Elektronische Archive in virtuellen Organisationen: Flexibilisierte Zugriffskontrolle auf Basis von Komponententechnologie

Gunnar Stevens[1] und Volker Wulf[2,3]

[1]ProSEC - Informatik III, Universität Bonn, Römerstr. 164, 53117 Bonn

[2] Fraunhofer FIT, Schloß Birlinghoven, 53754 Sankt Augustin

[3] IISI - Internationales Institut für Sozio-Informatik, Heerstr. 148, 53111 Bonn

In der letzten Ausgabe des Informatik-Spektrums erschien der erste Teil dieses Aufsatzes, der das OrgTech-Forschungsvorhaben vorstellte. Darin wurde die Kooperation zwischen einem Stahlwerk („Bausig“) und der externen Dienstleistern („Schmidt & Partner“ und „Lange“) im Bereich der Instandhaltungskonstruktion untersucht. Die Schaffung eines externen Zugangs zum elektronischen Archiv des Stahlwerks erwies sich als eine wichtige Aufgabe zur Verbesserung der interorganisatorischen Kooperation. Unsere Untersuchung zeigte aber auch: (a) wie verwoben das Verhältnis zwischen Kooperation und Konkurrenz in virtuellen Organisationen sein kann und (b) dass die tätsachliche Arbeitspraxis von den vorgeschriebenen Prozessen teilweise erheblich abweichen kann. Aus dieser Untersuchung ergaben sich neue Anforderungen an die Gestaltung der Zugriffskontrolle auf elektronische Archive in virtuellen Organisationen. Diese Anforderungen lassen sich mit der traditionellen „ex-ante“-Spezifikation von Zugriffsrechten nicht erfüllen. Im folgenden zeigen wir die komponeneten-basierte Implementierung einer flexibilisierten Zugriffskontrolle, die zusätzlich „uno-tempore“ und „ex-post“-Kontrollmechanismen anbietet. Somit erlaubt die Anwendung den Eignern eines elektronischen Archivs, verschiedene dem jeweiligen Arbeitskontext und den externen Kooperationspartner angemessene Formen der Zugriffskontrolle zu spezifizieren. Im technischen Teil wird kurz das FlexiBean-Modell eingegangen, das den technischen Hintergrund der Anwendung bildet. Danach werden die Grundkomponenten und eine daraus zusammengesetzte Anwendung erläutert, mit der die verschiedenen Strategien realisiert werden. Abschließend wird ein Ausblick darüber gegeben, welche Möglichkeiten sich durch die gegeben Komponenten noch ergeben.

ADOS-X: Eine komponenten-basierte Anwendung zur Zugriffskontrolle in virtuellen Organisationen

Wir haben im OrgTech-Projekt aufgrund der Anforderungen der Akteure aus den verschiedenen Organisationen, eine Anwendung entwickelt, mit dessen Hilfe den Externen ein Zugriff auf das elektronische Archiv des Stahlwerks (ADOS) ermöglicht wird. Im Folgenden soll die prototypische Umsetzung, ADOS-X, vor allem unter dem Gesichtspunkt der Zugriffskontrolle vorgestellt werden.

Um auch während der Laufzeit die Zugriffskontrollstrategie anpassen zu können, ist die Anwendung aus Softwarekomponenten (sogenannten FlexiBeans) aufgebaut, die von den Nutzem im Anwendungsfeld zur Laufzeit (re-)konfiguriert werden können (vgl. Stiemerling 2000).

Das Grundproblem bei der Entwicklung komponentenbasierter Software besteht darin für die Anwendung eine passende Zerlegung in Komponenten zu finden. Die Zerlegung von Anwendungen in FlexiBeans stellt gegenüber traditioneller Softwareentwicklung eine besondere Herausforderung dar, weil das System nicht nur von den Entwicklern einfach (re-)implementiert werden, sondern auch von den Nutzern angepasst werden muss. Dementsprechend müssen die Komponenten eine semantische Nähe zum Anwendungsfeld des Benutzers haben (vgl. Nardi 1993).

Damit stellt sich insbesondere die Frage, wer der Nutzer ist. Wie sich aus der Voruntersuchung ergibt, besteht eine implizite, aber wichtige Anforderung darin, dass das neue System nicht das Abhängigkeitsverhältnis der externen Büros zur internen Konstruktionsabteilung aufheben darf. Dementsprechend verbietet es sich, eine Lösung zu entwickeln, in der die Sicherheitspolitik nicht von der internen Konstruktionsabteilung, sondern z.B. von der EDV-Abteilung festgelegt und kontrolliert wird. Insofern sollte die Zerlegung in Komponenten für die Sachbearbeiter der internen Abteilung verständlich sein.

Da die Forschung zur komponenten-basierten Anpassbarkeit relativ jung ist, gibt es bisher noch keine Methodik zur Dekomposition. Hier kann jedoch auf die Ergebnisse zur objekt-orientierten Softwareentwicklung zurückgegriffen werden. Eine Methode, die für sich beansprucht, den semantischen Graben zwischen Anwender und Entwickler klein zu halten, ist der WAM-Ansatz von Züllighoven (1998). Der WAM-Ansatz wurde von M. Wulf auf den Bereich der kooperativen Arbeit angewandt (vgl. Wulf 1995a; Gryczan 1996). Dabei hat sie das Konzept der Postfachmetapher entwickelt. Die Kernthese der Metapher ist die, dass kooperative Tätigkeit mittels Postfächern koordiniert werden kann. ADOS-X baut auf den Ansatz auf, erweitert ihn jedoch dahingehend, dass der Benutzer die Möglichkeit hat, routinesierte Abläufe zu automatisieren. Über die automatische Weiterleitung kann die Zugriffskontrolle realisiert werden. Durch die Anwendung der Postfachmetapher stellt sich ADOS-X dem Benutzer wie ein E-Mail-

Programm dar (siehe Abb. 2).

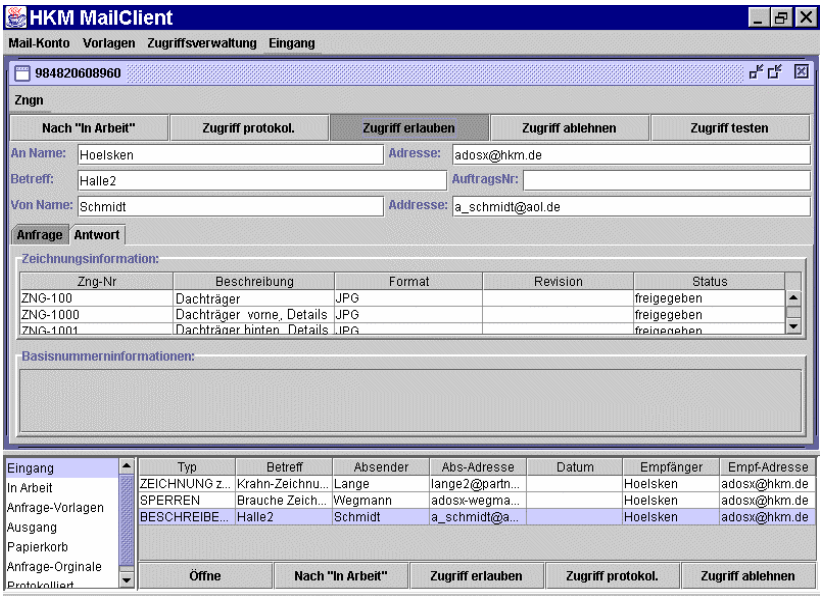


Abb. 2: Ein Fenster von ADOS-X zur Bearbeitung durch den internen Sachbearbeiter

Die Faktoren, die aus der Sicht der Mitarbeiter von Bausig für die Regelung des Zugriffs relevant sind, sind in Tab. 2 dargestellt. Interessanterweise wurden hier im Gegensatz zu der Untersuchung von von Stiemerling, Won und Wulf (2000) die Zugriffsdimensionen der Benutzerrolle, Organisationseinheit und Gruppenzugehörigkeit in unserem Anwendungsfeld als nicht relevant erachtet. Bei ihnen spielten diese Dimensionen dagegen eine wichtige Rolle zugemessen. Dieser abweichende Befund könnte damit zusammenhängen, dass dort die Kooperation innerhalb einer Organisation abläuft.

Ebenso unterscheiden sich die Faktoren, die sich auf das zuzugreifende Objekt beziehen. Im Falle des Stahlwerks, bei dem auf, in einer relationalen Datenbank gespeicherten, Zeichnungen zugegriffen wurde, waren die dort abgelegten, beschreibenden Daten zur den Zeichnungen von besonderer Bedeutung. Insbesondere waren das die Zeichnungsnummern und die Basis nummern, mit denen Zeichnungen inhaltlich gruppiert wurden. Demgegenüber waren in Stiemerling, Won und Wulfs (2000) Studie die folgenden Faktoren besonders relevant für die Vergabe von Zugriffsrechten: *Name des Dokuments, Inhalt des Dokuments, Entwicklungsstand des Dokuments, Objektlage* und *Elektronische Signatur.* In Anwendungsfeldern, bei denen mit semi-strukturierten Dokumenten gearbeitet wird, können die objektbezogenen Faktoren wiederum anders aussehen. Insgesamt

kann man wohl davon ausgehen, dass in jedem Anwendungsfeld diese Faktoren unterschiedlich ausgeprägt sein werden.

Parameter	**Faktor**	**Beschreibung**
Objekt	Inhalt	Merkmale bei den beschreibenden Daten zu einer Zeichnung (Zeichnungs-Nr., Basis-Nr., ...)
	Zustand der Zeichnung	Ist die Zeichnung aktuell in Bearbeitung?
Subjekt	Benutzer	Von wem geht der Zugriffswunsch aus?
Situation	Zeitangaben	Projektabhängiger Verfall von Zugriffsrechten
	Auftrag	Zuordnung vom Objekt/Subjekt zu einem Auftrag
	Priorität der Auftrags	Welche Priorität hat der Auftrag?
Operation	Art des Zugriffs	Nur beschreibende Daten lesen, die eigentliche Zeichnung lesen oder diese Daten modifizieren?

Tab. 2: Relevante Faktoren für Zugriffskontrolle beim OrgTech-Projekt

Technische Umsetzung

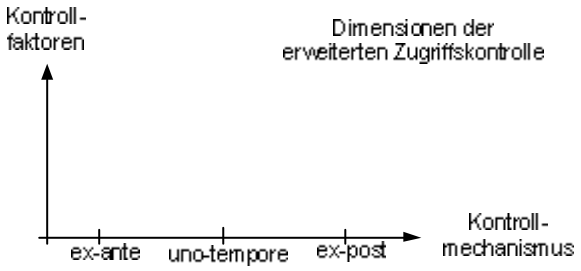


Abb 3.: Bei der erweiterten Zugriffkontrolle gibt zusätzlich zu den Kontrollfaktoren die die Kontrollmechanismen als eigenständige Dimension

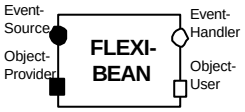
Bei einem erweiterten Zugriffskontrollsystem kann man zwischen den gewählten Kontrollmechanismus und den Faktoren unterscheiden, die die Bedingungen bestimmen, unter den der Mechanismus angewendet wird. Eine technische Umsetzung des Konzepts darin bestehen, ein traditionelles Zugriffskontroll-

System[1], um die Dimension der Kontrollmechanismus zu erweitern. Unser gewählter Ansatz sieht etwas anderes aus. Wir stellen einige Grundkomponenten zur Verfügung mit denen die verschiedenen Mechanismen realisieren lassen. Die Mover-Komponente stellt dabei ein zentrales Hilfsmittel zur Realisierung dar. Ein einzelner Mover kann man mit einem traditionellen Zugriffskontrollsystem vergleichen werden, bei dem man die Zugriffsmöglichkeiten einstellen kann.

FlexiBean Modell

Das von Stiemerling (2000) entwickelte FlexiBean-Modell ist eine Erweiterung des JavaBean-Modells (Hamilton 1997). Das Modell ermöglicht es, verteilte und zur Laufzeit anpassbare Systeme aus Komponenten aufzubauen.

Im FlexiBean-Modell gibt es, vereinfacht ausgedrückt, zwei Arten von Komponenten: Grundkomponenten und abstrakte Komponenten. Die Grundkomponenten sind in Java geschrieben und bilden, wie der Name schon sagt, die Grundbausteine für weitere Konstruktionen. Abstrakte Komponenten zeichnen sind dadurch aus, dass sie zusammengesetzt sind. Sie sind durch eine Menge von Komponenten und deren Verbindungen definiert. Einmal definierte Komponenten können dann zu der Konstruktion weiterer Komponenten verwendet werden. Das erlaubt es hierarchische Strukturen zu entwickeln. Die ADOS-X Komponente in Abb. 4 ist ein Beispiel für eine abstrakte Komponente.

Komponente	**Beschreibung**
	**FLEXIBEAN:** Die Kreise und Vierecke sind benannte Ports, über die die einzelnen Komponenten miteinander agieren können.

Tab 3: Graphische Darstellung einer FlexiBean

Zur Kommunikation zwischen Komponenten stehen zwei Schnittstellenarten zur Verfügung: *Events* und *SharedObjects*. Die intendierte Semantik von *Events* ist es, dass eine Komponente Änderungen seines Zustands durch Events weiterleitet (*push*-Mechanismus). *SharedObject* dienen dazu, dass der Zustand einer Komponente darüber abgefragt werden kann (*pull*-Mechanismus). In der graphischen Darstellung (siehe Tab. 3) sind *Event*-Quellen mit einem ausgefüllten, die Empfänger mit einem unausgefüllten Kreis gekennzeichnet. Mit einem ausgefüllten Viereck sind *SharedObject*-Anbieter und mit einem unausgefüllten

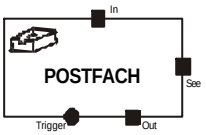
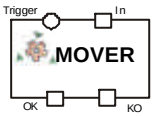
[1] Ein traditionelles Zugriffskontroll-System zeichnet sich dadurch aus, das es nur den Mechanismus „Erlaubt/Nicht Erlaubt“ kennt.

die Abnehmer gekennzeichnet. Die Schnittstellen sind benannt und besitzen einen Typ, der hier aber zur Vereinfachung weggelassen wurde. Nur Schnittstellen mit gleichen Typ aber entgegengesetzter Polarität können dabei verbunden werden.

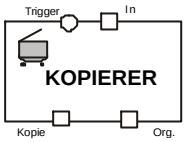
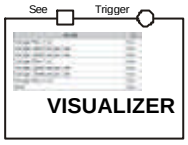
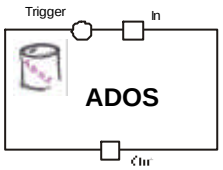
Die Komponentenkomposition definiert ein Programm, das in einer speziellen Umgebung, der Evolve-Plattform ausgeführt werden kann. Die Evolve-Plattform bietet die Möglichkeit, zur Laufzeit Komponenten hinzufügen bzw. zu löschen und die Verbindungen zwischen ihnen zu verändern (vgl. Stiemerling, Hinken und Cremers 1999).

Grundkomponenten

Die in Tab. 4 aufgelisteten und erläuterten Komponenten bilden die Grundbausteine für ADOS-X. Die wichtigsten Komponenten sind dabei das Postfach und der Mover. Dabei ist das Postfach ein Aufbewahrungsort für Dokumente bildet, mit dem Dokumente automatisch weitertransportiert werden können. Als Dokumentenformat wurde das MIME-Format mit anwendungsspezifischen Subtypen gewählt. Damit ist es auch möglich, die Externen über bestehende E-Mail Systeme an Bausig anzukoppeln[2].

Komponente	Beschreibung
	**Postfach:** Das Postfach ist der Aufenthaltsort für Dokumente. Über den *In*-Port können Dokumente hinein- und über den *Out*-Port, herausgenommen werden. Wenn sich der Zustand des Postfachs ändert, wird über den *Trigger*-Port ein Event gesendet. Der *See*-Port dient der Introspektion durch einen Visualizer.
	**Mover:** Die Mover-Komponente hat einen Eingang und zwei Ausgänge, die jeweils an ein Postfach angeschlossen werden können. Je nach Einstellung des Movers wird ein Dokument aus dem *In*-Port in den *OK*- bzw. in den *KO*-Ausgang transportiert. Der Mover stellt somit das klassische Zugriffskontrollsystem dar. Im Prototypen standen nur einige der in Tab. 2 aufgelisteten Felder zur Verfügung.

[2] Bei den Subtypen bietet sich jedoch an, dafür XML-Format zu benutzen, zumal davon auszugehen ist, dass in naher Zukunft geeignete XML-Editoren als JavaBeans auf den Markt kommen. Diese werden leicht in die Applikation einzubinden sind.

	**Kopierer:** Der Kopierer hat zwei Eingänge (In-Port und Trigger) und zwei Ausgänge. An letztere kann jeweils ein Postfach angeschlossen werden. Dabei wird das Original von dem *In*-Port in den *Org.*-Port transportiert. Gleichzeitig wird eine Kopie erstellt und zu dem *Kopie*-Port weitergeleitet. Der Kopierer wird über den *Trigger*-Eingang aktiviert.
	**Visualizier:** Mit Hilfe des Visualizers kann der Inhalt des Postfachs angeschaut werden. Der Visualizier wird über den *Trigger*-Port aktualisiert. Am *See*-Port wird das Postfach angeschlossen, das visualisiert werden soll.
	**ADOS:** Die ADOS-Komponente stellt die Verbindung zur Datenbank her. Das Postfach mit den Anfrage-Dokumenten wird am *In*-Port angeschlossen. Die Komponente fragt die Datenbank ab, erstellt eine Antwort, hängt diese an das Anfrage-Dokument an und leitet es dann an den Out-Port weiter. Die Komponente wird über den Trigger-Eingang aktiviert.

Tab 4: Grundkomponenten von ADOS-X und ihre Bedeutung

Einstellmöglichkeiten des Movers

Bei der Systemgestaltung kann man zwischen der Anpassung einer einzelnen Komponenten und der Anpassung der Komposition der Komponenten unterscheiden werden. In unserem Falle besteht der erste Fall hauptsächlich in der die Anpassung eines Movers.

Mit der Einstellung des Movers kann bestimmt werden, welches Dokument automatisch weitergeleitet werden soll und welches nicht. Er stellt in gewisser Weise so etwas wie ein traditionelles Zugriffskontrollsystem dar. Die Zugriffsstrategie drückt sich in Einstellung des Movers aus. In der aktuellen Systemversion sind die Einstellmöglichkeiten auf die zwei in diesem Anwendungsfeld wichtigsten Gesichtspunkte beschränkt[3]. So können Zugriffsregelungen hinsichtlich der Operation und dem Subjekt des Zugriffs spezifiziert werden Aus der

[3] Anfänglich wurde ein Mover eingesetzt, der die Dokumentenstruktur analysierte, und so dynamisch die Einstellmöglichkeiten erzeugte. Dies wurde bei der Vorstellung des Prototypen von Seiten der zukünftigen Anwender als übertrieben angesehen.

Sicht der externen Kooperationspartner sind die wichtigsten Operationen, der Zugriff auf die eigentliche Zeichnung (“Anschauen von Zeichnungen”), der Zugriff auf die zu einer Zeichnung gehörigen beschreibenden Daten (“Beschreibende Daten”) und die Sperrung einer Zeichnung für die Modifikationen (“Sperren von Zeichnungen”). Der Einstelldialog ist in Abb. 3 zu sehen.

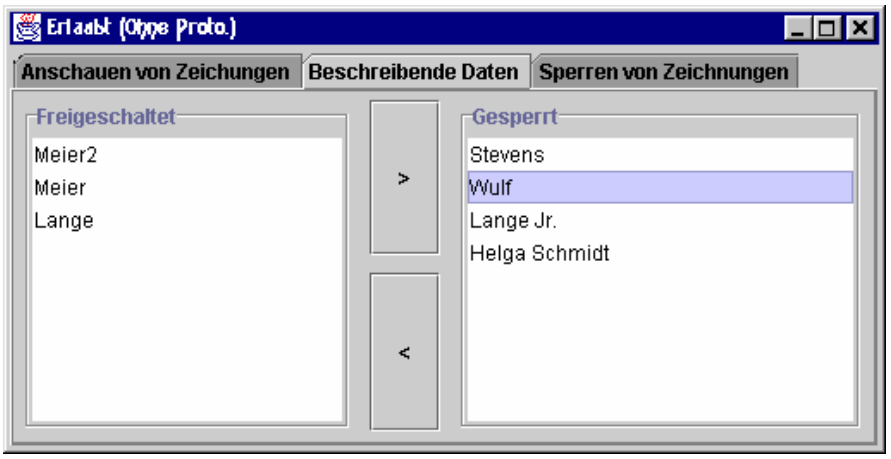


Abb. 3: Ein Screenshot der Einstellmöglichkeiten des Erlaubt-Movers

Das Einstellen des Movers geht dann wie folgt: Der Sachbearbeiter legt zunächst die Personen fest, die überhaupt für einen Zugriff in Frage kommen[4]. Für diesen Personenkreis ist der Zugriff erstmal gesperrt, der Sachbearbeiter kann dann den Einzelnen den Zugriff freischalten. Im Screenshot ist ein solches „Freischalten“ für die Operation „Beschreibende Daten“ dargestellt. Durch ein Klicken auf den „<“-Button würde die Person „Wulf“ von der Liste der gesperrten Personen auf die Liste der Personen geschoben, denen ein Zugriff gestattet ist. Durch diese Einstellmöglichkeiten sind folgende Szenarien realisierbar.

Komposition für erweiterte Zugriffskontrolle

Aus den Grundkomponenten können weitere abstrakte Komponenten zusammengesetzt und mit einem Typnamen versehen werden. Für die Bausig Mitarbeiter wurde aus den Grundkomponenten eine solche abstrakte Komponente, wie in Abb. 4 dargestellt, zusammengesteckt und mit dem Namen SACHBEARBEITER versehen. Durch das Zusammenspiel von Movern, Postfächern und dem Kopierer

[4] Je nach der konkreten Implementierung kann jeder Sachbearbeiter entweder seine eigene Liste von externen Kooperationspartnern pflegen. Ansonsten kann diese Liste auch geshared werden. In der hier beschriebenen Systemversion verwaltet jeder Sachbearbeiter seine eigene Liste.

sind hier die oben erläuterten Kontrollmechanismen realisiert. Die Visualiser sind dazu dar, dem Sachbearbeiter die Dokumente anzuzeigen[5], die eigentliche Anfrage wird in der ADOS-Komponente verarbeitet.

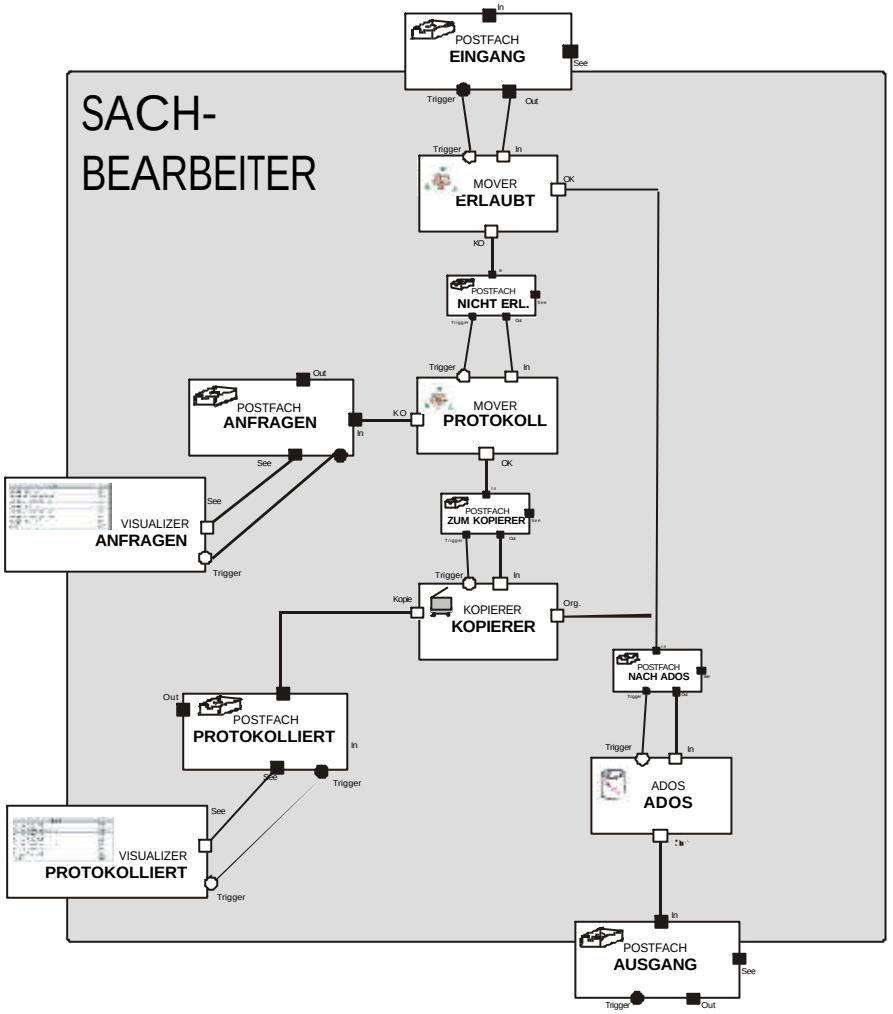


Abb. 4: Komponenten-Aufbau von ADOS-X für den internen Sachbearbeiter

[5] Visualiser ist eine abstrakte Komponente mit deren Hilfe der Sachbearbeiter die Dokumente auch bearbeiten und an diverse Postfächer weiterleiten kann. Um die Darstellung zu vereinfachen sind jedoch die Möglichkeiten zur Weiterverarbeitung wie Editieren des Dokuments, Weiterleitung zu ADOS, Zurückschicken, etc. hier weggelassen.

Die Funktionsweise der Komposition soll anhand dreier Einsatzszenarien von ADOS-X erläutert werden. Diese Szenarien kann der Sacharbeiter der Instandhaltungskonstruktion des Stahlwerks durch das Einstellen der Mover ERLAUBT und PROTOLL bewerkstelligen.

1. Fall „Nichts ist erlaubt“

ADOS-X kann so konfiguriert werden, dass alle Anfragen vom Sachbearbeiter abgesegnet werden müssen. Dazu müssen die Mover *ERLAUBT* und *PROTOKOLL* so eingestellt werden, dass sie alle eingehenden Dokumente in den *KO*-Ausgang befördern. Dadurch wandert das Dokument, das sich im Postfach *EINGANG* befindet, erst mal in das NICHT ERL. Postfach, um von dort in das ANFRAGEN Postfach weitergeleitet zu werden. Dort kann der Sachbearbeiter es sich über den Visualisierer anschauen. Bei dieser Einstellung muss jeder Zugriff von einem Bausig-Mitarbeiter abgesegnet werden, und stellt damit eine uno-tempore Kontrolle dar.

Dieser Fall ist die Standardkonfiguration von ADOS-X. Sie entspricht der momentanen Praxis insoweit, als das momentan Anfragen auch via Email gestellt werden, die jedoch nicht automatisch weiterverarbeitet werden können.

2. Fall „Es wird überwacht“

Stellt man den PROTOKOLL-Mover so sein, dass die Dokumente nicht in den KO-, sondern in den OK-Ausgang transportiert werden, werden zwar die Anfragen bearbeitet, aber der Sachbearbeiter erhält eine Kopie des Vorgangs. Der Vorgang ist wie im Fall 1, nur dass die Anfragen nun im Postfach ZUM KOPIEREN landen. Die Kopierer-Komponente leitet eine Kopie des Dokuments in das PROTOKOLL-Postfach, das Original in das NACH ADOS Fach. Die ADOS-Komponente verarbeitet die Anfrage und leitet sie zum Ausgang weiter.

Dadurch dass die Aktionen der Externen aufgezeichnet werden, sind sie für den zuständigen Bausig Mitarbeiter einer nachträglichen Kontrolle zugänglich.

3. Fall „Manches ist erlaubt“

Der Umweg über den Kopierer kann dadurch abgekürzt werden, dass der ERLAUBT-Mover entsprechend einstellt. Dies geschieht dadurch, dass man die Aktion für die Person freischaltet. Darf Meier z.B. Zeichnungen anschauen, so muss im Dialog beim Reiter „Zeichnung anschauen“ die Meier in die Liste der Freigeschalteten aufgenommen werden. Anfrage-Dokumente des Typs „Zeichnung anschauen“ von der Person Meier werden dann über den OK-Ausgang direkt an ADOS geschickt.

Anpassen durch Ändern der Komposition

Abschließend soll noch gezeigt werden, wie sich andere Mechanismen durch das Hinzufügen von Komponenten und dem Umgestalten von Verbindungen ebenfalls implementieren lassen.

Ein Beispiel wie durch Neugruppierung der Komponenten so etwas wie kontrollierte Zugriffskontrolle erreicht werden kann, ist in Abb. 5 gezeigt. In den Gruppengesprächen bei Bausig konnte man gewisses Misstrauen gegenüber einer dezentralen Sicherheitslösung heraushören. Eine Möglichkeit dieses Bedenken in die Systemgestaltung mit aufzunehmen, besteht darin, alle automatisch beantworten Anfragen durch einen Sicherheitsadministrator kontrollieren zu lassen. Seine Aufgabe ist es, darauf zu achten, dass die Firmenrichtlinien eingehalten werden.

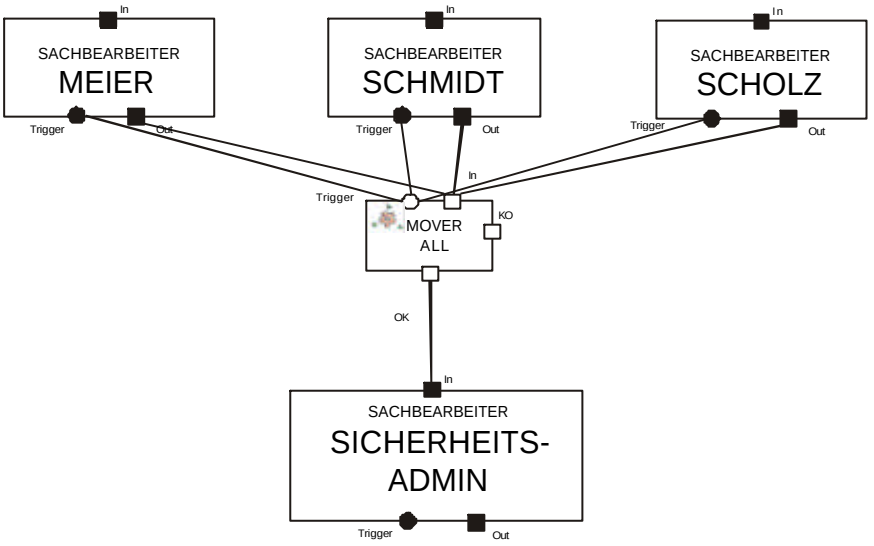


Abb. 5: Komponenten-Aufbau für die Ausübung einer zentralen Kontrolle

Bei der Umsetzung dieser Anforderung kommt einen die Hierarchisierungseigenschaft der FlexiBeans zu Gute. Die in Abb. 4 dargestellten zusammen Komponenten kann als eine eigenständige abstrakte SACHBEARBEITER-Komponente wiederverwendet werden. Der Out- und der Trigger-Port des AUSGANG-Postfach und der In-Port des EINGANG-Postfach bilden den Out-, den Trigger und den In-Port der SACHBEARBEITER-Komponente. Wie in Abb. 5 zu sehen, hat jeder Mitarbeiter seine eigene SACHBEARBEITER-Komponente. Doch statt die verarbeiten Dokumente direkt zurückzuschicken, werden sie alle von dem ALL-Mover eingesammelt und zur einer „Nachkontrolle“ an die SICHERHEITS-ADMIN-Komponente geschickt. Diese Komponente des müßte

noch an die Bedürfnisse angepaßt werden. So kann man z.B. die NACH-ADOS und die ADOS Komponente weglassen, und die Dokumente direkt ins AUSGANG-Postfach schicken, da die Anfragen verarbeitet worden sind.

Ein andereres Sicherheitsbedürfnis, dass durch Einführen einer neuen MOVER-Komponente Rechnung tragen werden kann, ist die Kontigentierung. So war aus den Gesprächen herauszulesen, dass das Anschauen einzelner Zeichung nicht problematisch war. Es gab aber die Befürchtung, dass von Aussen das ganze Archiv „leergesaugt“ wird. Dem kann gegengewirkt werden, wenn man die Anzahl der zurückgeschickten Zeichnungen begrenzt. Technisch kann dies mit einem „Kontigentierungs“-Mover bewerkstelligt werden, der in einem gewissen Zeitraum nur eine gewisse Anzahl von Dokumenten weiterleitet, z.B. fünf am Tag. Die Einstellungsmöglichkeiten des Movers bestehen in der Vorgabe des Kontingents. Ein solcher Mover könnte dann zwischen der ADOS-Komponente und dem AUSGANG-Postfach geklemmt werden.

Zusammenfassung

Allgemein kann man davon ausgehen, dass bei der Kooperation in virtuellen Organisationen erhöhte Sicherheitsanforderungen an das Computersystem gestellt werden. Diese beschränken sich nicht nur darauf, die Vertraulichkeit der Daten gegenüber Dritten zu schützen, sondern auch dem Kontrollbedürfnis der Beteiligten Rechnung zu tragen.

Vor diesem Hintergrund haben wir neue Konzepte der Zugriffskontrolle auf elektronische Archive untersucht. Bei traditionellen Zugriffskontrollsystemen kann der Anwender meist nur zwischen den Optionen ‚Erlaubt’ und ‚Verboten’ wählen. Implizit liegt dabei die Prämisse zu Grunde, dass im *vornherein* bestimmt werden kann, was erlaubt, und was verboten ist. Wir haben gezeigt, dass gerade bei der Zusammenarbeit in virtuellen Organisationen dieser Ansatz zu kurz greift. In solchen Konstellation, durch die Gleichzeitigkeit von Kooperation und Konkurrenz geprägt sind, wird der Zugriff bei traditionellen Systemen über Gebühr eingeschränkt. Wir haben gezeigt, wie mit erweiterten Zugriffsmechanismen der Zeitpunkt der Entscheidung über den Zugriff verlagert werden kann und so neue Möglichkeiten der zwischenbetrieblichen Kooperation eröffnet werden.

Bei der Realisierung dieser Möglichkeiten sind die Interdependenzen, die zwischen Technikgestaltung und Organisationsstruktur bestehen, zu beachten. Sie sprechen dafür, beide in einem integrierten Prozess zu entwickeln, wie es das OTD-Vorgehensmodell vorschlägt (vgl. Wulf und Rohde 1995). Dabei ist die Informatik gefordert, für die durch die Virtualisierung des Zugriffs entfallenden Kontrollinstanzen einen adäquaten Ersatz zu schaffen. Andererseits ist auch die Organisationstheorie gefordert, die Folgen der Virtualisierung zu untersuchen und

sie in ihren Konzepten der Organisationsgestaltung zu berücksichtigen.

Kompentenbasierte Anpassbarkeit ermöglicht es dabei, sich potentiell während der Nutzung sich verändernde Anforderungen an die Technikgestaltung schon während der Implementierung zu antizipieren. Die dabei zu entwickelnden Anwendungen, in unseren Falle ADOS-X, sollten an die aktuelle Kooperationspraxis anknüpfen. Gleichzeitig sollten sie so flexibel gestaltet werden, dass sie bei einer Veränderung der Zusammenarbeit nicht zu einem Hindernis werden, sondern solche Organisationsentwicklungsprozesse vielmehr durch „sanfte" Übergänge unterstützt. Diesem Praxistest muss ADOS-X noch unterzogen werden.

Danksagung

Das OrgTech Projekt wurde im Rahmen der ADAPT-Initiative von der EU-Kommission und dem Land NRW über einen Zeitraum von drei Jahren gefördert. Wir bedanken uns bei unseren Kollegen H. Chudora (FhG-IGD), J. Hinrichs (Universität Bremen), M. Krings (Universität Bonn), B. Nett (Universität Freiburg und Internationales Institut für Sozio-Informatik), T. Reichling (Fraunhofer FIT), O. Stiemerling (Universität Bonn) und A. Stork (FhG-IGD) für die enge Zusammenarbeit im Projekt. Ebenso sei I. Wienke (Universität Frankfurt) für seine Hilfe bei der Analyse der Interviews gedankt. Die Anmerkungen der anonymen Reviewer haben wesentlich dazu beigetragen, die Darstellung unserer Ergebnisse zu verbessern.

Literaturverzeichnis

Arnold, O./Härtling M. (1995): *Virtuelle Unternehmen: Begriffsbildung und –diskussion*; Arbeitspapiere der Reihe Informations- und Kommunilationssystem als Gestaltungselement virtueller Unternehmen; Bern; 1995.

Bensman, J/Gerver, I. (1963): *Vergehen und Bestrafung in der Fabrik*; in: Symbolische Interaktion; Klett; Stuttgart; 1973; S. 126-138.

Boland, R.J./Pondy, L.R. (1983): *Accounting in Organizations: A Union of Natural and Rational Perspectives*; in: Accounting; Organizations and Society Vol. 8, No. 2/3; 1983; S. 223-234.

Coulouris G. (1998): *Securing Groupware for the Internet*; in: Information Security Bulletin; 1998 (zit. n. http://www.dcs.qmw.ac.uk/research/distrib/perdis/papers/InfoSecurity98/InfoSecurity-Coulouris.html - 14.9.2000).

Coulouris, G./Dollimore J./Roberts M. (1998): *Secure communication in non-uniform trust environments;* vorgelegt bei: ECOOP Workshop on Distributed Object Security; Brussels; 1998 (zit. n. http://www.dcs.qmw.ac.uk/research/distrib/perdis/papers/secure-communication.ps - 14.9.2000).

Davidow, W. H.; Malone, M. S. (1993): The Virtual Corporation. New York: Harper Collins

Denning, D.E. (1976): *A Lattice Model of Secure Information Flow*; in: Communication of the ACM; 19(5); 1976; S. 236-241.

Eckert, C. (1996): *Leitlinien zur Klassifikation und Bewertung von Sicherheitsmodellen*; in: Fachtagung Sicherheit in Informationssystemen, SIS'96; Wien; 1996 (zit. n. http://sunspies17.informatik.tu-muenchen.de/forschung/papers/eigene/eck_WienSIS96.ps - 14.9.2000).

Ellis, C. A./Gibbs, S. J./Rein, G. L. (1991): *Groupware - some Issues and Experiences*; in: Communications of the ACM, vol. 34, 1; 1991; S. 38-58.

Everling, W. (1995): Leserbrief in: Informatik-Spektrum 18 (1995).

Fuchs-Frohnhofen P./Nett P./Wulf V. (2001): Integrated Organizational and Technological Development (OTD): The OrgTech Project, in: Proc. 7th International Symposium Automated Systems Based on Human Skill, International Federation of Automatic Control (IFAC), Pergamon Press, London 2001, S. 229 – 232

Gryczan G. (1996): *Prozeßmuster zur Unterstützung kooperativer Tätigkeit*; Deutscher Universitätsverlag; Wiesbaden; 1996.

Hamilton, G. (1997): *JavaBean Version 1.01*; Sun Microsystems; 1997 (zit. n. ftp://ftp.javasoft.com/docs/beans/beans.101.pdf - 15.10.2000).

Harms, V. (1973*): Interessenlagen und Interessenkonflikte bei der zwischenbetrieblichen Kooperation*; Würzburg; Physica-Verlag; 1973.

Iacucci, G./Peters, R/Stiemerling, O/Wulf, V. (1998): *Telecooperation Systems in Engineering Companies Supplying the Metallurgy Industry: The Experience of the OrgTech Project*; in: Globlization of Manufacturing in the Digital Communications Era of the 21st Century –Innovation, Agility, and the Virtual; Kluwer; Dordrecht; 1998; S. 107 – 119.

Mambrey, P; Robinson, M. (1997): Understanding the role of of documents in a hierarchical flow of work, in: Proceedings of GROUP'97, ACM-Press, New York 1997, S. 119 – 127

Mertens, P.; Griese, J.; Ehrenberg, D. (1998): Virtuelle Organisationen und Informationsverarbeitung, Springer Heidelberg

Nardi B.A.: A Small Matter of Programming. Perspectives on End User Programming; The MIT Press; London; 1993

Nett, B.; Fuchs-Frohnhofen, P.; Wulf, V.: Obstacles to Telecooperation in Engineering Networks of the Building Industry, in: Proceedings of the Participatory Design Conference 2000, 29.11. – 1.12.2000, New York, S. 143 - 147

Oevermann U. (1997): *Thesen zur Methodik der werkimmanenten Interpretation vom Standpunkt der objektiven Hermeneutik*; vorlegt bei: 4. Arbeitstagung der Arbeitsgemeinschaft objektive Hermeneutik e.V.; Frankfurt a. M.; April 1997 (zit. n. http://www.rz.uni-frankfurt.de/~hermeneu/Werkimman-Interpret-1997.rtf - 14.9.2000

o.V. (Wirtschaftslexikon): *Gabler Wirtschafts-Lexikon Bd. 3*; Gabler, Wiesbaden; 1997.

Peltzer, U. (1998): *Auswirkungen neuer Organisationsform*; in: Formen der Kooperation: Bedingungen und Perspektiven; hrsg. von Erika Spieß; Verl. Für Angewandte Psychologie; Göttingen; 1998; S. 169-176.

Picot/Neuberger (1997): *Virtuelle Unternehmen*; in: Gabler Wirtschafts-Lexikon Bd. 4; Gabler, Wiesbaden; 1997

Pfitzmann, A./ Müller, G. (Hrsg.) (1997): *Mehrseitige Sicherheit in der Kommunikationstechnik*, Bonn: Addison-Wesley

Povey, D.: *Optimistic Security: A new access control paradigm*; in: Proceedings of the 1999 New Security Paradigms Workshop; 1999 (in Druck) (zit. n. http://security.dstc.edu.au/staff/povey/papers/optimistic.pdf - 14.9.2000)

Povey, D. (1999): Optimistic Security: A new access control paradigm. Panel Presentation: *Highlights of the 1999 New Security Paradigms Workshop*. National Information Systems Security Conference (NISSC); Arlington; Virginia. October; 1999 (zit. n. http://security.dstc.edu.au/staff/povey/presentations/optimistic.ppt)

Rittenbruch, M./Kahler, H./Cremers, A.B. (1999): *Unterstützung von Kooperation in einer Virtuellen Organisation*; in: Proceedings der Wirtschaftsinformatik; 1999; S. 585-604.

Rohde, M.; Rittenbruch, M.; Wulf, V. (Hrsg.) (2001): Auf dem Weg zur virtuellen Organisation, Physica, Heidelberg

Schefe, P. (1998): *Softwaretechnik und Erkenntnistheorie;* Universität Hamburg; ASI; (zit n. http://asi-www.informatik.uni-hamburg.de/personen/schefe/priv/SWT-Erk.html – 10.92000).

Schüppler D. (1998*): Informationsmodelle für überbetrieblich Prozesse*; Frankfurt a.M; Peter Lang; 1998 .

Schneiders, S. (1998): *Sicheres Teleworking*; SIUK '98; (zit. n. http://crypto.mchh.siemens.de/vortraege/vortrag2/siuk98.doc - 14.9.2000).

Schneiders, S. (1999): *Security für Home und Office*; NetSiKom Köln 1/99 (zit. n. http://crypto.mchh.siemens.de/vortraege/vortrag5/netsicom2000text.pdf - 14.9. 2000).

Shen, H/Dewan, P.(1992): *Access Control for Collaborative Environments*; in: Proceedings of the Conference on Computer-Supported Cooperative Work (CSCW92); ACM Press; New York; 1992; S. 51-58.

Sieber, P. (1998): Virtuelle Unternehmen in der IT-Branche, Haupt Bern

Sikkel, K. (1997): *A Group-based Authorization Model for Computer-Supported Cooperative Work*; Arbeitspapiere der GMD 1055; GMD; Sankt Augustin; 1997 (zit. n. http://wwwhome.cs.utwente.nl/~sikkel/papers/ps/arbeitspapier1055.ps.gz - 14.9. 2000).

Stiemerling, O. (1996): *Anpaßbarkeit von Groupware – ein regelbasierter Ansatz;* Diplomarbeit; Universität Bonn; Institut für Informatik III; Dezember 1996.

Stiemerling, O. (2000): *Component-Based Tailorability*; Doktorarbeit; Universität Bonn, Institut für Informatik III; 2000

Stiemerling, O/Hinken, R./Cremers, A. B.(1999): *The EVOLVE Tailoring Platform: Supporting the Evolution of Component-Based Groupware*; in: Proceedings of EDOC'99, IEEE Press; Mannheim, Sept. 27.-30. ; 1999; S. 106-115.

Stiemerling, O./Wulf, V. (2000): *Beyond 'Yes or No' - Extending Access Control in Groupware with Awareness and Negotiation*; Group Decision and Negotiation 9; Kluwer Academic Publishers; 2000.

Stiemerling, O./Won, M./Wulf, V. (2000): *Zugriffskontrolle in Groupware – Ein nutzerorientierter Ansatz, in: WIRTSCHAFTSINFORMATIK, 42. Jg., Heft 4, 2000, S. 318 - 328*

Strausak, N. (1998): *Résumé of VoTalk*; in: Organizational Virtualness, Proceeding of the VoNet – Workshop, April 27-28; Bern; 1998; S. 9-24.

Sydow, J./Windeler A./Krebs, M./Loose, A./van Well, B. (1995): *Organisation von Netwerken, Strukturationstheoretische Analysen der Vermittlungspraxis in Versicherungsnetzwerken*; Westdeutscher Verlag; Opladen; 1996.

Travica, B. (1997): The Design of the Virtual Organisation: A Research Mode. In: Proceedings of the Association for Information Systems '97, Americas Conference, Indianapolis. Verfügbar unter http://hsb.baylor.edu/ramsower/ais.ac.97/papers/travica.htm, *Stand: 04.10.2000*

Weltz, F/Lullies,V./Ortmann, R.G. (1991): *Häufig geht es bei der Software-Entwicklung gar nicht so sehr um die Sache*; in COMPUTERWOCHE vom 18.01.1991.

Wulf M.(1995): *Konzeption und Realisierung einer Umgebung zur Koordination rechner-*

gestützter Tätigkeiten in kooperativen Arbeitsprozessen; Diplomarbeit Universität Hamburg Fachbereich Informatik; Arbeitsbereich Softwaretechnik; September 1995

Wulf, V. (1995b): *Negotiability: A Metafunction to Tailor Access to Data in Groupware*; in: Behaviour & Information Technology, Vol. 14, No. 3; 1995; S. 143 – 151.

Wulf, V. (1997): *Konfliktmanagement bei Groupware.* Braunschweig; Wiesbaden; Vieweg 1997.

Wulf, V. (2000): Zu anpaßbaren Gestaltung von Groupware, Habilitationsschrift, Fachbereich Informatik, Universität Hamburg, Hamburg 2000

Wulf, V./Krings, M./Stiemerling, O./Iacucci G./Maidhof, M./Peters, R./Fuchs-Fronhofen, P./Nett, B. Hinrichs, J. (1999): *Improving Inter-Organizational Processes with Integrated Organization and Technology Development*, in: Journal of Universal Computer Science (JUCS), Vol. 5, No. 6, 1999, S. 339 – 365.

Wulf, V./Rohde, M. (1995). *Towards an Integrated Organization and Technology Development*; in: Proceedings of the Symposium on Designing Interactive Systems, 23. - 25.8.1995, Ann Arbor (Michigan); ACM-Press; New York; 1995; S. 55 - 64.

Züllighoven H. (1998): *Das objektorientierte Konstruktionshandbuch nach dem Werkzeug & Material-Ansatz*; dpunkt-Verlag; Heidelberg; 1998.