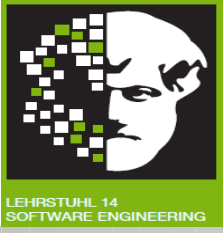


Konzeption und Entwicklung eines sicheren Cloud-basierten Internetbanking-Systems mit anschließender Sicherheitsanalyse auf Basis von Business Process Mining

im SoSe 2011 & WS 2011/12

Prof. Jan Jürjens, Dr. Holger Schmidt, Stephan Fassbender
TU Dortmund, Fakultät Informatik, Lehrstuhl XIV

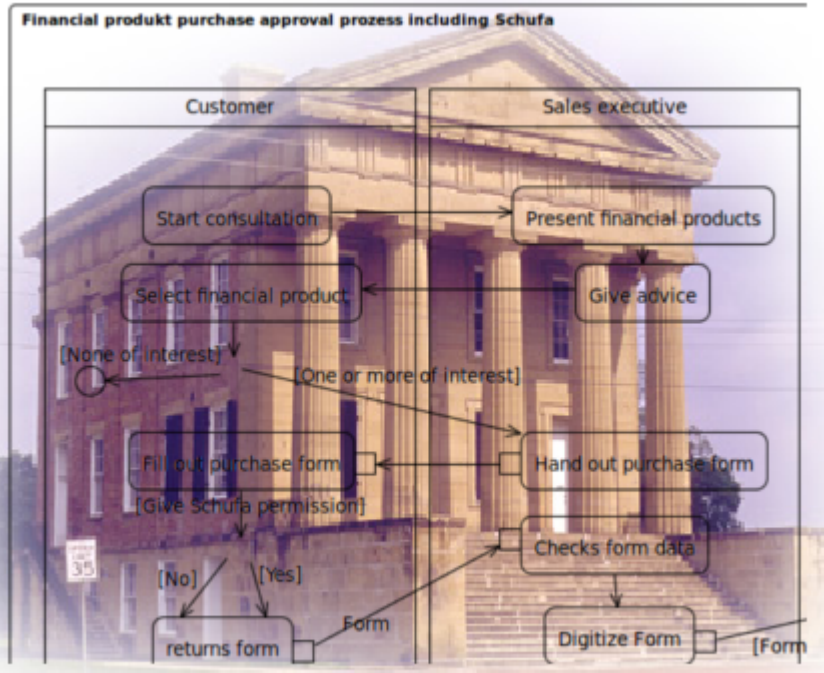
Agenda

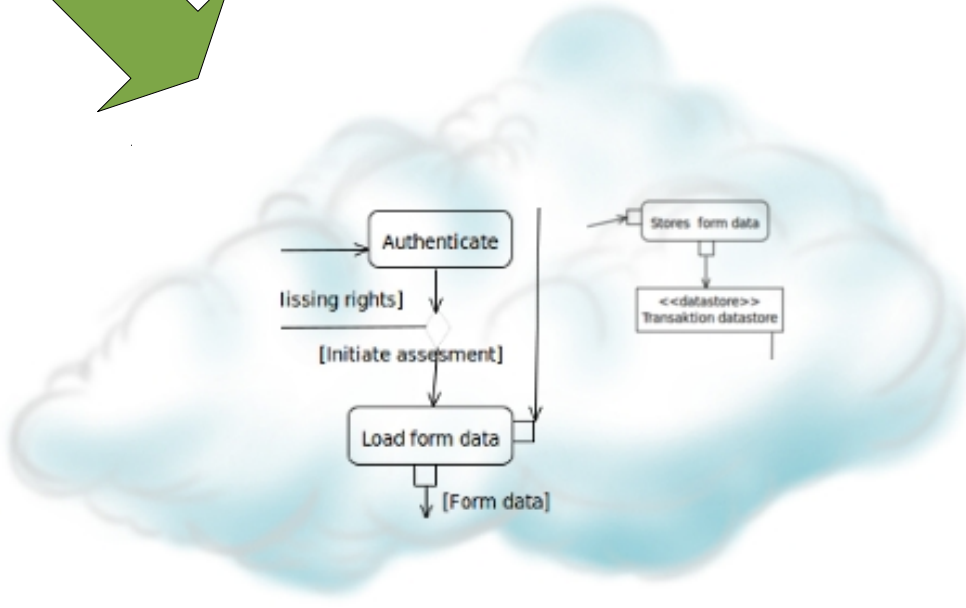
1. Das Thema
2. Das Vorgehen
3. Die Schwerpunkte
4. Die Werkzeuge
5. Das Organisatorische

Worum geht es?

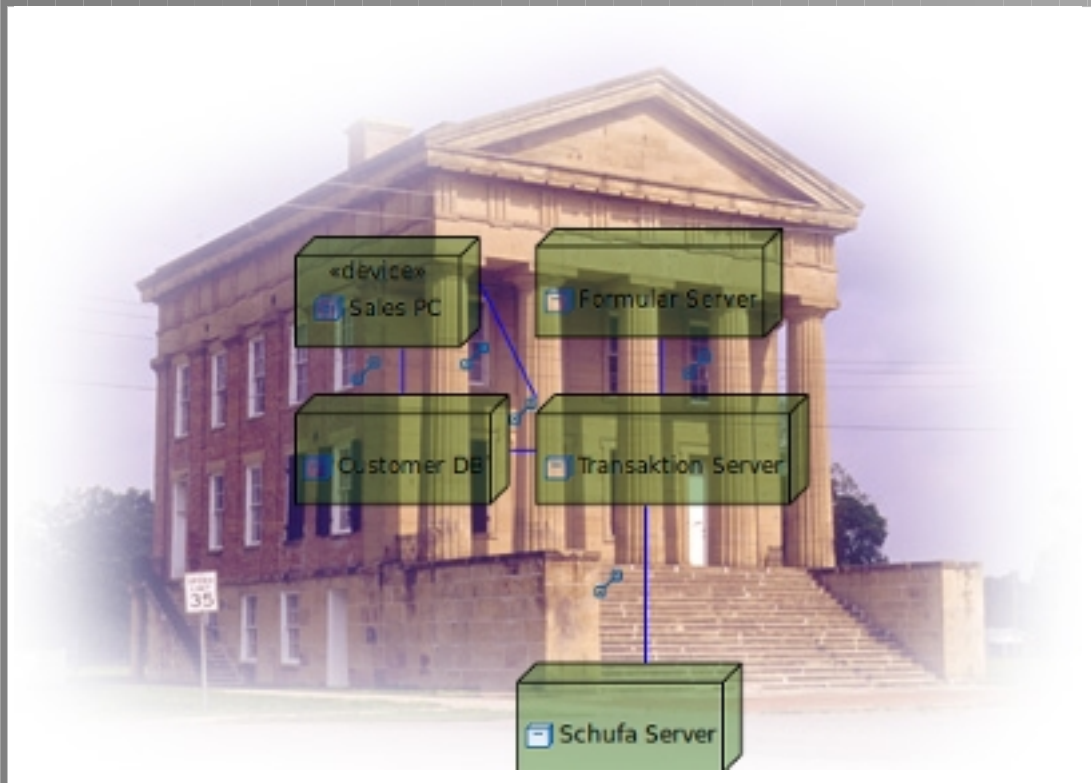
1. Das Thema
2. Das Vorgehen
3. Die Schwerpunkte
4. Die Werkzeuge
5. Das Organisatorische

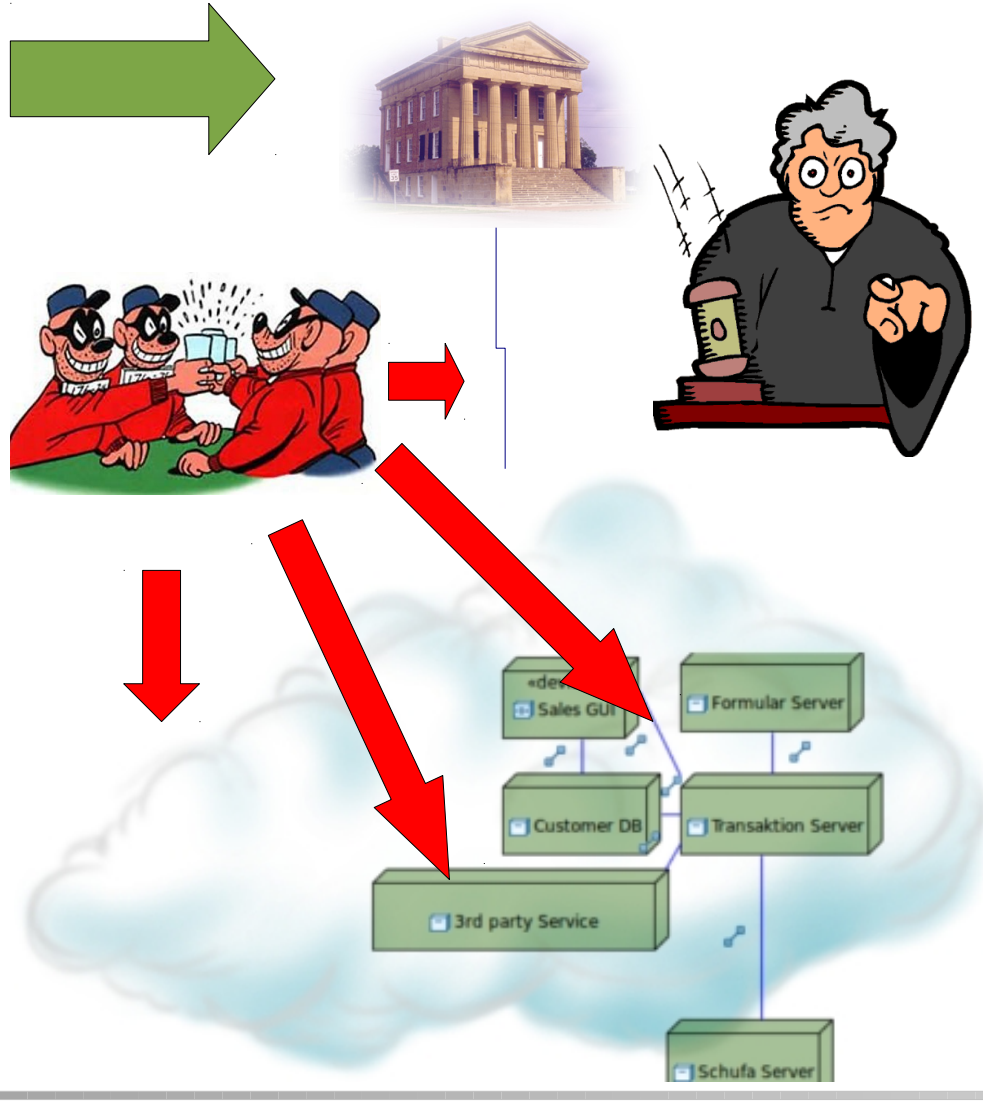
Worum geht es?
Prozessmigration in die Cloud





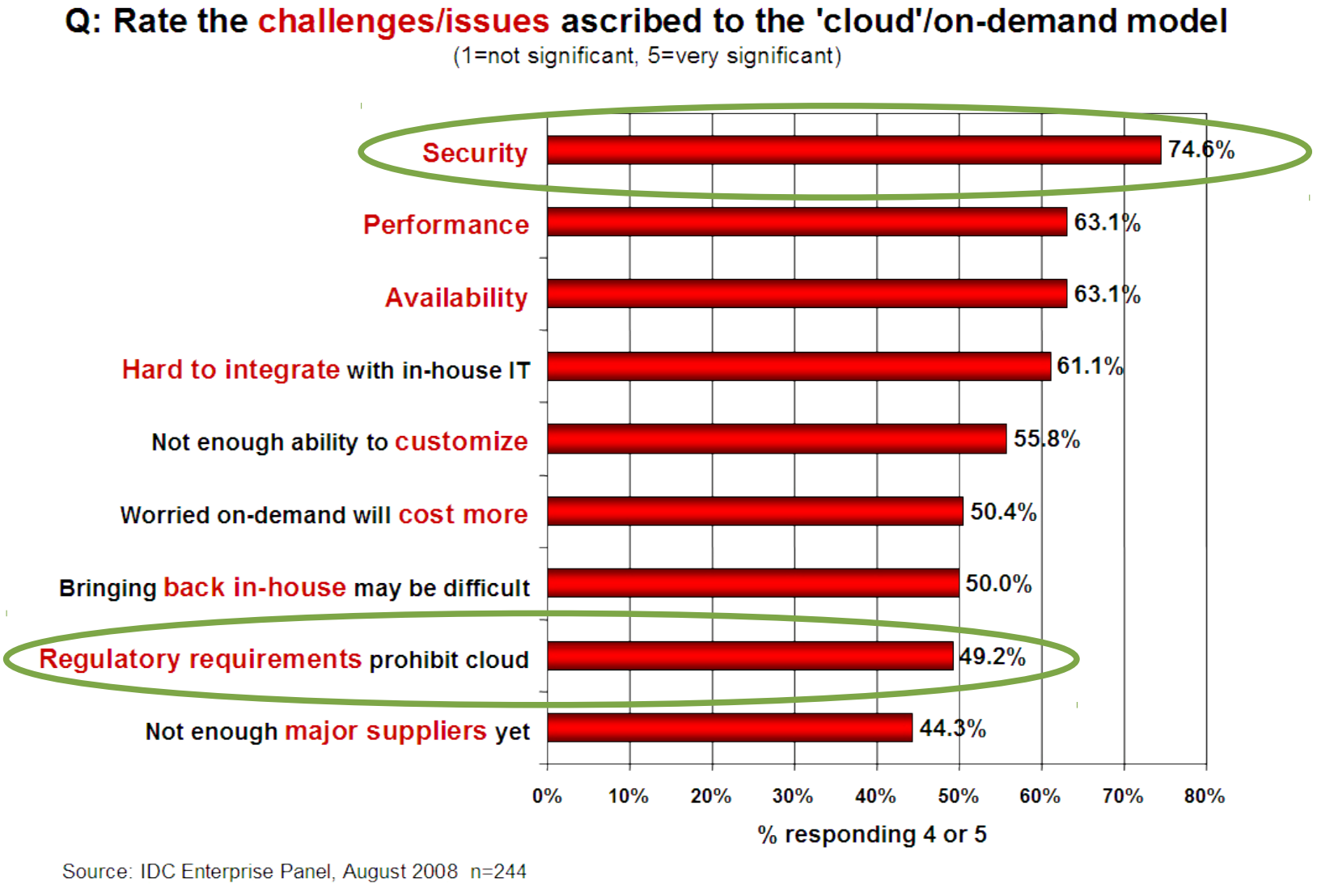
Worum geht es?
Herausforderungen: Security & Compliance





Worum geht es?
Show Stopper: Security & Compliance

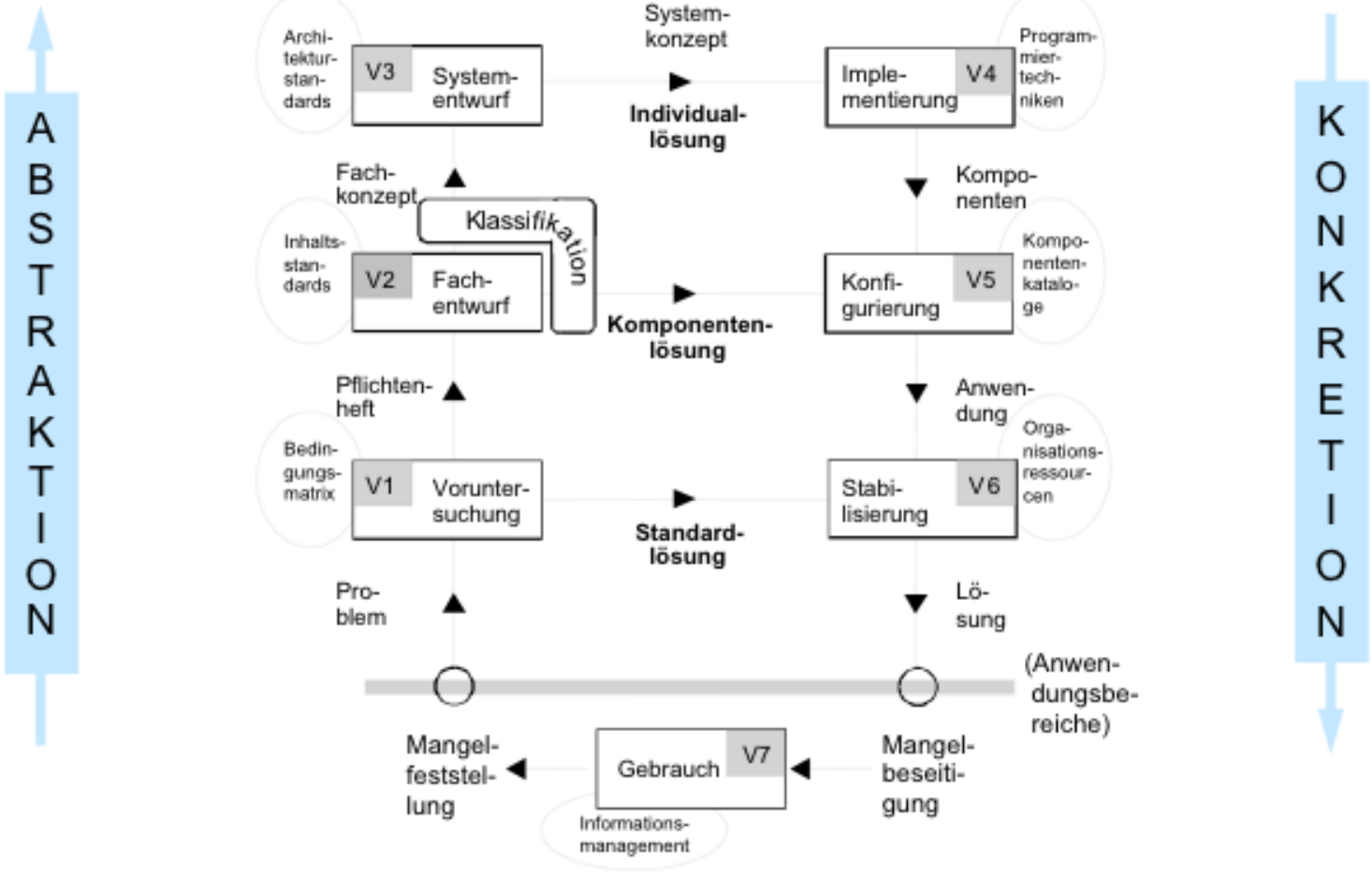
LEHRSTUHL 14
SOFTWARE ENGINEERING



Wie soll Vorgegangen werden?

1. Das Thema
2. Das Vorgehen
3. Die Schwerpunkte
4. Die Werkzeuge
5. Das Organisatorische

Wie soll Vorgegangen werden?
Vorgehensmodell



Wie soll Vorgegangen werden?
Projektplan SoSe

Aufgabe	Anfang	Ende	Wochen
Einarbeitungsphase			
- Vorbereitung u. Seminar	KW15	KW16	2
- Projektplan erstellen	KW17	KW17	1
Voruntersuchung			
- Anforderungserhebung und -analyse	KW18	KW20	3
- Spezifikation	KW21	KW22	2
Fachentwurf			
- Prozessmodellierung	KW23	KW25	3
- Grafische Benutzeroberfläche	KW26	KW26	1
Systementwurf			
- Auswahl von Technologien	KW27	KW27	1
- Architekturentwurf	KW28	KW29	2
Dokumentation			
- Zwischenbericht	KW15	KW29	15

Wie soll Vorgegangen werden?
Projektplan WS

Aufgabe	Anfang	Ende	Wochen
Implementierung	KW41	KW51	11
Konfigurierung	KW2	KW2	1
Stabilisierung - Unit-Testen - Anwendungsbeispiele - Seminar zu Softwaresicherheit - Penetrationstesten	KW3	KW6	4
Dokumentation - Endbericht	KW41	KW6	16

Wie soll Vorgegangen werden?
Seminarphase

- Teammitglieder vermitteln Wissen untereinander
- Jeder
  - bekommt ein PG relevantes Thema
  - recherchiert Quellen
  - wird Fachmann
  - vermittelt Wissen mittels Vortrag
  - steuert Kurzzusammenfassung zum PG Handbuch bei

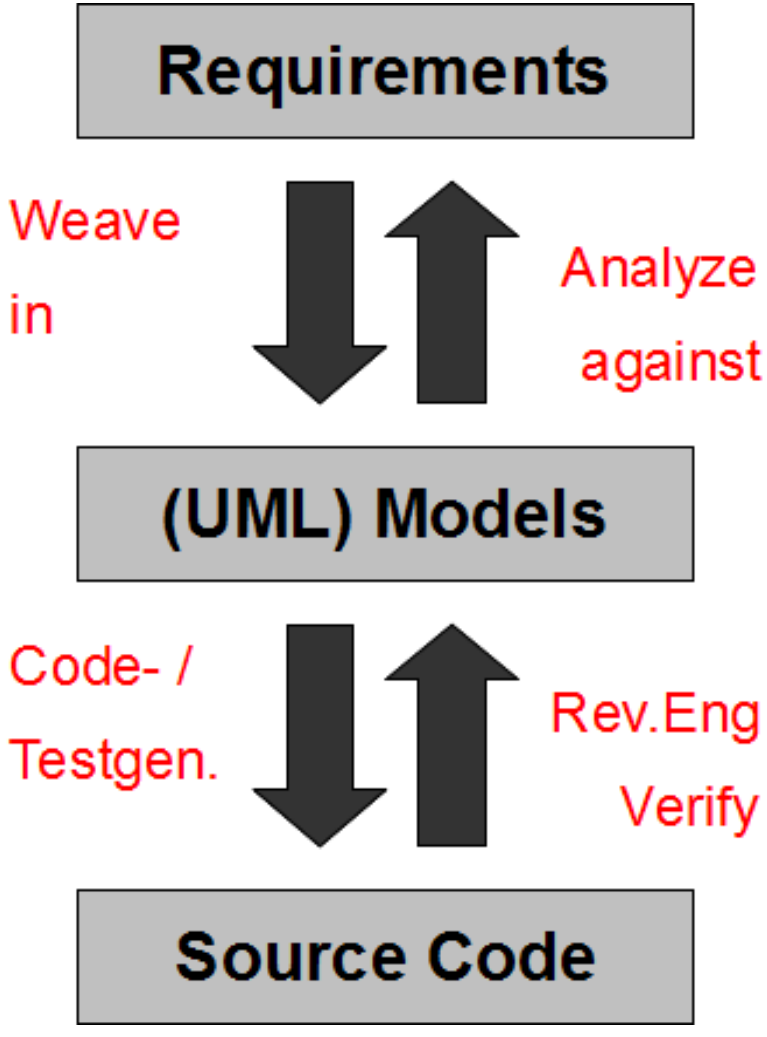
Wie soll Vorgegangen werden?
Mögliche Themen

- IT Projektmanagement
- Compliance
- Qualitätssicherung & Dokumentation
- Cloud Infrastruktur & Programming & SOA
- Requirements Engineering
- IDE & Team Developing Tools
- Modeling & Code Generation
- Testing
- Security & Testing

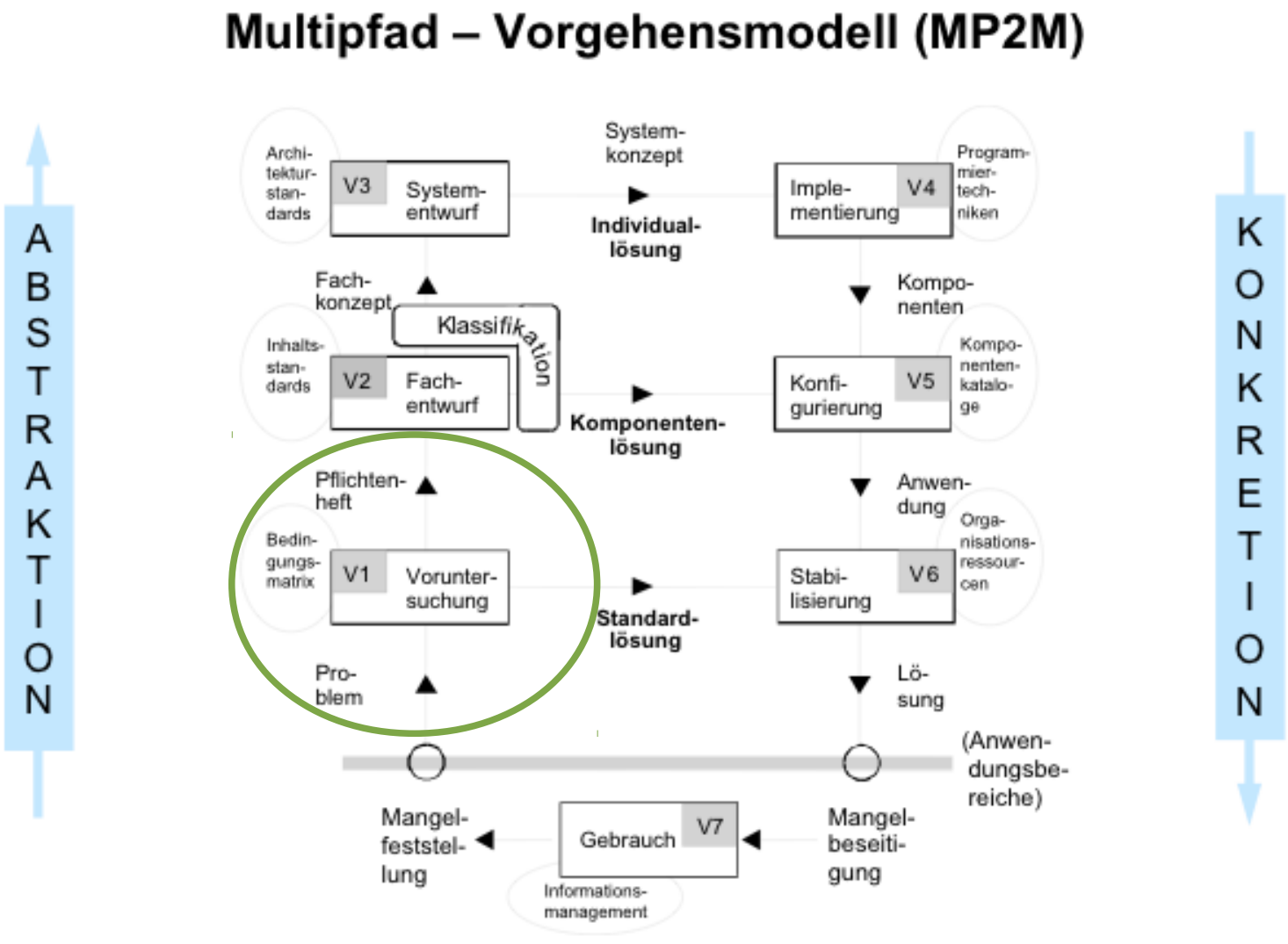
Wie soll Vorgegangen werden?
Rollen während der PG

- Jeder muss in jeder Phase arbeiten!!
- Aber:
  - Pro Phase gibt es min. einen Fachmann
  - Es gibt Phasenübergreifende Rollen
- Bsp.:
  - Projektmanager
  - Qualitätsmanager
  - Requirements Analyst
  - Softwarearchitekt
  - Testing Planner

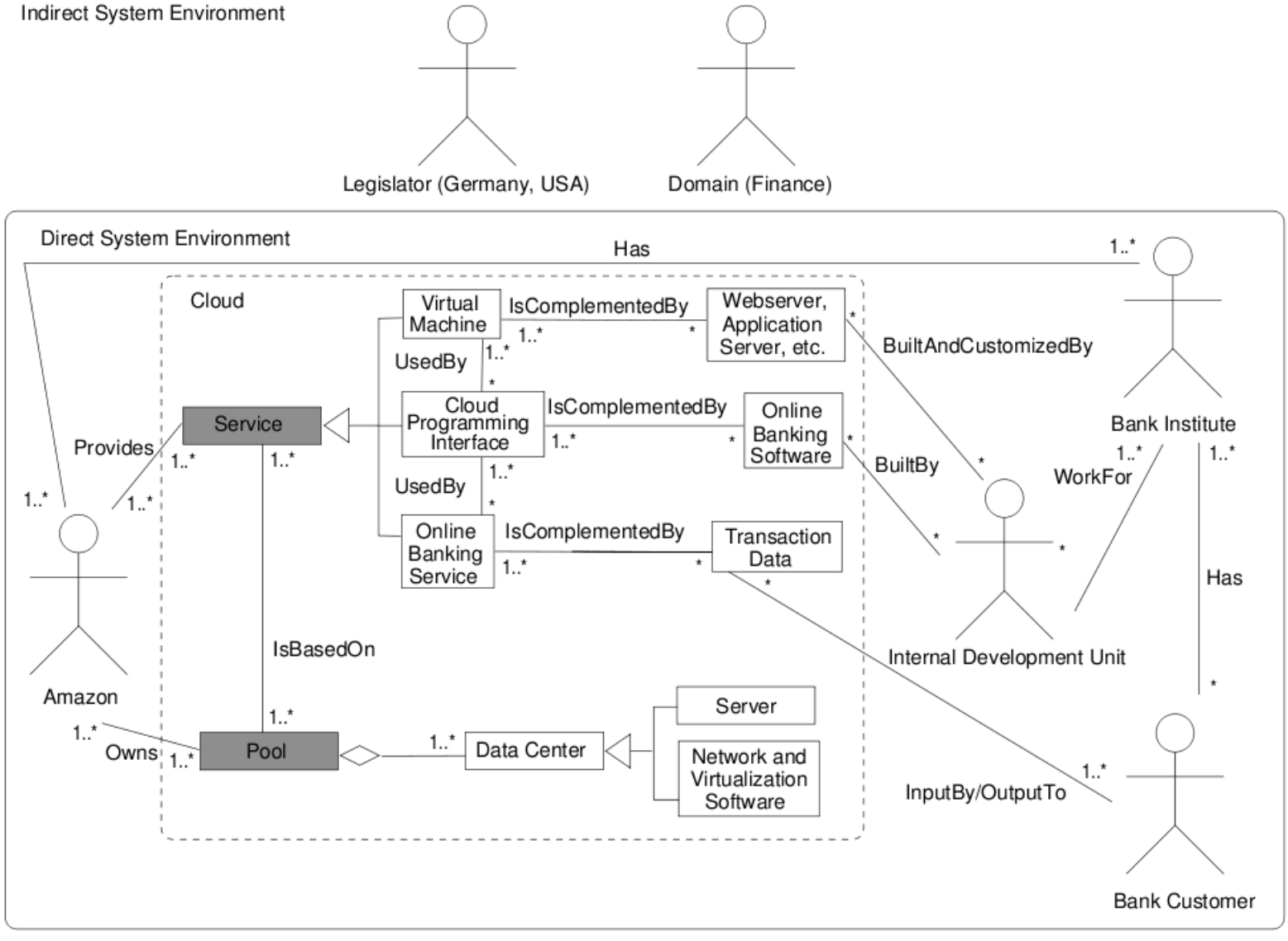
Wie soll Vorgegangen werden?
Modellbasiert



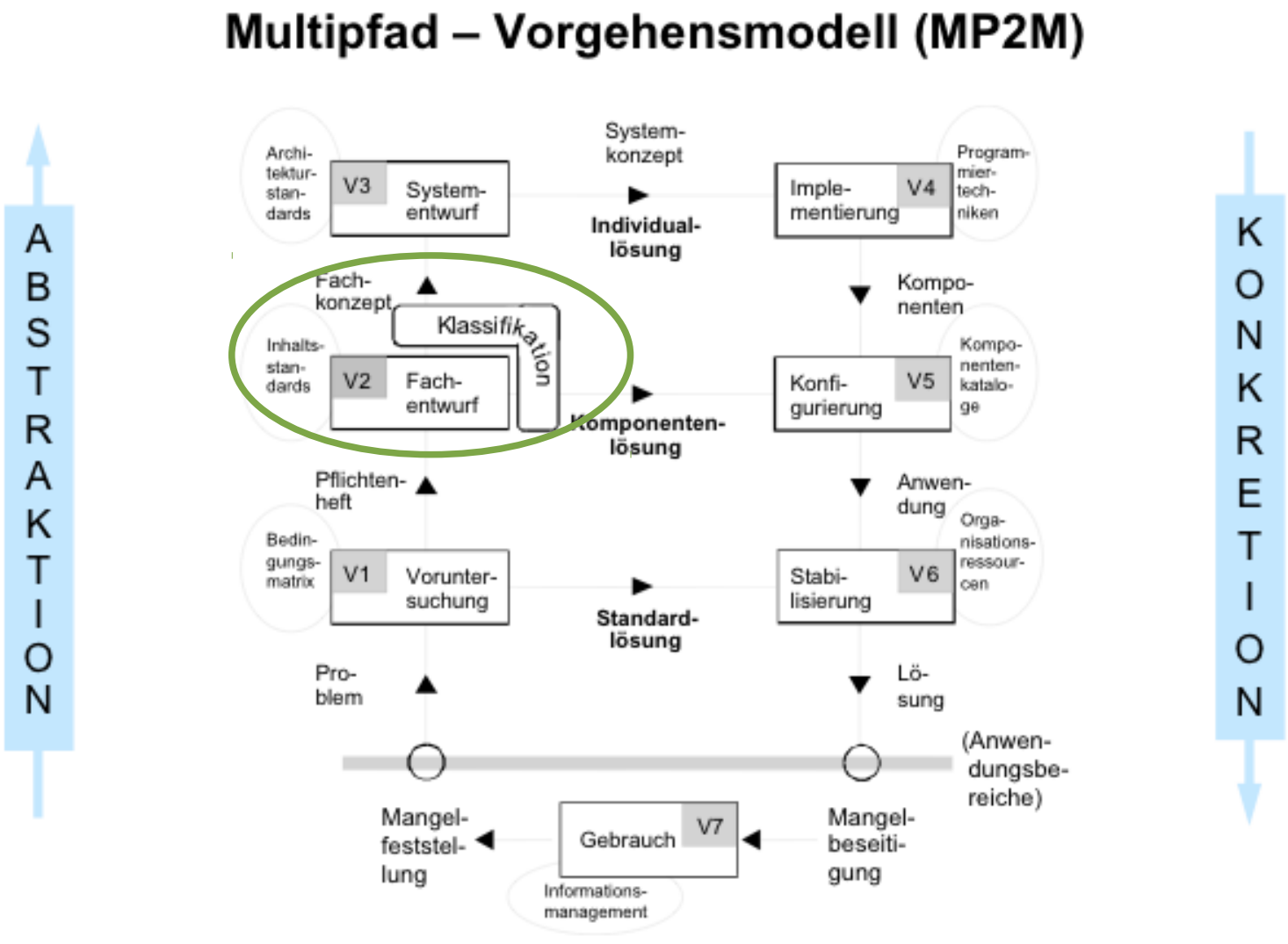
Wie soll Vorgegangen werden?
Voruntersuchung



Wie soll Vorgegangen werden?
V1: Requirements Engineering



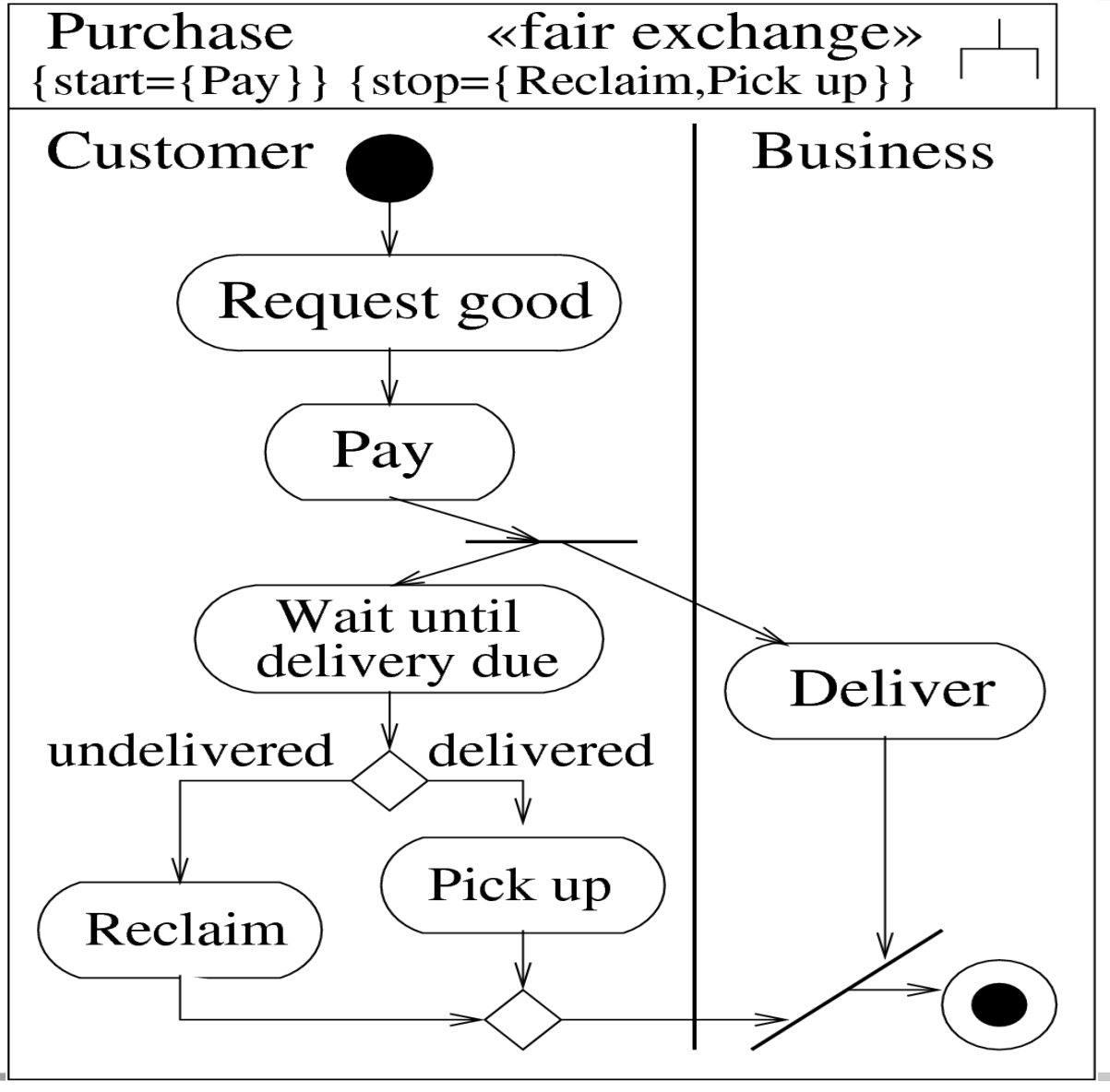
Wie soll Vorgegangen werden?
Fachentwurf



Wie soll Vorgegangen werden?
V2: Fachliche Lösungsbeschreibung

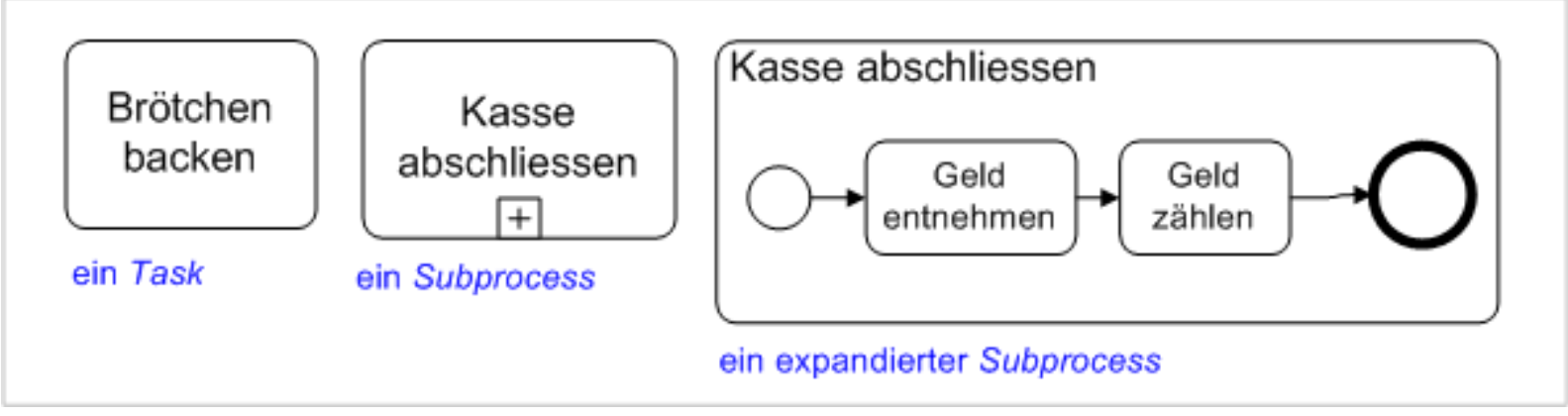
- Modelle:
  - Z.B. UML

    Aktivitätsdiagramm



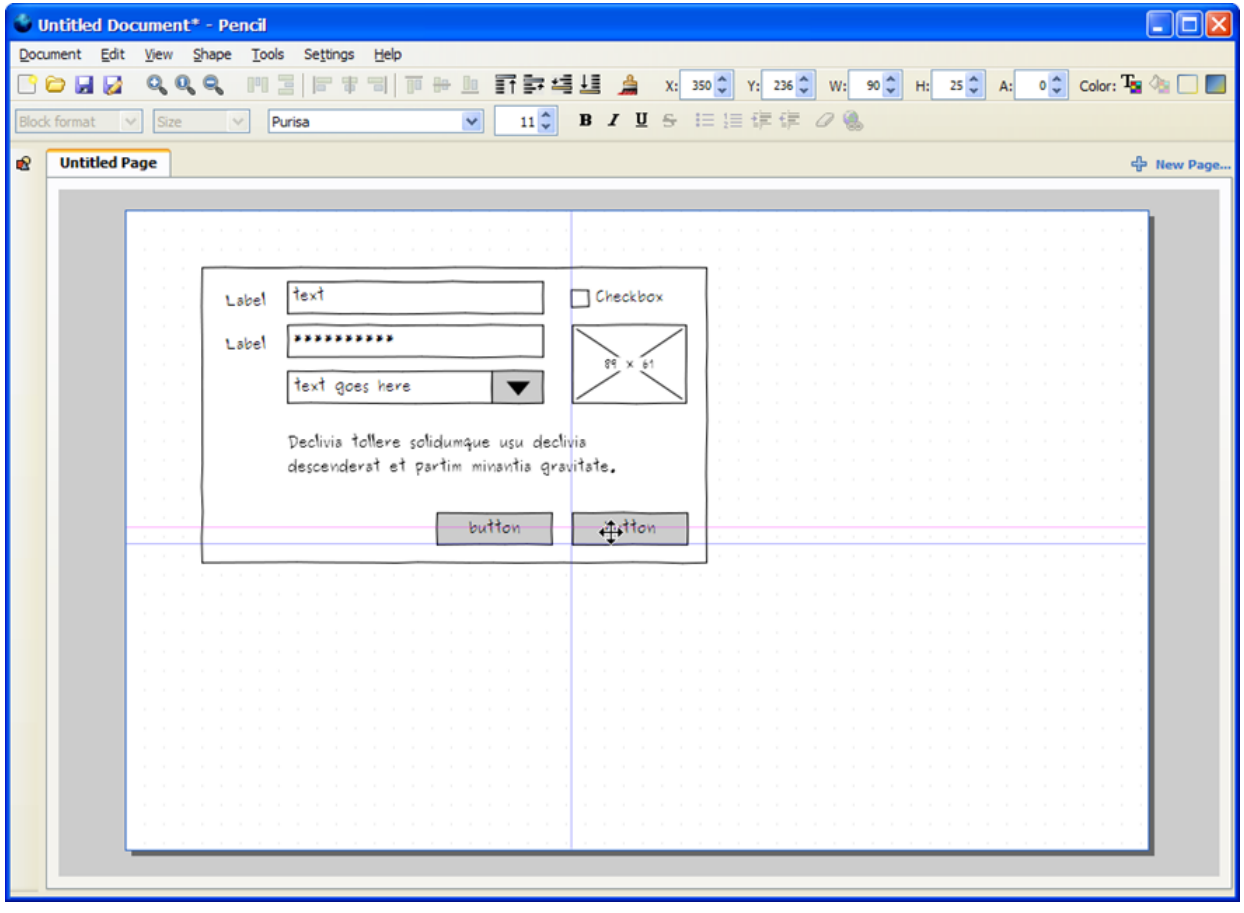
Wie soll Vorgegangen werden?
V2: Fachliche Lösungsbeschreibung

- Modelle:
  - Z.B. UML Aktivitätsdiagramm
  - Z.B. BPMN 2.0



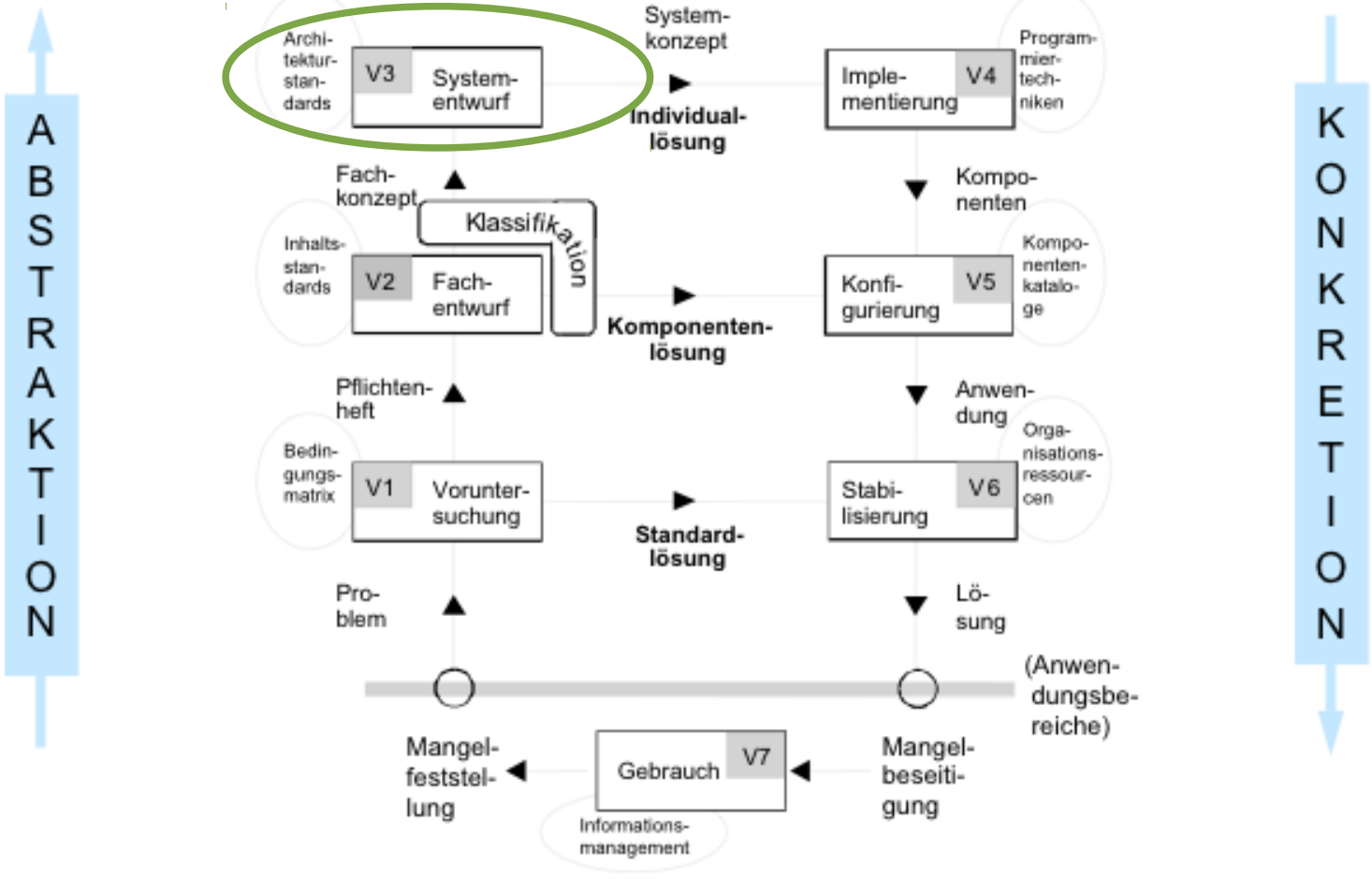
Wie soll Vorgegangen werden?
V2: Fachliche Lösungsbeschreibung

- Modelle:
  - Z.B. UML Aktivitätsdiagramm
  - Z.B. BPMN 2.0
- Mensch – Maschinen Schnittstellen
  - Z.B. GUI Prototypen



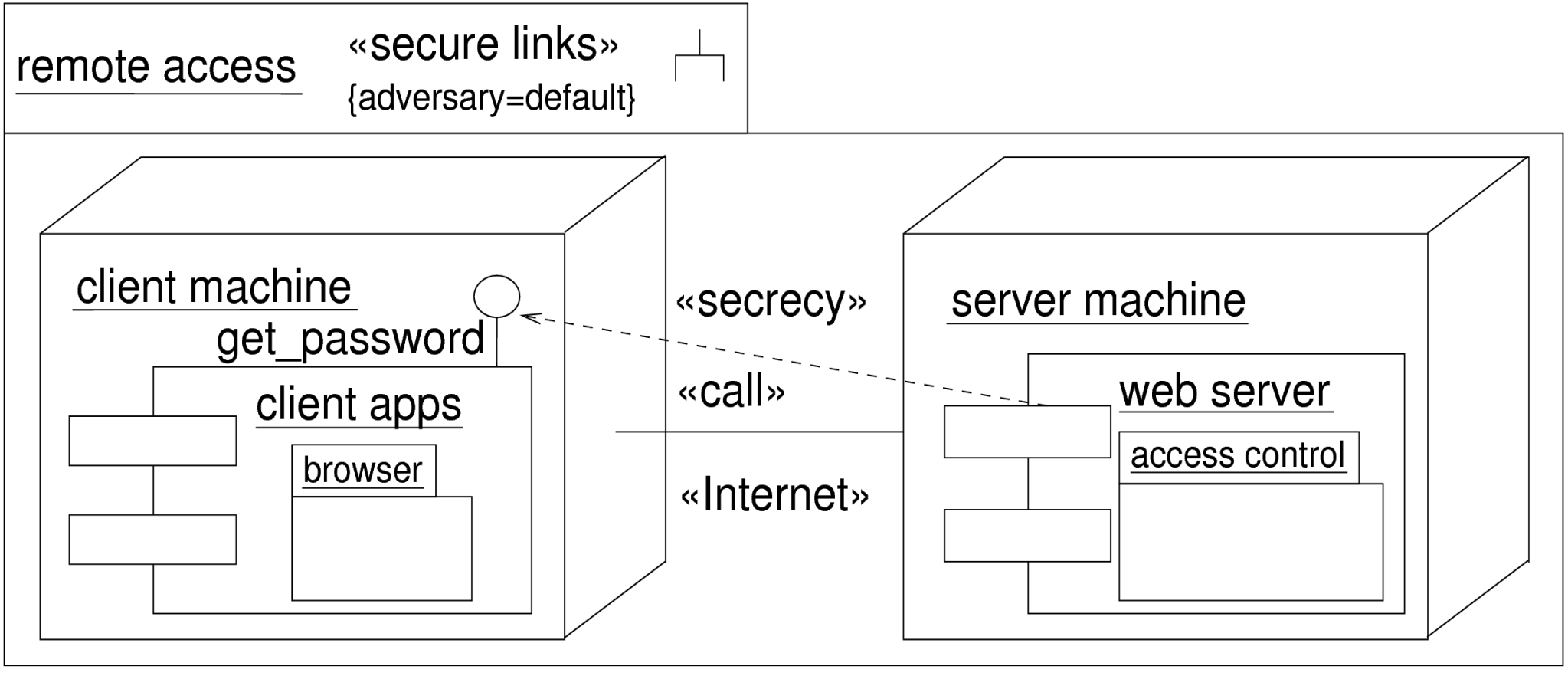
Wie soll Vorgegangen werden?
Systementwurf

Multipfad – Vorgehensmodell (MP2M)



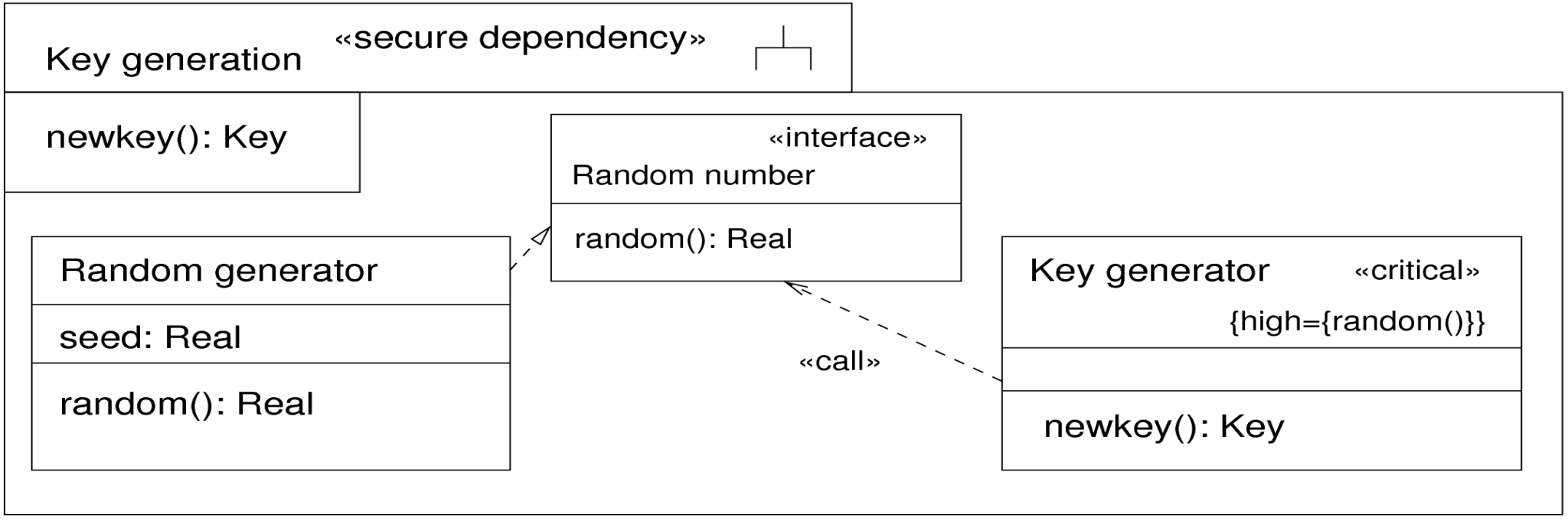
Wie soll Vorgegangen werden?
V3: Systemarchitektur & Technologiewahl

- Architekturwahl & Design
  - Z.B. SOA



Wie soll Vorgegangen werden?
V3: Systemarchitektur & Technologiewahl

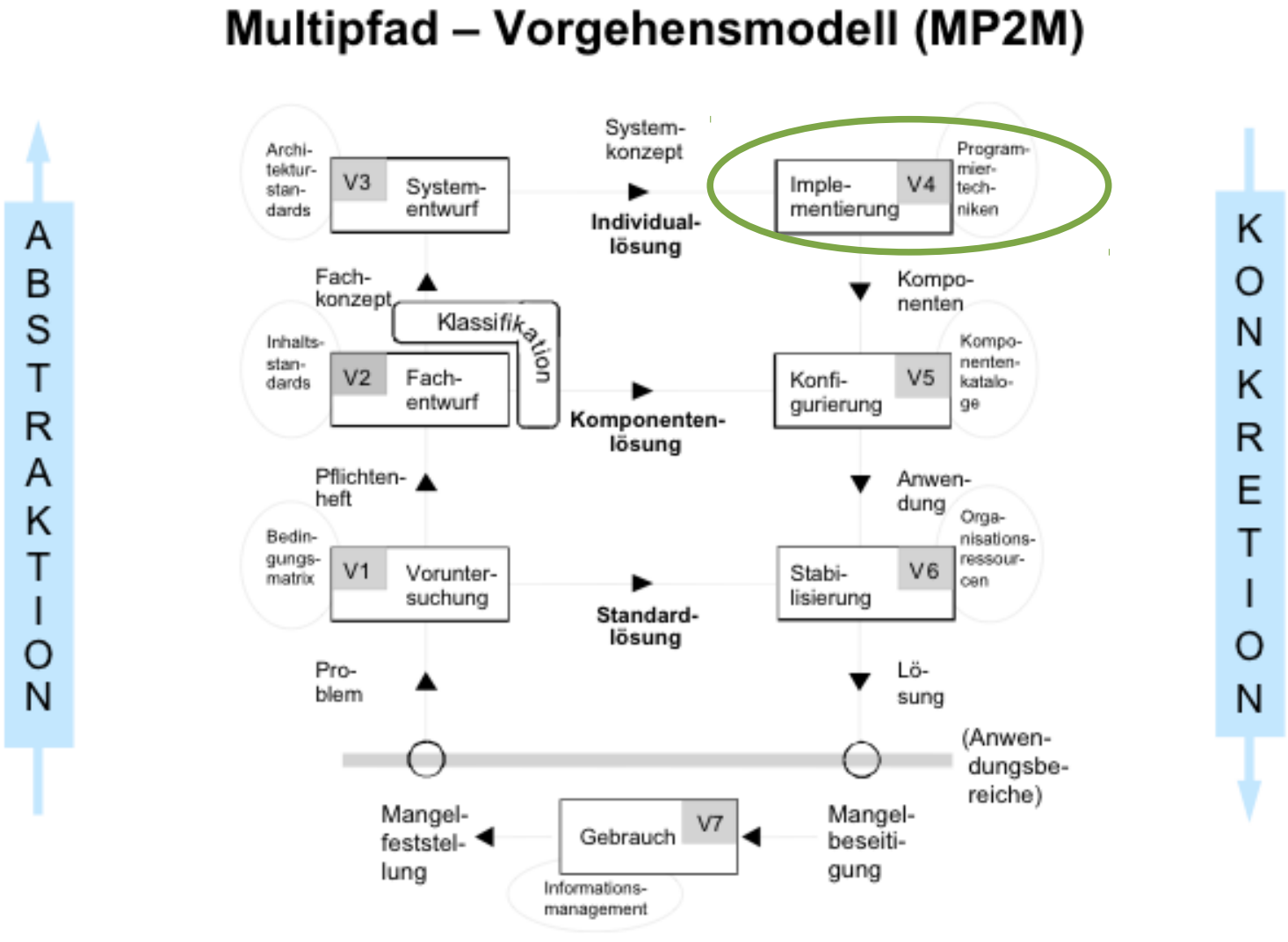
- Architekturwahl & Design
  - Z.B. SOA
- Funktions- & API-Beschreibung
  - Z.B Object-oriented



Wie soll Vorgegangen werden?
V3: Systemarchitektur & Technologiewahl

- Architekturwahl & Design
  - Z.B. SOA
- Funktions- & API-Beschreibung
  - Z.B Objectoriented
- Protokollwahl
  - Z.B. SOAP oder REST
- Datenrepository & Repräsentation
- Programmiersprache & Frameworks

Wie soll Vorgegangen werden?
Implementierung



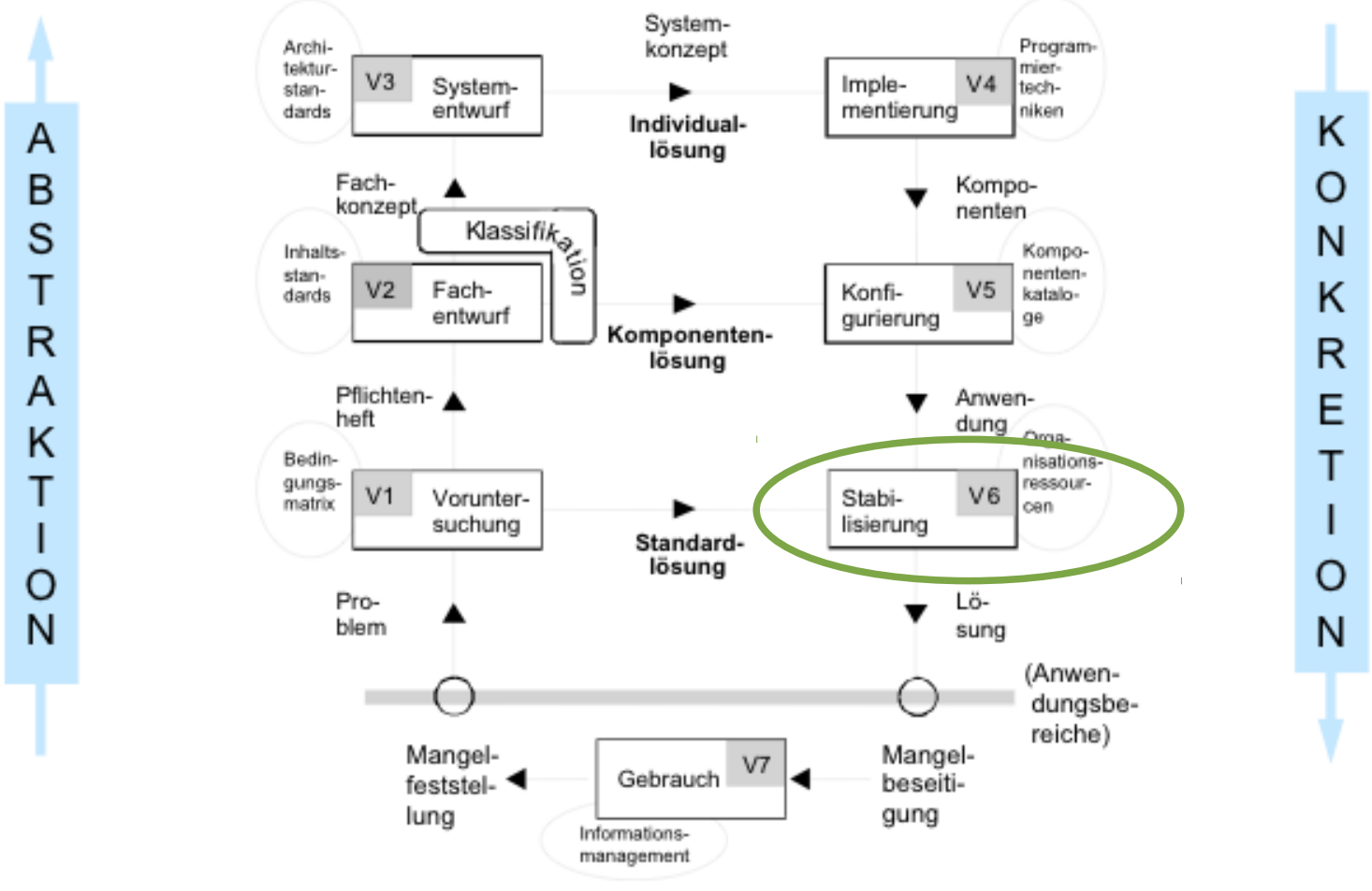
Wie soll Vorgegangen werden?
Implementierung

- Automatische Generierung
  - von Code (z.B. UML Klassenmodellen)
  - von Protokollabläufen (z.B. aus Sequenzdiagrammen)
- Protokollspezifikation
  - zum verbinden der Architekturteile
- Programmieren unter Nutzung
  - der gewählten Cloud API
  - der gewählten Datenrepräsentation
  - der gewählten Frameworks

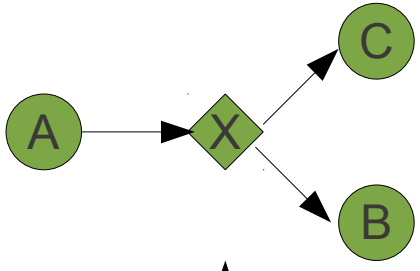
Wo liegt der Fokus?

1. Das Thema
2. Das Vorgehen
3. Die Schwerpunkte
4. Die Werkzeuge
5. Das Organisatorische

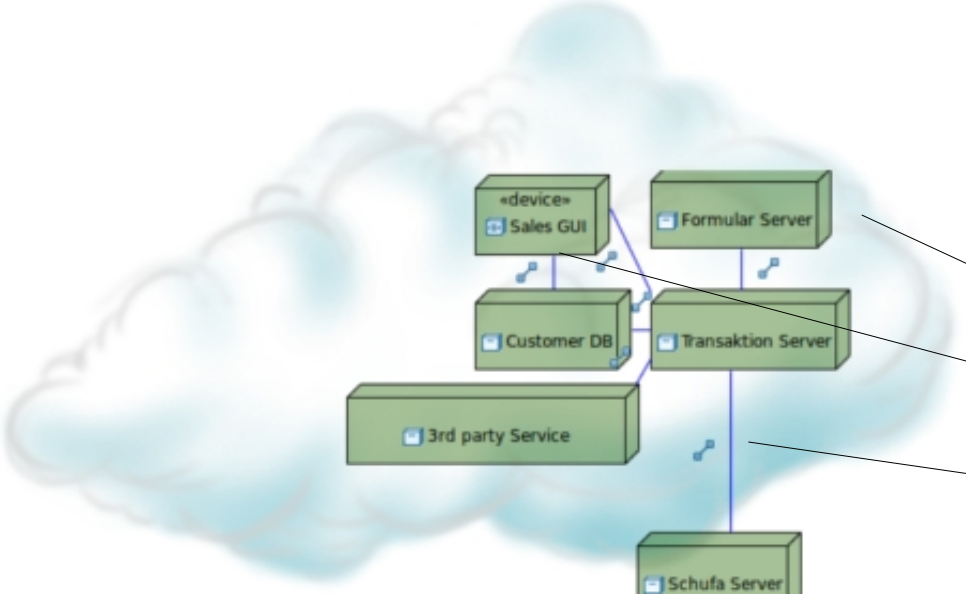
Wo liegt der Fokus?
Implementierung

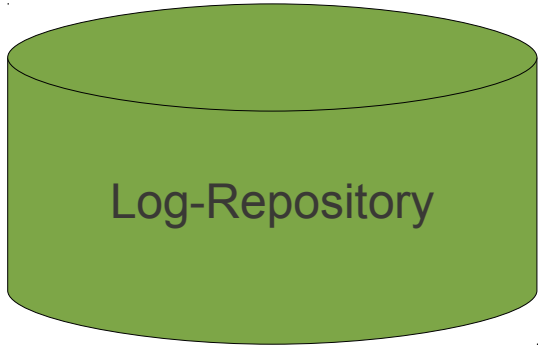


Wo liegt der Fokus?
Processmining



Prozess ID	Aktivitäts ID	Bearbeiter	Zeitstempel
1	A	John	9-3-10:15.01
2	A	Mike	9-3-10:15.12
1	B	Mike	9-3-10:16.07
2	C	Carol	9-3-10:18.25





Wo liegt der Fokus?
Testing & Security

- Testen während der Erstellung
  - WhiteBox z.B. Code Verification, ModelChecking
  - Greybox z.B. JUnit
  - BlackBox z.B. Code Fuzzer
- Test zur Laufzeit
  - BlackBox z.B. API / GUI Fuzzer
- Fokus auf Security
  - Penetration Testing
    - Insider / Outsider Attack
  - Protokollanalyse

Was soll genutzt werden?

1. Das Thema
2. Das Vorgehen
3. Die Schwerpunkte
4. Die Werkzeuge
5. Das Organisatorische

Was soll genutzt werden?

- Professionelle Cloudumgebung (Beteiligung an der neuen Cloud-Infrastruktur der Fak. Informatik)
  - z.B. Google App Engine oder Amazon EC2
- Cloud APIs und Frameworks
  - z.B. Google Web Toolkit
- State of the Art Modellierungswerkzeuge
  - EMF basiert z.B Papyrus oder Fujaba
- Standard Programmierwerkzeuge
  - IDE: Eclipse
    - + Plugins (FindBugs, MyLyn, CheckStyle...)
  - Versionskontrolle: z.B. SVN




Sonst noch was?

1. Das Thema
2. Das Vorgehen
3. Die Schwerpunkte
4. Die Werkzeuge
5. Das Organisatorische

Sonst noch was?
Voraussetzungen

- Vgl. PG-Infoheft.
- Softwaretechnik (V)
- Kenntnisse in objektorientierter Programmierung (V)
- Mensch-Maschine-Interaktion , Modellgestützte Analyse und Optimierung , Formale Methoden des Systementwurfs (M)
- Kenntnisse in UML (W)
- Kenntnisse in UMLsec (W)
- Kenntnisse in Cloud-Entwicklung (W)
- Kenntnisse in Sicherheitstesten von Software (W)

Sonst noch was?
Minimalziel

- Konzeption einer Cloud-basierten Internetbanking-Anwendung
- Prototypische Realisierung der Konzepte
- Sicherheitsevaluation der implementierten Systeme
- Soll- und Ist-Vergleich der ausgeführten Prozesse mittels Business Process Mining
- Erstellung eines Endberichts
- Fachgespräch

Sonst noch was?
Wann und wo geht es weiter?

- Anmeldung bis 1.12.2010
- Erstes PG Meeting im Januar
- Betreuer:
  - Prof. Jan Jürjens
  - Dr. Holger Schmidt
  - Stephan Faßbender
- In Zusammenarbeit mit dem Fraunhofer ISST Projekt APEX
- Weitere Informationen
  - http://inky.cs.tu-dortmund.de/main2/jj/teaching/pg/securecloudbanking