

Vorlesungen im WS 2021/22

Prof. Dr. Jan Jürjens

Universität Koblenz-Landau, Institut für Softwaretechnik

Einführung in Secure Software Engineering (Bachelor)

Durchführung: Online (asynchron).

Informationen:

<https://klips.uni-koblenz-landau.de/v/138977>

<https://olat.vcrp.de/auth/RepositoryEntry/3348464394>

Teil I:

Kapitel 1: Motivation: (Un-)Sichere Software

Kapitel 2: Einführung und Grundlagen

Kapitel 3: Von Zielen zu Mechanismen

Kapitel 4: Kryptographische Grundlagen: Verschlüsselung

Kapitel 5: Hashfunktionen

Kapitel 6: Authentifikation und Signatur

Kapitel 7: Sicherheitsprotokolle und Schlüsselaustausch



Einführung in Secure Software Engineering (Bachelor)

Teil II:

Kapitel 1: Motivation: Vertiefende Themen der IT-Sicherheit

- Einführung / Wiederholung der Sicherheitskonzepte

Kapitel 2: Security Engineering

- IT-Sicherheit entlang des Software-Lebenszyklus
- Microsoft Security Development Lifecycle (SDL)
- Security by Design



Kapitel 3: IT-Sicherheit im Praxiskontext: Angriffe und ihre Abwehr

Kapitel 4: Vertiefung Kryptographie: Protokolle und Mechanismen

Kapitel 5: IT-Sicherheit vs. Governance-Risk-Compliance (GRC)

Kapitel 6: KI, Datenräume & Security

- KI & Security
- International Dataspaces: Sicherheitsarchitekturen für verteilte Datenräume

Einführung in Smart Data Analytics (Bachelor)

Durchführung: Online (asynchron).

Informationen:

<https://klips.uni-koblenz-landau.de/v/138972>

<https://olat.vcrp.de/auth/RepositoryEntry/3359604794>

Teil I:

Kapitel 1: Einführung und Motivation:

Advanced Data Analytics: Big Data mit künstlicher Intelligenz

Kapitel 2: Data-Mining Grundlagen/Überblick

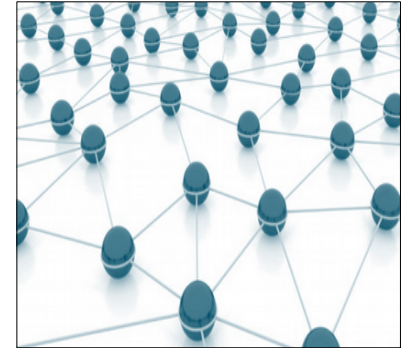
Kapitel 3: Prozessmodellierung und Analyse

Kapitel 4: Business Process Mining

Kapitel 5: Datenaustauschplattformen

Kapitel 6: Governance – Risk – Compliance in der Datenanalyse

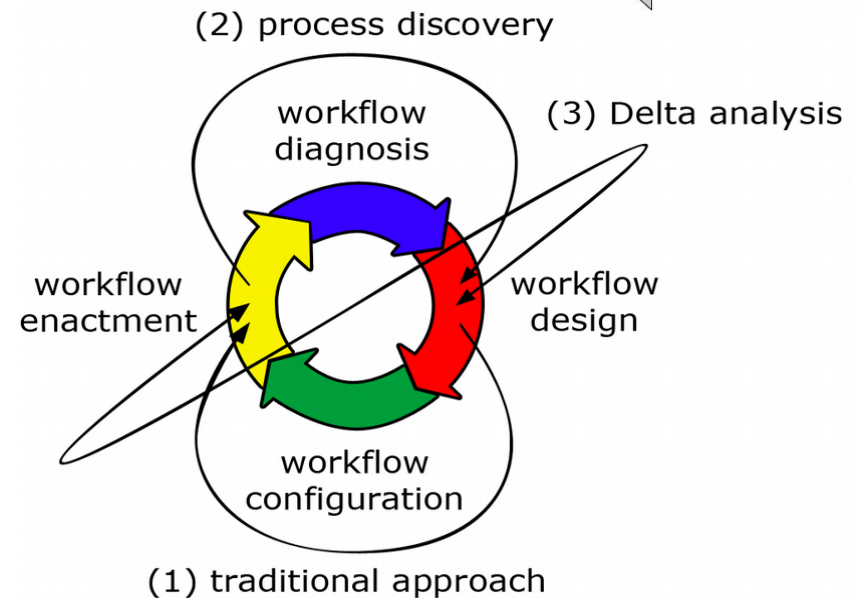
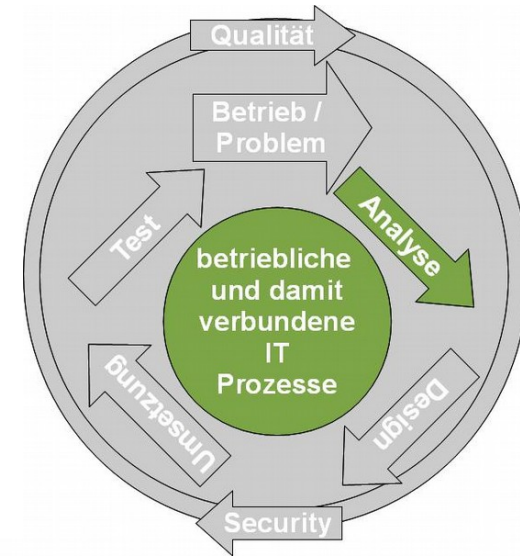
Kapitel 7: Versicherungswirtschaft digital: Quo Vadis?



Einführung in Smart Data Analytics (Bachelor)

Teil II:

- Teil 1: Grundlagen Geschäftsprozesse
- Teil 2: Einführung Business-Process-Mining
- Teil 3: Petri-Netze
- Teil 4: Data-Mining
- Teil 5: Datenbeschaffung
- Teil 6: Prozessextraktion
- Teil 7: Konformanzüberprüfung
- Teil 8: Mining: Zusätzliche Perspektiven
- Teil 9: Online-Analysen
- Teil 10: Werkzeugunterstützung
- Teil 11: "Lasagne"-Prozesse
- Teil 12: "Spaghetti"-Prozesse



Vertiefung Softwaretechnik (Master)

Durchführung: Online (asynchron).

Informationen:

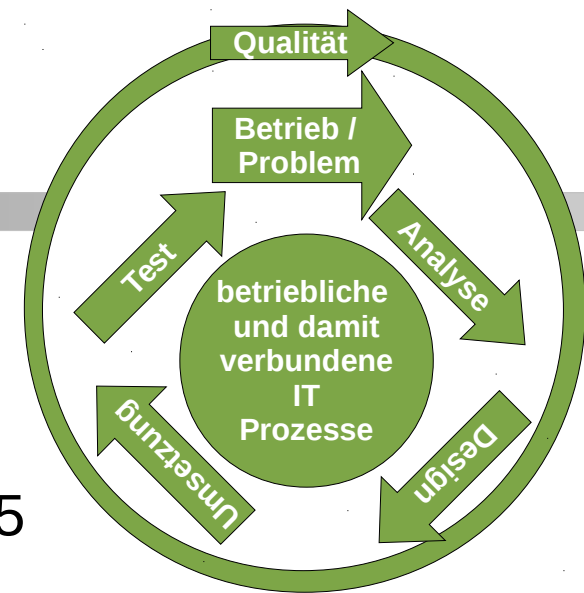
<https://klips.uni-koblenz-landau.de/v/138976>

<https://olat.vcrp.de/auth/RepositoryEntry/3359604795>

Ziel: Konstruktion qualitativ hochwertiger Software.

Unter anderem:

- Vertiefung in **Konzepten zur Spezifikation und zum Testen.**
- **Einbettung dieser Spezifikationskonzepte** in die Qualitätssicherung.
- **Modellbasiertes Software-Engineering.**
- **Fortgeschrittene Spezifikations- und Verifikationstechniken** (OCL, statische Analyse)
- Durchgängig: Verdeutlichung der o.g. Themen an Anwendungen im Bereich **Softwaresicherheit**



Vertiefung Softwaretechnik (Master)

Teil I) Einführung

1) Fortgeschrittene Techniken der Softwarequalitätssicherung und Softwaresicherheit

- 1.0) Softwarequalität und -sicherheit: Motivation und Einführung
- 1.1) Softwaredefekte und -schwachstellen

Teil II) Security Development Lifecycle (SDL)

2) Quality & Security by Design

- 2.0) Qualitäts- und Sicherheitsprinzipien
- 2.1) Modellbasierte Sicherheits- und Bedrohungsanalyse

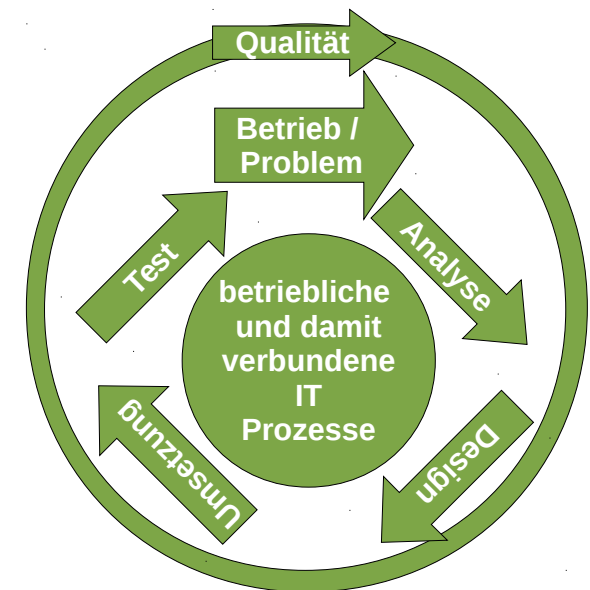
3) Codebasierte Analyse von Qualität und Sicherheit

- 3.0) Schwachstellensuche
- 3.1) Statische Analyse
- 3.2) Softwaremetriken
- 3.3) Bedingungs-basiertes Testen

Teil III) Quality & Security by Construction

4) Modellbasierte Softwareentwicklung

- 4.0) BPMN 2.0
- 4.1) Object Constraint Language (OCL)
- 4.2) Eclipse Modeling Framework (EMF)
- 4.3) Modellbasierte Entwicklung sicherheitskritischer Software
- 4.4) Software-Sicherheitsanalyse bei Systemänderungen
- 4.5) Sicherheit von Webanwendungen



Advanced Topics in Web-based and Data-intensive Software and its Security (Master, Englisch) (with Q. Ramadan)

Online (asynchronously)

Information:

<https://klips.uni-koblenz-landau.de/v/138993>

<https://olat.vcrp.de/auth/RepositoryEntry/3054698704>

Goal:

- Provide you with information you can use to make **your web applications more secure.**

Contents:

- **Current vulnerabilities (OWASP Top 10).**
- **Protective measures and best practices** against typical in web applications.
- Guide for a **systematic approach to creation of secure web applications.**
- **Existing**, as well as **new web applications to be developed.**



Advanced Topics in Web-based and Data-intensive Software and its Security (Master, Englisch) (with Q. Ramadan)

Chapter 1: Motivation: Web Application Security

Risks and Damages due to Web Application Vulnerabilities

Chapter 2: Foundations for Secure Web-based Architectures

- 1) Threat Modelling for Web-based Architectures
- 2) Security Principles for Web-based Architectures

Chapter 3: Securing Web-based Architectures against Vulnerabilities

- 1) Unvalidated Parameters
- 2) Insecure Access Control
- 3) Other Vulnerabilities in the Software
- 4) Vulnerabilities in Security Management

Chapter 4: Security Guide for Web Architectures

- 1) Building Blocks for Secure Web Architectures
- 2) Layer Model for Web Application Security Design
- 3) Web Application Security Tools



Fragen / Questions ?