (AUTONOMOS) (TU Braunschweig, Universität Lübeck)
- 9) Organisation and Control of Self-Organizing Systems in Technical Compounds (Universität Leipzig)
- 10) Architecture and Design Methodology for Autonomic Systems on Chip (ASoC) (Universität Tübingen, TU München)
- 11) Multi-Objective Intrinsic Evolution of Embedded Systems (MOVES) (Universität Paderborn)
- 12) Organic Computing Middleware for Ubiquitous Environment (Universität Augsburg)

⁸⁵ So hat begrenzte Automatisierung und Selbstorganisation z.B. auch haftungsrechtliche Gründe. So muss beispielsweise der Fahrer beim automatisierten Einparken noch Gas geben oder bremsen, um für Unfälle verantwortlich zu sein, obwohl genau dies technisch nicht mehr notwendig wäre.

⁸⁶ Was hat das System gelernt und wie hat es funktioniert? Bestehen Kunstfehler?

- 13) The Bio-chemical Information Processing Metaphor as a Programming Paradigm for Organic Computing (Universität Jena)
- 14) Energy Aware Self Organized Communication in Complex Networks (Universität Rostock)
- 15) Generic Emergent Computing in Chip Architectures (Universität Jena)
- 16) On-line Fusion of Functional Knowledge within Distributed Sensor Networks (Universität Passau)
- 17) A Modular Approach for Evolving Societies of Learning Autonomous Systems (Universität Paderborn)
- 18) Digital On-Demand Computing Organism for Real-Time Systems (Universität Karlsruhe)
- 19) Organic Self-organizing Bus-based Communication Systems (Universität Erlangen)
- 20) Learning to Look at Humans (Development of methods for autonomous extraction of structure from moving images by means of learning and self-organization) (Universität Bochum)
- 21) Coordination and infrastructure, task forces and status colloquiums of the DFG-Priority Program (1183) "Organic Computing".

In diesen Vorhaben wurden etwa bislang Fortschritte und Ergebnisse in folgenden Punkten erzielt (vgl. Schmeck 2009a:9-14):

- Bestimmung und Klassifizierung von Emergenz in selbstorganisierenden Systemen
- Bestimmung der Grundeigenschaften von OC-Systemen
- Design einer generischen Observer/Controller-Architektur
- Design generischer OC-middleware Komponenten
- Autonome/organische Systeme auf Chips
- Sicherheitsanalyse und –nachweis von OC-Anwendungen
- Formale Definition und Modellierung von Systemen mit Selbst-X-Eigenschaften
- Selbstorganisierende Algorithmen für Anwendungen von OC
- Design eines selbstkonfigurierenden und selbstheilenden Roboters
- Integrierte Performanzanalyse von OC-Systemen mithilfe einer Observer/Controller-Architektur
- Energie- und ressourcenbewusste selbstorganisierte Kommunikation und Kooperation (smarte Teams, Sensor-Netzwerke)
- Systematische Untersuchung von selbstorganisierenden Systemen in der Natur
- Anwendung von OC-Prinzipien im Verkehr
- Prinzipien, Methoden und Architekturen für eine evolutionäre Selbstadaptation an Realwelt-Probleme
- Prinzipien von Zusammenarbeit, Koordination und Lernen in Multi-Agenten-Systemen
- Analyse emergenten Verhaltens in sich herausbildenden Gruppen lernender autonomer Systeme
- Lernalgorithmen zum Auffinden und Verfolgen sich bewegender Menschen in Video-Sequenzen und zur Wiedererkennung von Individuen.

In der nun laufenden Phase III (2009-2011) des DFG-Schwerpunktprogramms werden noch 18 Forschungsprojekte gefördert, wobei es sich überwiegend um die Fortsetzung bereits geförderter Projekte handelt und gegenüber der Phase II 2 neue Vorhaben hinzugekommen sind: (1) Organic Self-organizing Bus-based Communication Systems (Universität Erlangen) und (2) Emergent radio: Emergent strategies to optimize collaborative transmission schemes (TU Braunschweig, KIT), (vgl. Schmeck 2009b)

Ohne diese Vorhaben hier näher zu beschreiben (vgl. <http://www.organic-computing.de/SPP>), wird doch deutlich, (1) dass sie ein breites Spektrum an unterschiedlichen, für OC(-Anwendungen) bedeutsamen Fragestellungen und Problemlösungen abdecken, (2) dass das DFG-Schwerpunktprogramm eine bewusst auf Austausch und Kooperation abzielende Zusammenfassung diverser SaSo-Themen und -Systeme untersuchender Forschungsvorhaben unter dem Etikett OC darstellt, und (3) dass es sich dabei primär um erste Versuche der genauen Analyse, Modellierung und prototypischen Anwendung von OC-Systemen handelt.

Neben generischen OC-Projekten gibt es zum einen in der DFG thematisch verwandte Sonderforschungsbereiche und Schwerpunktprogramme:

- SFB 614: Selbstoptimierende Systeme des Maschinenbaus
- SFB 368: Autonome Produktionszellen
- SFB 627: Umgebungsmodelle für mobile kontextbezogene Systeme
- SPP 1102: Adaptivität in heterogenen Kommunikationsnetzen mit drahtlosem Zugang
- SPP 1125: Kooperierende Teams mobiler Roboter in dynamischen Umgebungen
- SPP 114: Basissoftware für selbstorganisierende Infrastrukturen für vernetzte mobile Systeme
- SPP 1148: Rekonfigurierbare Rechensysteme
- SPP-Antrag: System und Anwendungssoftware für Sensornetze

Zum anderen gibt es insbesondere im Energie-IT-Bereich große, für OC relevante FE-Projekte über ca. 20 Mio. €, die u.a. am KIT (Karlsruhe Institute for Technology) verfolgt werden und sich mit der Optimierung von Energieverteilung und Energiespeicherung befassen, wie das im Rahmen des BMBF-Förderprogramms „Internetökonomie“ geförderte Verbundvorhaben zur „Selbstorganisation und Spontaneität in liberalisierten und harmonisierten Märkten“.

Ebenso werden im EU-FET Forschungsbereich „Complex Systems“ seit kurzem mehrere Forschungsprojekte gefördert, deren Themen einen deutlichen Bezug zum Organic Computing haben:

- BISON - Biology-Inspired techniques for Self-Organization in dynamic Networks
- COSIN - Coevolution and Self-Organization In dynamical Networks
- ISCOM - The Information Society as a Complex System
- LEURRE - Artificial Life Control in Mixed-Societies
- POETIC - Reconfigurable Poetic Tissue
- SOCIAL - Self Organised Societies of connectionist Intelligent Agents capable of Learning
- SWARM-BOTS - Swarms of self-assembling artefacts

Das DFG-Schwerpunktprogramm Organic Computing unterscheidet sich dabei von diesen Forschungsprojekten durch seine strenge Ausrichtung auf Möglichkeiten der Anwendung von Prinzipien der Selbstorganisation in technischen Systemen in Verbindung mit der dynamischen Anpassung der Funktionalität dieser Systeme insbesondere an Anforderungen menschlicher Nutzer.

Ergänzend sei schließlich nochmals festgehalten, dass sich – wenn auch nicht unter dem Oberbegriff OC – auch in der Industrie eine Reihe von Projekten finden lassen, die ähnliche Zielsetzungen verfolgen, aber im Rahmen dieses Vorhabens nicht weiter recherchiert wurden.

3.3 Marktanalyse und Bedingungen der Markteinführung

Bei OC-Entwicklungen geht es wesentlich darum, Software mit den Eigenschaften Selbstorganisation und dezentrale Steuerbarkeit zu entwickeln. Für die Marktperspektiven von OC sind deshalb vor allem folgende Gesichtspunkte von Belang (vgl. Petschow et al. 2009:73ff):

- 1) OC-Anwendungen gehören zum Bereich der Informations- und Kommunikationstechnologien (IuK), deren Anteil an der gesamten Wertschöpfung vorerst weiterhin wächst. IuK-Märkte werden in Produktions- und Dienstleistungsmärkte (ICT manufacturing und ICT services) unterteilt, die sich nach Eurostat aus folgenden Branchen zusammensetzen (EU-Commission 2006:130): office machinery and computers, insulated wire, electronic valves and tubes, telecommunications equipments, radio and TV receivers, scientific instruments; telecommunications, computer and related activities. 2005 betrug das Volumen des IuK-Marktes der EU ca. 600 Mrd. €, wobei Übertragungsdienstleistungen mit 43% Anteil am Gesamtumsatz die bedeutendste Rolle spielten und Software mit 11% einen verhältnismäßig kleinen Marktanteil besaß (EU-Commission 2006:131).⁸⁷
- 2) Das Interessante an den Anwendungen der OC-Forschung liegt jedoch weniger in der Tatsache, dass sie den Software-Markt um neue Software-Arten ergänzen werden. Vielmehr gehören OC-Anwendungen zu so genannten ‚befähigenden Technologien‘ (enabling oder general purpose technologies) gehören, die andere Technologien zu neuen Eigenschaften befähigen. Damit ergibt sich die ökonomische Relevanz von befähigenden Technologien nicht nur aus ihrem Marktwert, sondern auch aus ihrem Beitrag zur Wertschöpfung der Technologien, die sie technisch und wirtschaftlich mit ermöglichen.⁸⁸ Zu beachten ist im Hinblick auf die Marktperspektiven von OC, dass nicht nur OC-Software, sondern Software generell als ‚general purpose technology‘ angesehen wird. So betrug in 2002 in einer Reihe technologieintensiver Branchen (Fahrzeuge, Konsumelektronik, medizinische Ausstattung, Telekommunikationsausrüstung, Automatisierungstechnik, Raumfahrt) der Anteil der Entwicklungsausgaben für Software-Entwicklung zwischen 10% (Automatisierungstechnik) und 52% (Telekommunikation) und überstieg mit 58 Mrd. € die entsprechenden Entwicklungsaufwendungen von Software-Unternehmen und -Dienstleistern mit weltweit 40 Mrd. € deutlich. Für 2015 ist mit einem Anteil

⁸⁷ Zu Übertragungsdienstleistungen zählen Fest- und Mobilnetzdatenübertragungen, zu Software zählen Software und Software-Infrastruktur.

⁸⁸ So wird OC-Software in Ampelanlagen den Softwaremarkt zwar nur gering beeinflussen, könnte jedoch die Lichtsignal-Märkte enorm verändern. (vgl. Pissarskoi 2009:2)

von 15% bis 65% zu rechnen (vgl. TNO/IDATE 2006:41ff). Somit lässt sich *cum grano salis* festhalten, dass Software-Entwicklung einen bedeutenden Teil zur Wertschöpfung aller Branchen beiträgt und dass IuK-Technologien als ‚general purpose technologies‘ in den letzten Jahren zum Anstieg der Produktivität beigetragen haben.

- 3) Zwei technologische Trends tragen zur Realisierung von Weisers (1991) Vision des ubiquitous computing bei. Der eine Trend resultiert aus der Miniaturisierung der Prozessoreinheiten und der Steigerung der Rechengeschwindigkeiten. Sehr kleine und schnelle Prozessoren können in immer mehr Dingen eingebaut werden und immer mehr Daten berechnen. Werden diese Dinge mit einer Software ausgestattet, die es ihnen erlaubt, mit anderen Dingen Daten auszutauschen, entsteht die erste Stufe von smarten oder intelligenten technischen Geräten, sodass diese durch die durchgängige Verfügbarkeit und Vernetztheit von informationsverarbeitenden Technologien immer mehr über smarte bzw. intelligente Eigenschaften verfügen.
- 4) Der zweite Trend wird mit dem Oberbegriff ‚converging technologies‘ beschrieben⁸⁹, wonach verschiedene befähigende Technologien miteinander verknüpft werden, um weitergehende (technologische) Ziele zu erreichen (vgl. University of Twente 2009). Während dies auf der Ebene relevanter wissenschaftlicher Gebiete die multi- und transdisziplinäre Verknüpfung von Informatik, Kognitionswissenschaften, Biotechnologie, Nanotechnologie und Materialwissenschaften betrifft (vgl. Lieshout et al. 2006), geht es auf der Ebene ingenieurwissenschaftlicher-technischer Entwicklung darum, mithilfe intelligenter, selbstorganisierender, biokompatibler, anpassungsfähiger technologischer Lösungen neue Anwendungsmöglichkeiten zu realisieren, wobei sich Ingenieurwissenschaftler nach Minai et al. (2006) von der Entwicklung immer komplizierterer technischer Systeme hin zu komplexen (selbstorganisierenden) Systemen umorientieren sollten.
- 5) Im Ergebnis dürften beide Trends die ökonomische Bedeutung der IuK-Technologien weiter erhöhen. Denn die IuK-Anwendungen sollen wesentliche Bausteine zu der Smartheit der Dinge liefern, nämlich datenverarbeitende und kommunizierende Systeme. Insofern OC gerade auf die Realisierung selbstadaptiver selbstorganisierender Systeme mit kontrollierter Emergenz abzielt, sollten sich diese technologischen Trends vorteilhaft auf seine Marktperspektiven auswirken, weil die Bewältigung der Herausforderungen der Informationsgesellschaft auf ebensolche adaptiven Techniken und die Möglichkeit dynamischer Konfiguration einer Vielzahl von Sensoren angewiesen ist (vgl. ISTAG 2004).
- 6) Zur adäquaten Einschätzung des ökonomischen Potenzials einer Technologie sind zum einen mögliche konkurrierende technologische Entwicklungen zu berücksichtigen. Zum gegenwärtigen Zeitpunkt sind in dieser Hinsicht zwar unterschiedliche konkrete OC-Vorhaben und gleichfalls auf smarte IT-Systeme abzielende (spezifisch ausgerichtetere industrielle) OC-affine Entwicklungen (z.B. autonomic computing), jedoch keine in ihrer technischen Grundkonzeption alternativen Technologien erkennbar, sodass es bislang – bei konkreten anwendungsorientierten (Demonstrations-)Vorhaben – eher um die Optimierung von noch in relativ frühen Entwicklungsstadien befindlichen OC-Systemen gehen dürfte als um konkurrierende smarte IT-Systeme, wenn man einmal von der typischen Konkurrenz um notwendige Fördermittel absieht.

⁸⁹ Grundsätzlich wurden Technologiekonvergenzen, z.B. von Informations- und Kommunikationstechnologien oder von Biologie und Mikrotechnologie bereits in vorangegangenen Jahrzehnten bemerkt (vgl. Tofter 1980, Castells 1996).

- 7) Zum ändern muss sich eine neue Technologie gegenüber bereits bestehenden technischen Problemlösungen durchsetzen, die üblicherweise aufgrund entsprechender vested interests und sunk costs eine vor allem anfangs starke Position gegenüber einer konkurrierenden neuen Technologie innehaben, sodass sie sich im Allgemeinen, wie eingangs festgehalten, nur dann erfolgreich auf dem Markt zu etablieren vermag, wenn sie sich wie gesagt sowohl im Hinblick auf ihre technischen Reife und Zuverlässigkeit, ihre relativen Kostenvorteile, ihre Sicherheit für Hersteller, Nutzer und Drittparteien, der Bandbreite ihrer möglichen Anwendungen und ihre Umweltverträglichkeit als überlegen erweist als auch die Machtposition ihrer Promotoren und Implementatoren stark genug und ihre gesellschaftliche Akzeptanz gewährleistet ist. Diese Voraussetzungen sind gegenwärtig noch kaum gegeben. Zum einen bestehen teils noch nicht gelöste Herausforderungen, da sich OC trotz seiner Ausrichtung auf technologische Anwendungen noch weitgehend im Stadium grundlagenorientierter Forschung befindet. Denn in jedem Fall ist zu zeigen, dass OC bei konkreten Anwendungen in der Praxis funktioniert. So ist für eine breite Nutzung von selbstorganisierenden Technologien von zentraler Bedeutung, dass die Anwendungen trotz ihrer Fähigkeit zur Selbstorganisation steuerbar bzw. kontrollierbar bleiben. In dieser Hinsicht sehen die Informatiker selbst noch erheblichen Forschungsbedarf (vgl. Gesellschaft für Informatik et al. 2008, Müller-Schloer/Sick 2008). Zweitens erfordert die Realisierung von adaptiven und dezentral gesteuerten technischen Systemen, dass die Kommunikationsmechanismen zwischen den einzelnen Informationsträgern vereinheitlicht werden, was die Definition von einheitlichen Schnittstellen und Protokollen, Ein- und Ausgabemechanismen, flexible Middleware erfordert. Gerade sicherheitsrelevante Anwendungen wie in der Automobilindustrie sind aber mit bestimmten festen Normen und Standards verknüpft, die die Einführung von adaptiven und flexiblen Steuerungsinstrumenten erschweren. Drittens sind relative Kostenvorteile zwar für einzelne Anwendungen als zu erwarten begründbar, aber schon aufgrund bislang fehlender Umsetzung in der Praxis nicht nachweisbar. Ebenso sind die Bandbreite der möglichen Anwendungen und die Umweltverträglichkeit von OC zwar theoretisch belegt, aber nicht praktisch realisiert.⁹⁰
- 8) Sozial sind Anwendungen von OC (gerade als befähigender Technologie) auf ihre Einbettung in bestehende oder gleichfalls erst noch zu entwickelnde neue technische Systeme wie z.B. Ampelanlagen oder Logistik-Systeme und damit auf die Kooperation der in diese involvierten Akteure angewiesen. Die Machtposition der Promotoren und Implementatoren von OC (wissenschaftliche Arbeitsgruppen, u.U. dahinter stehende wissenschaftliche Institutionen) ist – bei häufig weitgehender Unkenntnis der OC-Initiative auf Seiten potenzieller (industrieller) Nutzer – vorerst erwartungsgemäß gering. Erst die Mitwirkung von Akteuren, die von der Sinn- und Vorteilhaftigkeit von OC in entsprechenden Anwendungsfeldern allmählich überzeugt wären, könnte mithilfe einer förderlichen Akteurkonstellation den exemplarischen Einsatz von OC-Systemen auf sozialer Ebene möglich machen. Schließlich ist bei derzeit erwartungsgemäß fehlendem öffentlichen Diskurs um OC seine gesellschaftliche Akzeptanz zwar bislang nicht in Frage gestellt, aber keineswegs gesichert.
- 9) Darüber hinaus müssen die für eine erfolgreiche Markteinführung notwendigen *anwendungsspezifischen* rechtlichen, politisch-administrativen, kulturellen, und auch infrastrukturellen Rahmenbedingungen vielfach erst noch geschaffen werden, wie das Beispiel der rechtlich bislang ungeklärten Verantwortungszuschreibung im Falle von aus unerwünschten emergenten

⁹⁰ So sind z.B. angesichts eines 2%-Anteils von IT-Systemen am Weltenergieverbrauch, was demjenigen des Flugverkehrs entspricht, mögliche Energieeinsparungen und Effizienzgewinne via OC von nicht vernachlässigbarer Größenordnung.

Effekten resultierenden Unfällen zeigt. Auch wenn im Rahmen einer gesellschaftspolitisch grundsätzlich erwünschten Entwicklung zum breiten Einsatz von smarten IT-Systemen eher selten mit grundlegenden Hemmnissen bei OC-Anwendungen zu rechnen ist, können diese im Einzelfall, z.B. im Falle eines wachsenden gesellschaftlichen Widerstands gegen intelligente Kamera(beobachtungs- und -überwachungs)systeme, eine solche durchaus blockieren oder verzögern, und sind notwendige und geeignete Rahmenbedingungen in der Praxis doch erst einmal zu schaffen.

- 10) Schließlich weisen technologische Trajektorien ihre eigene Dynamik bis hin zu Lock-in-Effekten auf, sodass eine erfolgreiche Marktdurchdringung von OC-Systemen auch von der Wahl und Gestaltung konkreter technischer Optionen abhängt. So könnten beispielsweise bei einer innerstädtischen Ampelsteuerung mithilfe von OC – neben den anfallenden Kosten – die räumliche Ausdehnung, die Wahl der Sensoren, das Ausmaß lokaler Selbstorganisation, die Festlegung der Steuerungsimperative, die Haftungsregeln im Falle von Fehlfunktionen, oder die Zulässigkeit bzw. inhärente Blockierung einer anderweitigen (unerlaubten) Nutzung der gewonnenen Verkehrsdaten maßgeblich dafür verantwortlich sein, ob ein derartiges OC-System in der Praxis sozial akzeptiert oder aber (wieder) aus dem Verkehr gezogen wird.

3.4 Entwicklungs- und Marktperspektiven von Organic Computing

Basierend auf den vorangehenden Abschnitten werden nun die Entwicklungs- und Marktperspektiven von OC zusammenfassend vorgestellt.

Nach relativ übereinstimmender Auskunft wird die vielfältige Nutzung von OC (als einer befähigenden Technologie) seitens der OC-Entwickler einerseits als in der Zukunft wahrscheinlich oder sicher, andererseits aber je nach Anwendung als noch Jahrzehnte bis zur praktischen Umsetzung benötigend eingestuft. Was die Zeithorizonte der beginnenden Vermarktung von (im Zuge der Marktpenetration noch zu verbessernden) OC-Systemen angeht, so seien für Kamerasysteme und Netzwerke ~ 5 Jahre, für Straßenverkehr, wo sich OC-Systeme erst in der Arena der bisherigen Hersteller mit dem Nachweis von wenigstens 10% Verbesserung und der Installation einer entsprechenden Infrastruktur durchsetzen müssen, mindestens 10 Jahre, für unternehmensinterne Logistik 10 - 15 Jahre, für die Fahrzeugelektronik mit sich selbst koordinierenden Teilsystemen und der Möglichkeit der Selbstheilung bei Elektronikausfall (unter Berücksichtigung der langen Entwicklungszeiten einer Fahrzeuggeneration in der Automobilindustrie) mindestens 15 Jahre, und für unternehmensübergreifende mit weiteren Transporten verbundene Logistiksysteme ~ 20 Jahre anzusetzen. Während es hier (teilweise) um einen Verdrängungswettbewerb gegenüber bereits existierenden Systemen geht, handelt es sich bei intelligenten Navigationssystemen eher um neue (SaSo-)Systeme, die keine vergleichbaren Systeme zu verdrängen brauchen.⁹¹ Die Umsetzung von OC in bereits bestehenden Systemen (mit konservativen Akteuren) dürfte hingegen mindestens 25 Jahre dauern.

⁹¹ Am Beispiel der RFID-Chips, die aus Datenschutzgründen mit politischem Gegenwind konfrontiert sind und im Prinzip bereits seit 10 - 15 Jahren verfügbar sind, wird deutlich, dass eine derartige Marktpenetration recht lange dauern kann.

So geht es etwa beim Autobau um die Nutzbarkeit und Kombinierbarkeit von Software-Komponenten seitens verschiedener Zulieferer und für verschiedene Hersteller mit entsprechender Standardisierung. All dies entwickelt sich als Infrastruktur bereits, und hierzu eignen sich passende OC-Systeme. Solche lassen sich jedoch sinnvoll nur in Kooperation von Autoherstellern, Komponentenzulieferern, Elektronikindustrie und OC-Entwicklern konzipieren, erproben und einführen, die sich jedoch selbst erst noch entwickeln muss.

Im Grunde geht es aus Sicht der OC-Proponenten (bei der Nutzung von SaSo-Systemen) um Brokerdienste, die mithilfe einer entsprechenden Infrastruktur verfügbare Datenbanken nutzen, um die gewünschten Informationen für den Nutzer bereitzustellen und zu kombinieren. All dies sei zentral (organisiert) nicht mehr möglich und bedürfe einer dezentralen technischen Infrastruktur. Dieser Entwicklungstrend und -prozess betreffe die gesamte (globalisierte) Weltwirtschaft und sei darum von riesiger Größenordnung mit Billionen € Umstellungskosten, der sich in einem Zeitrahmen von ~ 50 Jahren abspielen dürfte. OC ist hierbei nur eine Komponente im Kontext von entsprechender ICT (Information and Communication Technology) und angewandter Informatik. Bislang existiert in dieser Hinsicht aber noch kaum ein regulatorischer Rahmen.⁹²

Die Vision der Architektur eines nach 2010 realisierbaren OC-Systems beinhaltet nach Schmeck (2009a:5) mehr oder weniger die in Kapitel 2 benannten Elemente, dass es

- „will possess lifelike properties.
- will consist of autonomous and cooperating sub-systems and will work, as much as possible, in a self-organised way,
- will adapt to human needs,
- will be robust, adaptive, and flexible,
- will be controlled by objectives (“goal-driven”),
- will provide customized service in a user-friendly way,
- will be trustworthy“,

und seine Selbstorganisation ein adaptives, kontextsensitives Verhalten mit typischen Selbst-X-Eigenschaften erlaubt: „self-configuring, self-optimizing, self-healing, self-protecting, self-explaining, self-managing.“

Im Hinblick auf die oben genannten Gesichtspunkte einer Marktpenetration lässt sich festhalten:

- 1) Insofern es um wettbewerbsfähige Marktpenetration von OC-Systemen mit einem in der Tendenz eher langen Zeithorizont von ca. 10 - 30 Jahren geht, sind keine eindeutigen Prognosen möglich.

⁹² Insofern die jeweils etablierten konkreten Standards einen internationalen Wettbewerbsvorteil darstellen, interessiert sich z.B. DIN durchaus für die Entwicklungsrichtung von OC, um nach Möglichkeit den deutschen Verhältnissen entsprechende Normen als Standards durchsetzen zu können. So hat z.B. China im Ingenieur-Bereich DIN-Normen und nicht die US-amerikanischen ASA-Normen übernommen.

- 2) Zum einen ist noch offen, wie gut es gelingen wird, in diesem Sinne marktfähige Anwendungen von OC mit autonomer Selbstorganisation, Selbst-X-Eigenschaften und kontrollierter Emergenz zu realisieren.
- 3) Dabei bestehen für einfache OC-Systeme (z.B. bei der Ampelsteuerung) größere Chancen als für komplexe OC-Systeme (z.B. unternehmensübergreifende Logistik).
- 4) Relevante Aspekte von OC sind wie erwähnt bereits (in Form spezifischer Anwendungen) ausgeübte Praxis, z.B. bei ambient assisted living.⁹³ Mit der sukzessiven Ausweitung adaptiver Systeme zeichnet sich OC als Querschnittstechnologie durch seine ganzheitliche Perspektive aus. Auch von daher gibt es keinen eigenen (neuen) Markt für OC-Systeme, sondern OC spiegelt einen allgemeinen kontinuierlichen Trend (und Zwang) zum Einsatz smarter IT-Systeme zwecks Beherrschung von Komplexität wider. Dieser Trend impliziert einerseits ein großes Marktpotenzial, das aber andererseits nicht zwangsläufig durch genuine OC-Systeme ausgefüllt und erobert werden muss, sofern sie sich nicht als jeweils technisch überlegen und zugleich kostenkompetitiv erweisen sollten.
- 5) Neben der ausreichenden technischen Reife ist maßgeblich, ob der je anwendungsspezifische Einsatz von OC zu akzeptablen (wettbewerbsfähigen) Kosten der Einbettung und der Informationsbeschaffung möglich ist und auf hinreichende Nachfrage trifft.
 - Hohes ökonomisches Potenzial wird vor allem in der Realisierung von Assistenzsystemen im Gesundheits- und Lebensbereich, in der Entwicklung von Service-Robotern, die Dienstleistungen im häuslichen, aber auch im kommerziellen Bereich übernehmen, und in der Realisierung von intelligenten Automobilen gesehen (Gesellschaft für Informatik et al. 2008: 9ff).⁹⁴
 - Dabei beruht der erfolgreiche Einsatz von OC in der Autoelektronik allerdings nicht nur auf der Kooperationsbereitschaft der Autohersteller, kompatiblen Standards und geeigneten (haftungs)rechtlichen Regulierungen, sondern muss sich auch unter Bedingungen vermehrter Interferenzen von Elektroniksystemen etwa in Tunneln als robust erweisen.
 - Eine Ampelsteuerung mithilfe von OC kann bislang zumindest in Simulationen einen gegenüber herkömmlicher zentraler Ampelsteuerung verbesserten Verkehrsfluss belegen. Aber ob die Kosten überall eingelegter Sensoren sich bei über die Zeit variierenden Verkehrsverhältnissen durchweg durch besseren Verkehrsfluss amortisieren, ist eine derzeit noch gänzlich offene Frage.
 - Bei adaptiven Kamerasystemen könnte der Mehrwert gegenüber konventionellen Kamera-beobachtungssystemen – von Spezialfällen abgesehen – relativ begrenzt, im Ertrag unzureichend⁹⁵ und sogar unzulässig sein, insofern es mittelfristig vor dem Hintergrund weiterer Datenmissbrauchsskandale durchaus zu einem verbesserten Schutz von Privacy kommen kann (vgl. Kapitel 5.2). Dieses Beispiel weist darauf hin, dass technische Systeme auch

⁹³ Bei allen OC-Systemen geht es wie gesagt zumeist um Lernen, genetische und evolutionäre Algorithmen, Learning-Classifizier-Systeme.

⁹⁴ Alle diese Ziele sind auf selbstorganisierende, adaptive Techniken und die Möglichkeit dynamischer Konfiguration einer Vielzahl von Sensoren angewiesen.

⁹⁵ Wer wertet auf Dauer stets all die durch aufwändigere Kamerabeobachtungssysteme gewonnenen Daten aus, solange diese nicht selbst autonom über deren Nutzen entscheiden können?

durch sinkende Ertragsgewinne infolge nicht benötigter Überkapazität an mangelnder Nachfrage scheitern können.

- In der Logistik dürfte sich der Einsatz von OC im Falle technischer Überlegenheit und veringertener Lagerhaltungskosten grundsätzlich lohnen. Aber auch hier hängt der relative Kostenvorteil ausgeklügelter Produktions- und Lagerhaltungssysteme von den langfristigen Transport- und Lagerhaltungskosten dergestalt ab, dass nämlich räumlich aufwändige Transportsysteme und just-in-time Lagerhaltung ökonomisch vorteilhaft bleiben.
 - Günstige Marktperspektiven dürften im technischen und wirtschaftlichen Erfolgsfall für autonome On-Chip-Systeme bestehen (vgl. Bernauer et al. 2008), der allerdings bislang nicht gesichert ist.
 - OC hat im Falle voraussichtlich erreichbarer technischer und wirtschaftlicher Vorteilhaftigkeit mittelfristig auch gute Chancen bei der Energieverteilung, um je nach Bedarf einzelne Kraftwerke an- und abzuschalten, oder bei der Energiespeicherung, um sie z.B. in Batterien von Elektroautos zu optimieren oder die Energienutzung von Elektrogeräten wie Kühlschränke zeitlich zu steuern.⁹⁶ Die diesbezüglichen Kosten wären gering, da diese Informationen als Zusatzinformationen auf den Stromimpuls aufgesetzt würden.
- 6) Innovationen setzen sich wie gesagt nicht zwangsläufig aufgrund technischer und ökonomischer Überlegenheit durch, insofern zumeist Optimierungsmöglichkeiten bestehender Technologielinien bestehen und Technologien durch Pfad- und Zeitabhängigkeiten gekennzeichnet sind, weshalb beispielsweise Markteinführungsstrategien und Leitmärkte (lead markets) eine wichtige Rolle spielen (können). Deshalb hängen die Marktperspektiven von OC (darüber hinaus) entscheidend davon ab, ob OC-Systeme die (anwendungsspezifischen) Filter geeigneter sozialstruktureller Rahmenbedingungen und Akteurkonstellationen mit ihren vorherrschenden Interessenberücksichtigungsmustern passieren. Damit ist durchaus zu rechnen, solange keine OC direkt zurechenbaren Negativeffekte auftreten (wie z.B. jüngst beobachtete Risiken von Nano-Partikeln (vgl. Umweltbundesamt 2009)). Dennoch ist offen, ob dies tatsächlich geschehen wird. Sofern die maßgeblichen Akteure OC mehrheitlich als vorteilhaft und (für sie) nützlich wahrnehmen, ist daher bei Gewährleistung der bestehenden Sicherheits- und haftungsrechtlichen Anforderungen (vgl. Kapitel 7) mit keiner prinzipiellen Blockade seiner (anwendungsbezogenen) Marktpenetration zu rechnen; jedoch können situative, heute nicht prognostizierbare Umstände bestimmen, ob dies tatsächlich geschieht.
- 7) Welche konkrete Innovationsdynamik und welche Technologiepfade sich in Bezug auf OC herausbilden, ist noch völlig offen, z.B. ob kleine oder große Unternehmen dominieren werden. Am ehesten könnten zunächst kleine Firmen in gänzlich neuen (vermuteten) Anwendungsbereichen zentrale Player werden.
- 8) In diesem Zusammenhang ist das Vertrauen in OC-Systeme entscheidend (vgl. André et al. 2009), wie z.B. der Bereich des Cloud Computing deutlich macht, wo man (virtuell) jeweils gerade verfügbare Rechner nutzt, ohne zu wissen, um welche Rechner es sich jeweils handelt.⁹⁷ – Bislang gelingt etwa die Einbindung von (OC in der Praxis realisieren wollenden) Industrieun-

⁹⁶ Während dies bei Kühlschränken in Haushalten vermutlich kaum Kosteneinsparungen mit sich brächte, täte es dies bei Kühlgeräten in Unternehmen und Organisationen sehr wohl.

⁹⁷ Beim Grid Computing geht es hingegen nur um die (gleichzeitige) Nutzung bestimmter externer Rechner.

ternehmen nur sehr begrenzt. Die Industrie sträubt sich vorerst, in OC zu investieren, und entsprechende Kontakte und Bemühungen waren vergeblich.⁹⁸

- 9) Fragen der Umweltverträglichkeit, der Sozialverträglichkeit und der Nachhaltigkeit von OC sind bislang kaum ein Thema, soweit es nicht explizit z.B. um Energieeinsparung oder Verhinderung von Datenmissbrauch geht.⁹⁹ Im Hinblick auf die soziokulturelle Akzeptanz von OC kann sich dies noch als Einführungshemmnis erweisen, muss es aber nicht.

Im Ergebnis ist also mit einer allmählichen (teils impliziten) Marktpenetration von OC zu rechnen, wobei über das Ausmaß und die alternative Marktdurchdringung funktional äquivalenter SaSo-Systeme zum heutigen Zeitpunkt noch keine Aussagen möglich sind, die allerdings in Deutschland – abgesehen von möglichen, dem Autor nicht bekannten Vorhaben von Industrieunternehmen – bislang keine bedeutsame, OC vergleichbare Rolle zu spielen scheinen.

⁹⁸ Hierfür sind vermutlich bislang fehlende Nachweise erfolgreicher Praxis in Demonstrationsvorhaben, die Notwendigkeit der Einführung neuer Standards oder gar Systeme in der Produktion, zu erwartende beträchtliche Umstellungskosten etablierter Produktionssysteme, und die Präferenz für funktionierende Herstellungsroutinen verantwortlich.

⁹⁹ Nachhaltigkeit ist vor allem ein Thema der Anwendung. OC kann indirekt zu ihr beitragen, indem es qua Selbstoptimierung und interner Anpassung eines technischen Systems sowohl den Ressourcenverbrauch minimiert als auch größere Fertigungstoleranzen bei der Herstellung zulässt, mit der Folge geringeren Ausschusses.

4 Chancen und Risiken selbstorganisierender adaptiver Systeme

4.1 Analyseraster

Nachdem in Kapitel 3 die Entwicklungs- und Marktperspektiven von OC thematisiert wurden, geht es in diesem Kapitel allgemein um Chancen und Risiken von OC.

Angesichts der in Kapitel 2 beschriebenen Gegebenheiten¹⁰⁰ sollte ein Analyseraster der Chancen und Risiken von OC pragmatisch aufgebaut sein. Chancen und Risiken ergeben sich einerseits aus seinen Anwendungspotenzialen und Marktperspektiven und andererseits aus seiner Selbstorganisation, Autonomie und deren Schwachstellen, betreffen jedoch noch weitere von dem Analyseraster abzudeckende Aspekte.

- 1) Chancen und Risiken werden als allgemeine (weiche) Begriffe genutzt, die normativ auf als positive Potenziale (Nutzungsmöglichkeiten) eingestuft (im Prinzip intendierten) Chancen bzw. auf die als negative Potenziale (unerwünschte Effekte und Folgewirkungen) bewerteten (im Prinzip nicht intendierten) Risiken abheben.¹⁰¹ Chancen und Risiken sind analog wie Vor- und Nachteile sehr allgemein gehaltene Begriffe, die erst durch ihre Spezifizierung und inhaltliche Ausfüllung in Bezug auf Angaben ihrer Nutznießer und Betroffenen, ihrer Art und Modi, ihrer Reichweite und Größenordnung etc. Relevanz erlangen.¹⁰² Bei der Analyse von Chancen und Risiken (von OC) wird die alte Regel bestätigt, dass diese konkret erst in der Einbettung und Wechselwirkung von technischen Systemen in/mit den sie umgebenden und nutzenden sozialen Akteuren und Systemen ausreichend identifiziert und verstanden werden können. Dies schließt die Formulierung von (erweiterten und vorsorgezentrierten) Risikomanagementstrategien und Gestaltungsansätzen nicht aus, die dann in differenzierter Form typische Aspekte von Risiken und Risikomanagement beachten (vgl. Renn 2008). Maßgeblich für die jeweiligen konkreten Chancen und Risiken von OC dürfte somit deren (fallspezifische) Sozialdimension sein.¹⁰³
- 2) Im Sinne eines in seiner Grundstruktur einfachen Analyserasters sei auf allgemeiner Ebene analytisch in einer Vierfeldertafel nur zwischen Chancen und Risiken in ihrer technischen und ihrer sozialen Dimension unterschieden (Tabelle 4.1), wobei die Chancen und Risiken von OC

¹⁰⁰ OC stellt keine eigenständige Technologie dar, befindet sich noch in der Forschungs- und Entwicklungsphase und ist eingebettet in technische Systeme mit der Folge anwendungsspezifischer Chancen und Risiken.

¹⁰¹ Auf die soziologische Diskussion und kommunikationstheoretische Einbettung des Risikobegriffs (informationstheoretischer, entscheidungstheoretischer, psychologischer, kulturtheoretischer, systemtheoretischer Risikobegriff), seine Unterscheidung vom Begriff der Gefahr und unterschiedliche (sozialwissenschaftliche) Risikotheorien soll hier nicht weiter eingegangen werden (vgl. Bechmann 1993, Beck 1986, Bora 2004, Conrad 1980, Japp 1996, Luhmann 1991).

¹⁰² Dabei sind Risiken bei selbstorganisierenden Systemen systeminhärent bedingt nicht allzu genau abschätzbar.

¹⁰³ Hierbei ist in Rechnung zu stellen, dass das, was für den einen eine Chance darstellt, für den anderen ein Risiko sein kann, und dies abhängig von den jeweiligen Wertmaßstäben (vgl. das Beispiel adaptiver Kamerasysteme in Kapitel 5.2). Zudem können spezifische Chancen (zwingend) mit bestimmten Risiken verbunden sein (z.B. bei Aktienspekulation).

jeweils differenziert nach positiven oder negativen (technischen) Potenzialen, der jeweiligen Gruppe von Anwendungsfällen und konkreten Fallbeispielen, als auch nach räumlicher Verteilung¹⁰⁴, zeitlicher Perspektive¹⁰⁵ und Spezifität¹⁰⁶ zu charakterisieren wären.

Tabelle 4.1: Analytisches Modell der Chancen und Risiken von OC

Technische Chancen	Technische Risiken
Soziale Chancen	Soziale Risiken

- 3) In der technischen Dimension ist zwischen technischen Potenzialen bzw. technischen Fehlfunktionsrisiken, spezifischen Anwendungs- und Nutzungsformen und -möglichkeiten bzw. Fehlbedienungs- und Fehlnutzungsrisiken, (neuartigen) experimentellen Optionen und Entwicklungen bzw. (intentionalen) Missbrauchsrisiken, sowie systeminhärenten (Komplexitäts-)Chancen bzw. (Komplexitäts-)Risiken¹⁰⁷ zu unterscheiden (Tabelle 4.2). Diese Unterscheidung hebt die Differenz zwischen grundsätzlich vorhandenen Chancen als auch Risiken, deren substantieller Realisierung in je anwendungs- und nutzungsspezifischen OC-Systemen, den im jeweiligen OC-Systemdesign zunächst einmal nicht intendierten Erweiterungs- und Missbrauchsmöglichkeiten und den systeminhärenten (letztlich nicht mehr kontrollierbaren) Entwicklungschancen und -risiken hervor.

Tabelle 4.2: Dimensionen technischer Chancen und Risiken

Technische Chancen	Technische Risiken
technische Potenziale	technische Fehlfunktionsrisiken
Anwendungs- und Nutzungsmöglichkeiten	Fehlbedienungs-/nutzungsrisiken
experimentelle Optionen	Missbrauchsrisiken
systeminhärente (Komplexitäts-)Chancen	systeminhärente (Komplexitäts-)Risiken

- 4) Die Sozialdimension kann nun ihrerseits analytisch als erweiterte Soziosphäre aufgegliedert und dargestellt werden (vgl. Abbildung 4.1). Sie erlaubt es, jeweils nach der psychischen, semiotisch-symbolischen, normativen, ordinativen, allokativen, operativen und physisch-

¹⁰⁴ So lassen sich lokale (wenige) versus globale (viele Personen oder Organisationseinheiten betreffende) Risiken unterscheiden. Erstere dürften bei (ubiquitären) Informationssystemen selten vorkommen, wohingegen sie keineswegs überall einzutreten brauchen und bei lokalem Eintritt auch durch Gegenmaßnahmen in ihrer Ausbreitung begrenzt werden können (z.B. Warnung vor neuartigen Viren).

¹⁰⁵ So kann man grob zeitnahe (und zeitlich begrenzte) von langfristigen Chancen und Risiken unterscheiden.

¹⁰⁶ Hier ist sinnvollerweise zwischen generellen unspezifischen Chancen und Risiken, solchen von Informations- und Kommunikationstechnologien allgemein, speziell von selbstorganisierenden adaptiven Systemen, und im Besonderen von organic computing zu differenzieren.

¹⁰⁷ Systeminhärente (Komplexitäts-)Risiken beziehen sich auf (unbeabsichtigte) soziale Folgewirkungen (z.B. Verselbständigung des Computers), also durch OC systemisch zwangsläufig und nicht vermeidbar generierte Risiken, die zwar im Einzelnen nicht eintreten müssen, aber anders als durch Sicherheitstechnologien und -systeme im Prinzip weitgehend beherrschbare Risiken nur allgemein vermutet und durch adaptive Maßnahmen lediglich kompensiert werden können. – Als Fokusthema wurden jüngst in der Zeitschrift GAIA die genuinen Charakteristika und konzeptionelle Abgrenzbarkeit systemischer Risiken debattiert (vgl. Renn/Keil 2008, 2009, Huber 2009, Neitzke et al. 2008, Schmidt et al. 2009).

ökologischen Relevanz von Chancen und Risiken von OC in systemischen und/oder primären Bereichen der Soziosphäre zu fragen. Dabei lassen sich entsprechend Chancen und Risiken unterscheiden, die Einzelpersonen, soziale Gruppen, soziale Subsysteme (Wirtschaft, Politik etc.) oder deren Interaktionen und Beziehungsmuster betreffen. Sie sind stets soziokulturell definiert und mit der Nutzung von OC (als Nebenwirkungen) einhergehende Folgewirkungen.¹⁰⁸ Im Falle relativ umfassender Folgewirkungen handelt es sich um gesamtgesellschaftliche (soziale) Chancen und Risiken. – Während sich diese auf deren etablierte gesellschaftliche Nutzung beziehen, ist ergänzend die Kategorie von mit der Einführung und (erstmaligen) Umsetzung von OC-Systemen verbundenen Chancen und Risiken anzuführen. Diese betreffen die im Zuge des Innovationsprozesses und der OC-Umsetzung entstehenden Pioniergewinne, Kontroversen, Akzeptanzprobleme und rechtliche Rahmensetzungen, die auch den Umgang mit Nichtwissen berühren und im Prinzip die Einführung und Nutzung von OC gleichermaßen bremsen oder blockieren können und dann als genuines Akzeptanzrisiko einzustufen sind. In diesem letzteren Fall kämen sämtliche mit OC substantiell verbundenen Chancen und Risiken infolge seiner Nichteinführung kaum mehr zum Tragen.

In den Tabellen 4.2 und 4.3¹⁰⁹ spiegelt sich nun das differenzierte, mehrdimensionale analytische Grundraster wider. Das Votum für dieses mehrdimensionale analytische Grundraster zur Einordnung der Chancen und Risiken von OC-Systemen ist darin begründet, dass unterschieden wird zwischen solchen Typen von (konkreten) Chancen und Risiken, die in ihren sehr wohl stets bestehenden sozialen Relationen und Bezügen mit der jeweiligen angestrebten bzw. genutzten IT-Technik erkennbar und nachvollziehbar verknüpft sind (technische Potenziale, Anwendungs- und Nutzungsmöglichkeiten, experimentelle Optionen, systeminhärente Chancen und Risiken), und solchen Typen von Chancen und Risiken, die sich – unter Vermittlung entsprechender sozialer Prozesse – hieraus mit einer gewissen Wahrscheinlichkeit in analytisch unterscheidbaren Dimensionen (psychisch, semiotisch-symbolisch, normativ, ordinativ, allokativ, operativ, physisch-ökologisch) als (indirekte) soziale Folgen auf Mikro- und Makroebene ergeben (können), auch wenn dies nachfolgend kaum durchweg durchgehalten werden kann.

¹⁰⁸ Ein Spezialfall solcher Risiken sind Gesundheits- und Umweltrisiken, insofern diese letztlich gleichfalls sozial definierte, aber auf die physische Natur im Sinne ihrer negativ bewerteten Veränderung bezogene Risiken darstellen.

¹⁰⁹ Letztere ist erkennbar aus Abbildung 4.1 abgeleitet.

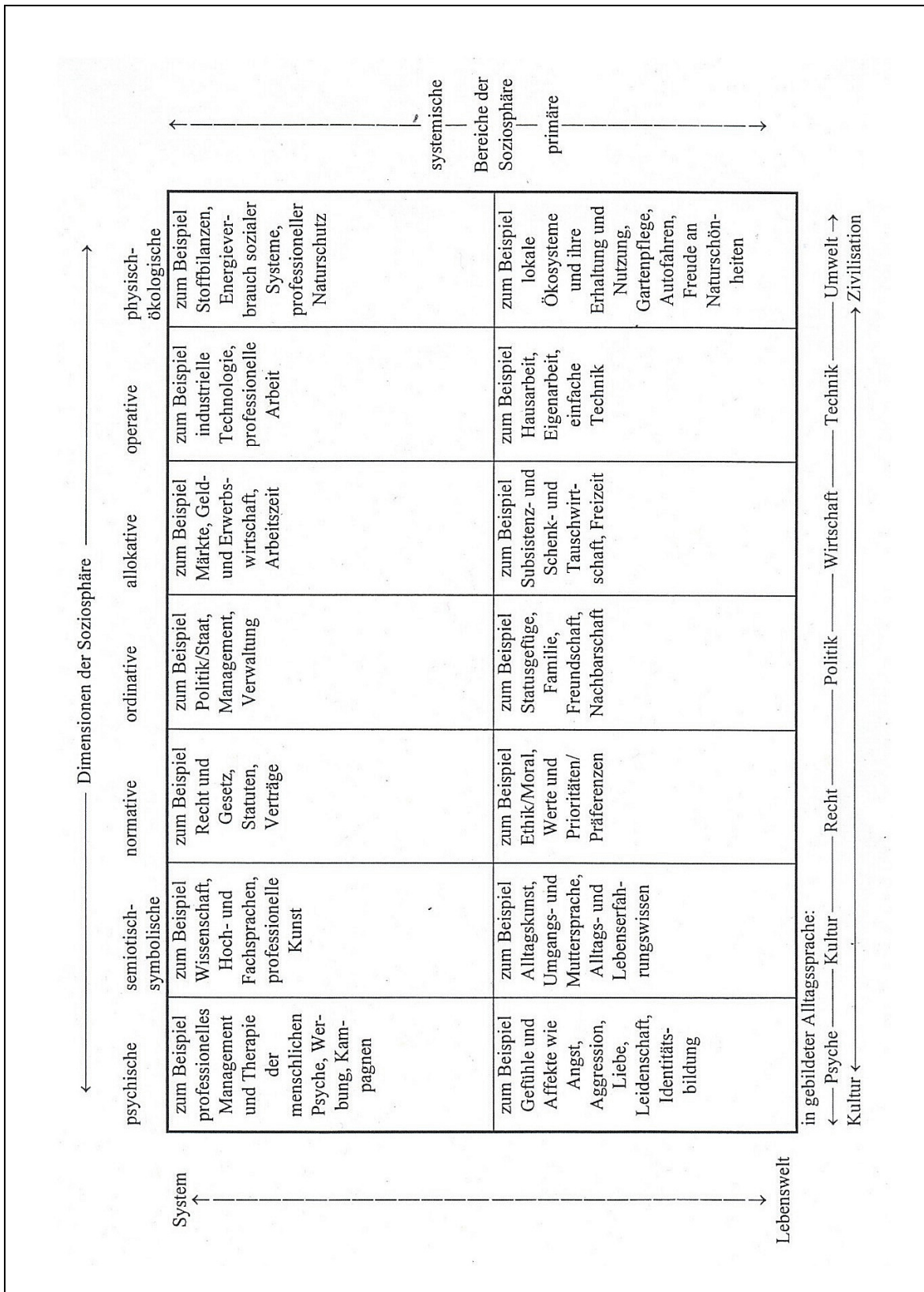


Abbildung 4.1: Erweiterte Gliederung der Soziosphäre

Quelle: Huber 1989: 207 mit eigenen Ergänzungen

Das Raster ist relativ umfassend und abstrakt angelegt, und geht damit z.B. über auf (smarte) IT-Systeme und OC bezogenen Risikotaxonomien hinaus, die etwa unterscheiden:

- technische (intentionale oder technische Störung), individuelle (Datenschutz, identity theft, Betrug, Falschinformation, Datenmanipulation), betriebliche (finanzielle und Imageverluste) und gesellschaftliche (z.B. gläserner Nutzer, cyber terrorism, information warfare) Risiken (Müller et al. 2006)

Tabelle 4.3: Dimensionen sozialer Chancen und Risiken

psychische Systemchancen	psychische Personchancen	psychische Systemrisiken	psychische Personrisiken
semiotisch-symbolische Systemchancen	semiotisch-symbolische Systemchancen	semiotisch-symbolische Systemrisiken	semiotisch-symbolische Systemrisiken
normative Systemchancen	normative Personchancen	normative Systemrisiken	normative Personrisiken
ordinative Systemchancen	ordinative Personchancen	ordinative Systemrisiken	ordinative Personrisiken
operative Systemchancen	operative Personchancen	operative Systemrisiken	operative Personrisiken
physisch-ökologische Systemchancen	physisch-ökologische Personchancen	physisch-ökologische Systemrisiken	physisch-ökologische Personrisiken
soziale Innovation und Akzeptanz		soziale Inakzeptanz und Kontroverse	
gesamtgesellschaftliche Chancen		gesamtgesellschaftliche (Katastrophen-)Risiken	

- Missbrauchs-, Fehlbedienungs- und systeminhärente Risiken (Müller et al. 2006)
- Daten-, soziale und Komplexitätsrisiken (Pissarskoi 2008)
- Gesundheits- und Umweltrisiken, Wahrnehmungsriskien, strukturelle Risiken, Wildcards (Pade/Petschow 2008)
- Simple vs. complexity-induced risk problems (Pade/Petschow 2008)
- uncertainty- vs. ambiguity-induced risk problems (Pade/Petschow 2008).

Diese Risikotypen korrelieren mit unterschiedlichen, das Risiko mindernden Schutz- und Sicherheitsstrategien, und sie lassen sich jeweils nach bestimmten (technologiespezifischen) Risikoklassen aufgliedern.¹¹⁰

¹¹⁰ So führt etwa Pissarskoi (2008) unter Datenrisiken Privacy (Datenschutz), Identity (Identitätsdiebstahl), Sicherheit, böswillige Angriffe und Technikpaternalismus, und unter soziale Risiken direkte soziale Risiken, digitale Spaltung der Gesellschaft, Stress, Verursacherprinzip (Verantwortlichkeit und Haftung), Unfreiwilligkeit (Zwang) und ökologische Nachhaltigkeit (Elektronikschrott) auf.

4.2 Probleme und Issues von smarten adaptiven Systemen

Ehe im Kapitel 4.3 die Chancen und Risiken von OC näher erörtert werden, werden zunächst typische, in den vorangehenden Kapiteln bereits teils angesprochene Probleme und Issues von selbstorganisierenden adaptiven (smarten) Systemen benannt, wie sie in der nachfolgend teils knapp resümierten, jedoch nicht weiter explizierten Literatur hervorgehoben werden; denn sie stellen den relevanten Kontext dar, in dem erstere erst zum Tragen kommen und zu spezifizieren sind.

Neben den durch smarte SaSo-Systeme gewonnenen Chancen und Freiheiten werden durchaus auch die damit verbundenen Risiken und Gefahren gesehen, die – neben altbekannten Gefahrenmomenten wie allgegenwärtiger Zugriff, Privacy/Datenschutz/digitale Identitäten¹¹¹, Zuverlässigkeit, Sicherheit, Vertrauenswürdigkeit, Kontextsensitivität – die insbesondere mit smarten Systemen verbundenen Risiken der aus emergenten Prozessen resultierenden Fehlentwicklungen mit potenziell katastrophalen Folgewirkungen implizieren, und die mit indirekten Folgen ihres breiten Einsatzes einhergehen können, wie: Exklusion von Nichtnutzern und digitale Spaltung der Gesellschaft, Nutzungszwang und Abhängigkeit von smarten Systemen, Verlust an Eigenkontrolle und Technikpaternalismus, Übermaß an (indirekter) sozialer Kontrolle und Überwachungsstress, Zurechenbarkeit von Schadensursachen, Abnahme direkter sozialer Kommunikation plus (Selbst)Isolierungs- und Vereinsamungstendenzen, etc, bis hin zum aufgrund der Selbstorganisation und -steuerung der IT-Systeme nur schwer kontrollierbaren Missbrauch.¹¹² Darüber hinaus sind mit der Zeit handhabbare und lösbare Probleme der Einführung smarter Systeme von Gewicht, die sie be- oder sogar verhindern können: (rechtliche) Verantwortlichkeit und Haftungsregelungen, kompatible oder gleichartige IT-Sicherheitsstrategien und -verfahren, Zugangs- und Nutzungsbedingungen, Energieeffizienz und ökologisch nachhaltige Entsorgungsregelungen.

¹¹¹ Müller et al. (2006) nennen hier insbesondere malware (wie Computerviren), ID cards (wie dauerhafte Verfügbarkeit biometrischer Daten), e-Health (wie elektronische Gesundheitskarten) und RFID-Store (wie Kaufverhaltensanalyse ohne Zustimmung). Ihre Schlussfolgerungen über die Risiken und die begrenzten Möglichkeiten des Risikomanagements smarter Systeme sind trotz ihrer grundsätzlicher Befürwortung recht eindeutig: „Current protection mechanisms are insufficient for security and privacy in highly dynamic systems and ubiquitous computing.“ – „No privacy and security method has reached technical maturity and acceptance by customers in personalized services. The risk of misuse remains with the customer.“ – „Emerging IT systems’ properties complicate the quantification of threats.“ – „Emerging risks in future IT systems could well be defended against by the use of liveness instead of safety properties. However, so desirable these properties are from a security point of view., so far away do they lie in the future as regards the technical development. Today, no mechanisms are available that achieve liveness.“ – „Privacy and security can only be achieved through data collection for later use – which is paradox, because this data is the source of privacy and security risks.“ – „Privacy by obscurity will fail in future IT systems because of the omnipresent and often invisible possibilities of data collection. Combining access control with usage control is a promising approach.“ – „In emerging IT systems, security and especially privacy rarely are achievable before or during execution. Evidence creation as an approach after execution complements existing privacy and security approaches.“ – „Juridical and legal regulations must guarantee security and privacy, enforcing the sanctioning of violations to reduce risks.“

¹¹² Die SWAMI-Studien von Wright et al. (2006) und Alahuhta et al. (2006) über „Safeguards in a World of Ambient Intelligence“ benennen als Schlüsselthemen „privacy, security, identity, trust, loss of control, dependency, exclusion, victimisation“ und als zentrale Risiken „surveillance, identity theft, malicious attacks, digital divide, spamming“ und plädieren für verstärkte Forschungsanstrengungen zur Entwicklung entsprechender Policy-Optionen und Regelungen betreffend: „issues such as privacy, anonymity, manipulation and control, intellectual property rights, human identity, discrimination and environmental concerns; new societal and policy options including responsibilities and ethics of digital behaviour; protection of rights for all citizens in all their roles (private and professional) in the Information Society; safeguards and privacy enhancing mechanisms to ensure user control, user acceptance and enforceability of policy in an accessible manner; equal rights and opportunities of accessibility to the Information Society and its ambient intelligence environment.“ (Wright et al. 2006:11)

Das zentrale Dilemma smarter Systeme und insbesondere von OC mit im Prinzip erwünschten emergenten Effekten besteht wie gesagt darin, dass sie einerseits eigenständig auf neue, nicht vorhergesehene Umwelteigenschaften reagieren können und sie andererseits nicht in der Lage sein sollen, katastrophale Folgen zu generieren (vgl. Pissarskoi 2008:19). Es geht also um die geeignete Balance zwischen Autonomie und Begrenzung von OC-Systemen, die bislang nicht wirklich gelöst ist, und genau hier liegt das genuine OC-Risiko.¹¹³ Es gibt nur pragmatische Lösungen, wo der Ingenieur in der Entwurfsphase Emergenz-Potenziale vorgibt, ohne die Details zu kennen, aber damit einen entsprechenden Rahmen für mögliche Entwicklungen des Systems festlegt.¹¹⁴ Gerade weil mit selbstorganisierten und sich selbst steuernden Systemen im Prinzip Kontrolldelegation und -verlust sowie weitreichende, nicht genau bekannte Folgewirkungen und Gefährdungen einhergehen (können), erfordern solche Lösungen aufgrund unzureichenden Wissens und wachsender Gestaltungsmacht von SaSo-Systemen im Grundsatz ein erweitertes und vorsorgezentriertes Risikomanagement, das etwa auf resiliente Eigenschaften wie Adaptivität, Lernfähigkeit, Reparaturfähigkeit, Vielfalt und Redundanz zentraler Elemente (Modularität), Rückkopplungsmechanismen mit einem geeigneten Verhältnis von positiven und negativen Rückkopplungen, und Pufferkapazitäten Wert legt (vgl. Gleich 2008).¹¹⁵

In ihrem generellen Überblick über gegenwärtige (2007), zu erwartende (2007-2010) und zukünftige Risiken von Informationssystemen und Datensammlungen resümiert die European Network and Information Security Agency (ENISA 2007b:107f) : „It seems that the most prevalent of the current risks continue to be related to compromised computing devices and phishing. Emerging risks, however, seem to be revolving around three main dimensions: **Mobility**: the increased penetration and sophistication of mobile phones will make them a prime target for new kinds of attacks. **Privacy**: the (almost invisible) collection of large amounts of personal data and the aggregation of these data into databases for (practically) long-term storage poses challenges to the protection of the privacy of ordinary citizens. **Interaction of the Internet with other infrastructures**: As the Internet has an increasingly higher interaction with (or even a direct connection to) other infrastructures, such as the telephone network or the power grid, attackers may use the Internet to directly (or indirectly) attack services provided by other infrastructures. For example, hackers may use VoIP clients to continually call victim telephone numbers, or may selectively and simultaneously turn on/off appliances they control in order to overload the power grid. Finally, **future risks seem to be**

¹¹³ Demgegenüber sind sonstige Risiken wie unzulässige Überwachung nicht OC-spezifisch.

¹¹⁴ „Für die Entwicklung autonomer Systeme ist es besonders wichtig, dass das resultierende System von hoher Qualität ist (worin diese Qualität konkret begründet ist, hängt vom jeweiligen System ab). Diese Tatsache ist in dem Anspruch begründet, dass autonome Systeme im Wesentlichen ohne manuellen Eingriff auskommen sollen. Daraus folgt, dass Fehler im System auf ein Minimum reduziert werden müssen, da anderenfalls die Autonomie durch notwendige, regelnde Maßnahmen von Außen gefährdet werden könnte. Die Qualität des resultierenden Systems kann stark von dem gewählten Prozessmodell und den eingesetzten Entwicklungsmethoden abhängen. Dazu kommt, dass sich Autonomie meist nicht nur auf Teilbereiche eines Systems bezieht, sondern einen Aspekt darstellt, der im gesamten System oder zumindest weiten Teilen berücksichtigt werden muss.“ (Heiß et al. 2008:14)

¹¹⁵ „Ein erweitertes Risikomanagement wird nötig, wenn viele der Rahmenbedingungen noch nicht so bekannt sind wie dies im Brandschutz der Fall ist, wenn Technologien erst entwickelt und mit unbekanntem Wirkungen gerechnet werden muss, wenn die Bewertungen noch unklar sind, was überhaupt ein Schaden sein könnte und es auch bei der Institutionalisierung noch hapert. Beim erweiterten Risikomanagement müssen – um die Ungeklärtheiten auszugleichen – weitere Vorsorgemaßnahmen aktiviert werden, Maßnahmen wohlgerichtet, die nicht auf Gewusstes, Erklärtes und Begriffenes reagieren, sondern auf Noch-Nichtwissen und tendenzielle Ahnungslosigkeit. Dies ist auch die Ausgangslage für das vorsorgezentrierte Risikomanagement. Ein solches muss zum Einsatz kommen, wenn wir extrem wenig wissen und mit wirklich besorgniserregenden Entwicklungen rechnen müssen. Bloßes Nichtwissen, weil irgendetwas neu ist, reicht dafür nicht aus. Wenn wir immer warten wollten, bis wir genug wüssten, würde es kaum noch Innovationen geben können.“ (Gleich 2006:43)

related to the proliferation of almost invisible computing and communication devices which will make their manageability and their security even more challenging. These devices may be used (i) to compromise the security of ordinary citizens; (ii) to invade their privacy and to jeopardize the security of the premises in which they are located.”¹¹⁶ Demgegenüber wird genuin technischen Risiken augenscheinlich weniger Beachtung geschenkt, wie z.B. dem Kontrollproblem, das mit der Zunahme der Vernetzungen unabhängiger Agenten in smarten Systemen einhergeht.

Der Bericht der Gesellschaft für Informatik/VDE/ITG (2008) bemüht sich um einen informativen Überblick über acht mit Schlüsseltechnologien für zukünftige industrielle Anwendungen korrelierte Themenbereiche und drei Anwendungsgebiete mit voraussichtlich hoher wirtschaftlicher Bedeutung. Diese sind omnipräsente Informationsverarbeitung, zukünftige Kommunikationsnetze, Vertrauenswürdigkeit und Zuverlässigkeit, Organic Computing Techniken, Energieeffizienz, Umweltverträglichkeit und Nachhaltigkeit, Multi-Core- und Many-Core-Prozessoren, massiv parallele und GRID-Systeme, unkonventionelles Rechnen. Die sich daraus ergebenden (wissenschaftlichen) Herausforderungen betreffen: „den Umgang mit Information, die Kommunikation mit und zwischen technischen Geräten, die Vertrauenswürdigkeit und Zuverlässigkeit der Infrastruktur, Techniken der Komplexitätsreduktion und -bewältigung, den verantwortungsbewussten Umgang mit Energie, Umweltverträglichkeit und Nachhaltigkeit bei der Herstellung, im Betrieb und der Entsorgung informationstechnischer Geräte, und neue Rechner-Entwicklungen, um die damit erreichbaren höheren Verarbeitungsleistungen für die Anwendungsziele verfügbar zu machen.“

In seiner breiter angelegten, systematischen Darstellung der Facetten und Probleme des Mensch-automatisierte-Maschine-Systems erörtert Sheridan (2002) viele Beispiele dieser Interaktion, wie Flugzeuge, Autos, Züge, Schiffe, Kernkraftwerke (KKWs), Krankenhäuser, virtuelle Realitäten und Unterhaltung, Bürosysteme, die smarte Wohnung, und weist auf den begrenzten Wert von Handbüchern und Richtlinien hin, gerade wegen der nicht ingenieurmäßigen Formalisierbarkeit menschlichen Verhaltens und der jeweils spezifischen Situationsgebundenheit von Mensch-Maschine-Systemen. Er diskutiert die verschiedenen (situationsgeprägten) Arten und Dimensionen menschlichen Verhaltens wie Geschwindigkeit, Genauigkeit, Robustheit, Adaptionsvermögen oder situativ angepasste Aufgabenbearbeitungsgeschwindigkeit sowie typische Einseitigkeiten und Vorlieben menschlicher Entscheidungen, die Rolle von Vertrauen (Vertrauenswürdigkeit des Systems aufgrund seiner wahrgenommenen Zuverlässigkeit, Robustheit, Vertrautheit, Nützlichkeit, oder aber fehlende Glaubwürdigkeit und Ablehnung oder Nichtnutzung trotz Verfügbarkeit) und menschliches Fehlverhalten. Sheridan sieht fünf Rollen von menschlicher supervisory control:¹¹⁷ Planen, Instruie-

¹¹⁶ An (1) gegenwärtigen, (2) zu erwartenden und (3) zukünftigen IT Risiken werden aufgeführt: (1) SPAM, botnets, phishing, identity theft, route hijacking, instant messaging, peer-to-peer systems, malware on cell phones, hackers in stock market, software vulnerabilities, no protection (e.g. antivirus) devices; (2) SCADA (supervisory control and data acquisition), increased home automation, turning home appliances on/off, massive collections of personal data, invisible data collection in public places, invisible data collection in private places, security is more in art than in science, DoS (denial of service) attack on the home telephone, hacking home heat and/or air-conditioning system, Internet users are younger, less experienced, and more prone to subtle attacks, Internet users may not have strong motives to clean up their compromised computers, malware over multiple networks (GSM, GPRS, Internet, Bluetooth); (3) Manageability, over-use of ICT, using home appliances to attack infrastructures, the security of most primitives cannot be formally proved.

¹¹⁷ „In a strict meaning, *supervisory control* means that one or more human operators are intermittently programming and continually receiving information from a computer that itself closes an autonomous control loop from the artificial sensors and through the actuators to the controlled process or task environment. In a more generic, or liberal, meaning, *supervisory control* means that one or more human operators are intermittently programming and receiving information from a computer that interconnects through artificial sensors and effectors to the controlled process or task environment.” (Sheridan 2002:115)

ren, Überwachen (Monitoring), Eingriff und Lernen. Automatisierung lohnt sich (aufgrund der mit ihr verbundenen Zusatzkosten) nicht für triviale und nicht für sehr komplexe Aufgaben (z.B. Außenreparaturen an Raumstationen durch Astronauten). Die Nutzung von (neuen) Mensch-Automationssystemen sollte abhängig gemacht werden von deren Simulation, Tests und Evaluation. Evaluationstechniken müssen zwangsläufig oft qualitativer Natur sein: Fokusgruppen, iterative Gruppenwahl, Delphi-Methode, usability testing, und multidimensionale Skalierung. Schließlich beschreibt Sheridan vielfältige mögliche Probleme der Mensch-Automatisierung-Interaktion, die etwa aus der Systemkomplexität und unerwartetem Verhalten, dem Monitoring, Computer-Ratschlägen (mit zu viel oder zu wenig Vertrauen des Operateurs), die Geschwindigkeit der Ein- und Fortführung von Automation, oder der letztlichen Zuschreibung von Entscheidungskompetenz resultieren.¹¹⁸ Sheridan benennt Kriterien anthropogen orientierten Designs automatisierter Systeme. Vorteile von automatisierten Systemen resultieren insbesondere aus der Geschwindigkeit der Informationsverarbeitung, ihrer raschen Reaktionsfähigkeit, ihrer mechanischen Kraft, ihrer Genauigkeit und Präzision, ihrer dauerhaften Arbeitsfähigkeit, ihrer Robustheit gegenüber (unterschiedlichen) Umweltbedingungen, ihrer Zuverlässigkeit und ihren Kostenvorteilen. Umgekehrt weist er neben konkreten Umgangsproblemen auf die Risiken (1) individueller und (2) sozialer Entfremdungseffekte hin¹¹⁹: (1) Gefahr von Arbeitslosigkeit, Unzufriedenheit, zentralisierte Managementkontrolle bei eigenem Kompetenzverlust, Dissozialität, Dequalifizierung, Furcht vor nicht mehr beeinflussbaren, machtvollen (technischen) Systemen, technologischer Analphabetismus, Mystifizierung und unangemessene Vertrauensseligkeit, Gefühl fehlender eigener Beiträge und der Überflüssigkeit, fehlende Verantwortlichkeit und Haftbarkeit, glückliche Unterwerfung und ‚Versklavung‘; (2) Verteilungsgerechtigkeit (wer entscheidet und wer profitiert), ‚Technikfreunde gegen Technikfeinde‘, Maschinenproduktivität statt menschlicher Produktivität, Rückgang (direkter) sozialer Kontakte, elektronische Herrschaft weniger Mächtiger, automatisierte Ressourcenübernutzung und Umweltgefährdungen, Kriegführung und Spionage mithilfe von Telerobotern, hohe Verletzbarkeit automatisierter Systeme durch terroristische Angriffe.

Autoren, die sich konkret mit smarten IT-Systemen befassen, sehen deren Probleme und schlagen – auf teils unterschiedlichen Ebenen – entsprechende Design-Richtlinien, Umgangsformen und Regulierungen vor, die sie als notwendig, aber auch praktikabel und hinreichend in ihrer Problemlösungskapazität einordnen.

So zielt die vorgeschlagene Methodologie von Gershenson (2007) darauf ab, selbstorganisierte Systeme zu entwerfen und zu kontrollieren, die entwickelt wurden, um komplexe Probleme zu lösen. Die nicht unbedingt sequentiell erfolgenden Schritte hierfür seien: representation, modeling,

¹¹⁸ Sheridan (2002:80) offeriert eine subjective 10-Stufen-Skala mentaler Belastung des Operateurs: „Operator mental effort is minimal, and desired performance is easily obtainable (1). Operator mental effort is low, and desired performance is attainable (2). Acceptable operator mental effort is required to attain adequate system performance (3). Moderately high operator mental effort is required to attain adequate system performance (4). High operator mental effort is required to attain adequate system performance (5). Maximum operator mental effort is required to attain adequate system performance (6). Maximum operator mental effort is required to bring errors to moderate level (7). Maximum operator mental effort is required to avoid large or numerous errors (8). Intense operator mental effort is required to accomplish task, but frequent or numerous errors persist (9). Instructed task cannot be accomplished reliably (10).“

¹¹⁹ „The term alienation is used to characterize a variety of negative impacts of automation on the individual human. When systems are automated and the human is removed not only spatially but also temporally, functionally, and cognitively from the ongoing physical process he or she is directing, that can be called alienation.“ (Sheridan 2002:170)

simulation¹²⁰, application und evaluation, die im Einzelnen erklärt werden, wobei zwischen *agent* (a description of an entity that acts on its environment) und *mediator* (he arbitrates among the elements of a system, to minimize conflict, interferences and frictions; and to maximize cooperation and synergy) unterschieden wird. Methoden der Spannungsminderung sind: tolerance, courtesy, compromise, imposition, eradication und apoptosis. Methoden der Förderung von Synergie sind: cooperation, individualism, altruism und exploitation. Trade-offs existieren, wenn ein System mit der Komplexität seiner Domäne umgehen können muss, um seine Ziele zu erreichen: complexity of elements/interactions, quality/quantity, economy/redundancy, homogeneity/heterogeneity, system/context, ability/clarity und generality/particularity.¹²¹

Fink/Fricke (2007:10) sehen fünf Bereiche, wo bei Beachtung entsprechender Design-Richtlinien die Risiken selbstorganisierender (autonomer) Systeme zumindest besser bewältigt werden können:

- „Awareness: Allowing human insight into system activities via cyber analytics.“¹²²
- Management: Enabling human influence over distributed autonomous systems via hierarchical design.
- Attribution: Certifying the correctness of independent actions of the system.
- Integrity: Ensuring that the system has not been subverted.
- Limits: Stating clearly what the autonomous system may and may not do.“

In den Fallstudien von Hanseth/Ciborra (2007) resultieren aus den jeweiligen Projektanstrengungen, mit unerwarteter Komplexität umzugehen, die sich aus der geforderten Integration und (zugleich) divergierenden Handlungsroutinen der beteiligten Einheiten ergibt, eher zwangsläufige, zu Komplikationen und Verzögerungen führende Probleme als genuine ‚Risiken‘. High-reliability Organizations¹²³ machen hierbei zumindest dann eine Differenz, wenn lose Kopplung, dezentrale Organisationsformen und begrenzte Veränderungsgeschwindigkeiten vorherrschen.¹²⁴

¹²⁰ „The Simulation and Experiments are strictly necessary in the design of self-organizing systems. This is because their performance cannot be evaluated by purely formal methods... The lack of predictability does not come only from chaotic processes. It might come also from new information generated by the interactions, so that the system behavior cannot be predicted from the behavior of the elements. Thus, one is forced to “let the system run and then see”, as with cellular automata.” (Gershenson 2007:58)

¹²¹ An den Fällen selbstorganisierter Ampelschaltung, Bürokratie und Artefakte wird deutlich, dass die Nutzung einer solchen generellen Methodologie mit deren zunehmender Komplexität und Sozialität schwieriger und aufwändiger wird, sodass nur im Falle selbstorganisierter Ampelschaltung einfache Modelle, Simulationen und Experimente realisiert werden konnten, während in den beiden anderen Fallstudien – neben einem hochabstrakten Modell von random agent networks für die Bürokratie – nur eher qualitativ formulierte Systembeschreibungen und Problemlösungen möglich waren. Cyber analytics is the science of analysis as it relates to people, computers, and infrastructures. Cyber Analytics tells the story behind cyber data Battelle Pacific Northwest National Laboratory

¹²² Nach dem von Battelle Pacific Northwest National Laboratory verfolgten Ansatz “Cyber Analytics is the science of analysis as it relates to people, computers, and infrastructures... Cyber Analytics tells the story behind cyber data.” (<http://i4.pnl.gov/publications/news/l4newsletter-Spring09-V5.pdf>)

¹²³ Als kaum zu übersetzender Begriff bezeichnen high-reliability organizations Organisationen, die ein hohes Maß an Zuverlässigkeit und Betriebssicherheit gewährleisten, indem sie in der Lage sind, den Konflikt zwischen zentralen und dezentralen Steuerungsmodi erfolgreich zu bewältigen und komplexe, eng gekoppelte Systeme zu managen und Spitzenlasten unter Zeitdruck zu bewältigen, ohne dass es zu Katastrophen kommt (vgl. LaPorte/Consoloini 1991)

¹²⁴ „High-reliability-Organisationen bewerkstelligen den ‚Spagat‘ zwischen scheinbar widersprüchlichen Anforderungen, indem sie die Fähigkeit entwickeln, in unterschiedlichen Modi zu operieren: Im bürokratischen Routine –Modus ope-

Zusammenfassend führt diese Darstellung der Probleme und Issues von (selbstorganisierenden) adaptiven smarten Systemen zu folgenden Ergebnissen:

- 1) Ihre Vorteile und Nutzen beruhen im Wesentlichen auf den Effizienzgewinnen und der effektiveren Bearbeitung komplexer (vernetzter) Aufgabenstellungen, die mit einer Vielzahl miteinander verknüpfter Informationsgewinnungs- und -verarbeitungsprozesse verbunden sind, die von smarten Systemen weitgehend eigenständig erledigt werden. Dazu gehören insbesondere auch solche neuartigen Arrangements, die bislang aus technischen oder Kostengründen nicht umsetzbar waren.
- 2) Neben möglichen Fehlfunktionsrisiken werden die Risiken solch smarterer Systeme vor allem in der Zuspitzung von im Prinzip bereits bekannten Datenschutzproblemen jedweder Art (Überwachung, Missbrauch) und daraus resultierenden sozialen Folgeproblemen (Exklusion, Entfremdung, digitale Spaltung, Nutzungszwang) gesehen.
- 3) Weniger wird in Rechnung gestellt, dass das, was für den einen eine Chance darstellt, für den anderen ein Risiko sein kann, und dies abhängig von den jeweiligen Wertmaßstäben, wie etwa das Beispiel adaptiver Kamerasysteme deutlich macht. Hier stellt die verbesserte optische Verfolgbarkeit von ausgewählten Personen für den Nutzer des Kamerasystems einen Vorteil dar, während sie für ebendiese mit ihrer verstärkten Überwachung infolge der datenschutzrechtlich für unbescholtene Personen nicht gewünschten Aufzeichnung ihrer Aufenthaltsorte und Bewegungsprofile verbunden ist (vgl. Müller 2008a).
- 4) Die Entwicklung und Nutzung selbstorganisierender adaptiver (smarter) Systeme wird von den beteiligten Akteuren laut Aussagen der interviewten Personen und in der Literatur zumeist im Kern akzeptiert und nicht als sozial zu gefährlich abgelehnt. Hierfür werden jedoch angemessene und wirksame Problemlösungen gefordert und vorgeschlagen, insbesondere adäquate rechtliche Rahmenbedingungen und ein intelligentes Management mit entsprechenden Design- und Schutzstrategien, wie z.B. eine geschützte Privatsphäre als Grundrecht (vgl. bereits OECD 1980) und die Beachtung der vier Hauptprinzipien des Datenschutzes: Datensparsamkeit und Datenvermeidung, Erforderlichkeit, Zweckbindung, Datensicherheit (vgl. Müller 2008b).
- 5) Als unausweichliches und nur pragmatisch handhabbares Grunddilemma smarterer Systeme wird die Spannung zwischen deren Eigenständigkeit in der Bewältigung hochkomplexer Aufgabenstellungen mit begrenzt erwünschten emergenten Effekten und ihrer noch möglichen

riert die Organisation gemäß den standard operation procedures (SOPs), die das Handeln der Beteiligten eindeutig festlegen und zudem die Autoritätsstrukturen innerhalb der Organisation definieren. Der Hochleistungs-Modus tritt beispielsweise bei Belastungsspitzen im morgendlichen Flugverkehr oder bei der Landung einer Staffel von Flugzeugen auf dem Flugzeugträger im Minutentakt ein. Hier ändern sich die Strukturen schlagartig hin zu teamförmigen Arbeitsformen, in denen die Funktion wichtiger ist als der formale Rang. Die Hierarchien flachen ab, die Vorgesetzten fungieren eher als Berater und Unterstützer; und die Entscheidungen werden von den Experten vor Ort getroffen, ohne dass diese befürchten müssen, für mögliche Fehler belangt zu werden. Im Notfall-Modus schließlich – einer Notlandung eines Flugzeugs mit brennendem Triebwerk – laufen wiederum vorprogrammierte, einstudierte Szenarien ab, die zudem regelmäßig trainiert werden, um die Fähigkeit der Organisation zur Bewältigung von Krisen aufrechtzuerhalten (LaPorte/Consolini 1991, Clarke/Short 1993, Roberts 1993). Auf diese Weise managen High-reliability-Organisationen komplexe, eng gekoppelte Technologien und bewältigen Spitzenlasten unter Zeitdruck, ohne dass es zu einer Katastrophe kommt, wie sie Perrow (1984) für derartige Systeme prognostiziert... Um komplexe Systeme erfolgreich zu managen, benötigt eine High-reliability-Organisation ausreichend Ressourcen, und zwar in finanzieller wie in personeller Hinsicht. Eine hohe Qualifikation des Personals, eine Kultur der Zuverlässigkeit sowie permanentes Training sind zudem unerlässlich, damit die menschlichen Komponenten des Systems die ihnen zugedachten Rollen effektiv ausfüllen und einen verlässlichen und sicheren Betrieb gewährleisten können... Zu einem effektiven Komplexitätsmanagement gehört also offenbar auch die Fähigkeit (von Organisationen wie von Individuen), in unterschiedlichen Modi operieren zu können, in denen einmal eine zentrale, hierarchische Kontrolle, ein anderes Mal das Prinzip der dezentralen Selbstorganisation vorherrscht. Intelligente Organisationen nutzen offenbar die Vorteile unterschiedlicher Governance-Modi und entwickeln die Fähigkeit zum ‚Switch‘ (vgl. Grote et al. 2004).“ (Weyer 2009:26f)

Kontrollierbarkeit benannt.¹²⁵ Demgemäß ist auch von einem (fallspezifisch variierenden) trade-off zwischen den Chancen und Risiken smarter Systeme auszugehen.

- 6) Außerdem werden – wie bei vielen Innovationen – jenseits ihrer erfolgreichen technischen Entwicklung Probleme ihrer gesellschaftlichen Implementation gesehen, die mit anders gelagerten und hinderlichen etablierten Standards, wie z.B. in der Automobilindustrie, mit bislang häufig unzureichenden rechtlichen Regulierungen, insbesondere von Verantwortungs- und Haftungsregelungen, mit (anfangs) hohen Kosten und damit unzureichenden wirtschaftlichen Vorteilen, mit der Notwendigkeit veränderter sozialer Verhaltensmuster und -arrangements, und mit (fallspezifischer) sozialer Inakzeptanz zusammenhängen.
- 7) Jenseits konkreter Fallspezifität sind Chancen und Risiken von Organic Computing zum einen anwendungs- und fallspezifisch (vgl. die unterschiedlichen Zwecke und Risiken von adaptiven Kerasystemen, Fahrerassistenzsystemen (Lorenz/Weyer 2008) oder eines automatisierten intelligenten Aktienhandels) und zum anderen als eher generelle von selbstorganisierenden adaptiven (smarten) Systemen zu identifizieren und einzustufen als OC-spezifische.

4.3 Chancen und Risiken von Organic Computing: Kontext und Spezifikation

Während manche Autoren (Hanseth/Ciborra 2007) mit Beck (1986), Giddens (1990) u.a. die praktisch immer wieder durchschlagende Nichtbeherrschbarkeit von Risiken durch komplexe Risikokontrollsysteme in ihrer sozialen Umsetzung – reduziert in HROs (high reliability organizations) – in den Vordergrund heben, bemühen sich ingenieurtechnisch geprägte Autoren z.B. um die systematische Kontrolle von Emergenz durch geeignete (technische) Konstruktionen, auch wenn sie die Problematik unerwarteten emergenten Verhaltens bei OC-Anwendungen sehen.

Versucht man auf allgemeiner Ebene (ohne konkrete Anwendungen und Fallbeispiele) in Bezug auf Chancen und Risiken von OC-Systemen einen Durchgang durch das analytische Raster, so lassen sich in der technischen Dimension zumindest folgende plausible Einschätzungen vornehmen:

- 1) Die technischen Potenziale von OC-Systemen sind langfristig aufgrund ihrer umfassenden Konzeption, der mit Selbstorganisation und Emergenz implizierten, potenziell weitreichenden Optionen und ihres Querschnittcharakters sehr groß und tendenziell globaler Natur, insofern sie sich im Erfolgsfalle weltweit verbreiten dürften. Sie sind eher spezifisch für smarte Systeme, jedoch aufgrund der Anlage und Grundarchitektur von OC besonders ausgeprägt für OC-Systeme mit hohem Autonomiegrad.
- 2) Da derartige OC-Systeme noch in der Entwicklung und nicht marktreif sind, sind ihre Anwendungs- und Nutzungsmöglichkeiten zwar langfristig vielfältig und umfangreich, hingegen kurz-

¹²⁵ „Je eigenständiger die Systeme sind, umso mehr Möglichkeiten haben sie, auf unerwartete Situationen zu reagieren. Dann haben sie aber auch mehr Möglichkeiten, katastrophale Folgen auszulösen. Um die katastrophalen Folgen zu verhindern, müsste den technischen Systemen bestimmte Rahmen gesetzt werden, die sie nicht verlassen können. Dann haben sie aber weniger Möglichkeiten, auf unerwartete Situationen zu reagieren. Oder mit anderen Worten: Je mehr wir die technischen Systeme unter unserer Kontrolle behalten, umso weniger helfen sie uns, die Komplexität zu reduzieren. Je mehr wir die Komplexität reduzieren, indem wir die Aufgaben an die selbstorganisierenden Maschinen abtreten, umso weniger haben wir sie unter Kontrolle.“ (Pissarskoi 2008:19)

fristig, abgesehen von ersten Versuchen bei der Ampelsteuerung, noch nicht gegeben und hier allenfalls mit denen anderer smarter Systeme vergleichbar.

- 3) Was experimentelle Optionen und systeminhärente (Komplexitäts-)Chancen anbelangt, so dürften solche sicherlich existieren, können an dieser Stelle jedoch nicht benannt bzw. lediglich spekulativer Fantasie überlassen werden.
- 4) Technische Fehlfunktionsrisiken von OC-Systemen sind derzeit naturgemäß vorhanden, da sie sich noch in der Entwicklung befinden und noch nicht marktreif sind. Langfristig sollten sie bei geeigneter Observer/Controller-Architektur und aufgrund ihrer Selbst-X-Eigenschaften infolge eigenständiger Fehleraufdeckung und Selbstheilung minimal werden und sich in ihrer Wahrscheinlichkeit nicht signifikant und eher positiv von denjenigen anderer smarter Systeme unterscheiden; denn OC bietet auch neue Potenziale, um aktiv auf Fehlverhalten zu reagieren, bis hin zu selbstorganisierten Ersatzmodulen, was dem Nutzer aber auch mitgeteilt werden muss.
- 5) Fehlbedienungs- und -nutzungsrisiken lassen sich auch bei marktreifen OC-Systemen nicht grundsätzlich vermeiden. Sie sollten aufgrund ihrer Selbstorganisation jedoch geringer ausfallen als bei anderen (komplexen) Informationssystemen.
- 6) Der Schutz vor Missbrauch kann bis zu einem gewissen Grad durch eine geeignete Kontrollstruktur und Architektur von OC-Systemen zwar gewährleistet sein; jedoch dürfte sich gerade aufgrund ihrer relativ großen Autonomie intelligenter Missbrauch nicht völlig verhindern lassen.
- 7) Systeminhärente (Komplexitäts-)Risiken ergeben sich vor allem aus möglichen ungewollten emergenten Effekten, die durch geeignete Kontrolle der Autonomie von OC-Systemen zwar systematisch begrenzt, jedoch nicht vollständig vermieden werden können (dürften).

Im Hinblick auf die sozialen Chancen und Risiken von OC-Systemen sei zusammenfassend festgehalten:

- 1) Auf der Ebene sozialer Funktionssysteme ist – in Abhängigkeit von Umfang und Breite der Nutzung von OC-Systemen – in allen Dimensionen der Soziosphäre mit Veränderungen in Form von Chancen und von Risiken zu rechnen. Diese betreffen Umweltbelastungen und ökologische Nachhaltigkeit, operativ Technologie- und Arbeitsstrukturen, ökonomisch insbesondere den Einsatz von Informationstechnologien und die damit verbundene Wettbewerbsfähigkeit, politisch relevante Management- und administrative Zertifizierungs- und Kontrollsysteme, normativ die Festlegung verbindlicher Standards und rechtlicher Regulierungen¹²⁶, die insbesondere Verantwortlichkeiten, Zugang und Haftung betreffen, semiotisch-symbolisch einerseits die (weitere) wissenschaftlich-technische Entwicklung und andererseits die gesellschaftliche Penetration und Etablierung einer entsprechenden Begrifflichkeit und von (sprachlichen) Konventionen des Umgangs mit OC-Systemen, sowie psychisch neben OC-Marketing einerseits das Management von selbstorganisierenden adaptiven Systemen und die Fähigkeit der kompetenten Nutzung von OC und andererseits auf gesellschaftlicher Ebene die soziale, ökonomische und politische Bearbeitung und Bewältigung von negativen Folgewirkungen (z.B. Exklusion, Überwachung, Identitätsdiebstahl, digital divide).

¹²⁶ Damit Zuständigkeiten und Verantwortlichkeiten nicht (zu) diffus werden. Grundsätzlich können autonome Systeme auch bei begrenzter Verantwortungszuschreibung kein Subjekt der Verantwortung darstellen, weil sie nicht zur Rechenschaft gezogen und finanziell haftbar gemacht werden können und weil sie ihren Zweck (bislang) nicht selbst bestimmen können. Von daher geht es beim Bau und Einsatz von OC-Systemen gerade auch darum, geeignete Vorkehrungen und Schadensdeckungsmodi zu treffen, um die moralische Zuständigkeit des Menschen zu erhalten (vgl. Christen 2004).

- 2) Aufgrund der Kontextgebundenheit dieser sozialen Folgen von OC werden sich seine Chancen und Risiken regional (und lokal) als auch in verschiedenen Zeiträumen in unterschiedlicher Art und Weise manifestieren und verteilen. Dabei dürften sie eher spezifisch für bestimmte Anwendungsbereiche und für smarte Systeme und weniger OC-spezifisch sein.
- 3) OC-Systeme dürften im Falle ihres breiten und durchgängigen Einsatzes auch auf der Ebene primärer Sozialsysteme mit der Zeit zu vielfältigen Veränderungen führen, die sich als mannigfaltige Chancen und Risiken darstellen lassen. Sie können z.B. Hausarbeit vereinfachen und automatisieren und Lebensstile verändern (z.B. ambient assisted living), zur Nutzung per saldo kostensparender alltagsrelevanter Technologien führen, soziale Nachbarschaftsgefüge und Kommunikationsmuster modifizieren (z.B. Entfremdung, Überwachung und Kontrolle), die auf IT-Systeme bezogene Alltagssprache verändern, im Falle diffuser Verantwortungs- und Haftungsregeln persönliche Verantwortungsübernahme untergraben, als auch Verzicht auf oder Abwehreffekte und technologischen Protest gegenüber als nicht mehr kontrollierbar eingestuft, sich selbst organisierenden adaptiven technischen Systemen induzieren.
- 4) Auch im primären Bereich der Soziosphäre dürften sich aufgrund der Kontextgebundenheit der sozialen Folgen von OC seine Chancen und Risiken regional (und lokal) als auch in verschiedenen Zeiträumen in unterschiedlicher Art und Weise manifestieren und verteilen. Dabei werden sie wiederum eher spezifisch für bestimmte Anwendungsbereiche und für smarte Systeme und weniger OC-spezifisch sein.
- 5) Generell ist im Hinblick auf eine (langfristig) viele Anwendungsbereiche umfassende und mehr oder weniger global verbreitete Durchsetzung von OC-Systemen anstelle ihrer mangelnden (gesellschaftlichen) Akzeptanz und bloßen Nischenexistenz anzunehmen, dass diese am ehesten dann eintreten dürfte, wenn OC zumindest (1) meist technisch gut und problemlos funktioniert, (2) volks- und betriebswirtschaftlich Kostenvorteile bietet, (3) hinreichend umweltverträglich ist, (4) für seine Nutzer mit erkennbarem Nutzen und keinen Katastrophenrisiken verbunden ist, (5) sozial anerkannte rechtliche Rahmenbedingungen und Regulierungen getroffen und implementiert wurden, (6) wirksame Kontroll- und Datenschutzmechanismen und -vorkehrungen existieren, die das Grundrecht auf informationelle Selbstbestimmung, Minimierung von Missbrauchsrisiken und die Gewährleistung der Vertrauenswürdigkeit von OC-Systemen absichern, und (7) hinreichend Vertrauen in die Kompetenz, Objektivität, Fairness, Konsistenz, Glaubwürdigkeit und Empathiefähigkeit der für smarte, insbesondere OC-Systeme verantwortlichen Institutionen besteht.

Diese Darstellung von sozialen Chancen und Risiken von OC-Systemen bleibt notwendig allgemein-abstrakt, weil ihre substanzuell-konkrete Darstellung zum einen nur fallspezifisch Sinn macht und zum anderen in Form eines illustrativen Kaleidoskops den Rahmen dieses Berichts sprengen würde.

Als Fazit im Hinblick auf die Chancen und Risiken von OC-Systemen lässt sich von daher festhalten:

- 1) Sie sind als soziale Chancen und Risiken primär auf der Ebene selbstorganisierender adaptiver (smarter) Systeme und weniger OC-spezifisch anzusiedeln.
- 2) Begrenzt OC-spezifisch sind ihr potenziell hoher Autonomiegrad, ihre Lernfähigkeit, ihre mögliche große Adaptivität, ihre Selbst-X-Eigenschaften und die gewünschten emergenten Effekte. Damit verbunden ist das Kontrolldilemma, trotz höherer Autonomiestufen und größerer Selbstorganisation und -steuerung ihre Autonomie soweit überwachen zu können, dass OC-Systeme vertrauenswürdig sind. Das OC-spezifische Risiko betrifft somit die Möglichkeit und Realisierbarkeit kontrollierter Autonomie und notwendiger Selbsterklärung.
- 3) Der IT-bezogene Diskurs ist allgemeiner Natur und thematisiert z.B. das Problem der digitalen Spaltung von Gesellschaft.
- 4) Substanzielle Aussagen über die Chancen und Risiken von OC sind in der Tendenz nur anwendungs- und fallspezifisch möglich, ohne damit erweiterte und vorsorgezentrierte Risikomanagementstrategien und Gestaltungsansätze obsolet werden zu lassen.
- 5) OC-Systeme bieten vielfältige und umfangreiche Anwendungs- und Nutzungsmöglichkeiten. Diese befinden sich allerdings noch in teils frühen Entwicklungsstadien, sodass ihre Realisierung und Marktfähigkeit noch nicht gesichert, sondern allenfalls wahrscheinlich ist.
- 6) Entscheidend für ihre breite Nutzung sind – wie bei fast allen technischen Innovationen – zunächst einmal ihre tatsächliche technische Machbarkeit und Marktreife.
- 7) Damit OC-Systeme in der Praxis eingesetzt werden (können), ist außerdem die Existenz bzw. Etablierung geeigneter sozialer Rahmenbedingungen in verschiedenen (rechtlichen, ökonomischen, politisch-administrativen, habituellen) Dimensionen notwendig.
- 8) Die breite Nutzung von OC-Systemen verstärkt insbesondere bereits vorhandene (bekannte und oben benannte) Risiken von Informations- und Kommunikationstechnologien, während systeminhärente (Komplexitäts-)Risiken zwar vorhanden, aber weniger virulent erscheinen.¹²⁷
- 9) Durch geeignete technische und soziale Vorkehrungen (wie Observer/Controller-Architekturen) und deren Verknüpfung sind die (genuinen) Probleme und Risiken von OC vermutlich weitgehend beherrschbar, insofern sie insbesondere mit Verzicht auf Überdehnung von OC durch Limitierung des Anwendungsspektrums, sozial- und umweltverträglich gestalteten Anwendungen, Begrenzung autonomer Selbstorganisation einschließlich verbleibender Eingriffsmöglichkeiten in OC-Systeme, kontrollierter Emergenz und erfolgreich realisierten Selbst-X-Eigenschaften, darunter Selbsterklärung einhergehen.

¹²⁷ So sind komplexe linear programmierte Systeme eher durch Ausfallrisiken betroffen.

5 Fallstudien zu Organic Computing

Im Rahmen des Vorhabens wurden drei Fallstudien zum angestrebten Einsatz von OC durchgeführt (vgl. Höhne 2009, Müller 2008a, 2008b, Pisko 2008, Petschow et al. 2009), die nachfolgend mit Blick auf ihre Chancen und Risiken mithilfe des in Kapitel 4 eingeführten analytischen Rasters resümiert und vergleichend betrachtet werden.

5.1 Ampel- und Verkehrssteuerung

Im Bereich der Ampelsteuerung und der mit ihr bezweckten Verkehrssteuerung gibt und gab es diverse Projekte, die über entsprechende Software der Ampelsteuerungssysteme – oder mithilfe von Informationsaustausch zwischen Fahrzeugen als reine Verkehrsinformationssysteme – den Straßenverkehr zu optimieren suchen. Im auf Grundlagenforschung ausgerichteten Vorhaben der Organic Traffic Control Initiative geht es um die Nutzung von OC zur sich selbstorganisierenden dezentralen Ampelsteuerung, wofür eine entsprechende Architektur (SuOC) entwickelt wurde, seine Vorteilhaftigkeit aufzeigende Simulationen durchgeführt wurden, seine praktische Erprobung jedoch noch aussteht (vgl. Cakar et al. 2008, Prothmann et al. 2008, 2009).

In diesem Fallbeispiel ist der Zweck auf genereller Ebene recht eindeutig definiert: Verbesserung des Verkehrsflusses; und dieser dürfte – wie in Teststudien belegt – im Erfolgsfall eines programmgemäß funktionierenden OC-Systems der Ampelsteuerung – auch erreicht werden. Die positiven Haupteffekte wären weniger Zeitaufwand für Transport für die Verkehrsteilnehmer und dadurch weniger Emissionen.¹²⁸

Was nun systematisch die technischen Potenziale, Anwendungs- und Nutzungsmöglichkeiten, experimentellen Optionen und systeminhärenten (Komplexitäts-)Chancen einer OC-Ampelsteuerung anbelangt, so betreffen erstere die dezentral strukturierte, weit- und großräumige Vernetzung und Kommunikation der Ampelanlagen. Zweckbezogen dürften weitere Anwendungs- und Nutzungsmöglichkeiten auf ähnliche Verkehrskonstellationen begrenzt sein. Experimentelle Optionen und systeminhärente Chancen könnten hingegen nicht erwartete anderweitige Nutzungsoptionen und Steuerungsmöglichkeiten sein, die über dezentrale OC-Ampelsteuerung hinausgehen, ohne solche hier spezifizieren zu können.

In der Sozialdimension betreffen die Chancen Entlastung durch Selbstregulierung (ordinative Ebene), Zeitersparnis (allokative und operative Ebene im systemischen und primären Bereich, psychische Erleichterungen) und physisch-ökologische Immisionsminderung, ohne jedoch gegenüber den bestehenden Systemen der Ampelsteuerung zu gemessen am Gesamtumfang durchschlagenden Reduzierungen zu führen.

¹²⁸ Allerdings würde im Falle von Verkehrsüberlastung und Staus zu den Hauptverkehrszeiten dieser Ertrag zusehends geringer werden, wie analog der Einsatz von floating phones bei Navigationssystemen (HD Traffic in den Niederlanden) zur Stauumgehung indiziert. Umgekehrt dürfte angesichts des bereits erreichten Massenverkehrsaufkommens durch die Bereitstellung verbesserter Transportmöglichkeiten – wie bislang der (Aus-)Bau von Umgehungsstraßen und Autobahnen – der Effekt dadurch induzierten zusätzlichen Verkehrsaufkommens allenfalls noch marginal sein.

Was die technischen Risiken einer OC-Ampelsteuerung anbelangt, so dürften sich technische Fehlfunktionsrisiken bei entsprechend programmierten Sicherheitsmargen in Grenzen halten und deren Folgen, ähnlich heutigen Ampelausfällen, kaum gravierend sein. Fehlbedienungs- und Fehlnutzungsrisiken sollten bereits infolge der systeminhärenten Selbstregulierung einer OC-Ampelsteuerung weitgehend entfallen. Missbrauchsrisiken etwa in Form einer gezielten Manipulation der Steuerungssoftware sind gerade bei geringer (externer) Systemüberwachung grundsätzlich gegeben und durch entsprechende Sicherheitsbarrieren wie bei anderen technischen Systemen zwar verringerbare, jedoch nicht zu vermeidende. Missbrauch jenseits der Verkehrssteuerung wäre dann möglich, wenn Sensoren der Ampelsoftware nicht nur (anonym) die Zahl und Frequenz einer Stelle passierender Fahrzeuge übermitteln, sondern z.B. wie bei den jetzt auf Autobahnen installierten Mautkameras oder bei Navigationssystemen mit floating phones (Handy-Ortung) Informationen über das Fahrzeug und seinen Besitzer oder Fahrer anfallen würden. Systeminhärente (Komplexitäts-)Risiken sind einerseits durch die Möglichkeit kontraproduktiver Effekte bei großräumiger dezentraler Ampelsteuerung und andererseits durch mögliche unerwünschte Emergenzen (wie der Extremfall von allen Ampeln an einer Kreuzung auf Grün-Stellung) gegeben, die jedoch in beiden Fällen (durch entsprechende Programmierung) als gering und beherrschbar einzustufen sind.

Die sozialen Risiken sind m.E. als relativ begrenzt und beherrschbar einzuschätzen. Die Notwendigkeit zur Anpassung an nicht standardisierte Ampelschaltungen erscheint u.E. im Allgemeinen problemlos. Während psychische, semiotisch-symbolische, normative, ordinative und physisch-ökologische Risiken nicht nur von einer OC-Ampelsteuerung, sondern allgemein von bestehenden Ampelsteuerungssystemen nur sehr eingeschränkt erkennbar sind, ist die Abklärung ihrer operativen Risiken bislang nicht hinreichend möglich, da eine OC-Ampelsteuerung noch nicht fertig entwickelt ist und praktisch eingesetzt wird. Kritisch könnten die Kosten solcher Systeme sein, die bis jetzt noch nicht wirklich hinreichend abschätzbar sind und die u.a. vor allem den erforderlichen Aufwand für die Kommunikation zwischen den Ampelanlagen oder für die notwendigerweise vielerorts im Boden zu verankernden Sensoren betreffen. Falls sich die Systemkosten jedoch von den Kosten anderer Ampelsteuerungssysteme nicht signifikant unterscheiden, wie von den an diesem Vorhaben der Universität Hannover Beteiligten vermutet (vgl. Pisko 2008), dann sollten die infolge systembedingter Zeitersparnis andernorts eingesparten Kosten diese mehr als kompensieren.

Während bei den bisherigen Überlegungen die Funktionsfähigkeit und gelungene Implementation einer OC-Ampelsteuerung unterstellt wurden, sind diese Voraussetzungen bislang noch nicht gegeben, sodass weder ihre soziale Akzeptanz bereits gesichert ist, deren Bestehen im Falle ihres Funktionierens jedoch unter ‚Normalbedingungen‘ kaum problematisch sein dürfte, noch ihre Vorteilhaftigkeit und Konkurrenzfähigkeit gegenüber anderen (smarten) Ampelsystemen erwiesen sind, noch die erforderlichen generellen Standards und rechtlichen Regulierungen verabschiedet worden sind. Von daher ist ihr tatsächlicher zukünftiger breiter Einsatz derzeit noch relativ offen. Realistische gesamtgesellschaftliche (Katastrophen-)Risiken einer OC-Ampelsteuerung lassen sich bislang kaum erkennen. Bei dieser Aussage ist allerdings die Prämisse zu beachten, dass es hier um die spezifischen Risiken einer Ampelsteuerung mithilfe von OC (oder anderer smarter Systeme) geht und nicht um die sehr wohl vorhandenen grundsätzlichen Risiken von Verkehrssteuerung insgesamt und von (Massen-)Verkehr allgemein. Auf dieser übergeordneten Ebene wären natürlich sehr viel mehr Chancen und Risiken anzuführen, die jedoch kaum etwas mit OC-Ampelsteuerung als solcher zu tun haben.

Grundsätzlich erscheint der Bereich der Ampelsteuerung jedenfalls als ein geeignetes ‚Spielfeld‘, um OC-Techniken in der Praxis zu erproben, ihre Vorteilhaftigkeit zu demonstrieren, sie zunächst

langsam einzuführen, die erforderlichen infrastrukturellen und rechtlichen Rahmenbedingungen zu schaffen und ihre soziale Akzeptanz (im Wege ihrer praktischen Erprobung) zu gewinnen.

5.2 Adaptive Kamerasysteme

Mithilfe von OC kann sich ein Kameranetzwerk selbst konfigurieren (Wahl eines für die Verfolgung verantwortlichen Masterknotens), optimieren (ständige Maximierung des überwachten Raumes), heilen und schützen (z.B. erkennen, wenn ein Knoten ausfällt) und dadurch adaptive Kamerasysteme verbessern. Sowohl bessere Bilderkennung der als auch Kommunikationsalgorithmen zwischen den Kameras werden entwickelt und im Simulator getestet, aber bislang noch nicht gekoppelt, sodass der tatsächliche Einsatz von OC-Kamerasystemen noch bevorsteht. (vgl. Breu 2008, Hoffmann/Hähner 2007, Hoffmann et al. 2008, Müller 2008a).¹²⁹

Anders als bei einer OC-Ampelsteuerung ist zwar auch bei adaptiven Kamerasystemen der *technische* Zweck eindeutig, nämlich die (autonome) Verschaltung von vielen Kameras zwecks Optimierung des überwachten Raums (Aufnahme und das räumliche Verfolgen von bildlich beobachtbaren Objekten und Bewegungen).¹³⁰ Die diesbezüglich möglichen und erkennbaren Anwendungsgebiete sind allerdings nahezu unbegrenzt, und nicht auf Verkehrsampeln oder einen anderen einzelnen sozialen Zweck beschränkt. Insofern sind sowohl soziale Chancen als auch soziale Risiken adaptiver Kamerasysteme zweifellos vielfältiger Natur, wobei die Nutzung des OC-Ansatzes weniger zu prinzipiell neuartigen Risiken, als vielmehr häufig zu deren Amplifizierung beitragen dürfte. Insofern adaptive Kamerasysteme aus der Sicht ihrer Nutzer zur besseren bzw. überhaupt erst möglichen Beobachtung und Datensammlung über sie interessierende Objekte, deren Bewegung und Verhaltensweisen beitragen, sind sie im Falle ihrer (bislang allerdings teils nur eingeschränkt gegebenen) Funktionsfähigkeit eindeutig von Vorteil, zumindest solange die anfallenden Kosten und der Aufwand für die Datenauswertung als akzeptabel eingestuft werden. Daher rührt auch ihr primärer Einsatz in solchen Anwendungsgebieten, wo *economies of scale* bestehen, wie in den Fällen von assisted living/health care, der Überwachung (großer) sicherheitskritischer Bereiche, von Industrie und von Kundenanalyse. Zugleich stellen adaptive Kamerasysteme ein Beispiel dafür dar, dass aufgrund tendenziell gegenläufiger Interessenlagen von Nutzern und Gefilmten die Chancen der Nutzer eher die Risiken der beobachteten und gefilmten Akteure darstellen, wobei sie jedoch auch (indirekt) davon profitieren mögen (z.B. Videokameras in Verkehrsstationen oder U-Bahnen zur Ermittlung von Tätern) und wo diese Risiken, abgesehen von der zwangsläufigen Verletzung von Privacy, von der Art der Nutzung und den Möglichkeiten des Missbrauchs abhängen.

Was nun systematisch die technischen Potenziale, Anwendungs- und Nutzungsmöglichkeiten, experimentellen Optionen und systeminhärenten (Komplexitäts-)Chancen OC-gestützter adaptiver Kamerasysteme angeht, so sind erstere in ihren Entwicklungsmöglichkeiten (einschließlich der Verknüpfung von und des Austausches zwischen mehreren, an unterschiedlichen Orten befindlichen Kameras) als immer noch beträchtlich, in ihrer Funktionalität hingegen als weitgehend festgelegt (systematische Beobachtung und Aufnahme durch Kameras) einzuschätzen. Die Bereiche

¹²⁹ Allerdings befindet sich ein entsprechendes Forschungsvorhaben gegenwärtig in der Genehmigungsphase.

¹³⁰ Gegenüber anderen bereits auf dem Markt verfügbaren, mit einer Recheneinheit ausgestatteten, nur auffälliges digitales Bildmaterial an einen Zentralrechner weiterleitenden Smart Cameras sind die einzelnen Smart Cameras in OC-basierten adaptiven Kamerasystemen über Netzwerke untereinander verbunden, können dadurch miteinander kommunizieren und lösen damit das Problem der mangelnden Flexibilität von Smart Cameras.

möglicher Anwendungs- und Nutzungsmöglichkeiten sind wie gesagt vielfältiger Natur und dürften eher via Kostenlimitierung, auswertbarer Datenmenge und rechtlicher Beschränkungen begrenzt bleiben. Experimentelle Optionen nicht erwarteter Nutzungsmöglichkeiten dürften eher unerwartete Entwicklungsoptionen bei der Software sowie weitere Anwendungsgebiete und weniger neuartige technische Arrangements betreffen. Systeminhärente Chancen können aus dem vielfältigen Einsatz adaptiver Kamerasysteme resultieren, die sich z.B. auf neue Software-Entwicklungen und die Verknüpfung oder die Selektion von Videoaufnahmen beziehen könnten.

In der Sozialdimension sind Chancen adaptiver Kamerasysteme auf allen Ebenen erkennbar. Psychologisch sind verbesserte Nutzungs-, Informations- und Kontrollmöglichkeiten zu nennen. Semiotisch-symbolisch sind neue Darstellungsmuster und Fachsprachen denkbar, die z.B. verschiedene Anwendungsgebiete und Nutzungsformen sprachlich und interpretativ aufeinander beziehen und aus einem übergeordneten Blickwinkel einzuordnen erlauben. Normativ sind Chancen eher in der funktions- und gruppenspezifisch erwünschten, anwendungsspezifisch geregelten Ausbreitung der ethischen und rechtlichen Akzeptabilität optischer Beobachtung und Datenspeicherung zu sehen, während die erforderlichen technischen Standardisierungen und Normierungen sowie die rechtlichen Regulierungen eher als Notwendigkeit denn als Chance einzustufen sind, und Fragen von Zulässigkeit, Datenschutz und Privacy vorrangig soziale Risiken auf normativer Ebene darstellen. Ordinativ bieten sich vermutlich zusätzliche (informationelle) Koordinations- und Abstimmungsoptionen an; allerdings dürfte es sich bei Management und Verwaltung in den betreffenden Anwendungsgebieten um Erweiterungen und optische Optionen handeln (z.B. auch Filmaustausch unter sich kennenden Personen), die wiederum eher als notwendige Aufgabe denn als Chance einzuordnen sind. Und wiederum betreffen die Gewährleistung und Organisation von Datenschutz und Privacy, einschließlich der Erfassung und Sanktionierung von Verstößen, auch auf ordinativer Ebene genuin soziale Risiken. Allokativ bieten sich (gerade bei OC-gestützten adaptiven Kamerasystemen) Chancen der Kosteneinsparung z.B. durch die Substitution personalaufwändiger Betreuung, Kontrolle oder Überwachung, solange die zusätzlichen Kosten für die Kamerasysteme, Software und Datenauswertung sich – als allokativen Risiken – in Grenzen halten. Die Chancen adaptiver Kamerasysteme kommen vor allem auf operativer Ebene zum Tragen, indem sie in einer Reihe von Anwendungsgebieten und Nutzungsmöglichkeiten erwünschte oder notwendige Arbeiten (rationell) ermöglichen, übernehmen und erleichtern können, wie bei assisted living/health care. Physisch-ökologisch bestehen die Chancen etwa darin, dass die substituierten Tätigkeiten umweltbelastender (und teils auch gesundheitsbelastender) sind und die zusätzlichen Nutzungsmöglichkeiten (z.B. Überwachung öffentlicher Räume) vergleichsweise wenige materiale Ressourcen benötigen und die dadurch ermöglichten Objekt- und Verhaltensnachweise mit geringeren, unter bisherigen Umständen aufwändigeren Ermittlungen und Nachweisprozeduren einhergehen.

Was die technischen Risiken adaptiver OC-Kamerasysteme anbelangt, so dürften sich genuine technische Fehlfunktionsrisiken einerseits in Grenzen halten, während andererseits die intendierte gezielte Erkennung und Verfolgung bestimmter beweglicher Objekte nicht immer erfolgreich verlaufen dürfte und adaptive Kamerasysteme (noch) an ihre Grenzen stoßen. Fehlbedienungs- und Fehlnutzungsrisiken sollten gerade im Falle von OC-basierten Kamerasystemen infolge der systeminhärenten Selbstregulierung weitgehend entfallen. Missbrauchsrisiken etwa in Form einer gezielten Manipulation der Steuerungs- und gegebenenfalls Bilderkennungs-Software sind gerade bei geringer (externer) Systemüberwachung grundsätzlich gegeben und durch entsprechende Sicherheitsbarrieren wie bei anderen technischen Systemen zwar verringerbar, jedoch nicht zu vermeiden. Systeminhärente (Komplexitäts-)Risiken sind – neben der bestehenden Möglichkeit kontraproduktiver Effekte bei dezentraler Kamerasteuerung und unerwünschter Emergenzen, die jedoch (durch entsprechende Programmierung) als gering und beherrschbar einzustufen sind – der unvermeidbare immanente Konflikt zwischen gewünschter gezielter Objekt- und Personenbeobach-

tung und -aufnahmespeicherung und dem Grundrecht auf Schutz der Privatsphäre. Dieser Konflikt besteht allerdings – wenn auch in unterschiedlichem Ausmaß – im Prinzip bei jeder systematischen (personenbezogenen) Datensammlung. Soziale Risiken adaptiver Kamerasysteme wurden auf normativer, ordinativer und allokativer Ebene bereits genannt. Zentral wird dabei die psychologische Ebene mangelnden Schutzes der Privatsphäre sein, dessen ausreichende Gewährleistung auf operativer Ebene mit signifikanten Problemen und Kosten verknüpft sein dürfte. Physisch-ökologische Risiken adaptiver Kamerasysteme können zum einen in der Unzahl an vielen Stellen angebrachter Kameras und der gezielten Beseitigung von für Beobachtungs- und Überwachungszwecke störenden Hindernissen in (öffentlichen) Räumen und zum anderen in psychosomatischen gesundheitlichen Belastungen infolge verstärkten (permanenten) Beobachtetwerdens liegen. Folgen einer stärker bildhaften Darstellung von Lebenswelten auf semiotisch-symbolischer Ebene wären genauer abzuschätzen, um damit möglicherweise verbundene Risiken zu identifizieren.

Während bei den bisherigen Überlegungen wiederum die Funktionsfähigkeit und gelungene Implementation OC-gestützter adaptiver Kamerasysteme unterstellt wurden, sind diese Voraussetzungen bislang allenfalls eingeschränkt gegeben, sodass ihre soziale Akzeptanz nicht nur aus Datenschutzgründen, sondern bei ihren Nutzern bislang auch wegen nicht zufriedenstellender Effektivität und Nutzbarkeit nicht bereits vorausgesetzt werden kann. Insbesondere müssen sich noch ihre Vorteilhaftigkeit und Konkurrenzfähigkeit gegenüber anderen smarten Kamerasystemen (vgl. Müller 2008a) erweisen, ebenso wie die erforderlichen generellen Standards und rechtlichen Regulierungen zu etablieren sind. Von daher ist ihr tatsächlicher zukünftiger breiter Einsatz derzeit noch relativ offen. Realistische gesamtgesellschaftliche (Katastrophen-)Risiken adaptiver Kamerasysteme könnten in ihrem maßgeblichen Beitrag zur sukzessiven weitgehenden Aushöhlung des Schutzes der Privatsphäre mit katastrophalen Folgewirkungen für gesellschaftliche Öffentlichkeit, Diskurs und Demokratie (vgl. Orwell 1984) liegen.¹³¹ Hierbei wäre allerdings davon auszugehen, dass adaptive Kamerasysteme wohl *nur ein* (wesentliches) Element eines solchen generellen Aushöhlungsprozesses wären. Andere gesamtgesellschaftliche Risiken sind derzeit eher nicht zu erkennen. Wiederum wird deutlich, dass es sich kaum um OC-spezifische Risiken adaptiver Kamerasysteme handelt, sondern primär um bereichs- und anwendungsspezifische Risiken ubiquitärer Datensammlung und -nutzung.

5.3 Logistik

Die Kosten logistischer Prozesse (Transportprozesse, Umschlag, Kommissionieren, Lagerprozesse, Verpackung, IuK-Prozesse; vgl. Arnold et al. 2008) sollen mithilfe von Selbststeuerung verringert werden, wobei bioanaloge, rationale und kombinierte Selbststeuerungsstrategien zum Tragen kommen können (Höhne 2009), die als formale Typen von Selbststeuerungsstrategien allerdings kaum als OC-spezifisch einzustufen sind. So existieren vielfältige Lösungsansätze, die in der Theorie einen leistungsfähigeren und robusteren Ablaufprozess im Bereich der Produktionsplanung und -steuerung ermöglichen, wobei einzelne Objekte der Logistikkette mithilfe von Selbststeuerungsalgorithmen selbständige Funktionen wahrnehmen. Die Potenziale und Grenzen der Evolution in der

¹³¹ Prinzipiell können sie in ihren Auswertungsmodalitäten auch restriktiv zugunsten eines verbesserten Datenschutzes programmiert werden. So bieten Smart Cameras gegenüber PC-basierten IBV-Systemen den Vorteil, dass unbedeutende Daten in der Kamera sofort gelöscht und nur auffälliges Verhalten, z.B. das Betreten einer verbotenen Zone überhaupt erst an die Zentrale weitergeleitet wird. Da bei großen Kamerasystemen immer noch IBV-Systeme effizienter sind, könnten OC-Techniken adaptive Kamerasysteme auch deshalb attraktiver machen können (vgl. Müller 2008a).

Logistik in Form der Selbststeuerung werden in dem von der Deutschen Forschungsgemeinschaft DFG geförderten Sonderforschungsbereich SFB 637 „Selbststeuerung logistischer Prozesse – Ein Paradigmenwechsel und seine Grenzen“ an der Universität Bremen untersucht (vgl. Scholz-Reiter 2007, Windt 2006, 2008). „Der in der Logistikforschung in den letzten Jahren zunehmend untersuchte Paradigmenwechsel von der konventionellen Fremdsteuerung logistischer Systeme hin zur Selbststeuerung dezentraler autonomer Systeme kann als Evolution in der Logistik bezeichnet werden, da dies eine scheinbare natürliche Weiterentwicklung ist, wie sie auch in anderen Wissenschaftsdisziplinen beobachtet werden kann. Beispielhaft sei hier die Informatik mit dem Trend zum Organic Computing sowie das Internet genannt, welches durch das dezentrale Routing eine große Flexibilität und Robustheit aufweist. Weiterhin ist aus der Biologie bekannt, dass sich soziale Insekten zu dezentral organisierten Systemen ohne eine zentrale Kontrollinstanz entwickeln, die eine hohe Adaptivität und Robustheit aufweisen.“ (Scholz-Reiter et al. 2007:1f (179f)) Tabelle 5.1 kennzeichnet diese Evolution der Planungs- und Steuerungsprozesse logistischer Objekte.

Laut Windt (2006:310) soll der Ansatz der Selbststeuerung intelligenter logistischer Objekte den Umgang mit dynamisch-komplexen (logistischen) Systemen verbessern und eine Erreichung logistischer Zielgrößen sicherstellen, wobei noch nachzuweisen ist, dass Selbststeuerung tatsächlich zu einer positiven Emergenz im Sinne einer diesbezüglich höheren Systemrobustheit führt. Der Einsatz von OC sollte dabei genau eine solche Selbststeuerung ermöglichen. Praktisch ist er nach Wissen des Autors allerdings bislang noch nirgends realisiert worden. Nutzbar wäre er im Prinzip in unterschiedlichsten logistischen Systemen. Grundsätzlich wäre OC-Selbststeuerung in der Logistik vor allem im Hinblick auf die praktische Systemoptimierung und nach Möglichkeit auf die Einsparung von (Personal-)Ressourcen vorteilhaft. Bis zum Einsatz generischer OC-Systeme in der Logistik bedarf es jedoch noch umfangreicher Entwicklungen und Praxistests.

Was die technischen Potenziale, Anwendungs- und Nutzungsmöglichkeiten, experimentellen Optionen und systeminhärenten (Komplexitäts-)Chancen von OC in der Logistik anbelangt, so betreffen erstere die selbstgesteuerte Optimierung logistischer Systeme, die insbesondere bei großen komplexen Systemen beachtliche Optimierungsmöglichkeiten gegenüber herkömmlichen Verfahren bieten sollten. Im Rahmen logistischer Systeme ist mit vielen Anwendungs- und Nutzungsmöglichkeiten zu rechnen, bei denen es jedoch im Kern um strukturanaloge Problemlagen gehen dürfte. Experimentelle Optionen und systeminhärente Chancen könnten nicht erwartete anderweitige Nutzungsoptionen und Steuerungsmöglichkeiten sein, ohne solche hier spezifizieren zu können.

Ähnlich wie bei OC-Ampelsteuerung betreffen die Chancen in der Sozialdimension Entlastung durch Selbstregulierung (ordinative Ebene), Zeitersparnis (allokative und operative Ebene im systemischen und primären Bereich, psychische Erleichterungen) und physisch-ökologische Immisionsminderung. Wie weit diese gegenüber bestehenden logistischen Systemen zu durchschlagenden Reduzierungen führen, wäre im Einzelnen festzustellen. Auf semiotisch-symbolischer Ebene könnte OC in der Logistik zur Entwicklung und Etablierung einer eigenen Fachsprache und Theorie der Logistik beitragen, die betriebswirtschaftliche und ingenieurwissenschaftliche Ansätze kombiniert, und damit allmählich auch auf normativer Ebene eine weitergehende Herausbildung logistischer Standards und Regulierungen induzieren.

Tabelle 5.1: Evolution der Planungs- und Steuerungsprozesse logistischer Objekte

Quelle: Pfohl 2007

Evolutionstufe	Datenhaltung *	Planung & Steuerung	Beispiel	Technologie
<u>1. klassische Sendungssteuerung</u> Manuelle Sendungsplanung und -steuerung durch die Empfängeradresse auf dem logistischen Objekt	ausschließlich dezentral (analog: am logistischen Objekt)	dezentral (manuell: durch den Mitarbeiter)	Paketpost	analoge Speichermedien (Adressaufkleber)
An jeder Station auf dem Transportweg wird der nächste Transportabschnitt auf Basis der Empfängeradresse ausgewählt.				
<u>2. manuelle Sendungssteuerung</u> Manuelle Sendungsplanung und -steuerung nach Erfassung der Auftragsdaten (ggf. mit DV-System-Unterstützung)	zentral (manuell, Papier)	zentral	Tourenplanung	analoge Speichermedien (z.B. Transportbegleitpapiere); Planung mittels Plantafeln
Sendungs-, Auftrags- und Statusdaten werden manuell erfasst und zur Transportsteuerung ausgewertet.				
<u>3. automatische Sendungssteuerung</u> Automatische Sendungsplanung und -steuerung durch virtuelle Vertreter des logistischen Objektes im zentralen DV-System	zentral (DV-System)	zentral / dezentral (Netzwerkknoten)	Klassisches Planungs- und Steuerungssystem (z.B. Tourenplanung, PPS)	Analoge, ggf. optische Speichermedien (Adressaufkleber, Barcode, Transportbegleitpapiere)
Sendungs-, Auftrags- und Statusdaten werden systemtechnisch erfasst und zur Transportsteuerung ausgewertet. Iterative Optimierung von Dispositionsprozessen in definierbaren Zeitabständen ist möglich.				
<u>4. eingeschränkte Selbststeuerung</u> (logisch dezentral) autonome Sendungsplanung und -steuerung durch virtuelle Vertreter des logistischen Objektes im zentralen DV-System	zentral (DV-System)	zentral	internetbasierte Frachtbörse auf Basis eines Agentensystem	zentrales Agentensystem
Agent als virtueller Vertreter des logistischen Objekts agiert auf zentralen Planungs- und Steuerungssystem.				
<u>5. absolute Selbststeuerung</u> (logisch und physisch dezentral) autonome Sendungsplanung und -steuerung durch das logistische Objekt	dezentral (am logistischen Objekt und in relevanten DV-Systemen der Prozessteilnehmer)	dezentral (automatisch: durch das logistische Objekt)	Selbststeuernde Planungs- und Steuerungssysteme	RFID, dezentrales, autonomes Agentensystem
Logistisches Objekt verfügt über eigene Rechen- und Speicherkapazität sowie die Fähigkeit zur Kommunikation. Dadurch ist das Vorhalten eines eigenen Zielsystems sowie das autonome Treffen von Entscheidungen möglich. Iterative Optimierung von Dispositionsprozessen in Echtzeit.				
* Die Datenhaltung ist bezogen auf für Planung und Steuerung relevante Daten.				

Hinsichtlich der technischen Risiken von OC in der Logistik dürften sich technische Fehlfunktionen bei entsprechend programmierten Sicherheitsmargen in Grenzen halten, wobei infolge der Selbststeuerung zunächst nicht bemerkte suboptimale logistische Arrangements mit beträchtlichen Folgewirkungen und Zusatzkosten verbunden sein können, jedoch nicht müssen, und ein hierbei ent-

stehender Systemzusammenbruch leicht gravierende Folgen haben kann. Fehlbedienungs- und Fehlnutzungsrisiken sollten hingegen infolge der systeminhärenten Selbststeuerung solcher logistischer Systeme weitgehend entfallen. Missbrauchsrisiken etwa in Form einer gezielten Manipulation der Steuerungssoftware sind wiederum gerade bei geringer (externer) Systemüberwachung grundsätzlich gegeben und durch entsprechende Sicherheitsbarrieren wie bei anderen technischen Systemen zwar verringerbar, jedoch nicht zu vermeiden. Missbrauch könnte in gezielter Störung logistischer Systeme oder in ihrer gezielter (disfunktionalen) Umorientierung z.B. zugunsten bestimmter Empfänger von Lieferungen sein. Systeminhärente (Komplexitäts-)Risiken sind durch die Möglichkeit unerwünschter negativer Emergenzen und misslingende selbstgesteuerte Anpassung logistischer Systeme an sich ändernde Umwelten gegeben, wobei es jedoch laut Windt durchaus systemtechnisch möglich ist, unerwünschte emergente Effekte zu vermeiden.

Die sozialen Risiken von OC in der Logistik sind gerade im Falle großer Systeme durchaus vorhanden, jedoch solange als relativ begrenzt und beherrschbar einzuordnen, solange es lediglich zu suboptimalen logistischen Arrangements mit vermeidbaren Engpässen kommt. Natürlich können aufgrund des Vertrauens auf gelingende Selbststeuerung damit beträchtliche ökonomische Zusatzkosten verbunden sein, was im Prinzip für jegliche großtechnischen Systeme gilt. Entscheidend scheinen u.E. die operativen Risiken zu sein, die noch genauer abgeschätzt werden müssten. Die übrigen sozialen Risikodimensionen dürften eher mit indirekten Folgewirkungen von OC in der Logistik zusammenhängen und im Falle funktionsfähiger logistischer OC-Systeme geringe Bedeutung besitzen.

Wie in den beiden anderen Fällen gibt es in der Logistik zwar inzwischen einige Erfahrung mit einzelne Elemente der gesamten Logistikkette selbst organisierenden Systemen, jedoch noch keine genuine OC-Nutzung. Von daher ist ihre soziale Akzeptanz bislang nicht gesichert, im Falle ihres Funktionierens jedoch unter ‚Normalbedingungen‘ voraussichtlich nicht allzu problematisch. Sie hätte allerdings erst noch ihre Vorteilhaftigkeit und Konkurrenzfähigkeit gegenüber anderen (smarten) Logistiksystemen erweisen, wozu auch noch die erforderlichen generellen Standards und rechtlichen Regulierungen zu verabschieden wären. Von daher ist ihr tatsächlicher zukünftiger breiter Einsatz derzeit noch offen. Realistische gesamtgesellschaftliche (Katastrophen-)Risiken von OC in der Logistik lassen sich bislang nur schwer erkennen. Allerdings wären auch die durchaus vorhandenen grundsätzlichen, nicht OC-spezifischen Risiken komplex-dynamischer Logistiksysteme erst noch näher zu betrachten.

Wie die Ampelsteuerung scheint somit auch die Logistik ein geeignetes ‚Spielfeld‘ für die praktische Erprobung, Demonstration und (allmähliche) Einführung von OC-Techniken darzustellen, zumal diese gut an bestehende, sich bereits partiell selbst organisierende Logistiksysteme anknüpfen und sie ihrem Ziel der Selbststeuerung näher bringen können. Außerdem ist die Kooperationsbereitschaft von Logistik-Unternehmen bzw. auf Logistiksysteme stark angewiesenen Unternehmen tendenziell größer als bei anderen Industrieunternehmen, weil der Einsatz von OC-Systemen als schrittweise realisierbar eingestuft und erwartet werden kann und dessen Mehrwert des klar erkennbar ist.

5.4 Vergleichende Zusammenfassung

OC erschließt im Prinzip in allen drei Anwendungen neue Funktionalitäten, die sich aus seinen generischen Eigenschaften ergeben. So kann sich ein OC-Kameranetzwerk selbst konfigurieren, optimieren und auch heilen und schützen, oder eine OC-Ampelsteuerung kann sich ohne zentrale Steuerung dezentral selbst konfigurieren und optimieren. In der Logistik geht damit wie gesagt ein

gewisser Paradigmenwechsel von der konventionellen Fremdsteuerung logistischer Systeme hin zur Selbststeuerung dezentraler autonomer Systeme einher. OC-Systeme versprechen jeweils zweckbezogen deutlich erkennbare Verbesserungen. Der daraus resultierende (ökonomische) Ertrag und Mehrwert gegenüber anderen (konventionellen) Steuerungssystemen bleibt im Allgemeinen jedoch vorerst (anwendungsspezifisch) relativ begrenzt.¹³²

Bislang wird OC in der Praxis noch in keinem Fall kommerziell genutzt. Am weitesten ist die Entwicklung für einzelne Objekte der Logistikkette sowie im Bereich adaptiver Kamerasysteme fortgeschritten, wo smarte Kameranetzwerke mit Gesichtserkennungsalgorithmen, Verfolgungsalgorithmen und Kommunikationsalgorithmen erprobt und getestet werden. Im Bereich der Ampelsteuerung, die mehr als adaptive Kamerasysteme von noch nicht bestehenden (rechtlichen) Standards und Regulierungen abhängt, werden OC-Systeme bislang nur in Simulationen getestet. In der Logistik werden große Potenziale in der (bioanalogen, rationalen oder kombinierten) Selbststeuerung, in Adaptivität und Selbstoptimierung gesehen und diesbezügliche Algorithmen entwickelt, ohne dass es sich hierbei bereits um genuine OC-Systeme handelt. In allen drei Anwendungsfeldern muss sich OC gegenüber bestehenden konkurrierenden (konventionellen) Methoden und Verfahren erst noch durchsetzen, und hierfür seine technische Überlegenheit, Kostengünstigkeit und rechtliche Einbettung nachweisen. All dies kann zwar als mittelfristig durchaus möglich, aber bislang weder als theoretisch gesichert noch praktisch belegt eingestuft werden.

Alle drei Anwendungen beziehen sich auf klar definierte technische Zwecke: Verbesserung des Verkehrsflusses, Aufnahme und räumliches Verfolgen von bildlich beobachtbaren Objekten und Bewegungen, Reduzierung der Kosten logistischer Prozesse. Während diese bei der Ampelsteuerung und in der Logistik sozial wenig kontrovers sind, kollidiert dieser Zweck bei adaptiven Kamerasystemen häufig mit den als grundsätzlich legitim erachteten Bedürfnissen nach Privacy und damit verbundenen rechtlichen Vorgaben des Datenschutzes. Während die mit diesen (technischen) Zwecken verbundenen sozialen Nutzungsmöglichkeiten – abgesehen von experimentellen Optionen, Missbrauchsrisiken und möglichen systeminhärenten (Komplexitäts-)Chancen und Risiken – bei Ampelsteuerung und (im Sinne der Optimierung logistischer Prozesse) auch bei der Logistik im Wesentlichen auf eine Nutzungsoption beschränkt bleiben, sind adaptive Kamerasysteme mit einem breiten möglichen Anwendungsspektrum und von daher mit vielfältigen sozialen Chancen und sozialen Risiken verbunden.

Überwiegend gehen mit den betrachteten Anwendungen kaum OC-spezifische Risiken einher, sondern solche, die diesen Anwendungen generell eigen sind. OC amplifiziert sie jedoch häufig (implizit), z.B. das Risiko der unzulässigen oder unerwünschten Beobachtung durch adaptive Kamerasysteme.

Technische Fehlfunktions- und Fehlnutzungsrisiken sind für alle drei Anwendungen durch geeignete Vorkehrungen und Programmierung als relativ begrenzt und beherrschbar einzuschätzen. Hingegen ist der Spielraum für Missbrauchsrisiken aufgrund der Autonomie und Selbstorganisation von OC-Systemen als tendenziell vergrößert einzustufen.

¹³² In solchen Fällen, in denen das OC-System neuartige, bisher nicht realisierbare Nutzungsoptionen erlaubt, kann der (perzipierte) Mehrwert natürlich deutlich größer sein.

Soziale Chancen bestehen bei allen drei Anwendungen in den meisten Dimensionen der Soziosphäre, jedoch ohne signifikant herauszuragen.

Während die sozialen Risiken für Ampelsteuerung und Logistik grundsätzlich überwiegend begrenzbar und beherrschbar erscheinen, sind sie bei adaptiven Kamerasystemen aufgrund des mit ihnen zumeist einhergehenden aufgezeigten Grundkonflikts zu erwarten und nur (unter zusätzlichen finanziellen und sozialen Kosten) begrenzt zu minimieren.

Genuine OC-Chancen und Risiken, die aus den Charakteristika der Selbstorganisation, Autonomie und Emergenz von OC herrühren, lassen sich im Prinzip relativ eindeutig ausmachen und benennen, sind in ihrem Stellenwert (im gesamten Chancen-Risiko-Portfolio) aber außer in Katastrophenfällen als wahrscheinlich eher sekundär einzustufen: weder erscheinen die dadurch implizierten Risiken außerordentlich groß, da sie sich unter der Voraussetzung kontrollierter Emergenz limitieren lassen, noch sind die Mehrerträge durch autonome Selbstorganisation überwältigend.

Der Vergleich der drei Fallbeispiele verdeutlicht, wie unterschiedlich Ausmaß und Art der *sozialen* Chancen und Risiken von OC strukturiert sein können, wie sehr sie von der konkreten Systemgestaltung und vom Kontext abhängen, und wie wenig sie OC-spezifisch sind. Größere (jedoch wiederum fallspezifische) OC-Spezifität ist hingegen für ihre *technischen* Chancen und Risiken anzunehmen.

Insofern bislang OC in keiner der Anwendungen implementiert wurde und breit genutzt wird, ist die soziale Akzeptanz solcher OC-Systeme noch offen, auch wenn sie bestehende Systeme der Ampelsteuerung, der Kameraüberwachung oder der Logistik lediglich allmählich verbessern und substituieren mögen.

Abschließend sei noch festgehalten, dass die in den Anwendungsfeldern strukturell verankerten sozialen Grundproblematiken durch OC-Systeme nicht aufgelöst, sondern durch die mit ihnen einhergehenden technischen Verbesserungen tendenziell verdeckt und damit implizit eher vergrößert werden. Dies ist allerdings auch nicht beabsichtigt und sollte daher nicht erwartet werden. So wird der Vorrang eines auf (privaten) Automobilen und ausgebauten Straßennetzes beruhenden massenhaften Individualverkehrs samt seiner problematischen wirtschaftlichen, ökologischen, gesundheitlichen und sozialen Folgen durch eine optimierte Ampelsteuerung ebenso wenig in Frage gestellt wie die Notwendigkeit (global) verteilter Formen der Produktherstellung mit just-in-time Lieferungen durch eine OC-gestützte Logistik, was bei hohen Lagerhaltungs- und demgegenüber geringen Transportkosten aus einsehbaren ökonomischen Gründen mit umfangreichen Transporten einhergeht. Und ebenso wird durch OC-gestützte adaptive Kamerasysteme – auch bei positiv zu wertendem ambient assisted living – bislang kaum die grundlegende Problematik einer sozialstrukturell bedingten und als notwendig angesehenen verstärkten Überwachung von Räumen mit der ausufernden Beschränkung von Privacy angegangen.

6 Debatten über Chancen und Risiken von Organic Computing: Soziale Diskurse und Argumentationsanalyse

Die bisherigen Analysen des Forschungsfeldes von Organic Computing (insbesondere Abschnitt 4) sowie die Fallstudien (Abschnitt 5) zeigen, dass die von der OC-Forschung angestrebten Anwendungen erwartungsgemäß neben Chancen auch Risiken in sich bergen. Eine Einführung solcher Anwendungen wird daher voraussichtlich in der Öffentlichkeit kontrovers diskutiert werden. Daher werden in diesem Kapitel zunächst Charakteristika sozialer Diskurse resümiert (Abschnitt 6.1) und dargestellt, welche Diskurse bezüglich der OC-Anwendungen sich bereits herausgebildet haben (Abschnitt 6.2).

Da der Stand der OC-Forschung noch vielfach grundlagenorientiert ist (vgl. Abschnitt 3.4), lautete unsere Hypothese, dass öffentliche Diskurse noch keine breite Wirkung entfaltet haben. Um ihre rationalen Grundlagen vorwegzunehmen, sind unter Federführung des Instituts für Philosophie der FU Berlin so genannte Argumentationsanalysen erstellt worden. Ihr Ziel besteht darin, die derzeit vertretenen Argumente für und gegen einen Einsatz der OC-Anwendungen zu rekonstruieren und daraus Fragen abzuleiten, die für die Entscheidung über die Richtigkeit des Einsatzes einer OC-Anwendung geklärt werden müssten. Die Ergebnisse der Argumentationsanalysen werden in Abschnitt 6.3 sowie im Anhang II zusammengefasst.

6.1 Charakteristika sozialer Diskurse

Soziale Diskurse (vgl. Bora 2005, Foucault 1982, Habermas 1981, 1985, Luhmann 1986, Wodak/Meyer 2001) prägen (in modernen Gesellschaften) die Wahrnehmung und Interpretation der Chancen und Risiken, die Einbettung und die Etablierung von sowie die Muster des Umgang mit (kontroversen) Technologien maßgeblich mit.

(Öffentliche) Diskurse spielen (in modernen Gesellschaften) eine maßgebliche Rolle, insofern in ihnen qua Verknüpfung von (neuen) Problemrahmungen mit alltäglichen Deutungsmustern eine überzeugende Problemdiagnose (*diagnostic framing*), die Definition einer Problemlösung (*prognostic framing*) und die Mobilisierung von Handlungsmotiven (*motivational framing*) kombiniert werden (vgl. Snow/Benford 1988, Brand 2000, Brand et al 1997, Eder 1995). Diskurse werden damit zu einer regulierenden Instanz, die Bewusstsein und darüber hinaus auch sonstige gesellschaftliche Strukturen formieren (Huber 2001:274f). Mithilfe der Bezugnahme auf kulturelle Deutungsbestände und Symbole, der Eingängigkeit der präsentierten *story lines*, entsprechender ‚Framing‘/Rahmungsstrategien (vgl. Dahinden 2006, Gerhards 1992) und von Diskurskoalitionen versuchen die am Diskurs teilnehmenden (Konflikt-)Parteien, ihre Realitäts- und Problemdefinitionen durchzusetzen.¹³³

¹³³ Mit Huber (2001:276) sei hierbei ergänzend festgehalten, dass soziale (formative) Diskurse als kommunikative Interaktionen „auch in einer leidlich zivilisierten Gesellschaft immer wieder an Grenzen stoßen – Grenzen der Verständigungsfähigkeit oder solcher der Verständigungsbereitschaft; sei es als Grenzen der Bewusstseinsbildung, oder als Statusgrenzen oder als effektive Funktionsgrenzen. Dann geht etwas erst einmal nicht recht weiter, mit der Gefahr sich aufstauernde Probleme. Bei Erreichen solcher Grenzen besteht immer die Gefahr, dass man auf Gewalt als Interaktionsmittel zurückfällt. In Verallgemeinerung von Clausewitz' Definition des Krieges als der Fortsetzung der Politik mit

Diskurse sind durch einen gemeinsamen Gegenstand bestimmt, der die Anschlussfähigkeit von Aussagen thematisch begrenzt, und durch die jeweiligen systemspezifischen Regularien der Inklusion/Exklusion und Transformation von Informationen (Weingart et al. 2002:22). Denn in modernen Gesellschaften finden in den verschiedenen sozialen Funktionssystemen wie Wissenschaft, Politik, Medien unterschiedliche parallele Diskurse statt, die unterschiedliche Diskursprofile und -dynamiken aufweisen und sich durch Diskursinterferenzen wechselseitig beeinflussen können. Entsprechend unterscheiden sich die Rezeptions- und Verarbeitungsmuster von Kommunikation in verschiedenen sozialen Funktionssystemen, weil die Diskurse unterschiedliche kommunikative Risiken wie solche des Glaubwürdigkeitsverlusts, des Legitimationsverlusts oder des Verlusts von Marktchancen generieren (vgl. Keller 1997, Weingart et al. 2002).

In Diskursen, die in einem thematisch zusammenhängenden Diskursstrang, einer *story line* verlaufen, geht es um die Geltung von Realitätsdefinitionen und somit um semantische Auseinandersetzungen um Deutungshoheit. Die Diskursteilnehmer konkurrieren um die Durchsetzung spezifischer Problemdeutungen und ringen von daher letztlich um Diskurshegemonie. Zu diesem Zweck gehen sie Diskurskoalitionen ein. Die sich dabei entfaltende Diskursdynamik hängt ab von erstens der kognitiven Akzeptierbarkeit von Argumenten, d.h. der faktischen Glaubwürdigkeit der Argumente, zweitens der Vertrauenswürdigkeit der Argumentierenden, und drittens der positionalen Akzeptierbarkeit der im Diskurs vermittelten Inhalte und Ziele, d.h. der Frage, inwiefern sie personelle/institutionelle Positionen bestärken oder bedrohen (vgl. Hajer 1995). Ein etablierter Diskurs kann andere mögliche Diskurse, und deren Realitätsdefinition, ein- oder ausschließen. Damit wird selektioniert, was in einer konkreten Situation resonanz- und anschlussfähig ist und was ausgeschlossen wird.

Da soziale Diskurse als im weiten Sinne intentional geprägte gesellschaftliche Kommunikations- und Rahmungsprozesse jedweder Art je nach Entstehungs- und Gestaltungszusammenhang wie angedeutet recht unterschiedlich strukturiert sein können, ist es u.a. wichtig, zwischen Stakeholder-Diskursen, öffentlichen Debatten und (innerhalb dieser geführten) Expertendiskursen zumindest analytisch zu unterscheiden, weil deren Leitkriterien verschieden sind. Was in Stakeholder-Diskursen und öffentlichen Debatten ungeschieden bleibt, trennen Expertendiskurse: Themen und Interessen, objektive Tatsachen und politische Wertungen, und die Rollen und Kompetenzen von Experten und Gegenexperten. Im (Experten-)Diskurs gilt eine andere Rationalität als in der politischen Öffentlichkeit (vgl. Bora/Döbert 1993). Dem regulativen Ideal einer deliberativen Politik kommen Diskursverfahren darum sehr viel näher als Auseinandersetzungen in der Arena der massenmedialen Öffentlichkeit. Dabei bestimmen jedoch die Regeln der politischen Öffentlichkeit und nicht die Regeln des Expertendiskurses, ob und wie Diskursergebnisse auf eine (öffentliche) Kontroverse zurückwirken. Es ist allerdings eher die Ausnahme als die Regel, dass ihre Resonanz dadurch gesichert wird, dass sich die Hauptakteure der öffentlichen Kontroverse im Expertendiskurs geeinigt haben und mit ebendieser Nachricht in die öffentliche Arena zurückkehren (Daele 1996). Expertenwissen bleibt bei aller in der öffentlichen Debatte behaupteten Verschmelzung wissenschaftlicher und politisch-normativer Gesichtspunkte im Diskurs durchweg zentral. Allerdings unterscheidet sich die geforderte (disziplinäre) wissenschaftliche Expertise signifikant je nach den interessierenden Fragestellungen deutlich.

Das Mandat der Experten in diesen Diskursen ist letztlich ein politisches. Solange die doppelte Bodenlosigkeit der Expertise latent bleibt, bleibt es unangefochten. Jeder offene Konflikt aber hebt die

anderen Mitteln, kann man sagen: Gewaltanwendung ist die interaktive Fortsetzung gescheiterter Diskurse. Die Übergänge vom kultivierten Diskurs zur nackten Gewalt sind fließend. Wie man weiß, gibt es außer Mord auch Rufmord. Ebenso kann man etwas oder jemanden totschießen.“

Latenz auf. Die Bodenlosigkeit der Expertise wird im Diskurs in voller Schärfe exponiert. Experten geben auf Diskursebene unter dem Druck solcher Kritik zumeist die Zuständigkeit für die Bewertung an die Gesellschaft, also an demokratische Entscheidungsverfahren zurück. Sie verteidigen nur mehr ein eingeschränktes Mandat, nämlich ihre fachliche Zuständigkeit für die Klärung empirischer Sachverhalte. Schließlich ist die Wissenschaft die letzte Rückzugslinie (Daele 1996).

Im Hinblick auf die Wirkungs- und Rezeptionsmuster sozialer Diskurse ist mit Huber (2001:274) festzuhalten: „Nicht nur sind gesellschaftliche Diskurse weit davon entfernt, bloße Reflexionen auf anderweitige Gegebenheiten und sich selbst zu sein. Diskurse vollziehen vielmehr die gesellschaftliche Bewusstseinsbildung, die Wissens-, Werte- und Willensbildung, aus der heraus formative, effektuative und divisionale Strukturen¹³⁴ originär erschaffen oder fortgebildet oder forterhalten werden.“ Soziale Diskurse sind somit von maßgeblicher Bedeutung für Prozesse sozialer Strukturbildung und sozialen Wandels, wobei sie wesentlich als *mind framing* zum Tragen kommen; denn es sind letztlich die Menschen, die ihre Geschichte auf der Basis ihrer Vorstellungen und Absichten selbst gestalten.

Ob und wie allerdings im Einzelnen je spezifische soziale Diskurse innerhalb und jenseits der Diskursgemeinschaften rezipiert und wirksam werden, hängt – wie bei anderen sozialen Prozessen auch – insbesondere von folgenden Faktoren ab: die (veränderliche) soziale Relevanz des Diskursthemas, die Interessenlage der den Diskurs strukturierenden Akteure, die (subsystemspezifische) kommunikative Anschlussfähigkeit des Diskurses und seine Resonanzfähigkeit in anderen gesellschaftlichen Teilsystemen. Dabei spielt auch eine Rolle, ob es im Diskurs vorrangig um die Klärung strittiger Sachverhalte oder um die Umsetzung beschlossener Maßnahmen geht. Somit bestimmen etwa subsystemspezifische (organisationsbezogene) Kriterien stark, ob Diskursbeteiligung und -ergebnisse zum Tragen kommen oder nicht; denn für die beteiligten Akteure macht es im Falle von diesen Kriterien nicht genügenden Diskursverläufen selten Sinn – und hat zumeist einen beträchtlichen Preis –, (z.B. als wissenschaftlich gültig behauptete) Diskursergebnisse nicht nur zur Kenntnis zu nehmen, sondern gar auch verhaltensrelevant (in der Organisation) umzusetzen.

6.2 IT- und OC-Diskurse

Um (moderne) Informationstechnologien und deren Anwendungen gibt es durchaus einen gesellschaftlichen Diskurs mit diesen gerade skizzierten Kennzeichen, der auch kritische Aspekte ihrer Muster und Folgewirkungen erörtert, wie insbesondere etwa Datenmissbrauch etc., der infolge bestehender Interessenlagen und technischer Optionen vor dem Hintergrund aktueller Fälle systematisch zu erwarten ist und den eine Reihe skandalöser Praktiken in jüngster Zeit belegen. Dieser Diskurs befasst sich in Maßen auch mit smarten IT-Systemen, im Wesentlichen konzentriert auf mit ihnen befassten Akteuren (vgl. Alahuhta et al. 2006, ENISA 2007a, 2007b, 2007c, Hilty et al. 2003, 2004, Kündig/Bütschi 2008, Mattern 2007, Wright et al. 2006, 2008). Hingegen findet speziell im

¹³⁴ Mit diesen Begriffen benennt Huber (2001:27ff) grundlegende Strukturdimensionen moderner Gesellschaften, nämlich ihre divisionale Struktur, die die sozialen Verhältnisse und positionale Struktur zwischen Akteuren sowie deren primäre und sich über Institutionen manifestierende sekundäre Beziehungen markiert, sowie ihre Funktionsstruktur, bei der sich zunächst grundlegend eine formative, jedwede kulturellen und politischen Prozesse umfassende Funktionsebene und eine effektuative, ordinative, ökonomische und operative Subsysteme beinhaltende Funktionsebene unterscheiden lassen, wobei sich formative Funktionen von den effektuativen dadurch unterscheiden, „dass formative Prozesse einen Subjektbezug besitzen, effektuative Prozesse dagegen einen bloßen Dingstatus. Dieser mag aktiv, automatisch, dynamisch selbstorganisierend sein, nicht aber autonom.“ (Huber 2001:40f)

Bereich OC trotz Offenheit der es tragenden (wissenschaftlichen) Akteure bislang kaum ein (solcher) Diskurs statt. Wie Beispiele anderer Technologien wie z.B. Nanotechnologien oder Carbon Capture and Storage (CCS) belegen, schließt dies – in Verbindung mit einer zukünftigen breiten Nutzung von OC – die (plötzliche) Entwicklung eines genuinen OC-Diskurses keineswegs aus.

Was die (soziale) Struktur des bisherigen (weitgehend im Wissenschaftssystem geführten) Diskurses um OC anbelangt, so lässt sich diese vor allem durch drei Merkmale kennzeichnen: (1) Bislang handelt es sich um einen reinen Expertendiskurs ohne öffentliche Parallel-Diskurse. (2) Der OC-Diskurs ist in lockerer Form in allgemeine Diskurse um IT-Technologien eingebunden. (3) Er findet ohne fundamentale Kontroversen statt; am ehesten existiert noch eine Kontroverse zwischen (regelungstechnischen) Traditionalisten und OC-Enthusiasten um die generische Neuartigkeit und Eigenständigkeit von OC.

6.3 Charakteristika von Argumentationsanalysen

Auch wenn die Debatten um OC-Anwendungen den Raum von Expertendiskursen noch nicht verlassen haben, werden bereits heute gemeinwohlorientierte Argumente für oder gegen den Einsatz von OC-Systemen in spezifischen Anwendungskontexten ausgetauscht. Diese Argumente könnten durchaus den rationalen Kern einer zukünftigen Debatte in der Öffentlichkeit bilden.

Im Rahmen einer Argumentationsanalyse werden die vorgebrachten Argumente für oder gegen den Einsatz von OC-Systemen logisch rekonstruiert und in Form von Argumentlandkarten visuell dargestellt. Die logische Rekonstruktion der Argumente expliziert die ihnen zugrunde liegenden Prämissen. Dadurch wird es möglich, einen Fragenkatalog zu erstellen. Dieser beinhaltet Fragen, die entschieden werden müssen, um den Einsatz von OC-Anwendungen zu rechtfertigen. Einige dieser Fragen werden derart sein, dass sie am besten von OC-Experten beantwortet werden können. Andere hingegen nicht. Dies werden Fragen sein, deren Beantwortung normative Überzeugungen involviert.

Das Ziel der Argumentanalyse besteht nun darin, diese Fragen herauszuarbeiten, um die möglichen zukünftigen Kontroversen besser einschätzen zu können.

Woher kommen die Argumente?

Der Argumentanalyse wurden Pro-OC-Argumente aus drei Quellen zugrunde gelegt: erstens aus den Texten der Projektpartner¹³⁵, zweitens aus den Diskussionen in den Projekt-Workshops¹³⁶, drittens aus einer Reihe von Interviews mit projekt-externen OC-Experten.¹³⁷

135 Bernard, Y., 2009a. Charakterisierungen der Organic Computing-Ansätze aus den Interviews.; Bernard, Y., 2009b. Herausforderungen des Organic Computing.; Bernard, Y., 2009c. OC und aktuelle Trends im Software Engineering.; Conrad, J., 2009. Chancen und Risiken selbstorganisierender adaptiver Systeme.; IÖW, Leibniz Universität Hannover & Freie Universität Berlin, 2009. Selbstorganisierende adaptive Systeme: Analyse der Chancen und Risiken sowie der Gestaltungsansätze neuer IKT – Ansätze;

136 Am 25. Mai 2009 fand ein Projekt-Workshop in Hannover statt, der eigens der Diskussion der Argumentlandkarten gewidmet war. Dieses Treffen war äußerst produktiv und führte zu einigen grundsätzlichen Änderungen und Ergänzungen in den Landkarten. Auch auf dem Abschlussworkshop wurde noch einmal ausführlich über die Endfassung der Argumentlandkarten diskutiert.

Schwieriger war es, Contra-OC-Argumente zu gewinnen, da es bisher aufgrund des frühen Stadiums der OC-Systeme weder eine kontroverse Fachdebatte, noch eine kontroverse öffentliche Debatte gibt. Deswegen wurde versucht, rationale Gegenpositionen zu erschließen. Dies wurde erheblich dadurch erleichtert, dass sich viele Äußerungen der OC-Proponenten bereits als Antworten auf mögliche und nahe liegende Kritiken verstehen lassen, so dass man die Leerstellen in der Debatte nur noch auszufüllen brauchte. An anderen Stellen bot sich stattdessen ein Trial-And-Error-Verfahren an: In den ersten Rekonstruktionsrunden wurden neue Gegenargumente konstruiert und dann in den Diskussionen und Interviews mit den OC-Proponenten ausgetestet. Die Argumente, die diese Feuerprobe überstanden, wurden ebenfalls in die Debatte aufgenommen.

Was sind die Ergebnisse?

Die so gewonnenen Argumente wurden logisch rekonstruiert und zueinander in Beziehung gesetzt. Die so entstehende Debatte wurde in Argumentlandkarten visualisiert. Eine interaktive Version dieser Argumentlandkarten ist unter http://www.argunet.org/debates/debate/sokrates/chancen_und_risiken_von_organic_computing verfügbar.

Aus den Argumentlandkarten wiederum ließ sich anhand der zentralen Prämissen in der Debatte ablesen, welche Fragen für die Anwendung eines OC-Systems in einem bestimmten Anwendungskontext geklärt werden müssen, damit diese Anwendung als für die Betroffenen gut gerechtfertigt gelten kann. Diese Fragen wurden in einem Fragenkatalog zusammengestellt. In Tabelle 6.1 sind die identifizierten Fragen zur Beurteilung der Verhältnismäßigkeit des Einsatzes von OC-Systemen aufgelistet.

Eine vollständige Übersicht über die rekonstruierten Argumente, ihre Visualisierung in den Landkarten sowie der sich daraus ergebende Fragenkatalog sind dem Bericht im Anhang II beigelegt.

Was steht im Zentrum der Debatte?

Im Laufe des Projekts zeigte sich schnell, dass viele Argumente für oder gegen einen OC-Einsatz anwendungsspezifisch sind und nicht für alle OC-Systeme generell gelten. Um derartig anwendungsspezifische Argumente berücksichtigen zu können, ohne dadurch die Debatte in eine Vielzahl unabhängiger Teildebatten zerfallen zu lassen, wurde eine Hauptthese ins Zentrum der Debatte gestellt, die den Einsatz eines OC-Systems für einen einzelnen Anwendungskontext fordert, der aber nicht weiter spezifiziert wird: „Im Anwendungsfall x sollte ein OC-System eingesetzt werden.“

So konnten alle anwendungsspezifischen Argumente in die Debatte aufgenommen werden, ohne den Teilnehmern unplausible Generalisierungen unterstellen zu müssen. In Abhängigkeit von den Eigenschaften des Anwendungskontextes, in dem ein OC-System eingesetzt werden soll, werden unterschiedliche Argumente in der Debatte relevant oder irrelevant sein. Diese Eigenschaften werden jeweils im Fragenkatalog abgefragt.

137 Besonderer Dank gebührt Prof. Herkersdorf, Prof. Müller-Schloer und Prof. Rosenstiel, die in ausführlichen Interviews spezifische Fragen zu den für den Zwischenbericht erstellten Argumentlandkarten beantworteten. Diese Interviews führten zu der Ergänzung mehrerer neuer und der Umformulierung der bestehenden Argumente. Berücksichtigt wurden außerdem die Interviews, die Jobst Conrad mit OC-Experten auf dem OC-Workshop in Bochum 2009 und Eugen Pissarskoi und Christian Voigt auf der Cebit 2009 durchgeführt haben.

Welche Struktur hat die Debatte insgesamt?

Wie lässt sich nun der Einsatz eines OC-Systems in einem Anwendungskontext rational rechtfertigen? Typischerweise wird instrumentell argumentiert: Im Anwendungskontext herrscht Bedarf nach Komplexitätsbewältigung und OC-Systeme sind geeignete, verhältnismäßige und erforderliche Mittel, um diesen Zweck zu erfüllen.

Bedarf, Eignung, Verhältnismäßigkeit und Erforderlichkeit werden nun in der Debatte jeweils einzeln begründet, so dass sich vier Unterdebatten unterscheiden lassen. In der Rekonstruktion zeigte sich nun, dass sich nur für die Verhältnismäßigkeitsthese angreifende Argumente ergaben und dass sich auch nur in diesem Teil der Debatte Argumente fanden, die direkt gegen den Einsatz des OC-Systems sprechen.

Dies ist nicht erstaunlich: Mit der Verhältnismäßigkeitsthese wird behauptet, dass der Nutzen des OC-Einsatzes es wert sei, dafür seine Risiken in Kauf zu nehmen. Es geht hier also um eine bewertende Abwägung von Folgen, die sich nicht einfach direkt aus den wissenschaftlichen Fakten ergibt. Sollte es zu einer öffentlichen Debatte um den Einsatz eines OC-Systems kommen, ist deswegen zu erwarten, dass vorrangig über die Verhältnismäßigkeit diskutiert werden wird. Ebenso sind die Eigenschaften der Anwendungskontexte vorrangig für diesen Teil der Debatte relevant.

Deswegen beschränkt sich diese Zusammenfassung im Folgenden darauf, die Argumentlandkarten und die sich daraus ergebenden Fragen dieses bereits jetzt kontroversen und ausdifferenzierten Debattenbereichs vorzustellen. Um ein Verständnis der Argumentlandkarten zu ermöglichen, folgen zuvor noch einige kurze Erläuterungen.

In Argumentlandkarten wird visualisiert, wie Thesen und Argumente von Argumenten unterstützt

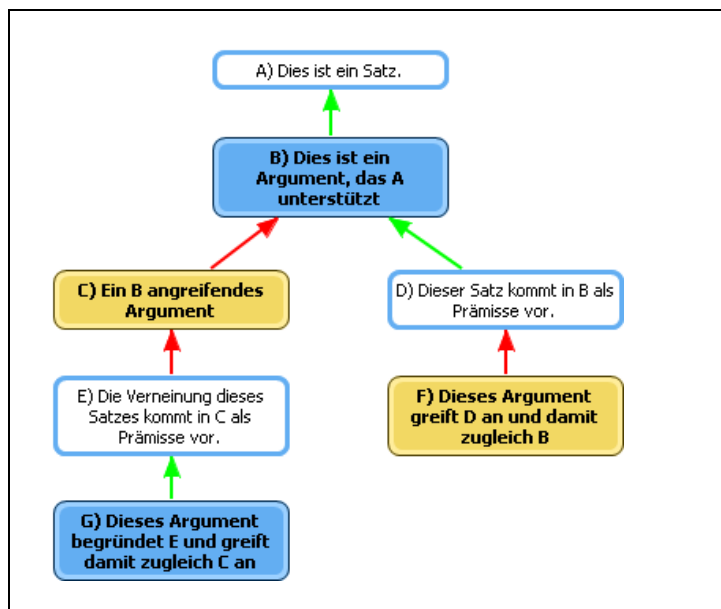


Abbildung 6.1: Argumentlandkarte: Entwicklung der Autonomie über die Zeit am Beispiel ausgewählter Architekturmuster

(grüne Pfeile) oder angegriffen (rote Pfeile) werden. Eine Debatte kann so als Netzwerk von Thesen und Argumenten dargestellt werden. Hinter jedem Argument steckt dabei jeweils eine logisch schlüssige Prämissen-Konklusion-Struktur, die nicht visualisiert wird (stattdessen wird das Argument nur mit einer Kurzbeschreibung repräsentiert, um Platz zu sparen). Nicht alle Prämissen eines Arguments sind jeweils auch als Thesen in der Argumentlandkarte eingefügt. In der Argumentlandkarte 1 werden die möglichen Beziehungen zwischen Thesen und Argumenten vorgestellt.

Aus einer derartigen logischen Analyse und Visualisierung einer Debatte ergibt sich noch lange nicht, welche Position recht hat: Denn welche Thesen und Prämissen wahr und welche falsch sind, wird nicht gesagt. Was gezeigt wird, ist nur Folgendes: Was folgt, wenn man in der Debatte bestimmte Aussagen als wahr voraussetzt und andere als falsch oder ungesichert? Welche Argumente muss man dann akzeptieren, welche nicht? In welchem Zusammenhang stehen diese Argumente zueinander? An welcher Stelle wird eine Behauptung oder Erwägung auf welche Weise argumentativ relevant? Die Argumentlandkarte hilft auf diese Weise dabei, die eigene Position in der Debatte zu verorten, sie gibt diese Position aber nicht vor, sondern bleibt neutral und offen für unterschiedliche Evaluationsperspektiven.

Eine weitere Einschränkung ist notwendig: Debatten sind selten endgültig abgeschlossen. Meist lassen sich immer weitere Argumente hinzufügen und auch diese Argumente enthalten wieder unbegründete Prämissen, die mit weiteren Argumenten angegriffen oder unterstützt werden können. Deswegen können auch Argumentlandkarten selten vollständig sein oder ein abschließendes Bild über eine Debatte verschaffen. Was sich aus einer Argumentlandkarte ablesen lässt, gilt immer nur für den derzeitigen Debattenstand. Dies ist für die hier analysierte Debatte besonders relevant, weil die Debatte um den Einsatz von OC erst am Anfang steht und in der Öffentlichkeit sogar noch gar nicht begonnen hat.

Es folgen nun die Argumentlandkarten, die die Diskussion um die Verhältnismäßigkeit des OC-Einsatzes in einem Anwendungskontext visualisieren. Aus den zentralen Thesen, die in dieser Diskussion eine Rolle spielen, ergeben sich dann die Fragen, die es zu klären gilt, um die Verhältnismäßigkeit des OC-Einsatzes in einem spezifischen Anwendungskontext beurteilen zu können. Um diesen Zusammenhang zwischen Argumentlandkarten und Fragenkatalog zu verdeutlichen, wurde jeweils die Nummer einer Frage vor den Titel der entsprechenden These geschrieben.

Aus diesen Argumentlandkarten ergeben sich die Fragen, die für den jeweiligen Anwendungskontext geklärt werden müssen, um zu entscheiden, ob ein OC-Einsatz verhältnismäßig wäre. Eine positive Antwort auf eine dieser Fragen unterstützt jeweils Argumente für die Verhältnismäßigkeit oder schwächt die Argumentation gegen die Verhältnismäßigkeit. Eine negative Antwort unterstützt jeweils die Argumente gegen die Verhältnismäßigkeit oder schwächt die Argumentation für die Verhältnismäßigkeit. Es handelt sich *nicht* in allen Fällen einfach jeweils um direkte Pro- und Contra-Gründe für oder gegen den Einsatz. Der Vorteil von Argumentlandkarten besteht gerade darin, auch komplexere argumentative Zusammenhänge darstellen zu können.

Dieser Fragenkatalog ist deswegen keine Checkliste im herkömmlichen Sinne: Eine negative Antwort bedeutet noch nicht, dass das OC-System nicht eingesetzt werden sollte. Welche Rolle eine Antwort auf eine der Fragen jeweils exakt in der Debatte spielt, ergibt sich aus den vorausgegangenen Argumentlandkarten. Der Fragenkatalog beginnt mit der Abfrage von Thesen, die direkt für die Verhältnismäßigkeitsthese relevant sind (sie ergeben sich aus den Argumenten F3.1-F3.6), und geht dann über zu Thesen, die nur indirekt für die Verhältnismäßigkeitsthese relevant sind (Argumente F3.7-F3.11):

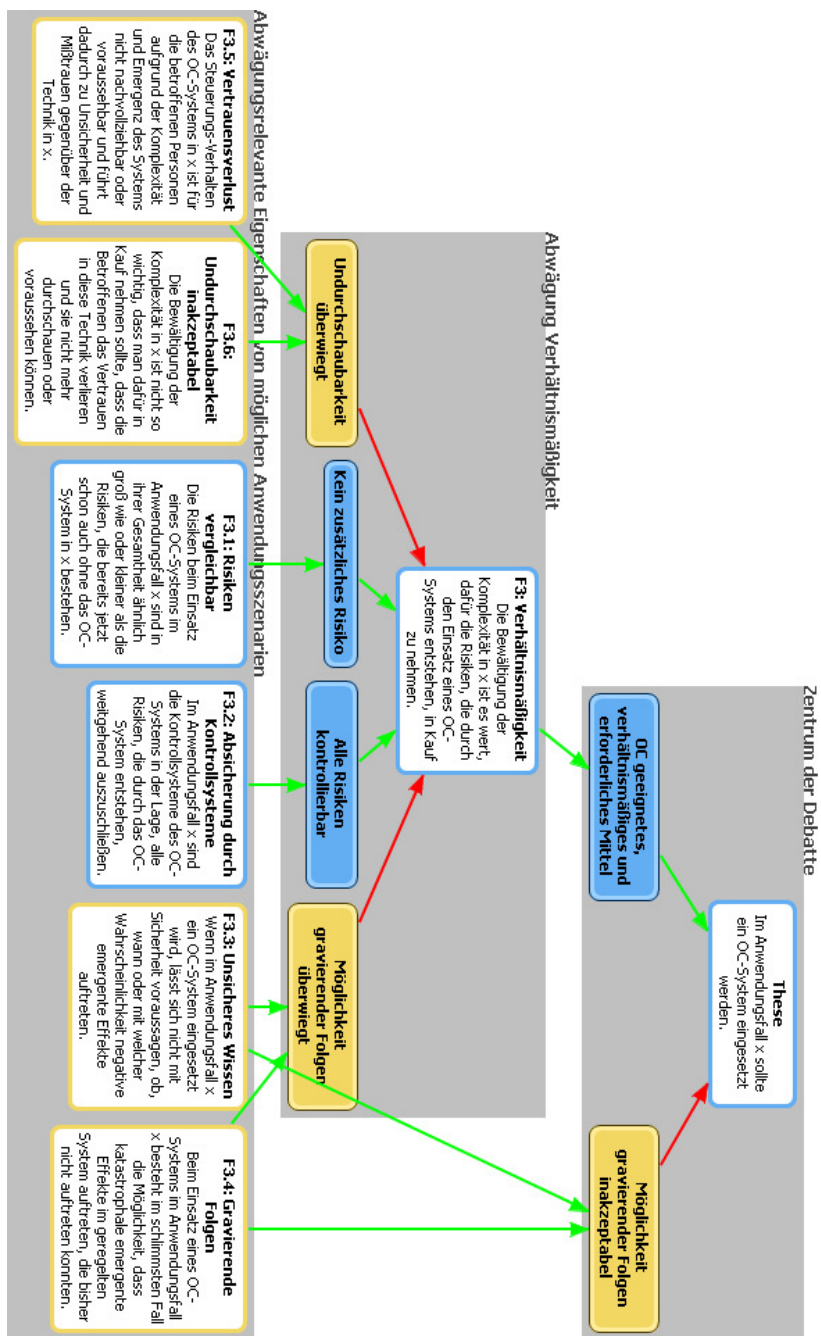


Abbildung 6.2: Argumentlandkarte: Diskussion um die Verhältnismäßigkeit, Ausschnitt 1