

Evolution von Zugriffsregelungen in Informationssystemen*

Manfred Reichert · Ursula Catrinescu-Wiedemuth · Stefanie Rinderle

Universität Ulm, Abteilung Datenbanken und Informationssysteme
{reichert, rinderle}@informatik.uni-ulm.de

Zusammenfassung

In (prozessorientierten) Informationssystemen erfolgt die Zugriffs- und Bearbeiterkontrolle oftmals auf Grundlage einfacher Rollenkonzepte. Dies hat den Vorteil, dass der Wechsel eines Mitarbeiters innerhalb des Unternehmens durch Änderung seiner Rollenzuordnung abgebildet werden kann, ohne dass weitere Anpassungen von Zugriffs- oder Bearbeiterregeln erforderlich werden. Dadurch sind auch Prozessdefinitionen robust gegenüber Änderungen der Personalstruktur. Bis heute jedoch nicht wirklich verstanden ist, wie Modelle zur Abbildung komplexer Organisationsstrukturen und deren Evolution (z.B. Fusion oder Aufspaltung von Einheiten, Änderung der Rollenzuordnung eines Mitarbeiters) systemseitig unterstützt werden sollen. Erfolgen Modelländerungen unkontrolliert, können inkonsistente oder fehlerhafte Zugriffs- und Bearbeiterregeln resultieren. Schlimmstenfalls ergeben sich sogar veraltete Arbeitslisten und damit Sicherheitslücken in der Bearbeiterkontrolle. In diesem Beitrag werden die mit der Änderung von Organisationsmodellen verknüpften Probleme erörtert, und es werden Lösungsansätze für die kontrollierte Evolution der darauf basierenden Zugriffsregeln skizziert. Diese Arbeiten sind im ADEPT-Projekt angesiedelt, in dem die technologischen Grundlagen für die Realisierung adaptiver, prozessorientierter Informationssysteme geschaffen werden.

1 Einleitung

Unternehmen, die am Markt erfolgreich sein wollen, müssen sich immer rascher auf neue Gegebenheiten einstellen. Vielfach führt dies zu Anpassungen der Aufbau- und Ablauforganisation, zu neuen Formen der Zusammenarbeit mit Partnern, Zulieferern und Kunden oder zu anderen mehr oder weniger gravierenden Veränderungen. Die Fähigkeit, ihre Informationssysteme rasch an derartige Änderungen anzupassen wird für Unternehmen zukünftig ein wesentlicher Wettbewerbsfaktor sein. Die in Form von sog. Workflow-Management-Systemen (WfMS) [LeRo00] derzeit kommerziell verfügbare Technologie wird diesen Ansprüchen ebenso wenig gerecht wie gängige Branchensoftware. Beide springen hinsichtlich Funktionalität zu kurz, auch Flexibilitäts- und Wartungsaspekte werden vernachlässigt. Insbesondere die starre Implementierung der Prozesse –

* Diese Arbeit wurde im Rahmen des von der Deutschen Forschungsgemeinschaft (DFG) geförderten Projektes „Änderungsmanagement in adaptiven Workflow-Management-Systemen“ erstellt.

von dem einmal hinterlegten Ablauf kann bei der Prozessausführung nicht abgewichen werden – stellt für den praktischen Einsatz ein ernsthaftes Hindernis dar. Im ADEPT-Projekt arbeiten wir deshalb an fortschrittlichen Konzepten zur Verwirklichung adaptiver, prozessorientierter Informationssysteme [ReDa98, RiRD04]. Die entwickelte ADEPT-Technologie

- bietet eine prozessorientierte Sicht- und Denkweise ("Process-Awareness")
- erlaubt die rasche und kostengünstige Realisierung neuer Prozesse (Prozesstypen)
- integriert sowohl eigenentwickelte als auch zugekaufte Anwendungskomponenten bzw. -dienste in prozessorientierter Art und Weise
- gestattet einzelfallbezogene Abweichungen der Anwender vom geplanten Prozess
- ermöglicht es, Änderungen am Geschäftsprozess (am Prozesstyp) auf bereits laufende Einzelprozesse dieses Typs – soweit sinnvoll und möglich – zu übertragen
- bietet umfangreiche Prozessunterstützungsfunktionen (z.B. für das Termin-Management und die Verwaltung von Arbeitslisten)

Den Fokus unserer bisherigen Arbeiten bildete die Umsetzung von Prozessänderungen: Hierunter fallen die Evolution von Prozessschemata, die Propagation von Schemaänderungen auf laufende Prozessinstanzen sowie die einzelfallbezogene Abänderung von sich in Ausführung befindlichen Prozessinstanzen, etwa um angemessen auf Ausnahmesituationen zu reagieren [ReDa98, RiRD04]. Noch nicht betrachtet wurden dagegen Änderungen der Aufbauorganisation und dadurch notwendige Anpassungen der sie beschreibenden Organisationsmodelle. – Ein Org.-Modell (siehe Abb. 1) definiert z.B. Einheiten, Rollen und Mitarbeiter sowie deren Beziehungen untereinander (z.B. Zuordnung von Mitarbeitern zu Org.-Einheiten und/oder Rollen; Generalisierungsbeziehungen zwischen Rollen).

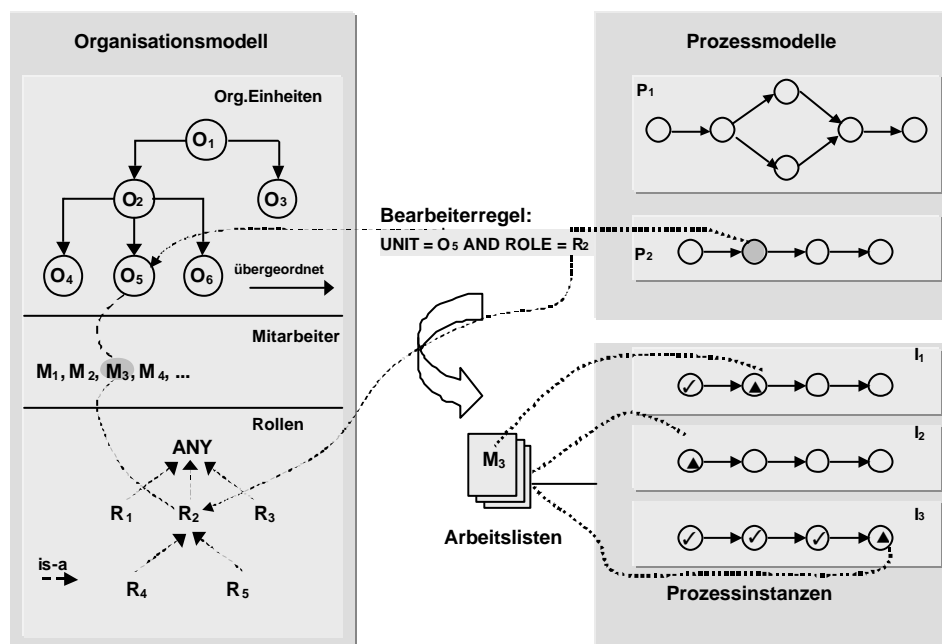


Abb. 1: Organisationsmodell, Bearbeiterregeln und Arbeitslisten

Ausgehend von einem Org.-Modell lassen sich Regeln für den Zugriff auf Objekte (z.B. Prozessdokumente) sowie die Bearbeitung von Prozessaktivitäten (z.B. Benutzer mit bestimmter Rolle) festlegen. Auch die Beschreibung von Berechtigungskonzepten für Ad-hoc-Änderungen kann auf Grundlage des Org.-Modells erfolgen [ReRi02]. In heutigen Unternehmen werden Rollen- und Mitarbeiter-Daten oftmals redundant von verschiedenen Applikationen verwaltet. Die Folge sind inkonsistente oder inkompatible Modelle sowie ein erhöhter Aufwand für deren Wartung und Pflege. Aus diesen Gründen werden entsprechende Daten vermehrt in ein zentrales Verzeichnis (z.B. einen LDAP-Server) eingepflegt, an das interessierte Applikationen dann Anfragen stellen können. In einem WfMS ist zu diesem Zweck bei der Prozessdefinition für jede interaktive Aktivität eine Bearbeiterregel zu hinterlegen (z. B. Unit = *Ambulanz* and Role = *Arzt*). Diese dient zur Laufzeit als Anfrage des WfMS an das Org.-Modell zwecks Ermittlung der potentiellen Bearbeiter einer auszuführenden Aktivität. Für diese wiederum werden Einträge für Benutzerarbeitslisten erzeugt.

Ein bekanntes Problem, das sich im Zusammenhang mit der Änderung von Org.-Modellen stellt, sind verwaiste Referenzen. Werden z.B. Org.-Einheiten oder Rollen zusammengelegt, aufgelöst oder (hierarchisch) umgehängt, können Zugriffs- oder Bearbeiterregeln ggf. nicht mehr in ihrer bisherigen Form genutzt werden. Hiervon kann auch die Zuordnung der Aktivitäten von Prozessinstanzen zu Bearbeitern betroffen sein. Werden im Bsp. aus Abb. 1 die Rolle R_2 oder die Org.-Einheit O_2 gelöscht, ist die dargestellte Bearbeiterregel nicht mehr auflösbar. Schlimmstenfalls werden für diesen Fall dann Aktivitäten falsch oder gar nicht mehr zugewiesen. Dieser Fall würde im Beispiel aus Abb. 1 auftreten, wenn die Rollenzuordnung des Mitarbeiters M_3 von R_2 auf R_1 geändert, die Arbeitsliste von M_3 aber nicht mit angepasst wird. Durch solche und ähnliche Fälle können Sicherheitsbestimmungen verletzt werden oder sogar der gesamte Workflow ins Stocken geraten. Zu beachten ist auch, dass Bearbeiterregeln oftmals durch das WfMS verwaltet werden, wohingegen Org.-Modelle von einer separaten Komponente gehalten werden sollten.

Im ADEPT-Projekt haben wir umfassende Konzepte zur Definition, Änderung und Pflege von Org.-Modellen entwickelt. Sie bieten eine vollständige Menge von Änderungsoperationen, die sich durch eine präzise Semantik auszeichnen und die sämtliche Änderungen des Org.-Modells unter Beachtung gewisser Konsistenzeigenschaften erlauben. Darauf aufbauend haben wir Konzepte für die Anpassung von Bearbeiterregeln, die ein (geändertes) Org.-Modell referenzieren, entwickelt. Je nach Semantik der Änderung bieten wir Lösungsansätze zur automatischen, semi-automatischen oder manuellen Anpassung "veralteter" Bearbeiterregeln. In diesem Zusammenhang gibt es verschiedene Strategien zur Feststellung, welche Bearbeiterregeln bei Org.-Modelländerungen angepasst werden müssen und wann diese Anpassungen erfolgen sollen. Darüber hinaus betrachten wir, welche Auswirkungen Org.-Modelländerungen auf laufende Prozessinstanzen und Benutzerarbeitslisten haben. Interessant ist hier vor allem die Frage, wann die Auflösung von Bearbeitern erfolgt und inwieweit evtl. Org.-Modelländerungen von einer Neuberechnung von Arbeitslisten begleitet werden müssen.

Kapitel 2 fasst Aspekte der Erstellung und Änderung von Org.-Modellen zusammen. Davon ausgehend diskutieren wir in Kapitel 3 bestehende Anforderungen und Lösungsansätze zur beglei-

tenden Adaption von Zugriffs- und Bearbeiterregeln. Kapitel 4 erweitert diese Betrachtungen im Hinblick auf die dynamische Anpassung von Arbeitslisten.

2 Erstellung und Änderung von Org.-Modellen

In diesem Abschnitt werden Grundlagen zur Erstellung und Änderung von Org.-Modellen skizziert – sie sind für das weitere Verständnis des Artikels erforderlich.

2.1 Beispiel eines Organisationsmetamodells

Zunächst stellen wir exemplarisch ein Metamodell vor, wie es auch in anderen Ansätzen gebräuchlich ist. Es gibt die Elemente und Strukturen vor, auf deren Basis sich Organisationen modellieren lassen. Die formale Darstellung der Modelle, die nicht den Fokus dieses Beitrags bildet, ist mengenbasiert. Dies erleichtert z.B. die Realisierung von Operationen zur Erstellung und Änderung von Org.-Modellen sowie die präzise Festlegung ihrer Semantik (vgl. Abschnitt 2.3). Das für die folgenden Betrachtungen zugrunde gelegte Metamodell zeigt Abb. 2.

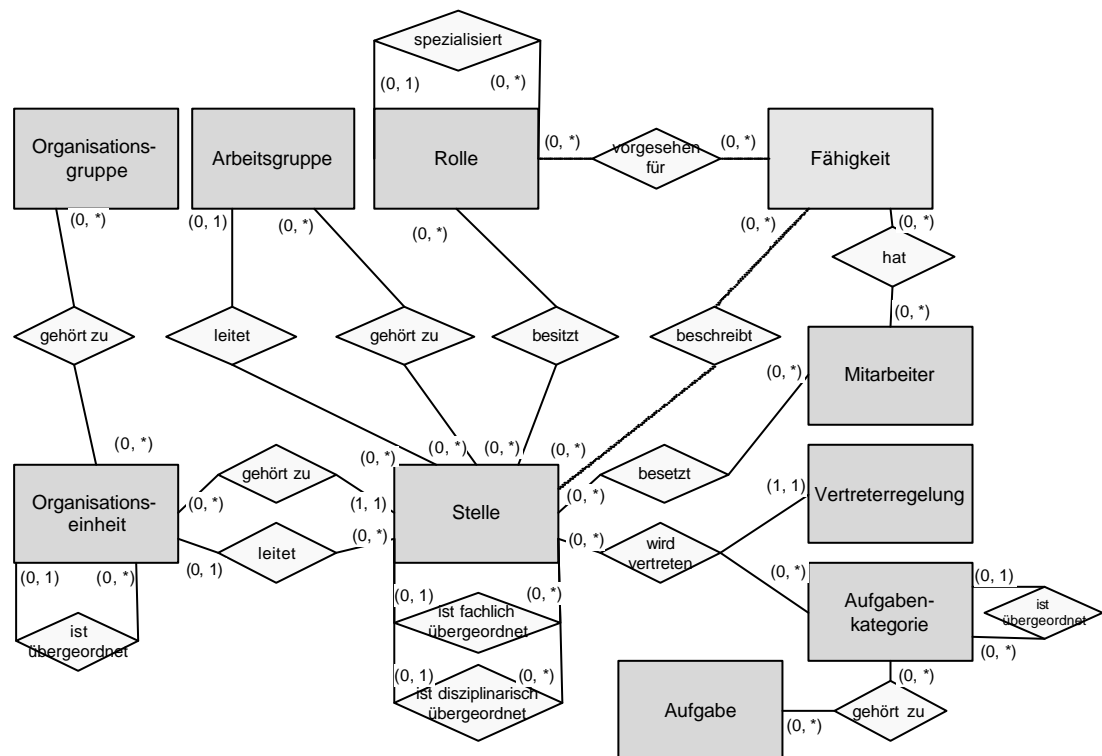


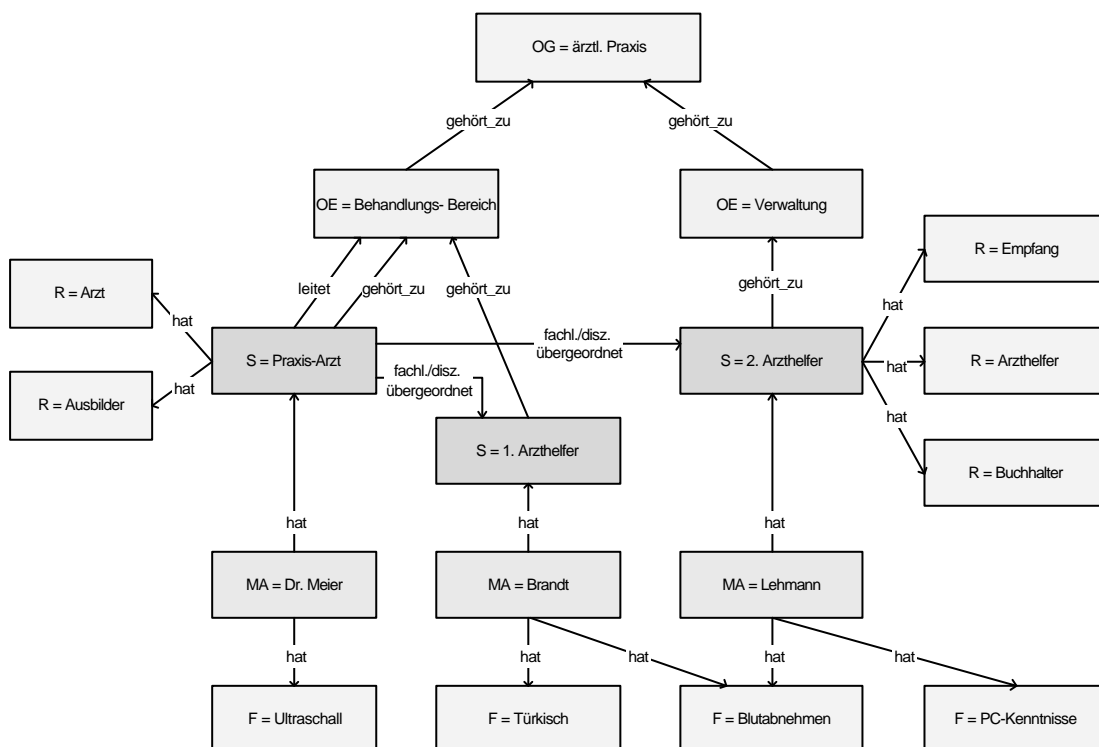
Abb. 2: Organisations-Metamodell

Ein Basiselement bildet *Stelle*. Eine Stelle bündelt immer bestimmte Aufgaben und kann durch einen oder mehrere Mitarbeiter besetzt werden. Sie wird immer genau einer *Org.-Einheit* zugeordnet, kann aber beliebig viele Org.-Einheiten leiten. Des weiteren können Stellen in *Arbeitsgruppen*

aggregiert werden, wodurch sich z.B. temporäre *Projektgruppen* modellieren lassen. Einer Stelle können beliebig viele *Rollen* zugeordnet werden. Eine konkrete Rolle beschreibt dabei Qualifikationen und Kompetenzen ihrer Rollenträger. Rollen können weiter spezialisiert werden. Dabei "erben" speziellere Rollen die Eigenschaften der weniger speziellen. Ein *Mitarbeiter* kann beliebig viele *Fähigkeiten* haben. Daneben steht er nur mit Stelle in Beziehung. Das hat den Vorteil, dass die übrigen Zuordnungen im Org.-Modell erhalten bleiben, wenn ein Mitarbeiter gelöscht wird. Schließlich gestattet das Metamodell auch die Modellierung von *Vertreterregelungen*. Diese haben die Form von Bearbeiterregeln, so dass sie sich auf feste Mitarbeiter, aber auch auf andere Org.-Modellelemente beziehen können (z.B. Vertretung durch bestimmte Rolle oder Stelle). Durch Angabe von Aufgabenkategorien lassen sich Vertretungen zudem auf bestimmte Aufgaben beschränken.

2.2 Organisationsmodelle

Org.-Modelle bilden die realen Organisations- und Personalstrukturen mit den Konstrukten des Metamodells ab. Ein einfaches Beispiel, das als Bezugsbasis für unsere weiteren Betrachtungen dienen soll, zeigt Abbildung 3.



(Pfeile stehen für die Leserichtung der Beziehungen; F = Fähigkeit; MA = Mitarbeiter; OE = Organisationseinheit; OG = Organisationsgruppe; R = Rolle; S = Stelle)

Abb. 3: Einfaches Organisationsmodell einer Ärztlichen Praxis

Beispiel (Organisationsmodell): Zu einer ärztlichen Praxis gehören zwei Bereiche: Verwaltung und Behandlungsbereich. Der Verwaltung ist die Stelle einer Arzthelferin zugeordnet, die Frau Lehmann inne hat. Zur Stelle gehören Aufgaben beim Empfang, als Arzthelfer und bei der Abrechnung. (Diese Aufgabenkomplexe werden als Rollen modelliert.) Frau Lehmann kann darüber hinaus Blut abnehmen und mit dem PC umgehen. Dem Behandlungsbereich sind eine Arztstelle und ein weiterer Arzthelfer zugeordnet. Der Praxis-Arzt ist Dr. Meier, der besondere Fähigkeiten mit Ultraschall hat. Er leitet die Praxis und ist fachlich und disziplinarisch den beiden Arzthelfern übergeordnet. Neben der Rolle als Arzt gehört auch die Rolle als Ausbilder zur Stelle. Die zugehörige Arzthelferstelle ist von Herrn Brandt besetzt, der neben Blut abnehmen auch Türkisch kann.

2.3 Organisationsmodelländerungen

Für die Praxis sehr typisch sind personelle Veränderungen, etwa infolge der Neueinstellung, Entlassung oder Rotation von Mitarbeitern. Strukturelle Änderungen werden z.B. in Verbindung mit der Neugestaltung von Geschäftsprozessen oder dem Outsourcing von Bereichen erforderlich. Zunächst betrachten wir typische Änderungsszenarien und beziehen uns dabei auf das Beispiel aus Abb. 3.

Personelle Änderungen sind wenig komplex (vgl. Tab. 1). Wichtig ist, dass konkrete Zugriffs-/Bearbeiterregeln i. A. nicht an feste Mitarbeiter, sondern z. B. an Stellen oder Rollen gekoppelt werden. Auf diese Weise können sie nach personellen Änderungen weiter aufgelöst werden. Dagegen sind *strukturelle Änderungen* nicht an konkrete Mitarbeiter gebunden, sondern betreffen relativ stabile Strukturen der Organisation. Selbst einfache Anpassungen, wie in Tab. 2 dargestellt, können weiteren Änderungsbedarf nach sich ziehen. Wenn wie in Szenario 9 aus Tab. 2 eine Org.-Einheit gelöscht wird, muss geklärt werden was mit den zugehörigen Stellen geschieht (z.B. Löschen oder Zuordnung zu anderer Einheit). Entsprechende Informationen sind auch für die begleitende Anpassung von Zugriffs- und Bearbeiterregeln wichtig. Tab. 3 zeigt einige Szenarien für komplexere Änderungen. Werden, wie beim Szenario 14, zwei Org.-Modelle vereint, müssen ein einheitliches Metamodell bestimmt sowie Namens- und Strukturkonflikte ermittelt und aufgelöst werden. Für das Szenario 16 schließlich werden gemeinsame Sichten oder Schnittstellen der beteiligten Org.-Modelle benötigt.

Tab. 1: Szenarien für personelle Änderungen

	Beschreibung	Art der Änderung
Szenario 1	Frau Lehmann scheidet aus Praxis aus	Mitarbeiter löschen
Szenario 2	Frau Schumann übernimmt die Stelle der 2. Arzthelferin	Mitarbeiter einfügen
Szenario 3	Frau Schumann kann Steno schreiben	Fähigkeit e. Mitarbeiter einfügen
Szenario 4	Herr Brandt wechselt auf die 2. Arzthelfer-Stelle in der Verwaltung	Mitarbeiter verschieben
Szenario 5	Frau Schumann hat geheiratet und damit ihre Steuerklasse geändert	Attribut ändern

Tab. 2: Szenarien für einfache strukturelle Änderungen

	Beschreibung	Art der Änderung
Szenario 6	Stelle eines Auszubildenden wird im Behandlungsbereich eingerichtet	Stelle einfügen
Szenario 7	Stelle des 1. Arzthelfers im Behandlungsbereich wird eingespart	Stelle löschen
Szenario 8	Bereich Krankengymnastik wird geschaffen	Org.Einheit einfügen
Szenario 9	Bereich Verwaltung wird aufgelöst	Org.Einheit löschen
Szenario 10	Verwaltung und Behandlungsbereich werden zusammengelegt	Org.Einheiten vereinen
Szenario 11	Behandlungsbereich wird in Arztbereich und Pflegebereich geteilt	Org.Einheit teilen
Szenario 12	Azubi-Stelle wird vom Behandlungsbereich der Verwaltung zugeordnet	Stelle verschieben
Szenario 13	1. Arzthelfer wird Azubi-Verantwortlicher	Rollenzuordnung einfügen

Tab. 3: Szenarien für komplexe strukturelle Änderungen

	Beschreibung	Art der Änderung
Szenario 14	Fusion zweier Kliniken zu Klinikverbund	Vereinigen der gesamten Org.-Modelle
Szenario 15	Bereich Krankengymnastik einer Klinik wird ausgelagert in eigenständige Organisation	Trennen des Org.Modells
Szenario 16	Zusammenarbeit zwischen zwei Kliniken bei klinik-übergreifenden Aufgaben	Schnittstellen zwischen den Organisationen nötig
Szenario 17	Bereich Nierentransplantation von Gefäß-Klinik zur Chirurgischen Klinik zugeteilt	Organisationseinheit aus Organisation in andere Org. verschieben

ADEPT umfasst Operationen zur Verwirklichung solcher Modelländerungen (vgl. Abb. 4). Im Einzelnen sind dies Operationen für das Einfügen von Entitäten/Relationen (Szenarien 2, 3, 6, 8 und 13), das Löschen von Entitäten/Relationen (Szenarien 1, 7 und 9), das Ändern von Attributen einer Entität/Relation (Szenario 5) sowie das Teilen, Vereinigen und Verschieben von Entitäten (Szenarien 4, 10, 11 und 12). Einige dieser Operationen sind nicht auf alle Entitätstypen anwendbar. Tab. 4 gibt einen Überblick über semantisch sinnvolle Änderungen:

Tab. 4: Semantische sinnvolle Änderungen bezogen auf Entitäten (Auswahl)

Entitätstyp	Einfügen	Löschen	Attr.Änderung	Teilen	Vereinigen	Verschieben
Mitarbeiter	x	x	x	-	-	x
Org.Einheit	x	x	x	x	x	x
Org.Gruppe	x	x	x	x	x	-
Rolle	x	x	x	x	x	-
Stelle	x	x	x	x	x	x

Elementare Änderungen sind auf alle Entitäts- und Relationstypen anwendbar, etwa die Operationen Einfügen, Löschen und Attributänderung. Komplexe Änderungen sind Vereinigen, Teilen und Verschieben von Entitäten; sie lassen sich nur auf bestimmte Entitätstypen anwenden. Des weiteren können komplexe Änderungen prinzipiell auf elementare Änderungen zurückgeführt werden. So entspricht das Verschieben einer Entität dem Einfügen und Löschen von Relationen. Eine spezielle Behandlung der Verschiebeoperation bietet jedoch eine höhere Semantik und Vorteile hinsichtlich der späteren Anpassung von Bearbeiteregeln.

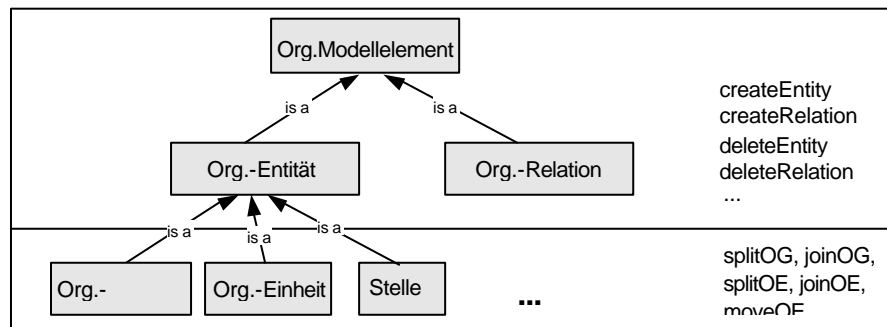


Abb. 4: Mehrere Ebenen für ADEPT-Änderungsoperationen auf Organisationsmodellen

Die ADEPT-Editoren bieten mächtige Funktionen zur Sicherung der Konsistenz von Org.-Modellen bei ihrer Änderung. Werden Entitäten z.B. vereinigt oder gesplittet, wird dafür gesorgt, dass zugehörige Relationen mit angepasst werden. Bestimmte Anpassungen können automatisch erfolgen, andere müssen manuell vom Modellierer durchgeführt werden.

Beispiel (Arbeitsgruppen vereinigen): Die Arbeitsgruppen *AG1* und *AG2* sollen zusammengelegt werden. Zu *AG1* gehört die Stelle *S-a*, sie leitet auch *AG1*. Zu *AG2* gehören sowohl *S-a* als auch *S-b*, sie wird von *S-a* geleitet (Abb. 5). Die resultierende Arbeitsgruppe *AG* beinhaltet beide Stellen *S-a* und *S-b*. Diese Anpassung kann automatisch erfolgen. Als Leiter für die resultierende Arbeitsgruppe *AG* schlägt das System in der aktuellen Konstellation die Stelle *S-a* vor, überlässt die endgültige Entscheidung aber dem Modellierer.

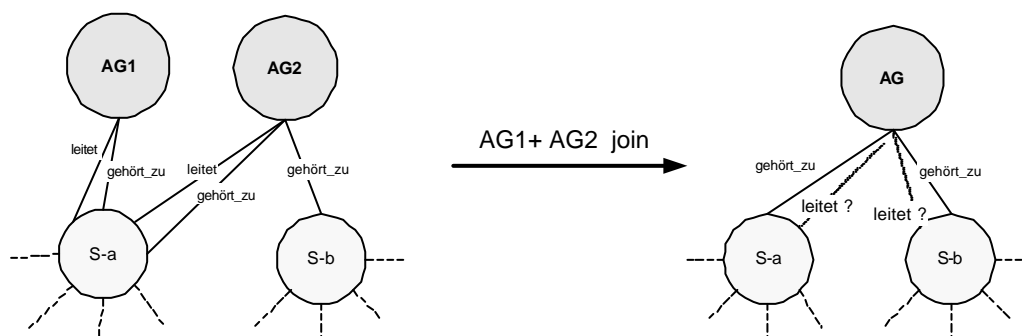


Abb. 5 Arbeitsgruppen vereinigen

Insgesamt bietet ADEPT eine vollständige Menge an Änderungsoperatoren an. Für sie liegt eine präzise formale Semantik vor. Des weiteren ist die Anwendung einzelner Operatoren an die Einhaltung bestimmter Vor- und Nachbedingungen gebunden. Insbesondere stellt ADEPT sicher,

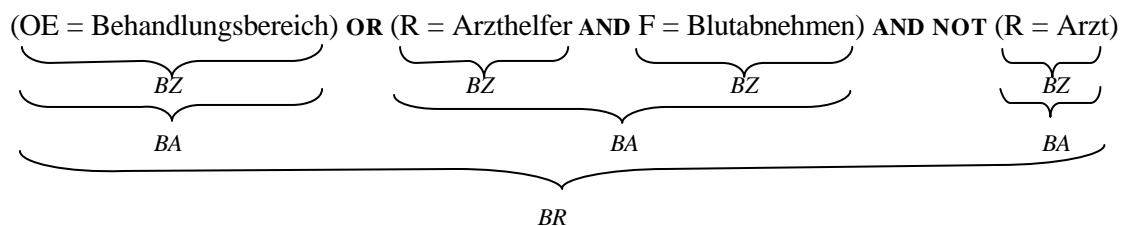
dass die Anwendung einer Menge von Änderungsoperationen auf ein korrektes Org.-Modell wieder zu einem korrekten Modell führt (i.S. der auf diesem Modell definierten Einschränkungen, etwa hinsichtlich Kardinalitäten und Referenzen). Die Zusammenfassung einer solchen Menge von Änderungsoperationen bezeichnen wir auch als Änderungstransaktion.

3 Adaption von Bearbeiterregeln

Bisher haben wir Änderungen des Org.-Modells isoliert betrachtet. Ihre Auswirkungen auf Bearbeiterregeln, welche das Org.-Modell referenzieren, sollen nun behandelt werden. Entsprechende Regeln werden nicht nur für die Zuweisung von Prozessaktivitäten zu Bearbeitern verwendet, sondern kommen auch bei der Vergabe anderer Zugriffs-, Änderungs- und Ausführungsrechte zum Einsatz. Wird nun das referenzierte Org.-Modell verändert, sind u.U. Teile der Bearbeiterregel nicht mehr korrekt definiert, etwa infolge verwaister Referenzen. Wir gehen in diesem Kapitel auf die Pflege von Querreferenzen zwischen Org.-Modell und Bearbeiterregeln ein. Es werden Lösungsansätze zur begleitenden Adaption von Bearbeiterregeln skizziert, die für Modellierer eine größtmögliche Unterstützung bieten sollen.

3.1 Bearbeiterregeln

Eine Bearbeiterregel referenziert Entitäten eines Org.-Modells. Sie determiniert eine Menge von Mitarbeitern, für welche die durch sie repräsentierten Berechtigungen gelten sollen. Typischerweise referenziert eine Bearbeiterregel Entitäten wie Stelle, Org.-Einheit oder Rolle. Die Auswertung der Regel liefert eine Menge von Mitarbeitern, die der Regel entsprechen. In ADEPT setzen sich Bearbeiterregeln (BR) aus Bearbeiterausdrücken (BA), die mittels Operatoren OR und AND NOT verknüpft werden, zusammen. Bearbeiterausdrücke selbst wiederum bestehen aus mittels AND-Operator verknüpften Bearbeiterzuordnungen (BZ). Eine BZ ist demnach die kleinste Einheit bei der Konstruktion von Bearbeiterregeln (siehe Tabelle 5). Beispiel:



3.2 Problemstellung

Wenn das Org.-Modell verändert wird, muss gewährleistet sein, dass bestehende Bearbeiterregeln konsistent und semantisch korrekt bleiben. Das heißt, die Transformation des Org.-Modells muss ggf. semantisch an die Bearbeiterregeln propagiert werden, so dass diese entsprechend angepasst werden können (vgl. Abb. 6). Ansonsten kann es vorkommen, dass eine Bearbeiterregel nicht mehr (vollständig) auflösbar ist, etwa wenn durch sie eine Entität referenziert wird, die aus dem Org.-Modell gelöscht wurde. Andererseits gibt es Modelländerungen, die für Bearbeiterregeln unkritisch

sind. Wenn z.B. eine Stelle neu geschaffen wird, kann sie bisher noch nicht referenziert worden sein. Dem entsprechend ist für Bearbeiterregeln keine Anpassung erforderlich. Aus der Semantik der angewandten Änderung können also Rückschlüsse auf erforderliche Anpassungen der Bearbeiterregeln getroffen werden.

Tab. 5: Beispiele für elementare Bearbeiterzuordnungen

Bearbeiterzuordnung	Bedeutung
AG = x	Bearbeiter ist Mitglied der Arbeitsgruppe x
AGl = x	Bearbeiter ist Leiter der Arbeitsgruppe x
F = x	Bearbeiter hat die Fähigkeit x
MA = x	Bearbeiter ist Mitarbeiter x
OE = x	Bearbeiter gehört der Org.Einheit x an
OE+ = x	Bearbeiter gehört einer Org.Einheit an, die der Org.Einheit x direkt oder indirekt übergeordnet ist
OE- = x	Bearbeiter gehört einer Org.Einheit an, die der Org.Einheit x direkt oder indirekt untergeordnet ist
OEl = x	Bearbeiter ist Leiter der Org.Einheit x
OEu = x	Bearbeiter ist Mitglied der Org.Einheit, die von Stelle x geleitet wird
OG = x	Bearbeiter ist Mitglied e. Org.Einheit, die der Org.Gruppe x angehört
R = x	Bearbeiter hat Rolle x
R+ = x	Bearbeiter hat angegebene oder speziellere Rolle
S = x	Bearbeiter besetzt Stelle x
S+ = x	Bearbeiter ist Vorgesetzter der Stelle x (bel. Ebene)

Bezogen auf eine Bearbeiterregel ist bei Änderung des referenzierten Org.-Modells zu klären, ob die Regel adaptiert werden muss oder nicht, und wie die Anpassung ggf. erfolgen soll. Neben einer vollautomatischen Anpassung, die das System selbständig durchführen kann, können Anpassungen semi-automatisch oder manuell vorgenommen werden. Bei der semi-automatischen Variante gibt der Benutzer dem System die Informationen, die es für eine automatische Anpassung der Bearbeiterregeln benötigt. Eine manuelle Anpassung führt er selbst aus.

3.3 Aspekte der Anpassung von Bearbeiterregeln

Ausgangspunkt unserer Betrachtungen sind Bearbeiterzuordnungen (BZ) als kleinste Einheit von Bearbeiterregeln (vgl. oben). Tab. 6 zeigt exemplarisch den Anpassungsbedarf für ausgewählte Änderungsoperationen des Org.-Metamodells (vgl. Abschnitt 2.3). Wie leicht zu erkennen ist, sind additive Änderungen (d.h. das Einfügen von Entitäten oder Relationen) hinsichtlich der Definition bestehender Bearbeiterzuordnungen unkritisch; dasselbe gilt in Bezug auf das Entfernen von Relationen aus dem Org.-Modell. Neu eingefügte Entitäten können in bestehenden BZ naturgemäß noch nicht referenziert worden sein. Relationen werden in BZ prinzipiell nicht referenziert. Deshalb besteht in beiden Fällen kein Anpassungsbedarf.

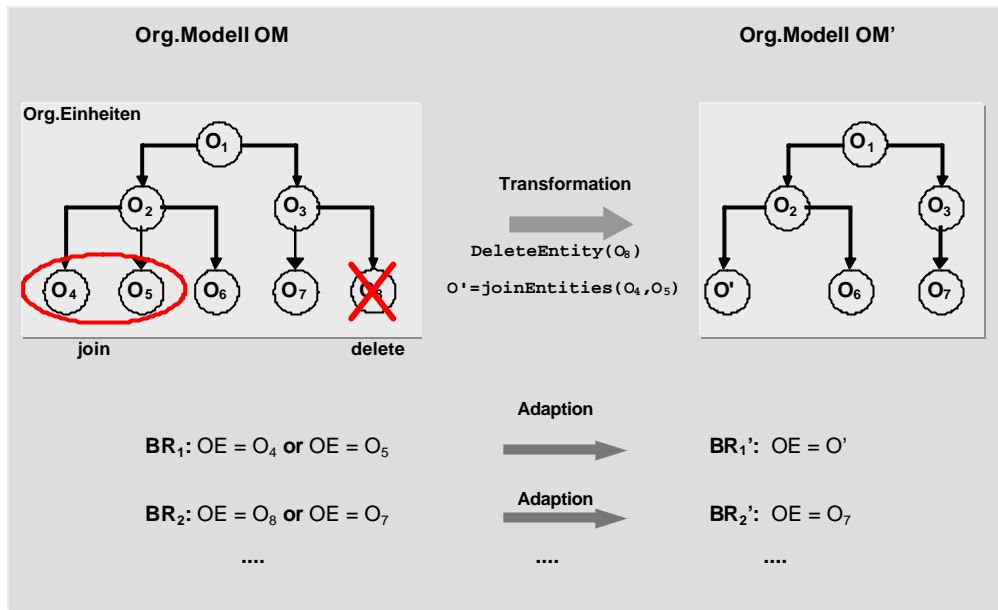


Abb. 6: Adaption von Bearbeiterregeln nach Änderung des Organisationsmodells

Tab. 6: Anpassungsbedarf von Bearbeiterzuordnungen (BZ) bei bestimmten Änderungen

Änderung	Anpassungsbedarf
CreateEntity	Keine Anpassungen erforderlich
DeleteEntity	Erfordert Anpassung der BZ, die das gelöschte Org.Element referenzieren
CreateRelation, DeleteRelation	Keine Anpassungen erforderlich
joinEntities	Erfordert Anpassung der BZ, die mind. eines der beiden vereinigten Org. Elemente referenzieren
splitEntity	Erfordert Anpassung der BZ, die das gesplittete Org.Element referenzieren

Kritisch sind dagegen Änderungen wie das Entfernen, Vereinigen oder Teilen von Entitäten, wenn die (veränderten) Entitäten direkt von den Bearbeiterzuordnungen referenziert werden. In diesen Fällen müssen Anpassungen erfolgen. Das Verschieben von org. Entitäten (z.B. Umhängen einer Org.-Einheit in der Org.-Hierarchie) ist an sich für Bearbeiterzuordnungen unkritisch. Wenn allerdings ein referenzierter Mitarbeiter einer anderen Stelle zugeordnet wird, sollte die Semantik der betroffenen BZ durch den Modellierer überprüft werden. Damit wird sichergestellt, dass die ursprüngliche Intention des Modellierers erhalten bleibt. Wir skizzieren kurz, wie sich die Adaption von Bearbeiterregeln konkret gestaltet. Dazu unterscheiden wir zwei Arten kritischer Org.-Modelländerungen:

1. Änderungen bei denen eine Entität aus dem Org.-Modell entfernt wird, so dass diese in Zukunft nicht mehr referenziert werden kann

2. Änderungen infolge derer die potentiellen Bearbeiter in der Organisation noch existieren, aber inzwischen anders referenziert werden müssen.

Im 1. Fall kann eine BZ nach Löschen einer von ihr referenzierten Entität nicht mehr aufgelöst werden, so dass die zugehörige Bearbeitermenge leer bleibt. Eine automatische Anpassung ist auf elementarer Ebene der Bearbeiterzuordnungen deshalb nicht möglich. Sinnvoll ist in diesem Fall eine Warnung an den Modellierer, mit der Aufforderung zur manuellen Anpassung. Auf Ebene komplexer Bearbeiterregeln sind weitergehende Strategien möglich, auf die wir später eingehen. Im 2. Fall existieren die potentiellen Bearbeiter noch, sind aber über die ursprüngliche Referenz nicht mehr erreichbar. Dieser Fall liegt z. B. bei Anwendung der Änderungsoperationen *Split* und *Join* vor. Die Anpassung einer betroffenen BZ kann hier automatisch oder semiautomatisch erfolgen. Das folgende Beispiel soll dies verdeutlichen.

Beispiel (Split-Operation): Wir gehen von $OE = o$ als BZ aus – sie referenziert die Org.-Einheit o . Angenommen o wird in die Einheiten o_1 und o_2 gesplittet ($splitOE(o) \text{ @ } o_1 + o_2$). Dann ist die Bearbeiterzuordnung $OE = o$ nicht mehr auflösbar. Soll die Anpassung der BZ automatisch vorgenommen werden, wird wie folgt verfahren: $OE = o$ wird durch $(OE = o_1 \text{ OR } OE = o_2)$ substituiert – beide BZ beschreiben dieselbe Bearbeitermenge. Alternativ kann die Anpassung semiautomatisch erfolgen. In diesem Fall werden dem Benutzer die Ausdrücke $OE = o_1$, $OE = o_2$ und $(OE = o_1 \text{ OR } OE = o_2)$ als Substitutionsalternativen angeboten.

Wie erwähnt, ergeben sich komplexe Bearbeiterregeln durch Verknüpfung (AND, OR, AND NOT) elementarer Bearbeiterzuordnungen (vgl. Abschnitt 3.1). Für ihre Anpassung gibt es vielfältigere Möglichkeiten. Sie nutzen sowohl die Struktur der Bearbeiterregeln als auch die Semantik der durchgeführten Org.-Modelländerung. Wir verzichten wir auf eine formale Darstellung und illustrieren dies anhand einfacher Szenarien.

Sind zwei BZ mittels AND-Ausdruck verknüpft, wird dadurch die Bearbeitermenge gegenüber den Einzel-BZs eingeschränkt. Wird eine Entität aus dem Org.-Modell gelöscht, die von einem dieser beiden BZ referenziert wird, sind die betreffende BZ und damit die Regel nicht mehr auswertbar. Das bloße Entfernen der nicht mehr auflösbaren BZ würde zu einer Vergrößerung der Bearbeitermenge führen. Da dies in der Mehrzahl der Fälle unerwünscht ist, sollte im vorliegenden Szenario die Anpassung der Bearbeiterregel manuell erfolgen. Ein Beispiel: Wird in einem Org.-Modell die Rolle *HNO-Arzt* gelöscht, ist dadurch die Bearbeiterregel $OE = Ambulanz \text{ AND } R = HNO-Arzt$ nicht mehr auflösbar. Würde man den Teilausdruck $R = HNO-Arzt$ automatisch entfernen, ergibt sich $OE = Ambulanz$ als neue Regel. Sie beschreibt eine weitaus größere Bearbeitermenge (alle Mitarbeiter der Ambulanz) als die ursprüngliche Regel, was in der Mehrzahl der Fälle nicht wünschenswert sein dürfte.

Sind zwei BZ mittels OR-Ausdruck verknüpft, wird dadurch die Bearbeitermenge gegenüber den einzelnen BZs vergrößert. Hier ist es prinzipiell möglich (und vielfach auch sinnvoll), die BZ automatisch aus der alten Regel zu entfernen, sofern aus der Auflösung der übrigen Ausdrücke eine nichtleere Bearbeitermenge resultiert. Dem folgend würde z.B. die Bearbeiterregel $S = Arzt-1 \text{ OR } S = Arzt-2$ nach Streichen der Stelle *Arzt-2* aus dem Org.-Modell durch die Bearbeiterregel $S = Arzt-$

I substituiert werden. Auch in Verbindung mit Ausschlussregeln (AND NOT-Verknüpfung) sind solche (semi-)automatischen Adaptionen möglich. Wird z.B. Mitarbeiter *Brandt* aus dem Org.-Modell gelöscht, kann die Bearbeiterregel $OE = \text{Ambulanz AND NOT } MA = \text{Brandt}$ automatisch adaptiert werden, indem der nun überflüssige Ausdruck $AND NOT MA = \text{Brandt}$ entfernt wird. Sowohl vor als auch nach ihrer Adaption liefert die Bearbeiterregel dieselbe Bearbeitermenge.

Die zuletzt genannten Anpassungsstrategien können aufwendige manuelle Anpassungen von Bearbeiterregeln ersparen. Trotzdem müssen Benutzer die Möglichkeit haben, diese Anpassungen auch selbständig durchzuführen, zum Beispiel wenn sie eine Entität durch eine andere "ersetzen" möchten. In diesem Fall wäre es nicht sinnvoll, beim Löschen der "alten" Entität alle entsprechenden Bearbeiterzuordnungen automatisch zu entfernen, um anschließend neue Bearbeiterausdrücke mit der "neuen" Entität anzulegen.

Für den Zeitpunkt der Anpassung von Bearbeiterregeln gibt es unterschiedliche Möglichkeiten. Anpassungen können prinzipiell sofort (*immediate*) oder zeitlich verzögert (*delayed / deferred*) nach der Org.-Modelländerung erfolgen. ADEPT unterstützt beide Varianten, abhängig davon, ob die Bearbeiterregeln zusammen mit dem Org.-Modell oder von separaten Komponenten verwaltet werden. Wir verzichten an dieser Stelle auf weitere Details.

4 Adaption von Arbeitslisten

In diesem Kapitel skizzieren wir kurz das weitergehende Problem der Pflege von Benutzerarbeitslisten in Verbindung mit Org.-Modelländerungen. Eine ausführliche Darstellung findet sich in [Wied02]. Änderungen eines Org.-Modells betreffen nicht nur die statische Definition der Bearbeiterregeln von Aktivitäten, sondern ggf. auch die Aktivitäteninstanzen selbst. Diese werden berechtigten Benutzern, deren Profil der Bearbeiterregel der jeweiligen Aktivität genügt, in deren Arbeitsliste angeboten. Wenn sich zur Laufzeit das Org.-Modell ändert, sind zuvor berechnete Arbeitslisten u.U. nicht mehr aktuell bzw. inkonsistent. So können bestimmte Aktivitäteninstanzen im Anschluss an die Org.-Modelländerung in Arbeitslisten enthalten sein, deren Inhaber aus dem Org.-Modell gelöscht wurde. Schlimmstenfalls ist einer Aktivitäteninstanz kein regulärer Bearbeiter mehr zugeordnet, was zu einer Blockierung oder zumindest zu einer Verzögerung des betreffenden Workflow führt. Umgekehrt spiegeln für Mitarbeiter mit modifizierter Stellen- oder Rollenzuordnungen die bisherigen Arbeitslisten möglicherweise nicht mehr die aktuellen Berechtigungen wider. Für diese Bearbeiter ist eine Invalidation der bisherigen Arbeitsliste (verbunden mit ihrer Neuberechnung) zwingend erforderlich. Diese Notwendigkeit ergibt sich auch nach der Änderung von Bearbeiterregeln in einem Prozess-Schema sowie deren Propagation auf laufende Prozessinstanzen.

Eine begleitende Anpassung von Arbeitslisten muss i.A. sowohl server- als auch clientseitig bewerkstelligt werden; bei naiver Realisierung (z.B. Invalidation, Neuberechnung und wiederholte Übertragung von Arbeitslisten für alle angemeldeten Clients) kann sich dabei ein hoher Rechen- und

Kommunikationsaufwand ergeben. Deshalb sollte genau geprüft werden, unter welchen Bedingungen und bis wann entsprechende Adaptionen vorzunehmen sind.

Die Arbeitslistenverwaltungskomponente von ADEPT berücksichtigt derartige Aspekte. Insbesondere wird bei Org.-Modelländerungen analysiert, für welche Benutzerarbeitslisten und für welche Aktivitäteninstanzen begleitende Anpassungen notwendig werden. Eine Invalidation und Neubestimmung der bisherigen Arbeitsliste eines Benutzers erfolgt nur dann sofort, wenn dieser aktuell angemeldet ist und wenn infolge der Org.-Modelländerung einzelne Arbeitslisteneinträge hinzukommen oder wegfallen. Um Letzteres festzustellen, nutzt ADEPT die Semantik der angewandten Änderungsoperationen, den Änderungskontext und die (aktualisierten) Bearbeiterregeln von Aktivitäteninstanzen. Letztere entsprechen im wesentlichen den Bearbeiterregeln der zugehörigen Aktivitätsdefinitionen, allerdings sind diese noch um evtl. Abhängigkeiten zu vorangehenden Aktivitäten bereinigt. Wir verzichten an dieser Stelle aus Platzgründen auf weitere Details.

Abschließend sei erwähnt, dass auf Grundlage derselben Mechanismen auch Änderungen der Bearbeiterregeln von Prozessaktivitäten (auf Prozessdefinitions- bzw. Prozessschemaebene) an bereits laufende Prozessinstanzen (und abhängige Datenstrukturen wie Arbeitslisten) propagiert werden. Insgesamt erreichen wir gegenüber bisherigen Ansätzen einen weitaus höheren Grad an Adaptivität bzgl. Zugriffs- und Bearbeiterregeln. Derzeit arbeiten wir an effizienten Implementierungen der Arbeitslistenverwaltungskomponente sowie an Konzepten zur effizienten Adaption von Arbeitslisten in großen Umgebungen. All diese Arbeiten bilden eine wichtige Ergänzung der von uns entwickelten Konzepte für die Evolution von Prozess-Schemata und die dynamische Adaption von Prozessinstanzen [RiRD04, ReDa98].

5 Zusammenfassung

Prozess-Management-Systeme unterstützen die Modellierung, Analyse und Steuerung von Geschäftsprozessen. Um ein möglichst breites Spektrum an Prozessen abbilden zu können, ist es notwendig, prozessorientierte Anwendungen flexibel zu gestalten. Dabei stand bisher die flexible Steuerung von Prozessen im Mittelpunkt unserer Arbeiten. Wenig Beachtung haben wir dagegen Änderungen der Aufbauorganisationen und den dadurch notwendig werdenden Anpassungen von Org.-Modellen sowie von Zugriffs- und Bearbeiterregeln geschenkt. In diesem Beitrag haben wir erstmals entsprechende Konzepte vorgestellt. Die Grundlage bildet ein mächtiges Org.-Metamodell, das es wegen seiner umfangreichen Entitäts- und Relationstypen erlaubt, Organisationen präzise und semantisch korrekt abzubilden. Anhand einfacher Änderungsszenarien haben wir gezeigt, welche Operationen erforderlich sind, um Modelländerungen adäquat abzubilden. Da zwischen Org.-Modell und anderen Komponenten eines Informationssystems zahlreiche Querbezüge bestehen, muss beachtet werden, dass diese Referenzen bei unkontrollierten Änderungen des Org.-Modells verwaist bzw. nicht mehr aktuell sein können. Insbesondere könnte die Zuordnung von aktivierten Workflow-Aktivitäten zu Bearbeitern von solchen Änderungen betroffen sein. In der Folge werden Aktivitäten möglicherweise falsch oder gar nicht mehr zugewiesen, wodurch Sicherheitsbestimmungen verletzt werden oder - noch schlimmer - der gesamte Workflow ins Stocken geraten kann.

Zur Behandlung dieser Probleme haben wir Lösungsansätze entwickelt, die - je nach Semantik der Änderung - eine automatische, semiautomatische oder manuelle Anpassung evtl. "veralteter" Bearbeiterregeln gestatten. Außerdem haben wir Überlegungen dazu angestellt, welche Bearbeiterregeln überhaupt angepasst werden müssen. Die Betrachtungen zur Adaption von Benutzerarbeitslisten und Bearbeiterregeln auf Instanzebene runden diese Arbeiten ab.

Literatur

- [BeFA99] E. Bertino, E. Ferrari, V. Atluri: The Specification and Enforcement of Authorization Constraints in Workflow Management Systems. *ACM Transactions on Information and System Security*, 2(1):65-104, 1999
- [FeBK99] D.F. Ferraiolo, J.F. Barkley, D.R. Kuhn: A Role-based Access Control Model and Reference Implementation Within a Corporate Intranet. *ACM Transactions on Information and System Security*, 2(1):34-64, 1999
- [HoSG01] T.A. Howes, M. Smith, G.S. Good: Understanding and Deploying LDAP Directory Services. New Riders, 2001
- [Klar01] J. Klarmann: A Comprehensive Support for Changes in Organizational Models of Workflow Management Sys.. Proc. 4th Int'l Conf. Inf. Sys. Mod., 2001, S. 165-172.
- [LeRo00] F. Leymann, D. Roller: Production Workflow: Concepts and Techniques. Prentice Hall, 2000
- [MoSu02] M. Momotko, K. Subieta: Dynamic Change in Workflow Participant Assignment. Proc. 6th East-European Conf. on Advances in Databases and Information Systems (ADBIS'02), Bratislava, September 2002
- [ReDa98] M. Reichert, P. Dadam: ADEPT_{flex} - Supporting Dynamic Changes of Workflows Without Losing Control. *JGIS*, 10(2):93-129, 1998
- [ReRi02] M. Reichert, S. Rinderle: Änderungsrechte in adaptiven Workflow-Management-Systemen. Proc. Konferenz Sichere Geschäftsprozesse, St. Leon-Rot, Sept. 2002, S. 30-42
- [RiRD04] S. Rinderle, M. Reichert, P. Dadam: Flexible Support of Team Processes By Adaptive Workflow Systems. *Distributed and Parallel Databases*, Kluwer, 16(1):91-116, 2004
- [SaAl03] R. Sandhu, M.A. Al-Kahtani: Induced Role Hierarchies with Attribut-based RBAC, Proc. Symp. on Access Control Models and Technologies, Juni 2003, S. 142-148
- [SCFY96] R. Sanhu, E.J. Coyne, H.L. Feinstein, C.E. Youman: Role-based Access Control Models. *IEEE Computer*, 29(2), 1996
- [Wied02] U. Wiedermuth-Catrinescu: Evolution von Organisationsmodellen in Workflow-Management-Systemen. Diplomarbeit, Universität Ulm, 2002
- [WSML02] S. Wu, A. Sheth, J. Miller, Z. Luo: Authorization and Access Control of Application Data in Workflow Systems. *JGIS*, 18(1):71-94, 2002