

Kritik am Stand der Technik

Viele am Markt angepriesene Rollenmodelle repräsentieren einen statischen Ansatz, der recht schnell an die Grenzen eines realistischen Einsatzes stößt. Solche Grenzen sind:

- eine ausufernde Anzahl von Rollen
- keine Trennung zwischen Fach- und Systemrollen: dies erschwert die Modellierung von Prozessen
- keine Möglichkeit der Berücksichtigung dynamischer Strukturen (Team- oder Projektorganisation)
- kein oder nur ein rudimentäres Regelwerk zur Steuerung der Prozesse
- keine geordnete Koexistenz zwischen rollenbasierter und direkter Zuordnung von Berechtigungen
- kein mehrdimensionales Rechte- Management

Wie kann ein fachlicher Ansatz zur Auflösung dieser Konflikte in der Realität aussehen?

Rollen- und Prozessmodell als einheitliches Konzept

Das iSM ist im Rahmen seiner Projektarbeit (ca. 10 Jahre) genau auf diese Problembereiche gestoßen und hat entsprechende Verfahren entwickelt, um hier eine deutlich höhere Qualität der Rollenmodellierung zu erreichen.

Im Laufe der Zeit wurden hierfür folgende Methoden entwickelt und exemplarisch auch in einem System (**bi-Cube**[®]) umgesetzt, um die Praktikabilität der jeweiligen Lösung zu prüfen:

- Integration von Rollenmodell und Prozesssteuerung
- Adaptives Rollenmodell
- Definitive Regeln und Inferenzmaschine
- Generische Prozessmodelle
- Security Classification
- Referenzierte Rollen

In einem deutlich iterativen Prozess (Verfahrensentwicklung <=> Validierung im realen Einsatz) mussten die jeweiligen Lösungen jedoch ständig verfeinert und verbessert werden. Dies führt auch zu dem Postulat, dass das logische Modell einer IPM - Lösung nur in Zusammenarbeit mit Entwicklern, Systemarchitekten und fachlichen Projekt-Managern zu einem leistungsfähigen System entwickelt werden kann.

Integration von Rollen-Modell und Prozesssteuerung

An der Rolle müssen bereits Prozess - Controls (PX-Controls) definiert werden, um die sachlich gegebenen Zusammenhänge im Modell hinreichend darstellen zu können. Hierzu gehören folgende Controls:

- Zuweisungsart (automatisch oder mit Freigabe)
- Antragsart (jeder User, nur sein Leiter, ...)
- Freigabeverfahren (mehrstufig, Vier-Augen-Prinzip, zufällige Weiterleitung)
- Min - Max Control
- Kritikalität (geschäftskritisch oder nicht)
- Security Classification

Alle diese so genannten PX-Controls an der Rolle beeinflussen maßgeblich den **bi-Cube**[®] Process Manager. Zusätzlich ist der Prozess der Änderung der Rolle sinnvoll zu steuern. Hier sind evtl. Einschränkungen auf den Owner und zusätzliche Sicherungen durch den Passwortschutz der Rolle vorzusehen.

Rollen- und Prozessmanager auf der Basis eines logischen Regelwerks



Adaptives Rollenmodell

Ein logisch separater Entwurf des Rollenmodells ohne Berücksichtigung der Prozesssteuerung führt zu einem statischen Modell und damit zu einer Explosion der Anzahl der Rollen, wenn trotzdem versucht wird, die Vielfalt der Realität zu berücksichtigen.

In dem System *bi-Cube*[®] wurde deshalb eine Differenzierung der System-Attribute in Berechtigungs- und technische Attribute vorgesehen. Die Berechtigungsattribute eines Zielsystems in der Rolle sind zwangsweise festzulegen. Evtl. spezifische aber erforderliche Ausprägungen (Datenbestand, Server, besondere Skills des Users, ...) von Systemattributen sind deshalb als technische Attribute klassifiziert und müssen während der Vergabe (Antragsverfahren) durch die jeweiligen Owner beigebracht werden. Dieser Freigabeprozess kann auch mehrstufig sein (Daten-Owner, Lizenz-Verwaltung, Kostenverantwortlicher, System-Techniker, ...), wobei jeder Akteur zugeordnete Attribute beibringen muss. Auf diesem Wege wird das Rollenmodell maßgeblich entlastet und die Rollen auf eine überschaubare Zahl gebracht.

Trennung von Fach- und System-Rollen

Fach-Rollen beschreiben ausschließlich die Aufgabe des Rolleninhabers. Wogegen die System-Rollen die Zuordnungen der Berechtigungen zu einer Rolle festlegen. Diese Trennung hat sich aus folgenden Gründen als unverzichtbar erwiesen:

1. Die Systemrollen enthalten die konkreten Systemberechtigungen und werden zentral definiert
2. Die Fachrollen werden in den Fachbereichen definiert und auch zugeordnet

Somit wird das Ziel der zentralen Modellierung und der dezentralen Administration ganz eindeutig gesichert. Gegenstand des Prozessmanagements sind ausschließlich die Fachrollen.

Segregation of duties

Die sichere Trennung von unzulässigen Kompetenzen erfolgt ebenfalls am einfachsten auf der Ebene der Fachrollen.

Team- und Projektorganisation

Formal ist ein projektbezogenes Rollenmodell wenigstens 2-dimensional (funktionelle Rechte, Datensichten). Mit einem statischen Rollenmodell würde diese $m \times n$ Matrix zu einem ebenfalls $m \times n$ Rollenmodell führen, was letztlich zu einer nicht mehr beherrschbaren und vor allem unsinnigen Zahl von Rollen führen würde.

Wenn auf dieses Problem das adaptive Rollenmodell angewendet wird, reduziert sich die Anzahl der Rollen auf die Zahl der funktionellen Rechtekombinationen (Projektleiter, -mitarbeiter, Controller, Konstrukteur, ...). Die jeweiligen Sichten auf die Projektdaten (Projekt-Dokumente, - Laufwerk, - Mailgruppe, ...) werden während der Rollenzuordnung im Prozess beigebracht. Ganz nebenbei lässt sich hier auch die Frage der *segregation of duties* lösen, indem nur zulässige Kombinationen von Datenbereichen (verschiedene Projektunterlagen) zur Auswahl angeboten werden.

Referenzierte Rollen

Eine weitere Möglichkeit zur Verschlankung des Rollenmodells sind die Objektreferenzen, die sich auf Rollen- und Systemebene definieren lassen.

Objektreferenzen werden als so genannte *vorgelagerte shared resources* (VSR) definiert. Dies sind Programme, die als Voraussetzung für andere Programme notwendig sind (z.B. CICS- oder DB-Client). Diese werden als VSR bereits auf Systemebene an die jeweilige Anwendung gebunden, womit sie im Rollenmodell nicht mehr zu berücksichtigen sind.

Analog lassen sich Basis-Rollen definieren, die über Objekt-Referenzen mehrfach an Fachrollen gebunden werden können und in den eigentlichen Fachrollen somit nicht mehr definiert werden müssen. Ganz nebenbei werden damit Änderungen an den Basisrollen deutlich einfacher und sicherer.

Rollen- und Prozessmanager auf der Basis eines logischen Regelwerks



Generische Prozessmodelle (GPM)

Für diverse Prozesse im Provisioning lassen sich Templates definieren, die dieses Teilprojekt in Aufwand und Zeitdauer um 70 bis 80% reduzieren. Diese Templates sind in allen Parametern getestet und können umgehend produktiv gesetzt werden.

In dem GPM - Projekt des iSM wurde ein Standard-Set von GPM definiert und explizit beschrieben. In **bi-Cube**[®] wurden und werden sie schrittweise realisiert. Schrittweise deshalb, da diese Palette ständig durch neue Anregungen aus den Projekten erweitert wird.

In der Zusammenfassung wurden bisher folgende Prozesse aus Anwendersicht ermittelt:

1. Antrag für Rollenzuteilung
2. Automatische Berechtigungsvergabe für neue Mitarbeiter (Mitarbeiter-Eintritt)
3. Richtlinien-Bestätigung und Richtlinien-Verwaltung (separat und integriert in den Antragsprozess)
4. Automatisches Mitarbeiteraustrittsverfahren
5. Sofortiges Usersperren
6. Berücksichtigung gleitender Übergänge / Wechselprozesse
7. Wiedereintritt in Konzernstrukturen
8. Allgemeiner dokumentenbasierter Antrags-Prozess
9. Antrag auf Einzelberechtigungen (mit Strukturierung der Rechte)
10. Re-Lizenzierung (regelmäßige Bestätigung einer bereits erteilten Lizenz)
11. Re-Zertifizierung (regelmäßige Bestätigung eines bereits erteilten Nutzungsrechts)
12. Re-Validierung (regelmäßige Bestätigung der Existenz eines Users)

Service Prozesse

- Antrag auf Arbeitsplatz für einen Mitarbeiter inkl. Ausstattungsvarianten
- Abwesenheits- / Urlaubsverwaltung (Zur Steuerung des Task-Managers)
- Antrag auf Zutrittsberechtigung
- Passwort Self-Service
- Supportanfrage an NBV (Nutzer- u Berechtigungsverwaltung)

Aus diesen Beispielen wurde folgende Klassifikation der IPM - Prozesse abgeleitet, in die sich alle anderen einordnen.

Prozess-Gruppen

- Wechselprozesse des Users
- Antragsverfahren
- Wiederholungsfreigaben
- Serviceprozesse
- Interne Prozesse

Definitorische Regeln und Prädikatenlogik

Die Integration von Rollen und Prozessen erfordert eine leistungsfähige Regelverarbeitung. In den IPM - Produkten findet sich ausschließlich (zumindest nach Kenntnis des Autors) ein Komplex von definitorischen Regeln, die zu den Objekten, Attributen und den einfachen Beziehungen zwischen diesen, direkt in der GUI definiert werden.

In den Bildern unten finden sich zwei Beispiele dieses Regeltyps aus dem System **bi-Cube**[®]. Eine etwas komplexere Regeldefinition mit einer rudimentären booleschen Logik findet sich bereits in der (User-) Attribut - Referenzierung von Rollen (Bild 2). Hierdurch wird die Gesamtheit der definierten Rollen sachlich derart eingeschränkt, dass nur wirklich zutreffende bzw. sinnvolle Kompetenzen über Rollen zuzuordnen sind. Es macht wenig Sinn, jedem User alle Rollen vom Vorstand bis zum Hausmeister anbieten zu wollen.

Rollen- und Prozessmanager auf der Basis eines logischen Regelwerks



Eine weitere Möglichkeit besteht darin, Konsequenzen zu definieren, die auf das interne Message - Protokoll von **bi-Cube®** aufsetzen. Hier wird jede Message geprüft, ob es dafür eine Regel (Konsequenz) gibt. Hierbei sind vier Kombinationen möglich:

Wenn Attribut 4711	Wert xy hat	Dann Attribut 3332	Setze Wert auf abc
Wenn Attribut 4711	Wert xy hat	Dann starte	Operation 1234
Wenn Operation	xyz	Dann starte auch	Operation 1234
Wenn Operation	xyz	Dann Attribut 3332	Setze Wert auf abc

Rolle
Praktikant

Referenz zwischen Praktikant und Externer MA
als unzulässige Referenz

Hinweis:
Die Rolle darf wegen Unverträglichkeit der auf der rechten Seite angegebenen Rolle nicht zugeordnet sein.

Rollen
Externer MA

Externer MA

FLAGLISTE
Flagliste

1. Flag

- Rolle ist genehmigungspflichtig
- Rolle ist nicht genehmigungspflichtig

2. Flag

- Rolle kann vom Leiter und vom User beantragt werden
- Rolle kann nur vom Leiter beantragt werden (Fremdantr)
- Rolle kann nur vom User beantragt werden (Eigenantr)
- Rolle kann automatisch beantragt werden

Oben: Regeln zur Steuerung des Antragsprozesses
Rechts: Segregation of duties

- Secu-Sys Basis
- Consulter
- Secu-Sys Filespace
- FP-Secu-Sys Slowakia
- FP-Secu-Sys Slowakia S
- Secu-Sys Basis
- Secu-Sys Basis S
- FP-Secu-Sys Slowakia

Eigenschaften Berechtigungen User User mit Objekt-Restriktionen Referenzierung Te

Sonstiges

Status der Referenz
✓ verfügbar

Stammattribut	Operator	Wert	Inhalt
Organisations-ID	OR	60000153	SS-S / Produktion
Organisations-ID	OR	60000152	SS-S / Vertrieb

Mit der weiteren Qualifizierung der Prozesse wurden komplexere Regeln erforderlich, die sich nicht mehr mit den vorhandenen separaten definitorischen Regeln steuern ließen. Z.B. stellt sich der Mitarbeiter-Eintritt für externe User komplett anders dar als bei einem internen. Weitere Bedingungen (z.B. Mandantenabhängigkeiten) erhöhten die Komplexität des Prozesses zusätzlich.

Der einfache Weg wäre gewesen, für diese Spezialfälle einzelne abgewandelte Prozessmodelle zu erstellen. Dies hätte das Problem jedoch nicht gelöst, sondern nur die Grenze der Modellierungen etwas weiter verschoben. Deshalb wurde eine Regelmaschine zur Verarbeitung einer Prädikatenlogik entwickelt und integriert. Diese Komponenten (**bi-Cube®** - Logi) verarbeitet einfache, komplexe und auch rekursive Prolog-Notationen. Die gewählte Syntax ist nahezu natürlich sprachlich entworfen worden.

Rollen- und Prozessmanager auf der Basis eines logischen Regelwerks



Damit können alle vorkommenden logischen Kombinationen zur Prozesssteuerung in entsprechenden Regeln abgefangen und nach einer gewissen Übung auch vom Anwender definiert werden.

Koexistenz von Rollen- und Systemberechtigungen

Es ist ein zu akzeptierender Fakt, dass das Erreichen einer komplett rollenbasierten Berechtigungsvergabe ein evolutionärer Prozess ist, der früher oder später oder auch nie erreicht wird. Deshalb muss es auch für die Koexistenz zwischen direkter und rollenbasierter Berechtigungsvergabe eine Regel geben, wenn beide Verfahren aufeinander treffen. Dies ist dann der Fall, wenn eine bestehende direkte Systemberechtigung (evtl. durch die Migration) mit einer rollenbasierten zusammentrifft. Dann gilt die allgemeine Regel, dass die rollenbasierte Berechtigung die bestehende direkte komplett überschreibt und u. U. damit auch Rechte entzieht.

Rollenkonflikte

An dieser Stelle werden Rollenkonflikte als das Zusammentreffen von unterschiedlichen Berechtigungsprofilen eines Systems aus zwei (oder mehreren) Rollen verstanden. Auch für diesen Fall muss es je System eine Regel zur automatischen Auflösung des Konfliktes geben. Die beiden typischen Regeln sind dann:

- Vereinigung beider Profile auf einem Account
- Anlegen eines weiteren Accounts mit dem abweichenden Profil
-

Diese Regel muss auch bei mehrfachem Auftreten eines solchen Konfliktes und vor allem beim Entzug einer Rolle sauber verarbeitet werden.

Security Classification

Es hatte sich als sinnvoll erwiesen, dass alle Objekte und Attribute mit einer Security Classification (SC) versehen werden können. Diese SC wird als eine weitere Reledgedimension innerhalb des IPM-Regelwerks angesehen.

Dieser Regelapparat kann zur Vorselektion von Zuordnungen genutzt werden. Z.B. muss ein User wenigstens die gleiche (oder eine höhere) Security Class haben, wie die gewünschte Rolle. Außerdem können bestimmte Aktionen von der SC der Rolle oder des Users abhängig gemacht werden. Z.B. wird ab einer definierten SC-Stufe eine weitere Freigabe oder eine Information an bestimmte Personen (z.B. Security - Team) generiert werden. Außerdem ist die SC ein wichtiges Kriterium innerhalb des Internen Kontroll-Systems (IKS).

Zusammenfassung

In diesem Manuskript wurden diverse Steuermöglichkeiten innerhalb des Rollen- und Prozess-Managers dargestellt, die alle zu einer besseren Modellierbarkeit der realen Anforderungen beitragen. Je nach der Leistungsfähigkeit des Regelwerks ist ein Produkt in der Lage, ein hohes IPM-Prozessniveau zu erreichen.

Generelle Erkenntnis aller Arbeiten war:

Rollenmodell und Process Manager müssen eine enge Integration miteinander realisieren, wozu ein leistungsfähiges Regelsystem unabdingbar ist.