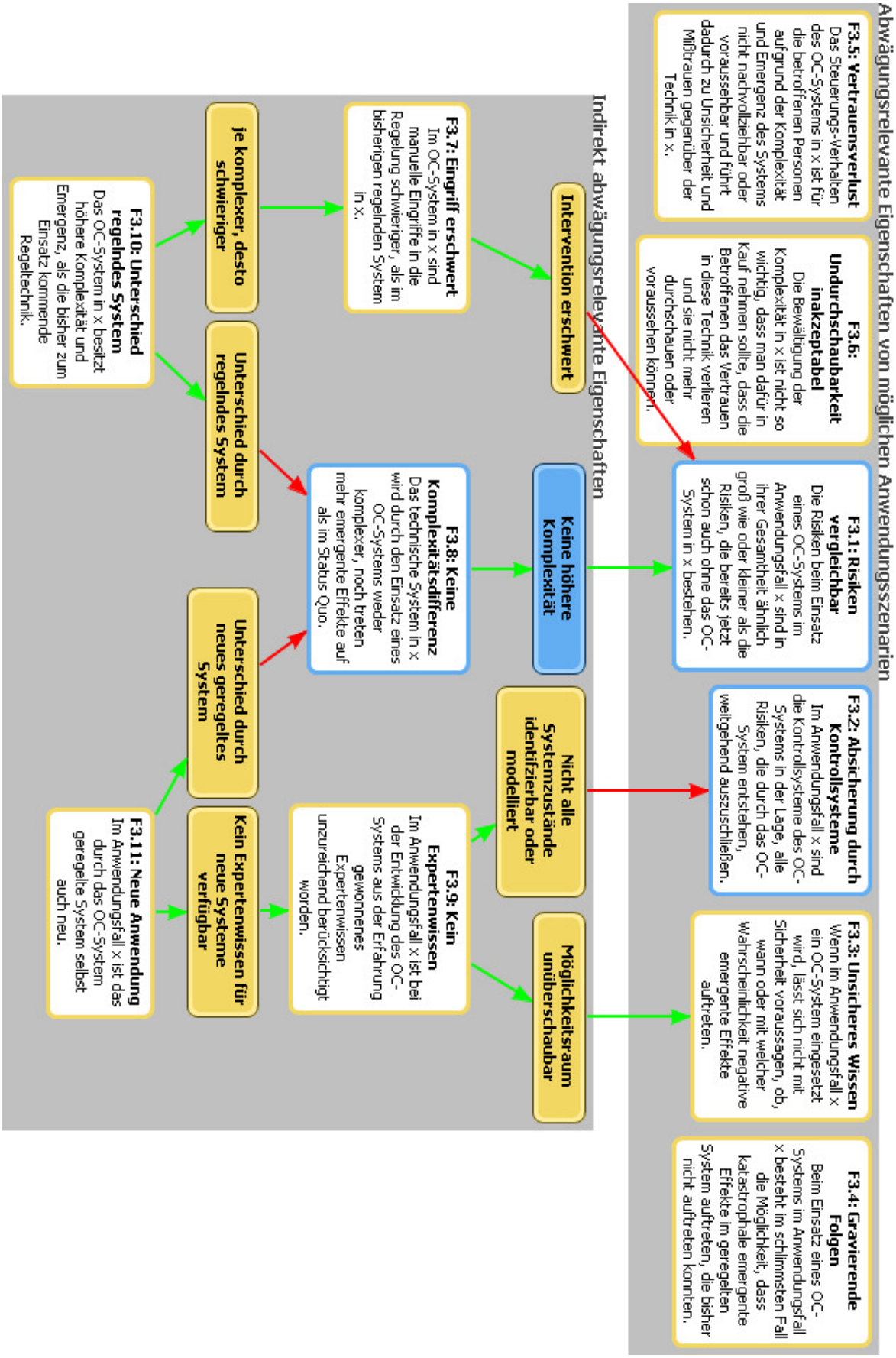

Abbildung 6.3: Argumentlandkarte: Diskussion um die Verhältnismäßigkeit, Ausschnitt 2

Tabelle 6.1: Ausschnitt aus dem Fragenkatalog: Fragen zur Verhältnismäßigkeit des OC Systems im Anwendungskontext

Ausschnitt aus dem Fragenkatalog
3 (Verhältnismäßigkeit): Ist die Komplexitätsbewältigung in x es wert, dafür die Risiken des OC-Systems in Kauf zu nehmen?
Direkt abwägungsrelevante Eigenschaften:
3.1 (Kein negativer Risikovergleich): Sind die Risiken, die durch den Einsatz des OC-Systems entstehen, mit den zuvor bestehenden Risiken vergleichbar oder sogar geringer?
3.2 (Ausreichende Kontrolle): Lassen sich die Risiken, die durch den Einsatz des OC-Systems entstehen derart durch Kontrollsysteme reduzieren, dass die Verhinderung des Restrisikos es nicht wert ist dafür die Komplexitätsbewältigung in x aufzugeben?
3.3 (Sicheres Wissen): Ist beim Einsatz eines OC-Systems die Unsicherheit darüber, ob, wann oder mit welcher Wahrscheinlichkeit negative Systemzustände im geregelten System auftreten, gering?
3.4 (Worst case nicht katastrophal): Wären die negativen Folgen auch im schlimmstmöglichen Fall nicht gravierend, inakzeptabel und katastrophal?
3.5 (Kein Vertrauensverlust): Ist das Steuerungs-Verhalten des OC-Systems in x für die Betroffenen nachvollziehbar und voraussehbar, so dass die Betroffenen dem System vertrauen?
3.6 (Undurchschaubarkeit akzeptabel): Ist es im Anwendungsfall x wichtiger die Komplexität zu bewältigen, als ein System einzusetzen, dessen Verhalten die Betroffenen durchschauen und voraussagen können?
***Indirekt abwägungsrelevante Eigenschaften*:**
3.7 (Manuelle Eingriffe nicht erschwert): Sind manuelle Eingriffe beim Einsatz eines OC-Systems genauso leicht, wie im bisherigen System?
3.8 (Kein Anstieg der Komplexität): Wird beim Einsatz eines OC-Systems ein Anwachsen der Komplexität des technischen Systems in x verhindert?
3.9 (Expertenwissen berücksichtigt): Wurde bei der Entwicklung des OC-Systems aus der Erfahrung gewonnenes Expertenwissen über den Anwendungsbereich x ausreichend berücksichtigt?
3.10 (Regelndes System nicht komplexer): Gleicht das regelnde OC-System in seiner Komplexität dem bisher zum Einsatz kommenden regelnden System?
3.11 (Keine neue Anwendung): Gab es das geregelte System auch schon vor der Einführung des OC-Systems?

7 Rechtliche Problemstellungen bei Organic Computing

Für die Erfolgschancen der Einführung und Marktdurchdringung von OC spielen deren rechtliche Rahmenbedingungen, insbesondere die Regelung der Haftung, in Bezug auf die mit selbstorganisierenden (adaptiven) IT-Systemen zwangsläufig verbundenen Risiken eine entscheidende Rolle. Dabei ist zwischen (1) den (in Deutschland) bestehenden, diesbezüglich relevanten rechtlichen Regelungen, (2) deren erkennbaren Regelungslücken und (3) der für eine sozial- und umweltverträgliche Realisierung und Praxis von OC wünschenswerte Gestaltung seiner rechtlichen Rahmenbedingungen zu unterscheiden. Dieses Kapitel fasst die hierfür eingeholte Rechtsexpertise zu selbstorganisierenden adaptiven IT-Systemen (Erben et al. 2009) zusammen..

Zunächst kommen im Hinblick auf SaSo-Systeme generelle und keine spezialgesetzlichen Regulierungen des sicheren Einsatzes von smarten Technologien zum Tragen. So gab es bis 2004 kein einziges Urteil zum Bereich Produkthaftung oder Delikthaftung für Computersysteme allgemein und existieren bis heute nur Ansätze in Urteilen zur Produkthaftung, aus denen man schließen kann, dass diese auch für Software, insbesondere Embedded Software, anwendbar sind (vgl. Erben et al. 2009:33), sodass die Sicherheits- und Haftungsfragen von (Informations-)Technologien betreffende Rechtsprechung strittige Rechtsfragen bislang kaum genauer abgeklärt und entschieden hat. Hier setzen sich Erben et al. (2009) mit den entsprechenden (haftungsrechtlichen) Begriffen, Konstruktionen und Abwägungen auseinander und halten zusammenfassend fest, dass für ein konkretes OC-System jeweils das Ausmaß potenziell möglicher Schäden und das konkrete Risiko des Schadenseintritts im Einzelfall gegen die mit dem Produkt verbundenen Chancen und Vorteile (nur Komfortsteigerung oder z.B. Verhinderung von Unfällen) abzuwägen ist, ohne dass dieser (rechtswirksame) Abwägungsprozess entlang eines einheitlichen Entscheidungsbaums schematisch vorgenommen werden kann. „Ein auf OC-Techniken basierendes Produkt, das nur relativ geringe Körperschaden herbeiführen kann und bei dem dieses Risiko gering ist, und das gleichzeitig geeignet ist, in einer Vielzahl von Fällen vor schweren Körperschäden zu bewahren, kann aus produkthaftungsrechtlicher Sicht dann zulässig sein, wenn die entsprechenden Warnhinweise gegeben werden, wenn alle zumutbaren Sicherheitsvorkehrungen getroffen wurden und wenn bzgl. Herstellung und fertigem Produkt alle in dieser Expertise dargestellten Voraussetzungen eingehalten wurden. Ein Produkt, das nur Sachschäden herbeiführen kann, kann zulässig sein, wenn dieses Risiko so gering ist, wie es die berechtigten Erwartungen an das Produkt vorgeben und wenn die ggf. erforderlichen Hinweis- und Warnpflichten erfüllt werden.“ (Erben et al. 2009:66f)

Allgemeine haftungsrechtliche Regelungen

Als Produkthaftung (vgl. ProdHG) und Produzentenhaftung (vgl. § 823 BGB) bestimmende (rechtliche) Voraussetzungen werden angeführt:[138]

[138] Ergänzend ist noch die vertragsrechtliche Haftung zu nennen, die anders als die Produkt- und die Produzentenhaftung an das sogenannte Äquivalenzinteresse anknüpft, wonach wirtschaftliche Einbußen der Vertragspartner auszugleichen sind, die diese aufgrund schädigender Ereignisse aus dem Verantwortungsbereich des anderen Vertragspartners erleiden und die mit enormen Kosten z.B. eines Softwarehauses wie etwa für eine weltweite Rückrufaktion oder für die Versicherungsprämie für potenzielle Schäden in dreifacher Millionen-Euro-Höhe verbunden sein können.

1) Für die Produkthaftung ist das Vorliegen eines Fehlers im Sinne von § 3 Abs.1 ProdHG maßgeblich, wonach ein Produkt fehlerhaft ist, wenn es „[…] nicht die Sicherheit bietet, die unter Berücksichtigung aller Umstände, insbesondere a) seiner Darbietung, b) des Gebrauchs, mit dem billigerweise gerechnet werden kann, sowie c) des Zeitpunkts, in dem es in den Verkehr gebracht wurde, berechtigterweise erwartet werden kann.“ Damit betrifft die gesetzliche Produkthaftung – ebenso wie die öffentlich-rechtlichen Produktsicherheitsvorschriften wie z.B. das GPSG – die *Sicherheit* des Produkts, wie sie die Allgemeinheit erwarten darf,[139] und schützt dadurch das Integritätsinteresse jedes Benutzers und Dritten daran, dass die Sache die berechtigterweise erwartbare Sicherheit für Leben, Gesundheit und Sachwerte bietet.[140]

2) Jedoch muss die Sicherheitserwartung berechtigt sein, insofern die Allgemeinheit nicht von jedem Produkt in jeder Situation völlige Risikolosigkeit erwarten kann. Auch müssen konstruktive Maßnahmen zur Beseitigung von Produktgefahren dann nicht getroffen werden, wenn die Benutzer dies im Bewusstsein der bestehenden konkreten Gefahr nicht für erforderlich halten. Von daher muss letztlich die Rechtsprechung anhand der Kriterien von § 3 Abs. 1 ProdHG die entsprechende Wertungsfrage entscheiden[141], wozu alle Umstände wie einerseits der *Gebrauch* und die *Darbietung* eines Produkts und andererseits die *gesamten objektiven Umstände des konkreten Schadensfalles* zu berücksichtigen sind.

3) Insofern bei OC-Systemen nicht sicher ausgeschlossen werden kann, dass sie sich auch in einer schadenstiftenden Weise (weiter)entwickeln können, müssen deshalb in jedem Fall bezüglich der dann drohenden Gesundheitsgefahren entsprechende Warnungen ausgesprochen werden und die Herstellung als auch die Instruktion müssen auch auf den über die Zweckbestimmung hinausgehenden üblichen Gebrauch und nicht ganz fernliegende versehentliche Fehlanwendungen abstellen.[142]

4) Gerade weil sich argumentieren lässt, dass genau der bestimmungsgemäße Gebrauch von OC-Systemen einschließt, auch unvorhergesehene Anwendungen (im Sinne nicht programmierbaren Anpassungsverhaltens) vorzunehmen, müssen zur Erfüllung der Anforderungen des Gesetzes in jedem Fall „die potenziell gefährlichen Anwendungen von Vornherein aussortiert werden, d.h. sie dürfen in den Lernprozess im Sinne einer *conditio sine qua non* gar nicht erst

---

Allerdings betrifft die vertragsrechtliche Haftung nicht primär Fragen der Sicherheit der Allgemeinheit (vgl. Erben et al. 2009:40).

139 Demgegenüber betrifft die vertragliche Mängelhaftung die vom Erwerber erwartbare Gebrauchsfähigkeit, Funktionsfähigkeit und den Wert einer Sache.

140 Nach dem ausdrücklichen Wortlaut des Gesetzes ist auf die objektive (!) Erwartung abzustellen, „ob das Produkt diejenige Sicherheit bietet, die die Allgemeinheit nach der Verkehrsauffassung in dem entsprechenden Bereich für erforderlich hält… Ist ein Produkt für den Endverbraucher bestimmt, muss es z.B. erhöhten Sicherheitsanforderungen genügen, die auf das Wissen und Gefahrsteuerungspotential des durchschnittlichen Konsumenten Rücksicht nehmen.“ (Erben et al. 2009:13)

141 In Bezug auf die Produkthaftung sind dabei etwa die jüngsten Urteile des BGH vom 17.3.2009 (Az. VI ZR 176/08) zur Produktsicherheit eines Gebäckstücks mit einer Kirschfüllung (Kirschtaler) und 16.6.2009 (Az. VI ZR 107/08) zur Haftung eines Fahrzeugherstellers für die Fehlauslösung von Airbags anzuführen, nach denen die Produkthaftung für das Auftreten eines Kirschkerns in Gebäckstücken nicht unterstellt werden kann, sie jedoch für die Fehlauslösung von Airbags durch ein Schlagloch anzunehmen ist.

142 „Gerade bei lernenden Systemen, deren Zweckbestimmung ja gerade darin besteht, Entscheidungen in Abhängigkeit von sich ändernden Situationen treffen zu können bzw. sogar zu sollen, ist die Wahrscheinlichkeit einer nicht ganz fernliegenden und versehentlichen Fehlanwendung sehr hoch. Dazu kommt ggf. als zusätzliches Problem, dass ein Nutzer aufgrund der Funktionalität von OC Systemen, die sich ja gerade an unvorhergesehene Situationen anpassen sollen, evtl. durch diese Eigenschaft gerade dazu verleitet werden kann, OC Systeme außerhalb ihres vorgesehenen Einwendungsgebiets einzusetzen. Daher sind hier jedenfalls in beide genannten Richtungen Warnhinweise erforderlich.“ (Erben et al. 2009:17f)

aufgenommen werden, sondern gewissermaßen *a priori* verboten sein. Denn wenn (auch nur) die (relativ konkrete) Gefahr besteht, dass das System selbstständig potenziell gefährliche Situationen nicht meistern kann, bietet dieses konkrete lernende System nicht die nach dem ProdHG erforderliche Sicherheit." (Erben et al. 2009:18)

5) Die gesamten objektiven Umstände eines konkreten Schadensfalles betreffen die *Natur der Sache*, die *Preisgestaltung*[143], den *Stand von Wissenschaft und Technik*, *technische Normen und gesetzliche Sicherheitsbestimmungen*.

- Da für OC-Systeme aufgrund ihrer gewollten Emergenz-Eigenschaften im Unterschied zu rein adaptiven IT-Systemen nicht vorhergesagt werden kann, welche Handlung in einer bestimmten Situation vorgenommen wird, kann man nach Eintritt des Schadensfalles im Nachhinein die Einwilligung des Nutzers nicht ohne weiteres unterstellen. Für Anwendungen in sicherheitskritischen Bereichen wird zudem häufig gerade für Software in sicherheitsempfindlichen Bereichen schon kraft Natur der Sache eine nach dem Stand der Technik 100%-ige Sicherheit verlangt. „Ist das, aus welchen Gründen auch immer, nicht gewährleistet, muss man sich fragen, welche Konsequenz daraus zu ziehen ist. Möglicherweise darf das konkrete Produkt dann gar nicht in den Verkehr gebracht werden. Diese Frage ist unter Abwägung von Art und Umfang der Risiken, ihrer Eintrittswahrscheinlichkeit und des mit dem Produkt verbundenen Nutzens zu prüfen." (Erben et al. 2009:20)
- „Sind bestimmte mit der Produktnutzung einhergehende Risiken nach dem maßgeblichen Stand von Wissenschaft und Technik nicht zu vermeiden, ist unter Abwägung von Art und Umfang der Risiken, der Wahrscheinlichkeit ihrer Verwirklichung und des mit dem Produkt verbundenen Nutzens zu prüfen, ob das gefahrträchtige Produkt überhaupt in den Verkehr gebracht werden darf.[144] Klar ist damit bzgl. auf OC-Techniken basierender Produkte, dass diese jedenfalls nur dann überhaupt in Verkehr gebracht werden dürfen, wenn und soweit alle erforderlichen Warn- und Hinweispflichten eingehalten werden. Nach dem derzeitigen Stand der Wissenschaft und Technik ist das Risiko, dass sich OC-Produkte (u.U. auch) in einer Weise entwickeln, die zu einem Schaden führt, wohl nicht zu vermeiden. Hier ist deshalb zum einen zu prüfen, wie hoch das Risiko des Schadenseintritts im konkreten Fall angesichts der Anwendung ist, sowie welche Art von Schäden und in welchem Maße diese zu erwarten sind (nur Sachschaden, leichter Personenschaden, schwerer Personenschaden, etc.). Die so erkannten Risiken sind sodann mit dem mit dem konkreten Produkt konkret verbundenen Nutzen (nur Komfortsteigerung oder z. B. Verhinderung von Unfällen) abzuwägen." (Erben et al. 2009:22)
- Bei Einhaltung der anwendbaren technischen Normen und gesetzlichen Sicherheitsbestimmungen (wie DIN-Vorschriften, VDE-Bestimmungen, das Gesetz über die elektromagnetische Verträglichkeit von Geräten von 2002, das Geräte- und Produktsicherheitsgesetz (GPSG) von 2004, das Lebensmittel- und Futtermittel-Gesetzbuch (LFGB) von 2005) ist zu vermuten, „dass das Produkt (die Instruktion) den anerkannten Regeln der Technik und damit den Sicherheitserwartungen entspricht. Kommt es zu einem Schaden, muss dann der Geschädigte darlegen und begründen, warum dennoch ein Fehler (Konstruktionsmangel) vorliegen soll. Die Einhaltung genügt aber dann nicht, wenn die technische Entwick-

143 „Die Preisgestaltung kann nach gesicherter Rechtsprechung auf die Verkehrserwartung Einfluss haben, denn erhöhte Sicherheit hat ihren Preis." (Erben et al. 2009:20)

144 BGH Az. VI ZR 107/08, Rdnr. 17 „Airbag"

lung bzw. die wissenschaftlichen Erkenntnisse über die Normen hinaus gegangen sind und/oder wenn sich bei der Benutzung des Produkts Gefahren gezeigt haben, die in ihnen noch nicht berücksichtigt sind (wobei hierfür der Geschädigte die Beweislast trägt). Denn in diesem Fall sind die bestehenden Normen ergänzungsbedürftig, und zwar nach dem objektiv erkennbaren oder ermittelbaren Stand von Wissenschaft und Technik." (Erben et al. 2009:23f) Allerdings darf ein entsprechendes Monitoring des Herstellers erwartet werden, das gegebenenfalls (durch ihm bekannt werdende Mängel) zu Rückrufaktionen und/oder Verbesserungen in der zukünftigen Herstellung führen kann.

- Bei Fehlern wird unterschieden zwischen Konstruktions-, Fabrikations- und Instruktionsfehlern, wobei sich der Hersteller eines Produkts bei Konstruktion, Produktion (Fabrikation) und Instruktion nach dem erkennbaren und ermittelbaren Stand von Wissenschaft und Technik richten muss. Fehler in adaptiven Systemen sind als Software-Programmierfehler wohl per definitionem Konstruktionsfehler. Haftung für Fabrikationsfehler ergibt sich aus der Gefährdungshaftung nach dem ProdHG und mangels Verschuldens nicht aus dem allgemeinen Haftungsrecht des BGB. Bei Instruktionsfehlern muss die Verletzung der Hinweispflicht in jedem Fall ursächlich für den eingetretenen Schaden sein.[145]

6) Ein wesentlicher Unterschied der Produzentenhaftung gegenüber der Produkthaftung besteht darin, dass der Hersteller im Rahmen der Produzentenhaftung nur bei Verschulden haftet, wobei er gegebenenfalls den Gegenbeweis führen kann und muss, um bei Vorliegen eines Fehlers seine Haftung vermeiden zu können. Des Weiteren besteht die Pflicht, Produkte nach Inverkehrbringen auf noch unbekannt gebliebene schädliche Eigenschaften hin zu beobachten und sich über sonstige eine Gefahrenlage schaffende Verwendungsfolgen zu informieren, was bei nachträglicher Erkennbarkeit von Gefahren eine Abwendungspflicht einschließen kann.

7) Auch wenn das Rechtsgut der Sicherheit der Allgemeinheit aufgrund des mit dem ProdHG verfolgten Schutzzwecks letztlich immer schwerer wiegt als die anderen Interessen, insbesondere wirtschaftliche Interessen Einzelner, aber auch potenzielle politische bzw. gesamtwirtschaftliche Interessen der Allgemeinheit, kann ein Produkt gerade aufgrund seiner Eigenschaften auch der Sicherheit der Allgemeinheit dienen. Von „daher ist im Hinblick auf die Zulässigkeit von OC-basierter Softwaresysteme abzuwägen, ob ein Produkt, auch wenn es ein bestimmtes Gefahrenpotenzial aufweist, ggf. (trotzdem) dann in den Verkehr gebracht werden darf, wenn nach dem Stand der Technik Fehler nicht auszuschließen sind." (Erben et al. 2009:42f)

Angemessenheit und Spezifizierungen des bestehenden Rechtsrahmens

Während die bisherigen Ausführungen zur Produkt- und Produzentenhaftung genereller Natur waren, die fallweise für OC-Systeme exemplifiziert wurden und deutlich machen, welche Rechtsvorschriften für OC besondere Beachtung finden (müssen) bzw. wie OC-Systeme gesetzeskonform auszugestalten sind, und während spezialgesetzliche Regelungen bislang keine bedeutsame Rolle spielen, sind darüber hinaus insbesondere auch folgende Fragestellungen relevant:

145 „Auf OC Systeme übertragen (z. B., wenn die temperaturabhängige Steuerung der Heizspirale durch ein OC System erfolgt) könnte dies z. B. bedeuten, dass trotz einer ggf. selbstheilenden Funktion dieses Systems darauf hingewiesen werden muss, dass das System nicht in jedem Fall in der Lage ist, sich selbst zu heilen und daher entsprechende zusätzliche Sicherheitsmaßnahmen zu ergreifen sind (z. B. Einbau einer konventionellen Abschaltautomatik bei Überhitzung)." (Erben et al. 2009:32)

- „Wer ist für das Handeln und für mögliche Fehler eines selbstorganisierenden Systems verantwortlich?
- Stößt das sog. Verursacherprinzip an seine Grenzen, wenn (= weil) das Verhalten organischer Computer auch von seinen Entwicklern systemimmanent *per definitionem* sowie aufgrund der Komplexität nicht vorhergesagt werden kann?
- Wenn die Antwort auf die vorhergehenden Fragen ja ist: Braucht es dann nicht zwingend neuer gesetzlicher Regelungen für Organic Computing und wie sind diese ggf. auszugestalten?“ (Erben et al. 2009:6)

Infolge der generellen Unvermeidbarkeit von Fehlern in der Software(-Entwicklung) ist bislang die Frage umstritten, ob und wann Software überhaupt ein Produkt im Rechtssinne (des ProdHG) ist bzw. als solches eingestuft werden kann, wobei die überwiegende Ansicht in der Literatur dies für Software bejaht, die auf einem Datenträger vertrieben wird. Zudem müsse man die Sacheigenschaften von Software bei Embedded Software wegen ihrer engen Verknüpfung mit der Hardware bejahen, sodass Software-Fehler als Fehler eines Gesamtprodukts einzustufen seien. Dafür spricht auch das benannte BGH-Urteil zur Fehlauslösung von Airbags vom 16.6.2009 (vgl. Erben et al. 2009:37).[146]

Während Organic Computing zum einen stets auch wie konventionelle Software zu beurteilen ist, stellt sich zum anderen vorrangig die Frage der Zurechenbarkeit des (emergenten) Verhaltens von OC-Systemen. Die diesbezügliche Diskussion gelangte mehr oder minder zu dem Ergebnis, dass selbstorganisierende Computer- oder Peer-to-Peer-Systeme kein genuines Rechtssubjekt darstellen (können) und ihnen deshalb keine eigene (rechtliche) Verantwortung für Handlungen zugeschrieben werden kann (vgl. Lenk 2003).[147] Gerade weil SaSo-Systeme mit emergenten Eigenschaften nach dem Inverkehrbringen keiner (direkten) Kontrolle mehr unterliegen, müssen die produkthaftungsrechtlichen Grundsätze auf den Hersteller angewendet werden; denn er ist das Rechtssubjekt, das jedenfalls kontrolliert, ob das Produkt überhaupt in den Verkehr gebracht werden darf.[148] Dabei können für Produkthaftungsfragen weder Parallelen zum Umweltrecht in Bezug auf die Haftungsfreistellung von (keinem individualisierbaren Schädiger zuordenbaren) Summationsschäden noch solche zum Inverkehrbringen von Arzneimitteln herangezogen werden. Zum ei-

---

146 „Im Ergebnis ist damit auch und gerade im Hinblick auf die mittlerweile nahezu Omnipräsenz von Software in unseren Lebensbereichen nicht einzusehen, warum bzgl. Softwareleistungen ein geringerer Maßstab an die Anforderungen des Verschuldens im Rechtssinne gelegt werden soll als bei anderen Leistungen. Aufgrund wohl ähnlicher Erwägungen hat auch die Rechtsprechung den lange Zeit als zulässig erachteten Ausschluss der Haftung für leichte Fahrlässigkeit in AGB im Zeitablauf nicht mehr als zulässig angesehen, und zwar insb. dann auch nicht (mehr) für den Bereich Software(-Leistungen).“ (Erben et al. 2009:42)

147 „Für Organic Computing Techniken und damit adaptive und auch lernende IT-Systeme bedeutet das, dass eine Haftung des Systems selbst für die von ihr vorprogrammierten Entscheidungen ausscheidet, und zwar mangels Verantwortlichkeit der Maschine und damit im Ergebnis mangels Möglichkeit eines Verschuldensvorwurfs. Auch eine Gefährdungshaftung nach dem ProdHG, die kein Verschulden voraussetzt, scheidet aus den dargestellten Gründen aus.“ (Erben et al. 2009:52)

148 „Das gilt dann auch bzgl. Organic Computing: Auch wenn die möglichen Anwendungsgebiete des Organic Computing nahezu unbegrenzt sind, da Computersysteme, die sich selbst-optimieren können, potenziell überall eingesetzt werden können und ihr potenzieller Nutzen damit enorm sein kann, so muss doch gleichzeitig ganz klar sein, dass auch solche Systeme nur im Rahmen der bestehenden Gesetze und der von diesen vorgesehenen Rechtsfolgen eingeführt werden dürfen. Diese sehen vor, dass bei potenziellen Gesundheitsschäden bei Fehlern die Anforderungen an die Sicherheit des Produkts deutlich höher sind als wenn lediglich Sachschäden drohen, weil hier die berechtigten Erwartungen der Allgemeinheit höher liegen. Soweit technische Normen unterschiedliche Anwendungen je nach Risikoklasse stellen, sind diese Anforderungen als Mindeststand der Technik einzuhalten.“ (Erben et al. 2009:48f)

nen lassen sich OC-bedingte Schäden eindeutig dem Hersteller zuordnen, da er über das Inverkehrbringen entschieden hat. Zum anderen besteht zwar keine Produkthaftung, wenn der den Schaden verursachende Fehler des Produkts zum Zeitpunkt des Inverkehrbringens nach dem Stand von Wissenschaft und Technik nicht erkennbar war. „Ein solcher Entwicklungsfehler, der zu einem Haftungsausschluss führen würde, setzt aber voraus, dass die potenzielle Gefährlichkeit des Produkts im Zeitpunkt des Inverkehrbringens nach dem Stand der Wissenschaft und Technik nicht erkannt werden konnte. Allerdings ist unter potenzieller Gefährlichkeit des Produkts nicht der konkrete Fehler des schadensstiftenden Produkts, sondern das zugrundeliegende allgemeine, mit der gewählten Produktion verbundene Fehlerrisiko zu verstehen.

Man kann daher wohl nicht argumentieren, aufgrund der Fehleranfälligkeit von Software allgemein, aufgrund der unvollständigen Abbildung der Wirklichkeit bei Expertensystemen oder bei Organic Computing Systemen, bei der sich die Software ja gerade unabhängig von Vorgaben selbständig entwickeln soll, sei die potenzielle Gefährlichkeit in sicherheitskritischen Bereichen aus der Natur der Sache heraus nicht vorhersehbar. Es ist richtig, dass bei einem überragenden Nutzen des Systems – wie bei Arzneimitteln – dennoch ein überwiegendes Interesse daran bestehen kann, das System in Verkehr zu bringen, ohne das der Hersteller dafür haftet. Dieses Problem kann aber nicht dadurch gelöst werden, dass der Hersteller aufgrund der Unvorhersehbarkeit von Fehlern gar nicht haftet. Denn das könnte (auch) dazu führen, dass Systeme mit wenig Nutzen, aber hohem Risiko bei im Übrigen ordnungsgemäßer Entwicklung ohne Haftungsrisiken in den Verkehr gebracht werden könnten. Das darf nicht sein. Die Problematik muss deshalb vielmehr wohl bei der Frage angesiedelt und auch gelöst werden, ob bzw. unter welchen Voraussetzungen das konkrete Produkt unter Abwägung von Nutzen und Risiken überhaupt in den Verkehr gebracht werden durfte. Dabei wird man der Frage, ob Sicherungsmaßnahmen nach dem Stand der Wissenschaft und Technik evtl. nicht zumutbar sind, einen besonderen Stellenwert einräumen müssen.“ (Erben et al. 2009:36f) Im Ergebnis müssen die potenziellen kreativen Verhaltensmöglichkeiten von OC-Systemen zielgerichtet in sichere Bahnen gelenkt und der Korridor für Selbst-X-Eigenschaften möglichst eng gehalten werden, weil andernfalls der verantwortliche Hersteller haftet. „Denn gerade weil das System potenziell so gefährlich ist, müssen erhöhte Sicherheitsanforderungen gelten, und zwar in jeder Phase, also in der Entwurfs- bzw. Konzeptionsphase, Testphase, sowie bei und erst recht auch nach der potenziellen Markteinführung. Ferner müssen auch aus dem gleichen Grunde auch gegenüber den allgemeinen Anforderungen stark erhöhte Beobachtungs-, Sorgfalts- und Rückruf(plan)pflichten gelten, wenn (= weil) das System sich zur Laufzeit selbst – wenn auch gesteuert – fort schreibt… Deshalb ist die Produktbeobachtungspflicht auch vor dem Hintergrund der potenziellen strafrechtlichen Verantwortlichkeit von enorm wichtiger Bedeutung für den Hersteller.“ (Erben et al. 2009:50f)

OC-Techniken müssen somit gerade auch im Hinblick auf ihre (potenzielle) gesellschaftliche Akzeptanz sicherstellen, dass sie bestimmte Mindestanforderungen mit an Sicherheit grenzender Wahrscheinlichkeit erfüllen.

Angesichts der aufgeführten (haftungs)rechtlichen Anforderungen bedarf es im Prinzip keiner Anpassung des Rechtsrahmens für OC-Systeme, was insbesondere eine mögliche *Haftungsverschärfung* oder umgekehrt eine *Haftungseinschränkung* gegenüber den Haftungskriterien des ProdHG und geltenden technischen Normen betrifft. Eine Haftungsverschärfung ist nicht erforderlich, „weil die Verantwortung für Schäden aus OC Systemen nach der geltenden Gesetzeslage – im Rahmen der üblichen Auslegungsfragen, die abstrakte Normen mit sich bringen – relativ klar zugewiesen ist.“ (Erben et al. 2009:53f) Umgekehrt sind ein Haftungsausschluss bzw. eine Haftungseinschränkung für aus OC resultierenden Risiken „wohl weder (politisch) durchsetzbar, noch von der Sache her gewünscht und evtl. sogar verfassungsrechtlich nicht möglich bzw. jedenfalls bedenklich. Das

ProdHG ist – im Gegenteil – sogar zwingend notwendig und eine der zentralen Rechtsnormen in Deutschland und der EU. Als solche sollten sie im Hinblick auf die potenzielle Einführung von OC-Techniken keinesfalls geändert werden. Eher muss wohl in Konsequenz auf die Einführung von OC-Techniken verzichtetet werden, jedenfalls solange und soweit nicht sichergestellt ist, dass diese den Maßstäben des ProdHG sowie den übrigen anwendbaren sicherheitsrelevanten Gesetze und Normen entsprechen." (Erben et al. 2009:54)

Von daher geht es viel eher um Maßnahmen, die gewährleisten, dass OC-Systeme den geltenden rechtlichen Anforderungen entsprechen (können). Hierzu können etwa entsprechende von der Industrie und/oder der Wissenschaft selbst entwickelte Standards gehören, die sicherstellen, dass OC-Systeme auch bei emergentem Verhalten den bestehenden rechtlichen Anforderungen genügen. Wenn für ein konventionelles System eine bestimmte Reaktionsgeschwindigkeit Mindeststand der Technik ist, würden etwaige Lockerungen solcher technischer Standards, z.B. die Zulassung einer geringeren Reaktionsgeschwindigkeit bei sicherheitsrelevantem Verhalten wie der Auslösung eines Bremsvorgangs, rechtlich zu keiner Haftungseinschränkung führen, insofern technische Standards eben nur Mindestanforderungen definieren. Dies gilt nicht unbedingt für Normen, die den Herstellungsprozess an sich regeln, da nur das (fertige) Produkt die gemäß dem durch technische Normen festgelegten Mindeststand der Technik zu erwartende Sicherheit bieten muss, während die Art und Weise, wie diese erreicht wird, auch im Sinne des technischen Fortschritts dem Hersteller überlassen bleiben muss.[149]

Was z.B. die von der International Electrotechnical Commission (IEC) herausgegebene (internationale) Norm IEC/EN-61508 zur Schaffung von elektrischen, elektronischen und programmierbar elektronischen (E/E/PE) Systemen angeht, die eine Sicherheitsfunktion ausführen, bei der Teil 3 die Anforderungen an die Software für die funktionale Sicherheit solcher Systeme festlegt (vgl. Kemman 2005), so werden die Anforderungen aus Ziffer 7.8.2.2 der IEC-61508-3 für auf OC-Techniken basierende Software wohl regelmäßig „nicht erfüllt sein und auch kaum erfüllt werden (können), da hiernach eine Modifikation der Software erst nach detaillierter Analyse der möglichen Gefahren der Änderungen stattfinden darf. Soweit auf OC basierende Software sich zur Laufzeit deshalb selbst modifiziert und neu konfiguriert, verstößt das wohl gegen das in IEC 615068 vorgesehene Verfahren für Modifikationen. Soweit es deshalb nicht möglich sein sollte, die Anforderungen der IEC-61508-3 innerhalb des Systems anderweitig zu erfüllen, etwa indem alle potenziellen Änderungsfolgen vorab entsprechend analysiert werden, könnte eine mögliche Lösung dieser Problematik evtl. darin bestehen, die Zielsetzung der IEC-61508-3 auf andere Weise zu erreichen, z. B. dadurch dass sichergestellt wird, dass keine der möglichen Änderungen zu Gefahren führt. Dazu ist als Minimum zwingend erforderlich, dass Änderungen nur in einem vom Hersteller definierten eng begrenzten Korridor systemimmanent zulässig und damit auch tatsächlich (nur) möglich sind." (Erben et al. 2009:56)

Falls bislang keine allgemeingültigen selbstgesetzten industriellen und/oder wissenschaftlichen Standards bestehen, die entsprechend angepasst werden könnten, sind für OC-Systeme neuartige Standards in Erwägung zu ziehen. Diese hätten (rechtlich) den Vorteil eines Mindeststandards, bei

149 „Allerdings muss der Hersteller bei Eintritt eines Schadens beweisen, dass sein ggf. vom technischen Standard abweichender Herstellungsprozess für das Produkt mindestens die gleiche Sicherheit gewährleistet (hat) wie der normgerechte Herstellungsprozess, während derjenige, der entsprechend der Norm entwickelt, sich zunächst auf die Vermutung berufen kann, dass das Produkt fehlerfrei ist, d.h. der Geschädigte muss darlegen und begründen, warum dennoch ein Fehler (Konstruktionsmangel) vorliegen soll." (Erben et al. 2009:55f)

dessen Einhaltung sich ein Hersteller zunächst auf die Vermutung berufen könnte, dass das Produkt fehlerfrei ist.[150]

Schließlich können Lernprozesse von OC-Systemen durch Selbstheilung von Fehlern gegebenenfalls das faktische Haftungsrisiko verringern. Allerdings ist das Gefahrenpotenzial bei eigenständig lernfähigen Systemen nur schwer vorhersehbar. Deshalb dürfen sie nicht eigenständig Bedingungen ändern können, die mit Personenschäden verbunden sein können.[151] Darüber hinaus muss ein permanentes Rückkopplungssystem zuverlässig sicherstellen können, dass das System weder im Leerlauf verharrt oder gar keine Signale mehr senden oder empfangen kann noch dass es, „bevor es auch nur potenziell den Korridor des Spezifizierten (Zuverlässigen) verlässt, etwa um auf Unvorhergesehenes zu reagieren, erst einmal in einen abgesicherten Modus übergeht, in dem es erst durch Eingriff von außen durch einen eigenverantwortlich handelnden Menschen … Aktionen ausführt, oder, in zeitkritischen Fällen, nur solche Lösungen selbstständig aktiviert, die im Korridor des Spezifizierten liegen.“[152] (Erben et al. 2009:57)

Rechtsvermittelte Vertrauenserzeugung

Über Maßnahmen hinaus, die die Einhaltung rechtlicher Vorgaben in OC-Systemen gewährleisten (sollen), geht es für deren Markteinführung und Akzeptanz (im Sinne einer sozial- und umweltverträglichen Realisierung und Praxis von OC) um Vertrauen(sbildung) in und Wissen(svermittlung) über Organic Computing, dessen Sicherheit und Kontrollierbarkeit, Nutzungs- und Schadenspotenziale, sowie die Rechtslage mit Verantwortlichkeiten und Haftungsfolgen.[153] Hierzu können auch rechtsvermittelte Vorkehrungen beitragen. Dazu zählen neben Standardisierungs- und Zertifizierungsmaßnahmen eine definierte Mensch-Maschine-Schnittstelle, die die Einwirkung auf OC-Systeme zulässt, nachvollziehbare OC-Techniken und -Methoden, die zum Vertrauen in die Verlässlichkeit von OC beitragen[154] und den Schutz der Privatsphäre gewährleisten[155], und soweit machbar die Reduktion der Komplexität der (OC-)Systeme.

---

150 „Voraussetzung dafür ist aber immer, dass die (neuen) Standards diese Anforderungen soweit möglich berücksichtigen, z. B. indem in ihnen auch festgelegt wird, dass aufgrund der begrenzten Testbarkeit der Einsatz der Systeme durch ein herkömmliches System ersetzt wird, sobald sich sicherheitskritische Situationen ergeben bzw. dass ggf. festgelegt wird, in welchen Situationen OC Systeme wegen nicht beherrschbaren Risikos von vornherein unzulässig sind (und damit im Umkehrschluss dann aber auch in welchen diese mangels entsprechender Risiken grundsätzlich zulässig sein können, wobei Letzteres eine genaue Prüfung im Einzelfall natürlich nicht entbehrlich machen kann, da es letztlich bei der rechtlichen Betrachtung immer auf das konkrete Produkt im konkreten Anwendungsbereich ankommt).“ (Erben et al. 2009:59)

151 „Z. B. darf das System nicht die Frage eigenständig entscheiden dürfen, unter welchen Bedingungen ein Airbag auslöst.“ (Erben et al. 2009:57)

152 „Das Problem, dass die Systeme nicht vorhersehbar agieren, muss so kontrolliert werden bzw. zumindest so kontrolliert werden können, dass auch die Ergebnisse in dem Sinne vorhersehbar sind, dass – jedenfalls innerhalb bestimmter Grenzen – zwischen gewollt und nicht gewollt unterschieden werden kann. Dazu ist in jedem Fall für das konkrete System ein Satz vordefinierter Parameter bereit zu stellen, der nicht änderbar ist. Dieser Satz muss den absoluten Worst Case (Super-GAU) abdecken, der unter keinen Umständen und/oder keinen denkbaren Bedingungen eintreten darf. Auch wenn das einen bestimmten Systembruch bedeutet, da dadurch die Kreativität der Systeme gehemmt wird, so ist doch dieses Hemmnis eine notwendige Bedingung dafür, dass eine bestimmte im Sinne von: in ihrem Korridor spezifizierte Kontrolle möglich ist und damit letztlich wohl eine notwendige, wenn auch ggf. nicht hinreichende Bedingung dafür, dass OC Techniken in sicherheitskritischen Bereichen bzw. Anwendungen eingeführt werden können und in rechtlicher Hinsicht zulässig sind. (Erben et al. 2009:61)

153 keine Verletzung elementarer Rechtsgüter und Sanktionsfähigkeit von Rechtsgutverletzungen

154 Hierzu gehören Funktionalität, Ausfallsicherheit, Zuverlässigkeit, (Daten-)Sicherheit, Glaubwürdigkeit und Benutzerfreundlichkeit von OC-Systemen (vgl. André et al. 2009).

Schlussfolgerungen

Zusammenfassend kann hinsichtlich der rechtlichen Problemstellungen von OC festgehalten werden, dass sie im Kern mit dem mehrfach angesprochenen immanenten Dilemma von Emergenz zwischen Selbststeuerung und Außenkontrolle, zwischen eigenständiger Lernfähigkeit und der Gewährleistung der Sicherheit von OC-Systemen zu tun haben, wofür eine (letztlich einzelfallspezifisch zu entscheidende) rechtliche Balance zwischen der innovative Potenziale realisierenden Entwicklung und erfolgreichen Markteinführung von OC-Systemen mit entsprechender Innovations- und Risikobereitschaft von Wissenschaftlern, Entwicklern und Herstellern einerseits, und hinreichender, letztlich Priorität besitzender Sicherheit und (Produkt-)Haftung bei der Nutzung von OC-Systemen andererseits zu finden und zu gewährleisten ist. Hierfür reichen (in Deutschland) die bestehenden (haftungs)rechtlichen Regeln weitgehend aus, wobei es jedoch im Bereich von Computersystemen und insbesondere von eingebetteten Systemen bislang praktisch keine diese abstrakten Normen konkret auslegende Rechtsprechung in Form eigener Urteile gibt. Dementsprechend lassen sich – in Abhebung von IT-Technologien und Software im Allgemeinen – erst recht keine speziellen rechtlichen Regulierungen für OC-Systeme ausmachen, die zudem bislang auf dem Markt auch noch gar nicht angeboten und genutzt werden.

[155] „Daher braucht es aus rechtlicher Sicht u.a. sorgfältiger Observer-Controller-Architekturen, die sicher stellen, dass ein selbstorganisierendes System kein unerwünschtes globales Verhalten zeigt.“ (Erben et al. 2009:63)

8 Zusammenfassender Überblick

Dieses Kapitel fasst die erörterten Aspekte zu einem Gesamtbild der Entwicklungsdynamik und -perspektiven von OC zusammen.

Die für die (bisherige) Entwicklung von OC auf Handlungsebene relevante *Akteurkonstellation* ist gekennzeichnet durch einen Kern, der aus rund 20 kleinen Wissenschaftlergruppen mit jeweils 5-10 Mitarbeitern besteht, die genuine, im Einzelnen durchaus unterschiedlich ausgerichtete OC-Projekte verfolgen, als OC-Proponenten auftreten und weitgehend im Rahmen eines durch wenige Schlüsselpersonen (Müller-Schloer, Schmeck, Ungerer) dieses Kerns ausgearbeiteten und erfolgreich beantragten DFG-Schwerpunktprogramms finanziert werden. Neben der jeweiligen als Rahmenbedingung relevanten universitären Infrastruktur ist dieser Kern eingebettet in weltweite FE-Programme und -Projekte im Bereich von IuK-Technologien, die auf die Entwicklung und praktische Anwendung von selbstadaptiven selbstorganisierenden Systemen abzielen, die im Wesentlichen von Informatikern, Computer-Wissenschaftlern und Forschern aus benachbarten Disziplinen aus akademischen Forschungsinstituten sowie IT-Unternehmen in vielfach multidisziplinärer Kooperation bearbeitet werden. Der Kern ist mit Blick auf technische Anwendungen und die hierfür erforderlichen Entwicklungskosten offen für und interessiert an einem verstärkten (finanziellen und personellen) Engagement relevanter Industrieunternehmen, da die praktische Erprobung und Nutzung von OC-Systemen in vorhandene technische Systeme eingebettet werden und entsprechende Schnittstellen aufweisen muss, und von daher auf das Engagement und die Kooperation solcher Unternehmen, etwa aus der Elektro-, Energie- oder Automobilbranche, angewiesen ist. Diese industriellen, an SaSo-Systemen durchaus interessierten, aber speziell gegenüber OC bislang zurückhaltenden Akteure verfügen somit über eine beachtliche Veto-Macht, die allerdings durch den generellen Trend eines verstärkten Einsatzes von SaSo-Systemen und die Abhängigkeit ihrer Wettbewerbsfähigkeit von ihrer diesbezüglichen Kompetenz begrenzt wird. Staatliche Technologie- (und Wirtschafts-)politik ist – zumindest im Hinblick auf ihre Rolle als Querschnittstechnologie – vor allem auf EU-Ebene grundsätzlich an der Entwicklung von OC-Systemen interessiert, wie die in Abschnitt 3.2 aufgelisteten Forschungsvorhaben belegen. Ebenso ist die Etablierung von Normen, Schnittstellen-Standards und Zertifizierungsverfahren als wesentliche Bedingung des (kommerziellen) Einsatzes von OC aufgrund des noch jungen Alters von OC vorerst noch kaum Thema für staatliche Organe, wobei politische Akteure hier ebenfalls über eine gewisse Veto-Macht verfügen. Angesichts eines fehlenden öffentlichen OC-Diskurses spielen andere Akteure wie kritische Beobachter prekärer sozialer Folgen und des Missbrauchs der Ausbreitung von IuK-Technologien (wie digitale Spaltung der Gesellschaft, unzureichender Datenschutz, Nutzungszwang) in der Entwicklung von OC bisher keine Rolle.

Die für OC maßgeblichen *institutionellen Settings* betreffen – neben den allgemeinen organisatorischen und rechtlichen Gegebenheiten (und Zielvorgaben) der beteiligten Forschungsinstitutionen – die für die jeweiligen Anwendungen relevanten, durchaus auch unterschiedlichen Rahmenbedingungen, die für OC bislang noch kaum ausgefüllt sind, wie die angesprochenen fehlenden Normen, Schnittstellen-Standards und Zertifzierungsverfahren indizieren.

So sind etwa für eine Ampelsteuerung mithilfe von OC zum heutigen Zeitpunkt aus durchaus gut nachvollziehbaren Gründen bislang weder die relevanten haftungsrechtlichen Fragen geklärt, noch die Verkehrsleitstellen auf autonome Ampelsteuerung vorbereitet, noch die Herstellung und verkehrstechnische Unterbringung der benötigten Sensoren geklärt, noch ihre Finanzierung budgetiert, noch das Monitoring des Funktionierens und gegebenenfalls die Korrektur der für die Ampelsteuerung verantwortlichen Observer/Controller-Architektur gesichert.

Umgekehrt dürfte die Nutzung von OC in bereits im Einsatz befindlichen adaptiven Kamerasystemen im Falle ihrer nachgewiesenen technischen Funktionsfähigkeit relativ problemlos möglich sein, da dann die in diesem Anwendungsbereich bereits bestehenden und wirksamen institutionellen Settings zum Tragen kämen. So sind im Bereich adaptiver Kamerasysteme (weltweit) eine Reihe industrieller und Forschung betreibender Akteure aktiv und nehmen die Bemühungen um bislang noch nicht existierende einheitliche Interface-Standards zu.[156] Trotz einer Reihe von Hemmnissen wie langsame mechanische Reaktionszeit, aufwändige Installation, Hardware- und Software-Restriktionen, erforderliche Adaptivität und Konnektivität, die durch OC-Techniken teils behoben werden könnten, sind Entwicklungsdynamiken zu immer effektiveren und effizienteren adaptiven Kamerasystemen unverkennbar.[157]

Was die *Innovationsdynamik* von OC anbelangt, so lässt sich diese aufgrund des für sie verantwortlichen Zusammenspiels vieler verschiedener Einflussfaktoren nicht prognostizieren. – Bis zur gegenwärtigen Phase des Designs, der Analyse und erster Erprobung von OC-Systemen wird sie im Wesentlichen von einem jeweils vergleichsweise homogenen Setting von relevanten Faktoren im Wissenschaftssystem bestimmt, nämlich kleinen Wissenschaftlergruppen, die über Kompetenz und Erfahrung in der Untersuchung smarter IT-Systeme verfügen, überzeugt und engagiert OC-Systeme zu entwickeln suchen, als Ingenieurwissenschaftler ihre Forschungsprojekte häufig anwendungsorientiert konzipieren, sich vor allem im Rahmen des DFG-Schwerpunktprogramms über Ergebnisse, Probleme und Fortschritte ihrer Vorhaben austauschen und diese evaluieren, und hierüber auch akzeptable finanzielle Bedingungen vorfinden.

Ob und wie sich eine weiterreichende Innovationsdynamik[158] für OC – als einer mehr als inkrementellen, jedoch nurmehr bedingt radikalen Innovation im Rahmen der Entwicklung innovativer SaSo-

---

156 Der Weltmarkt für Bildverarbeitung belief sich in 2005 auf 7,4 Mrd. € und dürfte in 2015 16 Mrd. € betragen (vgl. BMBF 2007).

157 Diese werden von Müller (2008a:18) mit entsprechenden Literaturangaben wie folgt beschrieben: „Zahlreiche Weiterentwicklungen in Sensor- und Kameratechnik haben direkte Auswirkungen auf die Einsetzbarkeit und Leistungsfähigkeit von Bildverarbeitungsanwendungen. Bildverarbeitungssysteme werden immer kompakter und dadurch platzsparender integrierbar. Bildverarbeitungssysteme werden vermehrt kommunikationstechnisch in komplexe Fertigungsanlagen eingebunden. Der Trend geht hin zu general-porpose, lower end, lower cost vision systems. Die Anbieter fangen an mehr Wissen in die Software zu integrieren. [Infolgedessen kann] das Konfigurieren von CV-Software nun auch von einfachen Ingenieuren, nicht mehr nur von Informatikern vorgenommen werden. Die Trennung zwischen Vision Board Herstellern und Kamera Herstellern löst sich auf: Der Trend geht dahin, dass Vision Board Hersteller ihre eigenen Kameras produzieren bzw. Kamerahersteller in ihre Kameras eigene Vision Systeme integrieren. Durch Schnittstellenstandards wird die Integration von Bildverarbeitungskomponenten und -systemen vereinfacht. Bei Single Smart Cameras geht der Trend hin zu stetig ansteigender Rechnerleistung, bei der Autonomie des Systems wird der Fokus auf Selbstkonfiguration gelegt, um die Systemanwendungen zu vereinfachen. Bei Distributed Smart Cameras liegt der Forschungsschwerpunkt auf höheren Rechen- und Speicherkapazitäten, um die Zuverlässigkeit des Systems zu optimieren und Großraumüberwachung zu ermöglichen Bei Wireless Smart Cameras geht der Trend in Richtung Ubiquitious Computing, also die Integration der Smart Cameras in ein ‚Internet der Dinge'. Dafür muss vor allem die Autonomie der Systeme ausgebaut werden, um die Handhabung auch für Laien zu ermöglichen. Hierfür wird der Fokus auf erhöhten Kommunikationsfähigkeiten zwischen den Knoten gelegt."

158 Das Konzept der Innovationsdynamik hebt ab auf einen mehr oder minder kontinuierlichen Strom von Innovationen, der auf einer Eigendynamik beruht, die aus dem Zusammenspiel fördernder Push- und-Pull-Faktoren in einem entsprechenden sozialen Setting resultiert, das den der Moderne innewohnenden abstrakt-allgemeinen Innovationsdruck in aufeinander bezogene konkrete Innovationen überführt. Im Konzept der Innovationsdynamik stehen somit nicht einzelne Innovationen, sondern ein sozialer Prozess im Brennpunkt, der einerseits den gesellschaftlichen Entstehungs- und Bedingungszusammenhang technischer Entwicklungspfade und andererseits die diesen zugrunde liegende Interaktionsdynamik betont, in die die Gestaltung und Verbreitung jeweils konkreter Technologien notwendig eingebettet sind. Dabei ist eine solche Innovationsdynamik noch schwerer zu messen als (erfolgreiche) Innovationen selbst, deren Messung bereits durch die Definition von Innovation deutlich beeinflusst wird und durchaus zu Ergebnis-

Systeme – in Richtung seiner Marktpenetration entwickelt, hängt primär vom gelingenden Zusammenwirken vor allem unternehmensstrategischer Faktoren der ab (vgl. Conrad 2005:29):

- Verfügbarkeit ausreichender Ressourcen für FE-Investitionen,
- Eingehen strategischer Allianzen und Kooperation in Innovationsnetzwerken,
- Verbindung rascher Umsetzung von (innovativen) Unternehmensstrategien mit langem Atem bis zur Markteinführung innovativer Produkte und Verfahren,
- Orientierung auf innovationsfördernde Standorte, Lead-Märkte und Triade-Patente,
- effektives FE-Management und
- eine an Wertschöpfungsketten orientierte, integrierte Unternehmensstrategie.[159]

Als zentrale Rahmenbedingungen solcher Innovationsdynamiken sind festzuhalten, (1) dass der Zwang zur Innovation selbst zur Tradition der Moderne geworden ist, (2) dass mit der Kopplung von Wissenschaft und Technik ein wichtiger Innovationsmechanismus entstanden ist, der Neuerungen aus sich heraus schafft, indem die Erforschung und Änderung auf Dauer gestellt wird (vgl. Bechmann/Grunwald 1998:8), (3) dass sich neue Technologien keineswegs notwendig und widerstandslos in einer Gesellschaft durchzusetzen pflegen und ihre Einführung eher vermehrt mit technologischen Kontroversen einhergeht (vgl. Conrad 1990, Kitschelt 1984, 1985, Sieferle 1984, Simonis et al. 2001, Winner 1986), (4) dass die Möglichkeiten der Techniksteuerung und -kontrolle in modernen Gesellschaften nicht nur sozialstrukturell, sondern auch kulturell deutlich begrenzt sind[160], und (5) dass 85% bis 95% aller Entwicklungen nie zur Marktreife gelangen, Erfolg die Ausnahme und Scheitern die Regel ist (vgl. Bauer 2004, Braun 1992).

In historischer Retrospektive wird eine ausgesprochen resistente Innovationskultur des deutschen Innovationssystems deutlich, die sich technologiepolitisch kaum verändern lässt.[161] Die institutionellen Strukturen des deutschen Innovationssystems mit ausdifferenzierten netzwerkartigen Strukturen von Forschung, Entwicklung und Technologietransfer und einer korporativen Technologiepolitik verweisen jedoch auf seine ausgeprägte Fähigkeit zu zwar langsamer, aber erfolgreicher Adaption an Strukturwandel und Globalisierung von Innovationsprozessen (vgl. Harding 1999, Wengenroth 2009).

Für OC heißt dies, dass (1) es zwar technisch zunächst vor allem in Deutschland entwickelt werden mag, aber angesichts der institutionellen Strukturen des deutschen Innovationssystems und

---

sen führen kann, die nach zugrunde liegenden (evolutionstheoretischen) Konzepten (z.B. Nelson/Winter 1982) nicht zu erwarten waren (Stock et al. 2002).

159 Eine solche Innovationsdynamik führt tendenziell zu Produktivitätssteigerungen, wertintensiven (Hightech-)Produkten, erfolgreicher Marktpenetration und -beherrschung, sodass die sie erzeugenden Akteure eine Innovationsrendite erzielen, die es ihnen erlaubt, sich im globalen Wettbewerb wirtschaftlich zu behaupten und ihre Position zu stärken.

160 Nur wenn aus der Nutzung von Technologien unvermeidbare Gefahren für in der Wertordnung moderner westlicher Industriegesellschaften (gesetzlich) ebenfalls geschützte Rechte oder Gemeinschaftsgüter resultieren, stehen ansonsten durch garantierte Individualrechte gedeckte technische Möglichkeiten politisch zur Disposition. Von daher ist Gefahrenabwehr nicht nur ein, sondern meist der einzig mögliche Ansatz politischer Technikeinschränkung (Conrad 1994, Daele 1989). Daher weist staatliche (Technologie-)Politik in Bezug auf Innovationen relativ durchgängig die Janusköpfigkeit von Förderpolitik einerseits und Schutzpolitik andererseits auf.

161 „Die mentale Verfassung der Forscher, das Selbstverständnis der Unternehmen und Konsumenten sowie das gesellschaftliche Aushandeln von Prioritäten reagieren nicht unmittelbar auf Außenanreize monetärer oder institutioneller Art.“ (Grupp et al. 2002: xxii)

der hierzulande nur partiell konkurrenzfähigen IT-Industrie (z.B. SAP) nicht unbedingt von in Deutschland beheimateten Unternehmen vermarktet zu werden braucht, (2) offen ist, ob das erforderliche Zusammenwirken unternehmensstrategischer Faktoren und damit eine Marktdurchdringung von OC zustande kommt, (3) die Ausbildung eines entsprechenden, auf wenige marktfähige Anwendungen ausgerichteten Lead-Markts (im Bereich von SaSo-Systemen) OC zum Durchbruch verhelfen könnte, und (4) das Aufkommen einer technologischen Kontroverse um OC bislang unwahrscheinlich ist, aber angesichts seiner potenziellen Chancen und Risiken keineswegs ausgeschlossen werden kann.

Demgemäß sind die in den Kapiteln 3.3 und 3.4 thematisierten *Entwicklungsperspektiven* von OC noch recht offen. Als auf Autonomie, Selbstorganisation und kontrollierte Emergenz ausgerichtet verspricht OC im Erfolgsfall durchweg erwünschte Resultate zu zeitigen, zumal unter den beteiligten Forschern bislang durchaus ein Problembewusstsein möglicher OC-Risiken vorhanden ist. OC kann dabei von der Eigendynamik der Entwicklung von SaSo-Systemen[162] profitieren, aber auch noch von konkurrierenden, funktional äquivalenten IT-Systemen verdrängt werden. Eine (allmähliche) Marktpenetration von OC dürfte voraussichtlich in eingebetteter Form erfolgen, indem (zielgerichtet anwendungsbezogene) OC-Systeme im Rahmen der Verbesserung oder Erneuerung von bestimmten technischen Systemen (der Ampelsteuerung, der Kameraführung, der Logistik, der Energieverteilung und -einsparung) als hierbei zu verwendende (neuartige) IT-Systeme eingeführt werden.

Die *Folgewirkungen* einer Marktpenetration durch OC-Systeme können vielfältiger Natur sein und lassen sich (trivialerweise) nicht eindeutig bestimmen, da sie von den konkreten Nutzungs- und Anwendungsformen und den dabei gegebenen, auf OC reagierenden sozialen Kontexten abhängen (vgl. Grunwald 2002, Petermann 1992, Porter et al. 1982, Rip et al. 1995). Sofern die Markteinführung im von den beteiligten Wissenschaftlern grundsätzlich angestrebten Sinne gelingt, „the available technology for the utmost benefit to humans“ (Schmeck 2009a:4) zu nutzen, dürften die zu beobachtenden Folgewirkungen überwiegend positiv bewertet und akzeptiert werden. Unterstellt man jedoch realistischerweise, dass die vested interests der involvierten Industrieunternehmen entscheidendes Gewicht besitzen, dann ist mit mehr kontrovers bewerteten OC-Anwendungen und -Folgewirkungen zu rechnen. Generell dürfte OC eher einen Verstärkereffekt in Bezug auf die (in der Literatur und öffentlichen Diskursen) erörterten Risiken von IT-Systemen, wie Datenmissbrauch, Einschränkung von Privacy, Nutzungszwang, digitale Spaltung der Gesellschaft etc., haben, während genuine OC-Risiken unerwünschter Emergenzen aufgrund entsprechenden Designs der OC-Systeme vermutlich eher selten auftreten und kaum mit katastrophalen Folgewirkungen verbunden sein dürften. Umgekehrt sollte – wie bei der Einführungneuer Technologien typischerweise zu erwarten – zumindest anfangs durchaus damit gerechnet werden, dass OC-Systeme nicht den angestrebten Mehrwert erbringen oder Systemabstürze induzieren, was dann zu unerwünschten Folgewirkungen, personellen und finanziellen Mehrkosten und zeitlichen Verzögerungen führen kann.

162 „It is not the question, **whether** adaptive and self-organising systems will emerge, but **how** they will be designed and controlled.“ (Schmeck 2009a:6)

9 Ergebnisse und Schlussfolgerungen

Dieses Kapitel fragt nach der Validität und Generalisierbarkeit der Ergebnisse des Vorhabens, fasst diese noch einmal kompakt zusammen und benennt (politische) Gestaltungsmöglichkeiten im Hinblick auf die weitere Entwicklung von Organic Computing.

9.1 Validität und Generalisierbarkeit

Die Reliabilität[163] und Validität der Ergebnisse einer Untersuchung hängen zum einen von der Klarheit und Stringenz des Untersuchungsdesigns und zum andern von der methodischen Abgesichertheit der erhobenen Befunde ab. Validität ist dann gegeben, wenn die erhobenen Daten und Befunde tatsächlich die Sachverhalte repräsentieren, die sie messen sollen, wenn sie also als deren Abbildung Gültigkeit beanspruchen können.[164]

Hinsichtlich der Validität der Ergebnisse müssen sich die Autoren auf die wissenschaftliche Qualität der Befunde in der Fachliteratur, die fachliche Reputation ihrer Verfasser und die Fachkompetenz und Offenheit ihrer Interviewpartner verlassen. Dennoch ist ihre Validität aus den in Kapitel 1 angeführten methodologischen Gründen (offene Zukunft der Realisierung und Folgewirkungen von OC, fehlende Detailanalysen, keine Theorieprüfung) nicht gesichert, sodass die getroffenen Aussagen vor dem Hintergrund der relativen Validität strukturanaloger Arbeiten über IT-Systeme, Innovationsdynamiken und die Folgen neuer Technologien nur Plausibilität beanspruchen können.

Schließlich können aufgrund der hermeneutischen Anlage der Studie die präsentierten Interpretationen sozialer Sachverhalte diesen stets nur mehr oder weniger angemessen sein, aber keine Eindeutigkeit beanspruchen, insofern sie unterschiedliche Befunde nutzen und diese verschieden interpretieren können. Somit behält eine problemorientierte, empiriegeleitete, Theoriekonzepte eklektisch kombinierende, auf hermeneutisches Verständnis abzielende Arbeit eine interpretative Offenheit. Von daher lassen sich Reliabilität und Validität bei solchen Arbeiten prinzipiell nur vage, aber nicht strikt bestimmen.

Die dargestellten Befunde des Vorhabens zeigen zwar die große mögliche Bandbreite zukünftiger OC-Entwicklungen auf, ohne diese jedoch infolge von deren immanenter Offenheit signifikant einschränken zu können. Da hierbei keine gänzlich unerwarteten Ereignisse vermutet werden, enthält dieser Bericht auch keine signifikanten Aussagen über neuartige, in den jeweiligen Fachdiskursen nicht erörterte Entwicklungspfade.

Vor diesem methodologischen Hintergrund sind auch die nachfolgenden Ausführungen über (politische) Gestaltungsmöglichkeiten sachlich durchaus begründet und nicht arbiträr, aber von nur eingeschränkter Validität.

---

163 Formal ist Reliabilität dann gegeben, wenn die wiederholte Untersuchung desselben Objekts unter gleichen Bedingungen (möglichst durch andere Personen) zum gleichen Ergebnis führt.

164 Hierfür müssen etwa in psychologischen Untersuchungen die Testergebnisse mit einem für den betreffenden Sachverhalt relevanten äußeren, als Validitätskriterium bestimmten Merkmal statistisch möglichst hoch korrelieren.

Generalisierungen werden in dieser Studie in begrenztem Ausmaß auf zwei Ebenen vorgenommen. Zum einen finden sich allgemeine Aussagen über Chancen, Risiken oder Entwicklungsmuster von OC, die auch auf den drei durchgeführten Fallstudien beruhen, jedoch primär die Nutzung und Anwendung von (noch) allgemeineren Analysen der Chancen, Risiken, Innovations- und Entwicklungsmuster von (neuen) Technologien und IT-Systemen darstellen. Zum anderen finden sich nur wenige Generalisierungen von OC-Systemen auf SaSo-Systeme, weil dies nicht wirklich Ziel dieses Vorhabens war und es vielmehr gerade auch um die Bestimmung von OC-Spezifika gegenüber generellen Eigenschaften smarter Systeme ging. Von daher steht eindeutig Organic Computing im Mittelpunkt dieses Vorhabens, das demgemäß keinen weitergehenden Generalisierungsanspruch seiner auf OC bezogenen Ergebnisse erhebt.

9.2 Zentrale Ergebnisse

Die in den vorangehenden Kapiteln bereits vorgestellten Untersuchungsergebnisse sind in diesem Abschnitt nochmals kompakt zusammengefasst:

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 SaSo-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 die 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 stärker gemeinsamer Forschungsziele und -linien (Selbst-X-Eigenschaften, kontrollierte Emergenz) führt(e).[165]
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 techni-

[165] Sozialhistorisch entstanden OC und SaSo dabei etwa zeitgleich aus verschiedenen Forschungsfeldern.

sche Systeme und nicht allein um größere, komplexere und vernetztere IT-Systeme, die sowohl die Verbesserung bereits in der Praxis eingesetzter technischer Systeme, z.B. adaptive Kamerasysteme, als auch die Realisierung neuartiger technischer Systeme, z.B. die Organisation und Kontrolle selbstorganisierender Systeme in technischen Materialien[166], 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 substanzielle 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 bis hin zu AC, die sich primär um ein besseres Verständnis und die Modellierung dezentraler SaSo-Systeme bemühen, eher als einander ergänzend denn als miteinander konkurrierend wahrgenommen. Dessen unbeschadet konkurrieren die verschiedene OC-Themen behandelnden Forschungsvorhaben natürlich durchaus um jeweils verfügbare Fördermittel.

8) Es geht bisher im Wesentlichen um (anwendungsorientierte) Grundlagenforschung mit zwar in ihrem Zeithorizont differierenden, aber durchweg mittel- bis langfristigen 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.[167]

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).

---

166 vgl. das Ziel des OC-Projekts „Organisation and Control of Self-Organising – Systems in Technical Compounds“: “Another aim of the project is it to show how compounds of self-organizable systems can be created that do not exist in nature in this form and that are technically realizable and manageable. New methods for the organisation and control of such compounds will be developed.”

167 Demgemäß existieren im Hinblick auf das technische Potenzial von OC bislang kaum Kooperationen zwischen wissenschaftlichen und industriellen Akteuren.

13) Insofern es bei der Realisierung von OC-Systemen stets sowohl um die Förderung erwünschter Autonomie als auch um die Vermeidung unerwünschter Autonomie geht, beziehen sich die entsprechenden Maßnahmen – wie in Kapitel 2.4 ausgeführt – einerseits auf die Auswahl geeigneter Architekturmuster in der Designphase, die Bekämpfung architekturinduzierter Schwachstellen durch Abschwächung etwa der autonomiefördernden Auslegung von Eigenschaften, Selbststabilisierung und Superstabilisierung, Fehlereindämmung, und Sicherstellung der Lebendigkeit, und andererseits auf 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).

14) Für die entsprechenden Risikomanagementsysteme, in die diese Maßnahmen zur (autonomieinduzierten) Schwachstellenbekämpfung einzubetten sind, erscheinen nach Renn (2008) je nach der Risikostruktur der zu realisierenden OC-Systeme unterschiedliche Ziele, Funktionen, Strategien und Instrumente angemessen, je nachdem, ob es sich um ‚lineare', komplexitäts-, unsicherheits- oder ambiguitätsinduzierte Risikoprobleme handelt; hierbei spielen typischerweise unterschiedliche Diskursformen, Akteure, Konflikttypen und Problemlösungen eine Rolle. Dabei beruht die Abschätzung und Bewertung von risk management Optionen[168] auf Kriterien wie Effektivität, Effizienz, Minimierung externer Nebenfolgen, Nachhaltigkeit, Fairness, politische und rechtliche Implementation(sfähigkeit), ethische Akzeptabilität und öffentliche Akzeptanz. So basiert das Vertrauen in die für das Risikomanagement verantwortlichen Institutionen auf ihrer wahrgenommenen Kompetenz und Objektivität, ihrer Fairness, der Konsistenz ihrer Aktionen, ihrer Ernsthaftigkeit, ihrer Glaubwürdigkeit und ihrer Fähigkeit zu Empathie (vgl. Renn 2008:179/185, 280, 173, 122).

15) Abschließend ist auch festzuhalten, dass Organic Computing vom Grundgedanken her eine technical-fix Lösung zur Bewältigung der mit dem Trend zu ubiquitous computing auftretenden, technisch verstandenen Problemlagen ist, die die Notwendigkeit und Sinnhaftigkeit dieses Trends als gegeben annimmt und alternative (soziale) Umgangsformen und Lösungsmuster ausblendet, die diesen Trend hinterfragen und als gesellschaftlich problematisch zu begrenzen suchen.

9.3 Roadmap und (politische) Gestaltungsmöglichkeiten

Fragt man zum Abschluss dieses Berichts nach dem erwünschten Entwicklungspfad von OC und den entsprechenden (politischen) Gestaltungsmöglichkeiten, so ergeben sich beide cum grano salis aus der Kombination von seitens der OC-Proponenten propagierten Zielvorstellungen (menschlichen Bedürfnissen dienende OC-Anwendungen), von verfügbarem Wissen über Innovationsprozesse und technologische Trajektorien, über technologische Kontroversen, über die Steuerungsmöglichkeiten von Forschungs- und Technologiepolitik, über Chancen und Risiken von IT-Systemen, und von den Handlungsoptionen, Gestaltungsvorstellungen und -intentionen maßgeblicher Akteure, insbesondere der Innovationspolitik.

[168] im Rahmen eines entsprechenden Politikzyklus: Generierung, Abschätzung, Evaluierung, Selektion, Implementation, Monitoring und Feedback von Optionen

Was den angestrebten Entwicklungspfad 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 (vgl. Abbildung 9.1),
- 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[169],
- und um die durch diese Aktivitäten induzierte Eigendynamik, um eine breitenwirksame Durchsetzung von OC zu erreichen.

Forschungs-, Technologie- und Innovationspolitik kann nun im Rahmen der ihr zur Verfügung stehenden Möglichkeiten einen solchen Entwicklungspfad unterstützen, wobei sich ihre Rahmenbedingungen im Hinblick auf die faktisch zentrale Rolle von internationaler Wettbewerbsfähigkeit und einer diese stärkenden Innovationsdynamik in den letzten Jahrzehnten sukzessive markant verändert haben (vgl. Dolata 2004, Conrad 2005). Allerdings sind ihre Gestaltungsmöglichkeiten wie bereits angedeutet sozialstrukturell und soziokulturell begrenzt.

[169] Im Hinblick auf mögliche Gestaltungsansätze von OC-Systemen lassen sich dabei relevante Gesichtspunkte eines wirksamen Risikomanagements und einer risk governance nutzen, was etwa die Gewährleistung von Vertrauen in verantwortliche Institutionen durch entsprechende Kompetenzen und Fähigkeiten, die Beachtung relevanter Kontextebenen, Risikobewertung je nach Risikotypus (primär tolerierbare, aber zu reduzierende, als auch intolerable Risiken), Abschätzung und Bewertung von risk management Optionen, oder Formen der Risikokommunikation und Partizipation anbelangt (vgl. Renn 2008).

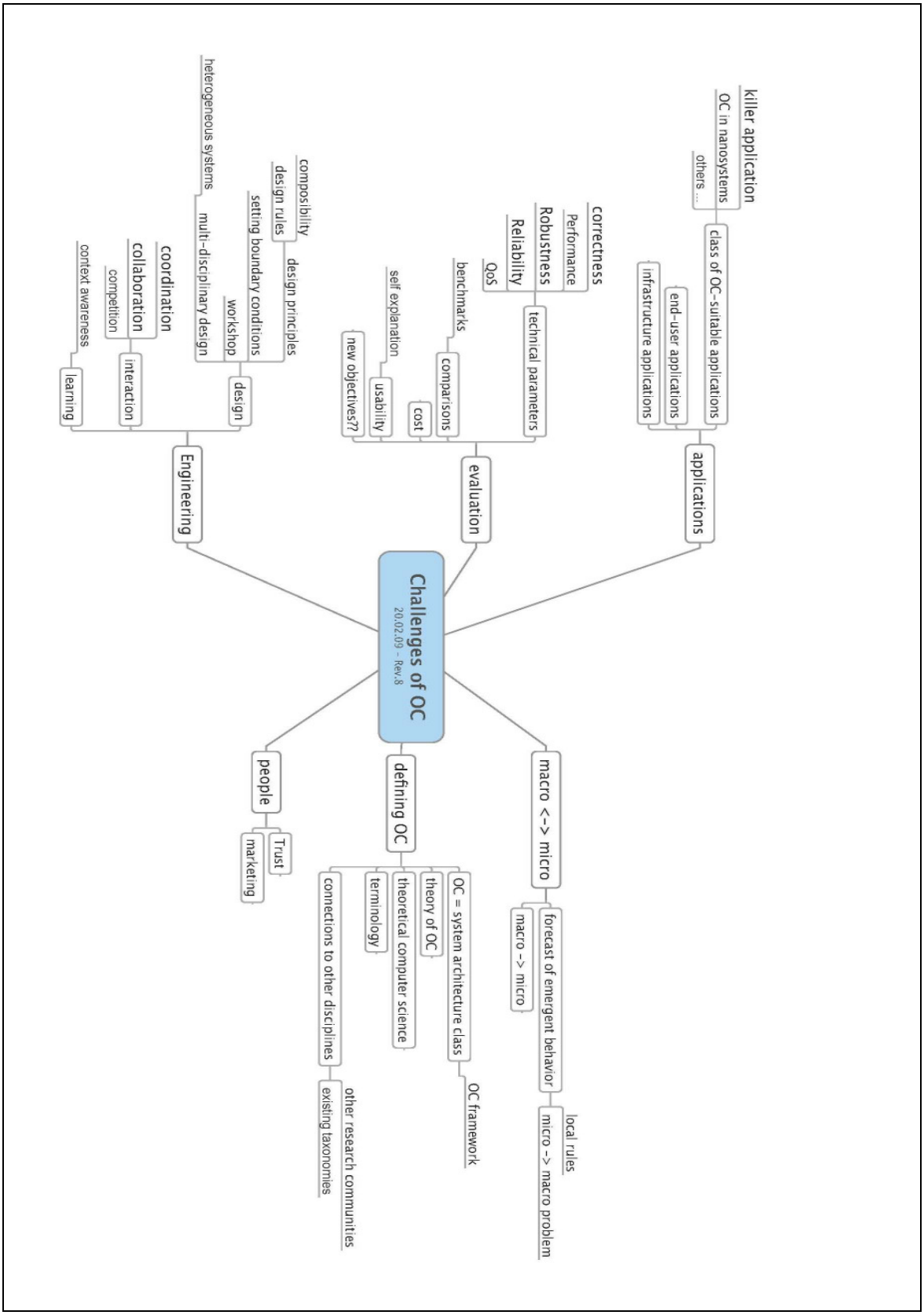

Abbildung 9.1: Herausforderungen von OC

Quelle: Müller-Schloer 2009

Insofern Forschungs- und Technologiepolitik Forschungs- und Entwicklungsprozesse nicht selbst auf substanzieller Ebene direkt steuern kann[171], sind nicht Forschungshandlungen, sondern Forschungseinrichtungen, also formale Organisationen, der primäre Zugriffspunkt forschungspolitischer Steuerung.[172] „Forschungspolitik kann bestimmte Forschungseinrichtungen *etablieren* bzw. wieder auflösen; Forschungspolitik kann Forschungseinrichtungen mit – mehr oder weniger – finanziellen und personellen Ressourcen *alimentieren*; Forschungspolitik kann Forschungseinrichtungen über die – mehr oder weniger maßgebliche – Beteiligung an der Definition der Forschungsthemen und des Forschungstypus *programmieren*; und Forschungspolitik kann Forschungseinrichtungen hinsichtlich ihrer Finanz-, Personal- und Organisationsstrukturen und hinsichtlich der äußeren Grenzen ihres Forschungshandelns – z.B. über das Verbot oder die Genehmigungspflichtigkeit bestimmter Untersuchungsmethoden und Forschungsthemen – *regulieren*." (Schimank 1991: 506f.) Mit der Ausrichtung der Forschungs- und Technologiepolitik auf Kontextsteuerung (vgl. Werle/Schimank 2000, Willke 1989) beschränkt sie sich zwecks Förderung von Technikentwicklung und Innovationsdynamik zunehmend darauf, für die Innovationen hervorbringenden Akteure (in Wissenschaft und Wirtschaft) Rahmenbedingungen zu setzen, ihre Such-, Konflikt- und Konsensprozesse zu moderieren, FE-Programme und FE-Projekte zu koordinieren und entsprechende Anstöße zu geben. Trotz ihres primär reaktiven Charakters kann Technologie- und Innovationspolitik durchaus, etwa zur Entwicklung ausgewählter Schlüsseltechnologien, initiativ werden und entscheidende Anstöße geben, ohne die es nicht oder nur sehr viel später zu entsprechenden Technikentwicklungen gekommen wäre, wie sich gerade in der deutschen Technologiepolitik an einer Reihe von Fällen demonstrieren lässt und wofür sowohl das BioRegio-Programm als auch das InnoRegio-Programm gute Beispiele darstellen. Allerdings sind ihre Wirksamkeit und ihr Erfolg – ebenso wie bei anderen Akteuren im Innovationsprozess – abhängig von der Mitwirkung der Politikadressaten und darüber hinaus meist auch von weiteren Akteuren sowie vom positiven Zusammenspiel der für gelingende Innovationen relevanten Faktoren, wie dies exemplarisch in dem ‚Porter-Diamanten'[173] (Porter 1990) und in der für die Innovationskapazität eines Landes mitentscheidenden Qualität der Verknüpfung von allgemeiner Innovationsinfrastruktur und clusterspezifischen Umweltbedingungen (Furman et al. 2002) zum Ausdruck kommt.

Angesichts der Vorreiterrolle deutscher OC-Forschung, ihrer Anwendungsorientierung sowie der vorteilhaften ingenieurwissenschaftlichen Bedingungen kann die deutsche Technologie- und Innovationspolitik im Hinblick die besondere Bedeutung von Lead-Märkten für die internationale Wettbewerbslage eines Landes Lead-Markt-Strategien verfolgen und die Bildung ebensolcher, stets produkt- oder prozessspezifischer Lead-Märkte zu fördern versuchen (vgl. Beise 2001, Jacob et al. 2005, Jänicke/Jacob 2006), wobei sie allerdings Gefahr läuft, auf das falsche Pferd zu setzen, insofern sich potenzielle Lead-Märkte kaum ex ante bestimmen lassen, da sie sich erst als solche

---

171 „Systemtheoretische Analysen gesellschaftlicher Differenzierung machen darauf aufmerksam, dass eine *direkte* politische Steuerung des *basalen* Handelns in einem bestimmten Teilsystem der modernen Gesellschaft nur um den Preis von Dilettantismus bzw. einer regressiven Entdifferenzierung möglich ist." (Schimank 1991: 506)

172 Dabei erhalten Forschungsförderorganisationen als intermediäre Institutionen, die weder einfach die politische Steuerungsfähigkeit des Staates erhöhen noch einfach von der Wissenschaft vereinnahmt werden, die institutionalisierte Ambivalenz von wissenschaftlichen Qualitäts- und politischen Relevanzinteressen in einem Fließgleichgewicht und erlauben damit, unter Entwicklung entsprechender Eigeninteressen (der Bestandserhaltung) grundsätzlich dezentrale Kontextsteuerung (Braun 1997).

173 Der Porter-Diamant verweist auf den auf nationaler Ebene gegebenen systematischen Zusammenhang von Unternehmensstrategie, -struktur und -wettbewerb, von Produktionsfaktoren, von Nachfragebedingungen und von der Existenz international wettbewerbsfähiger Ausrüstungs- und branchenverwandter Industrie für die nationale Wettbewerbsfähigkeit, auf die die Politik in diversen Formen Einfluss nehmen kann.

erweisen, wenn andere Länder in der Folge das gleiche Innovationsdesign ebenfalls und kein konkurrierendes nutzen.[174] Mit Blick auf die fünf maßgeblichen Lead-Markt-Faktoren, nämlich Preis- oder Kostenvorteile, Nachfragevorteile, Exportvorteile, Transfervorteile und Marktstrukturvorteile kann Technologie- und Innovationspolitik

- aufgrund der hohen Bedeutung anspruchsvoller Nachfrage für Lead-Märkte Regulierungen z.B. im Hinblick auf hohe Energieeffizienz oder geringe umweltschädliche Emissionen so gestalten, dass daraus bei zukünftig international verschärften Umweltstandards nationale Nachfrage- und Vorreitervorteile für eine innovative nationale Umweltindustrie resultieren[175],
- durch anspruchsvolle staatliche Nachfrage Innovationsprozesse fördern und die Risiken der diese Innovationen entwickelnden Firmen reduzieren,
- Anreize für den Export durch die kompatible Gestaltung von Regulierungen im Hinblick auf Auslandsmärkte schaffen oder
- Marktstrukturvorteile durch staatliche Forschungsförderung und durch Stärkung marktorientierter Selektionsmechanismen kreieren, um so alternative technologische Optionen offen zu halten und nationale Lock-ins zugunsten idiosynkratischer Technologien zu vermeiden (Beise 2001).[176]

Dabei sprechen die bislang technisch unzureichend erreichte kontrollierte Emergenz und die Abwesenheit von Standards für SaSo-Systeme allerdings dafür, OC-Anwendungen inkrementell einzuführen. Von daher sollten erste Anwendungen in Bereichen realisiert werden, in denen die Risiken von Autonomie und Emergenz kontrollierbar sind. Das könnten z.B. Ampelanlagen sein, bei denen die Freiheitsgrade der Selbstorganisation zunächst klein sind. Durch Kooperation mit einem wichtigen Marktakteur im Bereich der Ampelanlagen könnten in der Einführungsphase die technischen Standards festgelegt werden. Gleichzeitig ließe sich eine Kommune zur Mitwirkung gewinnen, auf deren Gebiet die ersten selbstorganisierenden Ampeln aufgestellt werden würden.[177] Mit der Zeit könnten die Freiheitsgrade der Selbstorganisation der Ampeln erweitert und weitere Standards definiert werden. Ein Erfolg eines solchen Feldversuchs würde eine gute Grundlage dafür bieten, OC-Technologie auch in anderen, ökonomisch relevanteren Bereichen zu erproben und einzuführen.

Da OC-Anwendungen im Allgemeinen einer etablierten (oder neuen) Technologie nur eine Eigenschaft, nämlich Selbstorganisation und dezentrale Steuerung hinzufügen, spricht dabei zum einen viel für OC-Anwendungen in solchen Technologien, die besonders stark von den Eigenschaften der Selbstorganisation und der dezentralen Steuerbarkeit profitieren können, und dürfte zum ande-

---

174 Ein prägnantes Beispiel für einen solchen Fehlschlag ist das in Frankreich in den 1980er Jahren forcierte Minitel, das sich gegen das Internet nicht behaupten konnte (vgl. Beise 2001).

175 Dabei beeinflusst staatliche Politik die branchen- und sektorspezifischen Nachfragebedingungen „in many often unintentional and counterproductive ways because it has an incomplete view of what determines competitive advantage.“ (Porter 1990: 644)

176 Allerdings kann eine auf die Stärkung von Marktstrukturvorteilen (Faktorpreisrelationen, Infrastruktur, Wettbewerbsverhältnisse) gerichtete Politik nur die Selektionsmuster von Technologien im Allgemeinen verbessern.

177 Dabei sollte die Öffentlichkeit über den Test informiert werden, sodass sich gegebenenfalls ein öffentlicher Diskurs über SaSo- und speziell OC-Systeme entwickeln könnte, in den Verkehrsteilnehmer diesbezüglich (erste) Erfahrungen sammeln und einbringen könnten. Diese Erfahrungen böten zudem eine Basis dafür, dass die OC-Technologie in der Bevölkerung eher akzeptiert würde.

ren die Kooperation zwischen universitär eingebunden Forschern und den jeweils relevanten Marktakteuren zumeist Voraussetzung für eine erfolgreiche Markteinführung von OC-Systemen sein. Da Letzteres bislang noch kaum stattfindet, bietet sich hier für die Technologie- und Wirtschaftspolitik neben der Förderung einer anwendungsorientierten OC-Forschung ein geeignetes Betätigungsfeld der kooperativen Einbettung von OC-Entwicklungen, in das die Erfahrungen aus analogen innovationspolitischen Programmen (BioRegio, InnoRegio) eingehen können, gerade was angesichts bestehender (globaler) sozialstruktureller Verhältnisse, Macht- und Akteurkonstellationen die Gestaltungsoptionen von Politik einerseits und ihre begrenzten Einflussmöglichkeiten andererseits anbelangt.[178] Gerade vor diesem Hintergrund ist es entscheidend, im Rahmen unvermeidbarer realer Entwicklungstrends in Richtung smarter IT-Systeme Optionen der Entwicklung geeigneter Prinzipien für die technologische Basis einer zukünftig beherrschbaren und anpassungsfähigen (insbesondere menschenfreundlichen) Gestaltung der uns umgebenden Informationsverarbeitungsinfrastruktur wahrzunehmen und sich hierbei unter Anerkennung unvermeidlich bestehender vested interests der maßgeblichen Akteure mögliche win-win-Konstellationen zunutze zu machen.

Da angesichts der relativen Frühphase und der vielfältigen möglichen Anwendungsfelder von Organic Computing sehr wohl unterschiedliche Entwicklungspfade möglich sind, sollte die Forschungs- und Technologiepolitik sachlich, zeitlich und sozial Flexibilität bewahren und wie oben ausgeführt auf Kontextsteuerung fokussieren, indem sie sich zwecks Förderung von Technikentwicklung und Innovationsdynamik darauf beschränkt, für die Innovationen hervorbringenden Akteure (in Wissenschaft und Wirtschaft) Rahmenbedingungen zu setzen, ihre Such-, Konflikt- und Konsensprozesse zu moderieren, FE-Programme und FE-Projekte zu koordinieren und entsprechende Anstöße zu geben. Dazu kann durchaus auch die Bereitstellung zusätzlicher Mittel für auf kontrollierte Emergenz in OC-Systemen abzielende Verfahren und Sicherheitstests gehören, um das frühzeitige und ausreichende Management genuiner Risikoaspekte von OC zu gewährleisten.

Über die Präferenz für eine inkrementelle Einführung von OC-Anwendungen in Bereichen hinaus, die von Selbstorganisation und dezentraler Steuerung direkt profitieren würden und/oder in denen sich kontrollierte Emergenz absehbar realisieren lässt, können zum heutigen Zeitpunkt hingegen keine validen Empfehlungen zugunsten bestimmter, eine erfolgreiche Marktpenetration sicherstellender Entwicklungspfade gegeben werden, die über die bereits bekannten und angeführten Anwendungsbereiche hinausreichen.[180]

Demnach könnte der Markt der Ampelsteuerungen ein für die Einführung von OC-Systemen geeigneter Markt zu sein, weil er eine Art Spielfeld für OC-Systeme darstellen kann. Sofern – wie von ihren Befürwortern behauptet – für OC-Ampelsysteme im Vergleich mit herkömmlichen Ampelsteuerungen keine zusätzlichen Sicherheitsrisiken bestehen, kann in diesem Bereich die Einsatzfähigkeit der OC-Technologie in der Praxis demonstriert werden. Ein ähnliches Spielfeld könnten auch adaptive Kamerasysteme mithilfe von OC sein. Sie bieten darüber hinaus den Vorteil, dass ihre möglichen Anwendungen – wie ihr Einsatz zwecks Analyse von Käuferverhalten oder Überwa-

---

178 Deshalb ist die Unterscheidung von (technologischen) Potenzialen und tatsächlich erwartbaren Entwicklungspfaden wesentlich; denn letztere hängen viel mehr von bestehenden (situativen) Akteurkonstellationen, Interessenlagen und -berücksichtigungsmustern, (internationalen) Strukturgegebenheiten sowie Deutungs- und Diskursmustern ab.

180 Denn gegenwärtig ist eine umfassende Evaluierung von OC-Systemen nicht möglich, da sich diese noch weitgehend im (frühen) FE-Stadium befinden.

chung – keine bestehenden Technologien verdrängen, sondern neue Einsatzmöglichkeiten für technische Systeme eröffnen.[181] Schließlich bietet sich auch der Bereich der Logistik für eine relativ kontinuierlichen Einführung von OC-Techniken an, da diese an Objekte der Logistikkette mit Selbststeuerungsalgorithmen anschließen können, da sich der Bereich sich selbst steuernder Objekte in der Logistikkette sukzessive erweitern lässt, da sich Logistiksysteme aufgrund ihrer Prozessstruktur gut für den Einsatz von OC-Techniken eignen, und da die Logistik relativ übereinstimmende Zielvorstellungen und kaum Kontroversen der maßgeblichen Akteure (win-win Konstellation) kennzeichnen.

Großes ökonomisches Potenzial wird für OC-Anwendungen in Bereichen der Automobilindustrie (smart car) und im Gesundheits- und Lebensbereich gesehen. Allerdings sind dort die Sicherheitsanforderungen an marktfähige Produkte wesentlich höher und es besteht ein großer Bedarf hinsichtlich der Vereinheitlichung von Normen (wie Schnittstellen, Protokollen etc.).[182]

---

181 Allerdings darf hier nicht außer Acht gelassen werden, dass die beobachtbare gesellschaftliche Abneigung gegen Technologien, die der Verhaltensanalyse oder der Überwachung dienen, einen breiteren Einsatz dieser Anwendungen verhindern könnte.

182 Aufgrund der im Einzelnen bislang nicht absehbaren konkreten sozio-ökonomischen Arrangements derartiger OC-Anwendungen sind hierüber keine substanziellen tragfähigen, über die aus der Literatur über Innovations- und Marktdurchdringungsprozesse bekannten Aussagen möglich (vgl. Dogson 2000, Dogson/Rothwell 1994, Dosi et al. 1988, Freeman 1974, Freeman/Soete 1990, Grupp 1997, 1998, Mowery/Nelson 1999, Porter 1986, 1990).

10 Literatur

Accenture/The Center for Education and Research in Information Assurance and Security (CERIAS), 2001: CERIAS Security Visionary Roundtable. Call to Action. Purdue University, West Lafayette

Alahuhta, P. et al, 2006: Safeguards in a World of Ambient Intelligence (SWAMI). Deliverable D2. Dark scenarios in ambient intelligence: Highlighting risks and vulnerabilities. Sevilla

André, E. et al. 2009: Antrag zur Bewilligung einer DFG-Forschergruppe mit Schwerpunkt OC-Trust. Augsburg u.a.

Arnold, D. et al. (Hg), 2008: Handbuch Logistik. Berlin: Springer

Bar-Yam, Y, 2004: A mathematical theory of strong emergence using multiscale variety, Complexity 9 (6): 15-24

Bauer, M. (Hg), 1995: Resistance to New Technology. Cambridge: Cambridge University Press

Bauer, R, 2004: Scheitern als Chance? Fehlgeschlagene Innovationen als Gegenstand der technikhistorischen Forschung, in: Wissenschafts Management. Zeitschrift für Innovation, 10 (5): 26-31

Bechmann, G. (Hg), 1993: Risiko und Gesellschaft. Grundlagen und Ergebnisse interdisziplinärer Risikoforschung. Opladen: Westdeutscher Verlag

Bechmann, G., Grunwald, A,1998: Was ist das Neue am Neuen, oder: wie innovativ ist Innovation (Einleitung), TA-Datenbank-Nachrichten 7(1): 4-11 (Schwerpunktthema Innovation)

Beck, U, 1986: Risikogesellschaft. Auf dem Weg in eine andere Moderne. Frankfurt: Suhrkamp

Bedau, M, 1997: Weak Emergence, in: J. Tomberlin (Hg), Philosophical Perspectives 11: Mind, Causation, and World. Malden (MA): Blackwell

Beise, M, 2001: Lead Markets: Country-specific Success Factors of the Global Diffusion of Innovations. Heidelberg: Physica

Bellman, K. et al, 2008: Systems Engineering for Organic Computing: The Challenge of Shared Design and Control between OC Systems and their Human Engineers, in: R.P. Würtz (Hg), Organic Computing. Berlin: Springer

Bendel, O, Hauske, S, 2004: E-Learning: Das Wörterbuch. Aarau: Sauerländer Verlag

Bernard, Y, 2008: Selbstorganisierende adaptive Systeme: Chancen, Risiken und Gestaltungsansätze von Organic Computing. Literaturüberblick Organic Computing. Ms. Hannover

Bernard, Y, 2009: OC und aktuelleTrends im Software Engineering. Ms. Hannover

Bernauer, A. et al, 2008: Evaluation of the Learning Classifier System XCS for SoC run-time control**,** Lecture Notes in Informatics 134: 761-768

Bizer, J. et al, 2006: Technikfolgenabschätzung Ubiquitäres Computing und Informationelle Selbstbestimmung: Studie im Auftrag des BMBF. Kiel/Berlin (http://www.taucis.hu-berlin.de/_download/TAUCIS_Studie.pdf

Blaze, M. et al, 1999: The role of trust management in distributed systems security, in: Vitek, Jensen (Hg), Secure Internet Programming: Security Issues for Mobile and Distributed Objects. Berlin: Springer

BMBF, 2007: Optische Technologien – Wirtschaftliche Bedeutung in Deutschland. Bonn

Bohn, J. et al, 2005: Social, Economic, and Ethical Implications of Ambient Intelligence and Ubiquitous Computing, in: W. Weber et al. (Hg), Ambient Intelligence. Berlin http://www.vs.inf.ethz.ch/publ/papers/socialambient.pdf

Bonabeau, E. et al, 1999: Swarm Intelligence: From Natural to Artificial Systems. Santa Fe Institute Studies on the Sciences of Complexity, Oxford University Press

Bora, A, 2004: Technologische Risiken. Ms. Bielefeld

Bora, A, 2005: Zum soziologischen Begriff des Diskurses. Ms. Bielefeld

Bora, A, Döbert, R,1993: Konkurrierende Rationalitäten: Politischer und technisch-wissenschaftlicher Diskurs im Rahmen einer Technikfolgenabschätzung von genetisch erzeugter Herbizidresistenz in Kulturpflanzen, Soziale Welt 44: 75-97

Brancovici, G-S, 2008: Architecture and Framework for Trustworthy Autonomous Systems. Diss. Hannover

Braun, H.-G. (Hg), 1992: Symposium on „Failed Innovations“, Social Studies of Science 22

Brand, K-W, 2000: Kommunikation über Nachhaltigkeit: eine resonanztheoretische Perspektive, in : W. Lass, F. Reusswig (Hg), Strategien der Popularisierung des Leitbildes „Nachhaltige Entwicklung“ aus sozialwissenschaftlicher Perspektive. Tagungsdokumentation Band II: Tagungsbeiträge. UBA-Forschungsbericht 29817132, Berlin

Brand, K-W. et al,1997: Ökologische Kommunikation in Deutschland. Opladen: Westdeutscher Verlag

Branke, J, Schmeck, H, 2002: Designing evolutionary algorithms for dynamic optimization problems, in: S. Tsutsui, A. Ghosh, A (Hg), Theory and Application of Evolutionary Computation: Recent Trends. Berlin: Springer

Branke, J. et al, 2006: Organic computing – addressing complexity by controlled self-organization, in T. Margaria et al. (Hg), Post-Conference Proceedings of the 2nd International Symposium on Leveraging Applications of Formal Methods, Verification and Validation (ISoLA). Paphos, Zypern

Braun, D, 1997: Die politische Steuerung der Wissenschaft. Ein Beitrag zum „korporativen“ Staat. Frankfurt: Campus

Braun, H.-G. (Hg), 1992: Symposium on „Failed Innovations“, Social Studies of Science 22

Breu, L, 2008: Distributed Smart Cameras. Ms. ETH Zürich

Bundesamt für Sicherheit in der Informationstechnik (BSI), 2005: BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS). http://www.bsi.bund.de/literat/bsi_standard/index.htm

Bundesamt für Sicherheit in der Informationstechnik (BSI), 2006: Pervasive Computing: Entwicklungen und Auswirkungen. Ingelheim: SecuMedia Verlag

Cakar, E. et al, 2007: Towards a quantitative notion of self-organisation, Evolutionary Computation, 2007. CEC 2007. IEEE Congress: 4222-4229

Cakar, E. et al, 2008: Investigation of Generic Observer/Controller Architectures in a Traffic Scenario, in H.G. Hegering et al. (Hg), INFORMATIK 2008, Beherrschbare Systeme – dank Informatik, Bd. 2. Bonn: Köllen Druck & Verlag

Castells, M, 1996: The Rise of the Network Society. Malden/Oxford: Blackwell

Christen, M, 2004: Schuldige Maschinen? Autonome Systeme als Herausforderung für das Konzept der Verantwortung, Jahrbuch für Wissenschaft und Ethik 9: 163-191

Chu, Y-H. et al, 1997: Referee: Trust management for web applications. World Wide Web Journal 2:127-139

Clarke, D. et al, 1999: Model Checking. The MIT Press

Clarke, L, Short, J, 1993: Social Organization and Risk: Some Current Controversy, American Review of Sociology 19: 375-399.

Coenen, C, 2008: Konvergierende Technologien und Wissenschaften. Der Stand der Debatte und politischen Aktivitäten zu „Converging Technologies“. TAB Hintergrundpapier 16, Berlin

Conrad, J. (Hg), 1980: Society, Technology and Risk Assessment. London: Academic Press

Conrad, J, 1990: Technological Protest in West Germany: Signs of a Politicization of Production?, Industrial Crisis Quarterly 4: 175-191

Conrad, J, 1994: Technikentwicklung, Unsicherheit und Risikopolitik, in: M. Jänicke et al. (Hg), Umwelt Global. Veränderungen, Probleme, Lösungsansätze. Berlin: Springer

Conrad, J, 2005: Grüne Gentechnik – Gestaltungschance und Entwicklungsrisiko. Perspektiven eines regionalen Innovationsnetzwerks. Wiesbaden: DUV

Conrad, J, 2008a: Prozedurale und Strukturvorschläge, Klarstellungen und Fragen zum OC-Projekt. Ms. Berlin

Conrad, J, 2008b: Analytisches Raster der Chancen und Risiken von Organic Computing. Ms. Berlin

Conrad, J, 2008c: Probleme, Fragen und Thesen aus Literatur im Umfeld „Organic Computing“. Ms. Berlin

Coroama, 2006: Pervasive Computing im Alltag. digma 2006.3: 106-109

Daele, W. van den, 1989: Kulturelle Bedingungen der Technikkontrolle durch regulative Politik, in: P. Weingart (Hg), Technik als sozialer Prozeß. Frankfurt: Suhrkamp

Daele, W. van den, 1996: Objektives Wissen als politische Ressource: Experten und Gegenexperten im Diskurs, in: W. van den Daele, F. Neidhardt (Hg), Kommunikation und Entscheidung. Politische Funktionen öffentlicher Meinungsbildung und diskursiver Verfahren. WZB-Jahrbuch 1996. Berlin: edition sigma

Daele, W. van den, 1999: Von rechtlicher Risikovorsorge zu politischer Planung. Begründungen für Innovationskontrollen in einer partizipativen Technikfolgenabschätzung zu gentechnisch erzeugten herbizidresistenten Pflanzen, in: A. Bora (Hg), Rechtliches Risikomanagement. Form, Funktion und Leistungsfähigkeit des Rechts in der Risikogesellschaft. Berlin: Duncker & Humblot

Dahinden, U, 2006: Framing. Eine integrative Theorie der Massenkommunikation. Konstanz: UVK

DFG (Deutsche Forschungsgemeinschaft), 2009: DFG Jahresbericht 2008. Bonn

Dodgson, M, 2000: The Management of Technological Innovation: An International and Strategic Approach. Oxford: Oxford University Press

Dodgson, M., Rothwell, R. (Hg), 1994: The Handbook of Industrial Innovation. Aldershot: Edward Elgar

Dolata, U, 2004: Unfassbare Technologien, internationale Innovationsverläufe und ausdifferenzierte Politikregime. Perspektiven nationaler Technologie- und Innovationspolitiken. artec-paper 110, Bremen

Dosi, G. et al. (Hg), 1988: Technical Change and Economic Theory. London: Pinter

EATMP (European Air Traffic Management Programme), 2003: Guidelines for Trust in Future ATM Systems: A Literature Review. European Organisation for the Safety of Air Navigation, Brüssel

Ebenhöh, E, 2006: Modelling human behaviour in social dilemmas using attributes and heuristics. Diss. Osnabrück

Eckert, C, 2001: IT-Sicherheit. München: Oldenbourg

Eddon, G, Eddon, H, 1998: Inside Distributed Com. Microsoft Press

Eder, K, 1995: Framing and Communication of Environmental Issues. Final Report to the EU-Commission. Florenz: European University Institute

Engler, M, 2007: Fundamental Models and Algorithms for a Distributed Reputation System. Diss. Stuttgart

ENISA (European Network and Information Security Agency), 2007a: ENISA Roadmap for contemporary and Emerging Risks. Heraklion: ENISA

ENISA, 2007b: ENISA Study: Emerging-risks-related Information Collection and Dissemination. Heraklion: ENISA

ENISA, 2007c: Risk Management / Risk Assessment in European regulation, international guidelines and codes of practice. Heraklion: ENISA

Erben, M. et al, 2009: Rechtsexpertise zu selbstorganisierenden adaptiven IT Systemen. Heidelberg

EU-Commission, 2006: European Competitiveness Report 2006. Brüssel

Fink, G, Frincke, D, 2007: Autonomic computing: freedeom or threat? Login 32 (2): 6-14

Foucault, M, 1982: Die Ordnung des Diskurses. München: Carl Hanser

Freeman, C, 1974: The Economics of Industrial Innovation. Harmondsworth: Penguin

Freeman, C, 1991: Networks of innovators: a synthesis of research issues, Research Policy 20: 499-514

Freeman, C, 1992: The Economics of Hope. Essays on Technical change, Economic Growth and the Environment. London: Pinter

Freeman, C., Soete, L. (Hg), 1990: New Explorations in the Economics of Technical Change. London: Pinter

Friedewald, M. et al. (Hg), 2006: Safeguards in a World of Ambient Intelligence (SWAMI). The brave new world of ambient intelligence: A state-of-the-art review. Report, Sevilla

Friedewald, M. et al, 2007: Privacy, identity and security in ambient intelligence: A scenario analysis, Telematics and Informatics 24/1: 15-29

Fromm, J, 2005a: Types and Forms of Emergence. Technical Report: http://arxiv.org/abs/nlin.AO/0506028

Fromm, J, 2005b: Ten questions about emergence. Technical Report: http://arxiv.org/abs/nlin.AO/0509049

Furman, J. et al, 2002: The determinants of national innovative capacity, Research Policy 31: 899-933

Gabbai, J. et al, 2005: Self-organization, emergence and multi-agent systems, Proceedings of the International Conference on Neural Networks and Brain. Band 3, Peking

Gabriel, P. et al, 2006: Pervasive Computing: Entwicklungen und Auswirkungen. Bonn: BSI http://www.bsi.bund.de/literat/studien/percenta/Percenta_bfd.pdf

Gerhards, J, 1992: Dimensionen und Strategien öffentlicher Diskurse, Journal für Sozialforschung 32: 307-318

Gershenson, C, 2007: Design and Control of Self-organizing Systems. Diss. Brüssel

Gesellschaft für Informatik et al, 2008: Grand Challenges der Technischen Informatik. Report, Bonn

Giddens, A., 1990: The Consequences of Modernity. Standford University Press

Gleich, A. von, 2006: Fortschritt der Ahnungslosigkeit, Politische Ökologie 101: 41-44

Gleich, A. von, 2008: Resiliente Systeme. Möglichkeiten und Grenzen einer leitbildorientierten Technikgestaltung. Vortragsfolien, Bremen

Gleich, A. von, et al, 2007: Bionik. Aktuelle Trends und zukünftige Potenziale. Eigenverlag IÖW: Berlin

Graefe, A. et al, 2008: Der Umgang mit Barrieren bei der Einführung von Pervasive Computing. Ein Literaturüberblick, Technikfolgenabschätzung. Theorie und Praxis 17 (1): 13-19

Grote, G. et al, 2004: Setting the Stage: Characteristics of Organizations, Teams and Tasks Influencing Team Processes, in: R. Dietrich, T. Childress (Hg), Group Interaction in High Risk Environments. Aldershot: Ashgate

Grunwald, A, 2002: Technikfolgenabschätzung – Eine Einführung. Berlin: edition sigma

Grupp, H, 1997: Messung und Erklärung des technischen Wandels. Berlin: Springer

Grupp, H, 1998: Foundations of the Economics of Innovation. Theory, Measurement and Practice. Cheltenham: Edward Elgar

Grupp, H. et al, 2002: Zur technologischen Leistungsfähigkeit Deutschlands 2001. Bonn: BMBF

Habermas, J, 1981: Theorie des kommunikativen Handelns. 2 Bände. Frankfurt: Suhrkamp

Habermas, J, 1985: Der philosophische Diskurs der Moderne. Zwölf Vorlesungen. Frankfurt: Suhrkamp

Hähner, J, Müller-Schloer, C, 2009: Organic Computing. Vortragsfolien, Hannover

Hajer, M, 1995: The Politics of Environmental Discourse. Ecological Modernization and the Policy Process. Oxford: Clarendon Press

Haniel, A, Stübinger, E, 1999: Technikgenese – zwischen Steuerung und Evolution. München: Herbert Utz Verlag

Hanseth, O, Ciborra, C, 2007: Risk, Complexity and ICT. Cheltenham: Edward Elgar

Harding, R, 1999: One best way? The case of German innovation in an era of globalisation. Ms. Köln

Heesen, J. et al, 2005: Leben in einer vernetzten und informatisierten Welt. Context-Awareness im Schnittfeld von Mobile und Ubiquitous Compting. Stuttgart: Universität Stuttgart, Nexus-Schriftenreihe http://www.uni-stuttgart.de/philo/index.php?id=65&no_cache=1&file=337&uid=761

Heiß, H-U. et al, 2008: Studie zur Modellierung von Autonomie in IT-Architekturen (ASA_2). TU Berlin

Hillis, W.D, 1988: Intelligence as an emergent behaviour, or the songs of Eden. Daedalus 117: 175-189

Hilty, L. et al, 2003: Das Vorsorgeprinzip in der Informationsgesellschaft. Auswirkungen des Pervasive Computing auf Gesundheit und Umwelt. Studie des Zentrums für Technologiefolgen-Abschätzung. Bern: TA-SWISS http://www.ta-swiss.ch/a/info_perv/2003_46_pervasivecomputing_d.pdf

Hilty, L. et al, 2004: Assessing the human, social, and environmental risks of pervasive computing, Human and Ecological Risk Assessment 10/5: 853-874

Hoffmann, M, Hähner, J, 2007: ROCAS: A Robust Online Algotithm for Spatial Partitioning in Disributed Smart Camera Systems. First ACM/IEEE International Conference on Distributed Smart Cameras 2007. Ms. Hannover

Hoffmann, M, et al, 2008: Towards Self-organising Smart Camera Systems, in: U. Brinkschulte et al. (Hg), Architecture of Computing Systems – ARCS 2008. Berlin: Springer

Höhne, J, 2009: Fallstudie Logistik. Ms. Berlin

Holtmannspötter, D. et al, 2006: Aktuelle Technologieprognosen im internationalen Vergleich. Übersichtsstudie. VDI, Düsseldorf www.bmbf.de/pub/technologieprognosen_int_vergleich_ZTC_bd_58_.pdf

Huber, J, 1989: Herrschen und Sehnen. Kulturdynamik des Westens. Weinheim: Beltz

Huber, J, 2001: Allgemeine Umweltsoziologie. Opladen: Westdeutscher Verlag

Huber, J. 2004: New Technologies and Environmental Innovation. Cheltenham: Edward Elgar

Huber, M, 2009: Was ist „systemisches Risiko"? Anmerkungen zu den Risiken der Risikokommunikation, GAIA 18: 9-12

Hütt, M-T, 2006: Was ist Selbstorganisation und was nützt sie zum Naturverständnis? Eine Einführung, in: M. Vec et al. (Hg), Selbstorganisation. Ein Denksystem für Natur und Gesellschaft. Köln: Böhlau Verlag

IBM Research, 2009: Autonomic Computing, http://www.research.ibm.com/autonomic/

ISTAG (Information Society Technologies Advisory Group), 2004: ISTAG Report on Grand Challenges in the Evolution of the Information Society. http://www.cordis.lu/ist/istag.htm

Jacob, K. et al, 2005: Lead Markets of Environmental Innovations. ZEW Economic Studies 27. Heidelberg: Physica

Jameson, A, 2003: Adaptive interfaces and agents. Lawrence Erlbaum Associates, Inc., Mahwah, NJ

Jänicke, M, Jacob, K. (Hg), 2006: Environmental Governance in Global Perspective. New Approaches to Ecological and Political Modernisation. FFU Report 01-2006, FU Berlin

Japp, K.P, 1996: Soziologische Risikotheorie. Funktonale Differenzierung, Politisierung und Reflexion. Weinheim: Juventa

Johnson, C.W, 2005: What are Emergent Properties and How Do They Affect the Engineering of Complex Systems? Ms. Glasgow

Johnson, S, 2001: Emergence – The Connected Lives of Ants, Brains, Cities, and Software. New York: Touchston

Keller, R, 1997: Diskursanalyse, in: R. Hitzler, A. Honer (Hg), Sozialwissenschaftliche Hermeneutik. Eine Einführung. Opladen: Leske + Budrich

Kemmann, S, 2005: Die IEC/EN Norm 61508-3:2001. Vortragsfolien, TU Kaiserslautern, Arbeitsgruppe Software Engineering (http://wwwagse.informatik.uni-kl.de/teaching/qsm/ws2004/material/Norm_61508-3_final.pdf)

Kephart, J, Chess, D, 2003: The Vision of Autonomic Computing, Computer 36: 41-50

Kitschelt, H, 1984: Der ökologische Diskurs. Frankfurt: Campus

Kitschelt, H, 1985: Materiale Politisierung der Produktion, Zeitschrift für Soziologie 14: 188-208

Kündig, A, Bütschi, D. (Hg), 2008: Die Verselbständigung des Computers. Zürich: vdf Hochschulverlag AG

LaPorte, Todd R, Consolini, P. M, 1991: Working in Practice But Not in Theory: Theoretical Challenges of "High Reliability Organizations", Journal of Public Administration Research and Theory 1: 19-47

Lenk, H, 2003: Können Informations- und Robotersysteme verantwortlich sein? Ethische und soziale Chancen sowie Probleme der neuen Informationstechnologien, in: W. Niederlag et al. (Hg), Ethik und Informationstechnik am Beispiel der Telemedizin 2: Dresden: Allgemeines Krankenhaus Eigenverlag

Lieshout, M. van et al. (Hg), 2006: Converging Applications enabling the Information Society. Trends and Prospects of the Convergence of ICT with Cognitive Science, Biotechnology, Nanotechnology and Material Sciences. Sevilla http://fiste.jrc.es/pages/horizontal.htm

Lorenz, A, Weyer, J, 2008: Fahrerassistenzsysteme und intelligente Verkehrssteuerung. Soziologische Analysen hoch automatisierter Verkehrssysteme. Arbeitspapier 21, Dortmund

Luhmann, N, 1986: Ökologische Kommunikation. Kann die moderne Gesellschaft sich auf ökologische Gefährdungen einstellen? Opladen: Westdeutscher Verlag

Luhmann, N, 1991: Soziologie des Risikos. Berlin: de Gruyter

Luhmann, N, 2000: Vertrauen. Ein Mechanismus der Reduktion sozialer Komplexität. Stuttgart: UTB

Mahr, B, 2007: Ein Modell des Modellseins, in: U. Dirks, E. Knobloch (Hg), Modelle. Berlin: Peter Lang

Mainzer, K, 2004: Thinking in Complexity. The Computational Dynamics of Matter, Mind, and Mankind. New York: Springer

Mainzer, K, 2008: Organic Computing and Complex Dynamical Systems – Conceptual Foundations and Interdisciplinary Perspectives, in: R.P. Würtz (Hg), Organic Computing. Berlin: Springer

Mattern, F. (Hg), 2007: Die Informatisierung des Alltags. Leben in smarten Umgebungen. Berlin: Springer

Meier, K, Stiftung Risiko-Dialog, 2006: Stakeholder-Dialog II über Pervasive Computing. Aussichten und Einsichten. riskDOK 004. Fakten aus dem Risiko-Dialog. St. Gallen: Stiftung Risiko-Dialog http://www.ictswitzerland.ch/files/webcontent/news/riskDOK004.pdf

Menezes, A. et al, 1996: Handbook of Applied Cryptography. Boca Raton (FL): CRC Press

Merlin, P.M, 1974: A study of the recoverability of computing systems. Diss. Irvine (CA)

Minai, A. et al, 2006: Complex Engineered Systems: A New Paradigm, in: D. Braha et al. (Hg), Complex Engineered Systems. Berlin: Springer

Mowery, D., Nelson, R. (Hg), 1999: Sources of Industrial Leadership. Studies of Seven Industries. Cambridge: Cambridge University Press

Müller, A, 2008a: Fallstudie: Adaptive Kamerasysteme. Ms. Berlin

Müller, A, 2008b: Privacy-Debatte. Ms. Berlin

Müller, G. et al, 2006: Security and Privacy Risks in Future IT. Report, Freiburg

Müller-Schloer, C, 2009: Challenges of OC. Folie der Ergebnisse einer Arbeitsgruppe des 8. Kolloquiums des Schwerpunktprogramms „Organic Computing“ in Bochum 2009

Müller-Schloer, C, Sick, B, 2008: Controlled Emergence and Self-Organization, in: R.P. Würtz (Hg), Organic Computing. Berlin: Springer

Müller-Schloer, C. et al, 2004: Organic Computing, Informatik_Spektrum_4: 332-336

Nafz, R. et al, 2006: Applications in Organic Computing. Report 2006-22, Universität Augsburg

Neitzke, H-P. et al, 2008: Risks of Ubiquitous Information and Communication Technologies, GAIA 17: 362-369

Nelson, R., Winter, S, 1982: An Evolutionary Theory of Economic Change. Cambridge: Belknap-Harvard Press

OECD, 1980: OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Paris http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html

Orwat, C. et al, 2008: Towards Pervasive Computing in Health Care – A Literature Review, BMC Medical Informatics and Decision Making 8: 26-43

Orwat, C. et al, 2008: Towards Pervasive Computing in Health Care – A Literature Analysis, BMC Medical Informatics and Decision Making

Orwell, G, 2008 (1949): 1984. München: Heyne

Pade, C, Petschow, U, 2008: Selbstorganisierende adaptive Systeme: Analyse der Chancen und Risiken sowie der Gestaltungsansätze neuer IKT-Ansätze. Vortragsfolien, Berlin

Perrow, C, 1984: Normal Accidents. New York: Basic Books

Petermann, Th. (Hg), 1992: Technikfolgen-Abschätzung als Technikforschung und Politikberatung. Frankfurt: Campus

Petschow, U. et al, 2007: Selbstorganisierende adaptive Systeme: Analyse der Chancen und Risiken sowie der Gestaltungsansätze neuer IKT-Ansätze. Projektantrag, Berlin

Petschow, U. et al, 2009: Selbstorganisierende adaptive Systeme: Analyse der Chancen und Risiken sowie der Gestaltungsansätze neuer IKT-Ansätze. Zwischenbericht, Berlin

Pfohl, H-C. (Hg), 2007: Innovationsmanagement in der Logistik. Hamburg: Deutscher Verkehrs-Verlag

Pisko, E, 2008: Verkehrssteuerung – neuere Ansätze unter Berücksichtigung von OC: Adaptive Systeme, Forschungs- und Praxisansätze, Standards und Normen. Ms. Berlin

Pissarskoi, E, 2008: Trends der IKT Forschung, OC und Risiken und Chancen. Ms. Berlin

Pissarskoi, E, 2009: Marktanalyse zu selbstorganisierenden technischen Systemen. Ms. Berlin

Porter, M, 1986: Wettbewerbsvorteile. Spitzenleistungen erreichen und behaupten. Frankfurt: Campus

Porter, A. et al, 1982: A Guidebook for Technology Assessment and Impact Analysis. New York: Elsevier

Porter, M, 1990: The Competitive Advantage of Nations. London: MacMillan Press

Prothmann, H. et al, 2008: Organic Control of Traffic Lights, in: C. Rong et al. (Hg), Proceedings of the 5th International Conference on Autonomic and Trusted Computing (ATC-08), volume 5060 of LNCS, Berlin: Springer

Prothmann, H. et al, 2009: Organic traffic light control for urban road networks, International Journal of Autonomous and Adaptive Communications Systems 2 (3): 203-225

Punie, Y. et al. (Hg), 2006: Safeguards in a World of Ambient Intelligence (SWAMI). Dark scenarios in ambient intelligence: Highlighting risks and vulnerabilities. Report, Sevilla

Renn, O, 2008: Risk Governance. Coping with Uncertainty in a Complex World. London: Earthscan

Renn, O, Keil, F, 2008: Systemische Risiken: Versuch einer Charakterisierung, GAIA 17: 349-354

Renn, O, Keil, F, 2009: Was ist das Systemische an systemischen Risiken?, GAIA 18: 97-99

Richter, K, Rost, J-M, 2004: Komplexe Systeme. Frankfurt: Fischer

Rip, A. et al, 1995: Managing Technology in Society: The Approach of Constructive Technology Assessment. London: Pinter

Roberts, Karlene A. (Hg), 1993: New Challenges to Understanding Organisations. New York: Macmillan

Rossmann, T, Tropea, C. (Hg), 2005: Bionik: Aktuelle Forschungsergebnisse in Natur- , Ingenieur- und Geisteswissenschaft. Berlin: Springer

Schimank, U, 1991: Politische Steuerung in der Organisationsgesellschaft – am Beispiel der Forschungspolitik, in: W. Zapf (Hg), Die Modernisierung moderner Gesellschaften (25. Deutscher Soziologentag). Frankfurt: Campus

Schmeck, H, 2006: Organic Computing. Vortragsfolien, Karlsruhe

Schmeck, H, 2009a: Organic Computing. Status and Outlook. Vortragsfolien für das 8. Kolloquium des Schwerpunktprogramms „Organic Computing“ in Bochum

Schmeck, H, 2009b: Introductory Remarks. Vortragsfolien für das 9. Kolloquium des Schwerpunktprogramms „Organic Computing“ in Augsburg

Schmeck, H. et al, 2009: Adaptivity and self-organisation in organic computing systems, ACM Transactions on Computational Logic V (N): 1-31

Schmidt, G. et al, 2009: Systemic Risks of Genetically Modified Organisms in Crop Production: Interdisciplinary Perspective, GAIA 18: 119-126

Scholz-Reiter, B. et al, 2007: Evolution in der Logistik – Selbststeuerung logistischer Prozesse. Ms. Bremen http://www.sfb637.uni-bremen.de/pubdb/repository/SFB637-A5-07-008-IIC.pdf

Sheridan, T.B, 2002: Humans and Automation. System Design and Research Issues. New York: Wiley & Sons

Sieferle, R. P, 1984: Fortschrittsfeinde. Opposition gegen Technik und Industrie von der Romantik bis zur Gegenwart. München: Beck

Simonis, G. et al. (Hg), 2001: Politik und Technik. Analysen zum Verhältnis von technologischem, politischem und staatlichem Wandel am Anfang des 21. Jahrhunderts. PVS-Sonderheft 31/2000. Wiesbaden: Westdeutscher Verlag

Snow, D, Benford, R, 1988: Ideology, frame resonance, and participant mobilization, in: B. Klandermans et al. (Hg), From Structure to Action: Comparing Social Movement Research Across Cultures (Vol. 1, International Social Movement Research). Greenwich, CT: JAI Press

Stachowiak, H, 1973: Allgemeine Modelltheorie. Berlin: Springer

Stein, S, 2004: Emergenz in der Software-Entwicklung – bereits verwirklicht oder Chance? Diplomarbeit, Dresden

Stephan, A, 1999: Emergenz. Von der Unvorhersagbarkeit zur Selbstorganisation. Dresden: Dresden University Press

Stephan, A, 2006: Zur Rolle des Emergenzbegriffs in der Philosophie des Geistes und in der Kognitionswissenschaft, in: D. Sturma (Hg), Philosophie und Neurowissenschaften. Frankfurt: Suhrkamp

Stock, G. et al, 2002: Firm size and dynamic technological innovation, Technovation 22: 537-549

TNO/IDATE, 2006: Software intensive systems in the future. Final Report. http://www.itea2.org/attachments/150/ITEA_SIS_in__the_future__Final_Report.pdf

Tofler, A, 1980: The Third Wave. New York: Bantam Books

Umweltbundesamt (Hg), 2009: Nanotechnik für Mensch und Umwelt. Chancen fördern und Risiken mindern. Dessau-Roßlau

University of Twente (Hg), 2009: Converging Technologies, Converging Societies. Proceedings of SPT 2009

VDE/ITG/GI, 2003: Organic Computing: Computer- und Systemarchitektur im Jahr 2010, VDE/ITG/GI Positionspapier. http://www.giev.de/fileadmin/redaktion/Presse/VDE-ITG-GI-Positionspapier_20Organic_20Computing.pdf

Vec, M. et al. (Hg), 2006: Selbstorganisation. Ein Denksystem für Natur und Gesellschaft. Köln: Böhlau Verlag

Voigt, C, 2009: Argumentationsanalyse: Für und wider den Einsatz von Organic Computing. Ms. Berlin

Weingart, P. et al, 2002: Von der Hypothese zur Katastrophe. Der anthropogene Klimawandel im Diskurs zwischen Wissenschaft, Politik und Medien. Opladen: Leske + Budrich

Weiser, M, 1991: The Computer for the 21st Century, Scientific American 265 (3): 94-104

Wengenroth, U, 2009: Innovation Culture in Germany. Frameworks of Science and Technology Policies. Paper, München

Werle, R., Schimank, U. (Hg), 2000: Gesellschaftliche Komplexität und kollektive Handlungsfähigkeit. Frankfurt: Campus

Werner, M, 2007: Eigenschaften verlässlicher Systeme. Habil. TU Berlin

Weyer, J, 2009: Dimensionen der Komplexität und Perspektiven des Komplexitätsmanagements, in: J. Weyer, I. Schulz-Schaeffer (Hg), Management komplexer Systeme. Konzepte für die Bewältigung von Intransparenz, Unsicherheit und Chaos. München: Oldenbourg

Willke, H, 1989: Systemtheorie entwickelter Gesellschaften. Dynamik und Riskanz moderner gesellschaftlicher Selbstorganisation. Weinheim/München: Juventa

Windt, K, 2006: Selbststeuerung intelligenter Objekte in der Logistik, in: M. Vec et al. (Hg), Selbstorganisation. Ein Denksystem für Natur und Gesellschaft. Köln: Böhlau Verlag

Windt, K, 2008: Ermittlung des angemessenen Selbststeuerungsgrades in der Logistik - Grenzen der Selbststeuerung, in: P. Nyhuis (Hg), Beiträge zu einer Theorie der Logistik. Berlin: Springer

Winner, L, 1986: The Whale and the Reactor. A Search for Limits in an Age of High Technology. Chicago: The University of Chicago Press

Wodak, R, Meyer, M. (Hg), 2001: Methods of critical discourse analysis. Introducing qualitative methods. London: Sage

Wolf, T. de, Holvoet, T, 2005: Towards a methodology for engineering self-organising emergent systems, Self-Organization and Autonomic Informatics (I), Frontiers in Artificial Intelligence and Applications 135:18-34

Wright, D. et al, 2006: Safeguards in a World of Ambient Intelligence (SWAMI). Deliverable D1. The brave new world of ambient intelligence: A state-of-the-art review. Sevilla

Wright, D. et al, 2008: Safeguards in a World of Ambient Intelligence. Heidelberg: Springer

Würtz, R. P. (Hg), 2008: Organic Computing. Berlin: Springer

A-I ANHANG I:

Liste der interviewten Personen

Dipl. Inf. Andreas Bernauer, Universität Tübingen, Institut für Informatik

Prof. Dr. Brockmann, Universität Osnabrück, Institut für Informatik

Dr. Peter Dittrich, Universität Jena, Nachwuchsgruppe "Biosystemanalyse" am Institut für Informatik

Dr. Thomas Fuhrmann Technische Universität München, Institut für Informatik, Lehrstuhl für Netzarchitekturen und Netzdienste

Prof. Dr. Hans-Ulrich Heiß, Technische Universität Berlin, Fakultät IV; Institiut für Telekommunikationssysteme; Fachgebiet Kommunikations- und Betriebssysteme

Prof. Dr.-Ing. Andreas Herkersdorf, technische Universität München, Lehrstuhl für Integrierte Systeme

Dipl.-Inform. Silvian Kaiser, Technische Universität Berlin, Fakultät IV – Elektrorechnik und Informatik

Dipl.-Ing. Florian Kuzmany Technische Universität München, Wissenschaftlicher Mitarbeiter Lehrstuhl für Fördertechnik Materialfluss Logistik

Dipl.-Ing. Klaus Dieter Müller IBM Senior Consultant Executive Briefing Center, System & Hardware, Technical Marketing, Competence Center Europe,

Prof. Dr. Christian Müller-Schloer, Leibniz Universität Hannover, Institut für Systems Engineering - System und Rechnerarchitektur

Prof. Dr. Franz Josef Rammig, Universität Paderborn, Heinz Nixdorf Institut; Fachgruppe Entwurf paralleler Systeme

Prof. Dr. Wolfgang Rosenstiel, Universität Tübingen, Lehrstuhl Technische Informatik
Prof. Dr. Hartmut Schmeck (KIT Karlsruhe) Institut für Angewandte Informatik und Formale Beschreibungsverfahren (AIFB)

Prof. Dipl.-Ing. Markus Ullmann, Referatsleiter Wissenschaftliche Grundlagen und Neue Technologien, Bundesamt für Sicherheit in der Informationstechnik (BSI)

Prof. Dr. Rolf Würtz, Universität Bochum, Institut für Neuroinformatik

A-II ANHANG II:

Argumentationsanalyse für und wider den Einsatz von Organic Computing

Inhalt

1. Einleitung II-3

2. Das Hauptargument für den Einsatz von OC II-6

3. Checkliste: Sollte im Anwendungsfall x ein OC-System eingesetzt werden? II-35

4. Literatur II-40

1. Einleitung

Dieser Text präsentiert und analysiert die innerhalb des Projekts erstellten Argumentlandkarten. Ergebnis dieser Analyse ist eine Checkliste für den Einsatz von OC-Systemen, die sich im Schlussteil dieses Textes befindet. Diese Checkliste hilft dabei zu überprüfen, ob ein OC-System in einem Anwendungsgebiet eingesetzt werden sollte oder nicht. Mit jeder Frage in dieser Checkliste wird eine These in der Argumentlandkarte überprüft. Jede positive Antwort unterstützt die Argumentation für oder schwächt die Argumentation gegen den Einsatz des OC-Systems. Jede negative Antwort unterstützt die Argumentation gegen oder schwächt die Argumentation für den Einsatz des OC-Systems.

Der Text stellt jeweils einzeln diese Fragen und die hinter ihnen stehenden Thesen und Argumente vor. Die Landkarten selbst geben dabei einen Überblick darüber, welche spezifische argumentative Funktionen die in der Checkliste abgefragten Thesen besitzen. Die Rollen dieser Thesen in der Debatte sind höchst unterschiedlich. Es handelt sich keinesfalls jeweils um einzelne Gründe für oder gegen die Hauptthese, wie in einer einfachen Pro-Kontra-Liste. Das bedeutet insbesondere, dass sich an der Antwort auf eine einzige Frage noch nicht entscheidet, ob das OC-System eingeführt werden sollte oder nicht. Um zu überprüfen, welche Bedeutung die Antworten jeweils für diese Hauptfrage haben, empfiehlt es sich, jeweils den entsprechenden Abschnitt dieses Textes zu lesen.

Die Argumente wurden aus drei Quellen gewonnen: Erstens aus den Texten der Projektpartner (Bernard 2009a; Bernard 2009b; Bernard 2009c; Conrad 2009; IÖW et al. 2009), zweitens aus den Diskussionen in den Projekt-Workshops[1] und drittens aus einer Reihe von Interviews mit projekt-externen OC-Experten.[2] Die Argumentlandkarten werden im Internet unter www.argunet.org/debates/sokrates/organic-computing veröffentlicht.

Da bisher noch kein breiterer Diskurs zum Einsatz von OC oder verwandten Ansätzen entstanden ist, fehlt es bisher an direkten Kontrahenten der OC-Befürworter. Deswegen wurde versucht, rationale Gegenpositionen zu erschließen und so mögliche Brennpunkte einer zukünftigen Debatte vorwegzunehmen. 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

1 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.

2 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.

in den Diskussionen und Interviews mit den OC-Proponenten ausgetestet. Die Argumente, die diese Feuertaufe überstanden, wurden ebenfalls in die Debatte aufgenommen.

Zur Struktur dieses Textes: Nach einer kurzen Einführung in die Analyse- und Visualisierungsmethode wird zunächst das Hauptargument für den Einsatz von OC vorgestellt und erläutert. Dieses Argument besteht aus vier substantiellen Prämissen, in denen jeweils der Bedarf, die Eignung, die Verhältnismäßigkeit und die Erforderlichkeit des OC-Einsatzes behauptet wird. Daraus ergeben sich dann die vier ersten Fragen der Checkliste. Jedes der weiteren Pro-OC-Argumente kann als direkte oder indirekte Unterstützung für jeweils eine dieser Prämissen aufgefasst werden. Der Text folgt dieser Debattenstruktur: Die folgenden Abschnitte stellen die Diskussion von Bedarf, Eignung, Verhältnismäßigkeit und Erforderlichkeit der OC-Systeme vor. In jedem dieser Abschnitte werden weitere Fragen der Checkliste vorgestellt, die jeweils der Beantwortung der entsprechenden übergeordneten Frage dienen.

In jedem dieser Bereiche der Debatte kann kontrovers diskutiert werden. Die oben vorgestellte Methode der hypothetischen Erschließung von Gegenargumenten ergab aber nur für die Verhältnismäßigkeit von OC-Systemen eine kontroverse Debatte. Bei der Verhältnismäßigkeit geht es um die Frage, ob die Chancen eines OC-Systems es wert sind, die Risiken seines Einsatzes in Kauf zu nehmen. Dass die OC-Proponenten besonders an dieser Stelle möglichen Gegenargumenten zuvor kamen, bestätigte den Eindruck, dass es sich hier um den zentralen Schauplatz der Debatte handelt. Gerade bei einer breiteren, gemeinwohlorientierten (nicht rein ökonomischen) Diskussion mit OC-kritischen Teilnehmern sollte diese Frage zunächst im Vordergrund stehen.

Worin besteht die logische Rekonstruktion und wie liest man Argumentlandkarten?

Zunächst eine knappe Einführung in die Rekonstruktionsmethode und die Form der Visualisierung: Argumente werden deduktiv schlüssig als Prämissen-Konklusion-Strukturen (begründende Sätze plus begründeter Satz) und mit den zwischen ihnen bestehenden dialektischen Beziehungen (Angriff, Unterstützung) rekonstruiert. Zwischen zwei Argumenten besteht eine *Unterstützungsbeziehung*, wenn ein Argument begründet, warum die Prämisse eines anderen Arguments wahr ist. Eine *Angriffsbeziehung* besteht, wenn ein Argument begründet, warum die Prämisse eines anderen Arguments falsch ist.

Eine Argumentlandkarte visualisiert diese Beziehungen. Sie enthält zwei Arten von Elementen: Einfache Sätze (z.B. zentrale Thesen) werden als *umrahmte weiße Kästchen* visualisiert, Argumente (die Sätze als Prämissen und Konklusionen enthalten) als *ausgefüllte Kästchen*. Um die Argumentlandkarte übersichtlich zu halten sind nicht alle Sätze, die in den Argumenten vorkommen, auch als Sätze in der Landkarte visualisiert, sondern nur Sätze mit besonderer Bedeutung in der Debatte.

Wenn ein Satz, der in der Argumentlandkarte visualisiert wurde, zugleich in einem Argument als Prämisse vorkommt, so wird dies mit einem *grünen Pfeil* dargestellt, der von dem Satz auf das Argument zeigt. Wenn die Verneinung eines solchen Satzes als Prämisse in einem Argument vorkommt, so wird dies mit einem *roten Pfeil* visualisiert. Ebenso werden Konklusion-Prämissen-Beziehungen zwischen Argumenten dargestellt: Wenn ein Argument ein anderes unterstützt, so wird dies durch einen *grünen Pfeil* visualisiert, wenn es ein anderes Argument angreift, durch einen *roten Pfeil*.

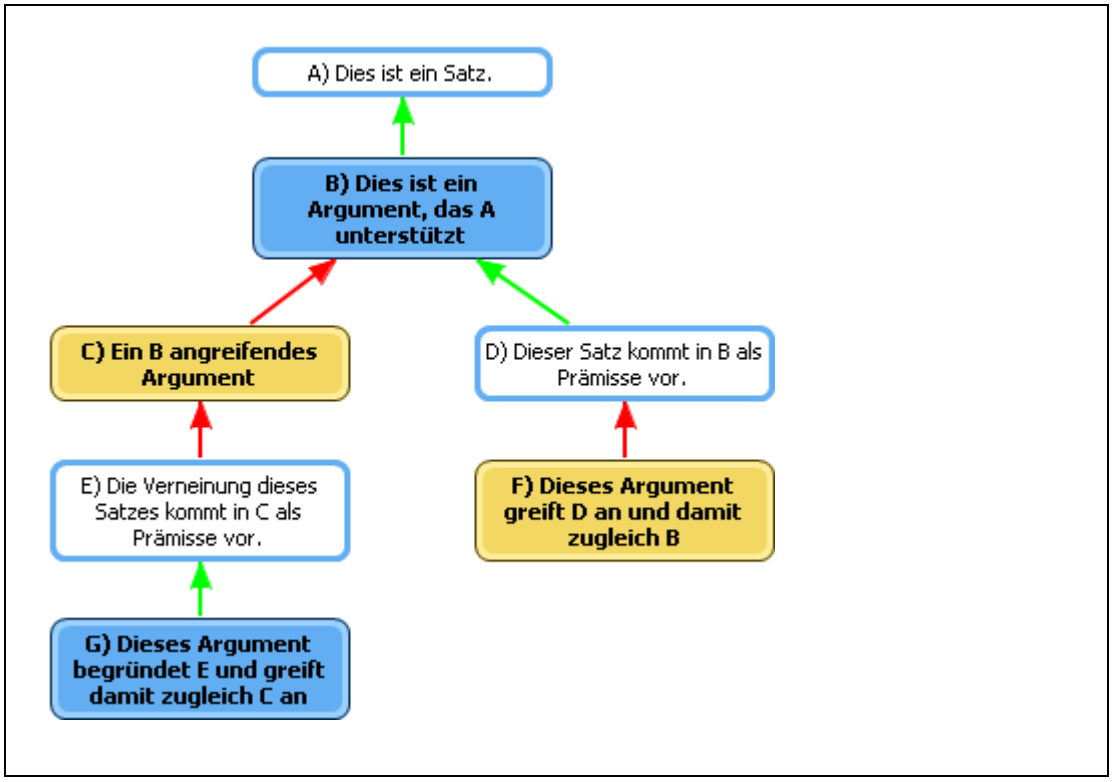

Abbildung i: Argumentlandkarte: Demonstration der Elemente und Beziehungen in einer Argumentlandkarte

Wichtige Vorbemerkungen: Neutralität, Offenheit und Unvollständigkeit jeder Rekonstruktion

Die Rekonstruktion selbst ist nicht wertend und kann niemals abschließend oder vollständig sein: Sie entscheidet nicht darüber, wer recht hat oder wer das letzte Wort in einer Debatte hat.

Erstens ist die Rekonstruktion nicht wertend: Aus ihr selbst folgen direkt zunächst nur Wenn-Dann-Aussagen: *Wenn* bestimmte Aussagen wahr sind, *dann* müssen notwendigerweise auch bestimmte andere Aussagen in der Debatte wahr sein. Welche Aussagen wahr sind geht aus der Argumentlandkarte selbst nicht hervor, sie ist deswegen neutral und offen für unterschiedliche Evaluationen (je nachdem welche Aussagen man für wahr, falsch oder ungesichert hält). Anders gesagt: Aus der Argumentlandkarte geht hervor, welche Fragen beantwortet werden müssen, um sich in der Debatte zu verorten und welche Konsequenzen die Antworten auf diese Fragen haben. Aus diesem Grund werden die Ergebnisse dieser Analyse in einem Fragenkatalog und nicht in einem Thesenkatalog zusammengefasst.

Zweitens ist die Rekonstruktion niemals abschließend oder vollständig: Es gibt immer Prämissen, die selbst unbegründet oder unangegriffen bleiben müssen, aber durchaus begründet oder angegriffen werden könnten.

Beide Eigenschaften führen dazu, dass eine These, die von vielen Argumenten unterstützt wird, deswegen noch lange nicht wahr und eine These, die von vielen Argumenten angegriffen wird, noch lange nicht falsch sein muss. Dasselbe gilt für Argumente: Ein Angriff auf ein Argument bedeutet noch nicht, dass dieses Argument entkräftet ist. Es kann z.B. sein, dass das angreifende Argument selbst wieder aus der Evaluationsperspektive haarsträubende Prämissen enthält, die sich leicht durch Ergänzung weiterer Argumente kritisieren lassen.

Dieser Kommentar geht über eine reine Beschreibung der Rekonstruktion hinaus und versucht bei der Evaluation der Debatte behilflich zu sein, ohne dabei Partei zu ergreifen. Der Kommentar setzt also keine spezifische Evaluationsperspektive voraus (welche Sätze sind wahr, welche falsch?), macht aber durchaus auf Schwächen und Stärken in der Argumentation aufmerksam.

2. Das Hauptargument für den Einsatz von OC

Die Hauptfrage: Sollte im Anwendungsfall x ein OC-System eingesetzt werden?

Im Laufe des Projekts trat immer deutlicher zutage, dass viele argumentativ relevante Eigenschaften von OC-Systemen anwendungsabhängig sind. Dies zeigte sich insbesondere in der Diskussion um die Risiken von OC. Damit entstand ein Problem: Einerseits sollten in der Rekonstruktion nur allgemeine Aussagen über Organic-Computing gemacht und nicht über spezifische Anwendungsszenarien (z.B. Ampelsysteme) geredet werden. Andererseits galten die interessantesten Ergebnisse weder generell für alle Anwendungen von Organic Computing noch für eine einzige, abgrenzbare Untergruppe von Anwendungen. Es erschien deswegen sinnvoll einerseits die Anwendungsvielfalt, soweit sie relevant ist, in der Rekonstruktion zu berücksichtigen, andererseits dennoch so weit es geht von der konkreten Anwendung zu abstrahieren, um möglichst allgemeingültige Erkenntnisse zu gewinnen.

Eine Möglichkeit wäre gewesen, die Diskussion zu vervielfachen und jeweils für mehrere charakteristische Gruppen von Anwendungsfällen anzupassen. Diese Herangehensweise erwies sich aber letzten Endes als zu umständlich und redundant, zumal sich bald ein sehr viel eleganterer Ausweg anbot. Statt ins Zentrum der Debatte eine generelle Aussage über alle OC-Systeme zu stellen (z.B.:"OC-Systeme sollten generell überall dort eingesetzt werden, wo Komplexität bewältigt werden muss") oder eine Aussage, die nur spezielle Anwendungsfälle betrifft (z.B.: "OC-Systeme sollten dazu genutzt werden, Computerchips zu optimieren") war es mithilfe eines Platzhalters möglich, einen Zwischenweg zu eröffnen. Die Hauptthese lautet deswegen: "Im Anwendungsfall x sollte ein OC-System eingesetzt werden."

Dadurch wird es nun möglich, die Argumente, die nur für unterschiedliche Gruppen von Anwendungsfällen gelten, dennoch in einer einzigen Argumentlandkarte zusammenzufügen, ohne damit Teilnehmern unplausible Behauptungen unterstellen zu müssen. Generelle Aussagen wie "OC-Systeme haben generell die Eigenschaft F" können deswegen an vielen Stellen vermieden werden. Es ergibt sich damit vielmehr ein Argumentationsschema, das wie eine Checkliste genutzt werden kann, um für jeden Anwendungsfall zu überprüfen, welche Gründe relevant sind und welche nicht. Es wird also nicht behauptet, dass es einen bestimmten Anwendungsfall x gibt, der wirklich alle Eigenschaften besitzt, die ihm in den einzelnen Argumenten zugesprochen werden. Je nachdem über welchen Anwendungsfall man diskutiert werden vielmehr unterschiedliche Argumente "aktiviert" und andere "deaktiviert",

je nachdem welche Beschreibung auf diesen Anwendungsfall zutrifft. Durch diese Schematisierung wird es möglich, die Gesamtdebatte um Organic Computing zu erfassen, ohne den Teilnehmern unplausible Generalisierungen unterstellen zu müssen.

Das Schema des Hauptarguments: Instrumentelle Handlungsrationalität

Damit steht nun die Konklusion des Hauptarguments fest: Es wird für einen einzelnen (aber nicht näher bestimmten) Anwendungsfall der Einsatz eines OC-Systems gefordert. Es handelt sich damit bei der Hauptthese um eine normative Aussage, um eine Handlungsaufforderung. Es gibt unterschiedliche Arten, eine solche Handlungsaufforderung zu begründen. Sowohl im Alltag als auch in der Politik ist die instrumentelle Begründung sicherlich am weitesten verbreitet (in speziellen Bereichen wie z.B. der Ökonomie überwiegen andere Begründungsarten). Diese Begründungsart lässt sich zunächst so formulieren:

a) Die Maßnahme M sollte ergriffen werden, weil b) m ein Mittel ist um z zu erreichen und c) Bedarf nach z besteht.

Von dieser Begründungsart soll auch hier ausgegangen werden, weil sie der Argumentationsweise der OC-Proponenten am besten zu entsprechen scheint. Um das Schema verwenden zu können muss zunächst der Zweck von OC-Systemen zumindest grob umrissen werden (später wird er dann ausführlicher begründet). Das ist nicht schwierig, weil hier von allen OC-Proponenten immer wieder derselbe Zweck genannt wird: Wir müssen in vielen Bereichen lernen besser mit der Komplexität technisch geregelter Systeme umzugehen. Dies scheinen alle Anwendungsfälle gemeinsam zu haben: Überall wo der Einsatz von OC-Systemen in Erwägung gezogen wird, besteht Bedarf danach, Komplexität zu bewältigen.

Da der Begriff der Komplexität so zentral in dieser Debatte ist, sollte er möglichst exakt definiert sein. Nach Rücksprachen mit den OC-Experten legen wir der Rekonstruktion folgende Definition zugrunde: Die Komplexität eines Systems bestimmt sich danach, aus wie vielen Komponenten es besteht und wie viele Abhängigkeiten zwischen diesen Komponenten bestehen. Alternativ kann die Komplexität eines Programms auch anhand der minimalen Anzahl von einfachen Rechenschritten bestimmt werden, mit der dieses Programm implementiert werden kann. (Mainzer 2007; Mainzer 2008) Diese zweite Definition ist aber in der folgenden Diskussion nicht argumentativ relevant. (Mainzer 2007; Mainzer 2008)

Zur Komplexitätsbewältigung können so unterschiedliche Dinge wie der Umgang mit den Grenzen traditioneller Entwicklungsmethoden, die Optimierung bisher suboptimaler Ergebnisse, die Reduzierung oder Kontrolle negativer Emergenz oder die Nutzung positiver Emergenz gezählt werden. Dieser Oberbegriff scheint deswegen sinnvoll, um das Hauptargument anwendungsneutral zu formulieren. Damit lässt sich nun das einfache Schema der instrumentellen Begründung ausfüllen:

a) Im Anwendungsfall x sollte ein OC-System eingeführt werden, weil b) OC-Systeme in der Lage sind Komplexität zu bewältigen und c) im Anwendungsfall x Bedarf nach Komplexitätsbewältigung herrscht.

Hierbei handelt es sich allerdings keinesfalls um ein logisch zwingendes Argument, d.h. auch wenn die Prämissen b) und c) wahr sind, muss a) noch lange nicht wahr sein. Es gibt eine Vielzahl typischer Einwände, die gegen einen derartigen Schluss sprechen. Erst wenn man folgende Prämisse d) einführt wird der Schluss logisch zwingend:

d) Wenn m ein Mittel für z ist und z wünschenswert ist, dann ist es zwingend so, dass m getan werden sollte.

Diese Prämisse macht die einfache instrumentelle Begründung zwar zu einem logisch zwingenden Schluss. Dafür ist diese Prämisse in vielen Fällen aber offensichtlich falsch, z.B. in Fällen, in denen es mehrere Mittel gibt, um denselben Zweck zu erreichen und m in dieser Gruppe verfügbarer *Alternativen* das ungeeignetste Mittel ist. M wäre in diesem Fall nicht *erforderlich*, um den Zweck zu erreichen. Diese Prämisse ist außerdem in den Fällen falsch, in denen m derart gravierende *Nebenwirkungen* hat, dass m angesichts dieser Risiken *unverhältnismäßig* wäre. Um diese Kritikmöglichkeiten transparent zu machen und um das verwendete Schlussprinzip (die ergänzte generelle Prämisse) unangreifbarer zu machen bietet sich deswegen folgende explizierende Erweiterung an, für deren Schlussprinzip sich nur schwer Gegenbeispiele konstruieren lassen:

Argument1: Begründung einer Maßnahme mithilfe des Schlussmusters der instrumentellen Handlungsrationalität

1) Bedarf: In der Situation S besteht Bedarf nach x, d.h.: In S ist x nicht der Fall und in S sollte x der Fall sein.
2) Eignung: y ist geeignet, um x in S herzustellen.
3) Verhältnismäßigkeit: x ist es wert die Risiken (mögliche, wahrscheinliche, sichere negative Folgen) des Einsatzes von y in S in Kauf zu nehmen
4) Erforderlichkeit: Es gibt keine alternativen Methoden x in S herzustellen, die besser geeignet oder verhältnismäßiger wären als y.
5) Schlussprinzip der instrumentellen Handlungsrationalität: Wenn Bedarf nach x besteht und y ein geeignetes, verhältnismäßiges und erforderliches Mittel für x ist, dann sollte y herbeigeführt werden.
6) y sollte herbeigeführt werden.

Daraus ergibt sich nun direkt das Hauptargument für die Einführung eines OC-Systems, das die gesamte OC-Debatte und damit auch die folgende Darstellung dieser Debatte strukturiert:

Argument 2: Das Hauptargument pro OC: OC geeignetes, verhältnismäßiges und erforderliches Mittel

1) Bedarf: Im Anwendungsbereich x besteht Bedarf nach Komplexitätsbewältigung, d.h. erstens ist die Komplexität in x bisher wenig oder gar nicht bewältigt und zweitens ist ihre Bewältigung wünschenswert.
2) Eignung: OC Systeme sind hervorragend geeignet, um die Komplexität im Anwendungsfall x zu bewältigen.
3) Verhältnismäßigkeit: Die Bewältigung der Komplexität in x ist es wert, dafür die Risiken, die durch den Einsatz eines OC-Systems entstehen, in Kauf zu nehmen.
4) Erforderlichkeit: Es gibt für die Komplexitätsbewältigung in x nicht andere technische Lösungen, die besser geeignet oder risikoärmer sind.

5) Schlussprinzip der instrumentellen Handlungsrationalität: Wenn Bedarf nach x besteht und y ein geeignetes, verhältnismäßiges und erforderliches Mittel für x ist, dann sollte y herbeigeführt werden.

6) Im Anwendungsfall x sollte ein OC-System eingesetzt werden.

Wichtig zu beachten ist erstens, dass dieses Argument voller normativer und evaluativer Behauptungen steckt, die sich nicht direkt aus den wissenschaftlichen Fakten ergeben: In der Bedarfsprämisse wird nicht nur behauptet, dass ein bestimmter Zustand derzeit nicht besteht, sondern auch, dass er hergestellt werden sollte. In der Verhältnismäßigkeitsprämisse wird nicht nur das Wissen über mögliche, wahrscheinliche oder sichere Konsequenzen von OC-Systemen vorausgesetzt, sondern diese negativen Konsequenzen werden auch gegen positive Konsequenzen (Deckung des Bedarfs) abgewogen und also bewertet (gewichten heißt hier ja nichts anderes als präferieren). Weil in der Erforderlichkeitsprämisse auf die Eignung und Verhältnismäßigkeit der verfügbaren Alternativen Bezug genommen wird, stecken auch in dieser Prämisse normative und evaluative Aussagen.

Normative und evaluative Aussagen sind gerade in Debatten, in denen es um das Gemeinwohl geht, von besonderer Bedeutung, weil nicht in jedem Fall unter allen Betroffenen Konsens darüber besteht, was dem Gemeinwohl in welchem Maße dient und weil bei der Bestimmung des Gemeinwohls die Präferenzen der Betroffenen berücksichtigt werden sollten. Diese Fragen müssen deswegen häufig öffentlich diskutiert werden, Konsens kann nicht immer vorausgesetzt, sondern sollte teilweise erst hergestellt werden. Die Argumentrekonstruktion führt dazu, dass die normativen und evaluativen Bestandteile der Argumentation deutlich zutage treten und besser von den rein deskriptiven Fragestellungen getrennt werden können.

Wichtig ist außerdem zweitens, dass eine Kritik an diesem Hauptargument noch keiner Widerlegung der Hauptthese gleichkommt: Mit dem Hauptargument wird nur behauptet, dass die Wahrheit der Hauptthese aus der Wahrheit der Prämissen des Hauptarguments logisch zwingend folgt. Es wird nicht behauptet, dass aus der Falschheit einer der Prämissen auch zwingend die Falschheit der Hauptthese folgt. Akzeptiert man einen Angriff auf das Hauptargument, dann ist für die Hauptthese damit nur gezeigt, dass sie nicht allein aufgrund des Hauptarguments wahr sein kann, sondern dass sie, wenn überhaupt, dann aus anderen Gründen wahr sein muss. Will man die Hauptthese direkt angreifen, dann muss man ein Gegenargument formulieren, aus dessen Prämissen direkt die Falschheit der Hauptthese folgt. Ein solches Argument findet sich im Abschnitt zur Verhältnismäßigkeit.

Aus dem Hauptargument ergeben sich die vier Hauptfragen der Checkliste, die jeweils die Wahrheit der vier Prämissen überprüfen:

Frage 1 (Bedarf): Besteht im Anwendungsbereich x Bedarf nach Komplexitätsbewältigung?

Frage 2 (Eignung): Ist das OC-System im Anwendungsbereich x zur Komplexitätsbewältigung geeignet?

Frage 3 (Verhältnismäßigkeit): Ist die Komplexitätsbewältigung in x es wert, dafür die Risiken des OC-Systems in Kauf zu nehmen?

Frage 4 (Erforderlichkeit): Gibt es andere verfügbare Alternativen in x, die zur Komplexitätsbewältigung besser geeignet oder verhältnismäßiger wären?

In den weiteren Abschnitten werden nun jeweils die Argumente für eine der substantiellen Prämissen des Hauptarguments vorgestellt und analysiert. Der Schwerpunkt liegt dabei auf der Verhältnismäßigkeitsbehauptung, weil sich hier bereits eine kontroverse Debatte abzeichnet, die zumindest in ihren Grundzügen bereits vorweggenommen werden kann.

Frage 1 (Bedarf): Besteht im Anwendungsbereich x Bedarf nach Komplexitätsbewältigung?

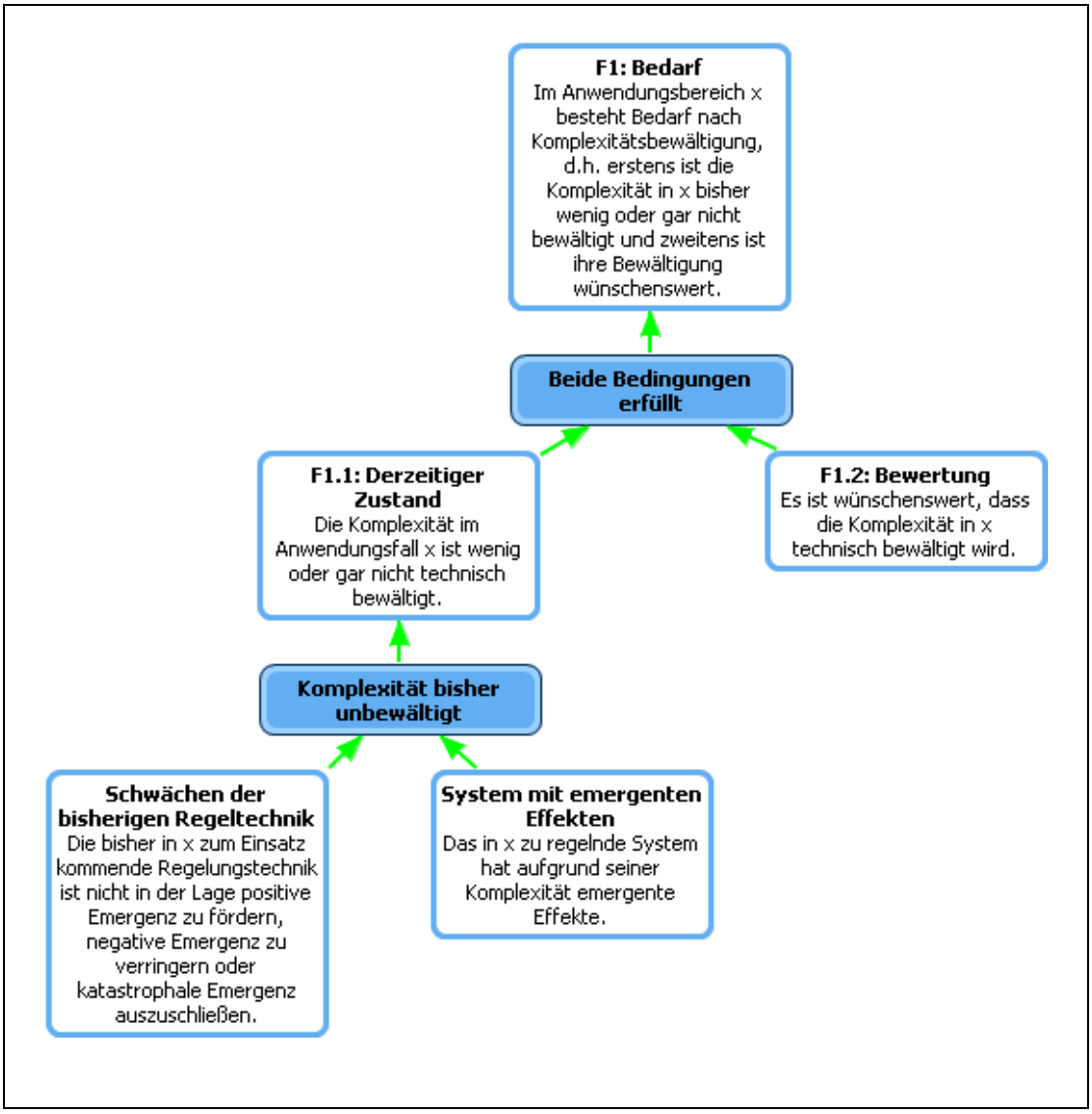

Abbildung ii: Argumentlandkarte: Begründung des Bedarfs

Wie schon gesagt besteht die Bedarfsbehauptung aus zwei Teilen: Einer deskriptiven Bestandsaufnahme ("Die Komplexität im Anwendungsfall x ist wenig oder gar nicht technisch bewältigt.") und einer bewertenden Aussage ("Es ist wünschenswert, dass die Komplexität in x technisch bewältigt wird."). Diese beiden Bestandteile müssen unterschiedlich begrün-

det werden, sie werden in der Rekonstruktion deswegen zunächst voneinander getrennt, so dass sie als einzelne Thesen in der Argumentlandkarte sichtbar werden.

In den Interviews, Workshops und den zugrundegelegten Texten wird die positive Bewertung technischer Komplexitätsbewältigung als selbstverständlich vorausgesetzt. Dies ist auch in den allermeisten Anwendungsfällen plausibel. Dennoch wird diese Bewertung nicht in jedem Fall für alle Betroffenen selbstverständlich sein. So kann man z.B. erwarten, dass manchem die Visionen des Ambient- oder Ubiquitous-Computing, in denen Haushaltsgeräte ständig miteinander kommunizieren, ihren Besitzer über Überwachungskameras verfolgen und der Kühlschrank die Einkäufe überprüft, eher als Dystopien, denn als Utopien erscheinen werden, gleichgültig wie gut ein derart selbstorganisierender Haushalt Komplexität bewältigt.

Es kann also nicht ausgeschlossen werden, dass in manchen Anwendungsfällen auch diese wertende Prämisse zum Ausgangspunkt einer kontroversen Diskussion werden könnte. Allein der Verweis auf technisch unbewältigte Komplexität reicht auf jeden Fall noch nicht aus, um den Bedarf nach technischer Komplexitätsbewältigung zu begründen. Zusätzlich muss die Bewältigung dieser Komplexität positiv bewertet werden.

In den innerhalb des Projekts untersuchten Fallbeispielen (Ampel, Kamerasysteme, Logistik) ist die technische Komplexitätsbewältigung aber als eindeutig positiv zu bewerten und insofern muss nur begründet werden, dass die Komplexität bisher nur wenig oder gar nicht technisch bewältigt wurde. Alle diese Fälle haben miteinander gemeinsam, dass es bereits herkömmliche technische Lösungen gibt, die die durch Komplexität bestehenden Probleme aber nur unzureichend lösen. Der Bedarf lässt sich deswegen mit den Mängeln der herkömmlichen Technik begründen.

Alle befragten OC-Experten (z.B. Müller-Schloer, Herkersdorf, Hähner) verweisen hier darauf, dass bisherige Techniken nicht in der Lage sind emergente Effekte systematisch zu beherrschen und zu nutzen. Negative Emergenz wird nicht reduziert und ausgeschlossen, so dass Ineffizienzen oder sogar gravierende negative Folgen auftreten (Müller-Schloer nennt als Beispiele Stromausfall im Stromnetz, Stau auf der Autobahn usw.). Positive Emergenz bleibt ungenutzt, so dass suboptimale Lösungen gefunden werden (schleppender Autoverkehr, hohe Lagerkosten in der Logistik, beschränkte Leistung von Computerchips).

Emergente Effekte innerhalb eines Systems sind Effekte, die sich nicht durch die Einzelanalyse der Komponenten dieses Systems bereits erkennen lassen, sondern erst aus dem komplexen Zusammenspiel dieser Komponenten heraus entstehen. Emergente Effekte sind deswegen nur mithilfe von Simulationen des Gesamtsystems ableitbar und treten ansonsten überraschend und unvorhersehbar auf (Bedau 1997).

Nicht jedes komplexe System weist notwendigerweise emergente Effekte auf. Nicht für alle komplexen Systeme lässt sich also auf diese Weise der Bedarf für technische Komplexitätsbewältigung begründen. Das ist für die Pro-OC-Argumentation aber kein Problem, solange sie keine generellen Aussagen über komplexe Systeme trifft, sondern sich auf die Anwendungsfälle beschränkt, in denen mit der Komplexität auch emergente Phänomene einhergehen (auf diese Einschränkung wurde auf dem Argumentlandkarten-Workshop hingewiesen). Schon hier bewährt sich deswegen die schematische Formulierung der Hauptthese, die generelle Aussagen vermeidet.

Um den Bedarf in einem Anwendungsgebiet zu überprüfen müssen also zwei Fragen beantwortet werden:

Frage 1.1 (Komplexität unbewältigt): **Ist die Komplexität im Anwendungsbereich bisher wenig oder gar nicht technisch bewältigt?**

Frage 1.2 (Komplexitätsbewältigung wünschenswert): **Sollte die Komplexität im Anwendungsbereich überhaupt technisch bewältigt werden?**

Frage 2 (Eignung): Ist das OC-System im Anwendungsbereich x zur Komplexitätsbewältigung geeignet?

Warum sind OC-Systeme besonders zur Komplexitätsbewältigung geeignet? OC-Experten verweisen zunächst auf die Entstehungsgeschichte von OC (z.B. Müller-Schloer, Herkersdorf): Die Grundidee von OC-Systemen wurde von natürlichen, selbstorganisierenden Systemen, wie z.B. Ameisenhaufen, abgeschaut. Und weil OC-Systeme in allen für die Komplexitätsbewältigung relevanten Eigenschaften solchen natürlichen Systemen ähneln, ist es auch plausibel zu erwarten, dass sie ähnlich gut zur Komplexitätsbewältigung geeignet sind.

Argument3: Von der Natur abgeschaut

1) In der Natur gibt es viele selbstorganisierende Systeme, die in der Lage sind komplexe Aufgaben hervorragend zu bewältigen.
2) Alle Eigenschaften dieser natürlichen Systeme, die sie zur Komplexitätsbewältigung befähigen, sind ebenfalls Eigenschaften von OC-Systemen.
3) Wenn x alle Eigenschaften besitzt, die y zu F befähigen, dann ist auch x zu F in der Lage.
4) OC Systeme sind hervorragend geeignet, um die Komplexität im Anwendungsfall x zu bewältigen.

Mit dieser Analogie ist allerdings noch nicht gesagt, welche Eigenschaften es genau sind, die OC-Systeme zur Komplexitätsbewältigung befähigen.

Deswegen ist ein weiteres Argument sinnvoll, in dem gezeigt wird, dass Organic-Computing-Systeme alle Anforderungen erfüllen, die zur Komplexitätsbewältigung nötig (und zusammengenommen hinreichend dafür) sind. Die OC-Proponenten nennen hier unterschiedliche Arten von Anforderungen für Systeme zur Steuerung komplexer Systeme: Erstens sollen die Systeme sehr stabil, erweiterbar, lernfähig und skalierbar sein (z.B. IÖW et al. 2009 11ff.; Bernard 2009a), zweitens sollen sie emergente Effekte beherrsch- und nutzbar machen (z.B. Interview Müller-Schloer) und drittens soll ihre Entwicklung zeit- und kosteneffizient sein (z.B. Interview Herkersdorf, Argumentations-Workshop).

Aus dieser Liste von Anforderungen lassen sich die entscheidenden Fragen gewinnen, die beantwortet werden müssen, um zu entscheiden, ob OC zur Komplexitätsbewältigung geeignet ist:

Frage 2.1 (Anforderungen I): **Sind OC-Systeme im Anwendungsbereich x stabil, erweiterbar, lernfähig und skalierbar?**

Frage 2.2 (Anforderungen II): **Machen OC-Systeme im Anwendungsbereich x emergente Effekte beherrschbar und nutzbar?**

Frage 2.3 (Anforderungen III): **Lassen sich mit der Entwicklung von OC-Systemen im Anwendungsbereich x langfristig Zeit und Kosten einsparen?**

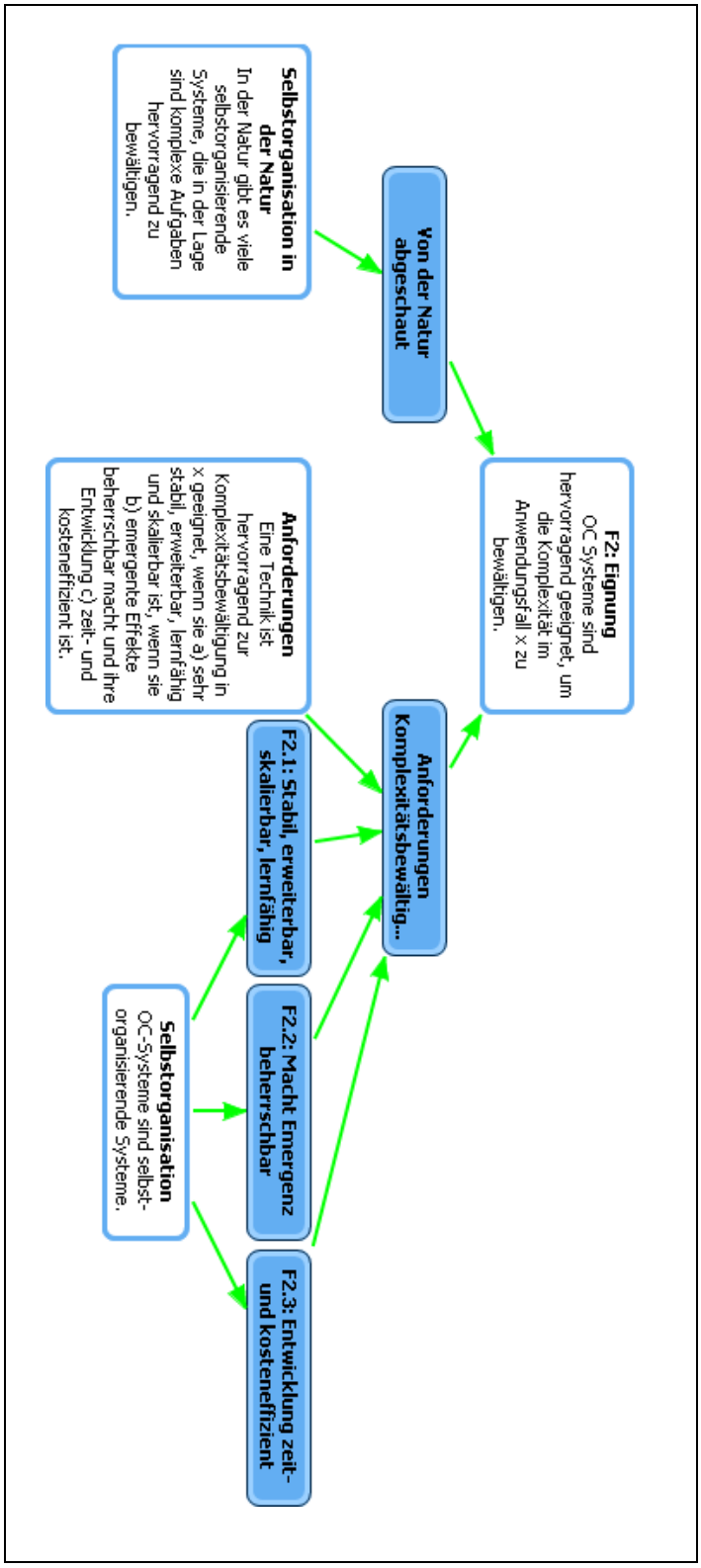

Abbildung iii: Argumentlandkarte: Begründung der Eignung

Die positiven Antworten auf diese Fragen, werden von den OC-Proponenten jeweils auf ähnliche Weise mit drei Argumenten begründet. Alle drei Argumente beziehen sich auf dieselbe grundlegende Eigenschaft von OC-Systemen: OC-Systeme sind selbstorganisierend. Und mit dieser Selbstorganisation gehen laut OC-Proponenten alle angeforderten Eigenschaften einher (siehe z.B. IÖW et al. 2009, 11 ff.).

Argument 4: Stabil, erweiterbar, skalierbar, lernfähig

1) OC-Systeme sind selbst-organisierende Systeme.
2) Selbstorganisierende Systeme sind selbstheilend.
3) Selbst-heilende Systeme laufen sehr stabil.
4) **OC-Systeme laufen sehr stabil.**
5) Selbstorganisierende Systeme sind sehr gut erweiterbar und skalierbar.
6) **OC-Systeme sind sehr gut erweiterbar und skalierbar.**
7) Selbstorganisierende Systeme sind selbst-optimierend.
8) Selbst-optimierende Systeme sind sehr lernfähig.
9) **OC-Systeme sind sehr lernfähig.**
10) **OC-Systeme sind stabil, erweiterbar, skalierbar und lernfähig.**

Argument 5: Macht Emergenz beherrschbar

- Emergente Effekte beherrschbar zu machen heißt, in der Lage zu sein positive Emergenz zu nutzen, negative Emergenz zu verringern und katastrophale Emergenz zu verhindern.
- OC-Systeme sind selbst-organisierende Systeme.
- Selbst-organisierende Systeme sind per se Systeme, die positive Emergenz nutzen und können derart entwickelt werden, dass sie negative Emergenz verringern und katastrophale Emergenz verhindern.
- **OC-Systeme machen emergente Effekte beherrschbar.**

Argument 6: Entwicklung zeit- und kosteneffizient

1) OC-Systeme sind selbst-organisierende Systeme.
2) Selbst-organisierende Systeme können sich entweder während der Entwicklungs- oder während der Laufzeit selbst weiterentwickeln.
3) Systeme, die sich selbst weiterentwickeln können, sind mit weniger Zeit- und Kostenaufwand zu entwickeln, als herkömmliche komplexe Systeme.
4) Es gibt keine andersartigen neuen Techniken für komplexe Systeme, deren Entwicklung noch weniger aufwändig wäre.
5) Wenn die Entwicklung einer neuen Technik im Vergleich zur Entwicklung herkömmlicher Techniken Zeit und Kosten spart und es auch keine alternativen Techniken gibt, die noch sparsamer sind, dann ist die Entwicklung der neuen Technik zeit- und kosteneffizient.

6) Die Entwicklung von OC-Systemen ist zeit- und kosteneffizient.

Wie man sieht gehen in diese Argumentation keine eindeutig evaluativen oder normativen Aussagen ein. Ob OC-Systeme wirklich in der Lage sind Komplexität zu bewältigen ist eine Fachfrage, über die sich Außenstehende zwar einen Einblick verschaffen können und sollten, die letzten Endes aber zwischen Experten entschieden werden muss. Nach Auskunft der OC-Proponenten findet eine solche Diskussion bisher allenfalls mit Verteidigern der traditionellen Regelungstechnik statt (Ergebnis aus dem Argumentations-Workshop). Diese Gegner sprechen Organic-Computing aber lediglich ab, sich wesentlich von herkömmlichen Ansätzen zu unterscheiden. Das ist hier aber irrelevant: Es kommt an dieser Stelle in der Debatte nur darauf an, ob OC zur Komplexitätsbewältigung geeignet ist, gleichgültig, ob OC nun grundlegend neu ist oder nicht.

Weil es sich hier um Fachfragen handelt und es anscheinend keine kontroversen Fachdebatten um die Eignung von OC zur Komplexitätsbewältigung gibt (OC-Experten verwiesen auf dem Argumentations-Workshop auch darauf, dass es sich um ein noch relativ junges Feld handelt, das noch nicht als echte Konkurrenz wahrgenommen wird und deswegen wenig kritisiert wird), war es anders als im folgenden Abschnitt hier nicht möglich, plausible Gegenargumente zu erschließen oder zu konstruieren.

Frage 3 (Verhältnismäßigkeit): Ist die Komplexitätsbewältigung in x es wert, dafür die Risiken des OC-Systems in Kauf zu nehmen?

Mit dieser Frage beginnt nun die Debatte um die Risiken von Organic-Computing. Ihren Ausgangspunkt nimmt diese Debatte von der Verhältnismäßigkeitsprämisse im Hauptargument, mit der behauptet wird, dass die Risiken eines OC-Einsatzes in x nicht so gravierend sind, dass die Vermeidung dieser Risiken wichtiger wäre, als die Bewältigung der Komplexität in x.

Was muss gegeben sein, damit sich diese Verhältnismäßigkeitsbehauptung begründen lässt? Im Zentrum der Debatte stehen sechs Eigenschaften von Anwendungsszenarien, die für die Beurteilung der Verhältnismäßigkeit eine zentrale Rolle spielen. Für jedes Anwendungsszenario müssen deswegen folgende sechs Fragen beantwortet werden:

Frage 3.1 (Kein negativer Risikovergleich): Sind die Risiken, die durch den Einsatz des OC-Systems entstehen mit den zuvor bestehenden Risiken vergleichbar oder sogar geringer?

Frage 3.2 (Ausreichende Kontrolle): Lassen sich die Risiken, die durch den Einsatz des OC-Systems entstehen derart durch Kontrollsysteme reduzieren, dass die Verhinderung des Restrisikos es nicht wert ist dafür die Komplexitätsbewältigung in x aufzugeben?

Frage 3.3 (Sicheres Wissen): Ist beim Einsatz eines OC-Systems die Unsicherheit darüber, ob, wann oder mit welcher Wahrscheinlichkeit negative Systemzustände im geregelten System auftreten gering?

Frage 3.4 (Worst case nicht katastrophal): Wären die negativen Folgen auch im schlimmstmöglichen Fall nicht gravierend, inakzeptabel und katastrophal?

Frage 3.5 (Kein Vertrauensverlust): Ist das Steuerungs-Verhalten des OC-Systems in x für die Betroffenen nachvollziehbar und voraussehbar, so dass die Betroffenen dem System vertrauen?

Frage 3.6 (Undurchschaubarkeit akzeptabel): Ist es im Anwendungsfall x wichtiger die Komplexität zu bewältigen, als ein System einzusetzen, dessen Verhalten die Betroffenen durchschauen und voraussagen können?

Im folgenden wird gezeigt, wie sich jeweils die Antworten auf diese sechs Fragen auf die Debatte um die Verhältnismäßigkeit auswirken. Eine positive Antwort auf die ersten beiden Fragen ergibt jeweils ein unterstützendes Argument für die Verhältnismäßigkeitsbehauptung und also eine positive Antwort auf Frage 3. Negative Antworten auf die Fragen 3.3 und 3.4 ergeben zusammen ein angreifendes Argument auf diese Behauptung, also eine negative Antwort auf Frage 3 und einen direkten Angriff auf die Hauptthese und damit eine negative Antwort auf die Hauptfrage. Negative Antworten auf die Fragen 3.5 und 3.6 ergeben zusammen ebenfalls ein angreifendes Argument auf die Verhältnismäßigkeitsbehauptung, also eine negative Antwort auf Frage 3.

Im zweiten Teil dieses Abschnittes wird dann untersucht, wie diese Fragen miteinander zusammenhängen: Was bedeutet jeweils eine positive oder negative Antwort auf eine dieser Fragen für die Antworten auf die anderen Fragen? Es zeigt sich, dass eine positive Frage auf die Fragen 3.1 und 3.2 eine positive Antwort auf 3.3-3.5 (unter Annahme weiterer Prämissen) erzwingen. Eine negative Antwort auf eine der Fragen 3.3-3.5 erzwingt wiederum eine negative Antwort auf die Fragen 3.1 und 3.2. Im dritten Teil dieses Abschnittes wird dann auf die Diskussion um die Frage 3.3 (Sicheres Wissen) eingegangen. Im letzten Abschnitt wird gezeigt, wie sich aus charakteristischen Eigenschaften von Anwendungsszenarien jeweils bestimmte Antworten auf die Fragen 3.1, 3.2 und 3.3 ergeben. Diese indirekt abwägungsrelevanten Eigenschaften sollten für die Beurteilung der Verhältnismäßigkeit ebenfalls überprüft werden, so dass dem Fragenkatalog weitere Fragen hinzugefügt werden (Fragen 3.7-3.11).

Da hier nun zum ersten Mal Gegenargumente auftauchen, sei noch einmal darauf hingewiesen, dass diese Gegenargumente sich teilweise aus den Reaktionen der OC-Proponenten auf diese Einwände ergaben, teilweise aber auch neue Gegenargumente konstruiert wurden, die dann in der Diskussion mit den OC-Experten diskutiert wurden. Deswegen kann nicht der Anspruch auf Vollständigkeit erhoben werden. Eine zukünftige kontroverse Diskussion mit OC-Gegnern könnte weitere Einwände ergeben. Außerdem sei noch einmal darauf hingewiesen, dass die folgende Analyse erstens nicht beurteilt welche Argumente gut und welche schlecht sind, sondern nur darauf hinweist, welche Fragen beantwortet werden müssen, um die Güte der Argumente zu beurteilen. Zweitens werden keine allgemeinen Aussagen über OC-Systeme getroffen, sondern es wird lediglich darauf hingewiesen, welche Eigenschaften von OC-Systemen innerhalb spezifischer Anwendungsszenarien für die Verhältnismäßigkeit des Einsatzes problematisch sein könnten. Sollte sich erweisen, dass es wirklich solche Anwendungskontexte gibt, in denen die OC-Systeme diese Eigenschaften besitzen, heißt das noch nicht, dass damit auch die Verhältnismäßigkeit in allen anderen Anwendungsszenarien widerlegt ist.

Frage 3.1 (Kein negativer Risikovergleich): Sind die Risiken, die durch den Einsatz des OC-Systems entstehen mit den zuvor bestehenden Risiken vergleichbar oder sogar geringer?

Beantwortet man die Frage 3.1 positiv, dann ist es plausibel, dass die Einführung eines OC-Systems in x eine verhältnismäßige Maßnahme ist. Denn dann können zwar durch diese Maßnahme eventuell gegenüber dem Status Quo neue Risiken entstehen. Die möglichen negativen Konsequenzen des OC-Systems sind vielleicht andere, als die möglichen negativen Konsequenzen im Status Quo. Die Beschreibung der Risikolage ändert sich also. Was sich aber nicht ändert, ist die *Bewertung* oder *Gewichtung* der Risiken: Zusammengenommen sind die Risiken, die im neuen Zustand bestehen, nicht größer, als die Risiken, die im alten Zustand bestanden.

Solange dann die Komplexitätsbewältigung überhaupt wünschenswert ist, überwiegt dieser Nutzen die Risiken, gleichgültig wie gering der Nutzen ist. Denn in die Kosten-Nutzen-Abwägung sollten die Risiken des OC-Systems nur insoweit eingehen, insoweit sie schlimmer sind als im Status Quo (man kann hier also von Grenz-Risiko sprechen). Da behauptet wird, dass die Risiken nur genauso schlimm oder weniger schlimm als im Status Quo sind, gehen also überhaupt keine Risiken in die Abwägung ein.

Argument 7: Kein zusätzliches Risiko

1) Die Risiken beim Einsatz eines OC-Systems im Anwendungsfall x sind in ihrer Gesamtheit ähnlich groß wie oder kleiner als die Risiken, die bereits jetzt schon auch ohne das OC-System in x bestehen.
2) Der Zweck des OC-Systems in x ist die Komplexitätsbewältigung und dieser Zweck ist verfolgenswert.
3) Wenn eine Handlung die Risikolage vielleicht verändert, aber nicht verschlimmert und der Zweck dieser Handlung verfolgenswert ist, dann ist dieser Zweck es wert, die (möglicherweise neuen) Risiken in Kauf zu nehmen.
4) **Die Bewältigung der Komplexität in x ist es wert, dafür die Risiken, die durch den Einsatz eines OC-Systems entstehen, in Kauf zu nehmen.**

Auf die Bedeutung dieses Risikovergleichs und auf das darauf aufbauende Argument wurde insbesondere von Müller-Schloer im Laufe der zweiten Rekonstruktionsrunde aufmerksam gemacht.

Frage 3.2 (Ausreichende Kontrolle): Lassen sich die Risiken, die durch den Einsatz des OC-Systems entstehen derart durch Kontrollsysteme reduzieren, dass die Verhinderung des Restrisikos es nicht wert ist dafür die Komplexitätsbewältigung in x aufzugeben?

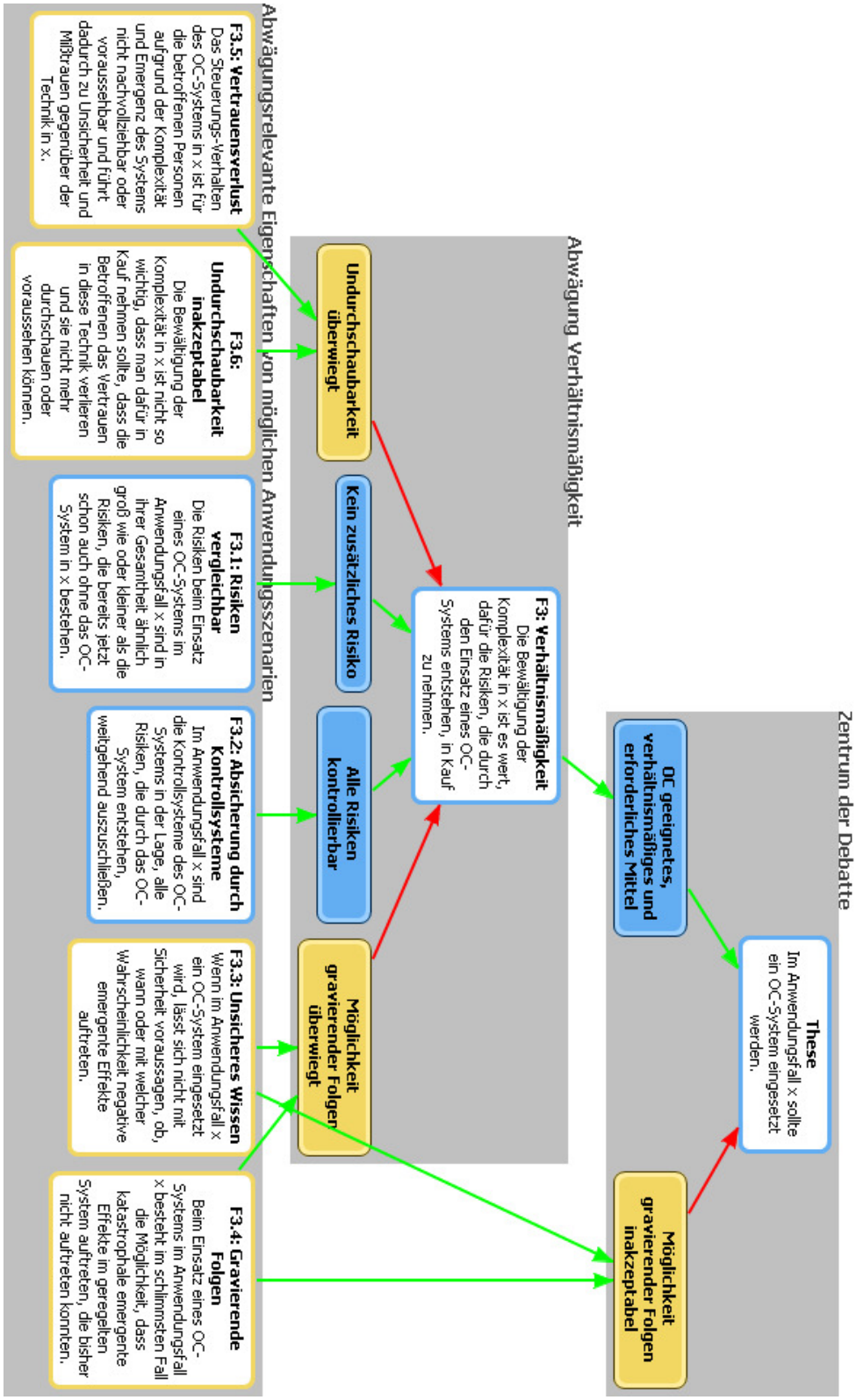

Abbildung iv: Argumentlandkarte: Diskussion um die Verhältnismäßigkeit, Ausschnitt 1
Erläuterungen zur Abb. falls notwendig (z.B. Quellen usw.), ggf. löschen.

Beantwortet man die Frage 3.2 positiv so ist es noch offensichtlicher, dass die Einführung eines OC-Systems in x eine verhältnismäßige Maßnahme ist, weil dann durch das Kontrollsystem gewährleistet wird, dass das OC-System weitgehend risikolos ist. Für eine Unterstützung der Verhältnismäßigkeitsbehauptung reicht es dann erneut aus, dass die Komplexitätsbewältigung überhaupt verfolgenswert ist (gleichgültig wie gering man den Nutzen der Bewältigung einschätzt). (Bernard 2009a)

Argument 8: Alle Risiken kontrollierbar

1) Im Anwendungsfall x sind die Kontrollsysteme des OC-Systems in der Lage, alle Risiken, die durch das OC-System entstehen, weitgehend auszuschließen.
2) Die Komplexitätsbewältigung ist es wert, dafür das verbleibende Restrisiko in Kauf zu nehmen.
3) **Die Bewältigung der Komplexität in x ist es wert, dafür die Risiken, die durch den Einsatz eines OC-Systems entstehen, in Kauf zu nehmen.**

Frage 3.3 (Sicheres Wissen): Ist beim Einsatz eines OC-Systems die Unsicherheit darüber, ob, wann oder mit welcher Wahrscheinlichkeit negative Systemzustände im geregelten System auftreten gering?

Frage 3.4 (Worst case nicht katastrophal): Wären die negativen Folgen auch im schlimmstmöglichen Fall nicht gravierend, inakzeptabel und katastrophal?

Beantwortet man die Fragen 3.3 und 3.4 negativ, dann lässt sich ein Gegenargument gegen die Verhältnismäßigkeitsbehauptung konstruieren. Denn da unbekannt ist, wie wahrscheinlich der schlimmstmögliche Fall ist und in diesem schlimmstmöglichen Fall gravierende negative Folgen auftreten können, sollte man lieber Vorsicht walten lassen.

Wenn man über keine Wahrscheinlichkeiten verfügt, lässt sich der Erwartungsnutzen nicht gegen die Erwartungskosten abwägen. Da aber katastrophale Folgen vollständig ausgeschlossen werden sollten, ist es rational für die Abwägung hypothetisch vom schlimmstmöglichen Fall ausgehen und die katastrophalen möglichen Folgen direkt mit dem Nutzen, der durch die Erfüllung des Zwecks entsteht, abzuwägen. Ist der Zweck der Maßnahme wichtiger, als die Verhinderung der katastrophalen Folgen? Das ist für die Komplexitätsbewältigung in vielen Fällen unplausibel. In diesen Fällen lässt sich gegen die Verhältnismäßigkeitsbehauptung argumentieren:

Argument 9: Möglichkeit gravierender Folgen überwiegt

1) Beim Einsatz eines OC-Systems im Anwendungsfall x besteht im schlimmsten Fall die Möglichkeit, dass katastrophale emergente Effekte im geregelten System auftreten, die bisher nicht auftreten konnten.
2) Wenn im Anwendungsfall x ein OC-System eingesetzt wird, lässt sich nicht mit Sicherheit voraussagen, ob, wann oder mit welcher Wahrscheinlichkeit negative emergente Effekte auftreten.
3) Die Komplexitätsbewältigung ist nicht wichtiger als die Verhinderung katastrophaler emergenter Effekte.

4) Wenn für ein Maßnahme zur Erreichung eines bestimmten Zwecks nicht bekannt ist, wie wahrscheinlich es ist, dass der schlimmste Fall eintritt und im schlimmsten Fall katastrophale Folgen auftreten können, die ohne diese Maßnahme nicht auftreten würden, dann ist die Maßnahme nur dann verhältnismäßig, wenn der Zweck wichtiger ist, als die Verhinderung dieser möglichen katastrophalen Folgen.

5) **Die Komplexitätsbewältigung in x ist es nicht wert, dafür die Risiken, die durch den Einsatz eines OC-Systems im Anwendungsfall x entstehen, in Kauf zu nehmen.**

Hat man aber einmal akzeptiert, dass man im Fall unsicheren Wissens über die Folgen einer Maßnahme lieber vom "worst case scenario" ausgehen sollte, dann liegt es nahe, aus der Möglichkeit, dass beim Einsatz eines OC-Systems in x katastrophale Folgen auftreten können, direkt darauf zu schließen, dass auf den Einsatz eines OC-Systems in x verzichtet werden sollte. Hier bietet es sich an, mit dem *Vorsorgeprinzip* zu argumentieren.

Das Vorsorgeprinzip ist ein Entscheidungsprinzip für Entscheidungen unter unsicherem Wissen. Es hat inzwischen insbesondere in der Umweltpolitik breite Anerkennung und Verbreitung gefunden[3] und wird z.B. verwendet, wenn es darum geht für den Klimaschutz oder gegen die Einführung grüner Gentechnik zu argumentieren. 1992 verpflichteten sich die UN-Mitgliedstaaten, das Vorsorgeprinzip zur breiten Anwendung kommen zu lassen (United Nations 1992, Principle 15). In seiner einfachsten Fassung lautet das Vorsorgeprinzip: Wenn Du weißt, dass eine Handlung inakzeptable Folgen haben könnte, aber nicht weißt, wie wahrscheinlich es ist, dass diese Folgen auftreten, dann unterlasse diese Handlung lieber. Oder in den Worten der UN, in der Anwendung auf Umweltschäden: „Where there are threats of serious or irreversible damage, lack of full scientific certainty shall not be used as a reason for postponing cost-effective measures to prevent environmental degradation.“ (United Nations 1992, Principle 15)

In dieser einfachen Fassung lassen sich aber Gegenbeispiele konstruieren, in denen eine Anwendung dieses Entscheidungsprinzips irrational wäre. Deswegen sollten die Anwendungsbedingungen für dieses Prinzip enger gefasst werden. Gardiner schlägt in Anlehnung an John Rawls (Rawls 1978) eine präzisierte Fassung vor, die die Gegenbeispiele durch zusätzliche Bedingungen ausschließt und die wir unserer Argumentrekonstruktion zugrunde legen (Gardiner 2006). Das derart erweiterte Prinzip lautet dann so:

Vorsorgeprinzip: Wenn (i) es keine zuverlässigen Wahrscheinlichkeitsprognosen über die Konsequenzen einer Handlung gibt, (ii) die schlechtmöglichsten Fälle der Handlungsalternativen gravierend sind und (iii) die potentiellen Gewinne im Vergleich zu den drohenden Verlusten vernachlässigbar sind, dann sollte die Handlungsoption mit dem relativ besten schlechtmöglichsten Fall gewählt werden.

Mit diesem Entscheidungsprinzip und der Behauptung, dass es möglich sei, dass der Einsatz eines OC-Systems in x katastrophale Folgen hat, lässt sich nun gegen die Einführung des OC-Systems in x argumentieren:

3 Für einen Überblick über die weitverbreitete Zustimmung siehe den ersten Teil von (Gardiner 2006)

Argument 10: Möglichkeit gravierender Folgen inakzeptabel

1) Im Anwendungsfall x kann entweder ein OC-System eingesetzt werden oder es kann alles beim Alten bleiben.
2) Beim Einsatz eines OC-Systems im Anwendungsfall x besteht im schlimmsten Fall die Möglichkeit, dass katastrophale emergente Effekte im geregelten System auftreten, die bisher nicht auftreten konnten.
3) Wenn im Anwendungsfall x ein OC-System eingesetzt wird, lässt sich nicht mit Sicherheit voraussagen, ob, wann oder mit welcher Wahrscheinlichkeit negative emergente Effekte auftreten.
4) Die möglichen Vorteile, die im besten Fall durch den Einsatz eines OC-Systems in x entstehen können, sind im Vergleich zu den katastrophalen emergenten Effekte im schlimmsten Fall vernachlässigbar.
5) Bleibt alles beim Alten, dann kann es im schlimmsten Fall nicht zu katastrophaler Emergenz kommen, sondern nur zu harmloseren Konsequenzen.
6) Vorsorgeprinzip: Wenn (i) es keine zuverlässigen Wahrscheinlichkeitsprognosen über die Konsequenzen einer Handlung gibt, (ii) die schlechtmöglichsten Fälle der Handlungsalternativen gravierend sind und (iii) die potentiellen Gewinne im Vergleich zu den drohenden Verlusten vernachlässigbar sind, dann sollte die Handlungsoption mit dem relativ besten schlechtmöglichsten Fall gewählt werden.
7) **Im Anwendungsfall x sollte alles beim Alten bleiben.**
8) **Im Anwendungsfall x sollte kein OC-System eingesetzt werden.**

Dieses Argument greift die Hauptthese frontal an. Es ist deswegen noch einmal wichtig zu betonen, dass sich aus der obigen Analyse dieses Arguments noch nicht ergibt, dass die Hauptthese widerlegt ist. Die Analyse zeigt nur eines: Wer die Fragen 3.3 und 3.4 negativ beantwortet und das Vorsorgeprinzip als allgemeines Entscheidungsprinzip akzeptiert, der wird es schwierig haben, den Einsatz eines OC-Systems im konkreten Anwendungsfall x zu rechtfertigen. In allen Fällen, in denen 3.3 oder 3.4 positiv beantwortet werden, verliert dieses Argument aber seine Relevanz, weil dann die Prämissen 2 und 3 falsch sind.

Vier Argumente für die Unsicherheit des Wissens (3.3): Nicht-Linearität, Komplexität, Emergenz, fehlende praktische Erfahrung

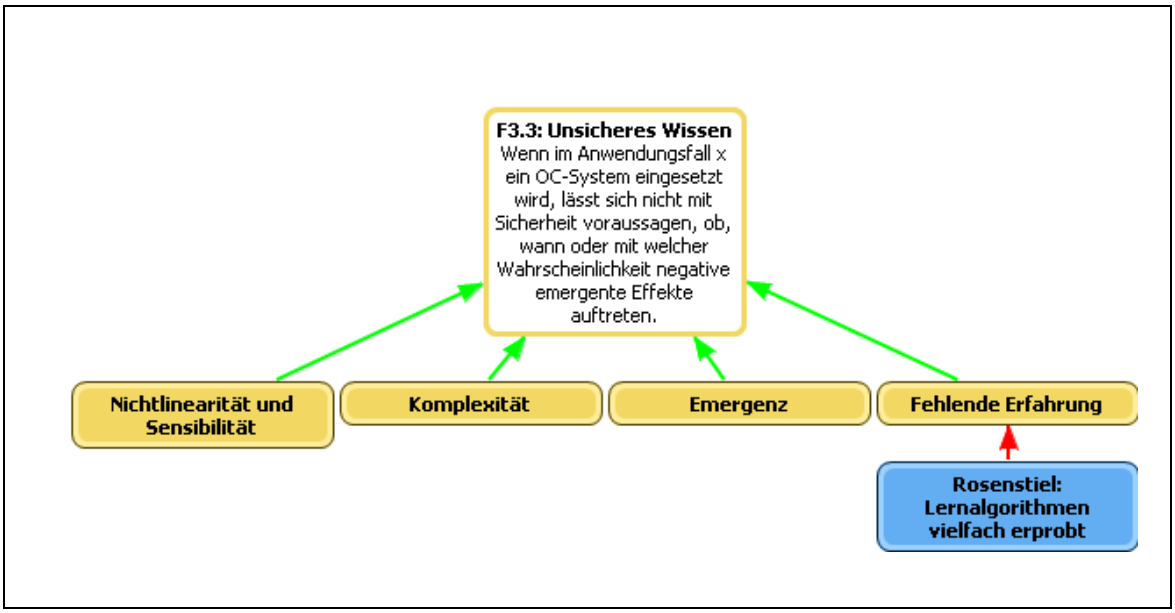

Abbildung v: Argumentlandkarte: Begründung der Unsicherheit des Wissens
Erläuterungen zur Abb. falls notwendig (z.B. Quellen usw.), ggf. löschen.

Ob wirklich, wie in Prämisse 2 behauptet, gravierende Folgen auftreten können (z.B. Bedrohung von Menschenleben) ist natürlich vom jeweiligen Anwendungsszenario abhängig. Anders ist es mit Prämisse 3: Es scheint grundsätzliche Überlegungen zu geben, die dafür sprechen, dass das Wissen über OC-Systeme unsicher ist. An dieser Stelle werden allgemeine und charakteristische Eigenschaften von OC-Systemen relevant. Weil die Unsicherheitsbehauptung (und also Frage 3.3) von zentraler Bedeutung für die Abwägung der Risiken ist, sollen diese Gründe, die für eine negative Antwort auf 3.3 sprechen, hier in kurzen Zusammenfassungen vorgestellt werden, ohne aber näher auf die logischen Rekonstruktionen einzugehen. Die Rekonstruktion dieser Argumente geht vor allem auf eine ausführliche Diskussion dieser Frage auf dem Argumentations-Workshop zurück.

Aus vier Gründen ist es plausibel, dass sich in OC-Systemen nicht mit Sicherheit voraussagen lässt, ob, wann oder mit welcher Wahrscheinlichkeit negative emergente Effekte auftreten:

Nicht-Linearität und Sensibilität: Erstens sind OC-Systeme *nicht-lineare Systeme*, die äußerst sensibel gegenüber ihren Anfangsbedingungen sind. Solche Systeme lassen sich zwar häufig simulieren, aber nicht voraussagen, weil die Simulation nicht schnell genug ist.

Komplexität: Zweitens ist das Wissen unsicher, weil OC-Systemen höchst *komplex* sind. Da (entsprechend der obigen Definition) das bedeutet, dass OC-Systeme aus äußerst vielen Einzelteilen mit äußerst vielen Abhängigkeiten bestehen, ist es äußerst zeit- und kostenaufwändig, OC-Systeme vollständig oder weitgehend zu testen.

Emergenz: Drittens liegt es (ebenfalls entsprechend der obigen Definition) gerade im Wesen *emergenter Effekte*, dass sie unvorhersehbar und überraschend sind. Da OC-Systeme

gerade darauf ausgelegt sind, emergente Effekte zu erzeugen, sollte es nicht verwundern, dass unser Wissen über ihr Verhalten unsicher ist.

Fehlende Erfahrung: Viertens wurden OC-Systeme bisher noch nicht in der Praxis eingesetzt. Es fehlt deswegen die jahre- oder jahrzehntelange praktische Erfahrung, die bereits mit herkömmlichen Systemen gesammelt wurden. Solche Erfahrungen verschaffen uns Sicherheit darüber, dass sich ein System so verhält, wie es soll. Tests können (u.a. aus Kosten- und Zeitgründen) diese Erfahrung nicht ersetzen.

Für all diese Eigenschaften gilt, dass herkömmliche Systeme sie entweder gar nicht oder in geringerem Ausmaß besitzen, so dass die Unsicherheit des Wissens ein spezifisches Problem der OC-Systeme zu sein scheint, das für herkömmliche Systeme zwar durchaus auch, aber zumindest nicht in gleichem Umfang besteht.

In den Diskussionen mit OC-Experten blieben diese Argumente weitgehend unwidersprochen. Nur beim vierten Argument wandte Prof. Rosenstiel im Interview ein, dass man bereits umfangreiche praktische Erfahrungen mit Lernalgorithmen gesammelt habe, z.B. in Spracherkennungssoftware oder Software zum Qualitätsmanagement. Da diese Lernalgorithmen den Kern von OC-Systemen bilden würden, habe man durchaus schon ausreichende Sicherheit darüber, dass OC-Systeme sich so verhalten würden, wie man es intendiert habe (Argument: „Rosenstiel: Lernalgorithmen vielfach erprobt“).

Frage 3.5 (Kein Vertrauensverlust): Ist das Steuerungsverhalten des OC-Systems in x für die Betroffenen nachvollziehbar und voraussehbar, so dass die Betroffenen dem System vertrauen?

Frage 3.6 (Undurchschaubarkeit akzeptabel): Ist es im Anwendungsfall x wichtiger die Komplexität zu bewältigen, als ein System einzusetzen, dessen Verhalten die Betroffenen durchschauen und voraussagen können?

Werden diese beiden Fragen negativ beantwortet, dann reicht das bereits für ein logisch zwingendes Argument gegen die Verhältnismäßigkeitsbehauptung aus. Frage 3 muss dann negativ beantwortet werden:

<u>Argument 11</u>: Undurchschaubarkeit überwiegt

1) Das Steuerungs-Verhalten des OC-Systems in x ist für die betroffenen Personen aufgrund der Komplexität und Emergenz des Systems nicht nachvollziehbar oder voraussehbar und führt dadurch zu Unsicherheit und Misstrauen gegenüber der Technik in x.
2) Die Bewältigung der Komplexität in x ist nicht so wichtig, dass man dafür in Kauf nehmen sollte, dass die Betroffenen das Vertrauen in diese Technik verlieren und sie nicht mehr durchschauen oder voraussehen können.
3) **Die Komplexitätsbewältigung in x ist es nicht wert, dafür die Risiken, die durch den Einsatz eines OC-Systems im Anwendungsfall x entstehen, in Kauf zu nehmen.**

Dieses Argument wurde vor allem von Prof. Müller-Schloer ins Spiel gebracht. Es handelt sich dabei nach seiner Auskunft bisher um einen häufig vernachlässigten Aspekt. Ein typisches Beispiel sei z.B. der Einsatz eines OC-Systems zur Steuerung der Autoelektronik: Würde dieser Einsatz Irritationen und Unsicherheit beim Autofahrer hervorrufen könnte das

z.B. zu Unfällen führen. Die Undurchschaubarkeit wäre in diesem Anwendungsfall inakzeptabel, weil sie das Leben der Autoinsassen gefährden würde. Aber auch unabhängig von solchen indirekt verursachten Katastrophen ist es plausibel, dass eventuell fehlende „Usability“ des OC-Systems in x als negative Folge in die Abwägung mit eingehen sollte.

Um dieses Argument zu entkräften fordert Müller Schloer von OC-Systemen eine weitere self-x-Eigenschaft: OC-Systeme müssen selbst-erklärend sein, damit die Frage 3.5 positiv beantwortet werden kann.

Wie die Fragen 3.1-3.5 untereinander zusammenhängen

Die Antworten auf die Fragen 3.1-3.6 sind keinesfalls logisch voneinander unabhängig. Vielmehr ergibt sich teilweise aus der Antwort auf die eine Frage auch schon (unter Hinzunahme weiterer Aussagen) die Antwort auf die andere Frage. Diese argumentativen Interdependenzen führen dazu, dass bestimmte Positionen innerhalb der Debatte (bestimmte Antwortkombinationen) von vornherein als inkonsistent ausgeschlossen werden können.

Vereinfacht gesagt widersprechen sich positive Antworten auf 3.1 oder 3.2 mit negativen Antworten auf die Fragen 3.3-3.5. Dies ist eine Vereinfachung, weil vier dieser fünf konträren Beziehungen nur vor dem Hintergrund weiterer Annahmen gelten. Diese Beziehungen werden im Anhang ausführlicher vorgestellt.

Die Fragen 3.7-3.9: Eigenschaften von Anwendungsszenarien, die für die Beantwortung der Fragen 3.1-3.3 relevant sind

Was sind typische Fälle, in denen eine der Fragen in der Diskussion um die Verhältnismäßigkeit eindeutig beantwortet werden kann? In den Diskussionen mit OC-Experten wurde auf vier weitere Eigenschaften von OC-Anwendungen aufmerksam gemacht, von denen zumindest die ersten drei eindeutig für die Beantwortung dieser Fragen relevant sind. Diese drei Eigenschaften sollten ebenfalls für Anwendungsszenarien überprüft werden, um die Verhältnismäßigkeit des OC-Einsatzes zu beurteilen (auf die vierte Eigenschaft wird im Anschluss eingegangen):

Frage 3.7 (Manuelle Eingriffe nicht erschwert): Sind manuelle Eingriffe beim Einsatz eines OC-Systems genauso leicht, wie im bisherigen System?

Frage 3.8 (Kein Anstieg der Komplexität): Wird beim Einsatz eines OC-Systems ein Anwachsen der Komplexität des technischen Systems in x verhindert?

Frage 3.9 (Expertenwissen berücksichtigt): Wurde bei der Entwicklung des OC-Systems aus der Erfahrung gewonnenes Expertenwissen über den Anwendungsbereich x ausreichend berücksichtigt?

Im zweiten Teil dieses Abschnittes wird dann der Fragenkatalog für die Diskussion um die Verhältnismäßigkeit mit zwei weiteren Fragen abgeschlossen. Die Beantwortung dieser zwei Fragen hilft dabei, die Fragen 3.7-3.9 zu entscheiden.

Frage 3.7 (Manuelle Eingriffe nicht erschwert): Sind manuelle Eingriffe beim Einsatz eines OC-Systems genauso leicht, wie im bisherigen System?

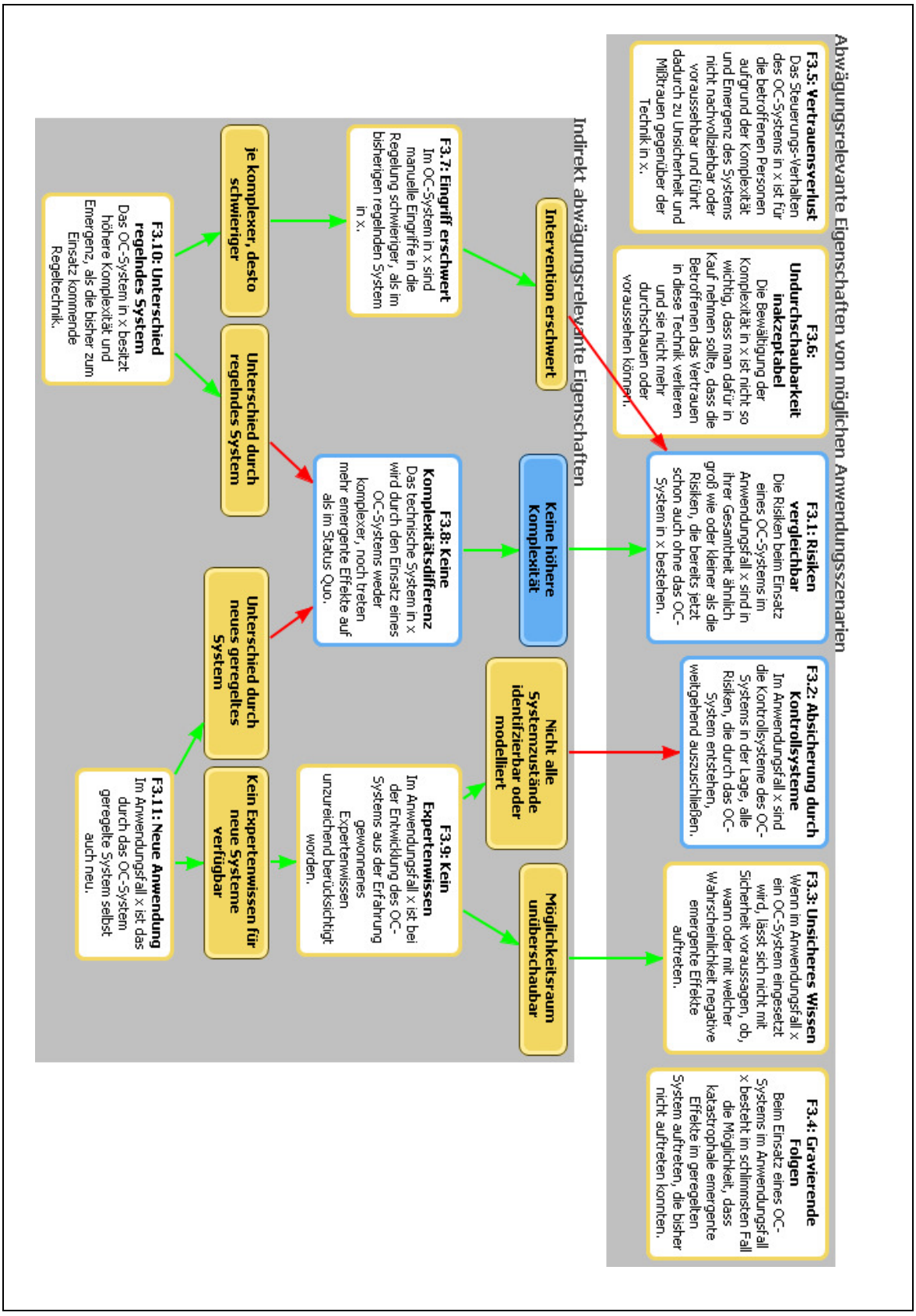

Abbildung vi: Argumentlandkarte: Diskussion um die Verhältnismäßigkeit, Ausschnitt 2

Beantwortet man diese Frage negativ, so ergibt sich daraus ein Argument für eine negative Antwort auf Frage 3.1: Es lässt sich dafür argumentieren, dass die Risiken insgesamt durch den OC-Einsatz anwachsen (dieses Argument stammt aus dem Argumentations-Workshop).

Die Überlegung ist einfach: Solange ein manueller Eingriff ins gesteuerte System (z.B. Ampelsystem) möglich bleibt, solange kann man die schlimmsten Folgen im Notfall häufig noch verhindern. Wäre die manuelle Intervention durch ein OC-System erschwert, so könnte das dazu führen, dass man im Notfall tatenlos zusehen müsste.

Argument 11: Intervention erschwert

1) Im OC-System in x sind manuelle Eingriffe in die Regelung schwieriger, als im bisherigen regelnden System in x.
2) Die Möglichkeit manueller Eingriffe ins regelnde System reduziert die Gefahr negativer Folgen drastisch.
3) Diese Risikoreduktion wird bei der Einführung von OC-Systemen nicht auf andere Weise kompensiert.
4) **Durch den Einsatz von OC-Systemen wachsen die Risiken in x.**

Es ist unklar, ob Prämisse 1 zumindest in manchen Anwendungsszenarien wahr ist. Hier hilft die Differenzierung in geregeltes und regelndes System: Auch wenn ein Eingriff in das OC-System schwerer sein könnte, als ein Eingriff in ein herkömmliches System, heißt das noch nicht, dass damit auch der Eingriff ins geregelte System erschwert wird. Hier besteht weiterer Klärungsbedarf.

Frage 3.8 (Kein Anstieg der Komplexität): Wird beim Einsatz eines OC-Systems ein Anwachsen der Komplexität des technischen Systems in x verhindert?

Beantwortet man diese Frage positiv, so ergibt sich damit ein Argument für eine positive Antwort auf die Frage 3.1: Es ist dann plausibel, dass die Risikolage im Status Quo mit der Risikolage beim Einsatz eines OC-Systems vergleichbar ist.

OC-Experten, wie z.B. Müller-Schloer, Hähner oder Bernard argumentieren auf diese Weise, wenn sie betonen, dass sich an der Komplexität des technischen Systems im Anwendungsbereich durch den Einsatz eines OC-Systems ja nichts ändere. Ihr Argument lässt sich so verstehen: Nur wenn das System überhaupt erst durch den OC-Einsatz zu einem komplexen System werden würde, könnte man die Komplexitätsrisiken in x dem OC-System negativ anrechnen. Da das System aber auch schon vorher komplex war, sind die Risiken vergleichbar.

Argument 13: Keine höhere Komplexität

- Alle Risiken im Anwendungsgebiet x werden durch die Komplexität des technischen Systems und die dadurch auftretenden emergenten Effekte verursacht.
- Das technische System in x wird durch den Einsatz eines OC-Systems weder komplexer, noch treten mehr emergente Effekte auf als im Status Quo.

- Die Risiken beim Einsatz eines OC-Systems im Anwendungsfall x sind in ihrer Gesamtheit ähnlich groß wie oder kleiner als die Risiken, die bereits jetzt schon auch ohne das OC-System in x bestehen.

Frage 3.9 (Expertenwissen berücksichtigt): Wurde bei der Entwicklung des OC-Systems aus der Erfahrung gewonnenes Expertenwissen über den Anwendungsbereich x ausreichend berücksichtigt?

OC-Systeme regeln komplexe Systeme. Dies tun sie, indem sie diese zu regelnden Systeme mithilfe eines Modells repräsentieren, das geregelte System beobachten, aufgrund der Beobachtungen das System im Modell simulieren und aufgrund dieser Simulationen die Zustandsvariablen des Systems anpassen und optimieren. Die OC-Kontrollsysteme werden zwischen das geregelte System und das OC-System geschaltet: Sie beschränken entweder den Konfigurationsraum bereits zur Entwicklungszeit, so dass das OC-System nicht beliebig in das zu regelnde System eingreifen kann oder überprüfen die Konfigurationssätze zur Laufzeit und unterbinden problematische Konfigurationen "live" (Systems under Observation and Control (SuOCs), wie z.B. der Trustworthiness Enforcement Layer (TWEL)) (IÖW et al. 2009 4.2.3).

In beiden Fällen muss das Kontrollsystem in der Lage sein vorauszusagen, welche Effekte eine bestimmte Konfiguration durch das OC-System auf das geregelte System haben wird. Fehlt aber praktisches Expertenwissen über das geregelte System, ist unsicher, ob die Entwickler des OC-Systems in der Lage sind, anhand der Zustandsvariablen alle relevanten Systemzustände des geregelten Systems zu identifizieren und abzubilden. Mit anderen Worten: Es ist nicht sicher, ob alle relevanten Aspekte des geregelten Systems modelliert wurden. Ist das nicht Fall, dann kann das Kontrollsystem noch so gut sein, es wird nicht ausschließen können, dass nicht doch unvorhergesehene Dinge geschehen. In diesem Fall ist es plausibel, dass Frage 3.2 negativ beantwortet werden muss: Die Kontrollsysteme können keinesfalls alle Risiken ausschließen. Das könnten sie nur, wenn man alle relevanten Zustände des geregelten Systems anhand der Systemvariablen identifizieren und abbilden könnte.

<u>Argument 14</u>: Nicht alle Systemzustände identifzierbar oder modelliert

1) Nur unter zureichender Berücksichtigung von Expertenwissen ist es möglich, alle Zustände anhand der Zustandsvariablen des regelnden Systems zu identifizieren.
2) Im Anwendungsfall x ist bei der Entwicklung des OC-Systems aus der Erfahrung gewonnenes Expertenwissen unzureichend berücksichtigt worden.
3) **Im Anwendungsfall x lässt sich nicht jeder Zustand des durch das OC-System geregelten Systems anhand der Zustandsvariablen des OC-Systems identifizieren.**
4) Die weitgehende Verhinderung eines Zustandes im geregelten Systems ist mithilfe der Kontrollsysteme im Anwendungsfall x nur dadurch möglich, dass man diese Zustände anhand der Werte der Zustandsvariablen des OC-Systems identifiziert und diese Werteverteilung entweder von vornherein ausschließt oder während der Laufzeit ändert.
5) **Im Anwendungsfall x ist es nicht möglich mithilfe der Kontrollsysteme des OC-Systems alle negativen emergenten Effekte im geregelten System weitgehend auszuschließen.**

6) Derartige negative emergente Effekte gehören zu den Risiken des OC-Systems in x.

7) Die Kontrollsysteme des OC-Systems in x sind nicht in der Lage alle Risiken, die durch das OC-System entstehen, auszuschließen.

Dies ist nicht der einzige Grund, warum die Berücksichtigung von praktischem Expertenwissen von überragender Wichtigkeit für die Verhältnismäßigkeit des OC-Einsatzes ist: Bleibt dieses Wissen ungenutzt, liegt nicht nur eine negative Antwort auf 3.2 nahe, sondern auch auf 3.3: Je weniger dieses Expertenwissen berücksichtigt wird, desto größer ist die Unsicherheit darüber, ob sich vollständig überblicken lässt, was alles im geregelten System passieren kann. Wenn aber nicht einmal der Möglichkeitsraum überschaubar ist, kann auch niemand beanspruchen über sicheres Wissen zu verfügen:

Argument 14: Möglichkeitsraum unüberschaubar

1) Im Anwendungsfall x ist bei der Entwicklung des OC-Systems aus der Erfahrung gewonnenes Expertenwissen unzureichend berücksichtigt worden.
2) Bei unzureichender Berücksichtigung von Expertenwissen ist der Möglichkeitsraum des zu regelnden Systems nicht überschaubar: Es ist nicht sicher, welche und wieviele Möglichkeiten es innerhalb des Systems gibt, dass negative Folgen auftreten.
3) Wenn nicht einmal sicher ist, dass alle möglichen negativen Folgen eines Systems bekannt sind, dann lässt sich auch nicht voraussagen ob, wann und mit welcher Wahrscheinlichkeit negative emergente Effekte auftreten können.
4) Wenn im Anwendungsfall x ein OC-System eingesetzt wird, lässt sich nicht mit Sicherheit voraussagen, ob, wann oder mit welcher Wahrscheinlichkeit negative emergente Effekte auftreten.

Ausschließlicher Einsatz zur Entwicklungszeit – eine weitere relevante Eigenschaft?

Im Interview wies Prof. Herkersdorf auf eine weitere Differenzierung von Anwendungsfällen hin, die bis dahin unberücksichtigt geblieben war: OC-Systeme können als Entwicklungswerkzeuge während der Entwicklungszeit eingesetzt werden oder als Regelungssysteme während der Laufzeit. So werden OC-Systeme z.B. dazu genutzt, um Chipsysteme zu entwerfen, die selbst keine OC-Komponenten enthalten.

Unklar ist allerdings, inwieweit diese Unterscheidung für die Diskussion um die Verhältnismäßigkeit relevant ist. Zwei Überlgegungen besaßen zumindest eine gewisse Anfangsplausibilität, weshalb sie testhalber in die Debatte aufgenommen wurde: Wird das OC-System ausschließlich zur Entwicklungszeit eingesetzt, so könnte das bedeuten, dass auch nur während der Entwicklungszeit Risiken entstehen und diese Risiken sich auf relativ harmlose Folgen, wie z.B. erhöhten Zeitaufwand oder erhöhte Entwicklungskosten beschränken. Wäre das der Fall, dann würde man erstens dafür argumentieren können, dass im Anwendungsfall x keine neuen Risiken zur Laufzeit entstehen (Frage 3.1) und zweitens keine gravierenden negativen Folgen auftreten können (Frage 3.4).

Im letzten Workshop wies allerdings Andreas Bernauer darauf hin, dass diese Argumente kaum überzeugen können. Erstens ist der ausschließliche Einsatz zur Entwicklungszeit ein sehr seltener Ausnahmefall, so dass diese Argumente für die allermeisten Anwendungsfälle irrelevant sind. Zweitens wird das Problem des unvollständigen und unsicheren Wissens

auch beim ausschließlichen Einsatz zur Entwicklungszeit nicht beseitigt: Denn auch wenn sich das durch OC konfigurierte Regelungssystem zur Laufzeit nicht mehr verändert, ist schwer voraussagbar, welche Folgen diese Konfiguration auf das geregelte System haben wird, solange dieses System hochkomplex, nichtlinear und deswegen schwer zu testen ist. Es wurde deswegen darauf verzichtet, diese Argumente in die Argumentlandkarten aufzunehmen. Diese Eigenschaft wird auch nicht in der Checkliste abgefragt, da sie erstens selten ist und ihre Relevanz für die Verhältnismäßigkeit des OC-Einsatzes selbst in diesen seltenen Fällen unklar ist.

Die Fragen 3.10 und 3.11: Zwei weitere Anwendungseigenschaften, die für die Fragen 3.7-3.9 relevant sind

In einem letzten Schritt lassen sich noch genauere Bedingungen bestimmen, in denen die soeben vorgestellten Erwägungen besonders relevant sind. Dabei geht es nun um zwei weitere Eigenschaften, die beide für jeweils zwei der Fragen 3.7-3.9 relevant sind. Die Fragen nach diesen beiden Eigenschaften schließen den Fragenkatalog zur Verhältnismäßigkeit (Frage 3) ab.

Frage 3.10 (Regelndes System nicht komplexer): Gleicht das regelnde OC-System in seiner Komplexität dem bisher zum Einsatz kommenden regelnden System?

Eine negative Antwort auf diese Frage ergibt erstens ein Argument für die negative Antwort auf 3.7: Denn je komplexer das OC-System, desto schwerer wird der manuelle Eingriff.

Argument 16: Je komplexer, desto schwieriger

1) Das OC-System in x besitzt höhere Komplexität und Emergenz, als die bisher zum Einsatz kommende Regeltechnik.
2) Je komplexer ein regelndes System ist, desto schwerer ist es, manuell in dieses System einzugreifen.
3) **Im OC-System in x sind manuelle Eingriffe in die Regelung schwieriger, als im bisherigen regelnden System in x.**

Zweitens ergibt eine negative Antwort ein Argument gegen die positive Antwort auf Frage 3.8: Die Behauptung, dass sich die Komplexität des technischen Systems in x durch die Einführung eines OC-Systems nicht ändere. Diese Behauptung lässt sich bezweifeln, wenn man berücksichtigt, dass das technische System sich aus regelndem und geregeltem System zusammensetzt:

Argument 17: Unterschied durch regelndes System

1) Das OC-System in x besitzt höhere Komplexität und Emergenz, als die bisher zum Einsatz kommende Regeltechnik.
2) Das in x geregelte System verändert sich in seiner Komplexität nicht durch die Einführung eines OC-Systems.
3) Die Komplexität des technischen Systems in x setzt sich zusammen aus der Komplexität des geregelten Systems und der Komplexität des regelnden Systems.

4) **Durch den Einsatz eines OC-Systems wird das technische System in x komplexer als im Status Quo.**

Frage 3.11 (Keine neue Anwendung): Gab es das geregelte System auch schon vor der Einführung des OC-Systems?

Auch für diese Frage gilt: Wird sie negativ beantwortet, so spricht das gegen eine positive Antwort auf 3.8. Denn in diesem Fall ist es offensichtlich, dass die Komplexität mit der Einführung des OC-Systems ansteigt, weil auch das durch das OC-System geregelte System neu im Anwendungsgebiet eingeführt wird.

Argument 18: Unterschied durch neues geregeltes System

1) Die Komplexität des technischen Systems in x setzt sich zusammen aus der Komplexität des geregelten Systems und der Komplexität des regelnden Systems.
2) Im Anwendungsfall x ist das durch das OC-System geregelte System selbst auch neu.
3) Wenn es in x vorher weder das geregelte System, noch das regelnde System gab, dann gab es keine Komplexität des technischen Systems im Status Quo.
4) Das neue geregelte System in x ist komplex.
5) **Durch den Einsatz eines OC-Systems wird das technische System in x komplexer als im Status Quo.**

Noch wichtiger scheint aber ein anderes Argument, das sich aus einer negativen Antwort auf diese Frage ergibt: Wenn das geregelte System selbst auch neu ist, dann gibt es noch kein praktisches Expertenwissen mit diesem System. Ein solches Expertenwissen kann dann auch nicht in die Entwicklung des OC-Systems (in die Modellierung des Anwendungsgebietes zu Simulationszwecken) eingehen. Ist das geregelte System selbst neu, so spricht deswegen alles für eine negative Antwort auf 3.9.

Argument 19: Kein Expertenwissen für neue Systeme verfügbar

1) Im Anwendungsfall x ist das durch das OC-System geregelte System selbst auch neu.
2) Für neue Systeme ist kein aus der praktischen Erfahrung gewonnenes Expertenwissen verfügbar.
3) Wo kein Expertenwissen verfügbar ist, kann es auch nicht berücksichtigt werden.
4) **Im Anwendungsfall x ist bei der Entwicklung des OC-Systems aus der Erfahrung gewonnenes Expertenwissen unzureichend berücksichtigt worden.**

Für die innerhalb des Projekts untersuchten Anwendungsfelder ist dieses Argument irrelevant, weil die geregelten Systeme bereits vorhanden sind und ausreichend Expertenwissen zur Verfügung steht (z.B. Verkehrsingenieure, Logistiker usw.). Das heißt allerdings nicht, dass diese Erwägungen nicht für andere Anwendungsgebiete relevant werden könnten.

Damit ist nun die Vorstellung dieses Debattenteils abgeschlossen. Diese Debatte kann sicherlich noch fortgeführt und ergänzt werden. Hier ging es nur darum den derzeitigen Stand der Debatte darzustellen, wie er sich aus den Interviews und Workshops ergab und Einwände vorwegzunehmen, die sich bereits abzeichnen. Die Ergebnisse implizieren keines-

falls eine Entscheidung für oder gegen OC, weder allgemein, noch für spezifische Anwendungsfälle. Sie sollen nur die rationale Entscheidungsfindung unterstützen.

Frage 4 (Erforderlichkeit): Gibt es andere verfügbare Alternativen in x, die besser geeignet zur Komplexitätsbewältigung oder verhältnismäßiger wären?

Um diese Frage zu beantworten, muss zunächst eine vollständige Liste aller verfügbaren Alternativen aufgestellt werden, die überhaupt zur Komplexitätsbewältigung in Frage kommen. Es scheint hier, soweit dies aus den Äußerungen der OC-Experten zu erschließen ist, zwei Gruppen von technischen Lösungen zu geben: Auf der einen Seite die herkömmlichen Regelungs-Techniken, die hierarchisch, zentralistisch, top-down, nicht-adaptiv organisiert sind und teilweise manuell konfiguriert werden (z.B. Ampelsysteme). Auf der anderen Seite technische Innovationen, die teilweise noch in den Kinderschuhen stecken, also ähnlich wie Organic Computing noch in der Konzeptions-, Planungs- oder Testphase sind. Hier gibt es eine Vielzahl von Schlagwörtern, die teilweise neue Anwendungsbereiche, teilweise Eigenschaften der neuen Techniken beschreiben, z.B. Autonomic Computing, Ubiquitious Computing, Ambient Intelligence, Pervasive Computing, Natural Computing, Internet of Things oder SaSo.

Für beide Gruppen technischer Alternativen muss nun jeweils dafür argumentiert werden, dass sie nicht besser geeignet oder risikoärmer sind als OC-Systeme. Daraus ergeben sich die zwei Unter-Fragen von Frage 4:

Frage 4.1 (Herkömmliche Alternativen): Ist es falsch, dass herkömmliche Regelungstechniken im Anwendungsfall x besser geeignet oder risikoärmer sind als OC-Systeme?

Frage 4.2 (Innovative Alternativen): Ist es falsch, dass innovative Regelungstechniken, wie Autonomic Computing, Ubiquitious Computing, Ambient Intelligence, Pervasive Computing, Natural Computing, Internet of Things oder SaSo, im Anwendungsfall x besser geeignet oder risikoärmer sind als OC-Systeme?

Da bereits bei Frage 1, also der Diskussion um den Bedarf mit den Mängeln der herkömmlichen Techniken argumentiert wurde, ergibt sich die Argumentation für eine positive Antwort auf 4.1 bereits von selbst (es werden dabei ähnliche oder sogar dieselben Thesen verwendet): Herkömmliche Systeme sind schlecht geeignet, um Komplexität zu bewältigen. Und sie sind nicht in der Lage negative Emergenz in den Griff zu bekommen, weshalb sie zumindest genauso risikoreich wie OC-Systeme sind (Müller-Schloer).

<u>Argument 20</u>: Weniger geeignet

1) Herkömmliche Systeme sind weniger stabil, erweiterbar, skalierbar und lernfähig als OC-Systeme.

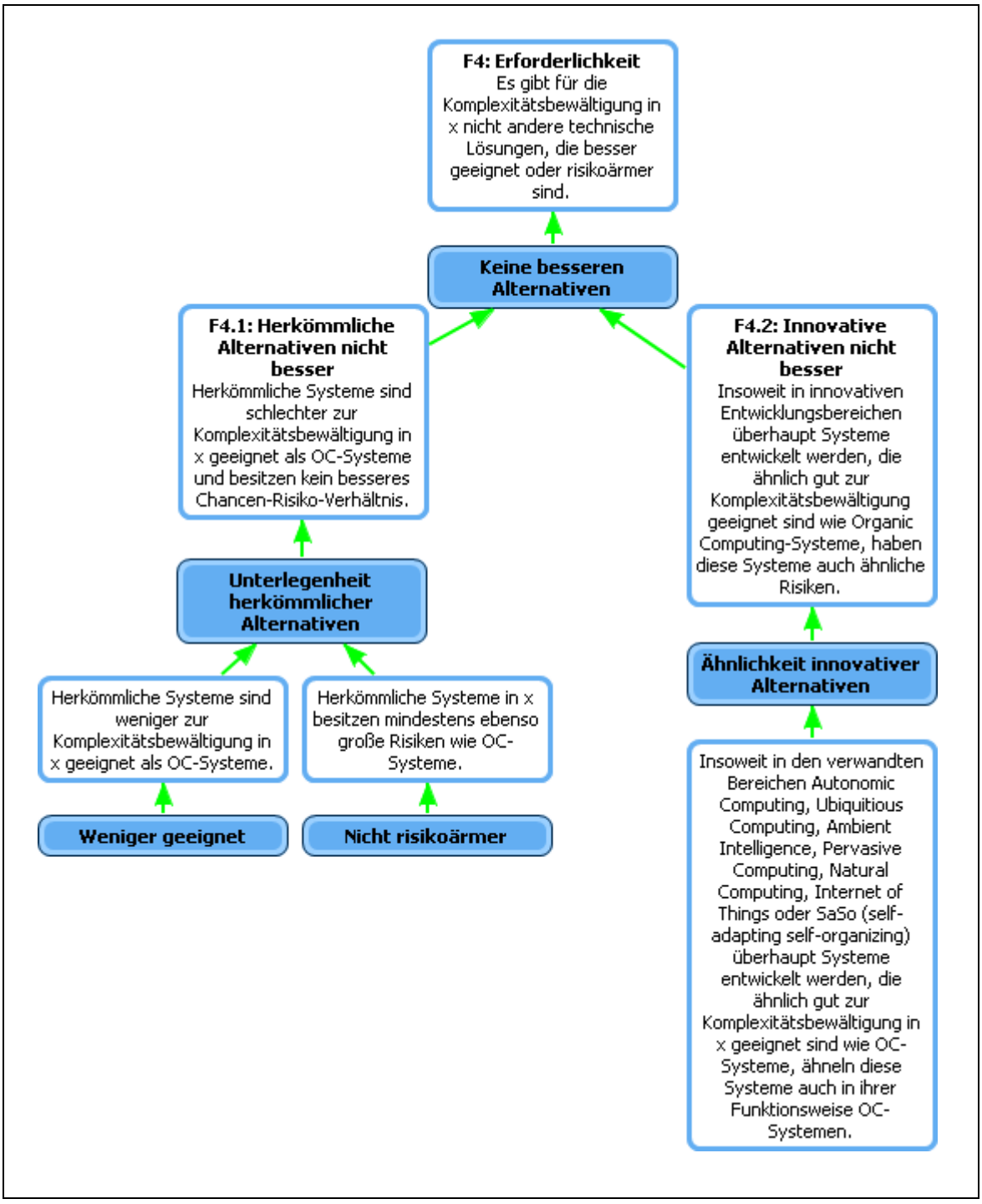

Abbildung vii: Argumentlandkarte: Bergründung der Erforderlichkeit

2) In herkömmlichen Systemen sind emergente Effekte nicht beherrschbar, in OC-Systemen schon.

3) Die Entwicklung herkömmlicher Systeme ist weniger zeit- und kosteneffizient als die Entwicklung von OC-Systemen.

1. Für zwei Systeme s1, s2 gilt: Wenn s1 a) stabiler, erweiterbarer, lernfähiger und skalierbarer ist, b) emergente Effekte beherrschbarer macht und c) zeit- und kosteneffizienter zu

entwickeln ist als ein anderes System und d) s2 sich nicht in Eigenschaften von s1 unterscheidet, die a, b und c kompensieren, dann ist a besser zur Komplexitätsbewältigung in x geeignet als b.

4) Herkömmliche Systeme unterscheiden sich nicht in anderer Hinsicht von OC-Systemen, die a), b) und c) kompensieren würde.

5) Herkömmliche Systeme sind weniger zur Komplexitätsbewältigung in x geeignet als OC-Systeme.

Argument 21: Nicht risiko-ärmer

1) In herkömmlichen Systemen, die der Komplexitätsbewältigung in x dienen, ist das Risiko negativer oder katastrophaler Emergenz höher als in OC-Systemen oder genauso hoch wie in diesen.

2) Es gibt keine anderen Risiken von OC in x, die diesen Unterschied kompensieren würden.

3) Die Risiken herkömmlicher Systeme sind nicht kleiner als die Risiken von OC-Systemen.

4) Die Chancen von herkömmlichen Systemen überwiegen nicht die Chancen von OC-Systemen.

5) Herkömmliche Systeme in x besitzen mindestens ebenso große Risiken wie OC-Systeme.

Interessanter ist die Argumentation für eine positive Antwort auf Frage 4.2. Die befragten OC-Experten argumentieren hier sehr zurückhaltend: Sie wollen den anderen Forschungsbereichen nicht ihre Berechtigung oder ihr Potential streitig machen. Stattdessen sehen sie diese Bereiche viel eher als verwandte Bereiche an, in denen an ähnlichen Ideen geforscht wird, mit teilweise anderen Schwerpunkten. Die unübersichtliche Vielfalt der Schlagwörter und die Ähnlichkeit der dahinterstehenden Forschungsprojekte lassen sich zumindest teilweise mit den unterschiedlichen Förderungs- und Marketinghintergründen (Deutschland, EU, USA, IBM usw.) erklären (Interviews Herkersdorf, Rosenstiel, Argumentations-Workshop und Abschluss-Workshop).

Die OC-Proponenten wollen deswegen nicht behaupten, dass Organic Computing sich grundlegend in Eignung und Verhältnismäßigkeit von diesen eng verwandten Ansätzen unterscheidet. Sie sehen diese Ansätze weniger als Konkurrenten, denn als Verbündete, als Mitstreiter für dasselbe Grundanliegen.

Diese Zurückhaltung ist, solange es um die Forschungsförderung geht, durchaus berechtigt: Um die Forschung an Organic Computing zu rechtfertigen muss Organic Computing *nicht* als beste Alternative gegenüber anderen Forschungszweigen verteidigt werden. Stattdessen reicht als Argument das Potential von Organic Computing, also die Möglichkeit, dass es einmal Anwendungen mit Alleinstellungsmerkmalen geben könnte. Zudem ist es plausibel, dass in der Forschung eine möglichst große Vielfalt gefördert werden sollte, weil es unmöglich ist die Gewinner vorauszusagen. Es ist sogar durchaus plausibel, dass man "out-of-the-box-thinking" (Herkersdorf) fördern sollte und also auch Außenseiter-Ansätze unterstützen sollte, die zunächst exotisch zu sein scheinen.

Wenn es aber nicht um die Forschungsförderung geht, sondern um den konkreten Einsatz einer Technik in der Praxis, gelten andere Beweislasten. Hier muss nun gezeigt werden, dass es im konkreten Anwendungsbereich keine besseren Alternativen zu der Technik gibt, für die man sich entschieden hat. Weder lässt sich hier mit dem Potential dieser Lösung für zukünftige Anwendungen, mit dem Vielfaltsargument oder mit der Bedeutung von out-of-the-box-thinking argumentieren.

Dennoch sollte in der Argumentation berücksichtigt werden, dass es sich bei den verwandten innovativen Ansätzen nicht um grundlegend andersartige Ansätze handelt, sondern eher um Ansätze, die viele Ähnlichkeiten mit Organic Computing haben und sich eher in der Schwerpunktsetzung oder den Anwendungsfeldern unterscheiden. Man könnte die Bemerkungen der OC-Experten deswegen so interpretieren:

Argument 22: Ähnlichkeit innovativer Alternativen

1) Insoweit in den innovativen Entwicklungsbereichen Autonomic Computing, Ubiquitious Computing, Ambient Intelligence, Pervasive Computing, Natural Computing, Internet of Things oder SaSo überhaupt Systeme entwickelt werden, die ähnlich gut zur Komplexitätsbewältigung in x geeignet sind wie OC-Systeme, ähneln diese Systeme auch in ihrer Funktionsweise OC-Systemen.
2) Je ähnlicher zwei technische Systeme funktionieren, desto mehr ähneln sich auch ihre Risiken.
3) **Insoweit in innovativen Entwicklungsbereichen überhaupt Systeme entwickelt werden, die ähnlich gut zur Komplexitätsbewältigung geeignet sind wie Organic Computing-Systeme, haben diese Systeme auch ähnliche Risiken.**

Diese Argumentationsweise ist geschickt, weil sie abstreitet, dass die scheinbaren Alternativen überhaupt *echte* technische Alternativen sind: Insofern die in diesen Bereichen entwickelten technischen Systeme zur Komplexitätsbewältigung infrage kommen, könnte man sie genauso gut als Organic-Computing-Systeme bezeichnen.

Damit ist nun die Vorstellung der rekonstruierten Debatte abgeschlossen. Es wurde jeweils gezeigt, wie sich die Prämissen des Hauptarguments begründen lassen. Für die Verhältnismäßigkeitsbehauptung (Prämisse 3 des Hauptarguments) wurden mögliche Gegengründe vorgestellt. Anstatt eines Fazits sollen nun die Ergebnisse dieser Analyse im gewonnenen Fragenkatalog übersichtlich zusammengefasst werden.

3. Checkliste: Sollte im Anwendungsfall x ein OC-System eingesetzt werden?

Diese Checkliste fasst die Ergebnisse der Argumentationsanalyse zusammen. Jede positive Antwort unterstützt die Argumentation für oder schwächt die Argumentation gegen den Einsatz des OC-Systems. Jede negative Antwort unterstützt die Argumentation gegen oder schwächt die Argumentation für den Einsatz des OC-Systems. Es handelt sich *nicht* in allen Fällen einfach jeweils um direkte Pro- und Contra-Gründe für oder gegen den Einsatz.

Dieser Fragekatalog ist deswegen keine Checkliste im herkömmlichen Sinne: Eine negative Antwort bedeutet noch nicht, dass das OC-System nicht eingesetzt werden sollte. Welche Auswirkung die Antworten auf die Fragen jeweils in der Debatte um den OC-Einsatz haben, wird jeweils in den vorausgegangenen Abschnitten beschrieben.

1 (Bedarf): Besteht im Anwendungsbereich x Bedarf nach Komplexitätsbewältigung?

1.1 (Komplexität unbewältigt): Ist die Komplexität im Anwendungsbereich bisher wenig oder gar nicht technisch bewältigt?

1.2 (Komplexitätsbewältigung wünschenswert): Sollte die Komplexität im Anwendungsbereich überhaupt technisch bewältigt werden?

2 (Eignung): Ist das OC-System im Anwendungsbereich x zur Komplexitätsbewältigung geeignet?

2.1 (Anforderungen I): Sind OC-Systeme im Anwendungsbereich x stabil, erweiterbar, lernfähig und skalierbar?

2.2 (Anforderungen II): Machen OC-Systeme im Anwendungsbereich x emergente Effekte beherrschbar und nutzbar?

2.3 (Anforderungen III): Lassen sich mit der Entwicklung von OC-Systemen im Anwendungsbereich x langfristig Zeit und Kosten einsparen?

3 (Verhältnismäßigkeit): Ist die Komplexitätsbewältigung in x es wert, dafür die Risiken des OC-Systems in Kauf zu nehmen?

Direkt abwägungsrelevante Eigenschaften:

3.1 (Kein negativer Risikovergleich): Sind die Risiken, die durch den Einsatz des OC-Systems entstehen mit den zuvor bestehenden Risiken vergleichbar oder sogar geringer?

3.2 (Ausreichende Kontrolle): Lassen sich die Risiken, die durch den Einsatz des OC-Systems entstehen derart durch Kontrollsysteme reduzieren, dass die Verhinderung des Restrisikos es nicht wert ist dafür die Komplexitätsbewältigung in x aufzugeben?

3.3 (Sicheres Wissen): Ist beim Einsatz eines OC-Systems die Unsicherheit darüber, ob, wann oder mit welcher Wahrscheinlichkeit negative Systemzustände im geregelten System auftreten gering?

3.4 (Worst case nicht katastrophal): Wären die negativen Folgen auch im schlimmstmöglichen Fall nicht gravierend, inakzeptabel und katastrophal?

3.5 (Kein Vertrauensverlust): Ist das Steuerungs-Verhalten des OC-Systems in x für die Betroffenen nachvollziehbar und voraussehbar, so dass die Betroffenen dem System vertrauen?

3.6 (Undurchschaubarkeit akzeptabel): Ist es im Anwendungsfall x wichtiger die Komplexität zu bewältigen, als ein System einzusetzen, dessen Verhalten die Betroffenen durchschauen und voraussagen können?

Indirekt abwägungsrelevante Eigenschaften:

3.7 (Manuelle Eingriffe nicht erschwert): Sind manuelle Eingriffe beim Einsatz

eines OC-Systems genauso leicht, wie im bisherigen System?

3.8 (Kein Anstieg der Komplexität): Wird beim Einsatz eines OC-Systems ein Anwachsen der Komplexität des technischen Systems in x verhindert?

3.9 (Expertenwissen berücksichtigt): Wurde bei der Entwicklung des OC-Systems aus der Erfahrung gewonnenes Expertenwissen über den Anwendungsbereich x ausreichend berücksichtigt?

3.10 (Regelndes System nicht komplexer): Gleicht das regelnde OC-System in seiner Komplexität dem bisher zum Einsatz kommenden regelnden System?

3.11 (Keine neue Anwendung): Gab es das geregelte System auch schon vor der Einführung des OC-Systems?

4 (Erforderlichkeit): Gibt es andere verfügbare Alternativen in x, die zur Komplexitätsbewältigung besser geeignet oder verhältnismäßiger wären?

4.1 (Herkömmliche Alternativen): Ist es falsch, dass herkömmliche Regelungstechniken im Anwendungsfall x besser geeignet oder risikoärmer sind als OC-Systeme?

4.2 (Innovative Alternativen): Ist es falsch, dass innovative Regelungstechniken, wie Autonomic Computing, Ubiquitious Computing, Ambient Intelligence, Pervasive Computing, Natural Computing, Internet of Things oder SaSo, im Anwendungsfall x besser geeignet oder risikoärmer sind als OC-Systeme?

12.2.3 Anhang: Wie die Fragen 3.1-3.5 untereinander zusammenhängen

Wenn die Antwort auf 3.1 positiv ist, dann auch die Antwort auf 3.4 (wenn die Antwort auf 3.4 negativ ist, dann auch die Antwort auf 3.1)

Eine positive Antwort auf 3.1 zieht unter Hinzunahme einer weiteren Prämisse eine positive Antwort auf 3.4 nach sich:

<u>Argument 23</u>: Gravierende Folgen vergleichbar

1) Die Risiken beim Einsatz eines OC-Systems im Anwendungsfall x sind in ihrer Gesamtheit ähnlich groß wie oder kleiner als die Risiken, die bereits jetzt schon auch ohne das OC-System in x bestehen.
2) Entstünde durch den Einsatz des OC-Systems in x neue Möglichkeiten katastrophaler emergenter Effekte und gäbe es bisher keine vergleichbar schwerwiegenden Risiken, dann müssten die Risiken des OC-Systems in jedem Fall größer sein, als die Risiken, die bereits jetzt schon auch ohne das OC-System bestehen.
3) **Durch den Einsatz von OC in x entstehen keine zusätzlichen Möglichkeiten katastrophaler emergenter Effekte.**

Solange man Prämisse 2 nicht bezweifelt, lässt sich diese Beziehung auch umkehren: Wer 3.4 negativ beantwortet, muss auch 3.1 negativ beantworten.

Wenn die Antwort auf 3.2 positiv ist, dann auch die Antwort auf 3.4 (wenn die Antwort auf 3.4 negativ ist, dann auch die Antwort auf 3.2)

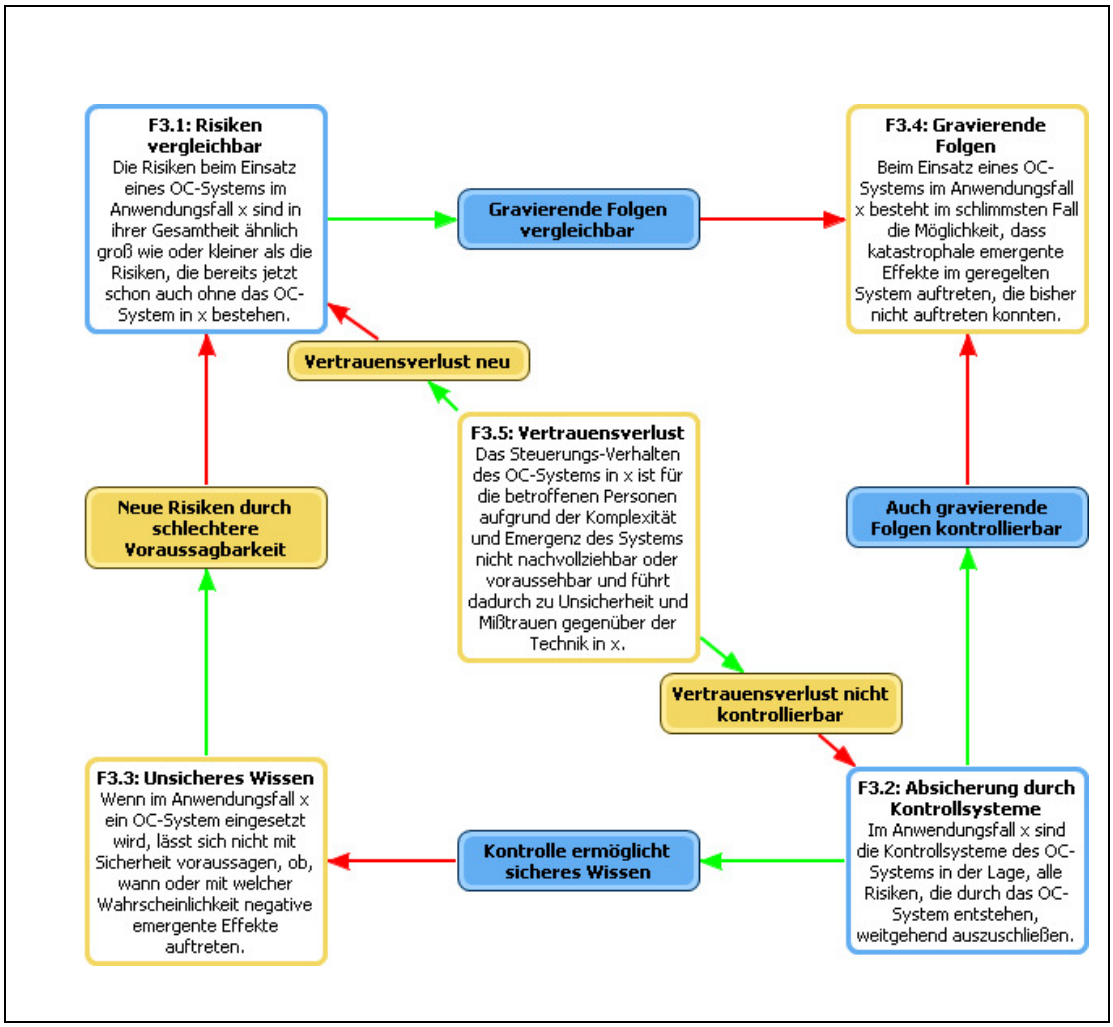

Abbildung viii: Argumentlandkarte: Beziehungen zwischen den abwägungsrelevanten Eigenschaften

Nun zur zweiten Frage: Wird sie positiv beantwortet, muss auch die vierte Frage positiv beantwortet werden. Denn da dann gilt, dass alle Risiken weitgehend kontrollierbar sind, sind trivialerweise auch gravierende Risiken kontrollierbar. Da es sich hierbei nur um eine Spezialisierung der generelleren Aussage handelt, muss keine weitere Prämisse hinzugenommen werden. Deswegen gilt auch: Wenn gravierende Risiken auftreten, dann ist es natürlich falsch, dass alle Risiken durch Kontrollmechanismen ausgeschlossen wurden.

Wenn die Antwort auf 3.2 positiv ist, dann auch die Antwort auf 3.3 (wenn die Antwort auf 3.3 negativ ist, dann auch die Antwort auf 3.2)

Eine positive Antwort auf die zweite Frage schließt ebenfalls eine negative Antwort auf die dritte Frage aus, wenn man eine weitere Prämisse hinzunimmt:

Argument 24: Kontrolle ermöglicht sicheres Wissen:

1) Im Anwendungsfall x sind die Kontrollsysteme des OC-Systems in der Lage, alle durch das OC-System verursachten negativen Effekte im geregelten System zu verhindern.
2) Wenn es möglich ist, alle negativen emergenten Effekte in einem OC-System zu verhindern, dann lässt sich mit Sicherheit voraussagen, dass diese Effekte nicht mehr auftreten werden.
3) **Im Anwendungsfall x lässt sich sehr wohl voraussagen, ob, wann oder mit welcher Wahrscheinlichkeit negative emergente Effekte auftreten werden.**

Auch hier gilt: Solange Prämisse 2 akzeptiert wird, kann man aus der Verneinung der Konklusion (aus der negativen Antwort auf die dritte Frage) auf die Verneinung der ersten Prämisse (die negative Antwort auf die zweite Frage) schließen.

Wenn die Antwort auf 3.5 negativ ist, dann auch die Antwort auf 3.1 (wenn die Antwort auf 3.1 positiv ist, dann auch die Antwort auf 3.5)

Dies gilt nur unter Voraussetzung einer zusätzlichen Prämisse:

Argument 25: Vertrauensverlust neu

1) Das Steuerungs-Verhalten des OC-Systems in x ist für die betroffenen Personen aufgrund der Komplexität und Emergenz des Systems nicht nachvollziehbar oder voraussehbar und führt dadurch zu Unsicherheit und Misstrauen gegenüber der Technik in x.
2) Dieses Risiko entsteht erst durch die Einführung des OC-Systems und wird nicht durch die restlichen Risiken kompensiert.
3) **Durch den Einsatz eines OC-Systems im Anwendungsfall x entstehen neue Risiken, die in ihrer Gesamtheit größer sind als die Risiken, die bereits jetzt schon auch ohne das OC-System in x bestehen.**

Wenn die Antwort auf 3.5 negativ ist, dann auch die Antwort auf 3.2 (wenn die Antwort auf 3.2 positiv ist, dann auch die Antwort auf 3.5)

Dies gilt nur unter Voraussetzung von zwei zusätzlichen Prämissen:

Argument 26:

1) Das Steuerungs-Verhalten des OC-Systems in x ist für die betroffenen Personen aufgrund der Komplexität und Emergenz des Systems nicht nachvollziehbar oder voraussehbar und führt dadurch zu Unsicherheit und Misstrauen gegenüber der Technik in x.
2) Dies ist ein Risiko, das durch den Einsatz des OC-Systems in x entsteht.
3) Dieses Risiko kann nicht durch Kontrollsysteme ausgeschlossen werden.
4) **Nicht alle Risiken, die durch den Einsatz des OC-Systems in x entstehen, können durch Kontrollsysteme ausgeschlossen werden.**

4. Literatur

Bedau, M.A., 1997. Weak Emergence. *Noûs*, 31, 375-399.

Bernard, Y., 2009a. Charakterisierungen der Organic Computing-Ansätze aus den Interviews.

Bernard, Y., 2009b. Herausforderungen des Organic Computing.

Bernard, Y., 2009c. OC und aktuelleTrends im Software Engineering.

Conrad, J., 2009. Chancen und Risiken selbstorganisierender adaptiver Systeme.

Gardiner, S.[., 2006. A Core Precautionary Principle. *Journal of Political Philosophy*, 14, 33-60.

IÖW, Leibniz Universität Hannover & Freie Universität Berlin, 2009. *Selbstorganisierende adaptive Systeme: Analyse der Chancen und Risiken sowie der Gestaltungsansätze neuer IKT - Ansätze*,

Mainzer, K., 2008. *Komplexität. UTB Profile* 1. ed., UTB, Stuttgart.

Mainzer, K., 2007. *Thinking in Complexity: The Computational Dynamics of Matter, Mind, and Mankind* 5. ed., Springer, Berlin.

Rawls, J., 1978. *Eine Theorie der Gerechtigkeit*, Suhrkamp.

United Nations, 1992. Report of the United Nations Conference on Environment and Development (A/CONF.151/26). Available at: http://www.un.org/documents/ga/conf151/aconf15126-1annex1.htm [Accessed July 22, 2009].

A-III ANHANG III:

Rechtsexpertise zu selbstorganisierenden adaptiven IT Systemen

Autoren: Dr. Meinhard Erben, Dr. Wolf Günther

Inhalt

0. Ziel der Expertise III-4

1. Hintergrund III-4

1.1. Einführung III-4
1.2. Konkretisierung der Fragestellung(en) III-5
1.3. Organische Computersysteme III-7
1.4. Anwendungsbeispiel: Elektronik im Kfz (Embedded Systems) III-8
1.4.1. Vertragliche Konstruktion in der Praxis III-8
1.4.2. Potenzielle Folge bei Fehler: Rückrufaktion III-9
1.4.3. Möglichkeiten mit Organic Computing Techniken III-10

2. Haftungsrecht bzgl. IT-Produkte, insb. Software III-10

2.1. Haftungsrechtliche Grundlagen III-11
2.2. Haftung nach dem ProdHG: Produkthaftung III-12
2.2.1. Sicherheit als Maßstab für Produktfehler III-13
2.2.2. Berechtigte Erwartung III-14
2.2.3. Berücksichtigung aller Umstände III-16
2.2.3.1. Darbietung III-16
2.2.3.2. Gebrauch, mit dem billigerweise gerechnet werden kann III-17
2.2.4. Gesamte objektive Umstände III-19
2.2.4.1. Objektiver Umstand: Natur der Sache III-19
2.2.4.2. Objektiver Umstand: Preisgestaltung III-21
2.2.4.3. Objektiver Umstand: Stand von Wissenschaft und Technik III-21
2.2.4.4. Objektiver Umstand: Technische Normen und gesetzliche Sicherheitsbestimmungen III-23
2.2.5. Unterscheidung nach Art der Fehler III-25
2.2.5.1. Konstruktionsfehler III-25
2.2.5.2. Fabrikationsfehler III-27
2.2.5.3. Instruktionsfehler III-27
2.3. Gibt es erste Präzedenzfälle mit „smarten Technologien“? III-32
2.3.1. Recherche bestehender rechtlicher Ansätze und einschlägiger rechtswissenschaftlicher Untersuchungen III-33
2.3.2. Welche Probleme existieren und welche offenen Fragen werden hierbei diskutiert? III-33
2.3.3. Haben sich in der diesbezüglichen rechtsfachlichen Diskussion erkennbar unterschiedliche (gegenläufige) Positionen herausgebildet? III-36
2.4. Haftung nach dem BGB: Produzentenhaftung III-38
2.4.1. Organisationspflichten bei Produzentenhaftung III-39
2.5. Vertragsrechtliche Haftung III-39
2.6. Gibt es haftungsrechtlich Besonderheiten bei der Haftung für Software? III-40
2.6.1. Besonderheit wegen Unvermeidbarkeit von Fehlern? III-40
2.7. Besonderheiten wegen Schnittstelle Mensch/Maschine: Wem sind die Fehler zuzurechnen, Mensch oder Maschine? III-42
2.7.1. Verursacherprinzip vs. Verschuldensprinzip III-42

2.7.2. Verantwortlichkeit von Maschinen für Handlungen ... III-44
2.7.3. Rechtliche Verantwortlichkeit ... III-47
2.7.4. Wie werden die Verantwortlichkeiten unter welchen Bedingungen zugeordnet? ... III-49
2.7.5. Strafrechtliche Haftung / Verantwortlichkeit / Produktbeobachtungspflicht ... III-50
2.8. Abwägung und Zwischenergebnis ... III-51

3. Welche Anpassungen des Rechtsrahmens bzw. von rechtlich relevanten Standards sind ggf. erforderlich? ... III-53

3.1. Anpassung des ProdHG und/oder geltender technischer Normen an die Besonderheiten des Organic Computing? ... III-53
3.2. Anpassung von Organic Computing an das ProdHG und/oder geltende technische Normen? ... III-53
3.3. Welche neuen Herausforderungen ergeben sich in diesen Bereichen für selbstorganisierende(n) adaptive(n) Systeme? ... III-56
3.4. „Lernprozesse“ von OC Systemen / Differenzierung zwischen Systemen, die adaptiv sind, und Systemen die „eigenständig“ lernfähig sind ... III-56
3.5. Sind neuartige Standards denkbar, die die begrenzte Testbarkeit der selbstorganisierenden Systeme berücksichtigen? ... III-58
3.6. Welche Auswirkungen haben emergente Eigenschaften auf die Festlegung der Standards und sind dabei Differenzierungen möglich? ... III-59
3.7. Abwägung und Zusammenfassung ... III-59

4. Entwicklung erster Ansätze zur rechtsvermittelten Vertrauenserzeugung gegenüber selbstorganisierenden, adaptiven Systemen und zum Rechtsgüterschutz ... III-60

4.1. Lernende Systeme – unter welchen Bedingungen können sie eingesetzt werden? ... III-61
4.2. Vertrauensaspekte (Trust) ... III-61
4.3. Standardisierungs- und Zertifizierungsmaßnahmen ... III-64
4.3.1. Soweit machbar: Reduktion der Komplexität der Systeme ... III-64
4.3.2. Geeignet zur Zielerreichung: Definierte Schnittstellen sowie standardisierte Verfahren ... III-65
4.3.3. Zertifizierung durch staatliche oder andere Stellen ... III-65
4.4. Wie kann Verlässlichkeit i.S.v. Reliability erreicht werden? ... III-65

5. Zusammenfassung ... III-66

0. Ziel der Expertise

Mit selbstorganisierenden adaptiven Systemen wie z. B. Organic Computing werden neue Wege beschritten. Das Ziel dieser Rechtsexpertise ist es, die potenziellen Rechtsfragen, insb. Haftungsfragen, darzustellen und auszuloten. Dabei sollen auch Regelungslücken identifiziert und ggf. Vorschläge für deren Überwindung entwickelt werden.

1. Hintergrund

Im Bereich IKT orientieren sich Entwicklungsanstrengungen zunehmend auf selbstorganisierende adaptive Systeme wie z. B. Organic Computing. Diese Systeme sind immer weniger statisch, sondern dynamisch in dem Sinne, dass sie sich zum einen an sich verändernde Umwelten anpassen und damit auch über neue Funktionalitäten verfügen, und zum anderen in der Lage sind, auftretende Fehler selbst zu „heilen“. Vielfach werden diese potenziellen neuen Eigenschaften als Self-X Eigenschaften bezeichnet.

1.1. Einführung

Mit selbstorganisierenden adaptiven Systemen sind sowohl Chancen als auch Risiken verbunden. Die Chancen ergeben sich u.a. durch neue Funktionalitäten und einen potenziell geringeren Aufwand, die Risiken im Wesentlichen dadurch, dass das Verhalten der Systeme nicht gänzlich vorhersehbar ist. Für die Marktdurchsetzung entsprechender Systeme und damit der Nutzung der Chancen ist es mit entscheidend, welche rechtlichen Regelungen existieren, insb. stellt sich die Frage des Produkthaftungsrechts für solche Systeme. Rechtliche Fragestellungen sind daher mit zentral dafür, ob bzw. in welchem Maße solche Systeme eingeführt werden können und ob bzw. wie sie sich ggf. im Markt durchsetzen können.

Dabei ist zu berücksichtigen, dass – ganz allgemein betrachtet – die Zahl von technischen Systemen und deren Komplexität immer mehr zunimmt. Dies gilt sowohl für einzelne technische Geräte, von denen wir im Alltag umgeben sind, als auch für diejenigen Systeme, die die Infrastruktur für die stark fortschreitende Vernetzung von technischen Einheiten bilden. Das Verständnis und die Beherrschbarkeit der zunehmenden Komplexität gilt als eine der größten Herausforderungen in der mittelfristigen Zukunft der Informationsverarbeitung bzw. -technologie. Klar ist, dass die zunehmende Komplexität beherrscht werden *muss*, will man weiterhin der rasanten Weiterentwicklung folgen können. Dementsprechend gibt es mittlerweile eine ganze Reihe von Projekten und Initiativen, die sich mit diesem Thema intensiv auf die verschiedensten Arten und Weisen beschäftigen und auseinandersetzen.

Beispielhaft hierfür kann man vor allem die sog. Grand-Challenge-Initiative der Gesellschaft für Informatik e.V. (GI) und der Informationstechnischen Gesellschaft (ITG) nennen, die im Jahre 2006 die Initiative „Grand Challenges der Technischen Informatik“ ins Leben gerufen hat[1]. Parallel dazu wurde vom BMBF das Forschungsförderprogramm IKT 2020 erarbeitet, das sich mit ähnlichen Themenbereichen beschäftigt[2].

Eine der acht (8) „Grand Challenges der Technischen Informatik“ ist als „Grand Challenge 4: Organic Computing Techniken“[3]. Die anderen Grand Challenges (GC) sind:

- GC 1: Omnipräsente Informationsverarbeitung
- GC 2: Zukünftige Kommunikationsnetze
- GC 3: Vertrauenswürdigkeit und Zuverlässigkeit
- GC 4: Organic Computing Techniken
- GC 5: Energieeffizienz, Umweltverträglichkeit und Nachhaltigkeit
- GC 6: HW-, SW-Architekturen und Werkzeuge für Multi-Core- und Many-Core-Prozessoren
- GC 7: Hardware-, Software-Architekturen und Werkzeuge für massiv parallele Systeme und GRID-Computer
- GC 8: Unkonventionelles Rechnen

Wenn man diese Aufstellung betrachtet, merkt man recht schnell, dass die Zukunft nicht nur vor der Tür steht, sondern bereits begonnen hat. Man gewinnt zudem den Eindruck, dass zeitlose Komponenten wie insb. die in der Grand Challenge 3 genannten Themen: Vertrauenswürdigkeit und Zuverlässigkeit in Gegenwart und Zukunft mindestens in dem gleichen wenn nicht noch höheren Maße gefordert sind wie in der Vergangenheit.

1.2. Konkretisierung der Fragestellung(en)

Alle der acht Grand Challenges sind für sich gesehen komplex und alle interoperieren in einer Art und Weise miteinander, dass das eine Thema

---

1 Einzelheiten sind in dem Dokument: „Grand Challenges der Technischen Informatik“ Report, März 08, der Gesellschaft für Informatik e.V. Fachausschuss 31/6.1 Informationstechnische Gesellschaft, dargestellt.

2 Siehe http://www.bmbf.de/pub/itk2020.pdf.

3 Siehe C. Müller-Schloer, H. Schmeck, U. Brinkschulte, F. Feldbusch, W. Trumler und Th. Ungerer, in: „Grand Challenges der Technischen Informatik“ Report, März 08, S. 31 ff.

ohne das andere letztlich unvollständig wäre. Im Ergebnis ist es so, dass zwar alle acht Grand Challenges für sich gelöst werden müssen, das aber nur im Sinne einer systemübergreifenden Lösung sinnvoll möglich ist. Das zeigt sich beispielhaft an dem Zusammenspiel der in GC 3 genannten Essentials: Vertrauenswürdigkeit und Zuverlässigkeit sowie dem in dieser Rechtsexpertise näher behandelten Komplex der in GC 4 behandelten Organic Computing Techniken, die einen guten Teil der adaptiven bzw. lernenden IT-Systeme ausmachen.

Ingesamt gesehen wird zudem deutlich, dass insb. die Fragen, die sich im Zuge sowie im Zusammenhang mit Organic Computing Techniken stellen, nicht nur reine Fragen der Informatik betreffen, sondern u.a. auch ethische Fragen aufwerfen, bis hin zu philosophisch ausgerichteten Fragestellungen wie z. B. der, ob es denn wirklich gewollt, gut und richtig ist, wenn über die herkömmlich bereits bestehenden Systeme mit den mittlerweise fast schon ubiquitär vorhandenen Man-Machine-Interfaces hinausgehend zukünftig tatsächlich Maschinen für Menschen nicht nur Arbeiten verrichten, sondern auch Gedankenüberlegungen anstellen und darauf basierend Entscheidungen treffen. Das ist möglich, wenn die Maschinen in Anlehnung bzw. Nachahmung menschlicher Gehirnprozesse programmiert werden, sodass sie im Ergebnis als Maschine für Menschen in der realen Umwelt Entscheidungen treffen (können) und sogar eigenkreativ Lösungsansätze für die Lösung unvorhergesehener Situationen in der realen Umwelt entwickeln (können). Schließlich sind mit dem Thema: Umsetzung von Organic Computing Techniken unmittelbar auch mikro- und makroökonomische Fragenbereiche angesprochen.

Das Feld ist also sehr weit und es würde den Rahmen dieser Rechtsexpertise bei Weitem sprengen, auf alle genannten Themenbereiche einzugehen. Diese Rechtsexpertise verfolgt daher (nur) das Ziel und beschränkt sich – soweit das möglich ist – darauf, den rechtlichen Rahmen für Organic Computing Techniken darzustellen. Innerhalb dieses Rahmens wird schwerpunktmäßig behandelt, welche Rechtsvorschriften im Zusammenhang mit den Organic Computing Techniken bzgl. der potenziellen Haftungsrisiken im Zusammenhang mit Organic Computing Techniken besondere Beachtung finden (müssen), sowie wie Organic Computing Techniken auszugestalten sind, damit sie den Anforderungen des bestehenden Rechtssystems in Deutschland Genüge tragen.

Im Zusammenhang mit diesen Themenbereichen werden insb. (auch) die folgenden Fragen behandelt:

- Wer ist für das Handeln und für mögliche Fehler eines selbst-organisierenden Systems verantwortlich[4]?
- Stößt das sog. Verursacherprinzip an seine Grenzen, wenn (= weil) das Verhalten organischer Computer auch von seinen Entwicklern systemimmanent *per definitionem* sowie aufgrund der Komplexität nicht vorhergesagt werden kann[5]?
- Wenn die Antwort auf die vorhergehenden Fragen ja ist: Braucht es dann nicht zwingend neuer gesetzlicher Regelungen für Organic Computing und wie sind diese ggf. auszugestalten[6]?

1.3. Organische Computersysteme

Die Besonderheit von Organischen Computersystemen gegenüber bestehenden herkömmlichen IT-Systemen lässt sich möglicherweise dadurch am Besten charakterisieren, dass (nur) die Organischen Computersysteme über sog. Self-X Eigenschaften verfügen. Unter diesem Begriff wird in dieser Rechtsexpertise verstanden, dass Organische Computersysteme Self-X-Eigenschaften in dem Sinne haben, dass sie

- selbst-konfigurierend
- selbst-optimierend,
- selbst-heilend,
- selbst-erklärend und
- selbst-schützend sind[7].

Organic Computing bedeutet damit im Extremfall, dass sich diese IT-Systeme selbst entwerfen – zumindest aber, dass sie sich zur Laufzeit anpassen (können)[8]. Die potenziellen Vorteile solcher Systeme bestehen darin, dass Systeme, die sich zur Laufzeit in der realen Umwelt an sich (ver)ändernde Gegebenheiten anpassen (können), mit klassischen Methoden nicht möglich sind, sowie dass die Umsetzung dieser Fähigkeit(en) wohl maximale Effizienz sowohl im Entwicklungsprozess bedeu-

---

4 S.u. 2.6.

5 S.u. 2.6.

6 S.u. 3 und 4.

7 C. Müller-Schloer, Organic Computing, Informatik Spektrum, 04, S. 332.

8 Siehe C. Müller-Schloer, H. Schmeck, U. Brinkschulte, F. Feldbusch, W. Trumler und Th. Ungerer, in: „Grand Challenges der Technischen Informatik“ Report, März 2008, S. 33.

ten kann als auch im aktuellen Lebensverfahren. Die potenziellen Nachteile bestehen darin, dass das systemimmanente Merkmal der sog. Emergenz, d.h. der Unvorhersehbarkeit einer bestimmten Handlung in einer bestimmten Situation zwar vom System selbst her durchaus erwünscht im Sinne von gewollt ist[9], dies aber äußerst problematisch ist bzgl. der damit aufgeworfenen Fragen der Haftung für das Verhalten dieser Systeme.

1.4. Anwendungsbeispiel: Elektronik im Kfz (Embedded Systems)

In dieser Rechtsexpertise dient das vielfach auch in der Fachliteratur zu Organic Computing gebrauchte Beispiel eines Embedded System im Kraftfahrzeug als Anwendungsbeispiel. Dabei wird bzgl. der in einem solchen System involvierten Hardware und Software einheitlich der Begriff: IT-System verwendet. Unter dem Begriff: Embedded System wird die Gesamtheit eines (1) Steuergeräts/ECU (Electronic Controller Unit) verstanden, bestehend aus allen dazugehörigen Komponenten (Hardware, Software, Betriebssystemsoftware, Applikationssoftware, Middleware, Firmware, sowie der jeweiligen Compiler/Linker-Kombination für ein bestimmtes Derivat eines bestimmten Mikroprozessors, etc.).

Heutzutage sind (rein) adaptive Systeme u.a. als Fahrerassistenzsysteme[10] im Kraftfahrzeug implementiert. Ein typisches Anwendungsbeispiel für ein adaptives IT-System ist die sog. Adaptive Cruise Control, bei der das Fahrzeug die gewählte Geschwindigkeit u.a. selbstständig abbremst, wenn in einem definierten Bereich Gegenstände auftreten, also z. B. ein Fahrzeug die Spur so wechselt, dass es in den definierten Bereich kommt. In der Praxis sind in einem Kfz heutzutage je nach Anwendungsklasse teilweise über 100 elektronische Steuergeräte enthalten. Diese sind über ein Bussystem miteinander verbunden und kommunizieren über dieses System. Zukünftig sollen diese IT-Systeme darüber hinaus mit anderen Systemen in anderen Fahrzeugen kommunizieren (Car2Car) sowie generell mit anderen IT-Systemen in der Umwelt.

1.4.1. Vertragliche Konstruktion in der Praxis

Die vertragliche Konstellation ist in der Praxis regelmäßig so, dass ein TIER1-Zulieferer als Systemintegrator gegenüber dem OEM[11] auftritt.

---

9 Siehe C. Müller-Schloer, H. Schmeck, U. Brinkschulte, F. Feldbusch, W. Trumler und Th. Ungerer, in: „Grand Challenges der Technischen Informatik“ Report, März 2008, S. 34.

10 Vgl. zur Haftung für softwarebezogenen Funktionen bei Fahrerassistenzsystemen auch Meyer/Harland, CR 07, 689 ff., die aber auf die besondere Problematik, die sich durch die adaptive Wirkung ergibt, nicht weiter eingehen.

11 OEM = Original Equipment Manufacturer.

Der Systemintegrator liefert dabei regelmäßig eigene Komponenten für das Steuergerät und besorgt beim Chip-Hersteller (TIER 2) den Mikroprozessor. Der Systemintegrator besorgt ferner von einem Softwareherstellen gängige Betriebssystemsoftware, sowie ggf. von diesem oder auch einem oder mehreren weiteren Softwareherstellern Applikations- und/oder andere Software. Es entsteht hierbei ein Geflecht unterschiedlicher vertraglicher Beziehungen zwischen den Beteiligten.

1.4.2. Potenzielle Folge bei Fehler: Rückrufaktion

Wenn in dem im Kfz bereits verbauten Steuergerät ein Fehler entdeckt wird und wenn die betreffenden Fahrzeuge bereits in Serie gefertigt wurden und im Feld sind und wenn bei Realisierung des Fehlers Personen- bzw. Körperschäden drohen, liegt eine Rückrufsituation für den OEM vor. Der OEM kann und wird von demjenigen, der letztlich verantwortlich für den Fehler und damit für den eingetretenen Schaden ist, im Wege des Regresses Ersatz der ihm entstandenen unmittelbaren und mittelbaren Schäden aus einer (erfolgten) Rückrufaktion verlangen. Ist der Fehler zwei oder mehreren Beteiligten in dem Vertragskonstrukt zurechenbar oder von beiden oder mehreren mitursächlich verursacht, z. B. wenn der Programmfehler relativ eindeutig ursächlich in der Betriebssystemsoftware liegt, dieser Fehler aber relativ deutlich bei den erforderlichen und angemessenen Tests vor Serienfertigung hätte erkannt werden können und damit müssen, und zwar vom Systemintegrator, ggf. im Verbund mit dem Softwarehaus, das die Betriebssystemsoftware hergestellt hat, sowie sodann (auch) vom OEM, der ja in jedem Fall auch noch einmal vor Serienfertigung die Gesamtkommunikation der einzelnen Steuergeräte prüfen muss, dann wird der Fehler letztlich im Verhältnis der Mitverursachungs- bzw. Mitverschuldensbeiträge der verschiedenen Beteiligten aufgeteilt.

Die Kosten einer Rückrufaktion können von einem Unternehmen der mittelständischen Industrie wirtschaftlich in der Regel nicht getragen werden. Die Eintrittswahrscheinlichkeit einer Rückrufaktion nimmt in dem Maße zu, in dem die zugelieferten Software-Komponenten in sicherheitskritischen Anwendungen wie z. B. Bremssysteme, Airbagsteuerung, o. Ä verbaut sind. Für die Entwicklung der zugrunde liegenden Technologien und die Lieferung der Produkte für die Serienfertigung müssen deshalb im Interesse aller Beteiligten besonders hohe Anforderungen sowohl an den Entwicklungsprozess als auch an das fertige Produkt gestellt werden. So muss beispielsweise im Interesse der Sicherheit der Allgemeinheit sichergestellt sein, dass der Airbag dann auslöst, wenn er auslösen *muss* und dann nicht auslösen *darf*, wenn das nicht der Fall ist. Bei einem Multimedia-System muss sichergestellt sein, dass es zu keinem Zeitpunkt, auch nicht bei plötzlich aufkommendem starkem Fremdlärm unerwartet auf absolute Höchstlautstärke schaltet.

1.4.3. Möglichkeiten mit Organic Computing Techniken

Anwendungen wie Adaptive Cruise Control oder Airbagsteuerung sind heute weit verbreitet. Ein System basierend auf Organic Computing Techniken würde es über solche Anwendungsbeispiele hinausgehend z. B. ermöglichen, dass Ampelsteuerungen komplett maschinell in Abhängigkeit von sich permanent ändernder Verkehrsparameter ausgestaltet werden könnten. Es wären weiterhin komplette selbstorganisierende Verkehrslenkungen im übergeordneten Sinne denkbar, d.h. Kommunikation zwischen Systemelementen im Fahrzeug selbst, z. B. Reaktion auf plötzlich auftretendes sehr starkes Gewitter mit der Folge der Überflutung eines bestimmten Straßenbereichs, was dazu führt, dass die ABS-Systeme und weitere Sicherheitssysteme in jedem Auto, das sich im Umfeld x dieses Gefahrenbereichs befindet, aktiviert werden oder sich im Hinblick auf die geänderte Situation konfigurieren können. Zusätzlich könnte dieser Umstand evtl. auch über die Kommunikations- und Navigationssysteme zwischen den einzelnen Fahrzeugen ausgetauscht werden (Car2Car Communication), und die Systeme könnten selbstständig dafür sorgen, dass der Verkehr systemübergreifend von der Gefahrenstelle weggelenkt wird, bis die Gefahr beseitigt ist. Dazu könnten z. B. die Ampeln, die zur Verkehrsstelle hinführen, längere Rotphasen haben, um den potenziellen Stau abzufedern, bis die Gefahr vorüber ist.

Dazu bedarf es komplexer Systeme, die mannigfaltige Kombinationen und Möglichkeiten eröffnen. Daraus folgt (fast schon) zwingend, dass die Auswahl der Möglichkeiten gezielt erfolgen muss und im Prinzip zu jedem Zeitpunkt überwacht und kontrolliert werden muss, da die Systeme sich jederzeit selbst fortschreiben können und das dann auch können müssen, z. B. um ein plötzlich auftretendes Schlagloch reagieren zu können, das gestern noch nicht vorhanden war.

Dazu bedarf es der genannten Self-X-Eigenschaften. “Organic Computing" will die Fähigkeit der Selbstorganisation mit den dazu gehörenden Eigenschaften der Selbstkonfiguration, Selbstoptimierung, Selbstheilung und des Selbstschutzes in realen Computersystemen anwenden. Zusätzlich sollen sich diese organischen Computersysteme an wechselnde Umweltbedingungen flexibel anpassen können und durch ihr Zusammenwirken emergentes Verhalten zeigen[12].

2. Haftungsrecht bzgl. IT-Produkte, insb. Software

Für IT-Produkte, insb. Software, gelten in Deutschland bzgl. der Haftung die allgemeinen rechtlichen Regelungen, und zwar auch bzgl. der Pro-

---

[12] S.o. 1.3.

dukthaftung. Bzgl. des Urheberrechts ist in das Urheberrechtsgesetz (UrhG) 1993 ein sog. Besonderer Abschnitt für Computerprogramme eingefügt worden (§§ 69a ff.), ergänzend gelten die allgemeinen Regelungen des UrhG. Das Urheberrecht regelt, wer die Rechtsherrschaft über die Software hat, wer also v.a. über die Vervielfältigung, Verarbeitung der Software entscheiden kann, § 69 c UrhG. Urheberrechtliche Fragen haben bzgl. der Haftung letztlich keine Relevanz. Sie haben aber möglicherweise Auswirkungen bzgl. der Frage, ob bzw. wer genau haftet, wenn das System sich selbst fortschreibt bzw. sich selbst den sich ändernden Parametern anpasst[13].

2.1. Haftungsrechtliche Grundlagen

Dem Schutzzweck: Sicherheit der körperlichen Integrität der Allgemeinheit dienen zahlreiche in Deutschland geltende Gesetze, insb. das Produkthaftungsgesetz (ProdHG), aber auch u. a. die Vorschriften aus dem Besonderen Teil des Bürgerlichen Gesetzbuchs über die sog. unerlaubten Handlungen (§§ 823 ff. BGB). Während das ProdHG die Verantwortlichkeit für Fehler eines in den Verkehr gebrachten Produkts bei Körper-, Gesundheitsschäden oder Sachschäden an anderen Produkten als dem Produkt selbst unabhängig von einem Verschulden des Herstellers regelt, greift die gesetzliche Haftung nach dem BGB nur bei einem Verschulden des Herstellers ein und zielt (daher) mehr auf den Herstellungsprozess ab.

Es ist derzeit nicht geklärt, ob und wann Software überhaupt ein Produkt im Rechtssinne, insb. i. S. d. ProdHG ist bzw. als solches eingestuft werden kann. In einigen Konstellationen wird man das wohl mit hoher Wahrscheinlichkeit annehmen müssen, in anderen kann das eher fraglich sein[14]. Aufgrund des überragend wichtigen Schutzzwecks des ProdHG: Sicherheit der Allgemeinheit wird man aber wohl jedenfalls bei als Standardsoftware in den Verkehr gebrachten Software-Produkten die Anwendbarkeit des ProdHG im Ergebnis kaum ablehnen können. Die Frage ist damit eher, ob dieses Ergebnis ggf. für Software basierend auf Organic Computing Techniken eine andere Betrachtung finden muss als bei „herkömmlicher“ Software.

---

[13] S.o. Ziffer 1.3 (Self-X-Eigenschaften) sowie unten Ziffer 2.7 konkret zu dieser Frage.

[14] Dieses Thema wird insgesamt unter Ziffer 2.3.3 näher ausgeführt.

2.2. Haftung nach dem ProdHG: Produkthaftung

Die Haftung des Herstellers nach dem ProdHG ist dann (und nur dann) ausgeschlossen, wenn:

(i) der Hersteller das Produkt nicht in den Verkehr gebracht hat (§ 1 Abs. 2 Nr. 1 ProdHG),

(ii) nach den Umständen davon auszugehen ist, dass das Produkt den Fehler, der den Schaden verursacht hat, noch nicht hatte, als der Hersteller es in den Verkehr gebracht hatte (§ 1 Abs. 2 Nr. 2 ProdHG),

(iii) der Hersteller das Produkt weder für den Verkauf oder eine andere Form des Vertriebs mit wirtschaftlichem Zweck hergestellt noch im Rahmen seiner beruflichen Tätigkeit hergestellt oder vertrieben hat (§ 1 Abs. 2 Nr. 3 ProdHG),

(iv) der Fehler darauf beruht, dass das Produkt in dem Zeitpunkt, in dem der Hersteller es in den Verkehr brachte, dazu zwingenden Rechtsvorschriften entsprochen hat (§ 1 Abs. 2 Nr. 4 ProdHG), oder

(v) wenn der Fehler nach dem Stand der Wissenschaft und Technik in dem Zeitpunkt, in dem der Hersteller das Produkt in den Verkehr brachte, nicht erkannt werden konnte (§ 1 Abs. 2 Nr. 5 ProdHG).

Es kommt also zunächst einmal darauf an, ob bzw. unter welchen Voraussetzungen ein Fehler i. S. d. ProdHG vorliegt.

Diese Frage ist in § 3 Abs. 1 ProdHG geregelt. Dort heißt es, ein Produkt ist fehlerhaft, wenn es

> „[…] nicht die Sicherheit bietet, die unter Berücksichtigung aller Umstände, insbesondere
>
> a) seiner Darbietung,
> b) des Gebrauchs, mit dem billigerweise gerechnet werden kann, sowie
> c) des Zeitpunkts, in dem es in den Verkehr gebracht wurde,
>
> berechtigterweise erwartet werden kann.“

Die gesetzliche Produkthaftung betrifft damit die Sicherheit des Produkts, wie sie die Allgemeinheit erwarten darf[15], während die vertragliche Mängelhaftung[16] die Gebrauchs-, Funktionsfähigkeit und den Wert einer Sache betrifft, wie sie der Erwerber aufgrund eines abgeschlossenen Vertrags erwarten darf. Schutzgut der vertraglichen Mängelhaftung ist mithin in erster Linie (auch) das wirtschaftliche Nutzungs- und Äquivalenzinteresse des Vertragspartners im Hinblick darauf, dass die Sache keine Mängel aufweist, die im Hinblick auf die erbrachte Gegenleistung ihren Wert und/oder ihre vertraglich vorgesehene Gebrauchsfähigkeit beeinträchtigen. Dagegen schützt die gesetzliche Produkthaftung – ebenso wie die öffentlich-rechtlichen Produktsicherheitsvorschriften wie z. B. das Geräte- und Produktsicherheitsgesetz (GPSG) –, das *Integritätsinteresse* jedes Benutzers und Dritten daran, dass die Sache diejenige Sicherheit für Leben, Gesundheit und Sachwerte bietet, die allgemein berechtigterweise erwartet werden kann[17]. In dieser Expertise geht es (nur) um Fragen der Sicherheit.

Im Folgenden wird zunächst die bekannte Rechtsprechung und ansatzweise Literatur zu § 3 ProdHG dargestellt. Anschließend wird auf die Frage eingegangen, ob bzw. ggf. welche Besonderheiten bzgl. adaptiven IT-Systemen ggf. notwendig sind und/oder zumindest geboten erscheinen – oder ob evtl. im Gegenteil gerade keine Besonderheiten bestehen, die eine differenzierte Betrachtungsweise und verschiedene Ergebnisse erfordern.

2.2.1. Sicherheit als Maßstab für Produktfehler

Ein i. S. d. ProdHG fehlerfreies Produkt muss bzgl. seiner Konstruktion und Herstellung/Fabrikation sowie ggf. Instruktion so beschaffen sein, dass es die körperliche Unversehrtheit des Benutzers oder eines Dritten nicht beeinträchtigt und sein sonstiges (d.h. außer der Sache selbst) privates Eigentum nicht beschädigt (vgl. § 1 Abs. 1 ProdHG).

Maßstab hierfür ist gem. § 3 ProdHG die berechtigte Erwartung bzgl. <u>aller Umstände</u>, wobei das Gesetz selbst in § 3 ProdHG insb. nach der Darbietung und dem Gebrauch, mit dem billigerweise gerechnet werden kann, im maßgeblichen Zeitpunkt des Inverkehrbringens unterscheidet.

---

15 Sprau, in Palandt, Bürgerliches Gesetzbuch, 68. Aufl. 09, Rdnr. 1 zu § 3 ProdhaftG.

16 Dazu unten 2.5.

17 BGH, Urteil vom 16.06.09, Az. VI ZR 107/08, Rdnr 15 „Airbag“; ausführlich BGH, Urteil vom 17.03.09, Az. VI ZR 176/08, Rdnr. 6 „Kirschtaler“; Sprau, in Palandt, Bürgerliches Gesetzbuch, 68. Aufl. 09, Rdnr. 1 zu § 3 ProdhaftG, m.w.N., insb. BGH NJW 85, 2420, BGHZ 86, 256.

2.2.2. Berechtigte Erwartung

Nach dem ausdrücklichen Wortlaut des Gesetzes ist nicht auf die subjektive Erwartung des jeweiligen Benutzers abzustellen, sondern auf die *objektive Erwartung*, ob das Produkt diejenige Sicherheit bietet, die die Allgemeinheit nach der Verkehrsauffassung in dem entsprechenden Bereich für erforderlich hält[18]. Dass bestimmte Benutzergruppen möglicherweise ein unterschiedliches Risiko- und Gefahrenbewusstsein haben bzw. dass dieses möglicherweise generell unter den Menschen nicht einheitlich ist, steht dem nicht entgegen. Vielmehr ergibt sich ja gerade aus dieser Überlegung heraus, dass ein objektiver Maßstabe gerade wegen des Schutzzwecks: Sicherheit der Allgemeinheit gelten muss.

Es kommt also nicht auf die subjektiven Sicherheitserwartungen des konkret Geschädigten an das Produkt an. Ungeachtet dessen sind in erster Linie die Sicherheitserwartungen des Personenkreises maßgeblich, an den sich der Hersteller mit seinem Produkt wendet[19]. Da der Schutzbereich der Haftung nach dem Produkthaftungsgesetz aber nicht auf die Erwerber oder Nutzer von Produkten beschränkt ist, sondern auch unbeteiligte Dritte einschließt, sind dabei nicht nur die Sicherheitserwartungen des Adressatenkreises des vermarkteten Produkts zu berücksichtigen, sondern darüber hinaus auch das Schutzniveau, welches Dritte berechtigterweise erwarten können, sofern sie mit der Sache in Berührung kommen[20]. Maßgeblich ist also der Sicherheitsstandard, den die in dem entsprechenden Bereich herrschende Verkehrsauffassung für erforderlich hält[21]. Ist ein Produkt für den Endverbraucher bestimmt, muss es z. B. erhöhten Sicherheitsanforderungen genügen, die auf Wissen und Gefahrsteuerungspotential des durchschnittlichen Konsumenten Rücksicht nehmen[22].

Die Haftung des Herstellers erweitert sich gegenüber den allgemeinen Maßstäben dann, wenn seine Produkte an Risikogruppen vertrieben werden bzw. diese typischerweise gefährden. Dementsprechend bestimmt Art. 2 lit. b der Produktsicherheitsrichtlinie 2001/95 EG[23], dass die

---

18 Sprau, in Palandt, Bürgerliches Gesetzbuch, 68. Aufl. 09, Rdnr. 2 zu § 3 ProdhaftG, unter zutreffendem Hinweis auf die Gesetzesformulierung: „erwartet werden kann“, die den objektiven Maßstab setzt, sowie m.w.N.

19 BGH, Urteil vom 17.03.09, Az. VI ZR 176/08, Rdnr. 6 „Kirschtaler“ mw.N. aus der Literatur.

20 BGH, Urteil vom 17.03.09, Az. VI ZR 176/08, Rdnr. 6 „Kirschtaler“ m.w.N. aus der Literatur.

21 BGH, Urteil vom 17.03.09, Az. VI ZR 176/08, Rdnr. 6 „Kirschtaler“ mit Verweis auf BGH, Urteil vom 16.02.72 Az. VI ZR 111/70, VersR 72, 559, 560.

22 BGH, Urteil vom 17.03.09, Az. VI ZR 176/08, Rdnr. 6 „Kirschtaler“ mit Verweis auf Schmidt-Salzer/Hollmann, Kommentar EG-Richtlinie Produkthaftung, 2. Aufl., Bd. 1, Art. 6 Rdnr. 122.

23 ABl. EG L 11 vom 15..01.02, S. 4.

Produktsicherheit auch von den Erwartungen solcher Produktbenutzer abhängt, die bei der Verwendung des Produkts einem erhöhten Risiko ausgesetzt sind. Wird ein Produkt mehreren Adressatenkreisen dargeboten, hat sich der Hersteller an der am wenigsten informierten und zur Gefahrsteuerung wenigsten kompetenten Gruppe zu orientieren, d.h. der Hersteller hat den jeweils höchsten Sicherheitsstandard zu gewährleisten[24]. An dieser Stelle kann man äußerst zweischneidige weitergehende Überlegungen gerade bzgl. adaptiver IT-Systeme, insb. lernender Systeme anstellen, wenn man sich hierzu die folgenden von der Rechtsprechung entschiedenen Fälle vor Augen führt:

- Konstruktive Maßnahmen zur Beseitigung von Produktgefahren müssen dann nicht getroffen werden, wenn die Benutzer dies im Bewusstsein der bestehenden konkreten Gefahr nicht für erforderlich halten[25].
- Die Sicherheitserwartung muss berechtigt sein, d.h. die Allgemeinheit kann nicht von jedem Produkt in jeder Situation totale Sicherheit erwarten[26].

Nach der Literatur liegt in derartigen Fällen letztlich eine durch den Richter zu entscheidende Wertungsfrage vor, für die § 3 Abs. 1 ProdHG die maßgeblichen Kriterien aufstellt[27]. Dabei wird man unter Berücksichtigung des Spielraums, der bei Wertungsfragen kraft Natur der Sache eröffnet ist, unter Anwendung des maßgeblichen objektiven Maßstabs gem. § 3 ProdHG etwa Folgendes sagen können:

- Auch wenn die im ersten Unterpunkt genannten zwei entschiedenen Fälle: Autoscooter und Pferdebox nicht wirklich vergleichbar sind mit dem Fall lernender IT-Systeme, so zeigen die Entscheidungen doch, dass bestimmte Einschränkungen jedenfalls bzgl. des *konkreten Anwendungsbereichs* durchaus möglich sind. Allerdings ist die Produktsicherheit hierdurch als solche wohl eher nicht betroffen, sondern eben (nur) der konkrete Anwendungsbereich. Auf den Fall lernender IT-Systeme übertragen würde das aber ungeachtet dessen bedeuteten, dass die Anwendung in einem bestimmten überschaubaren Bereich, also z. B. des Einsatzes eines automatischen Autoscooters innerhalb eines festen Autoscooter-Systems zulässig

---

24 BGH, Urteil vom 17.03.09, Az. VI ZR 176/08, Rdnr. 7 „Kirschtaler“ mit Verweis auf Foerste in: v. Westphalen, Produkthaftungshandbuch, 2. Aufl., Bd. 2, § 74, Rdnr. 46.

25 BGH VersR 77, 334: Autoscooter, BGH NJW 90, 906: Pferdebox.

26 OLG Düsseldorf, NJW-RR 08, 411: keine absolute Giftfreiheit von Naturdünger.

27 Sprau, in Palandt, Bürgerliches Gesetzbuch, 68. Aufl. 09, Rdnr. 3 zu § 3 ProdhaftG.

ist, wenn (= weil) in diesem überschaubaren Bereich die Produktsicherheit für die Benutzer und Dritte gewährleistet ist. Umgekehrt wäre aber die Fahrt des Autoscooters etwa als Beförderungssystem für bedürftige Rollstuhlfahrer, die im Prinzip ja keine vom ersten Anwendungsbeispiel abweichende andere Systemprogrammierung erfordert, außer dass das System eben nun unbegrenzt ist statt begrenzt, vor dem Hintergrund mangelnder Produktsicherheit in genau diesem Umfeld bzw. genau diesem Anwendungsbeispiel wohl unzulässig.

- In dem im zweiten Unterpunkt genannten Beispiel – keine absolute Giftfreiheit von Naturdünger – hat die Rechtsprechung formuliert: „[…] nicht von jedem Produkt kann in jeder Situation totale Sicherheit erwartet werden“.

  Ließe sich dieser Satz in dieser Form so allgemeingültig abstrahieren, wären damit – vorsichtig ausgedrückt – lernende Systeme möglicherweise dann legitimiert, wenn sie bestimmte Mindestsicherheitsvorkehrungen einhalten, sowie darüber hinaus bestimmte Super-GAU-Szenarien praktisch *per definitionem* bzw. *a priori* verhindert wären. Die (Rechts-)Frage ist aber, ob bzw. inwieweit dieser Satz sich verallgemeinern lässt, sowie insb. ob das auch bzgl. Organic Computing Techniken so gilt. Diese beiden Themen werden unter Ziffer 4.1 behandelt.

2.2.3. Berücksichtigung aller Umstände

Gem. § 3 ProdHG sind bzgl. der berechtigten Sicherheitserwartungen der Allgemeinheit *alle Umstände* zu berücksichtigen. Als Beispiele für alle Umstände nennt das Gesetz den Gebrauch und die Darbietung des Produkts.

2.2.3.1. Darbietung

Darbietung i. S. d. § 3 ProdHG ist jede Tätigkeit, durch die der Hersteller oder mit seiner Billigung ein Dritter das Produkt der Allgemeinheit, darunter auch dem jeweiligen Benutzer, vorstellt[28]. Hierunter fallen ganz allgemein die Produktbeschreibung, die Gebrauchsanweisung, die Verpackung und Ausstattung, aber auch produktbezogene Merkmale wie Gütezeichen bis hin zu konkret anwendungsbezogenen Merkmalen wie z. B. Hinweise auf besondere, auch gefährliche Eigenschaften.

[28] Sprau, in Palandt, Bürgerliches Gesetzbuch, 68. Aufl. 09, Rdnr. 5 zu § 3 ProdhaftG.

Es ist gesicherte Erkenntnis, dass ein Instruktionsfehler im Rechtssinne vorliegt, insb. auch i. S. d. ProdHG, wenn die erforderliche Aufklärung entweder gänzlich fehlt[29], oder lückenhaft ist oder unrichtig[30]. Weiter gesichert ist die Erkenntnis, dass auch die Werbung, allerdings unter Berücksichtigung gewisser Übertreibungen, mit denen die Allgemeinheit rechnet („verleiht Flügel"), den Erwartungshorizont bgl. der Produktsicherheit – um die es hierbei letztlich allein geht –, beeinflussen kann. Es müssen bzgl. der Darbietung auf jeden Fall alle erforderlichen Hinweise auf gefährliche Eigenschaften gegeben werden. Dabei gilt: Je größer die Gefahr ist, desto höher sind die Anforderungen, die in dieser Hinsicht gestellt werden müssen[31]. Hier sind sicherlich Wechselwirkungen mit dem allgemeinen Problem der Verlässlichkeit und der Vertrauenshaltung der Allgemeinheit gegeben. Ist durch ein Produkt die Gesundheit oder die körperliche Unversehrtheit von Menschen bedroht, ist schon dann eine Warnung auszusprechen, wenn aufgrund eines ernstzunehmenden Verdachts zu befürchten ist, dass Gesundheitsschäden entstehen können[32]. Soweit Organic Computing Systeme in dem Sinne risikobehaftet sind, dass nicht sicher ausgeschlossen werden kann, dass diese sich auch in einer schadensstiftenden Weise (weiter)entwickeln *können*, müssen deshalb jedenfalls bzgl. der dann drohenden Gesundheitsgefahren entsprechende Warnungen ausgesprochen werden.

2.2.3.2. Gebrauch, mit dem billigerweise gerechnet werden kann

Als weitere Konkretisierung der Kriterien zur Ausfüllung der Berücksichtigung aller Umstände sieht das ProdHG in § 3 vor, dass ein Produkt dann fehlerhaft i. S. d. ProdHG ist, wenn es nicht die Sicherheit bietet, die unter Berücksichtigung aller Umstände berechtigterweise unter Berücksichtigung des *Gebrauchs, mit dem billigerweise gerechnet werden kann*, erwartet werden kann.

Gemeint ist hiermit der sog. bestimmungsgemäße Gebrauch[33]. Dieser ergibt sich aus Art und Wesen des Produkts sowie aus der Zweckbestimmung, die ihm der Hersteller in Beschreibungen und Gebrauchsan-

---

29 Z. B. über das Risiko des Fehlauslösen von Airbags, BGH, Urteil vom 16.06.20, Az. VI ZR 107/08, Rdnr. 24 „Airbag".

30 BGH NJW 99, 2815: Es ist nahe liegend, dass der Verwender des Produkts Unfallverhütungs-Vorschriften zum Umgang mit dem Produkt nicht beachtet. Der Hersteller muss daher auf die Gefahren hinweisen, die bei Nichtbeachtung der Vorschriften entstehen.

31 BGH, Urteil vom 16.06.09, Az. VI ZR 107/08, Rdnr. 24 „Airbag" m.w.N.

32 BGH, Urteil vom 16.06.09, Az. VI ZR 107/08, Rdnr. 24 „Airbag" m.w.N.

33 BGHZ 51, 91.

weisungen gegeben hat[34]. Diese Umschreibung des bestimmungsgemäßen Gebrauchs ist interessant, erlaubt sie doch ganz generell die Einschränkung auf bestimmte Anwendungsbereiche sowie ggf. dann auch Einschränkungen des Gebrauchs innerhalb dieser Anwendungsbereiche. Damit diese Umgrenzung aber nicht ausufert bzw. umgekehrt betrachtet ggf. grenzenlos eingeschränkt werden kann, z. B. in Benutzerdokumentation oder sonstigen Programmbeschreibungen, Dokumenten und/oder Unterlagen, ist es gesicherte Rechtsprechung, dass sowohl die Herstellung als auch die Instruktion darüber hinaus auch auf den über die Zweckbestimmung hinausgehenden üblichen Gebrauch abstellen müssen sowie auch auf nicht ganz fernliegende versehentliche Fehlanwendungen[35].

Diese Ansicht ist nicht unumstritten in der Literatur[36]. Der Kritik hieran ist sicherlich zuzugeben, dass die Bestimmung, was (noch) als nicht ganz fernliegende sowie noch dazu versehentliche Fehlanwendung eingestuft werden kann und was darunter (nicht) mehr zu fassen ist, äußerst schwierig ist, zumal der Begriff: versehentlich schon für sich gesehen auslegungsfähig – da immer eine bestimmte konkrete Situation betreffend – und (daher) auch auslegungsbedürftig ist. Gerade bei lernenden Systemen, deren Zweckbestimmung ja gerade darin besteht, Entscheidungen in Abhängigkeit von sich ändernden Situationen treffen zu können bzw. sogar zu sollen, ist die Wahrscheinlichkeit einer nicht ganz fernliegenden *und* versehentlichen Fehlanwendung sehr hoch.

Dazu kommt ggf. als zusätzliches Problem, dass ein Nutzer aufgrund der Funktionalität von OC Systemen, die sich ja gerade an unvorhergesehene Situationen anpassen sollen, evtl. durch diese Eigenschaft gerade dazu verleitet werden kann, OC Systeme außerhalb ihres vorgesehenen Einwendungsgebiets einzusetzen. Daher sind hier jedenfalls in beide genannten Richtungen Warnhinweise erforderlich[37].

Das bei OC Techniken weiter hinzutretende Sonderproblem, dass das lernende System sich zur Laufzeit selbstständig weiter entwickelt, wird unter dem Gesichtspunkt der Zurechnung bzw. Zurechenbarkeit dieses Anwendungsverhaltens behandelt[38].

---

34 Sprau, in Palandt, Bürgerliches Gesetzbuch, 68. Aufl. 09, Rdnr. 6 zu § 3 ProdhaftG.

35 BGHZ 116, 60 = NJW 92, 560; BGH NJW 99, 2815: Es ist nahe liegend, dass der Verwender des Produkts Unfallverhütungs-Vorschriften zum Umgang mit dem Produkt nicht beachtet. Der Hersteller muss daher auf die Gefahren hinweisen, die bei Nichtbeachtung der Vorschriften entstehen.

36 Kritisch hierzu z. B. Möllers VersR 00, 1177 m.w.N.

37 S.o. 2.2.3.1.

38 S.u. 2.7 und 2.7.3.

Bzgl. OC Systemen ist vor allem problematisch, wie der sog. bestimmungsgemäße Gebrauch festzulegen ist. Denn es entspricht gesicherter Rechtsprechung, dass mit einem missbräuchlichen, völlig zweckfremden Gebrauch billigerweise nicht gerechnet werden muss[39]. Der dieser Entscheidung zugrunde liegende Sachverhalt: Verwendung eines technischen Lösungsmittels als Inhalierungsrauschgift zeigt das Spannungsfeld recht gut auf: Gerade eine derartige Anwendung wäre für eine programmierte, emotionslose Maschine, so sie denn ein Verständnis von Rauschzustand durch Programmierung implementiert bekommen hat, wohl eher sehr kreativ und damit aus lerntechnischer Sicht eine Herausforderung, die eher an vorderer Stelle stehen müsste denn an hinterer. Es wäre dann eine Frage des Reward-Systems innerhalb des lernenden Systems, wie das System diesen Fall bewertet.

Ungeachtet dessen kann man aber auch argumentieren, es sei gerade der bestimmungemäße Gebrauch des OC-Systems, unvorhergesehene Anwendungen vorzunehmen oder – etwas pointierter ausgedrückt –, es gehöre (eben auch) zum bestimmungsgemäßen Gebrauch von OC Systemen, dass diese auch für *nicht* bestimmungsgemäßen Gebrauch einsetzbar seien, weil OC Systeme sich ja gerade auch daran anpassen können. In jedem Fall müssen, um die Anforderungen des Gesetzes zu erfüllen, die potenziell gefährlichen Anwendungen von Vornherein aussortiert werden, d.h. sie dürfen in den Lernprozess im Sinne einer *conditio sine qua non* gar nicht erst aufgenommen werden, sondern gewissermaßen *a priori* verboten sein. Denn wenn (auch nur) die (relativ konkrete) Gefahr besteht, dass das System selbstständig potenziell gefährliche Situationen nicht meistern kann, bietet dieses konkrete lernende System nicht die nach dem ProdHG erforderliche Sicherheit.

2.2.4. Gesamte objektive Umstände

Die berechtigten Sicherheitserwartungen der Allgemeinheit sind nach dem ausdrücklichen und unmissverständlichen Gesetzeswortlaut „insbesondere“ an der Darbietung und dem Gebrauch, mit dem billigerweise gerechnet werden kann, zu messen, darüber hinaus an den *gesamten objektiven Umständen des konkreten Schadensfalles*[40].

2.2.4.1. Objektiver Umstand: Natur der Sache

Die Natur der Sache lässt Rückschlüsse auf den Erwartungshorizont zu. Gefahren, die typischerweise

---

39 BGH NJW 81, 2514: techn. Lösungsmittel als Inhalierungsrauschgift.

40 Sprau, in Palandt, Bürgerliches Gesetzbuch, 68. Aufl. 09, Rdnr. 4 zu § 3 ProdhaftG.

- mit der Benutzung eines Produkts verbunden sind,
- die dem Verbraucher bekannt sind,
- und die von dem Verbraucher in Kauf genommen werden,

braucht der Hersteller nicht abzuwenden.

Das gilt z. B. für die Gesundheitsgefahren beim Konsum von Zigaretten[41]. Damit kommen wir zum Kern der Sache. Denn genau diese Fragestellungen sind gerade im Hinblick auf adaptive Software bzw. lernende IT-Systeme hoch brisant. Hier könnte man ja argumentieren, dass gerade die Natur der Sache eben genau die Rückschlüsse auf den Erwartungshorizont zulässt. D.h. dass bestimmte Gefahren bzw. Gefährdungen genau eintreten können, was ja genau auch typischerweise mit der Benutzung des Produkts verbunden ist, sowie dem Verbraucher auch bekannt ist – vorausgesetzt es wird dem Verbraucher hinreichend bekannt was aber ein geringes Problem darstellen sollte –, und was genau unter diesen Voraussetzungen dann von dem Verbraucher, und das ist der springende Punkt, auch *in Kauf genommen* werden würde.

Letzteres ist bei lernenden IT-Systemen indessen äußerst problematisch. Denn hier liegt wohl eine Besonderheit vor, die lernende IT-Systeme gerade auch von rein adaptiven IT-System unterscheidet, nämlich die systemimmanente gewollte Eigenschaft der Emergenz, d.h. dass nicht mit Sicherheit vorhergesagt werden kann, welche Handlung in einer bestimmten Situation vorgenommen wird. Dass der Verbraucher hierein eingewilligt hätte, wird man jedenfalls wohl *im Nachhinein*, also wenn der Schaden eingetreten ist, nicht ohne Weiteres sagen können[42]. Auch ist es ist im Hinblick auf die Produktsicherheit und damit bereits auch den Entwicklungsprozess gerade erforderlich, dass genau dieses Verhalten nicht unkontrolliert als Produkteigenschaft hervorsticht, da sonst die nach dem ProdHG erforderliche Produktsicherheit nicht gewährleistet ist.

Zudem wird für Anwendungen in sicherheitskritischen Bereichen häufig schon kraft Natur der Sache eine nach dem Stand der Technik 100%-ige Sicherheit verlangt[43], und zwar insb. für Software in sicherheits*empfindlichen* Bereichen[44]. Ist das, aus welchen Gründen auch immer, nicht ge-

---

41 Sprau, in Palandt, Bürgerliches Gesetzbuch, 68. Aufl. 09, Rdnr. 4 zu § 3 ProdhaftG unter Hinweis auf: BGH NJW 90, 906; OLG Hamm NJW 05, 295: Zigaretten.

42 Ebenso Taeger, CR 96, 257, 265 für Fehler in Software allgemein.

43 Kullmann, ProdHG, Kommentar, 4. Aufl. 04, S. 111.

44 Taeger, CR 96, 257, 265 f.; Meyer/Harland, CR 07, 689 mit Verweis auf Kullmann, ProdHG, Kommentar, 4. Aufl. 04, S.111, dieser mit Verweis auf Engel, CR 86, 702, 707 der aber gerade keine 100-%ige Sicherheit fordert, sondern zu Recht darauf verweist (Engel, S. 708), dass die Rechtsprechung eine Zumutbarkeits-

währleistet, muss man sich fragen, welche Konsequenz daraus zu ziehen ist. Möglicherweise darf das konkrete Produkt dann gar nicht in den Verkehr gebracht werden. Diese Frage ist unter Abwägung von Art und Umfang der Risiken, ihrer Eintrittswahrscheinlichkeit und des mit dem Produkt verbundenen Nutzens zu prüfen[45]. Dieses für diese Expertise ganz zentrale Thema wird unter Ziffer 2.2.4.3 behandelt.

2.2.4.2. Objektiver Umstand: Preisgestaltung

Die Preisgestaltung kann nach gesicherter Rechtsprechung auf die Verkehrserwartung Einfluss haben, denn erhöhte Sicherheit hat ihren Preis[46]. So wissen – und *müssen* bei rechtlicher Bewertung das auch wissen – Benutzer eines Klein- oder Mittelklassewagens, dass sie nicht die höhere Sicherheit des teureren Komfortwagens erwarten können[47].

2.2.4.3. Objektiver Umstand: Stand von Wissenschaft und Technik

Ein weiterer objektiver Umstand für die Beurteilung, ob ein Produkt die nach dem ProdHG erforderliche Sicherheit bietet, ist, dass das Produkt bzgl. Konstruktion, Fabrikation und Instruktion dem aktuellen Stand von Wissenschaft und Technik entsprechen *muss*, soweit dieser objektiv erkennbar und ermittelbar ist, sowie ferner den anerkannten Regeln des Fachs[48]. Der Hersteller hat daher die Maßnahmen zu treffen, die zur Vermeidung einer Gefahr (i) objektiv erforderlich und (ii) nach objektiven Maßstäben zumutbar sind[49].

Objektiv erforderlich sind die Sicherungsmaßnahmen, die nach dem im Zeitpunkt des Inverkehrbringens vorhandenen (neuesten) Stands der Technik konstruktiv möglich sind und als geeignet und genügend erscheinen, um Schäden zu verhindern. Dabei darf der maßgebliche Stand der Technik nicht mit Branchenüblichkeit gleichgesetzt werden, denn die in der jeweiligen Branche praktizierten Sicherheitsvorkehrungen könnten ja hinter dem rechtlich Gebotenen zurückbleiben[50]. Umgekehrt ist der Hersteller nicht verpflichtet, Sicherheitskonzepte umzusetzen, die bisher

grenze anerkennt, die vom jeweiligen Gefährdungspotenzial abhängt, dazu auch unten 2.2.4.3, vgl. auch Oechsler in Staudinger, Kommentar zum Bürgerlichen Gesetzbuch, 03, § 2 ProdHG Rdnr. 70 m.w.N.

45 BGH, Urteil vom 16.06.09, Az. VI ZR 107/08, Rdnr. 17 „Airbag“.

46 BGH NJW 90, 906, 907.

47 Sprau, in Palandt, Bürgerliches Gesetzbuch, 68. Aufl. 09, Rdnr. 4 zu § 3 ProdhaftG.

48 BGH NJW 68, 248, BGH 80, 186.

49 BGH, Urteil vom 16.06.09, Az. VI ZR 107/08, Rdnr. 16 „Airbag“.

50 BGH, Urteil vom 16.06.09, Az. VI ZR 107/08, Rdnr. 16 „Airbag“.

nur "auf dem Reißbrett erarbeitet" oder noch in der Erprobung befindlich sind[51].

Die Frage, ob eine Sicherungsmaßnahme nach objektiven Maßstäben zumutbar ist, lässt sich nur unter Berücksichtigung sämtlicher Umstände des Einzelfalls beurteilen[52]. Maßgeblich ist insbesondere die Größe der vom Produkt ausgehenden Gefahr. Je größer die Gefahren sind, desto höher sind die Anforderungen, die in dieser Hinsicht gestellt werden[53]. Bei erheblichen Gefahren für Leben und Gesundheit von Menschen sind dem Hersteller weitergehende Maßnahmen zumutbar als in Fällen, in denen „nur“ kleinere körperliche Beeinträchtigungen zu befürchten sind[54]. Maßgeblich für die Zumutbarkeit sind darüber hinaus die wirtschaftlichen Auswirkungen der Sicherungsmaßnahme, im Rahmen derer insb. die Verbrauchergewohnheiten, die Produktionskosten, die Absatzchancen für ein entsprechend verändertes Produkt, sowie die Kosten-Nutzen-Relation zu berücksichtigen sind[55].

Sind bestimmte mit der Produktnutzung einhergehende Risiken nach dem maßgeblichen Stand von Wissenschaft und Technik nicht zu vermeiden, ist unter Abwägung von Art und Umfang der Risiken, der Wahrscheinlichkeit ihrer Verwirklichung und des mit dem Produkt verbundenen Nutzens zu prüfen, ob das gefahrträchtige Produkt überhaupt in den Verkehr gebracht werden darf[56]. Klar ist damit bzgl. auf OC-Techniken basierender Produkte, dass diese jedenfalls nur dann überhaupt in Verkehr gebracht werden dürfen, wenn und soweit alle erforderlichen Warn- und Hinweispflichten eingehalten werden[57].

Nach dem derzeitigen Stand der Wissenschaft und Technik ist das Risiko, dass sich OC-Produkte (u.U. auch) in einer Weise entwickeln, die zu einem Schaden führt, wohl nicht zu vermeiden. Hier ist deshalb zum einen zu prüfen, wie hoch das Risiko des Schadenseintritts im konkreten Fall angesichts der Anwendung ist, sowie welche Art von Schäden und in welchem Maße diese zu erwarten sind (nur Sachschaden, leichter Personenschaden, schwerer Personenschaden, etc.). Die so erkannten

---

51 BGH, Urteil vom 16.06.09, Az. VI ZR 107/08, Rdnr. 16 „Airbag“.

52 BGH, Urteil vom 16.06.09, Az. VI ZR 107/08, Rdnr. 18 „Airbag“.

53 BGH, Urteil vom 16.06.09, Az. VI ZR 107/08, Rdnr. 18 „Airbag“.

54 BGH, Urteil vom 16.06.09, Az. VI ZR 107/08, Rdnr. 18 „Airbag“.

55 BGH, Urteil vom 16.06.09, Az. VI ZR 107/08, Rdnr. 18 „Airbag“.

56 BGH, Urteil vom 16.06.09, Az. VI ZR 107/08, Rdnr. 17 „Airbag“.

57 S.u. 2.2.

Risiken sind sodann mit dem mit dem konkreten Produkt konkret verbundenen Nutzen (nur Komfortsteigerung oder z. B. Verhinderung von Unfällen) abzuwägen. Ein Produkt, dass ggf. „nur“ relativ geringfügige Sachschäden herbeiführen kann und bei dem das Risiko der Eintrittswahrscheinlichkeit relativ gering ist, kann, wenn es gleichzeitig geeignet ist, in einer Vielzahl von Fällen vor schweren Körperschäden zu bewahren, dann zulässig sein, wenn alle erforderlichen Warn- und Hinweispflichten erfüllt werden und wenn alle zumutbaren Sicherheitsvorkehrungen getroffen wurden, sowie der Herstellungsvorgang hinsichtlich aller konkret anwendbaren Gesetze und technischen Normen normgerecht erfolgt ist.

2.2.4.4. Objektiver Umstand: Technische Normen und gesetzliche Sicherheitsbestimmungen

Schließlich muss das Produkt (auch) alle geltenden technischen Normen und gesetzlichen Sicherheitsbestimmungen einhalten. Dazu gehören alle für das konkrete Produkt allgemein anwendbaren:

- DIN-Vorschriften,
- VDE-Bestimmungen,
- das Gesetz über die elektromagnetische Verträglichkeit von Geräten von 2002,
- das Geräte- und Produktsicherheitsgesetz vom 06.01.04,
- das Lebensmittel- und Futtermittel-Gesetzbuch (LFGB) vom 01.09.05,
- etc.

Denn diese technischen Normen und gesetzlichen Sicherheitsbestimmungen geben jedenfalls in der Regel den Mindeststand(ard) der Technik wieder[58] und damit den Mindeststandard an Sicherheit, dessen Einhaltung die Allgemeinheit berechtigterweise erwartet[59] und erwarten darf.

Es gilt insoweit Dreierlei:

- Die <u>Nichteinhaltung</u> der anwendbaren technischen Normen und gesetzlichen Sicherheitsbestimmungen ist anerkanntermaßen ein Konstruktionsfehler im Rechtssinne[60], sowie unter Umständen auch

---

58 OLG Koblenz, Urteil vom 29.08.05, Az. 12 U 538/04 (NJW-RR 06, 169).

59 Kollmer NJW 97, 2015, 2018; Möllers VersR 00, 1177.

60 Kollmer NJW 97, 2015, 2018; vgl. zum Rechtsbegriff „Konstruktionsfehler“ auch 2.2.5.1.

ein Instruktionsfehler[61] – wobei diese Unterscheidung letztlich für die Praxis wohl dahin stehen kann.

- Die Einhaltung der anwendbaren technischen Normen und gesetzlichen Sicherheitsbestimmungen begründet die Vermutung, dass das Produkt (die Instruktion) den anerkannten Regeln der Technik und damit den Sicherheitserwartungen entspricht[62]. Kommt es zu einem Schaden, muss dann der Geschädigte darlegen und begründen, warum dennoch ein Fehler (Konstruktionsmangel) vorliegen soll.
  - Die Einhaltung genügt aber dann nicht, wenn die technische Entwicklung bzw. die wissenschaftlichen Erkenntnisse über die Normen hinaus gegangen sind und/oder wenn sich bei der Benutzung des Produkts Gefahren gezeigt haben, die in ihnen noch nicht berücksichtigt sind[63] (wobei hierfür der Geschädigte die Beweislast trägt). Denn in diesem Fall sind die bestehenden Normen ergänzungsbedürftig[64], und zwar nach dem objektiv erkennbaren oder ermittelbaren Stand von Wissenschaft und Technik[65].
- Darüber hinaus erwartet die Allgemeinheit – und darf das auch – Produktbeobachtung, d.h. dass der Hersteller sein Produkt im Auge behält und aus ihm bekannt werdenden Mängeln, z. B. aufgrund berechtigter Reklamationen, Konsequenzen für die künftige Herstellung zieht[66], sowie vor allem aber natürlich auch erkannte mangelhafte Produkte im Extremfall zurückruft, jedenfalls aber vor ihrer Verwendung warnt, etc. – kurz gesagt muss der Hersteller alle gebotenen Pflichten bzgl. einer potenziellen Rückrufsituation beachten[67].
- Das Unterlassen von Rückrufmaßnahmen bzw. -pflichten kann unter Umständen die Fehlerhaftigkeit für später in Verkehr gebrachte Produkte mit dem gleichen Mangel begründen[68] und ist ggf. sogar

---

61 Vgl. hierzu Ziffer 2.2.5.3.

62 OLG Celle NJW 03, 2544; Kullmann, ProdHG, 4. Aufl. 04, S. 113.

63 Vgl. Sprau, in Palandt, Bürgerliches Gesetzbuch, 68. Aufl. 09, Rdnr. 4 zu § 3 ProdhaftG unter Hinweis auf BGH NJW 94, 3349; OLG Köln NJW-RR 05, 3292 für Instruktion.

64 BGH NJW 87, 372.

65 BGHZ 80, 186.

66 Sprau, in Palandt, Bürgerliches Gesetzbuch, 68. Aufl. 09, Rdnr. 4 zu § 3 ProdhaftG.

67 S.o. 2.4.

68 Sprau, in Palandt, Bürgerliches Gesetzbuch, 68. Aufl. 09, Rdnr. 4 zu § 3 ProdhaftG.

strafbar als versuchte vorsätzliche Körperverletzung durch Unterlassen bzw. vollendete vorsätzliche Körperverletzung durch Unterlassen, wenn ein Körperschaden eintritt und kausal auf den (die Rückrufpflichten unterlassenden) Schädiger zurückgeführt werden kann[69].

2.2.5. Unterscheidung nach Art der Fehler

Bzgl. der Art der Fehler wird in der Regel im Rechtssinne unterschieden nach:

- Konstruktionsfehlern,
- Fabrikationsfehlern, sowie
- Instruktionsfehlern.

Der Hersteller muss sich bei Konstruktion, Produktion (Fabrikation) und Instruktion nach dem erkennbaren und ermittelbaren Stand von Wissenschaft und Technik richten[70]. Maßgeblich sind dabei die Erkenntnisse, die zu der Zeit bestanden, als eine Schadensabwendung in Betracht kam[71].

2.2.5.1. Konstruktionsfehler

Konstruktionsfehler sind Fehler, die der ganzen Serie anhaften, da sie auf einem Verstoß gegen technische Erkenntnisse schon bei der Herstellung beruhen[72]. Ein Produkt darf bereits von Beginn an nicht unter dem gebotenen Sicherheitsstandard bleiben[73], die erforderliche Sicherheit des Produkts muss schon bei dem der Herstellung i.S. einer Fertigung/Produktion vorgelagerten Konstruktionsprozess eingehalten werden.

Fehler in adaptiven Systemen sind damit als Programmierfehler in Software wohl *per definitionem* Konstruktionsfehler. Bzgl. Softwareerstellung sind (ohnehin) bestimmte Erstellungstechniken geboten, wobei im Einzelnen streitig ist, welcher Ansatz letztlich der sicherste bzw. gebotene ist. Bei sicherheitsrelevanter Software sind darüber hinaus bei der Konstruktion bereits bestimmte Standards einzuhalten bzw. jedenfalls dieje-

---

69 BGH NJW 90, 2560 ff.

70 Sprau, in Palandt, Bürgerliches Gesetzbuch, 68. Aufl. 09, Rdnr. 169 zu § 823

71 BGHZ 80, 186.

72 BGH BB 84, 2150.

73 OLG Düsseldorf VersR 03, 912.

nigen Maßnahmen zu ergreifen, die zur Vermeidung eines Fehlers erforderlich und zumutbar sind[74]. Die IEC 61508 sieht hier als Regelfall das sog. V-Modell vor[75].

Beispiele aus der Rechtsprechung für Konstruktionsfehler sind:

- Gefährliches Gerät ohne ausreichende Schutzvorrichtung, z. B.:
  - Geschirrspülmaschine ohne elektrische Schutzschaltung[76],
  - Kettenantrieb von Transportbändern[77],
- Gefährliches Gerät, das den Unfallverhütungsvorschriften nicht entspricht[78],
- Möglichkeit des Ingangsetzens bei geöffneter Schutzvorrichtung[79],
- Fehlerhaft konstruiertes Vorderradschutzblech bei Fahrrad[80],
- Betriebsunsichere Kühlmaschine[81],
- Mangelhafte Befestigung eines Ölablaufrohrs[82],
- Nicht bruchfester Expander[83],
- Seilriss bei Förderkorb[84],
- Fehlende Funktionstüchtigkeit eines Hilfsmittels für Felsklettern[85],
- Fehlende Schutzvorrichtung gegen Entzünden eines Kondensators durch Erwärmung[86],

---

74 OLG Karlsruhe ZfS 03, 226: Buschholzhackmaschine.

75 Vgl. IEC-61508-3, 7.1.2.4; Abweichungen von der IEC und insbesondere vom V-Modell sind zulässig, wenn sie den gleichen Erfolg sicherstellen, IEC-61508-3, 7.1.2.5.

76 OLG Schleswig NJW-RR 08, 691.

77 BGH VersR 57, 584; Düsseldorf VersR 89, 1158.

78 OLG Hamm MDR 71, 488, BGH BB 72, 13.

79 OLG Bremen VersR 04, 207.

80 LG Berlin MDR 97, 246.

81 BGH VersR 60, 1095.

82 OLG Nürnberg NJW-RR 88, 378.

83 BGH DB 90, 577.

84 BGH VersR 72, 559.

85 OLG Köln VersR 93, 110.

- Hohe Chloridgasabscheidung bei Luftfilter[87],

Dagegen wurde ein Konstruktionsfehler in den folgenden Fällen zwar geprüft, im Ergebnis aber verneint:

- Zu hohe Druckentwicklung einer verklebten Knetmaschine bei Öffnungsversuch durch Fachmann entgegen der Gebrauchsanleitung[88],
- Verwendung raffinierten Zuckers zur Herstellung von Schokoriegeln[89],
- Verwendung von Zucker und Koffein für Cola[90],
- Verwendung von Tabak einschließlich zulässiger Zusatzstoffe für Zigaretten[91].

2.2.5.2. Fabrikationsfehler

Fabrikationsfehler sind Fehler, die während der Herstellung entstehen, sie haften nur einzelnen Stücken an und beinhalten eine Abweichung des konkreten Stücks vom allgemeinen Standard, den der Hersteller für die Produktserie vorgesehen hat und an dem der Verwender deshalb seine Sicherheitserwartungen orientiert[92]. Zu diesen Fehlern gehören insb. die sog. Ausreißer, also Fabrikationsfehler, die trotz aller zumutbaren – und damit notwendigen – Vorkehrungen unvermeidbar sind[93]. Für Fabrikationsfehler wird mangels Verschuldens nicht nach allgemeinem Haftungsrecht (Deliktshaftung des BGB) gehaftet, wohl aber aus *Gefährdungshaftung* nach dem ProdHG[94].

2.2.5.3. Instruktionsfehler

Schließlich gibt es die sog. Instruktionsfehler. Diese fallen teilweise (auch) unter den Begriff der Darbietung im Sinne von § 3 ProdHaftG[95].

---

86 OLG Karlsruhe NJW-RR 95, 594.

87 OLG Frankfurt/Main VersR 90, 981.

88 OLG Koblenz, Urteil vom 29.08.05, Az. 12 U 538/04 (NJW-RR 06, 169).

89 OLG Düsseldorf VersR 03, 912.

90 OLG Essen NJW 05, 2713, a.A. Adams/Kraas-Littger FS Wiegand 2005.

91 OLG Hamm NJW 05, 295; s.a. Adams u.a., Molitoris NJW 04, 3657, 3662, Merten VersR 05, 465, Rdnr. 13 a.E.

92 Sprau, in Palandt, Bürgerliches Gesetzbuch, 68. Aufl. 09, Rdnr. 9 zu § 3 ProdhaftG.

93 BGH 129, 53, OLG Koblenz NJW-RR 99, 1624.

94 Sprau, in Palandt, Bürgerliches Gesetzbuch, 68. Aufl. 09, Rdnr. 199 zu § 823.

95 Dazu schon ausführlich 2.2. 0.

Instruktionsfehler bestehen in mangelhafter Gebrauchsanweisung und/oder nicht ausreichender Warnung vor gefahrbringenden Eigenschaften, die in der Wesensart der – wenn auch als solcher fehlerfreien – Sache begründet sind[96]. Der Hersteller muss also auf die korrekte Handhabung und auf bestimmte Gefahren, die entstehen können, hinweisen[97]. Das gilt nicht, sofern die Gefahren nicht im Rahmen des Gebrauchs, mit dem billigerweise gerechnet werden kann[98], offen zu Tage liegen bzw. den zu erwartenden Verwendern ohnehin bekannt sind[99]. Der Hersteller kann durch solche Hinweise sein Haftungsrisiko auch für die Besonderheiten der Konstruktion zwar absenken, er darf aber deshalb die ihm technisch möglichen und zumutbaren konstruktiven Maßnahmen nicht durch (irgendwelche) Warnhinweise ersetzen[100]. So muss z. B. ein Arzneimittelhersteller schon dann warnen, wenn aufgrund eines zwar nicht dringenden, aber ernstzunehmenden Verdachts zu befürchten ist, dass Gesundheitsschäden entstehen können[101].

Bzgl. des Inhalts und Umfangs der Instruktionen gilt Folgendes:

- Die Instruktionen sind auszurichten an der am wenigsten informierten und damit am meisten gefährdeten Benutzergruppe[102]. Nur soweit das Produkt nach den berechtigten Erwartungen des Herstellers ausschließlich in die Hände von Personen gelangen kann, die mit den Gefahren vertraut sind, entfällt die Instruktionspflicht oder beschränkt sie sich auf Gefahren, deren Kenntnis der Hersteller auch bei solchen Personen nicht voraussetzen darf[103].
- Die Instruktionen müssen in jedem Fall deutlich und ausreichend sein. Soweit notwendig, müssen sie dem Produkt selbst beigegeben werden bzw. müssen die Hinweise im Produkt selbst enthalten sein[104].

---

96 Sprau, in Palandt, Bürgerliches Gesetzbuch, 68. Aufl. 09, Rdnr. 10 zu § 3 ProdHaftG.

97 BGH NJW 75, 1827: Werkzeug; allg. Bischoff VersR 03, 958.

98 Vgl. hierzu Ziffer 2.2. a).

99 Sprau, in Palandt, Rdnr. 10 zu § 3 ProdHaftG.

100 Müller VersR 04, 1073/75, Kloepfer/Grodenwald DD 07, 1342, 1343 zu Herstellerinstruktionen die Bedienungsanleitung.

101 BGHZ 106, 273.

102 BGH NJW 94, 932 „Milupa/Alete-Tee“.

103 BGH NJW 92, 560; 2016, 2018: spezialisierte Fachunternehmer.

104 Vgl. z. B. Software, mit Warnhinweisen vor der Installation bzw. beim Programmstart.

- Die Instruktionen müssen vollständig sein, d. h. die Art der drohenden Gefahren ist deutlich herauszustellen. Bei der Gefahr erheblicher Gesundheits- und Körperschäden ist der Funktionszusammenhang so darzustellen, dass erkennbar wird, warum das Produkt gefährlich werden kann[105].

- Gegebenenfalls muss außer dem Hinweis auf Gefahren auch angegeben werden, wie das Produkt gefahrfrei zu verwenden ist, welche Vorsorgemaßnahmen zu treffen sind und welche Verwendungsarten zu unterlassen sind[106].

- Dabei ist nicht nur auf den bestimmungsgemäßen Gebrauch, sondern darüber hinaus auch auf den naheliegenden Gebrauch, also auch auf eine nicht ganz fernliegende versehentliche Fehlanwendung abzustellen[107], ebenso auf naheliegende Missbrauchsmöglichkeiten[108].

- Hingegen muss auf Folgendes nicht ausdrücklich hingewiesen werden:

    - Gefahren, die sich aus einem vorsätzlichen oder leichtfertigen Fehlgebrauch ergeben[109].

    - Gefahren, die sich aus einem völlig zweckfremden, bewussten Missbrauch des Produkts ergeben[110].

    - Ebenso muss allgemeines Erfahrungswissen nicht zum Inhalt einer Gebrauchsanweisung oder Warnung gemacht werden[111].

Die Warn- und Hinweispflicht besteht dagegen insb. dann, wenn ein zur Abwendung von Gefahren bestimmtes Produkt zwar nicht gefährlich ist, sondern nur unter bestimmten Voraussetzungen wirkungslos ist, der Be-

---

105 BGH NJW 92, 560,95,1286, verfassungsrechtlich nicht zu beanstanden: Bundesverfassungsgericht NJW 97, 249.

106 BGH NJW 72, 2217 „Estil“, Hamm VersR 84, 243.

107 BGH 116,60; andere Ansicht Littbarski NJW 95, 217; BGH NJW 99, 2815: Es ist nahe liegend, dass der Verwender des Produkts Unfallverhütungs-Vorschriften zum Umgang mit dem Produkt nicht beachtet. Der Hersteller muss daher auf die Gefahren hinweisen, die bei Nichtbeachtung der Vorschriften entstehen.

108 BGH 106, 273.

109 BGH NJW 81,2514, NJW 99, 2815.

110 Karlsruhe NJW-RR 01, 11074.

111 BGH NJW 86, 1863: Montageanweisung.

nutzer aber im Vertrauen auf die Wirksamkeit von der Verwendung eines anderen, die Gefahr wirksam abwendenden Produkts absieht[112].

In jedem Fall muss die Verletzung der Hinweispflicht ursächlich sein für den eingetretenen Schaden. Das ist dann der Fall, wenn pflichtgemäßes Handeln den eingetretenen Schaden mit Sicherheit verhindert hätte, eine gewisse Wahrscheinlichkeit genügt hierfür nicht[113]. Dabei spricht für die Beachtung einer hinreichend deutlichen Gefahrenwarnung nach der Lebenserfahrung eine tatsächliche Vermutung, wenn nicht die unstreitig festgestellten und vom Kläger selbst vorgetragenen Umstände im Rahmen einer Gesamtbetrachtung für das Gegenteil sprechen[114]. Abgelehnt wurde z. B. für einen Warnhinweis auf Baby-Nuckelflaschen, dass generell vor einem Dauernuckeln von Getränken wie etwa Milch, ungesüßten Arznetees oder Mineralwasser zu warnen sei, weil ein solches Gebot eine Überspannung der Verkehrssicherungspflicht darstellen würde[115].

Beispiele aus der Rechtsprechung, in denen Instruktionsfehler bejaht wurden, sind:

- Ganz allgemein der ungenügende oder fehlender Hinweis auf die Gefährlichkeit des Produkts[116].
- Gefahr einer Überdosierung bei Pflanzenschutzmitteln[117].
- Unverträglichkeit bei gleichzeitiger Anwendung zweier Pflanzenschutzmittel[118].
- Sowie im jeweils konkreten Fall der ungenügende oder fehlende Hinweis auf:
    - Die ätzende Wirkung eines Fertigputzes[119].
    - Potenzielle Folgen bzw. Gefahren bei der Verwendung von Frischbeton[120], eines Rohrreinigungsmittels[121], eines Reinigungsmittels[122].

---

112 BGR 80, 186, Schmidt-Salzer Bd. 81, 1041, von Westphalen, WM 81, 1154/62.

113 Sprau, Randziffer 12 zu ProdHaftG 3 unter Hinweis auf BGH NJW 75, 1827.

114 BGH NJW 99, 2273.

115 OLG Frankfurt NJW-RR 99, 25, 27 u. 30; Revision vom BGH nicht angenommen, Beschluss vom 27.01.98, Az. VI ZR 126/97.

116 OLG Frankfurt/Main NJW-RR 97, 1519.

117 OLG Frankfurt/Main VersR 94, 231.

118 BGH DB 77, 1695.

119 OLG Düsseldorf VersR 91, 233.

- Aggressive Substanzen in Brandschutzmittel, die bei Hinzutritt von Wasser zur Korrosion führen können[123].
- Feuergefährlichkeit von Rostschutzmitteln[124].
- Feuergefährlichkeit von Klebemittel[125].
- Feuergefährlichkeit von Grundiermittel[126].

- Fehlender Hinweis auf Brennbarkeit nicht nur des Konzentrats, sondern auch der Aufgussmischung für Saunaaufgüsse[127],
- Notwendigkeit einer besonderen Brandisolierung bei Aufbau eines offenen Fertigkamins in einem Fertighaus[128],
- Nicht erkennbare Gefahr einer Fingerverletzung bei Papierreißwolf[129],
- Unzureichende Bedienungsanleitung von Betonbereitungsanlage[130],
- Unzureichende Bedienungsanleitung für ein elektrisches Messgerät[131],
- Fehlender Hinweis auf Gefahr des Berstens einer Spannhülse bei der Schalung von Betonteilen[132],
- Explosionsgefahr einer Flasche mit Rohreinigungsmittel[133],
- Ungenügende Bedienungsanleitung für Schnellspannvorrichtung eines Mountainbikevorderrads[134],

---

120 OLG Celle VersR 04, 864.

121 OLG Oldenburg NJW-RR 97, 1520.

122 OLG Celle VersR 85, 949.

123 OLG Karlsruhe NJW-RR 92, 285.

124 BGH NJW 59, 1676.

125 BGH VersR 60, 342.

126 BGH VersR 62, 273.

127 OLG Düsseldorf NJW-RR 92, 534.

128 OLG Düsseldorf VersR 90, 900.

129 BGH NJW 99, 2815.

130 BGHZ 47, 312.

131 OLG Stuttgart NJW-RR 92, 670.

132 BGH BB 75, 1031.

133 OLG Odenburg VersR 98, 65.

134 OLG Düsseldorf NJW 97, 2333.

- Ungenügende Bedienungsanleitung für Kfz-Abschleppstange[135],
- Fehlender Hinweis auf die Möglichkeit, dass sich bei Fallenlassen einer Pistole ein Schuss lösen kann[136],
- Sichere Befestigung eines Sportgerätes[137],
- Hohe Chloridabscheidung bei Luftfilter[138],
- Feuergefährlichkeit eines Auftautransformators[139].

Im zuletzt genannten Beispiel hatte der Hersteller eines Auftautransformators (eine Heizspirale, die um Wasserleitungen in Scheunen geführt wird, um Einfrieren zu verhindern) damit geworben, dass das Produkt „völlig gefahrlos" sei und „keine Brandgefahr" bestehe. Aufgrund einer falschen Montage wurde Stroh in Brand gesetzt, der Bauernhof brannte ab. Da die Montageanleitung nicht den Hinweis enthielt, dass bei einer fehlerhaften Montage Brandgefahr besteht, lag auch ein Instruktionsfehler vor, denn aufgrund der Werbung durfte erwartet werden, dass unter keinen Umständen Brandgefahr besteht.

Auf OC Systeme übertragen (z. B., wenn die temperaturabhängige Steuerung der Heizspirale durch ein OC System erfolgt) könnte dies z. B. bedeuten, dass trotz einer ggf. selbstheilenden Funktion dieses Systems darauf hingewiesen werden muss, dass das System nicht in jedem Fall in der Lage ist, sich selbst zu heilen und daher entsprechende zusätzliche Sicherheitsmaßnahmen zu ergreifen sind (z. B. Einbau einer konventionellen Abschaltautomatik bei Überhitzung).

2.3. Gibt es erste Präzedenzfälle mit „smarten Technologien“?

Bis ins Jahr 2004 gab es kein einziges Urteil zum Bereich Produkthaftung oder Deliktshaftung für Computersysteme allgemein[140]. Auch bis heute gibt es nur Ansätze in Urteilen zur Produkthaftung, aus denen man

---

135 AG Nürnberg NJW 04, 3123.

136 Karlsruhe VersR 98,63.

137 BGH VersR 88, 635.

138 Frankfurt/Main VersR 90, 981.

139 BGH VersR 63, 860.

140 Heussen, CR 04, 1, 4, Fn. 24.

schließen kann, dass diese auch für Software, insb. Embedded Software, anwendbar ist[141].

2.3.1. Recherche bestehender rechtlicher Ansätze und einschlägiger rechtswissenschaftlicher Untersuchungen

Selbstorganisierende Systeme werden in der Rechtswissenschaft soweit ersichtlich bisher nur unter dem Blickwinkel von Rechtsverletzungen, vorrangig von Urheber- und Persönlichkeitsrechten, bei selbstorganisierenden Empfehlungssystemen und Peer-to-Peer Systemen im Internet untersucht[142]. Da es hierbei auch um die Frage der Zurechnung des Verhaltens, insb. um Haftung geht, können diese Überlegungen aber auch hier herangezogen werden. Ferner diskutiert wird die Produkthaftung fehlerhafter Expertensysteme[143], eine Fragestellung, die zumindest in die gleiche Richtung geht wie die hier zu untersuchende[144]. Denn auch bei einigen dieser Expertensysteme geht es letztlich darum, ob und inwieweit menschliche Entscheidungen durch Software ersetzt[145] bzw. zumindest beeinflusst werden[146].

2.3.2. Welche Probleme existieren und welche offenen Fragen werden hierbei diskutiert?

Es wird nach wie vor die allgemeine Frage diskutiert, ob für Softwarefehler nicht gehaftet werden muss, weil Software nicht fehlerfrei hergestellt werden kann. Diese Frage stellt sich bzgl. OC-Techniken in besonders drängendem Maße. Der Meinungsstand zu dieser Frage allgemein wird unter Ziffer 2.6.1 dargestellt. Umstritten ist nach wie vor auch die Frage, ob Software überhaupt ein Produkt im Sinne des Produkthaftungsgeset-

---

141 BGH, Urteil vom 16.06.09, Az. VI ZR 107/08 Rdnr. 31 „Airbag“, vgl. zur Anwendung dieses Urteils auf Software unten 2.3.3.

142 Sorge, Christoph, Selbstorganisierende Empfehlungssysteme im Internet, Diss. Karlsruhe 2007.

143 Kardasiadou, Die Produkthaftung für fehlerhafte medizinische Expertensysteme, Hannoversches Forum der Rechtswissenschaften Band 5, Baden-Baden 98.

144 Die Beispiele in Hähner/Bernard, in: Antrag auf Einrichtung einer DFG-Forschergruppe OC-Trust, 08, S. 16 bei der vorgestellten Referenzstudie Reha-Klinik unterscheiden sich gar nicht so sehr von medizinischen Expertensystemen mit der Ausnahme, dass bei letzteren ein Arzt noch einmal die Entscheidung überprüft, was aber in dem Fall, in dem ein Expertensystem die Konsultation eines ggf. nicht verfügbaren Experten (z. B. Facharzt eines anderen Gebiets) ersetzen soll (vgl. Kardasiadou, Die Produkthaftung für fehlerhafte medizinische Expertensysteme, 98, S. 42), letztlich auf das Gleiche hinausläuft.

145 Vgl. die Definition bei Kardasiadou, Die Produkthaftung für fehlerhafte medizinische Expertensysteme, 98, S. 43: Programme […], die den Arzt […] unterstützen oder in ganz beschränktem Maße ersetzen.

146 Vgl. den von Kardasiadou, Die Produkthaftung für fehlerhafte medizinische Expertensysteme, 98, S. 15 zitierten Fall (HAZ v. 28.02.97), einer Software, die die Überlebenswahrscheinlichkeit von Patienten und der Behandlungskosten berechnete. Die Evaluation der Software ergab, dass von 53 Patienten, deren Sterbewahrscheinlichkeit von der Software mit 99,9% errechnet wurde, 16 überlebt hatten. Die Behandlungskosten von sechs (6) von ihnen überstiegen den Betrag von DM 100.000.

zes ist[147]. Das vorrangige Problem bzgl. Organic Computing ist aber die Frage der Zurechenbarkeit des Verhaltens von organischen Systemen: Auch *Sorge* sieht die Problematik darin, dass ein selbstorganisierendes System ermergentes Verhalten zeigt[148].

Sorge lehnt es ab, dass der jeweilige Nutzer jedenfalls das Risiko eines Fehlverhaltens des Systems zugewiesen bekommt, wenn er die Entscheidung für die Teilnahme am System getroffen hat und durch den Einsatz des Systems selbst profitiert[149]. Denn der Nutzer könne bezogen auf selbstorganisierende Peer-to-Peer Systeme gerade nicht absehen, wie sich das System verhalten wird und habe oft auch keine Kontrolle über das System[150]. Ferner könne bei einer Vielzahl von Teilnehmern nur schwer entschieden werden, welchem der Nutzer das Risiko zugewiesen werden soll[151]. Das System sei weder Rechtssubjekt, noch könne es durch ein einzelnes Rechtssubjekt ohne weiteres kontrolliert werden.

Letztlich gilt dies generell und nicht nur für Peer-to-Peer Systeme, allerdings ist unter dem Blickwinkel der Produkthaftung wohl zu ergänzen, dass gerade weil das System nach dem Inverkehrbringen insoweit keiner Kontrolle mehr unterliegt, die produkthaftungsrechtlichen Grundsätze auf den Hersteller angewendet werden müssen. Denn der Hersteller ist das Rechtssubjekt, das jedenfalls den Umstand kontrolliert, ob das Produkt überhaupt in den Verkehr gebracht werden darf. Ob das Inverkehrbringen dann Produkthaftung auslösen kann, ist nach den dargestellten Grundsätzen zu entscheiden[152]. Daher können die Parallelen, die *Sorge* zum Umweltrecht zieht[153] – keine Haftung für Summationsschäden, also wenn die Emission einer einzelnen Entität noch keinen Schaden auslöst, aber die Summation solcher Schäden –, für Produkthaftungsfragen wohl hier nicht herangezogen werden. Zwar geht es im Umwelthaftungsrecht ähnlich wie im Produkthaftungsrecht auch um Gefährdungshaftung[154]. Summationsschäden sind mit Schäden aus Organic Computing aber nicht vergleichbar: § 6 Abs. 1 S. 1 UmwHG lautet:

---

147 Unten 2.3.3.

148 Sorge, Christoph, Selbstorganisierende Empfehlungssysteme im Internet, Diss. Karlsruhe 2007, S. 208.

149 Sorge, Christoph, Selbstorganisierende Empfehlungssysteme im Internet, Diss. Karlsruhe 2007, S. 210.

150 Sorge, Christoph, Selbstorganisierende Empfehlungssysteme im Internet, Diss. Karlsruhe 07, S. 210.

151 Sorge, Christoph, Selbstorganisierende Empfehlungssysteme im Internet, Diss. Karlsruhe 07, S. 210.

152 S.o. 2.2.4.3.

153 Sorge, Christoph, Selbstorganisierende Empfehlungssysteme im Internet, Diss. Karlsruhe 07, S. 210.

154 BT-Drucks. 11/1704, Begründung A. V. 1.

> „Ist eine Anlage nach den Gegebenheiten des Einzelfalles geeignet, den entstandenen Schaden zu verursachen, so wird vermutet, dass der Schaden durch diese Anlage verursacht ist".

Bei einem Summationsschaden besteht damit nach dem ausdrücklichen Willen des Gesetzgebers[155] keine Haftung, da diese nicht einem individualisierbaren Schädiger zugeordnet werden können. Dagegen kann bei einem Schaden aufgrund Organic Computing der Schaden dem Hersteller zugeordnet werden, da der Hersteller über das Inverkehrbringen entschieden hat.

Im Hinblick auf die Zurechenbarkeit von Fehlverhalten von Expertensystemen wird zum Teil in der Literatur darauf hingewiesen, dass jedes Modell der Wirklichkeit weniger als die Wirklichkeit selbst sei und das System daher die Wirklichkeit nie vollständig abbilden könne. Daher sei mit Fehlern zu rechnen[156]. Diese abstrakte Vorhersehbarkeit von Fehlern führe aber nicht dazu, dass deshalb in jedem Fall aus Produkthaftung gehaftet werde, es könne dennoch die Produkthaftung ausgeschlossen sein, weil der konkrete Fehler nicht vorhersehbar sei. Insoweit sei die Sachlage dem Inverkehrbringen von Arzneimitteln vergleichbar[157].

Diese Auffassung ist mit der aktuellen Rechtsprechung wohl nicht zu vereinbaren. Zwar besteht keine Produkthaftung, wenn der den Schaden verursachende Fehler des Produkts im Zeitpunkt des Inverkehrbringens nach dem Stand der Wissenschaft und Technik nicht erkennbar war (sog. Entwicklungsfehler), vgl. § 1 Abs. 2 Nr. 5 ProdHG. Diese Bestimmung ist auch für Instruktionsfehler anwendbar[158]. Ein solcher Entwicklungsfehler, der zu einem Haftungssausschluss führen würde, setzt aber voraus, dass die potenzielle Gefährlichkeit des Produkts im Zeitpunkt des Inverkehrbringens nach dem Stand der Wissenschaft und Technik nicht erkannt werden konnte[159]. Allerdings ist unter potenzieller Gefährlichkeit des Produkts nicht der konkrete Fehler des schadensstiftenden Produkts, sondern das zugrundeliegende allgemeine, mit der gewählten

---

155 BT-Drucks. 11/1704, Begründung A. V. 14.: Durch das […] Umwelthaftungsgesetz werden nicht diejenigen Umweltbeeinträchtigungen erfasst, die keinem individualisierbaren Schädiger zugeordnet werden können. Diese auf die allgemeine Umweltbelastung zurückgehenden Schäden – wie vielfach […] Waldschäden […] – lassen sich mit den Mitteln des individuellen Haftungsrechts nicht regeln.

156 Kardasiadou, Die Produkthaftung für fehlerhafte medizinische Expertensysteme, S. 182.

157 Kardasiadou, Die Produkthaftung für fehlerhafte medizinische Expertensysteme, S. 182; so auch Meier/Wehlau, CR 90, 95, 98 für Softwarefehler allgemein.

158 BGH, Urteil vom 16.06.09, Az. VI ZR 107/08, Rdnr 27 „Airbag" m.w.N.

159 BGH, Urteil vom 16.06.09, Az. VI ZR 107/08, Rdnr 28 „Airbag" m.w.N.

Produktion verbundene Fehlerrisiko zu verstehen[160]. Man kann daher wohl nicht argumentieren, aufgrund der Fehleranfälligkeit von Software allgemein, aufgrund der unvollständigen Abbildung der Wirklichkeit bei Expertensystemen oder bei Organic Computing Systemen, bei der sich die Software ja gerade unabhängig von Vorgaben selbständig entwickeln soll, sei die potenzielle Gefährlichkeit in sicherheitskritischen Bereichen aus der Natur der Sache heraus nicht vorhersehbar. Es ist richtig, dass bei einem überragenden Nutzens des Systems – wie bei Arzneimitteln – dennoch ein überwiegendes Interesse daran bestehen kann, das System in Verkehr zu bringen, ohne das der Hersteller dafür haftet. Dieses Problem kann aber nicht dadurch gelöst werden, dass der Hersteller aufgrund der Unvorhersehbarkeit von Fehlern gar nicht haftet. Denn das könnte (auch) dazu führen, dass Systeme mit wenig Nutzen, aber hohem Risiko bei im Übrigen ordnungsgemäßer Entwicklung ohne Haftungsrisiken in den Verkehr gebracht werden könnten. Das darf nicht sein. Die Problematik muss deshalb vielmehr wohl bei der Frage angesiedelt und auch gelöst werden, ob bzw. unter welchen Voraussetzungen das konkrete Produkt unter Abwägung von Nutzen und Risiken überhaupt in den Verkehr gebracht werden durfte[161]. Dabei wird man der Frage, ob Sicherungsmaßnahmen nach dem Stand der Wissenschaft und Technik evtl. nicht zumutbar sind[162], einen besonderen Stellenwert einräumen müssen.

2.3.3. Haben sich in der diesbezüglichen rechtsfachlichen Diskussion erkennbar unterschiedliche (gegenläufige) Positionen herausgebildet?

Zu den Ansätzen zu Rechtsfragen bei Organic Computing s. oben[163], zur Frage, ob die generelle Unvermeidbarkeit von Fehlern in Software zur Einschränkung der Haftung führt, s. unten[164]. Umstritten ist nach wie vor die Frage, ob Software überhaupt ein Produkt im Sinne des Produkthaftungsgesetzes ist. Die überwiegende Ansicht in der Literatur bejaht dies jedenfalls für Software, die auf einem Datenträger vertrieben wird[165]. Ein

---

160 BGH, Urteil vom 16.06.09, Az. VI ZR 107/08, Rdnr 28 „Airbag“ m.w.N.

161 BGH, Urteil vom 16.06.09, Az. VI ZR 107/08, Rdnr 28 „Airbag“ m.w.N. So im Ergebnis dann auch – wobei die dogmatische Einordnung unklar bleibt, Kardasiadou, Die Produkthaftung für fehlerhafte medizinische Expertensysteme, S. 182.

162 S. Ziffer 2.2.4.3.

163 S. Ziffer 2.3.2.

164 S. Ziffer 2.6.1.

165 Kullmann, ProdHG, Kommentar, 4. Aufl. 04. S. 84 ff ;Oechsler in Staudinger, Kommentar zum Bürgerlichen Gesetzbuch, 03, § 2 ProdHG Rdnr. 65 m.w.N.

Teil der Literatur lehnt die Produkteigenschaft bei Downloads ab[166] oder zumindest, wenn die Software lediglich zeitweise während der Benutzung der Dienste eines Service Providers zur Verfügung gestellt wird[167]. Zu Recht wird aber darauf verwiesen[168], dass die Rechtsprechung[169] mittlerweile in anderem Zusammenhang die Sacheigenschaft für Software bejaht hat, da Software, um überhaupt lauffähig zu sein, auch bei einem online im Rahmen von Application Service Providing (ASP) genutzten Programm, irgendwo verkörpert sein müsse. Im Übrigen müsse man die Sacheigenschaften von Software bei Embedded Software, also fest in das System integrierter Software, wegen ihrer engen Verknüpfung mit der Hardware bejahen, so dass Softwarefehler als Fehler eines Gesamtprodukts einzustufen seien[170].

Für Letzteres spricht auch die neueste Rechtsprechung. So hat der BGH[171] jüngst entschieden, dass ein Airbag, der aufgrund von Schlaglöchern ausgelöst wurde, die einen Crash-ähnlichen Impuls verursacht haben, einen Konstruktionsfehler aufweist. Der BGH führt dazu u.a. aus, dass der Hersteller davon ausgegangen war, die Gefahr der Fehlauslösung durch eine geänderte Steuergerätesoftware beseitigt zu haben. Dem BGH war dabei bewusst, dass das Problem darin begründet lag, dass die Software nicht zwischen Stößen durch Unfälle und Stößen durch Schlaglöcher unterscheiden konnte. Auch wenn es sich hierbei nicht um einen „klassischen“ Softwarefehler handelt, sondern um einen typischen Konstruktionsfehler[172] – denn bei einer Auslösung des Airbags allein aufgrund von Sensoren, die ab einem Stoßimpuls größer X den Airbag auslösen, ohne dass Software dazwischengeschaltet wäre, wäre es ebenfalls zu einer Fehlauslösung gekommen – spricht das Urteil des BGH (sehr) stark dafür, dasas jedenfalls bei Embedded Software die Software als Teil einer anderen Sache im Rechtssinne eingestuft werden kann. Um derartige Fragen wird es wohl auch bzgl. Organic Computing gehen, insb. um die Frage, ob auf OC-Techniken basierende Software als Produkt im Sinne des Produkthaftungsrechts angesehen werden

---

166 Kullmann, ProdHG, Kommentar, 4. Aufl. 04. S. 84 ff.; Oechsler in Staudinger, Kommentar zum Bürgerlichen Gesetzbuch, 03, § 2 ProdHG Rdnr. 65 m.w.N.

167 Spindler, Rechtsfragen der Open Source Software, 03, S. 92.

168 Meyer/Harland, CR 2007, 689, 693 m.w.N. zum Streitstand.

169 BGH, Urteil vom 15.11.2006, Az. XII ZR 120/04, Rdnr. 16.

170 Meyer/Harland, CR 2007, 689, 693 m.w.N; Kullmann, ProdHG, Kommentar, 4. Aufl. 04, S. 84 ff. m.w.N. auch zur Gegenansicht, Foerste, NJW 1991, 1433, 1438 m.w.N..

171 BGH, Urteil vom 16.06.09, Az. VI ZR 107/08 Rdnr. 31 „Airbag“.

172 Zum Begriff s. Ziffer 2.2.5.1.

kann oder muss. Letztlich wird man das hier nicht anders beurteilen können als bei „konventioneller“ Software.

2.4. Haftung nach dem BGB: Produzentenhaftung

Die Haftung nach dem BGB im Bereich Produktfehler, die sog. „Produzentenhaftung“[173] als Ausprägung der Deliktshaftung nach § 823 BGB, knüpft anders als das ProdHG weniger an die Qualität des Produkts als Ergebnis eines Herstellungsprozesses an, sondern statt dessen mehr an den Herstellungsprozess selbst. Ein wesentlicher Unterschied der Produzentenhaftung zur Produkthaftung liegt darin, dass der Hersteller im Rahmen der Produzentenhaftung nur bei Verschulden haftet. Dabei kann und muss ggf. der Hersteller den Gegenbeweis führen, um seine Haftung bei Vorliegen eines Fehlers vermeiden zu können[174]. Der im Rahmen der Produzentenhaftung relevante Maßstab für die objektiv zu bestimmende Erkennbarkeit des Fehlers und damit für die objektive Pflichtwidrigkeit unterscheidet sich insoweit nicht vom Maßstab des § 1 Abs. 2 Nr. 5 ProdHG[175]. Daher kann auf die Ausführungen zu den Fehlerarten bei der Produkthaftung verwiesen werden[176].

Ein weiterer Unterschied der Produzentenhaftung[177] gegenüber der Produkthaftung nach dem ProdHG ist die Pflicht, Produkte nach Inverkehrbringen auf noch unbekannt gebliebene schädliche Eigenschaften hin zu beobachten und sich über sonstige eine Gefahrenlage schaffende Verwendungsfolgen zu informieren[178]. Es besteht bei nachträglicher Erkennbarkeit von Gefahren u.U. eine Abwendungspflicht[179], die es bei der gesetzlichen Produkthaftung nach dem ProdHG so nicht gibt[180].

---

173 Die Produzentenhaftung ist der von der Rechsprechung bereits lange vor Inkrafttreten des ProdHG im Jahr 1990 entwickelte Vorläufer der gesetzlichen Produkthaftung. Da Produzentenhaftung und Produkthaftung z. T. unterschiedliche Voraussetzungen und Rechtsfolgen aufweisen, bestehen sie nebeneinander, was der Gesetzgeber in § 15 Abs. 2 ProdHG ausdrücklich klargestellt hat.

174 BHGH 80, 186.

175 BGH, Urteil vom 16.06.09, Az. VI ZR 107/08, Rdnr. 28 „Airbag“.

176 S.o. 2.2.5

177 Produktbeobachtungsfehler werden vom Produkthaftungsgesetz nicht erfasst, Kullmann, ProdHG, Kommentar, 4. Aufl. 04, S. 101 m.w.N.

178 BGH NJW 81, 1606, 1607 f. „Benomyl“; BGH NJW 90, 906, 907 „Pferdeboxen“.

179 BGH, Urteil vom 16.12.08, Az. VI ZR 170/07, Rdnr. 16 „Pflegebetten“.

180 Kullmann, ProdHG, Kommentar, 4. Aufl. 04, S. 101 m.w.N. in Fn. 37.

2.4.1. Organisationspflichten bei Produzentenhaftung

Zu beachten sind hinsichtlich der Produzentenhaftung insb. die sog. Organisationspflichten: Der Hersteller muss den Betrieb so einrichten, dass Fehler in den drei Fehlerkategorien[181] möglichst ausgeschaltet oder durch Kontrollen entdeckt werden[182]. Z. B. muss der Hersteller ältere Mehrwegflaschen auf Berstdrucksicherheit vor dem Wiederauffüllen prüfen und den Prüfungsbefund sichern[183]. Der Hersteller muss auch die Zeugnisse von Zulieferern auf deren grundsätzliche einwandfreie Beschaffenheit hin zumindest stichprobenweise überprüfen[184]. Das gilt nicht, wenn der Zulieferer aufgrund besonderer fachlicher Einrichtungen diese Prüfungen bereits vorgenommen hatte[185].

2.5. Vertragsrechtliche Haftung

Die vertragsrechtliche Haftung knüpft anders als die Produkt- und die Produzentenhaftung an das sog. Äquivalenzinteresse an. Hierbei geht es nicht um die Interessen und Sicherheit der Allgemeinheit bzw. des Rechtsverkehrs allgemein, sondern um das bilaterale wirtschaftliche Verhältnis der Vertragspartner: Leistung und Gegenleistung müssen in einem angemessenen Verhältnis zueinander stehen, d.h. die vertragliche Haftung möchte wirtschaftliche Einbußen der Vertragspartner ausgleichen, die diese aufgrund schädigender Ereignisse aus dem Verantwortungsbereich des anderen Vertragspartners erleiden. Die vertragliche Haftung ist damit unmittelbar preisrelevant, denn wenn ein relativ kleines Softwarehaus den Preis für die Zahlung einer weltweiten Rückrufaktion oder auch nur die Versicherungsprämie für potenzielle Schäden in dreifacher Millionen-Euro-Höhe in den Preis für die Software einkalkulieren muss, wird schnell deutlich, dass der Preis für die Software ohne vertragliche Haftungsbeschränkungen erheblich höher sein müsste als mit Haftungsbeschränkung. Die vertragsrechtliche Haftung ist damit aber nicht entscheidend für die im Rahmen dieser Expertise zu behandelnden Fragen, weil sie nicht primär Fragen der Sicherheit betrifft.

---

181 Vgl. Ziffer 2.2.5.

182 Sprau , in Palandt, Bürgerliches Gesetzbuch, 68. Aufl. 09, Rdnr 169 zu § 823.

183 BGHZ104, 323, NJW 95, 2162, s. a. NJW 07, 762: anders ist das für Einwegflaschen: OLG Braunschweig VersR 05, 417.

184 BGH VersR 60, 855; OLG Oldenburg NJW-RR 05, 1338.

185 BGH NJW 75, 1827, Köln VersR 90, 863.

2.6. Gibt es haftungsrechtlich Besonderheiten bei der Haftung für Software?

Man kann sich fragen, ob bzgl. Software generell Besonderheiten gegenüber den allgemein geltenden Rechtsvorschriften gelten können, soll(t)en oder gar müss(t)en.

2.6.1. Besonderheit wegen Unvermeidbarkeit von Fehlern?

Bei der Haftung für Software ist ganz generell zu beachten, dass man Programmierung mit guten Argumenten als besonders schadensträchtige Arbeit einstufen könnte. Das hätte im Verhältnis Arbeitgeber – Arbeitnehmer zur Folge, dass bei leichter bis mittlerer Fahrlässigkeit keine Haftung des Arbeitnehmers für seine Fehler bestünde, im Übrigen bleibt die Haftung des Arbeitgebers aus Produkthaftung aber bestehen. Was die Haftung wegen Fehlern (einschließlich Produkt- und Produzentenhaftung) angeht, wird diskutiert, ob wegen der Unvermeidbarkeit von Softwarefehlern ein weniger strenger Verschuldensmaßstab anzusetzen sei als bei „normalen“ Fehlern. Einschlägige ständige Rechtsprechung gibt es hierzu indessen nicht[186].

In der Literatur wird zum Teil die Ansicht vertreten, fehlerfreie Software könne nicht erwartet werden[187]. Zu Recht wird aber darauf hingewiesen[188], dass der Nutzer erwartet, dass Software bei Verwendung für den Zweck, für den sie erstellt wurde[189], Rechtsgüter nicht verletzt. Zum Teil wird sogar gerade in sicherheitskritischen Bereichen eine 100 %-ige Sicherheit von Software gerade gefordert[190]. Auch werden die Besonderheiten bei Programmierung von Software wohl angemessen dadurch berücksichtigt, dass nach dem Stand von Wissenschaft und Technik anerkannt ist, dass Mängel in Software (= Fehler im Rechtssinne) selbst bei allen angemessenen und notwendigen Tests nicht 100 %-ig ausgeschlossen werden können. D.h. es ist anerkannt, dass Software nicht in

---

186 Heussen, CR 04, 1, 4, Fn. 24.

187 Meier/Wehlau, CR 90, 95, 98 diese Auffassung ist aber nach der neusten Rechtsprechung nicht haltbar s, o. 2.3.2; vgl. auch die Nachweise bei Oechsler in Staudinger, Kommentar zum Bürgerlichen Gesetzbuch, 03, § 2 ProdHG Rdnr. 70.

188 Taeger, CR 96, 257, 265.

189 Zur Haftung bei Fehlgebrauch s.o. 2.2.

190 Taeger, CR 96, 257, 265 f.; Meyer/Harland, CR 07, 689 mit Verweis auf Kullmann, ProdHG, Kommentar, 4. Aufl. 04, S.111, dieser mit Verweis auf Engel, CR 86, 702, 707 der aber gerade keine 100%ige Sicherheit fordert, sondern zu Recht darauf verweist (Engel, S. 708), dass die Rechtsprechung eine Zumutbarkeitsgrenze anerkennt, die vom jeweiligen Gefährdungspotenzial abhängt, dazu auch oben 2.2.4.3, vgl. auch Oechsler in Staudinger, Kommentar zum Bürgerlichen Gesetzbuch, 03, § 2 ProdHG Rdnr. 70 m.w.N.

allen Anwendungen 100 %-ig fehlerfrei funktionieren kann[191]. Dieser Umstand hat nun aber gerade nicht zur Folge, dass deshalb die Gewährleistung und/oder Haftung für Software von vornherein zwingend beschränkt werden oder gar ausgeschlossen sein müsste. Auch fragt sich, ob Programmierungsleistungen in einem Maße besonders sind gegenüber anderen (Dienst)Leistungen, dass dies eine andere rechtliche Beurteilung erfordere bzw. eine andere Anwendung der für alle anderen, z.T. ebenfalls sehr komplexen Waren oder Dienstleistungen bestehenden gesetzlichen Vorschriften.

Denkbar ist zwar evtl. im Ausgangspunkt, dass der Verschuldensmaßstab bei Programmierung von Software herabgesenkt wird, indem man sagt, kraft Natur der Sache müsste bei Programmierungsleistungen *per definitionem* ein anderer Verschuldensmaßstab angelegt werden[192]. Auch hierfür gibt es aber – mangels entsprechender gesetzlicher Ausnahmen für Programmierleistungen – letztlich wohl keine haltbare rechtliche Handhabe. Im Ergebnis ist damit auch und gerade im Hinblick auf die mittlerweile nahezu Omnipräsenz von Software in unseren Lebensbereichen nicht einzusehen, warum bzgl. Softwareleistungen ein geringerer Maßstab an die Anforderungen des Verschuldens im Rechtssinne gelegt werden soll als bei anderen Leistungen. Aufgrund wohl ähnlicher Erwägungen hat auch die Rechtsprechung den lange Zeit als zulässig erachteten Ausschluss der Haftung für leichte Fahrlässigkeit in AGB im Zeitablauf nicht mehr als zulässig angesehen[193], und zwar insb. dann auch nicht (mehr) für den Bereich Software(-Leistungen)[194].

Ein anderes Ergebnis wäre auch mit zentralen Rechtsvorschriften in Deutschland sowie in der Europäischen Union nicht vereinbar. Zu diesen zentralen Rechtsvorschriften zählt in Deutschland auch das Produkthaftungsgesetz und die für das gesamte Produkthaftungsrecht in Deutschland generell geltende Rechtsvorschrift, dass die Ersatzpflicht des Herstellers nach dem Produkthaftungsgesetz im Voraus weder ausgeschlossen noch beschränkt werden darf (§ 14 Satz 1 ProdHG). Diese Rechtsvorschrift ist sog. zwingendes Recht, d.h. ihr Regelungsgehalt kann nicht vertraglich abbedungen werden, wie Satz 2 dieser Vorschrift ausdrücklich noch einmal betont: „Entgegenstehende Vereinbarungen sind nichtig."

---

191 Engel, CR 86, 702, 707 der zu Recht darauf verweist (Engel, S. 708), dass die Rechtsprechung eine Zumutbarkeitsgrenze anerkennt, die vom jeweiligen Gefährdungspotenzial abhängt, dazu auch unten 2.2.4.3.

192 Für die vertragliche Haftung in diese Richtung Heussen, CR 04, 1, 9.

193 BGH NJW 93, 335.

194 Erben/Günther/Kubert/Zahrnt, IT-Verträge, Wirksame und unwirksame Allgemeine Geschäftsbedingungen, 4. Aufl. 07.

Damit ist ganz klar zum Ausdruck gebracht, dass das ProdHG und der mit ihm verfolgte Schutzzweck: Schutz der Sicherheit der Allgemeinheit vor Körperschäden und Sachschäden durch fehlerhafte Produkte in keiner Weise einschränkbar oder ausschließbar ist und dass das Rechtsgut der Sicherheit der Allgemeinheit letztlich immer schwerer wiegt als die anderen Interessen, insb. wirtschaftliche Interessen Einzelner, aber auch potenzielle politische bzw. gesamtwirtschaftliche Interessen der Allgemeinheit. Allerdings kann ein Produkt gerade aufgrund seiner Eigenschaften auch der Sicherheit der Allgemeinheit dienen. Daher ist im Hinblick auf die Zulässigkeit von OC-basierter Softwaresysteme abzuwägen, ob ein Produkt, auch wenn es ein bestimmtes Gefahrenpotenzial aufweist, ggf. (trotzdem) dann in den Verkehr gebracht werden darf, wenn nach dem Stand der Technik Fehler nicht auszuschließen sind[195].

2.7. Besonderheiten wegen Schnittstelle Mensch/Maschine: Wem sind die Fehler zuzurechnen, Mensch oder Maschine?

Die Produkthaftung nach dem Produkthaftungsgesetz ist eine verschuldensunabhängige (Gefährdungs-)Haftung, die ihren rechtspolitischen Grund darin hat, dass der Hersteller das Risiko für die Gefährlichkeit seines Produkts tragen soll, da er aus dem Inverkehrbringen des Produkts auch entsprechenden Nutzen (= Gewinn) zieht. Daher setzt die gesetzliche Produkthaftung eine rein kausale Verursachung des Schadens durch den Fehler voraus, und zwar weitgehend (s. zu den Ausnahmen ausführlich oben[196]) unabhängig davon, ob der Hersteller den Fehler auch verschuldet hat. Deshalb ist die kausale Verursachung von der Frage der Vorwerfbarkeit im Sinne eines Verschuldens zu trennen. In rechtspolitischer Hinsicht kann man sich fragen, ob möglicherweise wegen des fehlenden Verschuldens im Sinne eines vorwerfbaren Handelns die Produkthaftung bei Organic Computing eingeschränkt werden sollte oder müsste.

2.7.1. Verursacherprinzip vs. Verschuldensprinzip

Die häufig gestellte Frage, ob man einer Maschine (Computer) im zivil- oder strafrechtlichen Sinne einen Verschuldensvorwurf machen kann, geht wohl tendenziell in die falsche Richtung, da der Computer nicht für tatbestandsmäßige und schuldhaft vorwerfbare Aktionen strafrechtlich zur Verantwortung gezogen werden kann, sondern nur die Person, die hinter dem Computer steht und diesem das gegeben hat was der Computer ausführt, sei es gewollt oder ungewollt. Das betrifft auch die Frage

---

195 S. ausführlich Ziffer 2.2.4.3.

196 S. Ziffer 2.2.

der sog. Emergenz im Sinne eines unvorhersehbaren Verhaltens[197]: Derjenige, der das konkrete IT-System mit dem ihm offen oder latent und damit jedenfalls inzident vorhandenen emergenten Verhaltensweisen programmiert hat, ist letztlich für das von ihm generierte Verhalten verantwortlich und muss sich dafür zur Verantwortung ziehen lassen[198].

Da Computer weder soziale Wesen sind noch Gefühle haben, ist es wohl abwegig, Computern einen Verschuldensvorwurf zu machen, weil Verschulden eine wertende Wahl zwischen richtig und falsch bedeutet. Computer können nicht verantwortlich für ihre Wertung gemacht werden, sondern nur die hinter ihnen stehenden Personen, die die Parameter für diese Entscheidung gesetzt haben. Es ist zwar richtig, dass Computer mittlerweile in fast alle Lebensbereiche Einzug genommen haben und auch, dass damit in nahezu allen Lebensbereichen heutzutage mittlerweile bestimmte Entscheidungen immer mehr von IT-Systemen getroffen werden. Z. B. führt die Buchung eines Flugzeuges heutzutage nicht mehr die Boden-Stewardess aus, sondern ein Computer, entweder von dem Reisepersonal der Fluggesellschaft, sei es durch von diesem beauftragten Personal, z. B. ein Reisebüro, oder sei es vom Endanwender selbst, der von zu Hause aus über das Internet seinen Sitzplatz bucht. Ganz ähnlich wird die Entscheidung darüber, ob eine bestimmte Musik-CD am Lager verfügbar ist, nicht mehr durch einen Menschen getroffen, der den Lagerbestand durchsucht und uns diese Mitteilung macht, sondern durch ein Computersystem in Form eines Warenwirtschaftsprogramms, während der Verkäufer – wenn überhaupt noch – nur anhand des Computersystem prüft, ob der Artikel am Lager verfügbar ist bzw. wann er geliefert werden kann, ggf. in Abhängigkeit von der Lieferung eines Vorlieferanten, etc.. Wenn nun aber der Sitzplatz wegen Doppelbuchung oder fehlerhafter Ausführung der Buchung im Flugzeug bei Besteigen des Flugzeugs bzw. Einchecken am Flughafen nicht mehr verfügbar ist oder wenn der Artikel: Musik-CD nicht innerhalb der vom Computersystem bestätigten Lieferzeit geliefert werden kann, trägt im Ergebnis hierfür nicht das Computersystem die Verantwortung, sondern der Verkäufer, der das Computersystem einsetzt.

Ein weiteres Beispiel ist der Auto-Piloten im Navigationssystem eines Flugzeugs. Auch hier ist bei einem Fehler nicht der Computer haftbar, sondern der Mensch bzw. die Organisation hinter dem Computer als Hersteller des Computers. Nach allem ist es wohl verfehlt, Computersysteme selbst in irgendeiner Art und Weise für die von ihnen kausal verur-

---

197 Siehe Ziffer 2.2.4.1.

198 Siehe dazu ausführlich Ziffer 2.3.2.

sachten ggf. fehlerhaften Handlungen verantwortlich zu machen oder ggf. machen zu wollen.

2.7.2. Verantwortlichkeit von Maschinen für Handlungen

Der Versuch, Maschinen eigenverantwortlich zur Verantwortung ziehen zu wollen, ist wiederholt unternommen worden[199]. Bereits in den 80-er Jahren wurde verstärkt versucht, Computersystemen eine moralische bis hin zu einer rechtlichen Verantwortlichkeit zu geben. Alle derartigen bisherigen Versuche, die Maschine selbst für „ihr Fehlverhalten" verantwortlich zu machen bzw. machen zu wollen, können heute wohl als fehlgeschlagen gelten, jedenfalls hat sich diese Auffassung so nicht durchgesetzt.

Snapper[200] führt *Aristoteles*' Verantwortungstheorie (Nikomachische Ethik, 3. Buch) an, um die Verantwortlichkeit für überlegte Entscheidungen und Wahlen dem Computer zuzuschreiben mit der Folge, dass die Maschine ein verantwortlicher Handelnder sei, da der Computer unterschiedliche Alternativen und Bedingungen in einem Optimierungsmaßstab abwäge und deshalb eine überlegte Wahl treffe.

Diese Betrachtungsweise lässt außer Acht, dass Computersysteme zwar abwägende Entscheidungen treffen (können). Sie tun das aber ohne selbst reflektierende Bewusstseinsprozesse oder bewusste Repräsentationen, die das Selbst und die Lage des Handelnden sowie seine Einbettung im Kontext anderer Handelnder berücksichtigen[201]. Das bedeutet, dass man Computersystemen dann – aber auch nur dann – für ihre Entscheidungen und die daraus folgenden Handlungen verantwortlich machen kann, wenn man den Begriff Verantwortlichkeit von Kriterien wie Bewusstsein, Sozialität und Moralität abtrennt. Das geht indessen wohl nicht, weil der Begriff Verantwortlichkeit hiermit letztlich untrennbar verbunden ist und ansonsten seines Sinnes entleert würde.

---

199 Einen guten Überblick gibt Lenk: Können Informations- und Robotersysteme verantwortlich sein?, Ethische und soziale Chancen sowie Probleme der neuen Informationstechnologien, in: Ethik und Informationstechnik am Beispiel der Telemedizin, Ausgabe 2/03, auch abrufbar unter http://www.uibk.ac.at/psychologie/mitarbeiter/leidlmair/koennen_informations-_und_robotersysteme_verantwortlich_sein.pdf.

200 Responsibility for Computer-Based Errors. in: Metaphilosophy 16 (1985), 289-295.

201 So zurecht Lenk: Können Informations- und Robotersysteme verantwortlich sein?, Ethische und soziale Chancen sowie Probleme der neuen Informationstechnologien, in: Ethik und Informationstechnik am Beispiel der Telemedizin, Ausgabe 2/03, auch abrufbar unter http://www.uibk.ac.at/psychologie/mitarbeiter/leidlmair/koennen_informations-_und_robotersysteme_verantwortlich_sein.pdf, S. 11.

Einen ähnlichen Versuch hatte *Bechtel*[202] unternommen, der Bedingungen vorschlug, unter denen man Computer als verantwortliche Handelnde konstruieren könnte und sie damit für ihre Entscheidungen verantwortlich machen könnte. Ausgehend von der von ihm als Notwendigkeit erkannten Bedingung, dass der Handelnde in der Kausalkette, welche zur Entscheidung führt, auftritt oder wenigstens fähig war, in sie einzugreifen, müsse die Entscheidung vom Handelnden stammen und in der Kontrolle des Handelnden sein, müssten diese als intentionale Systeme[203] ihre Handlungen „als Ergebnis bestimmter Wünsche oder Meinungen“ auffassen können. Wichtig sei dabei, dass man Entscheidungen und Urteile nicht nur über interne Zustände, sondern auch über die Beziehung des intentionalen Systems zu seiner Umgebung dazurechne. Hierzu sei eine Metaebene der Erfassung und der Selbstreferentialität im Sinne der Fähigkeit zur Darstellung des internen Zustandes und der Bezugnahme auf diesen erforderlich. Solche intentionalen Systeme vermögen somit Symbole teleologisch und sozusagen mit Richtungsbedeutung behaftet zu verwenden und könnten damit auch adaptiv und evtl. auch lernfähig sein. Soweit Computer- und Entscheidungssysteme als Systeme mit interner Adaptionsfähigkeit in der Lage seien, ihre internen Zustandsbeschreibungen und Bezugnahmen den Signalen und Daten der äußeren Umgebung anzupassen, könnten sie ihre Reaktionen auf Daten entsprechend dem eingegebenen Programm oder den strategischen Metaprogrammen abändern: „Solche Systeme können ihr Verhalten und sogar ihr Verhaltensprogramm in Reaktion auf die Umgebung abändern“ (Bechtel, a.a.O). Hierzu bedürfe es der „Metaregeln, die dazu dienen, andere Regeln innerhalb des Systems zu ändern. Zum Beispiel erfordere Lernen innerhalb eines Produktionssystems innere Produktionsregeln, die, wenn sie aktiviert werden, geeignet seien, neue Erzeugungen hinzuzufügen oder andere aufzugeben oder zu ändern“. Zwar könne ein Computer der traditionellen sequentiellen Von-Neumann-Architektur dieses nicht leisten, aber es gäbe zunehmend Modelle und Realisierungen von „parallel verarbeitenden Prozessautomaten, die entsprechend der Neuronennetzwerke im menschlichen Gehirn modelliert sind“ (Bechtel, a.a.O.).

Bechtel schließt nun daraus, solche parallelverarbeitenden, lernenden umgebungsabhängigen und in eine Umgebung eingebetteten Systeme bräuchten zwar nicht interne Wünsche und Glaubenszustände im realistischen Sinne aufzuweisen, würden aber funktional entsprechend reagieren, ja, „handeln“, als hätten sie intentionale Zustände als ursächliche Faktoren für ihre Verhaltensentscheidungen. Die große Flexibilität, Adaptier- und Lernfähigkeit gegenüber den Signalen und Anstößen aus der Umgebung, die interne Fähigkeit zur Ausbildung von Lernstrategien und entsprechenden Metare-

---

202 William Bechtels (1985) Plädoyer für die „Zuschreibung von Verantwortlichkeit zu Computersystemen“.

203 Vgl. dazu Dennett (D.), 1978, Brainstorms, Cambridge MA 1978.

geln über Verhaltensregeln, würden es erlauben, das System so zu behandeln, als habe es Meinungen und Wünsche, die für die intern generierten Entscheidungen ursächlich – oder „verantwortlich"? – seien oder gemacht werden könnten. Entscheidungen müssten vom System stammen und unter seiner Kontrolle stehen, um von „Verantwortlichkeit" reden zu können. Dies sei so bei intentionalen Systemen: „Was wir behaupten, wenn wir Verantwortlichkeit einem intentionalen System zuschreiben, ist, dass es die gemachte Entscheidung traf, weil der Handelnde so geartet war. Das erklärt, wie die Entscheidungen eines intentionalen Systems aus ihm stammen" (Bechtel, a.a.O.). Entsprechendes gelte für die Reaktions- und Adaptionsfähigkeit eines lernenden Systems gegenüber der Umgebung, so dass man von einer Entscheidung sprechen könne, die unter der Kontrolle des Systems ist. „Wenn wir Computersysteme haben, die derart anpassungsfähige Systeme sind, dass sie in eine Umgebung eingebettet werden und ihre Reaktionen dieser Umgebung anpassen können, dann scheint es, dass wir alle jene Züge menschlicher Wesen erfasst haben, die wir berücksichtigen, wenn wir letztere für verantwortlich halten. Wenn wir dieses Ergebnis akzeptieren, dass einige Computersysteme für ihre Entscheidungen verantwortlich gemacht werden können, wenn sie anpassungsfähige Systeme sind, die es gelernt haben, sich in ihrer Umgebung in bestimmten Weisen zu verhalten, dann wird es Bedingungen geben, unter denen wir ihnen vergeben und sie nicht für verantwortlich halten" (Bechtel, a.a.O.). Hieraus schließt *Bechtel*, dass es möglich sei, Computersysteme zu entwerfen, die „für ihre Entscheidungen verantwortlich gemacht werden können" (Bechtel, a.a.O.).

Lenk[204] sieht Ausnahmen von der Verantwortungsfähigkeit, sowohl im rechtlichen als auch im moralischen Sinne. Insb. stelle sich nach *Lenk* die Frage, ob jemand für einen Schaden verantwortlich gemacht werden könne, den er beim Stande seines Wissens nicht hatte vorhersehen können[205] bzw. ob jemand außer in professionellen formal klar strukturierten Kontexten für ein Nichtwissen zur Verantwortung gezogen werden könne im Sinne eines: „Er hätte es wissen können, ja, wissen müssen...." [206]. *Lenk*[207] nimmt sodann an, dass dem Informations- und Entscheidungssystem keineswegs die Verantwortlichkeit dafür zugeschrieben werden könnte, dass es eine weitere Option

---

[204] Lenk: Können Informations- und Robotersysteme verantwortlich sein? Ethische und soziale Chancen sowie Probleme der neuen Informationstechnologien, in: Ethik und Informationstechnik am Beispiel der Telemedizin, Ausgabe 2/03, auch abrufbar unter http://www.uibk.ac.at/psychologie/mitarbeiter/leidlmair/koennen_informations-_und_robotersysteme_verantwortlich_sein.pdf, S. 14 Fn. 4.

[205] vgl. Lenk-Ropohl, 87, 130, Lenk, 92, 144f; s.a. ders. 97, 98; Können Informations- und Robotersysteme verantwortlich sein (Fn. 204), S. 14 Fn. 4.

[206] vgl. Lenk-Ropohl, 87, 130, Lenk, 92, 144f; s.a. ders. 97, 98: Können Informations- und Robotersysteme verantwortlich sein?, S. 14 Fn. 4.

[207] Lenk: Können Informations- und Robotersysteme verantwortlich sein? (Fn. 204), S. 14 Fn. 4.

in seinem Programm und seinem Strategienrepertoire der Metaregeln nicht aufweise. Hier scheint sich für *Lenk* auch deskriptiv eine entscheidende Differenz zwischen einem lernfähigen programmierbaren Entscheidungssystem und dem verantwortlichen Menschen zu ergeben, ganz abgesehen vom Aspekt der normativen Verantwortungszuschreibung.

2.7.3. Rechtliche Verantwortlichkeit

Man sieht an dieser Darstellung, dass die (auch) mit den Organic Computing aufgeworfenen Fragen jedenfalls im Ansatz bereits seit längerer Zeit Gegenstand verschiedener Überlegungen waren und begutachtet wurden, wenn auch nicht rein bzw. streng in einem rechtswissenschaftlichen Kontext.

Der Fall des Organic Computing zeigt, dass die Rechtswissenschaft tatsächlich nicht strikt den Geisteswissenschaften zuzuordnen ist, erst recht wohl aber nicht den Naturwissenschaften, sondern eine Wissenschaft eigener Art ist[208], und zwar interdisziplinär, weil bestimmte Fragen nicht aus ihrem gesamtgesellschaftlichen Kontext herausgerissen untersucht werden können bzw. dürfen, da zu viele Wechselwirkungen zu beachten sind. Bzgl. Organic Computing stellt sich z. B. die komplexe Frage, ob angesichts des potenziellen Nutzens solcher Systeme nicht in rechtspolitischer Hinsicht eine Öffnung des Rechtsrahmens erfolgen sollte, die die Einführung solcher Systeme klar erleichtern würde. Wie auch unter Ziffer 1.2 bereits dargestellt, gilt es aber vor dem Hintergrund der rechtswissenschaftlichen Analyse ganz unterschiedliche Aspekte zu berücksichtigen, die letztlich alle vor dem Hintergrund des überragend wichtigen Rechtsguts: Schutz und Sicherheit der Allgemeinheit zu begutachten sind. Der Auftrag für die Staatsgewalt: Schutz und Sicherheit der Allgemeinheit, der im ProdHG eine seiner konkreten Auswirkungen erfährt, hat Verfassungsrang.

Der Ansatz, die Verantwortlichkeit für Computerfehler dem Computer selbst zuzuschieben, ist deshalb vor dem Hintergrund der in Deutschland geltenden Verfassung und ihrer Ausgestaltung z. B. im ProdHG verfehlt. Es kann nicht richtig sein, die Verantwortlichkeit für das Handeln einer Maschine der Maschine selbst zuzuschreiben, jedenfalls nicht, was die *Haftungsfolgen* betrifft. Denn das geltende Rechtssystem sieht Regelungen über die Folgen unerlaubter Handlungen vor, und zwar zum Schutz der am Rechtsverkehr Beteiligten und zum Schutz des Rechtssystems selbst: Wenn das Rechtssystem aber keine Sanktionen gegen unerlaubte und damit rechtswidrige Handlungen vorsähe, würde es sich selbst

---

[208] Vgl. ganz aktuell zu diesem Thema: Hoeren, "Vom faulen Holze lebend" in F.A.Z., vom 30.07.09, „Staat und Recht"; vgl. auch Jehring, Ist die Jurisprudenz eine Wissenschaft?, Göttingen, 2. Aufl. 09.

die Grundlage und auch Rechtfertigung nehmen. Deshalb müssen die gesetzlich vorgesehenen Rechtsfolge, insb. auch die Haftungsfolgen uneingeschränkt gelten.

Das gilt dann auch bzgl. Organic Computing: Auch wenn die möglichen Anwendungsgebiete des Organic Computing nahezu unbedgrenzt sind, da Computersysteme, die sich selbst-optimieren können, potenziell überall eingesetzt werden können und ihr potenzieller Nutzen damit enorm sein kann, so muss doch gleichzeitig ganz klar sein, dass auch solche Systeme nur im Rahmen der bestehenden Gesetze und der von diesen vorgesehenen Rechtsfolgen eingeführt werden dürfen. Diese sehen vor, dass bei potenziellen Gesundheitsschäden bei Fehlern die Anforderungen an die Sicherheit des Produkts deutlich höher sind als wenn lediglich Sachschäden drohen, weil hier die berechtigten Erwartungen der Allgemeinheit höher liegen. Soweit technische Normen unterschiedliche Anwendungen je nach Risikoklasse stellen[209], sind diese Anforderungen als Mindeststand der Technik einzuhalten[210]. Gleichwohl muss das Produkt nicht in allen denkbaren Gefahrensituationen jede technisch mögliche Sicherheit bieten[211], z. B. kann nicht erwartet werden, dass jeder Pkw mit einem Airbag ausgestattet ist, sondern dass das nur bei dem vorgesehenen Gebrauch so sein muss. Dementsprechend kann man bzgl. OC Systemen evtl. auch wie folgt argumentieren: Wer es zulässt, dass das ein System in gewissem Maße selbständig Kontrolle ausübt, ist damit auch einverstanden. Aber selbst wenn das so ist, bedeutet das ja deshalb nicht, dass der einzelne Anwender damit auf Haftungsansprüche gegenüber dem Systemhersteller verzichtet hätte, genauso wie der Anwender nicht auf Haftungsansprüche verzichtet (hat), wenn der Autopilot fehlerhaft programmiert ist oder die Adaptive Cruise Control nicht abbremst, obwohl sie müsste.

Produkthaftungsansprüche bestehen nur im Rahmen der allgemein üblichen Verlässlichkeit (Reliability) des IT-Systems. Diese kann mal höher sein (z. B. bei sicherheitsgerechterer Software), mal niedriger (z. B. bei Trivialprogrammen). Dabei hängt das Maß an Sicherheit immer auch vom Preis des Produkts ab, wobei aber der Erwerber und insb. jeder Dritte erwarten darf, dass eine bestimmte Basissicherheit gegeben ist[212], z. B. gut funktionierende Bremsen. Es ist aber nicht erforderlich, dass jedes Kfz das nach dem Stand der Technik bestmögliche Bremssystem

---

209 Z. B. die IEC 61508 für Hardware.

210 S. Ziffer 2.2.4.4.

211 Kullmann, ProdHG, Kommentar, 4. Aufl. 04, S. 113.

212 Kullmann, ProdHG, Kommentar, 4. Aufl. 04, S. 114.

hat. Gleiches gilt auch im Hinblick auf den Einsatz bestimmter Konstruktionen[213] und eben auch bestimmter Systeme wie OC Systeme. Deshalb muss letztlich jedes System diejenige Sicherheit bieten, wie die Allgemeinheit sie je nach Einsatzgebiet erwarten darf. Z. B. ist bei einem Einsatz eines Systems in der Bremssteuerung die Einschaltung von Notfallsystemen unabdingbar, damit zumindest eine herkömmliche Bremsleistung immer gegeben ist, es kann aber z. B. im Hinblick auf den potenziellen Einsatz von OC Systemen im Bereich der Bremssteuerung nicht erwartet werden, dass das OC System in jedem Fall lernt, dass der Fahrer mit unüblich hohen Geschwindigkeiten fährt und es daher ständig die bestmögliche Bremsleistungen bereitstellen muss. Wenn sich aber der Eindruck einer solchen Funktionalität ergeben könnte, muss ggf. durch entsprechende Warnhinweise klargestellt werden[214], dass das System nur die Bremsleistung herkömmlicher Systeme sicher bereitstellt (und daher ggf. bei Überschreitung der Richtgeschwindigkeit eine Mithaftung des Fahrers bei Unfällen besteht).

2.7.4. Wie werden die Verantwortlichkeiten unter welchen Bedingungen zugeordnet?

Wie dargestellt[215], ist die Haftung aus dem Produkthaftungsgesetz eine Gefährdungshaftung. Es kommt also nicht darauf an, dass der konkrete Fehler ggf. nicht vorhersehbar war. Die Verantwortlichkeit ist zwar ausgeschlossen, wenn der den Schaden verursachende Fehler des Produkts im Zeitpunkt des Inverkehrbringens nach dem Stand der Wissenschaft und Technik nicht erkennbar war (sog. Entwicklungsfehler), § 1 Abs. 2 Nr. 5 ProdHG[216]. Unter potenzieller Gefährlichkeit des Produkts ist aber nicht der konkrete Fehler des schadensstiftenden Produkts, sondern das zugrundeliegende allgemeine, mit der gewählten Produktion verbundene Fehlerrisiko zu verstehen[217]. Dieses Fehlerrisiko ist bei OC Systemen ganz klar als solches vorhersehbar, weil das System sich selbstständig fortentwickelt, das ist ja gerade Sinn von OC Systemen. Man kann daher nicht argumentieren, bei Organic Computing Systemen, bei der sich die Software ja gerade unabhängig von Vorgaben selbständig entwickeln soll, sei die konkrete Gefährlichkeit in sicherheitskritischen Bereichen aus der Natur der Sache heraus nicht vorhersehbar, so dass (deshalb) keine Verantwortlichkeit gegeben sei. Das wäre wohl ein Zir-

---

213 Kullmann, ProdHG, Kommentar, 4. Aufl. 04, S. 100.

214 S. Ziffer 2.2.5.3.

215 S. Ziffer 2.1.

216 BGH, Urteil vom 16.06.09, Az. VI ZR 107/08, Rdnr 28 „Airbag“ m.w.N.

217 BGH, Urteil vom 16.06.09, Az. VI ZR 107/08, Rdnr 28 „Airbag“ m.w.N.

kelschluss. Vielmehr ist gerade bei solchen Systemen letztlich genau umgekehrt alles, was – und sei es nur irgendwie – vorhersehbar ist, auch zurechenbar.

Das gilt jedenfalls im zivilrechtlichen Sinne, aber wohl auch (sogar) strafrechtlich. Deshalb muss die potenzielle Kreativität von OC-Techniken Ziel gerichtet in Bahnen gelenkt werden, anderenfalls haftet der verantwortliche Hersteller. Denn gerade weil das System potenziell so gefährlich ist, müssen erhöhte Sicherheitsanforderungen gelten, und zwar in jeder Phase, also in der Entwurfs- bzw. Konzeptionsphase, Testphase, sowie bei und erst recht auch nach der potenziellen Markteinführung. Ferner müssen auch aus dem gleichen Grunde auch gegenüber den allgemeinen Anforderungen stark erhöhte Beobachtungs-, Sorgfalts- und Rückruf(plan)pflichten gelten, wenn (= weil) das System sich zur Laufzeit selbst – wenn auch gesteuert – fort schreibt.

2.7.5. Strafrechtliche Haftung / Verantwortlichkeit / Produktbeobachtungspflicht

Aus dem Vorstehenden folgt, dass die Herstellung von OC-Techniken auch vor dem Hintergrund der strafrechtlichen Haftung zu beurteilen ist. Insoweit gilt Folgendes: Wer wissentlich oder mit bedingtem Vorsatz oder bewusster Fahrlässigkeit Produkte in Verkehr bringt, die derart beschaffen sind, dass deren bestimmungsgemäße Verwendung für die Verbraucher – entgegen ihren berechtigten Erwartungen – die Gefahr des Eintritts gesundheitlicher Schäden begründet und/oder trotz erkannter derartiger Fehler im Verkehr lässt, d.h. insb. eine objektiv gebotene Rückrufaktion unterlässt, ist strafrechtlich haftbar, wenn sich die drohenden Gefahren realisieren, u. U. sogar wegen durch Unterlassen begangener vorsätzlicher Körperverletzung[218].

Deshalb ist die Produktbeobachtungspflicht auch vor dem Hintergrund der potenziellen strafrechtlichen Verantwortlichkeit von enorm wichtiger Bedeutung für den Hersteller. Das Verhältnis Produktbeobachtungspflicht zum Verhältnis adaptive IT-Systeme/Verursachungsbeitrag/Verantwortlichkeit ist im Einzelnen schwer zu beurteilen. Relativ klar ist, dass fahrlässig handelt, wer eine objektive Sorgfaltspflicht nicht beachtet, obwohl er sie nach seinen Fähigkeiten hätte beachten können. In der Regel wird man die Einhaltung von technischen Standards als Sorgfaltspflicht ansehen müssen, gerade bei einem Schadensrisiko mit Personenschaden (soweit es in der Norm um die Verhinderung der Schäden geht und die Nichteinhaltung kausal

[218] BGH NJW 1990, 2560 ff.

für den Schaden war). Ebenso gehört es zu den Sorgfaltspflichten, keine Produkte in den Verkehr zu bringen, die – bei bestimmungsgemäßer und rechtmäßiger Anwendung – zu unübersehbaren Schadensfolgen führen können. Wenn (= weil) die konkrete Anwendung sich aber systemimmanent zur Laufzeit fortschreiben kann, dann wird dieser Aspekt wohl jedenfalls bzgl. aller potenziell eintretenden Folgen bedingt durch denjenigen in Kauf genommen, der ein OC System mit derartigen potenziellen Folgen in Verkehr bringt. Denn für diesen war ja vorher absehbar, dass zur Laufzeit eine Selbstadaption stattfindet, das IT-System sich damit selbst (Self X) gewissermaßen fortschreibt und neue Reaktion(en) zur Laufzeit entwickelt und damit ein insgesamt geändertes Anwendungsverhalten emergent entwickelt (hat). Dieser Verantwortung kann man sich nicht ohne Weiteres entziehen oder entledigen.

2.8. Abwägung und Zwischenergebnis

Lenk[219] bemerkt Folgendes: „Zwar ist die Erfüllung bestimmter deskriptiver Bedingungen (wie die erwähnten der Intentionalität, des Verursachthabens, der Kontrolle und Willkürlichkeit der Handlungen) eine notwendige, aber keine hinreichende Bedingung für die normative Zuschreibung der Verantwortlichkeit." Dem ist zuzustimmen. Für Organic Computing Techniken und damit adaptive und auch lernende IT-Systeme bedeutet das, dass eine Haftung des Systems selbst für die von ihr vorprogrammierten Entscheidungen ausscheidet, und zwar mangels Verantwortlichkeit der Maschine und damit im Ergebnis mangels Möglichkeit eines Verschuldensvorwurfs. Auch eine Gefährdungshaftung nach dem ProdHG, die kein Verschulden voraussetzt, scheidet aus den dargestellten Gründen aus[220].

Dieses Ergebnis hat weitreichende Folgen für den Hersteller von adaptiven oder lernenden Systemen. Denn man kann nicht bzgl. Organic Computing Techniken argumentieren, dass derjenige, der hinter der Maschine steht und der diese Maschine in Kenntnis der ihr systemimmanent innewohnenden Eigenschaft: Emergenz, d.h. Unvorhersehbarkeit einer konkreten Entscheidung in einer konkreten Situation, hergestellt hat, nunmehr gleichzeitig zu seinen Gunsten verantwortungsverneinend argumentiert, er könne nicht für einen Schaden verantwortlich gemacht werden, weil er diesen beim Stande seines Wissens nicht habe vorher-

---

219 Lenk: Können Informations- und Robotersysteme verantwortlich sein? Ethische und soziale Chancen sowie Probleme der neuen Informationstechnologien, in: Ethik und Informationstechnik am Beispiel der Telemedizin, Ausgabe 2/03, auch abrufbar unter http://www.uibk.ac.at/psychologie/mitarbeiter/leidlmair/koennen_informations-_und_robotersysteme_verantwortlich_sein.pdf, S. 14.

220 S. Ziffer 2.7.1.

sehen können[221]. Denn die Unvorhersehbarkeit ist ja gerade eine, wenn nicht die hervorstechende Eigenschaft dieser Systeme. Im Gegenteil muss der Hersteller gerade zur Verantwortlichkeit gezogen werden *können*, weil er ja nicht nur hätte wissen können, sondern auch wissen musste, bzw. – noch viel weitergehender – es ja genau wusste, dass er die genaue Handlung der Maschine zur Laufzeit in der realen Umwelt nicht vorhersagen konnte, *wenn das tatsächlich so der Fall ist*.

Anders ausgedrückt: Wer IT-Systeme basierend auf OC-Techniken in Verkehr bringt, ohne bzgl. Herstellungsprozess und fertigem Produkt gegen alle für das konkrete System in dem ihm konkret zugewiesenen Anwendungsbereich potenziell bestehenden Risiken ausreichend Vorsorge zu treffen, bringt damit Produkte in den Verkehr, die einen Fehler i. S. d. ProdHG haben und ist dafür mit allen Konsequenzen auch verantwortlich. Denn die Produkte bieten dann unter Berücksichtigung aller Umstände, insb. des Gebrauchs, mit dem billigerweise gerechnet werden kann, nicht die Sicherheit, die von der Allgemeinheit berechtigterweise erwartet werden kann, jedenfalls solange die Allgemeinheit die spezifische Eigenschaft von Organic Computing: Emergenz und ihre potenziellen Folgen nicht als solche akzeptiert. Deshalb ist es wohl zwingende Voraussetzung für die Durchsetzung von IT-Systemen mit Organic Computing, dass diese einen für die Allgemeinheit akzeptablen Grad an Verlässlichkeit – und damit ist genau eine der weiteren Grand Challenges angesprochen[222] – erreichen, der ausreicht, damit die Anforderungen des ProdHG erfüllt werden, in etwa so, wie die Allgemeinheit es auch akzeptiert, dass Software nach dem Stand von Wissenschaft und Technik nicht 100 %-ig fehlerfrei hergestellt werden kann[223]. Aber selbst dann ist die Gewährleistung und/oder Haftung des Herstellers für das von ihm konkret in Verkehr gebrachte auf OC-Techniken basierende Produkt weder eingeschränkt oder entfällt gar[224].

OC-Techniken müssen damit in jeder Hinsicht, also nicht nur, aber auch ihre (allgemeine potenzielle) gesellschaftliche Akzeptanz betreffend, sicherstellen, dass sie *bestimmte Mindestanforderungen mit an Sicherheit*

---

221 Vgl. Lenk-Ropohl, 87, 130, Lenk, 92, 144f; s.a. ders. 97, 98, Lenk: Können Informations- und Robotersysteme verantwortlich sein?, Ethische und soziale Chancen sowie Probleme der neuen Informationstechnologien, in: Ethik und Informationstechnik am Beispiel der Telemedizin, Ausgabe 2/03, auch abrufbar unter http://www.uibk.ac.at/psychologie/mitarbeiter/leidlmair/koennen_informations-_und_robotersysteme_verantwortlich_sein.pdf, S. 14 Fn. 4.

222 S. Ziffer 1.1.

223 Engel, Produzentenhaftung für Software, CR 86, 702, 708; Oechsler in Staudinger, Kommentar zum Bürgerlichen Gesetzbuch, 03, § 2 ProdHG Rdnr. 70 m.w.N.

224 Siehe zu Ziffer 2.6.1.

grenzender Wahrscheinlichkeit erfüllen. Diese Mindestanforderungen werden im Folgenden behandelt.

3. Welche Anpassungen des Rechtsrahmens bzw. von rechtlich relevanten Standards sind ggf. erforderlich?

3.1. Anpassung des ProdHG und/oder geltender technischer Normen an die Besonderheiten des Organic Computing?

Die Anpassung des Rechtsrahmens, v.a. des ProdHG[225] im Sinne einer Haftungsverschärfung ist bzgl. OC-Techniken nicht erforderlich, weil die Verantwortung für Schäden aus OC Systemen nach der geltenden Gesetzeslage – im Rahmen der üblichen Auslegungsfragen, die abstrakte Normen mit sich bringen – relativ klar zugewiesen ist[226]. Umgekehrt betrachtet ist die Anpassung des Rechtsrahmens, also insb. des ProdHG, im Sinne eines Haftungs*ausschlusses* bzw. einer Haftungs*einschränkung* für Risiken aus OC Systemen wohl weder durchsetzbar (politisch), noch von der Sache her gewünscht und evtl. sogar verfassungsrechtlich nicht möglich bzw. jedenfalls bedenklich[227]. Das ProdHG ist – im Gegenteil – sogar zwingend notwendig und eine der zentralen Rechtsnormen in Deutschland und der EU. Als solche sollte sie im Hinblick auf die potenzielle Einführung von OC-Techniken keinesfalls geändert werden. Eher muss wohl in Konsequenz auf die Einführung von OC-Techniken verzichtetet werden, jedenfalls solange und soweit nicht sichergestellt ist, dass diese den Maßstäben des ProdHG sowie der übrigen anwendbaren sicherheitsrelevanten Gesetze und Normen entsprechen[228].

3.2. Anpassung von Organic Computing an das ProdHG und/oder geltende technische Normen?

Die Fragestellung geht daher wohl im Ergebnis eher in die Richtung, welche Maßnahmen ergriffen werden *müssen*, damit OC Systeme den geltenden rechtlichen Anforderungen entsprechen (können). Hierbei können entsprechende von der Industrie und/oder Wissenschaft selbst entwickelte Standards hilfreich sein, die sicherstellen, dass OC Systeme den dargestellten rechtlichen Anforderungen entsprechen. Denn (Indust-

---

225 Vgl. aber z. B. auch die Straßenverkehrszulassungsordnung (StVZO): „§ 30 Beschaffenheit der Fahrzeuge: (1) Fahrzeuge müssen so gebaut und ausgerüstet sein, dass 1.ihr verkehrsüblicher Betrieb niemanden schädigt oder mehr als unvermeidbar gefährdet, behindert oder belästigt, 2.die Insassen insbesondere bei Unfällen vor Verletzungen möglichst geschützt sind und das Ausmaß und die Folgen von Verletzungen möglichst gering bleiben.“ Letztlich sind die Anforderungen hier also ähnlich.

226 S. Ziffer 2.7.4.

227 S. Ziffern 2.8.

228 Z. B. der StVZO, vgl. Fn. 225.

rie-)Standards, die nicht vom Gesetzgeber ausdrücklich vorgegeben oder vorgeschrieben sind halten in der Regel den Mindeststandard der Technik fest, bei dessen Nichteinhaltung das Produkt einen Fehler hat[229], soweit es sich um sicherheitsrelevante Standards handelt[230]. Dabei hängt die Entscheidung, ob eine Norm sicherheitsrelevant ist, immer auch von den konkreten Umständen ab. So hat zwar die Rechtsprechung[231] entschieden, dass ein Produkt dann keinen Fehler im Sinne des ProdHG hat, wenn eine Norm auch die Angabe des Baujahrs auf dem Produkt erfordert und diese Angabe fehlt; das kann aber bei Software anders sein, weil z. B. für Modifikationen klar sein muss, welche Version geändert wird, weil der Standard dann insoweit sicherheitsrelevant ist. Klar ist aber ungeachtet dessen, dass ein OC System auch bei emergentem Verhalten zu jedem Zeitpunkt alle in technischen Standards vorgeschriebenen Verhaltensweisen – z. B. Reaktionsgeschwindigkeit bei sicherheitsrelevantem Verhalten wie der Auslösung des Bremsvorgangs – aufweisen muss. Insoweit würde deshalb auch eine etwaige Änderung technischer Standards, die z. B. für OC Systeme eine geringere Reaktionsgeschwindigkeit erlauben sollten, nicht helfen, weil technische Standards eben nur die Mindestanforderungen definieren. Wenn für ein konventionelles Systeme eine bestimmte (höhere) Reaktionsgeschwindigkeit Mindeststand der Technik ist, bliebe der Einsatz von OC Systemen auch bei Änderung derartiger Normen deshalb nicht dem Stand der Technik entsprechend.

Anders kann dies bei Normen sein, die den Herstellungsprozess an sich regeln, wie etwa die IEC 61508 oder der für den Straßenverkehr vorgesehene Normentwurf ISO/DIS 26262-6. IEC 61508-3 erlauben ausdrücklich[232], von dem Standard abzuweichen, wenn alle Ziele und Anforderungen des Softwarelebenszyklus (ggf. auch) anderweitig eingehalten werden können. Das muss wohl generell für Normen gelten, die nur den Herstellungs*prozess* regeln, auch ohne derartige ausdrückliche Bestimmungen. Denn nach dem eindeutigen Wortlaut von § 3 ProdHG kann berechtigter Weise nur erwartet werden, dass das (fertige) *Produkt* die Sicherheit bietet, die erwartet werden kann, also dass das *Produkt* den durch technische Normen festgelegten Mindeststand der Technik erfüllt.

---

229 S. Ziffer 2.2.4.4.

230 BGH NJW 1985, 1769, 1770.

231 BGH NJW 1985, 1769, 1770.

232 IEC 61508-3, 7.1.2.5.

Wie das erreicht wird, muss aber – auch im Sinne des technischen Fortschritts – dem Hersteller überlassen bleiben[233].

Allerdings muss der Hersteller bei Eintritt eines Schadens beweisen, dass sein ggf. vom technischen Standard abweichender Herstellungsprozess für das Produkt mindestens die gleiche Sicherheit gewährleistet (hat) wie der normgerechte Herstellungsprozess, während derjenige, der entsprechend der Norm entwickelt, sich zunächst auf die Vermutung berufen kann, dass das Produkt fehlerfrei ist[234], d.h. der Geschädigte muss darlegen und begründen, warum dennoch ein Fehler (Konstruktionsmangel) vorliegen soll.

Für auf OC-Techniken basierende Software werden wohl regelmäßig die Anforderungen aus Ziffer 7.8.2.2 der IEC-61508-3 nicht erfüllt sein und auch kaum erfüllt werden (können), da hiernach eine Modifikation der Software erst nach detaillierter Analyse der möglichen Gefahren der Änderungen stattfinden darf. Soweit auf OC basierende Software sich zur Laufzeit deshalb selbst modifiziert und neu konfiguriert, verstößt das wohl gegen das in IEC 615068 vorgesehene Verfahren für Modifikationen. Soweit es deshalb nicht möglich sein sollte, die Anforderungen der IEC-61508-3 innerhalb des Systems anderweitig zu erfüllen, etwa indem alle potenziellen Änderungsfolgen vorab entsprechend analysiert werden, könnte eine mögliche Lösung dieser Problematik evtl. darin bestehen, die Zielsetzung der IEC-61508-3 auf andere Weise zu erreichen, z. B. dadurch dass sichergestellt wird, dass keine der möglichen Änderungen zu Gefahren führt. Dazu ist als Minimum zwingend erforderlich, dass Änderungen nur in einem vom Hersteller definierten eng begrenzten Korridor systemimmanent zulässig und damit auch tatsächlich (nur) möglich sind.

In jedem Fall sollten diese Lösungsvorschläge bzw. -möglichkeiten in dem jeweils anwendbaren technischen Standard, bzgl. Modifikationen also in der (derzeit noch anwendbaren) IEC 61508-3 beschrieben werden, damit ein Anhaltspunkt dafür besteht, welcher Alternativprozess ein gleiches Mindestmaß an Sicherheit aufweist wie der bisherige Standard. Anderenfalls besteht die Gefahr, dass ein Gericht im Schadensfall einen Verstoß gegen technische Normen im Herstellungsprozess annimmt, mit der Folge, dass das konkrete Produkt fehlerhaft im Sinne des ProdHG

---

233 Kullmann, ProdHG, 4. Aufl. 04, S. 113 schreibt zwar, ein Produkt sei fehlerhaft, wenn bei der Herstellung gewisse Mindeststandards nicht eingehalten werden, die zitierte Rechtsprechung OLG Düsseldorf, Urteil vom 26.02.1993, Az. 13 U 110/97 bezieht sich aber auf ein Abweichung des Endprodukts von technischen Normen (Spalt zwischen Ladefläche und Ladeklappe).

234 OLG Celle NJW 03, 2544; Kullmann, ProdHG, 4. Aufl. 04, S. 113.

ist, der Hersteller ggf. haftet, und das konkrete Produkt u.U. dann so gar nicht hätte in den Verkehr gebracht werden dürfen.

3.3. Welche neuen Herausforderungen ergeben sich in diesen Bereichen für selbstorganisierende(n) adaptive(n) Systeme?

Aufgrund des Gefahrenpotenzials von OC Systemen besteht jedenfalls eine erhöhte Produktbeobachtungspflicht[235]. Weiterhin muss der Korridor für Self-X Eigenschaften in jedem Fall möglichst eng gehalten werden, um ein möglichst geringes Risikopotenzial zu erreichen. Denn nur dann kommt in Betracht, auf OC-Techniken basierende IT-Systeme vor dem Hintergrund der bestehenden Gesetze und Normen in den in dieser Expertise beschriebenen Voraussetzungen und Grenzen als zulässig einstufen zu können, insb. also wenn die im Einzelfall erforderliche Abwägung ergibt, dass das konkrete System einen derart hohen Nutzen hat, der die potenziellen Risiken bei weitem überwiegt, z. B. wenn das System schwere Körperschäden verhindern kann, während sein konkretes Schadensrisiko und die Eintrittswahrscheinlichkeit gering ist, wenn alle erforderlichen Hinweis- und Warnpflichten erfüllt sind[236], sowie wenn das konkrete System nachweislich über permanente und genau spezifizierte Überwachungs- und Kontrollfunktionen seitens des Herstellers verfügt.

3.4. „Lernprozesse“ von OC Systemen / Differenzierung zwischen Systemen, die adaptiv sind, und Systemen die „eigenständig“ lernfähig sind

Lernprozesse von OC Systemen können ggf. das faktische Risiko der Haftung verringern, wenn sie Fehler in den Systemen selbst heilen. Im Übrigen bleibt es aber bei den dargestellten Grundsätzen, d.h. (auch) das Ergebnis des Lernprozesses muss den gleichen Sicherheitsanforderungen genügen wie das Ausgangsprodukt. Hinsichtlich des Gefahrenpotenzials gilt für rein adaptive Systeme wie z. B. Adaptive Cruise Control, dass das Gefahrenpotenzial *vergleichsweise* einfach zu beurteilen ist, da es hierbei (nur) um relativ konstante Wenn-dann-Beziehungen unter fest vorhersehbaren und damit determinierbaren Bedingungen geht. Daher kann relativ einfach beurteilt werden, ob das System anhand der genannten Maßstäbe[237] in den Verkehr gebracht werden darf. Bei eigenständig lernfähigen Systemen indessen ist das Gefahrenpotenzial viel schwerer wenn überhaupt vorhersehbar. Eigenständig lernfähige Systeme dürfen deshalb keinesfalls eigenständig Bedingungen ändern

---

[235] Vgl. BGH NJW 81, 1606, 1607 f. „Benomyl“; BGH NJW 90, 906, 907 „Pferdeboxen“.

[236] Vgl. dazu ausführlich Ziffer 2.2.4.3 und Ziffer 5.

[237] S. Ziffer 4; ausführlich Ziffer 2.2.4.3 und Ziffer 5.

können, die dazu führen können, dass Personenschäden eintreten können. Z. B. darf das System nicht die Frage eigenständig entscheiden dürfen, unter welchen Bedingungen ein Airbag auslöst.

Zudem ist ein permanentes Rückkoppelungssystem unerlässlich, um zuverlässig sicher stellen zu können, dass das System, bevor es auch nur potenziell den Korridor des Spezifizierten (Zuverlässigen) verlässt, etwa um auf Unvorhergesehenes zu reagieren, erst einmal in einen abgesicherten Modus übergeht, in dem es erst durch Eingriff von außen durch einen eigenverantwortlich handelnden Menschen – im Beispiel Kfz: durch den Fahrer – Aktionen ausführt, oder, in zeitkritischen Fällen, nur solche Lösungen selbstständig aktiviert, die im Korridor des Spezifizierten liegen. Gleichzeitig muss in allen Situationen und zu allen Zeiten sicher gestellt sein, dass das System nicht im Leerlauf verharrt oder ggf. auch gar keine Signale mehr senden oder empfangen kann, sondern weiter arbeitet, aber eben sobald potenziell Gefährdung besteht, immer nur in einem Modus, der nur vorhergesehene und jedenfalls *in ihrem Korridor spezifizierte* Aktionen zulässt.

In besonders schwerwiegenden Fällen muss das System zudem eine Meldung geben, dass ein Systemeingriff durch Entwickler erforderlich ist, bevor überhaupt ggf. wieder ein Wechsel vom abgesicherten in den „normalen“ Modus erfolgt bzw. durch den Fahrer des Kfz erfolgen kann. Eine ähnliche Vorgehensweise wird auch in der Forschung vorgeschlagen: Bei Lernenden Systemen könne man ggf. einen Lernkorridor schaffen, z. B. durch die Anpassung von LCS[238], dessen Grenzen in sicherheitskritischem Verhalten liegt und gleichzeitig einen abgesicherten Modus, der immer dann eingreift, wenn der Korridor, gleich aus welchem Grunde, verlassen wird.

Klar ist, dass die Anwendung von Lernenden Systeme in weniger sicherheitsrelevanten Bereichen eher zulässig ist, da hier das Schadenspotenzial ggf. sogar ausgeschlossen ist oder z. B. bei nur geringen Verletzungspotenzialen je nach den übrigen Umständen ggf. die berechtigten Erwartungen der Allgemeinheit an die Sicherheit des Produkts geringer sind[239].

---

238 Learning Classifier Systems, vgl. dazu Prothmann/Rochner/Tomforde/Branke/Müller-Schloer/Schmeck, Organic Control of Traffic Lights, TC 2008, LNCS 5060, 2008, 219, 222.

239 S. Ziffer 2.2.4.3., ausführlich Ziffer 2.2.4.3 und Ziffer 5.

3.5. Sind neuartige Standards denkbar, die die begrenzte Testbarkeit der selbstorganisierenden Systeme berücksichtigen?

Wie dargestellt[240] sind Anpassungen von Rechtsnormen entweder nicht erforderlich bzw., soweit diese die Haftung für Körperschäden beschränken oder gar ausschließen würden, ohne dass dies umgekehrt mit einer Vermeidung noch weitergehender gravierender Schäden gerechtfertigt werden könnte[241], wohl weder politisch durchsetzbar noch mit dem Auftrag des Staates zu vereinbaren, die Staatsbürger vor Gefahren zu schützen,[242].

Soweit (noch) keine allgemeingültigen selbstgesetzten industriellen und/oder wissenschaftlichen Standards bestehen, die ggf. anzupassen wären[243], sind neuartige Standards für OC Systeme denkbar. Der Vorteil aus rechtlicher Sicht wäre dabei, dass damit ein Mindeststandard – nicht mehr, aber auch nicht weniger – geschaffen werden könnte, bei dessen Einhaltung sich der Hersteller zunächst auf die Vermutung berufen könnte, dass das Produkt fehlerfrei ist[244], der Geschädigte also dann darlegen und begründen müsste, warum dennoch ein Fehler vorliegen soll. Derartige Standards könnten darüber hinaus eine Arbeitserleichterung für die Hersteller darstellen und dem einzelnen Hersteller einen Anhaltspunkt bieten, wie er die rechtlichen Anforderungen erfüllen kann. Voraussetzung dafür ist aber immer, dass die (neuen) Standards diese Anforderungen soweit möglich berücksichtigen, z. B. indem in ihnen auch festgelegt wird, dass aufgrund der begrenzten Testbarkeit der Einsatz der Systeme durch ein herkömmliches System ersetzt wird, sobald sich sicherheitskritische Situationen ergeben bzw. dass ggf. festgelegt wird, in welchen Situationen OC Systeme wegen nicht beherrschbaren Risikos von vornherein unzulässig sind (und damit im Umkehrschluss dann aber auch in welchen diese mangels entsprechender Risiken grundsätzlich zulässig sein können, wobei Letzteres eine genaue Prüfung im Einzelfall natürlich nicht entbehrlich machen kann, da es letztlich bei der rechtlichen Betrachtung immer auf das konkrete Produkt im konkreten Anwendungsbereich ankommt).

Im Übrigen wird daran erinnert, dass derartige technische Standards stets nur als Mindeststand der Technik einzuhalten sind, d.h., dass sie

---

240 S. Ziffer 3.5.

241 Vgl. ausführlich Ziffer 2.2.4.3 und Ziffer 5.

242 S. oben Ziffer 2.7.3.

243 Dazu Ziffer 3.

244 OLG Celle NJW 03, 2544; Kullmann, ProdHG, 4. Aufl. 04, S. 113.

den Hersteller nicht vor den in dieser Expertise darstellten Anforderungen[245] befreien, sondern wie dargestellt bei ihrer Einhaltung nur eine Beweiserleichterung für den Hersteller darstellen.

3.6. Welche Auswirkungen haben emergente Eigenschaften auf die Festlegung der Standards und sind dabei Differenzierungen möglich?

Wenn ein entsprechendes Schadenspotenzial grundsätzlich ausgeschlossen ist, etwa bei nicht sicherheitskritischen Anwendungen, z. B. Software, die ausschließlich die Bildverarbeitung von Digitalkameras steuert[246], besteht keine Produkthaftung. Technische Standards hätten dann allenfalls Auswirkungen auf die vertragliche Haftung[247]. Da es aber aufgrund der Privatautonomie möglich ist, die vertraglichen Anforderungen an Produkte im jeweiligen Vertrag festzulegen, können technische Standards in nicht sicherheitskritischen Anwendungen allenfalls dann eine Rolle spielen, wenn eine vertragliche Beschaffenheit nicht vereinbart wird. Damit spielen technische Standards bei nichtsicherheitskritischen Anwendungen nur eine untergeordnete Rolle bzw. liegt es in der Hand der Vertragspartner, deren Bedeutung zu bestimmen. Wenn die Software dagegen grundsätzlich (auch) sicherheitskritisch ist bzw. sein kann, z. B. bei Steuerung auch mechanischer Teile der Digitalkamera bei Verletzungsgefahr, erwartet die Allgemeinheit eben auch bei derartigen Produkten, dass die Produkte die erforderliche Sicherheit bieten, wobei bei nur geringen Verletzungspotenzialen je nach den übrigen Umständen ggf. die berechtigten Erwartungen der Allgemeinheit an die Sicherheit des Produkts geringer sind[248].

3.7. Abwägung und Zusammenfassung

Bei einer Gesamtbetrachtung besteht die rechtspolitische Frage, ob man die Softwarehersteller und Innovationsbereitschaft schützen will, z. B. durch weniger Haftungsrisiken – was politisch und auch verfassungsrechtlich nur in engen Grenzen möglich sein dürfte – oder die Nutzer und übrige Bevölkerung durch hohe Sicherheitsstandards. Denn wenn unvorhersehbar ist, wie sich OC Systeme in sicherheitskritischen Systemen verhalten, wird solche Systeme entweder niemand anbieten, wenn

---

245 S. insbes. Ziffer 2.2.

246 Ein ggf. misslungenes Foto ist keine Rechtsgutsverletzung, da das Produkthaftungsrecht das Vermögen nicht schützt. Allenfalls kommt eine Verletzung vertraglicher Pflichten in Betracht, die aber bei den hier interessierenden Fragen nur sekundär ist, vgl. Ziffer 2.5 und im Text.

247 Dazu oben Ziffer 2.5. Vgl. auch § 434 Abs. 1 Nr. 2 BGB.

248 S. Ziffer 2.2.2.

(= weil) die Haftung unvorhersehbar ist – oder niemand kaufen, wenn (= weil) die erforderliche Sicherheit nicht gewährleistet ist.

Letztlich bietet die bestehende Rechtslage aber ein vernünftiges und verfassungsrechtlich gebotenes[249] Ergebnis in dem Sinne, dass die Haftung für Schäden aufgrund von OC Systemen nur dann ggf. entfällt, wenn diese Systeme – im konkreten Fall – in Verkehr gebracht werden durften, weil die im Einzelfall erforderliche Abwägung ergibt, dass das System im konkreten Fall einen sehr hohen Nutzen hat, weil es schwere Körperschäden verhindern kann, während bestehende gleichzeitig das Schadenspotenzial und -risiko sowie seine Eintrittswahrscheinlichkeit so gering ist, dass eine Abwägung der Vorteile die potenziellen Nachteile bei weitem überwiegt[250]. Ist das nicht der Fall, bleibt es für den Hersteller wie in anderen Bereichen auch, in denen potenziell gefährliche Produkte in Verkehr gebracht werden, im Gegenzug für die für den Hersteller mit dem Inverkehrbringen verbundenen Vorteile wie Gewinnerzielung, höhere Marktanteile aufgrund der Vorteile von OC Systemen etc. bei der vollumfänglichen potenziellen Haftung im Rahmen der bestehenden Gesetze.

4. Entwicklung erster Ansätze zur rechtsvermittelten Vertrauenserzeugung gegenüber selbstorganisierenden, adaptiven Systemen und zum Rechtsgüterschutz

Das bestehende Rechtssystem ordnet die Verantwortung für OC Systeme recht konkret zu und führt zu entsprechenden potenziellen Haftungsfolgen bei den Herstellern. Um Vertrauen in OC Systeme zu schaffen, sind daher wohl weniger neue Gesetze erforderlich – abgesehen von besonders kritischen Bereichen wie Straßenverkehr oder Zulassungsvoraussetzungen[251] –, sondern statt dessen eher eine frühzeitige und aktive Aufklärung der technischen Neuerungen häufig skeptisch gegenüberstehenden Bevölkerung über die Rechtslage sowie darüber, dass anders als etwa bei Umweltsummationsschäden[252] eine klare Verantwortungszuweisung gegeben ist, und ggf. auch darüber, welche Gefahren mit OC Systemen tatsächlich verbunden sind und welche Eigenschaften ein OC System nicht hat und auch nie haben wird (keine selbstbewussten Maschinen) und warum das so ist.

---

249 Vgl. dazu auch di Fabio, Udo, Die Risikoentscheidung im Rechtsstaat, Tübingen 1994.

250 Vgl. dazu ausführlich Ziffer 2.2.4.3und Ziffer 5; vgl. auch Fn. 225.

251 S. Ziffer 4.3.3

252 S. Ziffer 2.3.2.

4.1. Lernende Systeme – unter welchen Bedingungen können sie eingesetzt werden?

Das Problem, dass die Systeme nicht vorhersehbar agieren, muss so kontrolliert werden bzw. zumindest so kontrolliert werden *können*, dass auch die Ergebnisse in dem Sinne vorhersehbar sind, dass – jedenfalls innerhalb bestimmter Grenzen – zwischen gewollt und nicht gewollt unterschieden werden kann. Dazu ist in jedem Fall für das konkrete System ein Satz vordefinierter Parameter bereit zu stellen, der nicht änderbar ist. Dieser Satz muss den absoluten Worst Case (Super-GAU) abdecken, der unter keinen Umständen und/oder keinen denkbaren Bedingungen eintreten darf. Auch wenn das einen bestimmten Systembruch bedeutet, da dadurch die Kreativität der Systeme gehemmt wird, so ist doch dieses Hemmnis eine notwendige Bedingung dafür, dass eine bestimmte im Sinne von: in ihrem Korridor spezifizierte Kontrolle möglich ist und damit letztlich wohl eine notwendige, wenn auch ggf. nicht hinreichende Bedingung dafür, dass OC-Techniken in sicherheitskritischen Bereichen bzw. Anwendungen eingeführt werden können und in rechtlicher Hinsicht zulässig sind. – So muss z. B. sicher gestellt sein, dass bei Ampelsteuerung durch OC-Techniken an einer Kreuzung mit vier Ampeln zu keinem Zeitpunkt alle vier Ampeln gleichzeitig auf grün gestellt sind.

Man sollte in diesem Zusammenhang aber auch nicht übersehen, dass auch bei „herkömmlicher Software-Entwicklung“ nicht alle Anwendungskombinationen und Anwendungsszenarien vorhersehbar sind oder vor der Markteinführung des konkreten Systems konkret getestet wurden bzw. vom Hersteller, dem die konkrete Anwendung gar nicht bekannt gewesen sein muss, getestet werden konnten.

4.2. Vertrauensaspekte (Trust)

Es ist wohl richtig, dass es nicht so sehr eine Frage ist, ob adaptive Systeme kommen, sondern wie wir sie gestalten werden[253], jedenfalls in sicherheitsunkritischen Bereichen bzw. Anwendungen. Deshalb sollte unbedingt, damit nicht die Furcht vor der „Unkontrollierbarkeit“ selbstorganisierender Self-X–Systeme mit emergentem Verhalten überwiegt, nicht nur der Bevölkerung, sondern auch den Herstellern die rechtliche Situation und die Konsequenzen bei Nichteinhaltung der rechtlichen Anforderungen an die Produktsicherheit dargestellt werden, um zu gewährleisten, dass die Hersteller die in rechtlicher Hinsicht geltenden Anforderungen einhalten, auch um (aus Selbstschutz) soweit möglich Haftungs-

[253] Müller Schloer, Organic Computing, Informatik Spektrum 04, S. 336.

fälle zu vermeiden und damit die Bevölkerung darauf vertrauen kann, dass dies auch geschieht.

Dabei geht es um Fragen der Sicherheit in Richtung Safety, aber auch in Richtung Security. Security deshalb, weil die Systeme über drahtlose Netzwerke wie Bluetooth, UMTS oder Wireless-LAN interagieren und damit Sicherheitsrisiken auch im Sinne von Security entstehen, die gemanagt werden und kontrollierbar gemacht werden müssen. Die rechtlichen Anforderungen an die Sicherheit von lernenden OC Systemen werden daher *im Regelfall* die im Folgenden dargestellten sein, wobei dies natürlich letztlich vom konkreten Einsatzgebiet, Schadenspotenzial und den übrigen relevanten Umständen[254] abhängt und daher letztlich *für jedes System spezifisch festgelegt werden muss*: OC Systeme werden eine Mensch-Maschine-Schnittstelle haben müssen, die es zulässt, auf sie einzuwirken, das ist ein essentieller Bestandteil[255]. Sie müssen Methoden befolgen, die geeignet sind, Vertrauen in ihre Verlässlichkeit zu generieren und die gleichzeitig den Schutz der Privatsphäre sicher stellen und gewährleisten. Daher braucht es aus rechtlicher Sicht u.a. sorgfältiger Observer-Controller-Architekturen, die sicher stellen, dass ein selbstorganisierendes System kein unerwünschtes globales Verhalten zeigt, vgl. das MAPE Paradigma über Autonomic Computing[256].

Vor allem aber wird auch das Thema: Vertrauen (Trust), entscheidend für die Akzeptanz von OC Systemen sein. Aus rechtlicher Sicht bedeutet das, dass die bestehenden Rechtnormen sicherstellen müssen, dass OC Systeme keine elementaren Rechtsgüter verletzen und Rechtsgutverletzungen zivilrechtlich und strafrechtlich entsprechend sanktionsfähig sind in dem Sinne, dass die Verantwortlichkeiten entsprechend zugeordnet sind. Die geltende Rechtslage, insb. das Produkthaftungsgesetz, leistet dies[257]. Auch andere Rechtnormen, wie etwa das BDSG, geben einen Rechtsrahmen vor, der geeignet ist, je nach Einsatzgebiet aus rechtlicher Sicht Vertrauenserzeugung zu leisten. Insgesamt gesehen wird es vor allem auf die folgenden Vertrauensaspekte ankommen[258]:

---

254 S. Ziffer 2.2.3.

255 Schmeck, A New Vision for Distributed Embedded Systems“, S. 2.

256 Schmeck, A New Vision for Distributed Embedded Systems“, S. 3.

257 S. Ziffer 3.

258 Vgl. Hähner/Bernard, in: Antrag auf Einrichtung einer DFG-Forschergruppe OC-TRUST - Vertrauenswürdigkeit von Organic Computing-Systemen, 08, S. 5.

- **Funktionalität (Functionality)**
  - Die Funktionalität hängt aus rechtlicher Sicht eng mit den Fragen der Ausfallsicherheit, Zuverlässigkeit und Sicherheit zusammen.
  - Soweit das Verhalten von OC Systemen nicht vorhersehbar ist, dürfen diese aus rechtlicher Sicht in sicherheitskritischen Bereichen nur dann eingesetzt werden, wenn z. B. durch Verhaltenskorridore sichergestellt ist, dass das konkrete System nicht sicherheitskritisch verhalten kann bzw. dass es in sicherheitskritischen Bereichen keine Funktionalität ausüben kann. – Damit müsste den vor dem Hintergrund: Trust denkbaren rechtlichen Bedenken ausreichend Genüge getan sein.
  - Industrie-Standards zu schaffen, die auf besondere Bedürfnisse von OC Systemen zugeschnitten sind, wäre sicherlich ein vernünftiger Weg, um diese Anforderungen konkret zu erfüllen.
  - Die Einführung von Zertifizierungsprozessen und -verfahren kann hilfreich sein.
- **Ausfallsicherheit (Safety)**. Aus rechtlicher Sicht muss bei sicherheitskritischen Systemen sichergestellt sein, dass bei einem Ausfall des sicherheitskritischen OC Systems (z. B. Bremssteuerung in einem Kfz) ein herkömmliches System zur Verfügung steht, so dass die sicherheitskritische Funktionalität als solche jedenfalls weiter gegeben ist. – Die geltende Rechtslage ist geeignet, das entsprechende Vertrauen zu vermitteln.
- **Zuverlässigkeit (Reliability)**. Es muss sichergestellt sein, dass OC Systeme die je nach Anwendungsgebiet erforderliche Zuverlässigkeit haben, in sicherheitskritischen Bereichen also ggf. eine 100 %-ige Zuverlässigkeit bzw., wenn dies nicht möglich ist, die Abwägung erfolgen, ob das System dann unter Abwägung der mit dem System verbundenen Vorteile überhaupt in den Verkehr gebracht werden darf[259]. – Das ProdHG enthält die hierfür erforderliche rechtliche Grundlage.
- **Sicherheit (Security)**: Datenschutz, Geheimhaltung, Integrität, Authentizität. Dieser Hauptaspekt ist nicht nur durch das bereits ausführlich behandelte Thema Produkthaftung gewährleistet, sondern auch durch andere Rechtsnormen, wie etwa das Bundesdatenschutzgesetz (BDSG), das die Erhebung, Verarbeitung und Weiter-

[259] Vgl. Ziffer 2.2.4.3 und Ziffer 5.

gabe von Daten nur unter eng begrenzten Voraussetzungen zulässt.

- **Glaubwürdigkeit (Credibility)**. Soweit es um sicherheitskritische Aspekte geht, kann ein Lernen im Hinblick auf die Glaubwürdigkeit anderer Systeme (z. B. Meldungen durch Abstandssensoren) kritisch sein, wenn es nur um eine erhöhte Wahrscheinlichkeit und nicht um Sicherheit geht. Hierzu gilt das, was zur Funktionalität und Ausfallsicherheit ausgeführt wurde.

- **Benutzerfreundlichkeit (Usability)**. Diese Frage ist aus produkthaftungsrechtlicher Sicht von Bedeutung, soweit Schnittstellen mit Sicherheitsaspekten (z. B. Ablenkung des Fahrers vom Verkehrsgeschehen) vorhanden sind. Soweit dies nicht der Fall ist, sind rechtliche Vorgaben nicht wünschenswert, sondern sollte das Thema durch den Markterfolg geregelt werden.

4.3. Standardisierungs- und Zertifizierungsmaßnahmen

Standardisierungs- und Zertifizierungsmaßnahmen können letztlich nur den Zweck haben, die bestehenden rechtlichen Anforderungen auszufüllen bzw. dem Hersteller ein Instrument an die Hand zu geben, mit dem er Anhaltspunkte dafür hat, wie er dem Stand der Technik gerecht wird. Derartige Maßnahmen befreien den Hersteller aber nicht vor den in dieser Expertise dargestellten Anforderungen[260], sondern sind nur ein Hilfsmittel dafür, um diesen Anforderungen gerecht zu werden. Daher können auch die folgenden Ausführungen nur Anhaltspunkte dafür sein, welche Anforderungen dies im Einzelfall sein *könnten*. Inwieweit diese Anforderungen konkret gelten, hängt wie dargestellt[261] von den konkreten Umständen des Einzelfalls ab (Zeit, vorgesehene Verwendung, Gefahrenpotenzial etc.) und muss für jedes System spezifisch festgelegt werden und wird auch von der Rechtsprechung für jeden Fall anhand der genannten Kriterien einzeln entschieden werden. Anforderungen und Maßnahmen könnten z. B. die nachfolgend aufgeführten sein.

4.3.1. Soweit machbar: Reduktion der Komplexität der Systeme

Lernfähigkeit ermöglicht gerade die Vorhersage von Ausfällen, denn Lernen basiert systemgerecht auf zufallsorientierten Explorationen des Entwurfsraums und ist daher fehleranfällig[262]. Da unerwünschte Ergeb-

---

[260] S. insbes. Ziffer 2.2.

[261] S. Ziffer 2.2.

[262]. Müller-Schloer, H. Schmeck, U. Brinkschulte, F. Feldbusch, W. Trumler und Th. Ungerer, in: „Grand Challenges der Technischen Informatik“ Report, März 2008, S. 34.

nisse bei sicherheitsrelevanten Anwendungen soweit möglich ausgeschlossen sein müssen, muss es notwendigerweise zu einer Beschränkung des Lernraums kommen, um damit ein Ziel gerichtetes, kontrollierbares Lernen (design space self-exploration)[263] zu erreichen. Denkbar sind hier z. B. Lernverfahren auf entsprechenden Testgeländen mit entsprechend geschützten Testfahrern. Nur überprüfte Lösungen dürfen dann für den allgemeinen Einsatz freigegeben werden.

4.3.2. Geeignet zur Zielerreichung: Definierte Schnittstellen sowie standardisierte Verfahren

Im Automobilbereich könnten in Gremien, Verbänden wie derzeit: AUTOSAR[264] technische Spezifikationen Vorgaben für die Umsetzung von OC-Techniken geschaffen werden, die Schnittstellen und Verfahren erstellen, die die entsprechend rechtlich erforderlichen Maßnahmen umsetzen. Alternativ bzw. auch parallel können für die jeweilige Industrie verabschiedete Industriestandards bzgl. Spezifikationen zum Entwicklungs- und Herstellungsprozess eine effektive Lösung darstellen, ggf. kombiniert mit Zertifizierungsverfahren und ggf. speziell für OC-Techniken eingerichtete und/oder hierauf spezialisierte Zertifizierungsstellen[265].

4.3.3. Zertifizierung durch staatliche oder andere Stellen

In bestimmten kritischen Bereichen, etwa der Zulassung von Kraftfahrzeugen, sind Zulassungsverfahren durch staatliche oder vom Staat beliehene Stellen vorgesehen, die gewisse Mindestanforderungen überprüfen. Für derartige Bereiche ist eine Zertifizierung bzw. Anpassung der Verfahren auch (fast) zwingend notwendig, jedenfalls absolut wünschenswert, da das die Sicherheit erhöht und Zertifikate nur basierend auf bestimmten Mindest-Standards ausgestellt werden können und dürfen.

4.4. Wie kann Verlässlichkeit i.S.v. Reliability erreicht werden?

Zum einen wird Verlässlichkeit i.S.v. Reliability unterstützend erreicht durch Zertifikate unabhängiger Prüfdienste bzw. staatlicher Stellen. Zum anderen bietet aber wie ausgeführt[266] das geltende Recht mit der ent-

---

263 Müller-Schloer, H. Schmeck, U. Brinkschulte, F. Feldbusch, W. Trumler und Th. Ungerer, in: „Grand Challenges der Technischen Informatik“ Report, März 2008, S. 34.

264 Es handelt sich hierbei um ein Konsortium zur Standardisierung von Software im Automobilbereich; bzw. zukünftig: Car2Car Communication und/oder vergleichbaren Gremien.

265 Siehe Ziffer 4.3.3.

266 S. Ziffer 4.1.

sprechenden Zuordnung von Verantwortlichkeit und Haftung eine Grundlage für Verlässlichkeit i.S.v. Reliability, die wiederum ein Hauptaspekt dafür ist, dass Vertrauen in OC Systeme entstehen kann.

5. Zusammenfassung

Nach dem derzeitigen Stand der Wissenschaft und Technik ist das Risiko, dass sich Organic Computing Produkte auch in einer Weise entwickeln, die zu einem Schaden führt, wohl nicht zu vermeiden. Hier ist zum einen zu prüfen, wie hoch das konkrete Risiko des Schadenseintritts im Einzelfall bzgl. des konkreten OC Systems ist und welche Schäden potenziell möglich sind (nur Sachschaden, leichter Personenschaden, schwerer Personenschaden etc.). Letzteres ist dann mit dem mit dem Produkt verbundenen Nutzen (nur Komfortsteigerung oder z. B. Verhinderung von Unfällen) abzuwägen[267]. Ein auf OC-Techniken basierendes Produkt, das nur relativ geringe Körperschaden herbeiführen kann und bei dem dieses Risiko gering ist, und das gleichzeitig geeignet ist, in einer Vielzahl von Fällen vor schweren Körperschäden zu bewahren, kann aus produkthaftungsrechtlicher Sicht dann zulässig sein, wenn die entsprechenden Warnhinweise gegeben werden[268], wenn alle zumutbaren Sicherheitsvorkehrungen getroffen wurden und wenn bzgl. Herstellung und fertigem Produkt alle in dieser Expertise dargestellten Voraussetzungen eingehalten wurden.

Ein Produkt, dass nur Sachschäden herbeiführen kann, kann zulässig sein, wenn dieses Risiko so gering ist, wie es die berechtigten Erwartungen an das Produkt vorgeben und wenn die ggf. erforderlichen Hinweis- und Warnpflichten erfüllt werden.

---

[267] So auch die Rechtsprechung für Produkthaftung allgemein, BGH, Urteil vom 16.06.09, Az. VI ZR 107/08, Rdnr. 17 „Airbag, sowie die Literatur zu Software im Allgemeinen, Engel, CR 86, 702, 708, und zu Expertensystemen im Besonderen, Kardasiadou, Die Produkthaftung für fehlerhafte medizinische Expertensysteme, S. 182 (wobei die dogmatische Einordnung unklar bleibt); s. ausführlich Ziffer 2.2.4.3.

[268] S. dazu oben Ziffer 2.2.3.1.; aber auch Ziffer 2.2.3.2.

GESCHÄFTSTELLE BERLIN

MAIN OFFICE

Potsdamer Straße 105

10785 Berlin

Telefon: + 49 – 30 – 884 594-0

Fax: + 49 – 30 – 882 54 39

BÜRO HEIDELBERG

HEIDELBERG OFFICE

Bergstraße 7

69120 Heidelberg

Telefon: + 49 – 6221 – 649 16-0

Fax: + 49 – 6221 – 270 60

mailbox@ioew.de

www.ioew.de