technische universität
dortmund

Vorlesung (WS 2014/15)

Sicherheit:
Fragen und Lösungsansätze

Dr. Thomas P. Ruhroth

TU Dortmund, Fakultät Informatik, Lehrstuhl XIV

Vorlesungswebseite (bitte notieren):

http://www-secse.cs.tu-dortmund.de/secse/pages/teaching/ws14-15/sfl/index_de.shtml

0. Organisatorisches und Einleitung

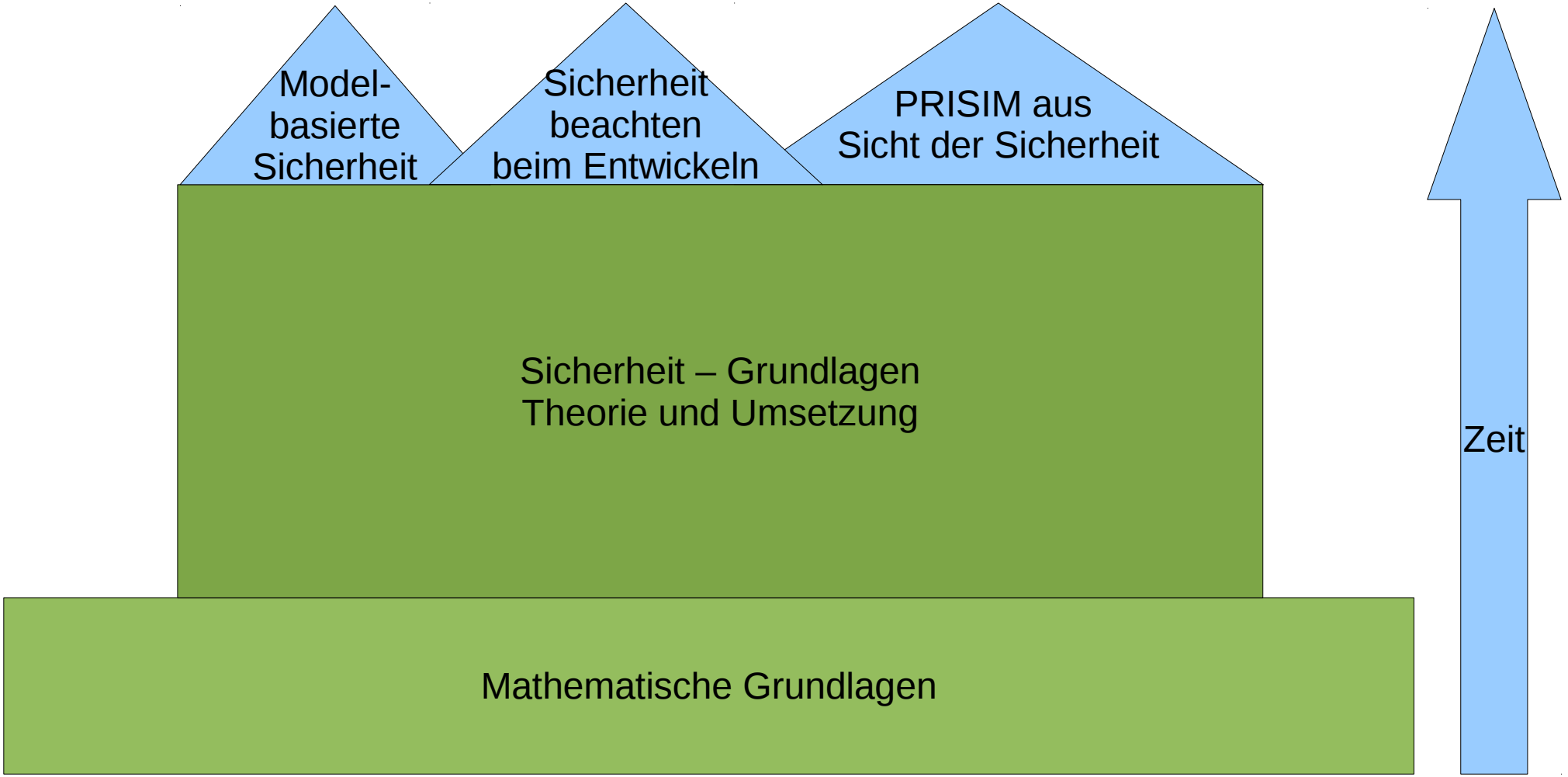
Agenda

- Organisatorisches
- Studienordnung: Einordnung / Kompetenzen / Struktur / Prüfung
- Vorlesung: Bildungsvertrag, Termine, Feedback
- Übung: Konzept / Termine
- Prüfung

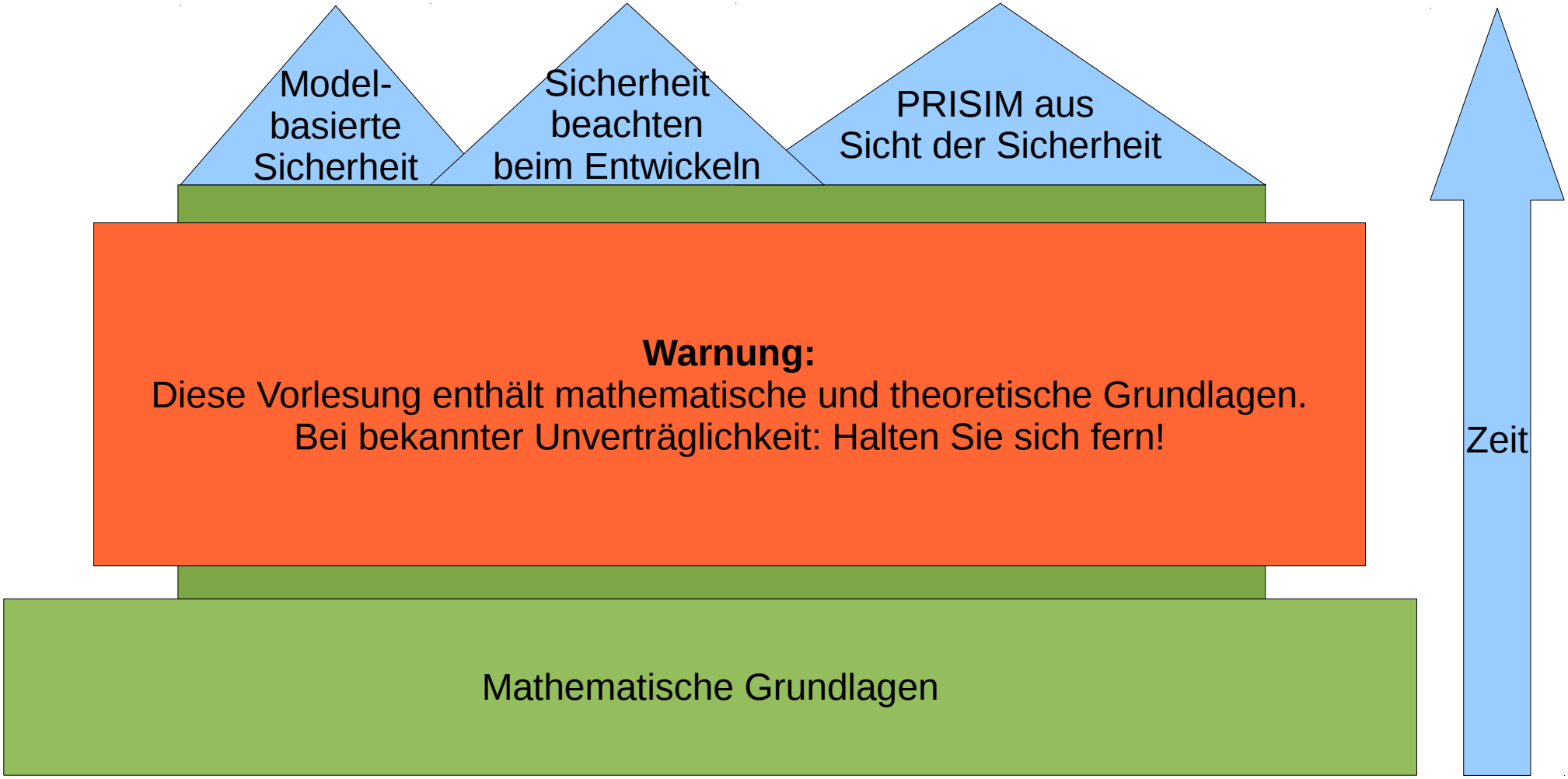
- Vorstellung des Fachgebietes

- Vorlesungsinhalte

Grobstruktur der Vorlesung



Grobstruktur der Vorlesung



Studienordnung
Einordnung

Bachelor Informatik / Angewandte Informatik

- **Wahlmodul**

Diplom Informatik

- **Spezialvorlesung**, Schwerpunktgebiete: 1 (Software-Konstruktion),
  3 (Verteilte Systeme), 5 (Sicherheit und Verifikation)

Master of Science „Datenwissenschaft“

- **Exportveranstaltung**

Studienordnung
vermittelte Kompetenzen

Studierende sollen **Fragen** zur Sicherheit umfassend verstehen und gängige **Lösungsansätze** mitsamt Nachweise der **Wirksamkeit** kennen und anwenden können.

Sie sollen weitergehende **Lösungsvorschläge** im Hinblick auf Sicherheitseigenschaften eigenständig untersuchen und **bewerten** können.

Achtung: mathematische und formale Grundlagen der o.g. Fragestellungen.

Studienordnung
Struktur laut Modulhandbuch (Bachelor)

3 SWS:

- 2 SWS Vorlesung
- 1 SWS Übung

4 Credits:

- 3 Credits Vorlesung
- 1 Credits Übung

Aufwand 120 Stunden über 15 Semesterwochen:

- 45 Stunden Präsenz (15*(2+1))
- 75 Stunden Vor-/Nachbereitung und Hausübungen (15*5)

Veranstaltungssprache Deutsch.

Vorlesung

Mi. 10:15 bis 11:45 Otto-Hahn-Str. 14 – 104

Übungen

Gruppe I&II: Mittwochs, 16:15 - 17:45, OH14 - 104

Bitte Plan auf der Webseite beachten!

1. Übung am 15. Okt 2013 (I) bzw. 22. Okt 2013 (II)

Anmeldung **AsSESS**:

- http://ess.cs.uni-dortmund.de/ASSESS/index.php?do=lecturelist
  Anmeldung **nach der heutigen Vorlesung** möglich.
- Verteilung wird am Freitag bekannt gegeben.

http://www-secse.cs.tu-dortmund.de/secse/pages/teaching/ws14-15/sfl/index_de.shtml

Feedback

Wir **bitten um vorlesungsbegleitendes Feedback**, um Verbesserungen Semester-begleitend durchführen zu können.

Übliche **Kontaktmöglichkeiten**:

- Nach der Vorlesung
- http://www-secse.cs-tu-dortmund.de/staff/ruhroth
- Anonymes Kontaktformular:
  http://www-secse.cs.tu-dortmund.de/secse/pages/teaching/feedback_de.shtml
  (s. Link von Vorlesungswebseite). SFL ankreuzen

Präsenzübung

Aufbau:

- 1/3 Besprechung der Heimübungen und Fragen zur Vorlesung
- 2/3 Aktive Übungen
  - Gruppenarbeiten
  - Simulationen (z.B. der Prüfungssituation, Problemlösung)

Präsenzübung II

- Gemeinschaftliches Erarbeiten und Vertiefen
- Erleben von Problemen in Simulationen
- Kennenlernen von Methoden für die Moderation und Erarbeitung von Ergebnissen
- Kommunikationshemmung der Informatiker brechen

Hausübungen

6 Übungszettel

- Abgabetermine sind strikt!
- **Gruppen** von max. 3 Studierenden
  Inhaltliche und konzeptionelle Zusammenarbeit sind entsprechend auf den Abgaben zu vermerken.
- **Abgabe**
  - im Briefkasten 52
  - Am Anfang der Vorlesung
  - Abgaben per Mail werden ignoriert
    - Außer es ist Teil der Aufgabe und ist explizit in der Aufgabe bemerkt!

Leistungsnachweis

Jede Hausübung wird auf **10 Punkte umgerechnet**.

- Diplom-Studierende nach DPO 2001
  - erhalten einen unbenoteten Schein durch erfolgreiche Teilnahme an der Prüfung.
  - Teilnahme an den Übungen und Hausübungen ist freiwillig.
- Bachelor-Studierende
  - benötigen für die Zulassung zur Klausur einen Leistungs-Nachweis über die erfolgreiche Teilnahme an den Übungen
  - **50%** der Punkte aus den **Hausübungen**
  - UND mindestens jeweils **30%** der Punkte aus den **Aufgaben 1+ 2 + 3 und 4 + 5 + 6**

Punktsysteme

- Bearbeitungspunkte (BP)
  - explorative Aufgaben
- Leistungspunkte (LP)
  - Übungsaufgaben

Inpud-Forum

- **Diskussion** der Studierenden untereinander
- **Inhaltliche Fragen**
  - Inhaltliche Fragen **per Mail an mich** werden ignoriert
  - Beantworte Fragen 2-3 Mal die Woche im Inpud
- Organisatorische Fragen
  - Wenn allgemein interessant → Inpud
  - Wenn persönlich → **Mail** oder **nach der Vorlesung**.
- Moderation durch Veranstalter

Studienordnung
Prüfungen

Modulprüfung: **Klausur (90 Minuten)** oder **mündliche Prüfung** (20-30 Minuten) gemäß Ankündigung nach Beginn der Veranstaltung (=> nächste Woche).

Leistungsnachweise:

- Diplom-Studierende nach DPO 2001 erhalten einen unbenoteten Schein durch erfolgreiche Teilnahme an der Prüfung.
  - Die Teilnahme an den Übungen und die Abgabe von Hausübungen sind freiwillig.
- Bachelor-Studierende benötigen für die **Zulassung** zur Prüfung/Klausur einen Leistungsnachweis über die **erfolgreiche Teilnahme an den Übungen**.

Folien

- Folien werden nach der Vorlesung online gestellt.
  - Dramaturgie
- Folienzeichen

Folienzeichen

Dies Folie wird nicht online gestellt

Sofort lernen, wichtige Grundlage ohne die weitere Themen nicht verständlich sind.

Diese Folien sind für die Nacharbeit und werden nicht in der Vorlesung ausführlich behandelt.

Diese Folien sind ein nicht prüfungsrelevant.

Unsere Arbeitsgruppe
Software Engineering für kritische Systeme

Vertrauenswürdige IT-Systeme

IT Systeme durchziehen fast alle Funktionen in Wirtschaft und Gesellschaft.

IT hat direkten (oft invasiven) **Einfluss auf fast alle Aspekte** menschlichen Lebens.

Erwartungen an Vertrauenswürdigkeit der Systeme daher in letzten 10 Jahren **stark gestiegen**.

Diese Erwartungen **werden oft nicht erfüllt**.

Teil des Problems: bislang verwendete System- und Software-**Entwicklungsmethoden** konnten mit gestiegenen Erwartungen bei gleichzeitig steigender Systemkomplexität nicht mithalten.

Offene Systeme

Aus Flexibiliäts- und Kostengründen:
Moderne IT Systeme meist über **offene Infrastrukturen** realisiert.

Zum Beispiel:

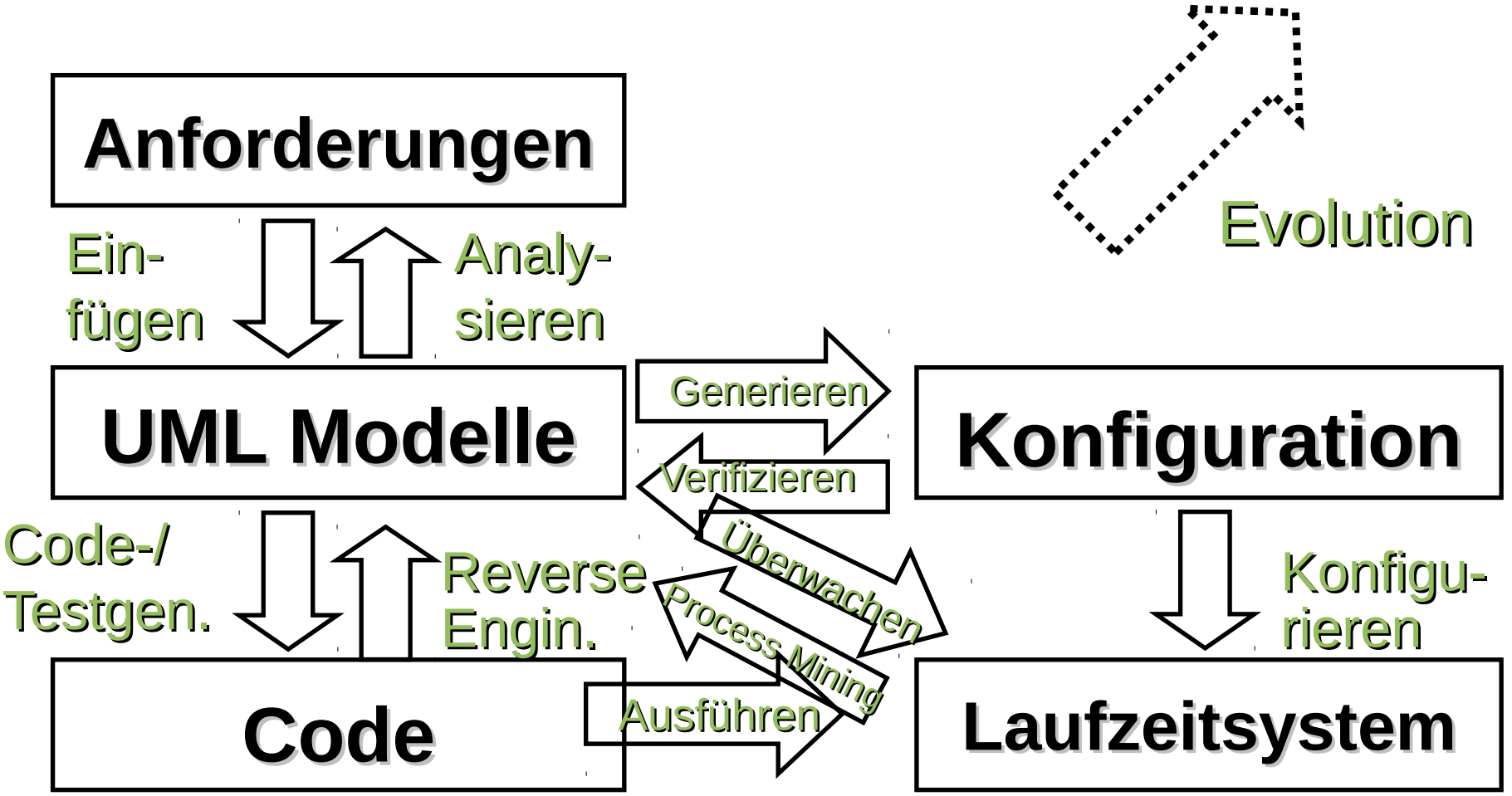
- Internet
- Mobile Netze

Sie sind somit dem **Zugriff** von Personen ausgesetzt, die in **nicht unbedingt vertrauenswürdig** sind.

Zugriff muss daher **systemseitig reguliert** werden. Aus Flexibilitäts- und Kostengründen oft auf Softwareebene gelöst.

Vertrauenswürdige **IT braucht also sichere Software**.

Modellbasierte Entwicklung



Beispiel-Themen für Abschlussarbeiten

- Modellierung und Automatische Sicherheits-Analyse für Cloud Computing Systems
- Business Process Mining
- Spezifikation von IT-Sicherheitszielen für die Geschäftsprozessmodellierung und deren Integration in die Ausführung im Workflow
- Werkzeuggestützte Modell-basierte Sicherheitsanalyse
- Werkzeugunterstützte Analyse von sicherheitskritischen SAP-Berechtigungen im Finanzbereich
- Modell-basiertes Return on Security Investment (ROSI) im IT-Sicherheitsmanagement

Informationen unter:

http://www-secse.cs.tu-dortmund.de/secse/pages/teaching/thesis/index_de.shtml

Hiwi-Tätigkeiten

Hiwi-Jobs am Fraunhofer ISST oder LS 14 / TUD:

- Unterstützung von **Forschungs-Projekte** (z.B.: "Architectures for Auditable Business Process Execution (APEX)", Seconomics, SecVolution, ClouDAT):
  z.B. Java-Programmierung für UML-Analyse-Werkzeug, konzeptuelle Arbeiten zu modellbasierter Sicherheitsanalyse
- Unterstützung in der **Lehre** (Tutorien, Folienerstellung etc)

Weitere Informationen:

http://www-secse.cs.tu-dortmund.de/secse/pages/home/jobs_de.shtml

Bei Interesse **bitte bei mir melden** !

Weitere Lehrveranstaltungen

Dieses Semester:

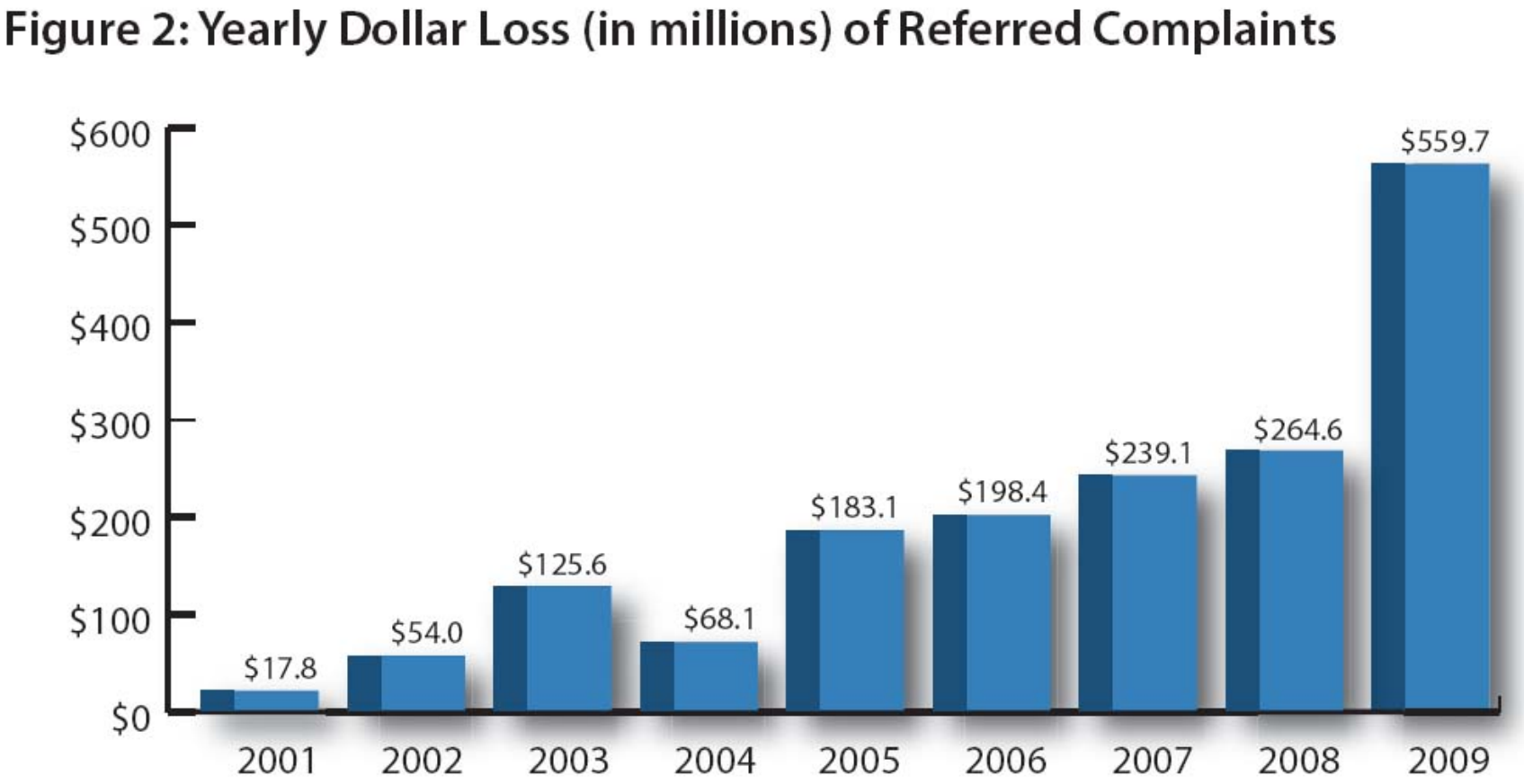
- **Seminar „Sicherheit und Softwareengineering“**:
  http://www-secse.cs.tu-dortmund.de/secse/pages/teaching/ws13-14/mbse-sem/index_de.shtml

  Bei Interesse **bitte bei mir melden**.
- **Vorlesung „Softwarekonstruktion“.**
  http://www-secse.cs.tu-dortmund.de/secse/pages/teaching/ws13-14/swk/index_de.shtml

- Proseminar: Plätze bereits vergeben.

Vorlesungsinhalte

Warum ist dies Ihre wichtigste Vorlesung in diesem Semester ?



[2009 Internet Crime Report, US Dep. Of Justice
www.securityprivacyandthelaw.com/
uploads/file/2009_IC3Report.pdf]

Beispiel (2010): Virusangriff auf Iranisches Nuclearprogramm

http://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html

Stuxnet was work of U.S. and Israeli experts, officials say

A damaging cyberattack against Iran’s nuclear program was the work of U.S. and Israeli experts and proceeded under the secret orders of President Obama, who was eager to slow that nation’s apparent progress toward building an atomic bomb without launching a traditional military attack, say current and former U.S. officials.

The origins of the cyberweapon, which outside analysts dubbed Stuxnet after it was inadvertently discovered in 2010, have long been debated, with most experts concluding that the United States and Israel probably collaborated on the effort. The current and former U.S. officials confirmed that long-standing suspicion Friday, after a New York Times report on the program. […]

Overall, the attack destroyed nearly 1,000 of Iran’s 6,000 centrifuges — fast-spinning machines that enrich uranium, an essential step toward building an atomic bomb. The National Security Agency developed the cyberweapon with help of Israel.

Beispiel (2011): Hacker attackieren den Währungsfond

http://www.zeit.de/digital/datenschutz/2011-06/hacker-iwf-wirtschaftsdaten

Hacker haben den Internationalen Währungsfonds angegriffen und offenbar Daten gestohlen. Der IWF geht von Spionage aus und macht eine "bestimmte Regierung" verantwortlich.

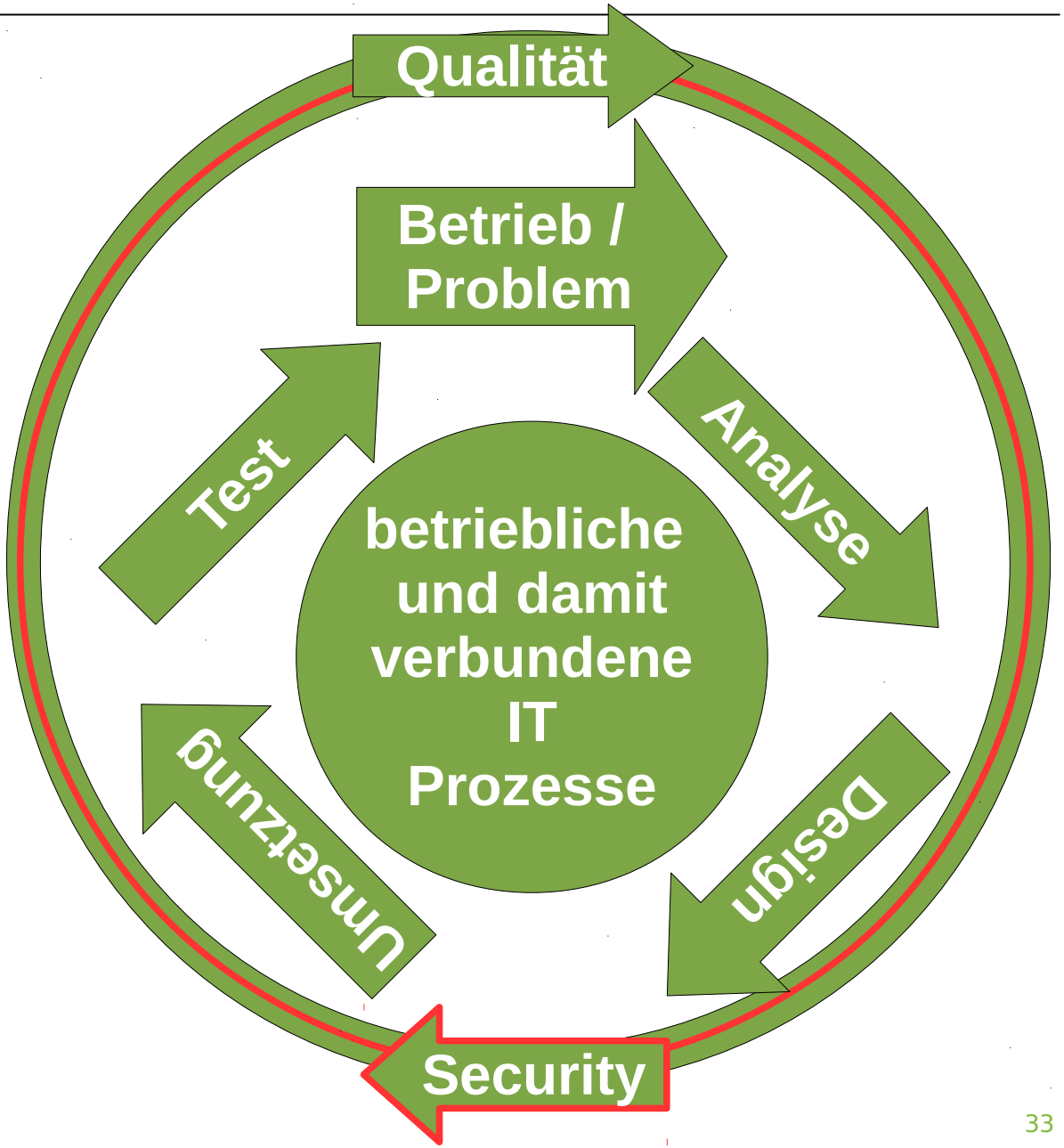
Der Internationale Währungsfonds (IWF) ist Opfer einer Attacke auf seine Computer geworden. Nach einem Bericht von Bloomberg News wurden bei dem Angriff E-Mails und weitere Dokumente gestohlen. Der Fonds habe Ermittlungen eingeleitet, wie es zu dem Hacker-Angriff kommen konnte, erklärte ein IWF-Sprecher. Die Arbeit der Organisation sei durch den Angriff aber nicht beeinträchtigt. Über das Ausmaß des Schadens machte der Sprecher keine Angaben. [...]
Nach Angaben des Internet-Sicherheitsexperten Tom Kellermann, der in dieser Funktion auch für den IWF und die Weltbank gearbeitet hat, zielte der Hackerangriff darauf, heimlich eine Software zu installieren, um einer bestimmten Regierung Zugang zu Insider-Informationen des IWF über andere Länder zu verschaffen. Um welche Regierung es sich handle sei noch unklar.

Mehr Beispiele: Einige der größten Schäden durch Cyber-Angriffe

http://www.businesspundit.com/10-most-costly-cyber-attacks-in-history

2011: Exposure of over 100 million PlayStation Network and Sony Online Entertainment accounts is forging a new chapter in the history of cyber-attacks. The personal information — including credit and debit card data — of tens of millions of users was stolen by an as yet unknown group of assailants. Experts predict that the damage may range from $1 to $2bn, making it possibly the costliest cyber-hack ever to have been pulled off.
2008: Trusted payments processor Heartland Payment Systems fell victim to a plot to steal credit and debit card numbers. By secretly infesting the company's computer network with spyware, the criminal gang responsible were able to steal over 100 million individual card numbers. The episode ended up costing around $140m.
2007: Grocery retailer Hannaford Bros suffered a four-month long breach of their security from the winter of 2007 to the spring of 2008. During this period, over 4.2 million credit and debit card numbers were exposed, along with other sensitive information. Experts table the costs incurred at an estimated $252m.
2005: Massachusetts-based retailing company TJX was attacked by a gang able to get their hands on over 45 million credit and debit card numbers, a selection of which they then used to fund a multi-million dollar spending spree from Wal-Mart's stock of electronics equipment. The damage from the data-breach ended up costing over $250m in total.
2004: Sven Jaschan unleashed a virus which infected millions of computers around the world, reaching its highest degree of destruction when it comprehensively disabled the Delta Air Lines computer system, causing the cancellation of several transatlantic flights. Jaschan was eventually arrested after a three-month hunt, during which Mircosoft placed a $250,000 bounty on the hacker's head. An estimated $500 million worth of damage was generated.
2000: 15-year-old Michael Calce conducted notorious attacks against huge companies with high levels of security. Amongst those attacked were computer manufacturer Dell, media giant CNN, and shopping sites Amazon and Ebay. Prosecution for the estimated $1.2bn worth of damage caused went pretty smoothly, from Calce's perspective. He ended up with a sentence of eight months open custody.

Sicherheit von IT-Systemen



Themen der Vorlesung

Kapitel 1: Einleitung

Kapitel 2: Math. Grundlagen (Wiederholung)

Kapitel 3: Kryptographische Grundlagen

Kapitel 4: Hashfunktion, Signatur und Schlüsselaustausch

Kapitel 5: Authentifikation

Kapitel 6: Zugriffs- und Informationsflusskontrolle

Kapitel 7: Sicherheitsprotokolle

Kapitel 8: Sicherheit im Licht der NSA

Kapitel 9: Security Engineering

Kapitel 10: Sicherheit beachten beim Programmieren

Literatur: Teil 1-6

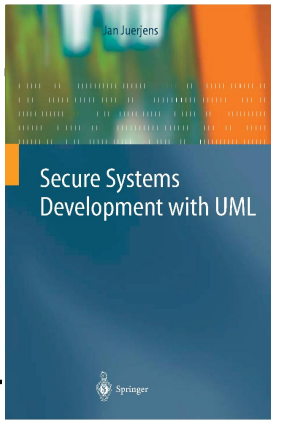
Claudia Eckert: **IT-Sicherheit: Konzept - Verfahren - Protokolle**, 7., überarb. und erw. Aufl., Oldenbourg, 2012.

- E-Book:
  http://www.ub.tu-dortmund.de/katalog/titel/1362263
  und
- Print-Version:
  http://www.ub.tu-dortmund.de/katalog/titel/1343058
  Bei Engpässen in der Ausleihe von letzterer gibt es auch noch ältere Ausgaben (6., 5., 4., 2. und 1. Auflage, s. Webseite.)

Literatur: Teil 8

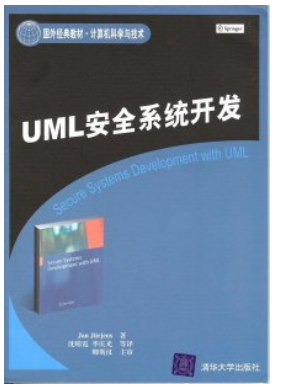
Hintergrundliteratur:

- Jan Jürjens, **Secure Systems Development wi**
  UML, Springer-Verlag 2005, s. http://umlsec.de



Vorhanden in der Universitätsbibliothek als:

- E-Book (http://www.ub.tu-dortmund.de/katalog/titel/1361
- Print-Version
  (http://www.ub.tu-dortmund.de/katalog/titel/1091324 ,
  Signaturen L Sr 531 bis L Sr 531+4)



Feedback, Vorlesungsanpassung und Startfragebogen

Wieso eigene Fragebögen?

- Zentrale Evaluation nicht zweckmäßig für mich
  - zu spät um etwas an der Vorlesung zu ändern
  - Mehr Wertung als Verbesserung
    z.B. Frage:

    Der Schwierigkeitsgrad und der Aufwand zum Lösen aller Übungsaufgaben ist optimal (Weder zu schwer oder zu aufwendig, noch zu leicht).
- Startfragebogen: Ich erfahre die Vorkenntnisse und muss mich nicht auf Vermutungen verlassen
  - Möglichkeit die Vorlesung anzupassen
- Zeitlicher Verlauf/Zusammenhänge

Zur Person

☐ männlich ☐ weiblich Persn-Code: _____

Studiengang: _____

Ich möchte: ☐ gesiezt werden ☐ gedutzt werden ☐ mir egal

☐ Vorlesung ist eine Pflichtvorlesung

☐ Ich werde sehr sicher die ganze Vorlesung besuchen

☐ Ich möchte mir die Vorlesung ansehen

Gebietsfragen

- ☐ Experte
  - Über den Unistoff hinaus Erfahrung
  - Kann schwierige Fälle ohne Hilfe lösen
- ☐ mittlere Erfahrung
  - Unabhängige und sicher Anwendung
- ☐ Grundkenntnisse
  - Kenntnisse aus Vorlesung ohne Erfahrung
- ☐ keine Erfahrung
  - Begriff bekannt
  - Keine Anwendung möglich
- ☐ nie gehört

Offene Fragen

- Kurze und knackige Antworten
- Wenn Sie es nicht wissen: k.A. (keine Ahnung)
- Es ist **keine** Leistungsüberprüfung

Hinweise

- Bitte füllen Sie wahrheitsgemäß aus
- Dies ist **keine** Leistungsüberprüfung
- Hinweise für mich, wenn ich etwas Wiederholen/Einführen muss
- Das Ergebnis wird in der nächsten Vorlesung vorgestellt
- Zeitliche Zusammenhänge sind über den geheimen Code herstellbar

10 Min
zum Ausfüllen

Nächste Woche

Sicherheit – Ein Überblick