

# Modellierung von IT-Sicherheit

## Analyse und Synthese

Galina Dzhendova · Dirk Kalmring

Fraunhofer-Institut für Sichere Informationstechnologie (SIT)  
{dzhendova | kalmring}@sit.fraunhofer.de

### Zusammenfassung

Der Artikel liefert einen Überblick (State of the Art) der Modelle und Methoden zur Modellierung von Geschäftsprozessen und Workflows. Er wählt für die Modellierung relevante Sicherheitsanforderungen aus und prüft die genannten Modelle und Methoden daraufhin, ob sie eine Abbildung der Anforderungen erlauben. Der Beitrag nimmt eine Bewertung der Modelle und Methoden vor. Es wird eine Auswahl hinsichtlich Modellierungsmethode und Vorgehensmodell getroffen. Das Metamodell der ausgewählten Methoden wird um Konstrukte zur Abbildung von Sicherheitsanforderungen ergänzt. Konkrete Beispiele für die Anwendung der erweiterten Methoden in der Modellierungspraxis werden erläutert.

## 1 Prozessmodellierung – Aspekte der IT-Sicherheit

Die Ergebnisse der Geschäftsprozessmodellierung im Rahmen eines Fachkonzeptes liefern die wesentlichen Anforderungen und Rahmenbedingungen für Softwareentwicklungsprojekte. Diese Abfolge aus Fachkonzept, DV-Konzept und schließlich Implementierung ist heute allgemein anerkannt und bildet die Grundlage beispielsweise für die Einführung großer Standard-Software-Pakete (vgl. z.B. [Sche97]). Aus diesem Grund erfreut sich die Geschäftsprozessmodellierung seit über zehn Jahren intensiver Aufmerksamkeit in der Praxis und der Theorie der Wirtschaftsinformatik [Ulri01].

Die Abbildung relevanter Ausschnitte der Realwelt in ein Modell mittels Ist-Aufnahme und Soll-Konzept ermöglicht die Vereinfachung von Systemen, das Überwinden von Komplexitätsgrenzen und ein einfacheres und besseres Verständnis des Ablaufs von Geschäftsprozessen (vgl. z.B. [Rose95]). Aus diesem Grund ist es notwendig, sich auf ein Metamodell zu einigen, welches die Modellierungsmethode bzw. ihren Gebrauch spezifiziert. Prozessmodelle dienen der Dokumentation, Analyse, Simulation und Gestaltung von Systemen sowie der Unterstützung der Kommunikation zwischen den Akteuren in diesen Systemen.

Mittels eines solchen Modells kann z.B. ersichtlich werden, welche Arbeitsschritte von einem Mitarbeiter mit welcher Qualifikation und welcher Funktion in welcher Reihenfolge unter Einsatz welcher Anwendungsprogramme auf der Basis welcher Daten und aus welchem Beweggrund heraus, auszuführen sind. Zur Reduktion dieser offensichtlichen Komplexität bedienen sich zahlreiche Methoden sichtenorientierter Ansätze:

- Funktionssicht: Was soll ausgeführt werden?

- Steuerungssicht: Wann und in welcher Abfolge geschieht die Ausführung der Arbeitsschritte?
- Arbeitsmittelsicht: Welche Werkzeuge und Betriebsmittel sind notwendig oder stehen bei der Ausführung zur Verfügung?
- Datensicht: Welche Daten werden benötigt und wie sind sie in das Datenmodell einzuordnen?
- Organisationssicht: Welche Rollen bzw. Organisationseinheiten sind an der Ausführung beteiligt und wie sind sie in das Organigramm einzuordnen?
- Normensicht: Welche organisatorischen Vorschriften sind zu beachten? [LeOr98]

Die Methodenauswahl hängt von der modellierungstechnischen Mächtigkeit des Metamodells und der spezifischen Anforderung an die Prozessmodellierung ab. Die Sicherung elektronischer Geschäftsprozesse erst im DV-Konzept zu berücksichtigen, ist offensichtlich unzureichend, da betriebswirtschaftliche, aufbau- und ablauforganisatorische sowie rechtliche Aspekte einzubeziehen sind. Die Berücksichtigung einer „*Sicherheitssicht*“ in der Prozessmodellierung findet in Theorie und Praxis bislang nicht oder nur unzureichend statt. Es bedarf daher der Entwicklung eines Vorgehensmodells sowie einer Modellierungsmethode, die alle relevanten Sicherheitsanforderungen eines Geschäftsfeldes berücksichtigt.

## 2 Beitrag zum wissenschaftlichen Diskurs

Methoden und Techniken in den Bereichen Management und Technologie für Datenschutz und Datensicherheit werden seit langem und in der gebotenen Tiefe bzw. Breite diskutiert (s. z.B. [Ecke04]). Die Einsatzmöglichkeiten und die Verwendung von Modellierungsmethoden auf Fachkonzeptebene für die Beschreibung der Sicherheit von Geschäftsprozessen unter Berücksichtigung ganzheitlicher und ggf. unternehmungssübergreifender Sicherheitsanforderungen sind dagegen weitgehend unerforscht. Die Berücksichtigung von Sicherheitsaspekten in (elektronischen) Geschäftsprozessen ist vor allem deshalb nicht trivial, da Sicherheitsanforderungen stark kontextabhängig sind. Erste Ansätze liefern [Thob98, HeRö99, HePe00, Röhr03, BHW+04, PrHo04] und [KoSc04]. Während etablierte Modellierungsmethoden den Aspekt Sicherheit nicht bzw. nicht explizit berücksichtigen, beschränken sich neuere Ansätze häufig auf einzelne Anforderungen, z.B. die rollenbasierte Zugriffskontrolle, oder bewegen sich in großer Nähe (Abhängigkeit) des DV-Konzepts. Diese Verfahren konzentrieren sich auf die Spezifikation von Anforderungen an die Anwendungssysteme, nicht an den Geschäftsprozess. Werden aber lediglich funktionale Aspekte modelliert, die für die Entwicklung von sicherer Software erforderlich sind, bleiben das Zusammenwirken von Mensch und Technik sowie die betriebswirtschaftlichen Rahmenbedingungen häufig unberücksichtigt. Hinzu kommt, dass viele Vorgehensmodelle ein existierendes Fachkonzept bereits voraussetzen, keine grafische Modellierung unterstützen oder mit UML eine objektorientierte Modellierungsmethode verwenden, die den Fachabteilungen in der Regel nicht bzw. kaum vermittelbar ist. Die Praxis zeigt, dass beispielsweise aktivitätsorientierte Methoden von den Mitarbeitern der Fachebene wesentlich besser verstanden werden.

Ziel dieser Arbeit ist es daher, bestehende Modellierungsmethoden und -modelle auf Fachkonzeptebene im Hinblick auf die Berücksichtigung des Aspektes Sicherheit zu analysieren. Im Rahmen einer Synthese wird darüber hinaus eine konkrete Empfehlung zur grafischen Modellierung von Sicherheit in Geschäftsprozessen gegeben.

## 3 Geschäftsprozess- und Workflowmodellierung

### 3.1 Typisierung von Modellen und Methoden

Zur Komplexitätsreduktion bei der Analyse der zahlreichen in der Literatur beschriebenen Modelle und Methoden verwenden wir die folgende Typisierung:

Ein *Modell* ist ein vereinfachtes und abstraktes Abbild der Realität. Die Erstellung solcher Modelle erfordert den Einsatz geeigneter *Methoden*, die die konsequente, systematische und nachvollziehbare Verfahrensweise garantieren.

Während *Geschäftsprozessmodelle* die konzeptionelle Ebene, also im Wesentlichen die abstrakte sachlogische Abfolge von Aktivitäten, betrachten, operationalisieren *Workflowmodelle* den Geschäftsprozess durch die Zuordnung von konkreten Tätigkeiten zu spezifischen Akteuren der Organisation (s. z.B. [LeSi97]).

*Architekturmodelle* beschreiben eine Organisation durch die Bildung fachlicher und technischer Schichten sowie die Modellierung derer Komponenten. *Sicherheitsmodelle* fokussieren die Spezifikation von Sicherheitsanforderungen an Organisation und Software. Beide Modellklassen können mit *Vorgehensmodellen* kombiniert werden, die die strukturierte Umsetzung des Modells in die Praxis beschreiben.

Bzgl. der Methoden zur Geschäftsprozessmodellierung lassen sich sprechakt-, aktivitäts- und objektorientierte Ansätze unterscheiden. Während der *sprechaktororientierte Ansatz* die Kommunikation zwischen Akteuren fokussiert, betont der *aktivitätsorientierte Ansatz* die Beschreibung von Vorgängen und Ereignissen sowie deren Anordnung im Prozess. Der *objektorientierte Ansatz* unterstützt vor allem die Softwareentwicklung durch das Konzept der Wiederverwendung.

**Tab. 1:** Modelle und Methoden zur Geschäftsprozess- und Workflowmodellierung










Modellierungsmodelle und Modellierungsmethoden		Quelle
sprechaktororientierte Prozessmodellierung	Sprechakt Methode	[MWFF92]
aktivitätsorientierte Prozessmodellierung	Petri-Netze	[Petr62]
	FUNSOFT-Netze	[EmGr91]
	Zielbasierter Ansatz	[KüBS95]
	Process Landscaping	[GrWe00]
	EPK	[KeNS92]
	PROMET	[BBB+97]
objektorientierte Prozessmodellierung	Statecharts	[WoWe97]
	Safecharts	[DaNi03]
	UML	[Omg05]
	EPE	[ErPe00]
	SecureUML	[LoBD02]
	oEPK	[ScNZ97]
	EMK	[Ritt99]
Architekturmodelle	ARIS	[Sche97]

Modellierungsmodelle und Modellierungsmethoden	Quelle	
	SOM	[FeSi95]
	ISA Kreisel	[Krcm90]
Methoden zur Workflowmodellierung	Trigger	[Joos94]
	MOBILE	[BuJa96]
	INCOME	[Jaes96]
	FlowMark	[RolI96]
	WorkParty	[Hans96]
	WIDE	[CGP+96]
	SecureFlow	[HuAt99]
Sicherheitsmodelle	MoSS	[HePe00]
	DROPS	[PrHo04]
	SECTINO	[BHW+04]
	PoSeM	[Röhr03]

### 3.2 Zu berücksichtigende Sicherheitsanforderungen

In der Literatur finden sich verschiedene Klassifikationen von Sicherheitsanforderungen sowie zugehörige Sicherheitsmaßnahmen (z.B. [HePe00, Ecke04]). Wie in Abschnitt 2 dargestellt, sind bei der Modellierung auf Fachkonzeptebene insbesondere das Zusammenwirken von Mensch und Technik sowie betriebswirtschaftliche und rechtliche Rahmenbedingungen zu berücksichtigen. Wir wählen daher folgende Sicherheitsanforderungen als für die Prozessmodellierung relevant aus und weisen Ihnen grafische Symbole zu.

**Tab. 2:** Auf Fachkonzeptebene abzubildende Sicherheitsanforderungen

Sicherheitsanforderungen	Symbol	Sicherheitsmaßnahmen und Techniken (Beispiele)
Verfügbarkeit		diversitäre Netze mit geringstmöglicher Entwurfskomplexität, Reglementierung der Systemnutzung
Urheberrecht		Kopierschutz, digitale Wasserzeichen, Digital Rights Management
Originalität		Authentisierungsverfahren, biometrische Verfahren, Digital Rights Management
Vertraulichkeit		kryptographische Verfahren/Verschlüsselung
Integrität		kryptografisch sichere Hashfunktionen
Authentizität/Identitätsprüfung		biometrische Verfahren, elektronische Signaturen
Autorisierung/Zugriffskontrolle		Authentisierungsverfahren, Rechtevergabe und -kontrolle, Firewalls
Verbindlichkeit		elektronische Signaturen; Protokollierung
Anonymität		Datenvermeidungs- und Verschleierungstechniken, Verschlüsselung
Pseudoanonymität		
Unbeobachtbarkeit		

Da Sicherheitsanforderungen auf Fachkonzeptebene stark kontextabhängig sind, sind sie nicht in jedem Anwendungsfall klar voneinander abzugrenzen. Beispielsweise kann die Aufrechterhaltung einer Sicherheitsanforderung die Gewährleistung einer anderen Anforderung beeinflussen. In Abbildung 1 betrifft dies die Datenintegrität und die Autorisierung von Benutzern.

### 3.3 Ergebnisse der Analyse

Die folgende Tabelle beantwortet die Frage, ob die in Abschnitt 3.1 genannten Modelle und Methoden eine Abbildung der in Abschnitt 3.2 aufgeführten Anforderungen erlauben.

**Tab. 3:** Analyse von Modellen und Methoden bzgl. der Abbildbarkeit von Sicherheitsanforderungen

Modellierungsmodelle und Methoden		Sicherheitsanforderungen										
		Verfügbarkeit	Urheberrecht	Originalität	Vertraulichkeit	Integrität	Authentizität/ Identitätsprüfung	Autorisierung/ Zugriffskontrolle	Verbindlichkeit	Anonymität	Pseudonymität	Unbeobachtbarkeit
sprechakt-orientiert	Sprechakt Methode	-	-	-	-	-	(x)	(x)	-	-	-	(x)
aktivitäts-orientiert	Petri-Netze	-	-	-	-	-	(x)	(x)	-	-	-	-
	FUNSOFT-Netze	(x)	-	-	-	-	(x)	(x)	-	-	-	-
	Zielbasierter Ansatz	(*)	(*)	(*)	(*)	(*)	(*)	(*)	(*)	(*)	(*)	(*)
	Process Landscaping	(*)	(*)	(*)	(*)	(*)	(*)	(*)	(*)	(*)	(*)	(*)
	EPK	(x)	(x)	(x)	(x)	(x)	(x)	(x)	(x)	(x)	(x)	(x)
	PROMET	(*)	(*)	(*)	(*)	(*)	(*)	(*)	(*)	(*)	(*)	
objekt-orientiert	Statecharts	-	-	-	-	-	-	-	-	-	-	-
	Safecharts	-	-	-	-	-	-	-	-	-	-	-
	UML	-	-	-	-	-	-	-	-	-	-	-
	SecureUML	x	-	-	x	x	x	x	-	-	-	-
	EPE	-	-	-	-	-	-	-	-	-	-	-
	oEPK und EMK	(x)	(x)	(x)	(x)	(x)	(x)	(x)	(x)	(x)	(x)	
Architekturmodelle	ARIS	(x)	(x)	(x)	(x)	(x)	(x)	(x)	(x)	(x)	(x)	(x)
	SOM	-	-	-	-	-	-	-	(x)	-	-	(x)
	ISA Kreisel	-	-	-	-	-	-	-	-	-	-	-
Methoden zur Workflowmodellierung	Trigger Modellierung	-	-	-	-	-	(x)	(x)	-	-	-	-
	MOBILE	(x)	(x)	(x)	(x)	(x)	(x)	(x)	(x)	(x)	(x)	(x)
	INCOME	(x)	-	-	-	-	(x)	(x)	-	-	-	-
	FlowMark	(x)	-	-	-	-	(x)	(x)	-	-	-	-
	WorkParty	-	-	-	-	-	(x)	(x)	-	-	-	-
	WIDE	-	-	-	-	-	x	x	-	-	-	-
	SecureFlow	-	-	-	-	-	x	x	-	-	-	
Sicherheitsmodelle	MoSS	-	*	*	*	*	*	*	*	*	*	*
	DROPS	*	*	*	*	*	*	*	*	*	*	*
	SECTINO	-	*	*	*	*	*	*	*	*	*	*
	POSeM	*	*	*	*	*	*	*	*	*	*	*

- Legende:** x ermöglicht Abbildung der Sicherheitsanforderung  
 - Abbildung der Sicherheitsanforderung nicht möglich oder nicht praktikabel  
 (x) Abbildung möglich bei Erweiterung des Metamodells um Sicherheitselemente  
 \* Modell grundsätzlich geeignet, benötigt zur Abbildung aber geeignete Modellierungsmethoden bzw. Beschreibungstechniken  
 (\*) grundsätzlich geeignet für die Unterstützung bei der Erstellung von Sicherheitspolitiken, setzt aber die Verwendung geeigneter (grafischer) Methoden voraus

Das Ergebnis der durchgeführten Analyse offenbart, dass adäquate Modellierungsmethoden für die Gestaltung sicherer Geschäftsprozesse fehlen. Dies ist ein Hinweis darauf, dass die grafische Modellierung der Sicherheitsanforderungen auf Fachkonzeptebene nicht trivial ist. Die meisten der analysierten Methoden bieten keine ganzheitliche Unterstützung aller relevanten Sicherheitsaspekte. Sind die Methoden grundsätzlich für eine solche Abbildung geeignet, muss in den meisten Fällen deren Metamodell um Sicherheitselemente erweitert werden.

Eine Besonderheit stellen die Methoden zur Workflowmodellierung dar, die den Geschäftsprozess durch die Zuordnung von konkreten Tätigkeiten zu spezifischen Akteuren der Organisation operationalisieren. Sie unterstützen daher die Identitätsprüfung und die Zugriffskontrolle vergleichsweise gut. Der Methode MOBILE kommt hierbei eine Sonderrolle insofern zu, als dass sie eine Abbildung aller relevanten Anforderungen ermöglicht, sollte das zugehörige Metamodell um entsprechende Sicherheitselemente erweitert werden. Allerdings würden die Modelle dann schnell unübersichtlich bzw. für eine Fachabteilung schwer verständlich, da MOBILE eine sehr systemnahe Betrachtung durch die Spezifikation von Modulschnittstellen mittels einer eigenen Skriptsprache in den Vordergrund stellt. Konzentrieren sich Verfahren also eher auf die Spezifikation von Anforderungen an die Anwendungssysteme als an die Geschäftsprozesse, führt dies zu einer häufig unzureichenden Berücksichtigung des Kontextes.

Eine Sonderrolle nehmen die Sicherheitsmodelle ein. Sie unterstützen zwar die Spezifikation von Sicherheitsanforderungen an Organisation und Software, setzen aber voraus, dass die Geschäftsprozesslogik bereits mit einer geeigneten Modellierungsmethode beschrieben wurde. Oft wird hierzu UML verwendet. Diese Sicherheitsmodelle sind alleine daher nicht ausreichend, um eine effektive Modellierung von IT-Sicherheit zu ermöglichen. Sie müssen um eine passende Modellierungsmethode ergänzt werden. Aus diesem Grund wird im folgenden Abschnitt im Rahmen der Synthese ein Sicherheitsmodell ausgewählt und die Anwendung geeigneter, erweiterter Methoden vorgeschlagen.

Ebenfalls eine Sonderstellung besitzen die aktivitätsorientierten Methoden „Zielbasierter Ansatz“, PROMET und Process Landscaping. Sie können bei der Erstellung von Sicherheitspolitiken (Policies) bzw. Ziel-Mittel-Hierarchien hilfreich sein, setzen aber ebenfalls die Verwendung geeigneter (grafischer) Methoden voraus.

Es bleibt die grundsätzliche Forderung nach Praktikabilität, insbesondere was die Kommunikation mit den betroffenen Fachabteilungen angeht. Aktivitätsorientierte Methoden werden i.d.R. von den Mitarbeitern der Fachebene wesentlich besser verstanden als abstrakte, objektorientierte Methoden wie z.B. UML. „Da jedoch der Anwender an der Erstellung des Fachkonzeptes in starkem Maße beteiligt ist, kann dies ein nicht zu unterschätzendes Problem darstellen. Was fast allen objektorientierten Modellierungstechniken fehlt, sind Konstrukte zur Beschreibung der von dem zu entwickelnden Softwaresystem zu unterstützenden Geschäftsprozesse und der Aufbauorganisation. Der Grund dafür ist darin zu sehen, dass die objektorientierten Methoden im Wesentlichen aus einer Abstrahierung der in den objektorientierten Programmiersprachen enthaltenen Konzepte entstanden sind. Das heißt, Basis für die Entwicklung waren existierende Programmiersprachen und nicht die Betriebswirtschaft des Unternehmens.“[ScJo96, S.38]

## 4 Synthese und Empfehlung

Auf Grundlage der vorangegangenen Analyse wird DROPS als Vorgehensmodell gewählt und notwendigerweise um geeignete Modellierungsmethoden ergänzt. Dabei erscheint es praktikabel, die Modellierung in zwei Schritten durchzuführen. In einem ersten Schritt wird die Methode EPK (Ereignisgesteuerte Prozesskette) gewählt und um geeignete Konstrukte für die Abbildung von Sicherheitsanforderungen auf einer betriebswirtschaftlich-organisatorischen und rechtlichen Ebene ergänzt (eEPK, erweiterte EPK). Hierbei handelt es sich um eine für die Mitarbeiter der Fachabteilungen leicht verständliche Abfolge von Ereignissen und Aktivitäten, erweitert um Elemente, die die Einbindung von organisatorischen und technischen Objekten ermöglichen. Ergänzend dazu werden die in Tabelle 2 eingeführten Sicherheitsanforderungen bzw. deren grafische Symbolisierung verwendet. In einem zweiten Modellierungsschritt wird aus dem mittels eEPK erstellten fachlichen Prozessmodell ein systemnäheres bzw. umsetzungsorientiertes Modell abgeleitet. Hierbei sollen nun die Vorteile der aktivitätsorientierten Modellierung mit den Vorteilen der objektorientierten Modellierung (Wiederverwendung; Generierung von Programmcode) verknüpft werden. Alternativ stehen hier die Methoden oEPK (objektorientierte EPK) und EMK (Ereignisgesteuerte Methodenkette) zur Verfügung. Im Zuge des Ableitungsprozesses werden aus den mittels eEPK abgebildeten Sicherheitsanforderungen Sicherheitsmethoden durch oEPK bzw. EMK spezifiziert (vgl. Tabelle 2).

Das Sicherheitsmodell DROPS (Dimensions-relacionales organisations- und problembezogenes Sicherheitsmodell, [PrHo04]) betrachtet „Komponenten“ aus jeweils zwei Sichten. Es handelt sich dabei um Komponenten von Informationssystemen, die potenzielle Schwachstellen darstellen (Hardware, Software, organisatorische Normen, Personen/Anwender, Daten, Informationsmanagement, Umwelt/externe Faktoren). Bei den Sichten handelt es sich um eine eher pragmatische „organisationsbezogene Sicht“, deren Ausgangspunkte die oben genannten Komponenten sind, und eine eher abstrakte „problembezogene Sicht“. Letztere geht von den „Sicherheitsaspekten“ Vertraulichkeit, Integrität, Verfügbarkeit und Verbindlichkeit aus und kann um die anderen in Abschnitt 3.2 dargestellten Sicherheitsanforderungen erweitert werden.

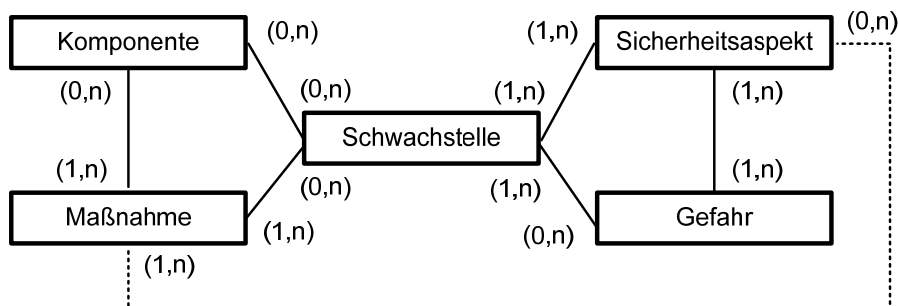

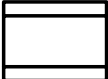








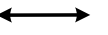




Abb. 1: DROPS-Relationenmodell

Das in Abbildung 1 dargestellte Relationenmodell stellt die in DROPS verwendeten fünf grundlegenden „Dimensionen der Sicherheit“ dar: Komponente, Sicherheitsaspekt, Gefahr, Schwachstelle und Maßnahme. Die Nähe zu etablierten Verfahren zur Erstellung von organisationalen Sicherheitspolitiken wird hier offensichtlich.

Im Folgenden werden nun die anzuwendenden Methoden anhand eines durchgängigen Beispiels erläutert. Zunächst gibt Abbildung 2 einen Überblick über die in den jeweiligen Meta-modellen verwendeten Konstrukte. oEPK und EMP wurden durch das Element „Sicherheitsmethode“ erweitert.

Symbol	Methode	Symbol	Methode
 Ereignis	EPK, oEPK, EMK	 Objektklasse	oEPK, EMK
 Aktivität / Vorgang	EPK	 Methode	oEPK, EMK
 Schnittstelle	EPK, oEPK, EMK	 Sicherheitsmethode	oEPK, EMK
 Organisationseinheit	EPK, oEPK, EMK	 Attribut	oEPK, EMK
 Datenbank	EPK	 Kontrollfluss	EPK, oEPK, EMK
		 Leistungsbeziehung	oEPK, EMK
		 ungerichtete Kante	EPK, oEPK, EMK
		 boolesche Konnektoren	EPK, oEPK, EMK

**Abb. 2:** Symbole für EPK, oEPK und EMK

Das folgende Beispiel (vgl. Abbildungen 3, 4 und 5) betrachtet die Prozesse, die im Rahmen des Einkaufs in einem Online Shop ablaufen. Der gesamte Prozess umfasst die Suche des Interessenten von Artikeln im Internetangebot des Anbieters, die Registrierung und Autorisierung eines Neukunden bzw. die Autorisierung eines Altkunden, die Zahlung und schließlich den Versand der Ware. Im Rahmen dieses Beitrags beschränken wir uns auf die Darstellung des Teilprozesses Registrierung und Autorisierung.

Eine generelle Empfehlung für die Verwendung einer der alternativen Methoden oEPK und EMK zu geben, ist nicht sinnvoll. Im Vergleich mit der Methode eEPK des ersten Modellierungsschrittes ersetzt die Methode oEPK im zweiten Modellierungsschritt die Aktivitäten/Vorgänge durch Objektklassen, die wiederum (Sicherheits-)Methoden aufrufen. Die genaue Abfolge des Methodenaufrufs wird nicht explizit modelliert. Dies ist hingegen bei der Alternativmethode EMK der Fall. Hier werden die Aktivitäten/Vorgänge der eEPK durch Methodenabfolgen ersetzt. Da man sich hier aber immer noch auf der Ebene der Fachkonzeptmodellierung befindet, ist es häufig schwer, sich schon zu diesem frühen Zeitpunkt auf eine exakte Methodenabfolge festzulegen.

## 5 Ausblick

Obige Prozessmodelle wurden mit den Anwendungen Microsoft Visio und Aha-soft ArtIcons auf einer rein grafischen Ebene erstellt. Der weitere Forschungsbedarf besteht nun darin, die für die Modellierung passenden Werkzeuge auszuwählen, anzupassen oder zu entwickeln. Ziel ist es dabei, die Wiederverwendung von Prozesspartikeln und Referenzprozessen ebenso zu ermöglichen, wie die Simulation ganzer Prozesse und die Generierung von Programmcode oder Dokumentationen zu unterstützen.

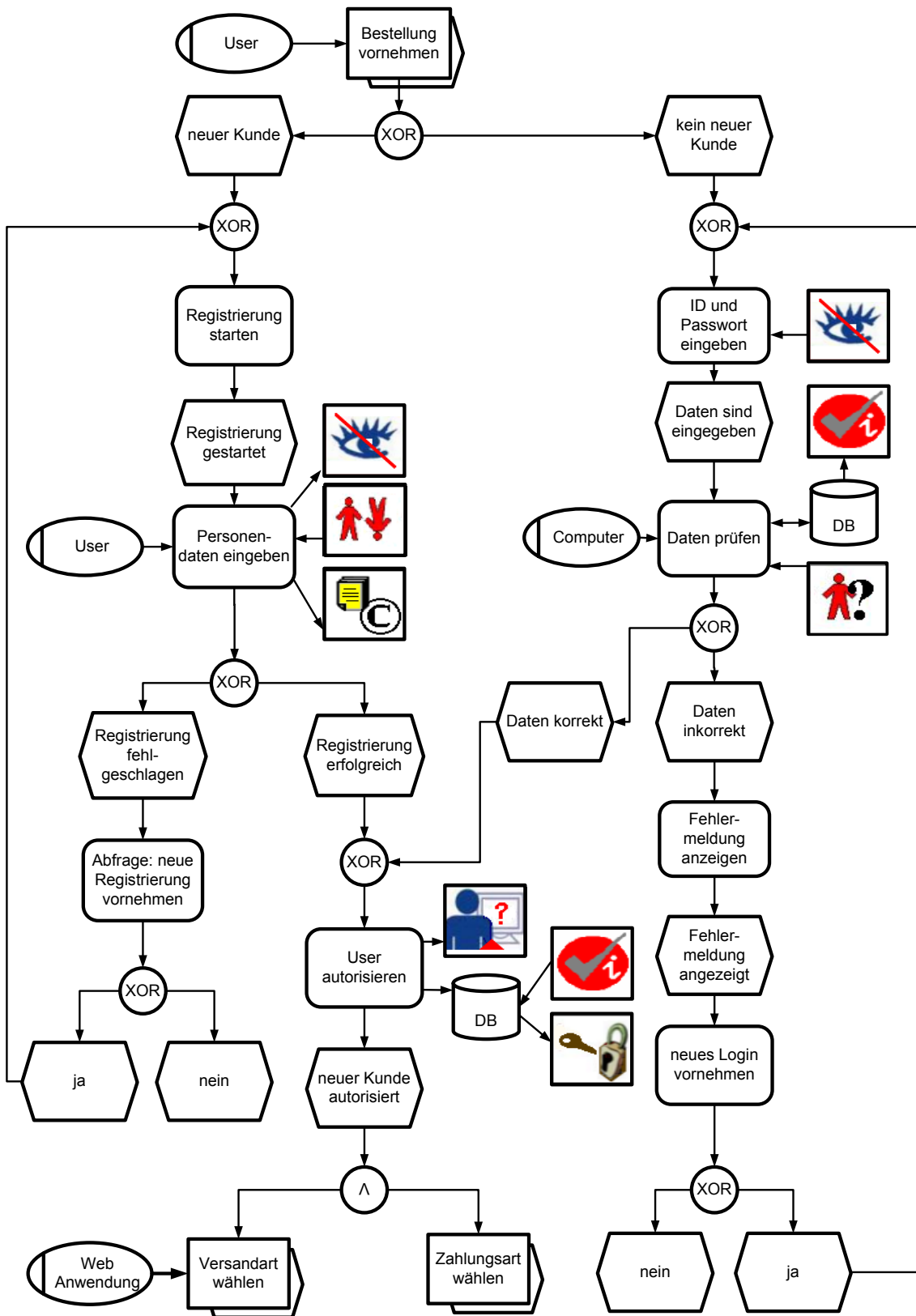


Abb. 3: Anwendungsbeispiel „Registrierung und Autorisierung in einem Web Shop“ mittels eEPK

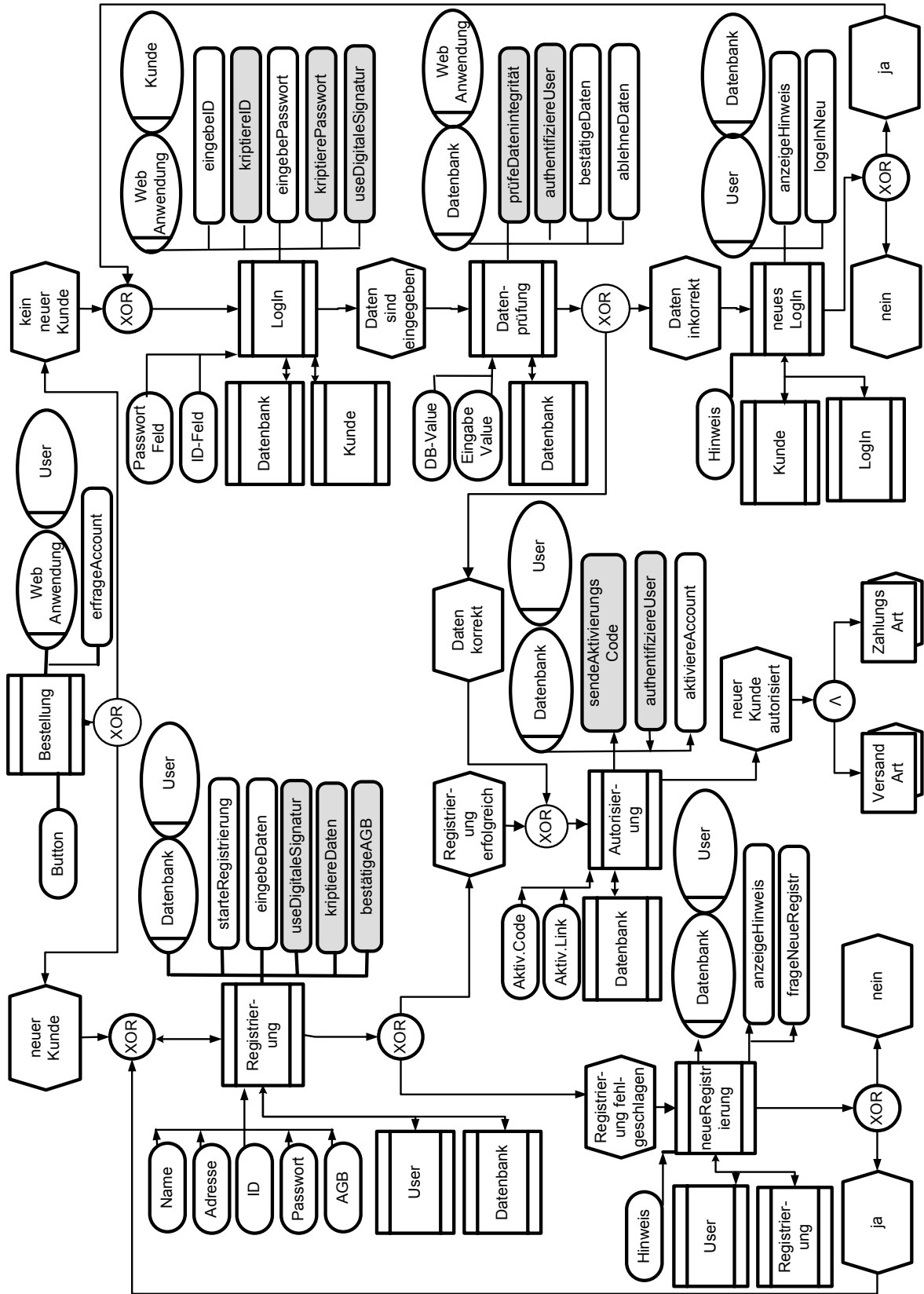


Abb. 4: Anwendungsbeispiel „Registrierung und Autorisierung in einem Web Shop“ mittels oEPK

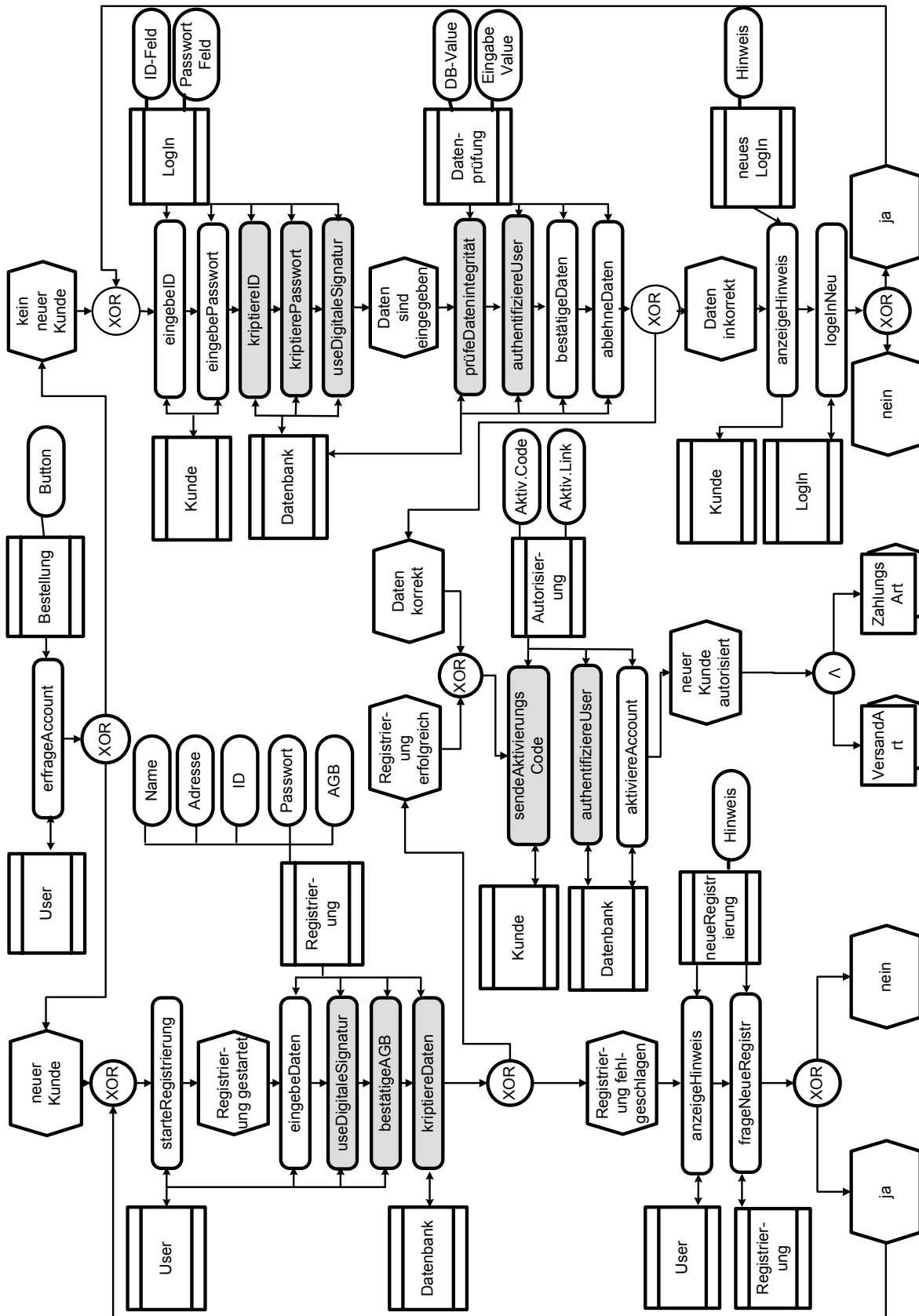


Abb. 5: Anwendungsbeispiel „Registrierung und Autorisierung in einem Web Shop“ mittels EMK

## Literatur

- [BBB+97] V. Bach, R. Benz et al.: Das Vorgehensmodell PROMET-BPR Version 2.0, Universität St.Gallen (1997).
- [BHW+04] R. Breu, M. Hafner et al.: Modellierung und Realisierung sicherheitskritischer Prozesse, P. Horster: Elektronische Geschäftsprozesse, syssec (2004) 396-407.
- [BuJa96] C. Bußler, S. Jablonski: Die Architektur des modularen Workflow-Management-System MOBILE, [VoBe96] 369-388.
- [CGP+96] F. Casati, P. Grefen et al: WIDE Workflow model and architecture, [www.wi.uni-muenster.de/imperia/md/content/wi-information\\_systems/lehveranstaltungen/lehveranstaltungen/bpmundwfm/ws0405/casati96wide.pdf](http://www.wi.uni-muenster.de/imperia/md/content/wi-information_systems/lehveranstaltungen/lehveranstaltungen/bpmundwfm/ws0405/casati96wide.pdf)
- [DaNi03] H. Dammag, N. Nissanke: A Mathematical Framework for Safecharts, <http://myweb.lsbu.ac.uk/~dammagh/files/ICEFM03.ps>
- [Ecke04] C. Eckert: IT-Sicherheit, Oldenbourg (2004).
- [EmGr91] W. Emmerich, V. Gruhn: FUNSOFT Nets: A Petri-Net based Software Process Modeling Language, IEEE (1991).
- [ErPe00] H.-E. Eriksson, M. Penker: Business Modeling with UML: Business Patterns at Work, Wiley & Sons (2000).
- [FeSi95] O. Ferstl, E. Sinz: Der Ansatz des Semantischen Objektmodells (SOM) zur Modellierung von Geschäftsprozessen, Wirtschaftsinformatik, 3 (1995) 566-585.
- [GrWe00] V. Gruhn, U. Wellen: Process Landscaping: Eine Methode zur Geschäftsprozessmodellierung, Wirtschaftsinformatik, 4 (2000) 297-309.
- [Hans96] J. Hanschmidt: Das Geschäftsprozessmanagementsystem WorkParty. Jörg Becker, M. Rosemann: Workflowmanagement, Inst. f. Wirtschaftsinformatik d. Uni. Münster (1996) 37-45.
- [HePe00] G. Herrmann, G. Pernul: Sicherheit durch Business Process Re-Engineering, INFORMATIK Zeitschrift, Heft 6 (2000) 18-23.
- [HeRö99] G. Herrmann, A.W. Röhm: ALMOST: Eine Modellierungsmethode für sichere elektronische Geschäftstransaktionen, A.W. Röhm et al: Sicherheit und Electronic Commerce Workshop Proceedings, Vieweg (1999) 147-162.
- [HuAt99] W-K. Huang, V. Atluri: SecureFlow: A Secure Web-enabled Workflow Management System, 4th ACM Workshop on Role-based Access Control (1999).
- [Jaes96] P. Jaeschke: Geschäftsprozessmodellierung mit INCOME, [VoBe96] 141-162.
- [Joos94] S. Joosten: Trigger Modelling for Workflow Analysis, Workflow Management CON'94, (1994) 237-247.
- [KeNS92] G. Keller, M. Nüttgens, A.-W. Scheer: Semantische Prozessmodellierung auf Grundlage Ereignisgesteuerte Prozessketten (EPK), A.-W Scheer: Veröffentlichungen des Inst. f. Wirtschaftsinf. d. Uni Saarbrücken, Heft 89 (1992).
- [KoSc04] F. Kollmann, M. Schaffer: Sicherheitsaspekte elektronischer Geschäftsprozesse, P. Horster: Elektronische Geschäftsprozesse 2004, syssec (2004) 158-175.

- [Krcm90] H. Krcmar: Bedeutung und Ziele von Informationssystem-Architekturen, Wirtschaftsinformatik, Heft 5 (1990) 395-402.
- [KüBS95] P. Küng, P. Bichler, M. Schrefl: Geschäftsprozeßmodellierung: ein zielbasierter Ansatz, <http://diuf.unifr.ch/is/staff/peterk/KuBiSc95.pdf>
- [LeSi97] Y. Lei, M. Singh: A Comparison of Workflow Metamodels, <http://osm7.cs.byu.edu/ER97/workshop4/ls.html>
- [LeOr98] F. R. Lehmann, E. Ortner: Workflowsysteme ein interdisziplinäres Forschungs- und Anwendungsgebiet, <http://www.svifsi.ch/revue/pages/issues/n982/in982.pdf>
- [LoBD02] T. Lodderstedt, D. Basin, J. Doser: SecureUML: A UML-Based Modeling Language for Model-Driven Security, [http://www.informatik.uni-freiburg.de/~tolo/pubs/secuml\\_uml2002.pdf](http://www.informatik.uni-freiburg.de/~tolo/pubs/secuml_uml2002.pdf)
- [MWFF92] R. Medina-Mora, T. Winograd, R. Flores, F. Flores: The Action Workflow Approach to Workflow Management Technology, ACM, CSCW 92 Proceedings (1992) 281-288.
- [Omg05] Object Management Group(OMG): UML, <http://www.omg.org/>
- [Petr62] C.A. Petri: Kommunikation mit Automaten, Schriften IIM Uni Bonn, 2 (1962).
- [PrHo04] A. Prieß, G. Hoppe: Modellierung der Sicherheit von Informationssystemen mit DROPS, [www.wiwi.uni-hannover.de/~fbwiwi/forschung/diskussionspapiere/dp-301.pdf](http://www.wiwi.uni-hannover.de/~fbwiwi/forschung/diskussionspapiere/dp-301.pdf)
- [Ritt99] P. Rittgen: Vom Prozessmodell zum elektronischen Geschäftsprozess, Arbeitsberichte des Inst. f. Wirtschaftsinf. d. Uni Koblenz, Nr. 17 (1999).
- [Roll96] D. Roller: Verifikation von Workflows mit IBM FlowMark, [VoBe96] 353-368.
- [Rose95] M. Rosemann: Komplexitätsmanagement in Prozessmodellen, Gabler (1995).
- [Röhr03] S. Röhrig: Using Process Models to Analyse IT Security Requirements, [http://www.ifi.unizh.ch/publications/diss/Jahr\\_2003/thesis\\_roehrig.pdf](http://www.ifi.unizh.ch/publications/diss/Jahr_2003/thesis_roehrig.pdf)
- [Sche97] A.-W. Scheer: Wirtschaftsinformatik, 7. Aufl., Springer (1997).
- [ScJo96] A.-W. Scheer, W. Jost: Geschäftsprozeßmodellierung innerhalb einer Unternehmensarchitektur. [VoBe96] 29-46.
- [ScNZ97] A.-W. Scheer, M. Nüttgens, V. Zimmermann: Objektorientierte Ereignisgesteuerte Prozeßkette (oEPK): Methode und Anwendung, A.-W Scheer: Veröffentlichungen des Inst. f. Wirtschaftsinf. d. Uni Saarbrücken, 141 (1997).
- [Thob98] W. Thoben: Sicherheit für Workflow-basierte Anwendungen, K. Bauknecht: Sicherheit in Informationssystemen SIS'98, Vdf Hochschulverlag (1998) 209-232.
- [Ulri01] F. Ulrich: Informatik und Wirtschaftsinformatik: Grenzziehungen und Ansätze zur gegenseitigen Befruchtung, J. Desel: Das ist Informatik, Springer (2001).
- [VoBe96] G. Vossen, J. Becker: Geschäftsprozessmodellierung und Workflow Management, Thomson (1996).
- [WoWe97] D. Wodtke, G. Weikum: A Formal Foundation for Distributed Workflow Execution Based on State Charts, Lecture Notes in Computer Science; (1997) 230-246.