Bausteine eines Prozessmodells für Security-Engineering

Ruth Breu

Universität Innsbruck

Forschungsgruppe Quality Engineering

Ruth.Breu@uibk.ac.at

Übersicht

1. **Einführung und Ausgangspunkt**
2. **Der Security-Prozess**
3. **Spezifikation von Sicherheitsanforderungen**
4. **Umsetzung von Anforderungen**
5. **Zusammenfassung und Ausblick**

1. Einführung und Ausgangspunkt

Typische Anwendungen – Beispiele:

- **E-Government**
  - » Abwicklung von Behördenvorgängen über das Internet
  - » Beispiel: Unternehmensgründung
- **Gesundheitswesen**
  - » elektronische Patientenakte
  - » Einsatz mobiler Geräte am Krankenbett

Gemeinsamkeit dieser Anwendungen

- **Komplexe organisatorische Abläufe**
  - » enge Verflechtung manueller und system-unterstützter Aktivitäten
  - » Abläufe oft institutionsübergreifend
  - » massiv verteilte Abläufe
  - » mit der Einführung des IT-Systems müssen die Abläufe neu organisiert werden
  - » Systemdienste müssen analysiert werden
- **Sicherheit spielt eine vorherrschende Rolle**
  - » rechtliche Aspekte
  - » wirtschaftliche Aspekte

➡ **Bedeutung der Konzeptionsphase wächst!**

Unser Ziel

- **Entwicklung einer Methode zum systematischen Entwurf zugriffssicherer Systeme**
  - » Möglichst frühes Erfassen von Sicherheits-anforderungen
  - » Umfassende Risikoanalyse
  - » Systematisches Ergreifen von Sicherheits-Maßnahmen
- **Integration von Aspekten der Zugriffssicherheit in objektorientierte Entwurfsmethoden**

Motivation

- **Reduzierung von Komplexität im Entwurf**
- **Dokumentation von Sicherheits-anforderungen**
- **Sicherheitsaspekte haben Auswirkungen auf Arbeitsprozesse und organisatorische Strukturen**
  - » Abstimmung mit dem Kunden notwendig
- **Großes Potential für patternorientiertes Vorgehen und Codegeneration**

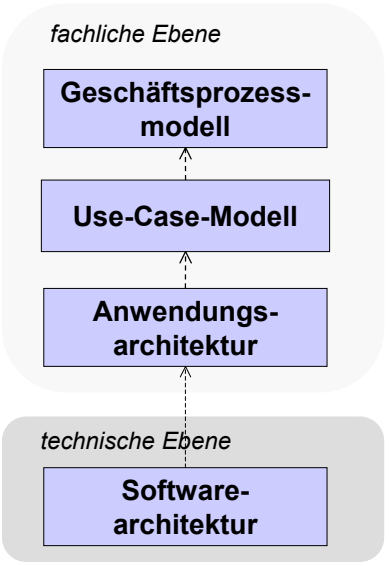
Ausgangspunkt

- **Objektorientiertes Vorgehensmodell (à la RUP)**
  - » Sprache: UML
  - » Entwurf mit Use Cases und Geschäftsprozessen
  - » Komponentenorientierter Entwurf
  - » Iteratives Vorgehen

Kernmodelle (1)

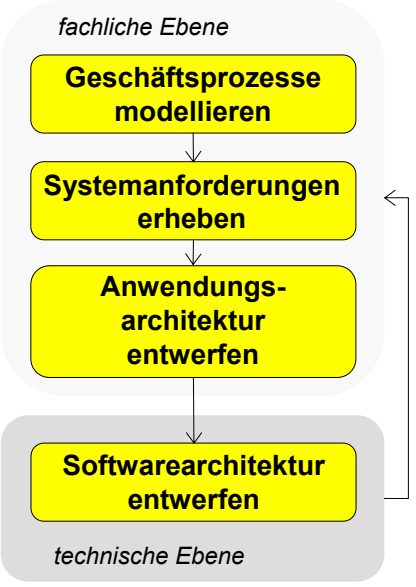
Geschäftsprozess-modell	► Analyse und Modellierung von Arbeitsabläufen
Use-Case-Modell	► Identifizierung und Beschreibung von Systemdiensten (Use Cases)
Anwendungs-architektur	► Beschreibung abstrakter Nachrichtenflüsse ► Identifikation fachlicher Komponenten
Software-architektur	► Verteilte Systemstruktur ► Definition technischer Komponenten

Kernmodelle (2)



A ----> B
Modell A bezieht sich auf Modell B

Prozess



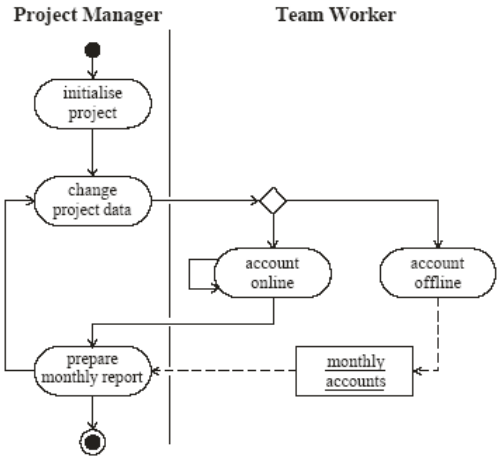
iterativer Entwurf

A ⟶ B
Aktivität B folgt Aktivität A

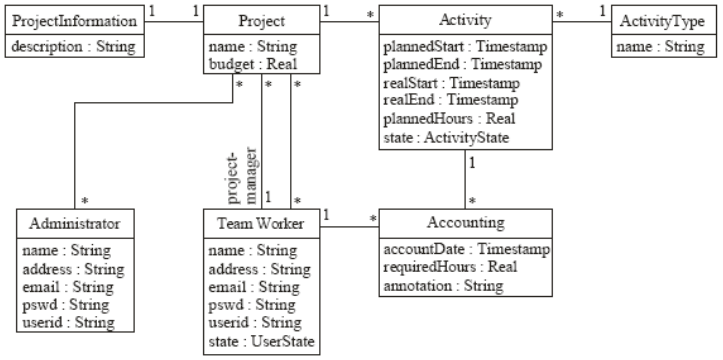
Beispiel - TimeTool

- **Projektmanagementwerkzeug**
  - » Zeiterfassung
  - » Abrechnung von Projekten
- **Implementierung mit Web-Interface**

Geschäftsprozessmodell



Klassendiagramm



Use-Case „Buchungsänderung“

Use Case: Adjustment Posting

Actor
Team Worker

Input
AccountingID, Modified Accounting Data

Output
Accounting Data, Acknowledgement

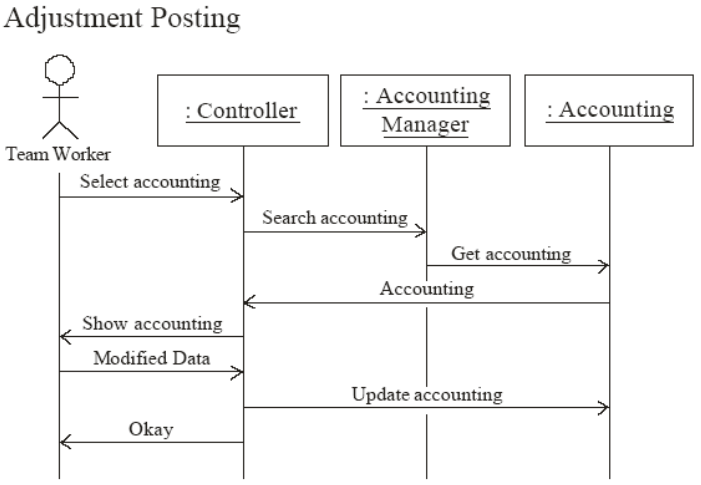
Modified classes in the application core
Accounting

Description
The system gets from the team worker an accounting identifier (e.g. from a prior search) and the system accounting manager searches the accounting and displays it to the team worker. He gives the modified data to the system and the system stores them. At the end, the system gives an acknowledgment back to the team worker.

Variants

- The system cannot find the accounting from the accounting identifier. The system ends with a negative acknowledgement.
- The team worker gets the accounting and does not modify the data. The system hasn't to store the known data again, but the system returns a positive acknowledgement.
- The team worker puts in incorrect values. The system informs the user about the mistake and waits for a new input.

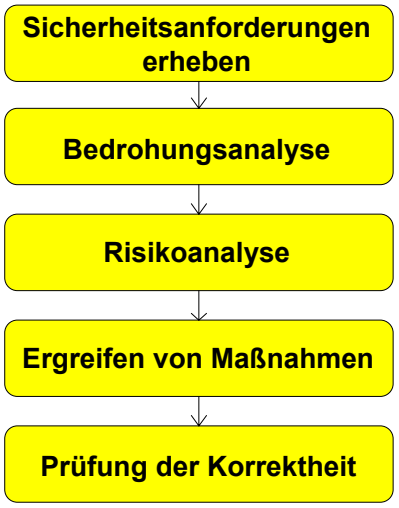
Szenario „Buchungsänderung“



Übersicht

1. **Einführung und Ausgangspunkt**
2. **Der Security-Prozess**
3. **Spezifikation von Sicherheitsanforderungen**
4. **Umsetzung von Anforderungen**
5. **Zusammenfassung und Ausblick**

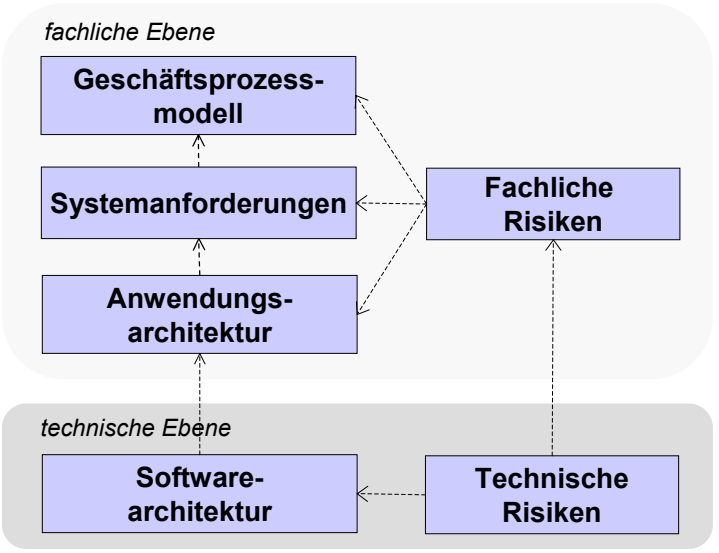
Sicherheitsanalyse als Mikroprozess



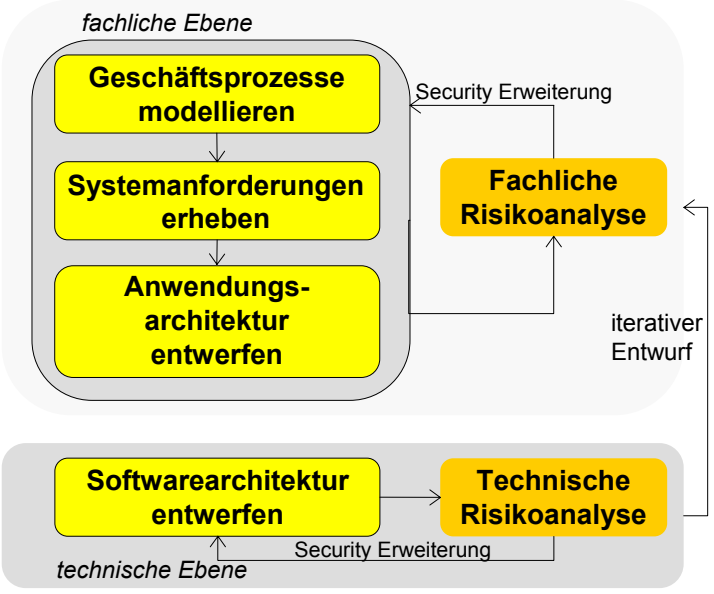
Anforderungen und Maßnahmen

- Sowohl Sicherheitsanforderungen als auch –maßnahmen werden in den Kernmodellen modelliert
- Meist kann nicht zwischen Anforderungen und Maßnahmen unterschieden werden
- Deshalb sprechen wir von Sicherheitsaspekten
- Sicherheitsaspekte sind durch eine Realisierungsbeziehung untereinander verbunden

Die Dokumente des Security-Prozesses



Der Security-Prozess



Übersicht

1. Einführung und Ausgangspunkt
2. Der Security-Prozess
3. Spezifikation von Sicherheitsanforderungen
4. Umsetzung von Anforderungen
5. Zusammenfassung und Ausblick

Sicherheitsziele

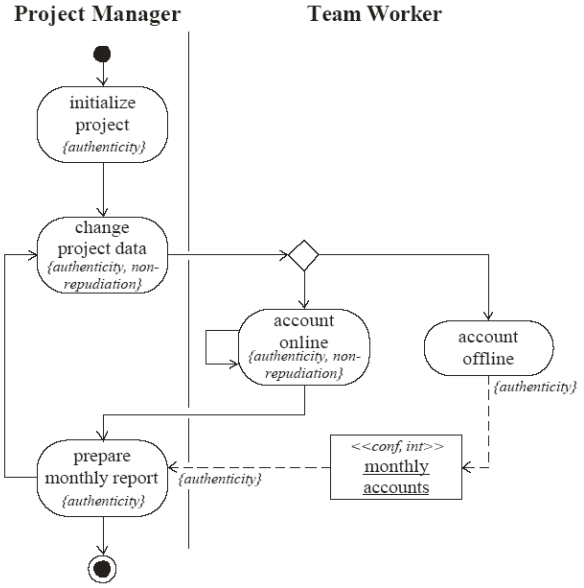
- Vertraulichkeit
- Datenintegrität
- Authentizität
- Nicht-Abstreitbarkeit
- Verfügbarkeit

- Spezifikation dieser Ziele im Geschäftsprozess- und Use-Case-Modell

Security-Geschäftsprozessmodell

- **Vertraulichkeit und Datenintegrität**
  - » Welche Akteure haben welche Sicht auf welche Objekte?
  - » Welche Objektflüsse sind kritisch?
- **Authentizität**
  - » Bei welchen Aktivitäten muss der ausführende Akteur authentifiziert sein?
  - » Müssen Akteure beim Objektaustausch authentifiziert sein?
- **Nicht-Abstreitbarkeit**
  - » Welche Aktivitäten kann der ausführende Akteur nicht abstreiten?

Beispiel



Spezifikation eines Rechtemodells - Beispiel

actor → / ↓ class	Team Worker		Project Manager	
Accounting	R: W/C:	all own accountings (independent of the project) own accountings from released activities	R/W/C:	all accountings of activities of own projects (i.e. where actor is the project manager of)
Activity	R: W/C:	all activities from projects allocated to the actor -	R/W: C:	all activities of own projects -
Project	R: W/C:	all projects -	R: W/C:	all projects -
User	R: W/C:	all users -	R: W/C:	all users -

Security Use-Case-Modell - Beispiel

use case Adjustment Posting

… (previous textual description of the use case from Figure 4)

security

A1 The adjustment posting is logged by the system.

A2 The team worker has to be authenticated before starting the use case.

A3 Web browser and TimeTool have to be authenticated before the transaction starts.

A4 The system must guarantee the confidentiality and integrity of the input data.

A5 The use case must be available during extended working hours (6a.m. to 22a.m.) with a maximum of 2 continuous working days breakdown per month.

Umsetzung von Anforderungen aus dem GP-Modell

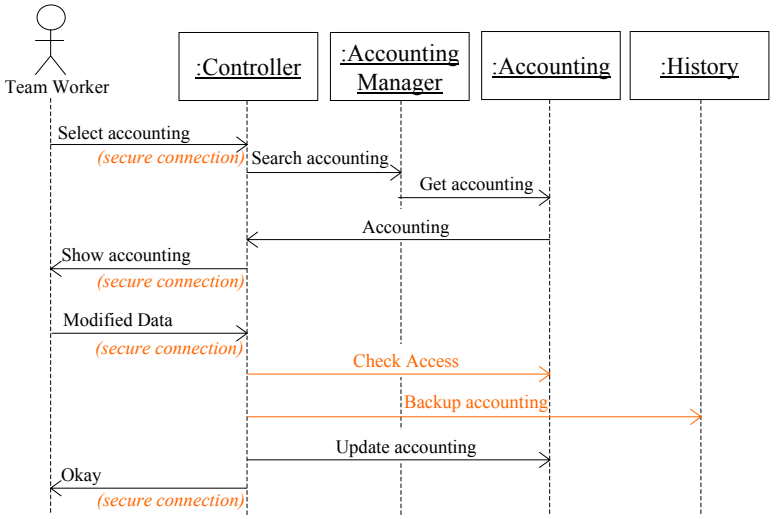
Anforderungen in Bezug auf externe Systeme

Verfügbarkeit

Übersicht

1. Einführung und Ausgangspunkt
2. Der Security-Prozess
3. Spezifikation von Sicherheitsanforderungen
4. Umsetzung von Anforderungen
5. Zusammenfassung und Ausblick

Beispiel – Erweitertes Szenario „Buchungsänderung“



Allgemeiner Ansatz

- **Trennung der fachlichen und der technischen Ebene**
- **Zwei Ansätze systematischer Konstruktion sicherer Lösungen:**
  - » patternorientiert
  - » model driven

Zusammenfassung und Ausblick

- **Erweiterung eines objektorientierten Vorgehensmodells um Aspekte der Zugriffssicherheit**
  - » Spezifikation und Management von Sicherheitsanforderungen (Traceability!)
  - » Management von Risiken
  - » Systematische Konstruktion sicherer Lösungen

Teilprojekte

- Formale Spezifikation von Rechtemodellen
- Management von IT-Sicherheitsrisiken
- Sicherheit in unternehmensübergreifenden Workflows
- Entwurf und Dokumentation von Sicherheitsarchitekturen