Formale Beteiligungsverfahren im WEB

Sylvia A. JOHNIGK

Sylvia A. Johnigk Institut für Autonome intelligente Systeme

EINFÜHRUNG

Arbeiten im Bereich raumplanerischer Öffentlichkeitsarbeit befaßten sich bislang überwiegend mit der Gestaltung von Kommunikations- und Diskussionsprozessen (siehe u.a. [Floeting1998a], [Glitz,1994], [Gordon1997b], [Gordon1999], [Grueniger1996], [Kurnol1998], [Kubicek1998], [Lenk1997], [Schmidt1997], [Streich1997] und [Voss1996]). Nur einige wenige Ansätze bezogen sich auf konkrete formale Beteiligungsverfahren (siehe u.a. [Schmidt1997], [Streich1998], [Hasemann1998], [Burg1999] und [Maerker1999]).

Die in formalen Beteiligungsverfahren aufgestellten Verfahrenregeln bestimmen wer, wie und zu welchem Zeitpunkt zu beteiligen ist. Aus technischer Sicht existiert ein Geflecht von Gesetzen, Richtlinien, Interpretationen und Erlassen, die den Planungsablauf, die Planungsinhalte und die Randbedingungen in der Grundstruktur, aber nicht in allen Details und in der genauen Abfolge festlegen (siehe [Gordon1996d]). Dies erfordert von denjenigen, die diese Vorschriften anwenden müssen, das ``Fehlende" mit ihrem ``Fuzzy-Gefühl"1 richtig bzw. angemessen in einer konkreten Situation ersetzen.

Dieser Beitrag diskutiert Anforderungen an formalen Beteiligungsverfahren, die mittels telekooperativer Plattformen durchgeführt werden sollen. Exemplarisch wird eine mögliche Einbettung am Mediationssystem Zeno [Gordon1997b], [Gordon1999], [Maerker1999] und [Voss1996] gezeigt. Außerdem werden Lösungsideen für eine Implementierung aufgezeigt, die die besonderen Eigenschaften der gesetzlichen Regelungen - z.B. ihre Nähe zur Informationsicherheit, aber auch die Probleme wie viele Ausnahmen von der Regel, grobe Grenzen, Verflechtungen - berücksichtigen.

1 PROBLEMBESCHREIBUNG

Stadtplanung ist ein komplexer Prozess bei dem verschiedene Personen(gruppen) und Institutionen zu beteiligen sind. Typischerweise kommen die Beteiligten aus verschiedenen Sphären (Stadtplanungsamt, Bauamt, beteiligte Bürger, Interessenvertretungen, etc.) und haben von daher unterschiedliche Interessen, unterschiedliches ``professionelle" Hintergrundwissen, unterschiedliches Ausbildungsniveau und eine andere Art und Weise Information zu ermitteln und zu verarbeiten. Eine Lösung um einen solchen konfliktreichen Kommunikations- und Diskussionsprozess zu unterstützen ist Mediation.

Mediationssysteme sind netzwerkbasierte Computersysteme mit dem Ziel zwischen konfligierenden menschlichen Akteuren eine faire, effektive und sichere Deliberation zu ermöglichen. In einer Anwendung wie das Zeno 2[Gordon1997a] Diskussionsforum gibt es einen Mediator - eine unabhängige dritte Person - der die Aufgabe hat die Teilnehmer zu unterstützen. Hierzu gehört das Strukturieren der Diskussion und die Aufrechterhaltung der Ordnung innerhalb des Forums. Der Mediator wird in seiner Arbeit durch eine Komponente bei der Strukturierung der Diskussion unterstützt (siehe [Gordon1999]).

Ein Konzept bzw. Modell, das den Mediator bei der Überprüfung unterstützt, ob die Verfahrensregeln eingehalten worden sind, existiert noch nicht. Ein Ansatz ist die Formalisierung von Roberts Rules of Order(RRO).3 Prakken hat hierzu ein formales Modell [Prakken1998a,Prakken1999a] entwickelt. Da es bei RRO sich um ``Verfahrensregeln" für synchrone Diskussionen handelt sind sie für Zeno nicht geeignet.

---

1 ``Wörter sind wie Wolken die in der Mitte dicht und eindeutig sind und zum Rand hin immer dünner und ausgefranster werden - eben fuzzy"[Droesser1996]

2 wird im Rahmen des GEOMED-Projekts (GEOgraphical MEDiation - gefördert von der EU im Rahmen des Telematik-Programms) entwickelt.

3 Robert's Rules of Order ist die Standard Prozedur für deliberative Gemeinschaften in den USA. Sie regulieren den Ablauf von Debatten.

2 PLANUNGSINSTRUMENTE IN DER STADTPLANUNG

Bei der Durchführung von Planungsmaßnahmen werden gesetzlich vorgeschriebene Planungsinstrumente angewandt. Die Planungsinstrumente bzw. die formalen Beteiligungsverfahren4 können als das Pendant zu RRO in Parlamenten angesehen werden. Durch diese Planungsinstrumente wird u.a. geregelt wer, wann und wie zu beteiligen ist. Solche formalen Beteiligungsverfahren definieren ein Mindestmaß an Beteiligung, das nicht unterschritten werden darf, wenn ein Plan rechtlichen Bestand haben soll. Ein solches Planungsverfahren ist das Planfeststellungsverfahren (nach dem VwVfG), welches im Rahmen von Fachplanungen durchgeführt wird. Es dient bei einer öffentlichen Maßnahme z.B. den Bau einer Bundesstrasse der Überprüfung der Zulässigkeit und der verbindlichen Regelung. Die gesetzlichen Grundlagen des Planfeststellungsverfahrens befinden sich im Verwaltungsverfahrensgesetz (§§ 72-78 VwVfG). Eine zentrale Rolle, insbesondere zur Regelung der Beteiligung, spielt dabei das Anhörungsverfahren (§73 VwVfG).

3 EIGENSCHAFTEN VON FORMALER PLANUNGSINSTRUMENTE

3.1 Planungsinstrumente sind individuell

Eine Eigenschaft von Planungsinstrumenten ist, dass sie individuell bzw. anwendungsspezifisch sind, das heisst dass für unterschiedliche Planungsvorhaben unterschiedliche gesetzliche Grundlagen gelten (z.B. in Deutschland die Bauleitplanung nach dem Baugesetzbuch, das Planfeststellungsverfahren gemäß dem VwVfG, in anderen Ländern gelten wieder andere Vorschriften). Möchte man nun vorhandene Werkzeuge (wie z.B. Mediationssysteme, GIS-Datenbanken, GIS-Viewer etc.) für die Planungsunterstützung einsetzen, so sollte man diese Werkzeuge nur gemäß den Vorschriften anwenden können, da sonst die Rechtssicherheit der Pläne und Entscheidungen gefährdet ist (z.B. wenn die Anhörungsphase zu kurz war, bzw. die Unterlagen nicht vollständig zur Verfügung standen). Da es verschiedene Planungsinstrumente gibt ist es erforderlich, die Planungsinstrumente in einer getrennten eigenen Komponente (Prinzip des objekt-orientierten bzw. komponeten-basierten Entwurfs) zu entwerfen und durchzusetzen, um die <werkzeuge für verschiedene Anwendungsfälle einsetzen zu können.

3.2 Planungsinstrumente sind eine »spezielle Art« von Sicherheitspolitiken im Sinne der Informationssicherheit

Während des Planfeststellungsverfahren ist eine Anhörungsphase obligatorisch. Diese Anhörungsphase muß mindestents eine Woche vorher angekündigt werden (§73 VwVfG), Diese Ankündigung darf nur von der zuständigen Behörde bzw. einem Vertreter (z.B. Sachbearbeiter dieser Behörde) getätigt werden und nicht von einem beliebigen Systembenutzer. Ein weiteres Beispiel ist: Wird während der Anhörungsphase im Diskussionsforum von einem Beteiligten ein Einwand gegen den Plan gemacht, so hat der Einwender i. d. R. einen Anspruch auf Behandlung und Erörterung (z.B. während des im Anschluss stattfindenen Erörterungstermin) des Einwands.

Aus diesen und weiteren Gründen ergeben sich Eigenschaften, die ein System, das für formale Beteiligungsverfahren eingesetzt wird, nachweisen muss: wie z.B. die Authentizität des Sachbearbeiters oder die Nichtabstreitbarkeit des eingegangenen Einwands. Alle genannten Eigenschaften (und man könnte an dieser Stelle die Liste noch lange ergänzen) gehören zum Themenbereich der Informationssicherheit.

Informationstechnisch lassen sich (Teile der) Verwaltungsvorschriften u.a. auf Subjekt - Objektbeziehungen beschränken, wobei handelnde Subjekte (z.B. Beteiligte) bzw. von ihnen gestartete Prozesse (zum Beispiel das Senden einer Datenbankanfrage) und Objekte (z.B. ein Datensatz einer Datenbank) fokussieren.,sodass der Planungs- und Diskussionsprozess als Subjekt - Objektbeziehung gesehen werden kann, bei dem ein Subjekt bestimmte Objekte bearbeiten kann (z.B. lesen im Diskussionsforum, schreiben von Einwänden, etc.).

Aufgrund der Komplexität der Subjekt - Objektbeziehung5 kann es sehr leicht dazu kommen, dass zum Beispiel über verdeckte Kanäle »Rechte« (das Recht für einen beliebigen Systembenutzer amtliche

4Planfestellungsverfahren VwVfG und Bauleitplanung BauGB

5Eigentlich sind es die Gesetze die komplex sind.

Mitteilungen zu erstellen) zu nicht Berechtigten diffundieren. Hierfür gibt es Sicherheitsmodelle (z.B. HRU [Harrison75a], BLP-Modell[Bell74a] Denning Modell[Denning76]6), mittels denen man sicherstellen kann, dass während des gesamten Vorgangs niemals jemand anderes als z. B. der Sacharbeiter, die Ankündigung im System erstellen kann bzw., dass es nicht möglich ist jemand mit Anspruch auf die Teilnahme an der Diskussion vorsätzlich auszuschliessen. Die Menge aller Regeln bilden zusammengefasst die Sicherheitspolitik eines Systems.

Da es für die Rechtsverbindlichkeit von Entscheidungen über Pläne unvermeidbar ist7, dass die Minimalstandards der Planungsvorschriften eingehalten werden müssen, müssen diese vom System durchgesetzt werden. Die Unterlagen, die dem Bescheid über die Bewilligung oder Ablehnung des Plans zugrunde liegen, müssen einer rechtlichen Überprüfung standhalten. Eine hierzu notwendige Voraussetzung wäre, wenn man mittels eines (Sicherheits)modells nachweisen kann, dass die mit dem System durchgeführte Plaunung und die erstellten Unterlagen, die Rahmenbedingungen erfüllen.

3.3 Planungsinstrumente ändern sich stetig, sind fast nie vollständig und lassen einen Ermessensspielraum

Verwaltungsvorschriften ändern sich stetig, aufgrund neuer Erfahrungen, erteilter Bescheide, gefällter Gerichtsurteile u.s.w., werden die Rechtsvorschriften ergänzt. Dies hat Einfluß auf die Abwicklung des Planverfahrens so dass sich der Ablauf immer wieder ändert. Dies macht es erforderlich, dass die Regeln leicht änderbar sein sollen.

Vor allem muß ein solches Regelwerk auch noch dann funktionieren, wenn sich die Regeln (scheinbar) widersprechen, bzw. wenn man so oder so entscheiden kann. In solchen Fällen muß das System zulassen, dass es mehr als nur eine Alternative gibt einen Planungsablauf zu gestalten. Dies ist eng mit dem Aspekt des Ermessens verknüpft, dem ein eigener Paragraph gewidmet ist (§40 VwVfG).

Alle letztgenannten Aspekte sind Themenbereiche, die aus der Betrachtung der Informationssicherheit weitestgehend8 herausfallen. Vage Begriffe wie: »wenn möglich«, »wenn viele .... dann .....«, etc. können bislang in Sicherheitsmodellen nicht formalisiert werden.

4 ZIELE

Soll eine Komponente die Teilnehmer und den Mediator bei ihren Aktionen unterstützen bzw. ihre Aktionen regelmentieren, so müssen einige Voraussetzungen geschaffen werden:

Die Komponente muss die Regeln nach denen kommuniziert werden darf kennen. Zum Bespiel: Die vom Sachbearbeiter erstellte Ankündigung wird zu Sachbearbeiter (Subjekt) erstellt (Kommunikationsprozess) die Ankündigung (Objekt). Die Komponente muss die Handlungen beobachten und protokollieren, damit die Komponente ständig einen Überblick über den Stand der Planung bzw. im Fall von Zeno über die Diskussion hat und entscheiden kann welche Mögllichkeiten die Beteiligten im System haben.

Die Regeln müssen so etwas wie einen Ermessensspielraum zulassen, sie müssen mit sich widersprechenden Handlungsalternativen umgehen können.

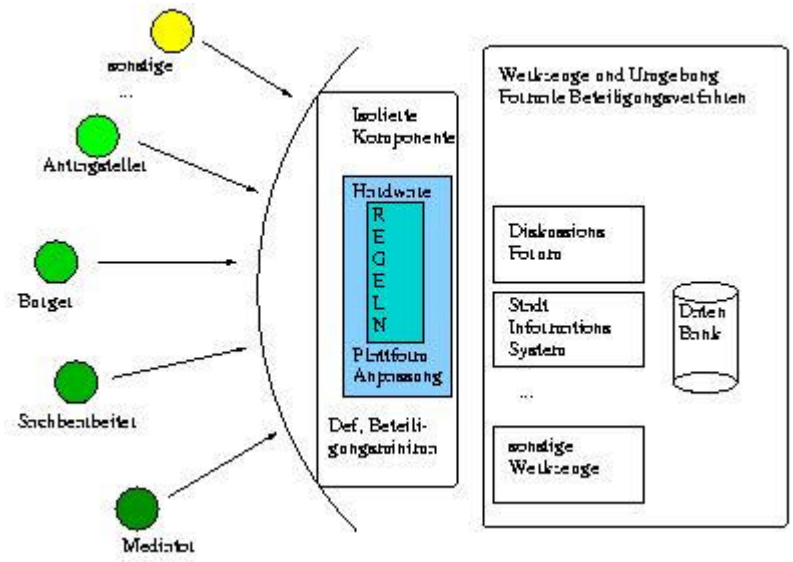
Auf der Eigenschaft, das sich die Regeln aufgrund von Änderungen der Voraussetzungen (neue Urteile, neue Vergleichsfälle, oder neue Fakten), müssen Regeln existieren, die es erlauben Regeln zu verändern.

Die Regeln dürfen nicht von aussen manipulierbar sein, das heisst die Komponente muss manipulationssicher sein (abgesehen von den gewollten Änderungen, die die Regeln selbst vorsehen).

6An dieser Stelle wird nur auf originäre Literatur und auf Sicherheitsmodelle, die die Zugriffssteuerung und den Informationsfluß betreffen, verwiesen Die drei aufgezählten Sicherheitsmodelle bilden die Ausgangsbasis für viele heute verwendete Sicherheitsmodelle.

7 Die Unvermeidbarkeit der Durchsetzung von Beteiligungsmindeststandard bei computergestützter Komunikation ist zwar nirgendwo direkt referenzierbar, ist aber unmittelbar aus der Verpflichtung die Planungsinstrumente für bei ``normalen" Beteiligungsverfahren anwenden zu müssen, ableitbar.

8So weit der Autorin bekannt ist.



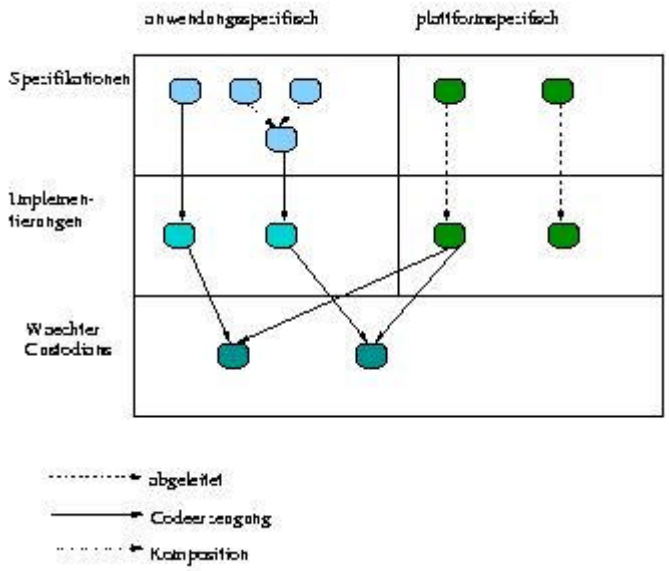
Der Zustand der Komponente muß persistent sein. Das heisst auch bei plötzlichen Ausfall des Systems (z.B. Stromausfall) muß sie im Anschluß wieder den aktuellen Zustand halten.

Die Komponente muss an die Anwendung nachträglich gebunden werden können, da für jeden Verwaltungsakt ein neuer Assistent mit einem eigenen Regeln und Zustand erforderlich ist.

Die Komponente muss auf jeder Plattform installierbar sein, da es kein Standardbetriebssystem gibt, und die Realisierung der Mechanismen sich unterschiedlich gestaltet.

Aus der obigen Aufstellung ergibt sich eine weitere Konsequenz für die Gestaltung einer Komponente, die die Verfahrensregeln durchsetzen soll. Es gibt einen anwendungsspezifischen Teil, das ist der Teil der Komponente, der die Regeln die den Umgang mit dem System enthält (siehe Ziel 1.) und einen »gemeinsamen« Teil, der systemspezifisch bzw. plattformspezifisch dafür sorgt, dass die Regeln durchgesetzt werden können (siehe Ziele 4. - 6). Für diese Aspekte gibt es Lösungsansätze die im folgenden kurz vorgestellt werden. Die verbleibenden Ziele, wie mit widersprüchlichen Regeln, mit sich ändernden Regeln oder mit dem vorhandenen Ermessensspielraum umzugehen ist, ist das eigentliche Problem. Im Bereich Informationssicherheit gibt es bislang noch keine Lösungen.

5 REALISIERUNG



Für die Entwicklung und Durchsetzung von Sicherheitspolitiken (bzw. formalisierten Planungsinstrumente) kann (teilweise) das in [Kuehn95b] vorgestellte Konzept verwendet werden (siehe Abb.2). Es gibt fünf

Objekte: Spezifikationen von anwendungsspezifischen Sicherheitspolitiken, deren Implementierung, Spezifikationen von plattformspezifischen Sicherheitspolitiken und durch Codegenierung gewonnene ausführbare Wächterobjekte (Custodians), die für ein gegebenen System, die die Regeln der Sicherheitspolitik durchsetzen (siehe Abb. 1). Bei diesem Konzept ist die Trennung des anwendungsspezifischen Teils und des plattformspezifischen Teils realisiert.

5.1 Anwendungsspezifische Sicherheitspolitiken

Um einem hohen Qualitätsanspruch gerecht zu werden, werden bei der Entwicklung und Durchsetzung von anwendungsspezifischen Sicherheitspolitiken (das ist die Zusammenfassung aller Regeln, die den Umgang mit dem informationstechnischen System bestimmen) spezielle Techniken und Methoden angewandt. Hierzu gehören u.a. zur präzisen Formulierung von anwendungsspezifischer Sicherheitspolitiken: Sicherheitsmodelle, Kalküle und Spezifikationssprachen (also formale Repräsentationen von Sicherheitspolitiken; siehe auch [Kessler93]).

Das Ziel von Sicherheitsmodellen ist es, für die als wesentlich erachteten Aspekte einer anwendungsspezifischen Sicherheitspolitik ein tiefes Verständnis zu erreichen, geforderte Sicherheitseigenschaften (Zugriffssteuerungsicherheit, Informationsflußsicherheit, etc.) und die Korrektheit der Implementierung versus ihrer Spezifikation mit formalen Verfahren nachweisen zu können.

Spezifikationen bzw. Modelle bilden die Grundlage für die Analyse von Sicherheitseigenschaften und sind die Ausgangsbasis für die Implementierung. Gesetzliche Bestimmungen die Planungsinstrumente) fordern für sensible Anwendungen hierzu die Evaluierung und Zertifizierung von Sicherheitspolitiken nach festgelegten mathematischen Verfahren (siehe hierzu [TCSEC83,ITSEC89,ITSEC90,CCITSE96]), sodaß die Verwendung von Sicherheitsmodellen und Spezifikationen bei der Einstufung in einer »hohen« Qualitätsklasse zwingend erforderlich ist.

5.2 Plattformspezifischen Teils einer Sicherheitspolitik

Ausgangsbasis für den plattformspezifischen Teil ist das Referenzmonitorkonzept [TCSEC83], welches die Eigenschaften einer abstrakten Maschine beschreibt, die eine Zugriffssteuerungpolitik durchsetzt. Eine Erweiterung dieses Konzepts wurde unter dem Begriff des Wächter-Konzepts (siehe [Kuehn95b]) entwickelt. Das Wächterkonzept verwirklicht das Konzept der Separation von anwendungsspezifischen und plattform-spezifischen Teilen einer Sicherheitspolitik. Im plattformspezifschen Teil einer Sicherheitspolitik gibt es neben den ursprünglichen Referenzmonitoreigenschaften: der totalen Kommunikationskontrolle aller Subjekte bzgl. der Objekte des Systems und die Manipulationssicherheit der Politik,zusätzlich Mechanismen, die die Politikpersistenz herstellen und das nachträgliche Binden des anwendungsspezifischen Teils einer Zugriffssteuerungspolitik an die Sicherheitsarchitektur ermöglichen.

Weitere Ansätze eines erweiterten Referenzmonitorkonzeptes sind in [Minear95a],[Olawski96a] zu finden. Als Fallbeispiel wurde eine Sicherheitsarchitektur implementiert für die Distributed Computing Environment (DCE) - Plattform der Open Systems Foundation (OSF) [Lux95] und [Halfmann99].

5.3 Widersprüchliche Regeln, sich ändernde Regeln und Ermessensspielräume

An dieser Stelle steht man vor einem großen Problem. Sicherheitspolitiken basieren zumindestens im Bereich von Zugriffssteuerung und Informationsfluß auf Kalküle bzw. Modelle mittels denen man vorhersagbar entscheiden kann, ob die geforderten Sicherheitseigenschaften in einem System gewährleistet werden können. Es ist grundsätzlich möglich Sicherheitspolitiken mit den Modellen der Logik oder mittels Expertensysteme auszudrücken (hierauf weisen selbst »einfache« Literaturquellen wie z.B. [Dowek95] hin). Es handelt sich nur, um eine andere Repräsentation einer Sicherheitspolitik in Form eines logischen Modells[9]. Sodass man bei der Formalisierung von Sicherheitspolitiken auf diese Methoden zurückgreifen kann ohne, dass man eine Eigenschaft wie der Nachweisbarkeit von Sicherheitseigenschaften verliert, zumindestens wenn man sie genau per Abbildung transformiert.

9Die Umkehrung das sich jedes logische Modell oder das logische Schliessen in ein Kalkül transformieren lässt ist nich gegeben(siehe ebenfalls [Dowek95]).

An diesem Punkt angekommen muß man sich mit den Grenzen, die den Nachweis von Sicherheitseigenschaften erfordern mit den Möglichkeiten, die man durch das logische Schliessen, durch Fuzzy-Logik oder ähnlichen Methoden erhält, auseinandersetzen.

Eine Hoffnung dabei ist, dass die Planungsinstrumente selbst den Ermessenspielraum zulassen, und somit den Grundstein dafür legen, dass man die Möglichkeit hat den Raum zwischen diesen Grenzen auszunutzen. Fuzzy-Logik bietet hier eine Möglichkeit nicht nur mit schaften Grenzen zu arbeiten[10]. Ebenso gibt Fuzzy Logik die Möglichkeit mit Widersprüchen, oder auch mit sich ändernden Regeln umzugehen. Es ist eine Eigenschaft der Fuzzy-Logik die Regeln »solange » zu ändern bis man »zufriedenstellende« Ergebnisse erhält. Allerdings beschränkten sich die Aktivitäten im Bereich von Fuzzy-Logik bislang weitestgehend auf technische Systeme.

6 ZUSAMMENFASSUNG UND AUSBLICK

Zusammenfassend kann man sagen, dass es sich bei Planungsinstrumente, um eine »spezielle« Art von Sicherheitspolitiken handelt, die sich bis zu einem gewissen Grad mit den aus der Informationssicherheit bekannten Methoden wie zum Beispiel das erweitertes Referenzmonitorkonzept, bei Regeln, die eindeutig sind (das heisst, man kann sie “ohne wenn und aber” mit ja oder nein beantworten), mit den formalen Methoden (Sicherheitsmodelle, Kalküle, Spezifikationen) formalisieren und durchsetzen.

Die am weitestgehende unbeantwortete Frage ist die, wie weit kann man Sicherheitseigenschaften noch nachweisen, wenn man bekannte Mechanismen (aus dem Bereich Expertensysteme, Logiken bzw. Fuzzy-Logik) benutzt, um Sicherheitspolitiken, wie sie von Planungsinstrumente gefordert werden, zu formalisieren. Ein weiterer Ansatz ist es, die Planungsinstrumente für den Zweck der computervermittelten Kommunikation anzupassen, und dabei so weit wie möglich zu vereinfachen. Dadurch würde sich die Formalisierung der Planungsinstrumente sehr vereinfachen.

7 LITERATUR

[Bell74a] Bell D.E. and LaPadula L.J., (1974) *Secure Computer Systems: A Refinement of the Mathematical Model*. Technical Report 78528 MITRE, Bedford Massachauttes

[Burg1999] Burg, A. (1999). *Einsatz telekooperativer Verfahren in der Öffentlichkeitsbeteiligung bei der Aufstellung städtebaulicher Pläne am Beispiel von Deutschland, Großbritannien und Schweden*. Shaker Verlag, Aachen Dissertation, Univ. Kaiserslautern.

[CCITSE96] Common (1996). Common Criteria for Information Technology Security Evaluation. Technical report, NIST (USA), CSE (Canada), BSI (Germany), NNCSA (The Netherlands), NSA (USA), UKITSCS (UK), SCSSI (France).

[Denning76] Denning D.E, (1976*) A Lattice Model of Secure Information Flow*. Communication of the ACM, 19(5):236-242

[Droesser1996] Drösser, C. (1996). *Fuzzy Logik: Methodische Einführung in krauses Denken*. Rowohlt.

[Floeting1998a] Flöting, H. and Grabow, B. (1998). Auf dem Weg zur virtuellen Stadt? *Raumordnung und Städtebau in der Informationsgesellschaft*, pages 17 -30.

[Glitz1994] Glitz, R. (1994). Virtuelle Realität. Arbeitsbericht zur Technikfolgenabschätzung, Düsseldorf.

[Gordon1999] Gordon, T. and Karacapilidis, N. (1999). The Zeno Argumentation Framework . *KI Künstliche Intelligenz*, 3:20 - 29. ISSS 0933-1875.

[Gordon1997b] Gordon, T. F. and Karacapilidis, N. (1997). The Zeno argumentation framework. In *Proceedings of the Sixth International Conference on Artificial Intelligence and Law*, pages 10-18. ACM.

[Gordon1997a] Gordon, T. F., Karacapilidis, N., Voss, H., and Zauke, A. (1997). Computer-Mediated Cooperative Spatial Planning. In Timmermans, H., editor, *Decision Support Systems in Urban Planning*, pages 299-309. E & FN SPON Publishers.

[Gordon1996d] Gordon, T. F. and Voss, H. (1996). ZENO - Kooperative Planungsunterstützung im World Wide Web. *Der GMD - Spiegel; Sonderdruck Planungsunterstützung auf der Basis des World Wide Web*.

[Grueniger1996] Grüniger, C. (1996). Computergestützte Gruppenarbeit im Büro. Entwicklung, Nutzung und Bewertung. Europäische Hochschulschriften, Frankfurt, Berlin, Bern, New York, Paris und Wien.

[Harrison75a] Harrison, M.A., Ruzzo, W.L. and Ullman, J.D. (1975) On Protection in Operating Systems. In Operating Systems Principles pages 14-24 ACM

[Hasemann1998] Hasemann, O. (1998). Netzgestützte Planungskommunikation und -kooperation. *RaumPlanung spezial*, pages 73 -84.

10Ein sehr einfaches (nicht pllanerisches) Beispiel(siehe [Doerner96] ist die Beantwortung der Frage, was ist ein dickes Buch. Die harte Entscheidung, dass ein dickes Buch mindestens 600 Seiten hat, hat die Konsequenz, dass ein Buch mit 599 Seiten kein dickes Buch ist. Mittels Fuzzy Logik würde man dazu kommen, dass auch ein Buch mit 599 Seiten dick ist.

[ITSEC89] ITSEC89 (1989). *IT-Sicherheitskriterien*. ZSI -- Zentralstelle für Sicherheit in der Informationstechnik, Bonn, Germany.

[ITSEC90] ITSEC90 (1990). *Information Technology Security Evaluation Criteria (ITSEC)*. Bundesminister des Inneren, Bonn, Germany, version 1 edition.

[Kessler1993] Kessler, V. and Mund, S. (1993). Sicherheitsmodelle. Studie des Verbundprojektes ,,Referenzmodell für sichere IT-Systeme", Siemens AG.

[Kopp1996] Kopp, F.O. (1996) VwVfF Verwaltungsverfahrensgesetz Verlag C.H. Beck

[Kubicek1998] Kubicek, F. (1998). Das Internet 1995 - 2005. Zwingende Konsequenzen aus unsicheren Analysen. In Klaus Leggewie, C. and Mahr, C., editors, *Internet & Politik. Von der Zuschauer zur Beteiligungsdemokratie*, pages 55 - 69. Köln.

[Kuehn95b] Kühnhauser, W. E. (1995). A Paradigm for User-Defined Security Policies. In *Proceedings of the 14th IEEE Symposium on Reliable Distributed Systems*, Bad Neuenahr, Germany. IEEE Computer Society Press.

[Kunol1998] Kurnol, J. and Lorenz-Henning, K. (1998). Telekommunikation und Raumordnung. Raumordnung und Städtebau in der Informaitongesellschaft Informationen zur Raumentwicklung, H. 1.18 Bundesamt für Raumplanung, Bonn.

[Lenk1997] Lenk, K. (1997). Partizipartionsunterstützung durch Informationssysteme. In Streich, B. and Schmidt, T., editors, *Computergestützte Assistenzsysteme für die Stadtplanung. Stadtmanagement auf neuen Wegen*, pages 99 - 109. Kurzfassung: http://wwwagr.informatik.uni-kl.de/stadt/lenk_kf.html.

[Lux195] Lux, W. (1995). Integrating Custodians into OSF-DCE. In *Proceedings of the Workshop on Anwendungsunterstützung für heterogene Rechnernetze*, Freiberg, Germany. Technical University of Freiberg Press.

[Maerker1999] Märker, O. (1999). Computer vermittelte Kommuniktion in der Stadtplanung. Unterstützung formaler Beteiligungsverfahren durch Issue Based Information Systems. GMD Research Series; zgl. Dipl. Uni Bonn 1998 10/1999, GMD Forschungszentrum für Informationstechnik, Sankt Augustin, Germany.

[Minear95a] Minear, S. E. (1995). Providing Policy Control Over Object Operations in a Mach Based System. In *Proceedings of the fifth USENIX UNIX Security Symposium*, pages 141-156. USENIX Association.

[Olawski96a] Olawski, D., Fine, T., Schneider, E., and Spencer, R. (1996). Developing and Using a "Policy Neutral" Access Control Policy. In *Proceedings of the New Security Paradigms Workshop*, pages 60-67. ACM SIG on Security, Audit, and Control, ACM Press.

[Ptakken1998a] Prakken H. (1998) Formalizing Robert's Rules Technical Report 12 GMD Sankt Augustin

[Prakken1999a] Prakken H. and Gordon T.F., (1999) Rules of Order for Electronical Decision Making – A Formal Methodlogy: In Proceedings of VIM Spring and Winter Workshop on a Virtual Multicomputer Spring Lecture Notes in AI, Berlin Springer Verlag

[Schmidt1997] Schmidt, T. (1997). Der intelligente Bebauungsplan - Partipartion auf neuen Wegen. In Streich, H. W. B., editor, *City Managment. Städteplanung zwischen Globalisierung und Virtualität*, pages 118 -129. Opladen.

[Streich1997] Streich, B. (1997). Digitale Stadt und virtueller Raum: Visionen zur Implementierung und Organisation des Immateriellen. In Hajo Weber, B. S., editor, *City Managment. Städteplanung zwischen Globalisierung und Virtualität*, pages 82-117. Opladen.

[Streich1998] Streich, B. (1998). Planungsethik in der Informationsgesellschaft. In Bernd Streich, T. K., editor, *Planung als Prozeß. Von klassischem Denken und Zukunftentwürfen im Städtebau [Festschrift für Klaus Borchard zum 60. Geburtstag]*, pages 294 - 311. Bonn.

[TCSEC83] TCS (1983). *Trusted Computer System Evaluation Criteria*. Department of Defense.

[Voss1996] Voss, H. (1996). Mehr Transparenz und Demokratie in Planungs- und Mediationsverfahren mit Zeno. In Edelgard Bulmahn, Kurt van Haaren, e. a., editor, *Informtiolnsgesellschaft - Medien - Demokaraie. Kritik - Positionen - Visionen*, volume 36. Forum Wissenschaft: Studien.