Hochschule
Albstadt-Sigmaringen
Albstadt-Sigmaringen University

Modulhandbuch

Fakultät Informatik

Studiengänge
Advanced IT Security M.Sc.
Business and Security Analytics M.Sc.
Systems Engineering M.Eng.

Sommersemester 2025
Version 1.0

Ersteller: Prof. Dr. German Nemirovski, Studiendekan
Verantwortlich: *Prof. Dr. German Nemirovski, Studiendekan*

Änderungshistorie

Datum	Version	Studiengang / Vertiefung	Modul	Änderung	Vorher	Nachher

Inhaltsverzeichnis

1 Beschreibung der Studiengänge

1.1 Advanced IT Security M.Sc.

Der Masterstudiengang Advanced IT Security M.Sc. ist ein praxisorientierter Master-Studiengang. Die Inhalte werden auf wissenschaftlichem Niveau bei einer ausgeprägten Anwendungsorientierung vermittelt. Die Studierenden erlangen Qualifikationen, die sie befähigen, als technische Fach- und Führungskräfte, weltweit aber auch für die regionale mittelständische Industrie tätig zu sein. Die Fähigkeiten, Fertigkeiten und Kenntnisse der Absolventen ermöglichen ihnen u.a. die Übernahme der folgenden Positionen in Industrie und Behörden:

- IT-Security-Experte
- System- und Softwareentwickler im Bereich IT Security
- Mitarbeiter im IT-Sicherheitsmanagement
- Mitarbeiter Incident Response Team
- Mitarbeiter im Bereich Pentesting und Security Audits
- Forensiker (Digitale Forensik)
- Leitender IT-Administrator

Folgende Qualifikationsziele werden in der Lehre gesetzt:

Sicherheitskompetenz
Die Studierenden sind in der Lage, im Rahmen einer eigenständigen Arbeit komplexe IT-Sicherheits- und -bedrohungsrelevante Fragen und Problemstellungen zu formulieren. Sie sind in der Lage mit analytischen Mitteln relevante Informationen zu Bedrohungen und Angriffen abzuleiten.

Methodenkompetenz
Die Studierenden verfügen über Kenntnisse von Methoden, Verfahren und Werkzeugen der IT-Sicherheit, darunter der Netzwerk- und Hardwaresicherheit, der digitalen Forensik, der Kryptographie und des Sicherheitsmanagements, und können diese in der Praxis anwenden.
Ferner können Studierende zweckdienliche Erkenntnisse auch aus anderen Wissenschaftsbereichen (z.B. Psychologie) und Anwendungsgebieten (z.B. IOT) zur Problemlösung heranziehen.

Ethische und Rechtliche Kompetenz
Die Studierenden sind in der Lage, ihr Vorgehen in einen rechtlich zulässigen, ethischen und moralischen Rahmen einzuordnen und kritisch zu hinterfragen. Insbesondere sind sie in der Lage, Datenerhebungs- und Datenverarbeitungsprozesse bezüglich Konflikte mit Datenschutz- und Persönlichkeitsrechten zu prüfen.

Konzeptionelle Fähigkeit
Die Studierenden sind in der Lage, eigenständig Konzepte und Analysen zu entwickeln. Besondere Bedeutung hat in diesem Zusammenhang die Fähigkeit, theoretische Konzepte auf die konkreten Anwendungsfälle zu übertragen.

Vernetztes Denken
Die Studierenden können Zusammenhänge aus unterschiedlichen Anwendungsgebieten innerhalb des Fachgebiets und in deren Umfeld herleiten. Sie sind in der Lage, fachübergreifend zu analysieren und Konzepte zu entwickeln.

Forschungskompetenz
Die Studierenden sind in der Lage, bei der Wissensakquirierung Forschungsbedarf zu erkennen und wissenschaftliche Methoden systematisch einzusetzen, um auf neue Erkenntnisse zu kommen. Die Studierenden können Forschungsergebnisse zielgruppengerecht aufbereiten und diese bei der Lösung von praktischen Aufgabenstellungen effizient einsetzen.

1.2 Business and Security Analytics M.Sc.

Der Masterstudiengang Systems Engineering ist ein praxisorientierter Master-Studiengang. Die Inhalte Werden auf wissenschaftlichem Niveau bei einer ausgeprägten Anwendungsorientierung vermittelt. Die Studierenden erlangen Qualifikationen, die sie befähigen als technische Fach- und Führungskräfte, weltweit aber auch für die regionale mittelständische Industrie tätig zu sein. Die Fähigkeiten, Fertigkeiten und Kenntnisse der Absolventen ermöglichen die folgenden Tätigkeitsfelder:

- Business Intelligence und Digitalisierung bei Beratungen sowie in Unternehmensabteilungen
- Analyst-Referent(in) direkt zugeordnet zum Direktorium oder Vorstand
- Risikomanagement bei Finanz-Unternehmen
- (IT-)Sicherheitsbeauftragte
- Security Information and Event Management

Folgende Qualifikationsziele werden in der Lehre gesetzt:

Konzeptionelle Fähigkeiten
Die Studierenden sind in der Lage, eigenständig Konzepte für Business Analytics-Werkzeuge und deren wirtschaftlichen Einsatz im Unternehmensumfeld zu entwickeln. Besondere Bedeutung hat in diesem Zusammenhang die Fähigkeit, theoretische Konzepte auf die konkreten Anwendungsfälle zu übertragen.

Vernetztes Denken
Die Studierenden können Zusammenhänge aus unterschiedlichen Anwendungsgebieten innerhalb des Fachgebiets und in deren Umfeld herleiten. Sie sind in der Lage, fachübergreifend zu analysieren und Konzepte zu entwickeln.

Führungskompetenz
Die Studierenden entwickeln sich in ihrer Führungsfähigkeit weiter. Sie sind in der Lage, Zielvereinbarungen zu treffen und deren Umsetzung zu steuern. Sie können ein Team motivieren und die Erfahrung von Personen unterschiedlicher Kompetenzen zielgerichtet zum Erfolg eines Teamprojekts einsetzen und nutzen.

Methodenkompetenz
Die Studierenden verfügen nicht nur über die Kenntnis von Methoden und Verfahren unterschiedlicher Fachgebiete der Informatik, sondern sind auch in der Lage, diese im jeweiligen Anwendungskontext anzuwenden.

Forschungskompetenz
Im Bereich Wissenschaft und Forschung sind die Studierenden in der Lage, wissenschaftliche Methoden einzusetzen und diese managementgerecht aufzubereiten.

Prozesskompetenz
Die Studierenden sind in der Lage, Konzepte und Strategien im Unternehmensumfeld erfolgreich umzusetzen. Sie haben das Rüstzeug, auch große Projekte von hoher Komplexität erfolgreich zu managen.

Analytische Kompetenz
Die Studierenden sind in der Lage, die für deren Problembereich relevanten Datenquellen zu identifizieren, die Daten formal zu beschreiben und diese für analytische Zwecke aufzubereiten. Sie sind darüber hinaus in der Lage, analytische Untersuchungen der Daten unter der Zielsetzung der Beantwortung komplexer Fragestellungen und des Generierens neuen, nicht trivialen Wissens selbstständig durchzuführen.

Sicherheitskompetenz
Die Studierenden sind in der Lage, im Rahmen einer eigenständigen Arbeit komplexe IT-Sicherheits- und - Bedrohungsrelevante Fragen und Problemstellungen zu formulieren. Sie sind in der Lage mit analytischen Mitteln aus Vorgangsdaten relevante Informationen zu Bedrohungen und Angriffen abzuleiten.

Ethische Kompetenz
Die Studierenden sind in der Lage ihr Vorgehen im rechtlich zulässigen, ethischen und moralischen Rahmen einzuordnen und kritisch zu hinterfragen. Insbesondere sind sie in der Lage Datenerhebungs- und Datenverarbeitungsprozesse bezüglich Konflikte mit Datenschutz- und Persönlichkeitsrechten zu prüfen.

1.3 Systems Engineering M.Eng.

Der Masterstudiengang Systems Engineering M.Eng. ist ein praxisorientierter Master-Studiengang. Die Inhalte werden auf wissenschaftlichem Niveau bei einer ausgeprägten Anwendungsorientierung vermittelt. Die Studierenden erlangen Qualifikationen, die sie befähigen, als technische Fach- und Führungskräfte, weltweit aber auch für die regionale mittelständische Industrie tätig zu sein. Die Fähigkeiten, Fertigkeiten und Kenntnisse der Absolventen ermöglichen die folgenden Tätigkeitsfelder:

- Entwurf und Realisierung von Lösungen für komplexe technische Systeme, bestehend aus Komponenten der Software, der Hardware, der Elektronik und der Mechanik.
- Integration heterogener softwareintensiver technischer Systeme, die vertiefte Kenntnisse in Technischer Informatik und Elektronik (Chipdesign, Sensoren und Aktoren, Kommunikationssysteme, eingebettete Systeme) sowie in den Bereichen digitale Signalverarbeitung, Steuerungs- und Regelungstechnik, Mustererkennung, Sprachen- und Automatentheorie erfordern.
- Übernahme von Leitungsfunktionen für Entwicklungsteams unterschiedlicher Größe und Zusammensetzung.

Folgende Qualifikationsziele werden in der Lehre gesetzt:

- **Praxisnahes und Fachübergreifendes Wissen**
  Die Studierenden können reale komplexe softwareintensive Systeme verstehen und entwerfen. Sie sind in der Lage solche Systeme gesamthaft zu überschauen und den Prozess der Projektabwicklung unter Beachtung aller funktionalen, prozessualen und wirtschaftlichen Randbedingungen zu beherrschen.

- **Methoden und Werkzeuge**
  Die Studierenden kennen Methoden und Werkzeuge der Systemtechnik sowie des Planungsmanagements (Projektmanagement, Qualitäts-management, Konfigurationsmanagement, betriebswirtschaftliche und soziale Aspekte). In Verbindung mit den im grundständigen Studium erworbenen Kenntnissen sind sie in der Lage aus Kundenanforderungen oder einer allgemein formulierten Bedürfnissituation folgend die insgesamt beste Systemlösung aus Software, Hardware, Elektronik und Mechanik zu finden und Aufgaben zu lösen.

- **Breites Wissen**
  Studierende haben ein breites Wissensgebiet in Bereichen von Softwareentwicklung, Internet, Kommunikationstechnik, Gerätetechnik, Fahrzeugbau mit Zulieferindustrie, Konsum- und Investitionsgüter-industrie, Automatisierungstechnik, Medizintechnik sowie in Anwendungssystemen in Industrie, Handel, Verkehr, Logistik, E-Business, Industrie 4.0. Darüber hinaus aber auch in Forschung und Wissenschaft und in der Aus- und Weiterbildung an Universitäten, Fachhochschulen, Berufsakademien etc.

- **Sicherheitskompetenz**
  Die Studierenden sind in der Lage, komplexe IT-Sicherheits- und IT-Bedrohungsszenarien in den Bereichen von Systems Engineering zu erkennen und Vorkehrungen zu treffen, um Gefahren abzuwenden oder offensive Methoden anzuwenden um auf Angriffssituationen vorbereitet zu sein. Sie sind in der Lage mit ethischer Fragestellung der IT-Sicherheit verantwortungsvoll umzugehen und die erforderlichen Datenschutzbestimmungen und Persönlichkeitsrechte Einzelner ausreichend zu beachten.

- **Wissenschaftliches Niveau und ausgeprägte Anwendungsorientierung**
  Die Studierenden sind in der Lage, komplexe IT-Sicherheits- und IT-Bedrohungsszenarien in den Bereichen von Systems Engineering zu erkennen und Vorkehrungen zu treffen, um Gefahren abzuwenden oder offensive Methoden anzuwenden, um auf Angriffssituationen vorbereitet zu sein. Sie sind in der Lage mit ethischer Fragestellung der IT-Sicherheit verantwortungsvoll umzugehen und die erforderlichen Datenschutzbestimmungen und Persönlichkeitsrechte Einzelner ausreichend zu beachten.

- **Industrie 4.0 und Digitale Transformation**
  Die Studierenden beherrschen das Technologieportfolio der Digitalisierung und sind in der Lage, innovative digitale Geschäftsmodelle sowie Geschäftsmodellmuster mit wissenschaftlichen Methoden zu analysieren, zu bewerten und aktiv an einer betrieblichen Umsetzung mitzuwirken.

2 Übersicht der Module nach Vertiefungsrichtung im Studiengang Systems Engineering M.Eng.

	Vertiefungsrichtung im Studiengang Systems Engineering M.Eng.		
Modul	**Advanced Computing**	**Industrie 4.0**	**Security Systems**
Eingebettete Systeme	X	X	X
Advanced Statistics	X		
Implementation Attacks and Countermeasures			X
IT Security Management and Incident Response			X
Virtuelle Modellierung		X	
Steuerung von Cyber Physical Systems	X	X	
Maschinelles Lernen	X	X	
Elektronik	X	X	X
Security Hardware Design			X
Security und Internet der Dinge	X	X	X
Einführung Industrie 4.0		X	
Seminar Industrie 4.0		X	
Projekt Industrie 4.0		X	
Wahlpflichtmodul 1a	X	X	X
Wahlpflichtmodul 2a	X	X	X
Wahlpflichtmodul 1b	X	X	X
Wahlpflichtmodul 2b	X	X	X
Master-Thesis	X	X	X

3 Qualifikationsziel-Modul-Matrix

3.1 Qualifikationsziel-Modul-Matrix Advanced IT Security M.Sc.

Modul-Nr.	Qualifikationsziel (QuZ) Modulbezeichnung Modulbezeichnung	Summe der Unterstützungspunkte	Sicherheitskompetenz	Methodenkompetenz	Ethische und Rechtliche Kompetenz	Konzeptionelle Fähigkeit	Vernetztes Denken	Forschungskompetenz
54000	Application Forensics	9	1	2	2	2	0	2
52000	Open Source Intelligence	9	1	2	2	0	2	2
51000	Implementation Attacks and Countermeasures	10	2	2	1	2	1	2
51500	IT Security Management and Incident Response	11	2	2	2	2	2	1
54500	Applied Cyberpsychology	9	1	1	2	1	2	2
55000	Human Factors in IT-Security	10	1	2	2	1	2	2
52500/ 53000	Wahlpflichtmodul 1a / 1b		X	X	X	X	X	X
55500/ 56000	Wahlpflichtmodul 2a / 2b		X	X	X	X	X	X
61000	Master Thesis	12	2	2	2	2	2	2

Unterstützung der Qualifikationsziele in den Modulen
(0=keine Unterstützung, 1=indirekte Unterstützung, 2=direkte Unterstützung)

3.2 Qualifikationsziel-Modul-Matrix Business and Security Analytics M.Sc.

Modul-Nr.	Qualifikationsziel (QuZ) Modulbezeichnung Modulbezeichnung	Summe der Unterstützungspunkte	Strategisches Denken	Konzeptionelle Fähigkeiten	Vernetztes Denken	Führungskompetenz	Methodenkompetenz	Forschungskompetenz	Prozesskompetenz	Analytische Kompetenz	Sicherheitskompetenz	Ethische und Rechtliche Kompetenz
52200	Advanced Statistics	8		2			2	2		2		
52700	Security Analytics	13		1	2		2	2		2	2	2
51500	Strategic IT-Management	13	2	1	2	2		2	2			2
52100	Business Process Management & Data Compliance	11	1	2	1	1	2	1	2	1		
51200	Data- and Webmining	8		2			2	2		2		
51300	Large-Scale Data Analysis & Parallelization	11	1	2	2		2		2	2		
52500/ 53000	Wahlpflichtmodul 1a / 1b	X	X	X	X	X	X	X	X	X	X	X
55500/ 56000	Wahlpflichtmodul 2a / 2b	X	X	X	X	X	X	X	X	X	X	X
60100	Master Thesis	11	1	2			2	2	1	1	1	1
60200	Mü. Masterprüfung (StuPO 18.2)	6	1	2	1		1			1		

Unterstützung der Qualifikationsziele in den Modulen
(0=keine Unterstützung, 1=indirekte Unterstützung, 2=direkte Unterstützung)

3.3 Qualifikationsziel-Modul-Matrix Systems Engineering M.Eng.

	Qualifikationsziel (QuZ)	Summe der Unterstützungspunkte	Praxisnahes und Fachübergreifendes Wissen	Methoden und Werkzeuge	Breites Wissen	Sicherheitskompetenz	Wissenschaftliches Niveau und ausgeprägte	Industrie 4.0 und Digitale Transformation
51000	Eingebettete Systeme	7	1	2	1	0	1	2
52200	Advanced Statistics	4	1	2	0	0	1	0
51000	Implementation Attacks and Countermeasures	9	1	2	1	2	2	1
51500	IT Security Management and Incident Response	7	2	2	0	2	1	0
52000	Virtuelle Modellierung	7	0	2	1	0	2	2
52500	Steuerung von Cyber Physical Systems	8	0	2	2	0	2	2
xxxxx	Maschinelles Lernen	9	2	2	2	0	2	1
55000	Elektronik	7	2	1	1	0	1	2
100110	Security Hardware Design	8	1	1	1	2	2	1
55500	Security und Internet der Dinge	11	2	2	1	2	2	2
53500	Einführung Industrie 4.0	7	1	1	1	1	1	2
xxxxx	Seminar Industrie 4.0 (1. Semester)	7	1	1	1	1	1	2
56500	Projekt Industrie 4.0	7	1	1	1	1	1	2
xxxxx	Seminar Industrie 4.0 (2. Semester)	7	1	1	1	1	1	2
53000	WPM 1a / 1b	6	1	1	1	1	1	1
56000	WPM 2a / 2b	6	1	1	1	1	1	1
60100	Master-Thesis	12	2	2	2	2	2	2

4 Studiengangs-Kompetenzmatrix

4.1 Studiengangs-Kompetenzmatrix Advanced IT Security M.Sc.

Kompetenzen		Fachkompetenz					Personale Kompetenz					
		Wissen		Fertigkeiten			Sozialkompetenz			Selbständigkeit		
Ausprägung		Tiefe	Breite	Instrumentelle Fertigkeiten	systemische Fertigkeiten	Beurteilungs-fähigkeit	Team-/ Führungs-fähigkeit	Mitgestaltung	Kommunikation	Eigenständigkeit / Verantwortung	Reflexivität	Lernkompetenz
51100	Application Forensics	7			7	7			7			7
52200	IT Security Management and Incident Response		7	7	7		7				7	
52300	Implementation Attacks and Countermeasures	7		7	7	7			7	7		
52700	Applied Cyberpsychology	7				7			7	7		
51500	Human Factors in IT-Security	7				7			7	7		
52100	Open Source Intelligence	7	7	7	7	7			7	7		7
52500/ 53000	Wahlpflichtmodul 1a/1b	X	X	X	X	X	X	X	X	X	X	X
55500/ 56000	Wahlpflichtmodul 2a/2b	X	X	X	X	X	X	X	X	X	X	X
61000	Master-Thesis	7	7	7	7	7	7	7	7	7	7	7

4.2 Studiengangs-Kompetenzmatrix Business and Security Analytics M.Sc.

		Kompetenzen	Fachkompetenz					Personale Kompetenz					
			Wissen		Fertigkeiten			Sozialkompetenz			Selbständigkeit		
		Ausprägung	Tiefe	Breite	Instrumentelle Fertigkeiten	systemische Fertigkeiten	Beurteilungs-fähigkeit	Team-/Führungs-fähigkeit	Mitgestaltung	Kommunikation	Eigenständigkeit/ Verantwortung	Reflexivität	Lernkompetenz
52200	Advanced Statistics		7		7					7	7		
52700	Security Analytics		7	7	7	7		7			7		7
51500	Strategic IT-Management			7	7	7		7		7	7		
52100	Business Process Management & Data Compliance		7		7			7		7	7		
51200	Data- and Webmining		7	7	7	7				7	7		
51300	Large-Scale Data Analysis & Parallelization		7	7	7			7			7		
52500/ 53000	Wahlpflichtmodul 1a/1b		X	X	X	X	X	X	X	X	X	X	X
55500/ 56000	Wahlpflichtmodul 2a/2b		X	X	X	X	X	X	X	X	X	X	X
60100	Master Thesis					7					7		
60200	Mü. Masterprüfung					7							7

4.3 Studiengangs- Kompetenzmatrix Systems Engineering M.Eng.

Kompetenzen		Fachkompetenz					Personale Kompetenz					
		Wissen		Fertigkeiten			Sozialkompetenz			Selbständigkeit		
Ausprägung		Tiefe	Breite	Instrumentelle Fertigkeiten	systemische Fertigkeiten	Beurteilungs-fähigkeit	Team-/Führungs-fähigkeit	Mitgestaltung	Kommunikation	Eigenständigkeit/ Verantwortung	Reflexivität	Lernkompetenz
51000	Eingebettete Systeme	7		7					7			7
52200	Advanced Statistics	7	7	7					7	7		
51000	Implementation Attacks and Countermeasures	7		7		7			7	7		
51500	IT Security Management and Incident Response	7	7	7	7		7		7		7	
52000	Virtuelle Modellierung	7	7	7								
52500	Steuerung von Cyber Physical Systems	7	7	7					7			7
xxxxx	Maschinelles Lernen	7	7	7					7	7		7
55000	Elektronik	7	7	7					7			7
xxxxx	Security Hardware Design	7		7		7	7			7		
55500	Security und Internet der Dinge	7		7			7			7		
53500	Einführung Industrie 4.0		7		7							
xxxxx	Seminar Industrie 4.0 (1. Sem.)	7	7						7	7		
56500	Projekt Industrie 4.0				7					7		7
xxxxx	Seminar Industrie 4.0 (2. Semester)	7	7						7	7		
53000	WPM 1a / 1b	7	7		7		7			7		
56000	WPM 2a / 2b	7	7		7		7			7		
60100	Master Theis				7					7		

5 Modulbeschreibungen

5.1 Gemeinsame Pflichtmodule mehrerer Studiengänge

5.1.1 Advanced Statistics

<table>
<tr><td colspan="7">Modul: Advanced Statistics</td></tr>
<tr><td colspan="2">Kennnummer
52200</td><td>Work-load
180 h</td><td>Modulart
PM</td><td>Studiensemester
1.</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS</td></tr>
<tr><td>1</td><td colspan="2">Lehrveranstaltung(en)
Vorlesung & Seminar Advanced Statistics
Übungen Advanced Statistics</td><td>Sprache
Deutsch und Englisch (deutsches und englisches Literaturstudium erforderlich)</td><td>Kontakt-zeit
4 SWS / 60 h</td><td>Selbst-studium
120 h</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="6">Lehrform(en) / SWS:
Vorlesung & Seminar: 2 SWS
Übungen: 2 SWS</td></tr>
<tr><td>3</td><td colspan="6">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Studierende kennen die grundlegenden Begriffe der Wahrscheinlichkeitstheorie und können diese anwenden [Wissen, 7]
Kompetenz Fertigkeiten
Die Studierenden können den Stoff praktisch in der Programmiersprache R für Analysen umsetzen [Instrumentelle Fertigkeiten, 7]
Sozialkompetenz
Die Studierenden können statistische Sachverhalte anderen vermitteln. [Kommunikation, 7]
Selbstständigkeit
Die Studierenden können selbstständig Analysen mittels der Programmiersprache R durchführen. [Eigenständigkeit/Verantwortung, 7]</td></tr>
<tr><td>4</td><td colspan="6">Inhalte:
R-Grundlagen.
Stochastische Grundlagen (Wahrscheinlichkeit, Bedingte Wahrscheinlichkeit, Satz von Bayes)
Zufallsvariablen, Erwartungswert, Varianz, Stichproben, Lage- und Streumaße
Bootstrapping, Konfidenzintervalle, Verteilungen (Binomialverteilung, Poisson-Verteilung, Geometrische Verteilung, Exponentialverteilung, Normalverteilung, Betaverteilung)

Signifikanz- und Hypothesentests (A/B-Tests, Permutationstests, ANOVA), Korrelationen, Maximum-Likelihood, Lineare Regression.

Empfohlene Literaturangaben:
Introduction to Statistical Thought
ISBN: 978-1616100483
http://people.math.umass.edu/~lavine/Book/book.html

Introduction to Probability and Statistics UsingR ISBN: 978-0-557-24979-4
http://cran.r-project.org/web/packages/IPSUR/vignettes/IPSUR.pdfAn Introduction to Statistical Learning: with Applications in R Gareth James, Daniela Witten, Trevor Hastie, Robert TibshiraniSpringer Texts in Statistics, 11. Juli 2016, ISBN-10: 1461471370

Die "'offizielle"' R-Einführung
ISBN: 978-0954612085</td></tr>
</table>

	cran.r-project.org/doc/manuals/R-intro.pdf R-Kurs der Uni Augsburg: stats.math.uniaugsburg.de/~theus/r-kurs.pdf
5	**Teilnahmevoraussetzungen:** Grundlegende Programmierkenntnisse
6	**Prüfungsformen***:* Klausur 90 min., benotet Referat, unbenotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandene Klausur und Referat
8	***Verwendbarkeit des Moduls:*** Business and Security Analytics, M.Sc., Systems Engineering M. Eng.
9	***Modulverantwortliche(r):*** Prof. Dr. Nemirovski
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul
11	***Bearbeitungsstand:*** *24.01.2025*

5.1.2 Implementation Attacks and Countermeasures

<table>
<tr><td colspan="7">Modul: Implementation Attacks and Countermeasures</td></tr>
<tr><td colspan="2">Kennnummer
51005</td><td>Workload
180h</td><td>Modulart
PM</td><td>Studiensemester
1. Semester</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS</td></tr>
<tr><td>1</td><td colspan="2">Lehrveranstaltung(en)
Vorlesung Implementation Attacks and Countermeasures
Projekt Implementation Attacks and Countermeasures</td><td>Sprache
Deutsch oder Englisch</td><td>Kontakt-zeit
4 SWS / 60h</td><td>Selbst-studium
120</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="6">Lehrform(en) / SWS:
Vorlesung Implementation Attacks and Countermeasures / 2 SWS
Projektarbeit Implementation Attacks and Countermeasures / 2 SWS</td></tr>
<tr><td>3</td><td colspan="6">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Die Studierenden können Seitenkanal-, und Fehler-Angriffe, sowie geeignete Gegenmaßnahmen verstehen und die Bedrohungslage durch solche Angriffe adäquat einschätzen. [Wissen, 7]
Kompetenz Fertigkeiten
Die Studierenden können Seitenkanal- und Fehler-Angriffe durchführen, sowie geeignete Gegenmaßnahmen implementieren. Dabei können die Studierende die Notwendigkeit und Auswahl der Gegenmaßnahmen an die Anwendung und die daraus resultierende Bedrohungslage anpassen. [Instrumentelle Fertigkeiten, 7]

Die Studierenden können die Sicherheit von Software und Hardware bezüglich Implementierungs-Angriffe beurteilen und Schwachstellen in Implementierungen aufdecken, sowie Gegenmaßnahmen entwickeln. [Beurteilungsfähigkeit, 7]
Sozialkompetenz
Die Studierenden können komplexe statistische und andere Sachverhalte zu Implementierungs-Angriffen mit anderen Experten diskutieren und weiterentwickeln, sowie die Notwendigkeit von geeigneten Gegenmaßnahmen kompetent und zielgruppengerecht vermitteln. [Kommunikation, 7]</td></tr>
<tr><td></td><td colspan="6">Selbstständigkeit
Die Studierenden können selbstständig komplexe Zusammenhänge der IT-Sicherheit verstehen, beurteilen und daraus geeignete Maßnahmen eigenverantwortlich ableiten. [Eigenständigkeit/Verantwortung, 7]</td></tr>
<tr><td>4</td><td colspan="6">Inhalte:
Vorlesung
- Physikalische Grundlagen von Seitenkanal-Angriffen
- Statistische Grundlagen der Seitenkanalanalysen
- Simple Power Analysis, Differential Power Analysis, Timing Attacks
- Vertikale und Horizontale Angriffe gegen Public Key Kryptografie
- Microarchitekturelle Angriffe
- Grundlegende Einführung zu Seitenkanal-Gegenmaßnahmen
- Masking und Higher-Order Masking von kryptografischen Algorithmen
- Hiding-Maßnahmen
- Gegenmaßnahmen für Public Key Kryptografie, wie z.B. Scalar Blinding, oder Point Randomization
- Konstruktive Maßnahmen, wie z.B. statistische Leakage-Detektion
- Physikalische Grundlagen für Fehlerangriffe
- Voltage-Glitch-Angriffe, Clock-Glitch-Angriffe, Laser-Fault Injection, EM-Fault Injection
- Beobachtbare Fehlerbilder und Ausnutzung der Fehler in unterschiedlichen Szenarien
- Gegenmaßnahmen wie Redundanz, Glitch-Detektoren, oder Laser-Detektoren
Projekt
- Praktische Umsetzung und Evaluation von ausgewählten Angriffen und Gegenmaßnahmen</td></tr>
</table>

	Empfohlene Literaturangaben: Mangard, S., Oswald, E., Popp, T. - Power Analysis Attacks: Revealing the Secrets of Smart Cards, Springer-Verlag, 2007 Kocher, P., Jaffe, J., Jun B. - Differential Power Analysis, CRYPTO '99, Springer-Verlag, 1999 Gilbert Goodwill, B. J., Jaffe, J., Rohatgi, P. - A testing methodology for side-channel resistance validation, NIST Non-invasive Attack Testing Workshop, Vol. 7, pp. 115-136, 2011 Kocher P., Horn J., Fogh A., Genkin D., Gruss D., Haas W., Hamburg M., Lipp M., Mangard S., Prescher T., Schwarz M., Yarom Y. - Spectre Attacks: Exploiting Speculative Execution, IEEE S & P, 2019
5	**Teilnahmevoraussetzungen:** Grundlagen der Kryptologie, Statistische Grundlagenkenntnisse, Programmierkenntnisse (idealerweise in ARM-Assembler oder VHDL)
6	**Prüfungsformen***:* Referat 20 min. inkl. Wissenschaftlicher Ausarbeitung zum Projekt, Diskussion benotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Ausreichend bewertetes Referat inkl. wissenschaftlicher Ausarbeitung.
8	***Verwendbarkeit des Moduls:*** Advanced IT Security M.Sc., Systems Engineering M.Eng.
9	***Modulverantwortliche(r):*** Prof. Dr. Bernhard Jungk
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul
11	***Bearbeitungsstand:*** *24.01.2025*

5.1.3 IT Security Management and Incident Response

<table>
<tr><td colspan="7">Modul: IT Security Management and Incident Response</td></tr>
<tr><td colspan="2">Kennnummer
51505</td><td>Work-load
180 h</td><td>Modulart
PM</td><td>Studiensemester
1. Semester</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS</td></tr>
<tr><td>1</td><td colspan="2">Lehrveranstaltung(en)
a. Vorlesung, Advanced IT Security Management
b. Projekt Incident Response</td><td colspan="2">Sprache
Englisch (Literaturstudium in Deutsch und Englisch erforderlich)</td><td>Kontakt-zeit
4 SWS / 60 h</td><td>Selbst-studium
120 h</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="6">Lehrform(en) / SWS:
a. Vorlesung, Seminar Advanced IT Security Management: 2 SWS
b. Vorlesung, Praktikum Incident Response: 2 SWS</td></tr>
<tr><td>3</td><td colspan="6">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Die Studierenden können die gesetzlichen Grundlagen und „Best Practice“ Methoden des IT-Sicherheitsmanagements (ISM) erklären. [Wissen, 7]

Die Studierenden können die Voraussetzungen für eine Incident Response nennen und die verschiedenen Phasen einer Incident Response erläutern. [Wissen, 7]

Kompetenz Fertigkeiten
Die Studierenden können ein Konzept für die Einrichtung eines ISM erstellen und umsetzen sowie ein bestehendes ISM anhand nationaler und internationaler Standards bewerten. [Instrumentelle Fertigkeiten, 7]

Die Studierenden können ein Incident Response Team etablieren und die einzelnen Phasen einer Incident Response durchführen. [Systemische Fertigkeiten, 7]

Sozialkompetenz
Die Studierenden können sich auf Expertenebene mit der Fachcommunity über Methoden und Werkzeuge des IT-Sicherheitsmanagements unterhalten, Erkenntnisse und Methoden diskutieren und ihr Expertenwissen und Forschungsergebnisse auch Fachabteilungen vermitteln. [Kommunikation, 7]

Die Studierenden können Laien für Fragen der IT-Sicherheit interessieren, die Notwendigkeit von Maßnahme der IT-Sicherheit darstellen und erläutern, und IT-Sensibilisierungskampagnen im Bereich der IT-Sicherheit planen und durchführen. [Team-/Führungsfähigkeit, 7]

Selbstständigkeit
Die Studierenden können den Umsetzungsgrad des ISM reflektieren und bei Änderungen der Rahmenbedingungen gegebenenfalls Änderungsbedarf erarbeiten, darstellen und umsetzen. [Reflexivität, 7]

Die Studierenden können die Fähigkeiten zur Incident Response unter Berücksichtigung der Bedrohungslage reflektieren und anpassen. [Reflexivität, 7]</td></tr>
<tr><td>4</td><td colspan="6">Inhalte:
Vorlesung, Seminar Advanced IT-Sicherheitsmanagement:
• Auffrischung IT-Sicherheitsmanagement
• Compliance, nationale und internationale Standards für IT-Sicherheitsmanagement
• Sensibilisierung
• Betrachtung und Diskussion aktueller Forschungsthemen und -ergebnisse

Vorlesung, Praktikum Incident Response
• Auffrischung IT-Sicherheitsmanagement, Digitale Forensik
• Voraussetzungen für Incident Response
• Phase von Incident Response
• Intrusion Detection Systems
Empfohlene Literaturangaben:</td></tr>
<tr><td>5</td><td colspan="6">Teilnahmevoraussetzungen:
Grundlagen der IT-Sicherheit, Programmierkenntnisse</td></tr>
<tr><td>6</td><td colspan="6">Prüfungsformen:
Referat 20 min. inkl. wissenschaftlicher Ausarbeitungen, Diskussion, benotet</td></tr>
</table>

	Laborarbeit, unbenotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Ausreichend bewertetes Referat erfolgreiche Teilnahme am Praktikum
8	***Verwendbarkeit des Moduls:*** Advanced IT Security M.Sc., Systems Engineering M.Eng.
9	***Modulverantwortliche(r):*** Prof. Dr. Henrich Dozent: Prof. Dr. Henrich
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul
11	***Bearbeitungsstand:*** *24.01.2025*

5.2 Pflichtmodule Advanced IT Security

5.2.1 Open Source Intelligence

<table>
<tr><td colspan="7">Modul: Open Source Intelligence</td></tr>
<tr><td colspan="2">Kennnummer
52000</td><td>Workload
180 h</td><td>Modulart
PM</td><td>Studiensemester
1</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS</td></tr>
<tr><td>1</td><td colspan="2">Lehrveranstaltung(en)
Vorlesung Open Source Intelligence
Praktikum Open Source Intelligence</td><td>Sprache
Deutsch oder Englisch (Literatur-studium in Deutsch und Englisch erforderlich)</td><td>Kontakt-zeit
4 SWS / 60 h</td><td>Selbst-studium
120</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="6">Lehrform(en) / SWS:
Vorlesung, Übungen, Seminar: 3 SWS
Praktikum: 1 SWS</td></tr>
<tr><td>3</td><td colspan="6">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Die Studierenden verfügen über ein breites Wissen über die technischen, gesellschaftlichen und rechtlichen Rahmenbedingungen für einen OSINT Einsatz. [Wissen, 7]

Die Studierenden verfügen über ein tiefes Wissen im Bereich von OSINT Terminologien, Methoden und Techniken. [Wissen, 7]
Kompetenz Fertigkeiten
Können einen OSINT Einsatz konzeptionell strukturieren und geeignete Methoden und Werkzeuge auswählen. [Instrumentelle Fertigkeiten, 7]

Können die Leistungsfähigkeit vorhandener OSINT Werkzeuge beurteilen und selbstständig neue OSINT Verfahren und Werkzeuge entwickeln. Dabei nutzen sie wissenschaftliche Methoden und bereiten aktuelle Forschungsergebnisse zielgruppen- und anwendungsgerecht auf. [Systemische Fertigkeiten, 7]

Können per OSINT ermittelte Daten hinsichtlich ihrer technischen und juristischen Verwertbarkeit beurteilen und ihren Informations- und Intelligence-Gehalt einschätzen. [Beurteilungsfähigkeit, 7]
Sozialkompetenz
Studierende können sich auf tiefer Expertenebene mit der Fachcommunity unterhalten, Erkenntnisse und Methoden diskutieren und ihr Expertenwissen auch Fachabteilungen vermitteln. [Kommunikation, 7]</td></tr>
<tr><td></td><td colspan="6">Selbstständigkeit
Studierende können neue OSINT Anwendungen eigenständig identifizieren und erforschen sowie mit der Fachcommunity diskutieren [Eigenständigkeit/Verantwortung, 7]

Aktuelle Aufgabenstellungen und Probleme aus dem OSINT Bereich können eigenständig anhand der aktuellen Forschung im Print- und Preprintbereich erschlossen werden. [Lernkompetenz, 7]</td></tr>
<tr><td>4</td><td colspan="6">Inhalte:
Vorlesung, Seminar, Praktikum
• Auffrischung relevanter Grundlagen der IT Sicherheit, Digitalen Forensik und Internettechnologien
• Anonymisierung und De-Anonymisierung im Surface-, Deep- und Darknet
• Ermittlungstaktisches- / nachrichtendienstliches Vorgehen
• OSINT Grundlagen, Terminologien, Taxonomien
• OSINT Methoden, Tools, Techniken
• Legaler, moralischer und ethischer Rahmen
• Analyse und Bewertung von OSINT Erkenntnissen
• Praktische Anwendungen
• Wissenschaftliche Recherche, Arbeit und Forschung im OSINT Bereich
• Relevante wissenschaftliche Konferenzen, Journals und Plattformen</td></tr>
</table>

	Empfohlene Literaturangaben: Akhgar, B., Bayerl, P.S., Sampson, F.S.: OpenSource Intelligence Investigation – From Strategy to Implementation, Springer, 2017 Bazzell, M.: Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information, 5. Auflage, CreateSpace Independent Publishing Platform, 2016 U.S.Army: NATO OpenSource Intelligencehandbook, online, http://www.au.af.mil/au/awc/awcgate/nato/osint_hdbk.pdf Attrill, A.: Cyberpsychology, 2015, Oxford University Press Gollmann, D.: Computer Security, 3. Auflage, Wiley, 2012 Tavani, H.T.: Ethics and Technology: Controversies, Questions, and Strategies for Ethical Computing, 4. Auflage, Wiley, 2013 Spinello, R.: Cyberethics: Morality and Law in Cyberspace 6th Edition, Jones & Bartlett Learning, 2016 A Gift of Fire: Social, Legal, and Ethical Issues for Computing Technology, 5th Edition, Pearson, 2017 Biskup, J.: Security in Computing Systems, Springer, 2010 Ausgewählte Literatur bekannter Top-Tier Konferenzen im OSINT Bereich Weitere Literatur wird in der Vorlesung vorgestellt.
5	**Teilnahmevoraussetzungen:** Grundlagen Betriebssysteme und Netzwerke, Grundlagen IT-Sicherheit und Digitaler Forensik, Programmierung in einer Skriptsprache
6	**Prüfungsformen***:* Referat 20 min. inkl. wissenschaftlicher Ausarbeitungen und Poster, Diskussion, benotet Laborarbeit, unbenotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Ausreichend bewertetes Referat erfolgreiche Teilnahme am Praktikum
8	***Verwendbarkeit des Moduls:*** Advanced IT Security M.Sc. WPM in Business and Security Analytics und Systems Engineering M.Eng.
9	***Modulverantwortliche(r):*** Prof. Morgenstern Dozenten: N.N.
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul
11	***Bearbeitungsstand:*** *24.01.2025*

5.2.2 Application Forensics

<table>
<tr><td colspan="7">Modul: Application Forensics</td></tr>
<tr><td colspan="2">Kennnummer:
54000</td><td>Work-load
180 h</td><td>Modulart
PM</td><td>Studiensemester
2</td><td>Dauer
1 Semester</td><td>Häufigkeit
SS</td></tr>
<tr><td>1</td><td colspan="2">Lehrveranstaltung(en)
Vorlesung/Seminar Application Forensics
Projekt Application Forensics</td><td>Sprache
Deutsch oder Englisch (Literaturstudium in Deutsch und Englisch erforderlich)</td><td>Kontakt-zeit
4 SWS / 60 h</td><td>Selbst-studium
120</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="6">Lehrform(en) / SWS:
Vorlesung, Übungen, Seminar: 2 SWS
Projekt: 2 SWS</td></tr>
<tr><td>3</td><td colspan="6">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Die Studierenden verfügen über grundlegende Methoden und spezialisierte Techniken zur forensischen Analyse von digitalen Anwendungsspuren. [Wissen, 7]

Kompetenz Fertigkeiten
Die Studierenden sind in der Lage neue Verfahren zur Analyse neuer Applikationen zu entwickeln. Dabei nutzen sie wissenschaftliche Methoden und bereiten aktuelle Forschungsergebnisse zielgruppengerecht auf. [Systemische Fertigkeiten, 7]

Analyseergebnisse können unter verschiedenen Maßstäben beurteilt werden. [Beurteilungsfähigkeit, 7]

Sozialkompetenz
Die Ergebnisse einer komplexeren forensischen Anwendungsanalyse können einem Fachpublikum vorgestellt und mit ihm diskutiert werden. [Kommunikation, 7]

Selbstständigkeit
Analysemethoden und Techniken zur Untersuchung unbekannter Applikationen können selbstständig erschlossen werden. [Lernkompetenz, 7]</td></tr>
<tr><td>4</td><td colspan="6">Inhalte:
Vorlesung, Seminar, Projekt
• Auffrischung relevanter Grundlagen der IT-Sicherheit, Digitalen Forensik
• Einführung Anwendungsforensik
• Methoden der Anwendungsforensik
• Legaler und ethischer Rahmen
• wissenschaftliches Arbeiten und Berichten
• Praktische Anwendungsanalyse
• wissenschaftlicher Fachvortrag

Empfohlene Literaturangaben:
• Andreas Dewald, Felix Freiling: Forensische Informatik. Books on Demand, 2. Auflage, 2015
Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.</td></tr>
<tr><td>5</td><td colspan="6">Teilnahmevoraussetzungen:
Grundlagen Betriebssysteme und Netzwerke, Grundlagen IT-Sicherheit und Digitaler Forensik, Programmierung in einer Skriptsprache (vorz. Python)</td></tr>
<tr><td>6</td><td colspan="6">Prüfungsformen:
Referat 30 min. inkl. wissenschaftlicher Ausarbeitungen und Poster, Diskussion, benotet
Praktische Arbeit, unbenotet</td></tr>
<tr><td>7</td><td colspan="6">Voraussetzungen für die Vergabe von Kreditpunkten:
Ausreichend bewertetes Referat
erfolgreiche Praktische Arbeit</td></tr>
</table>

8	***Verwendbarkeit des Moduls:*** Advanced IT Security M.Sc.
9	***Modulverantwortliche(r):*** Prof. Morgenstern Dozenten: Prof. Morgenstern
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul
11	***Bearbeitungsstand:*** *24.01.2025*

5.2.3 Applied Cyberpsychology

<table>
<tr><td colspan="8">Modul: Applied Cyberpsychology</td></tr>
<tr><td colspan="2">Kennnummer
54500</td><td>Work-load
180 h</td><td>Modulart
PM</td><td>Studien-semester
2. Semester</td><td>Dauer
1</td><td colspan="2">Häufigkeit
SS</td></tr>
<tr><td>1</td><td colspan="3">Lehrveranstaltung(en)
a.Vorlesung Applied Cyberpsychology
b.Projekt</td><td>Sprache
englisch</td><td>Kontakt-zeit
4 SWS / 60 h</td><td>Selbst-studium
120 h</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="7">Lehrform(en) / SWS:
a.Vorlesung mit Übungen / 2 SWS
b.Projekt / 2 SWS</td></tr>
<tr><td>3</td><td colspan="7">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Lernergebnisbeschreibung einer bestimmten Kompetenz z.B. Fachwissen mit Niveaustufe.
Die Studierenden besitzen ein breites Wissen über Anwendungen psychologischer Methodik und Erkenntnisse im Bereich der Cyberpsychologie.
Die Studierenden besitzen einen Überblick über die Anwendungsmöglichkeiten psychologischer Prinzipien und Methoden im Bereich der IT-Security. Die Studierenden sind vertraut mit den Grundlagen organisationspsychologischer Prinzipien und Entscheidungsprozesse in normalen und kritischen Situationen sowie der Kommunikation in komplexen soziotechnischen Systemen und interdisziplinärer Kooperation. [Wissen, 7]
Kompetenz Fertigkeiten
Selbstständiger Wissenserwerb zu verhaltensrelevanten Problemen und Problemlösungsansätzen unter Verwendung wissenschaftlicher Primärquellen. Kritisches Beurteilen und theoretische sowie methodische Einordnungen neuerer wissenschaftlicher Erkenntnisse. [Instrumentelle Fertigkeiten, 7]
Sozialkompetenz
Studierende können interdisziplinär schriftlich und mündlich verständlich kommunizieren und so zu gemeinsamer Problemlösung beitragen; Erkenntnisse und Methoden diskutieren und ihr Expertenwissen interdisziplinären Communities vermitteln. Fachwissen externer internationaler Experten kann zielgerichtet erlangt, verarbeitet und in vorhandenes Wissen integriert werden. [Kommunikation, 7]
Selbstständigkeit
Studierende erkennen eigenständig Anwendungsgebiete verhaltenswissenschaftlicher Methoden und Prinzipien und nutzen ihre Kenntnisse zu Leistungsverbesserungen bei sich selbst und anderen. Sie können forschungsmethodische Instrumentarien selbstständig auswählen und anwenden. [Eigenständigkeit/Verantwortung, 7]</td></tr>
<tr><td>4</td><td colspan="7">Inhalte:
Biopsychosocial concepts of perception, cognition and action
Decision-making in digital and hybrid environments
Performance under pressure
Expertise and accelerated learning
Foundations of behavior change and teaching concepts
Principles of organizational psychology
Particularities of human behavior in virtual environments and anonymity/pseudonymity
Macrocognition and group effects in online communities and social influences
Principles of neuro-ergonomics and neurocognition
Motivation, emotions and decision-making
Interdisciplinary cooperation and leadership styles, team communication

Empfohlene Literaturangaben:
Attrill-Smith, A., Fullwood, C., Keep, M., & Kuss, D. J. (Eds.). (2019). The Oxford handbook of cyberpsychology. Oxford University Press</td></tr>
<tr><td>5</td><td colspan="7">Teilnahmevoraussetzungen:
Aufnahme Master Advanced IT-Security M.Sc.</td></tr>
<tr><td>6</td><td colspan="7">Prüfungsformen:
Mündliche Prüfung 20 Minuten</td></tr>
</table>

7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandene Prüfung
8	***Verwendbarkeit des Moduls:*** Advanced IT Security M.Sc.
9	***Modulverantwortliche(r):*** Prof. Dr. Sütterlin Dozenten: Prof. Dr. Sütterlin
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul
11	***Bearbeitungsstand:*** *24.01.2025*

5.2.4 Human Factors in IT Security

<table>
<tr><td colspan="8">Modul: Human Factors in IT Security</td></tr>
<tr><td colspan="2">Kennnummer
55000</td><td>Work-load
180 h</td><td>Modulart
PM</td><td colspan="2">Studiensemester
2. Semester</td><td>Dauer
1</td><td>Häufigkeit
SS</td></tr>
<tr><td>1</td><td colspan="3">Lehrveranstaltung(en)
a. Vorlesung Human Factors in IT Security
b. Seminar</td><td>Sprache
englisch</td><td>Kontakt-zeit
4 SWS / 60 h</td><td>Selbst-studium
120 h</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="7">Lehrform(en) / SWS:
a. Vorlesung mit Übungen / 2 SWS
b. Seminar / 2 SWS</td></tr>
<tr><td>3</td><td colspan="7">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Die Studierenden kennen die Grundlagen der Human Factors-Forschung im Bereich der IT-Security. Sie sind vertraut mit der wissenschaftlichen Literatur im inhaltlichen und methodischen Sinne.
Die Studierenden kennen die relevanten Modelle und Theorien zur Erklärung des Zusammenhangs zwischen menschlichem Erleben und Verhalten und Implikationen für IT-Sicherheit. [Wissen, 7]

Kompetenz Fertigkeiten
Die Studierenden sind in der Lage, in sicherheitsrelevanten sozio-technischen Systemen menschliche Risikofaktoren für die IT-Sicherheit zu erkennen, zu quantifizieren, interdisziplinär zu vermitteln und Vorschläge zu entwickeln. Sie sind in der Lage, selbstständig sicherheitsrelevante Fragen mit Hilfe verhaltenswissenschaftlicher Methodik zu operationalisieren und durchzuführen und die Ergebnisse kritisch zu interpretieren. [Beurteilungsfähigkeit, 7]

Sozialkompetenz
Die Studierenden sind in der Lage, mit internationalen Experten in englischer Sprache fachspezifische Themen auf hohem Niveau zu diskutieren, die gewonnenen Informationen zu verarbeiten und vor einem Fachpublikum zu präsentieren. [Kommunikation, 7]

Selbstständigkeit
Die Studierenden verstehen das Lernen als einen komplexen Prozess der die Recherche, das Verständnis und die Verarbeitung von Informationen interdisziplinären Ursprungs beinhaltet. Sie verfügen über die Motivation und Ausdauer um sich in ungewohnte Themengebiete einzuarbeiten und schriftlich auf wissenschaftlichem Niveau auszutauschen. [Lernkompetenz, 7]</td></tr>
<tr><td>4</td><td colspan="7">Inhalte:
Psychological aspects of cybercrime
Internal threats
Social Engineering
Dark Patterns
Expertise and indicators of performance Typologies, profiles and motivations of perpetrators
Security awareness and interventions
Cooperation and communication of IT-security threats and incidents
Ergonomic aspects of IT-security behavior and interface design
Gamification approaches to improved IT-security behavior
Research Methods for IT-security
Recruiting, assessment, performance monitoring, predictors of success

Empfohlene Literaturangaben:
Christen, M., Gordijn, B., & Loi, M. (2020). The ethics of cybersecurity (p. 384). Springer Nature</td></tr>
<tr><td>5</td><td colspan="7">Teilnahmevoraussetzungen:
Aufnahme Master Advanced IT-Security M.Sc.</td></tr>
<tr><td>6</td><td colspan="7">Prüfungsformen:
Mündliche Prüfung, 20 min.</td></tr>
</table>

7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandene Prüfung
8	***Verwendbarkeit des Moduls:*** Master Advanced IT Security M.Sc.
9	***Modulverantwortliche(r):*** Prof. Dr. Sütterlin
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul
11	***Bearbeitungsstand:*** *24.01.2025*

5.2.5 Master-Thesis

<table>
<tr><td colspan="7">Modul: Master-Thesis</td></tr>
<tr><td colspan="2">Kennnummer
60100</td><td>Work-load
900 h</td><td>Modulart
PM</td><td>Studiensemester
3</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS und SS</td></tr>
<tr><td>1</td><td colspan="2">Lehrveranstaltung(en)
Projekt Master-Thesis
Mündliche Prüfung
Kolloquium</td><td>Sprache
Deutsch (deutsches und englisches Literaturstudium erforderlich)</td><td>Kontakt-zeit
--</td><td>Selbst-studium
(Präsenz & Selbst-studium)</td><td>Credits (ECTS)
30</td></tr>
<tr><td>2</td><td colspan="6">Lehrform(en) / SWS:
Projekt, betreute selbständige wissenschaftliche Arbeit</td></tr>
<tr><td>3</td><td colspan="6">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Abhängig vom Thema der Masterarbeit [Wissen, 7]</td></tr>
<tr><td></td><td colspan="6">Kompetenz Fertigkeiten
Mit der Master-Thesis zeigt der Student, dass er unter Anleitung selbständig umfangreiche wissenschaftliche Themen bearbeiten kann. Er wird praxisorientierte oder theoretische Themenstellungen nach wissenschaftlichen Kriterien analysieren, strukturieren und ergebnisorientiert bearbeiten. Die Master – Thesis dokumentiert seine Arbeit und erfüllt die Kriterien eines wissenschaftlichen Berichts. [Systemische Fertigkeiten, 7]</td></tr>
<tr><td></td><td colspan="6">Sozialkompetenz
Abhängig vom Thema und Ort der Ausarbeitung (z.B. ein externes Unternehmen) [Team-/Führungsfähigkeit, 7]</td></tr>
<tr><td></td><td colspan="6">Selbstständigkeit
Master-Thesis ist das größte Projekt im gesamten Master-Studium, das die Studierenden nachweislich selbständig und verantwortlich ausführen. [Eigenständigkeit/Verantwortung, 7]</td></tr>
<tr><td>4</td><td colspan="6">Inhalte:
Abhängig von Thema und Inhalt der Master-Thesis</td></tr>
<tr><td></td><td colspan="6">Empfohlene Literaturangaben:
Abhängig vom Thema und Inhalt der Master-Thesis</td></tr>
<tr><td>5</td><td colspan="6">Teilnahmevoraussetzungen:
Ggf. formal geregelt in der Prüfungsordnung</td></tr>
<tr><td>6</td><td colspan="6">Prüfungsformen:
Master-Thesis (Ma.), benotet.
Mündliche Prüfung 20 min., benotet
Referat 25 Min, benotet</td></tr>
<tr><td>7</td><td colspan="6">Voraussetzungen für die Vergabe von Kreditpunkten:
Bestehen die Masterthesis (schriftliche Ausarbeitung).
Bestehen die mündliche Prüfung, Bestehen des Referats</td></tr>
<tr><td>8</td><td colspan="6">Verwendbarkeit des Moduls:
Advanced IT Security, M.Sc.</td></tr>
<tr><td>9</td><td colspan="6">Modulverantwortliche(r):
Prof. Dr. German Nemirovski
Dozenten: abhängig vom Thema und Inhalt der Master-Thesis</td></tr>
<tr><td>10</td><td colspan="6">Optionale Informationen:
Studiengangsspezifische, zusätzliche Informationen zum Modul</td></tr>
<tr><td>11</td><td colspan="6">Bearbeitungsstand:
24.01.2025</td></tr>
</table>

5.3 Pflichtmodule Business and Security Analytics M.Sc.

5.3.1 Data and Web Mining

<table>
<tr><td colspan="7">Modul: Data and Web Mining</td></tr>
<tr><td colspan="2">Kennnummer
51300</td><td>Workload
180 h</td><td>Modulart
P</td><td>Studiensemester
1</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS und SS</td></tr>
<tr><td>1</td><td colspan="2">Lehrveranstaltung(en)
Vorlesung Data- and Web-Mining
Praktikum Semantic Web</td><td>Sprache
Deutsch (deutsches und englisches Literatur-studium erforderlich)</td><td>Kontakt-zeit
4 SWS / 60 h</td><td>Selbst-studium
120</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="6">Lehrform(en) / SWS:
Vorlesung: 2 SWS
Praktikum: 2 SWS</td></tr>
<tr><td>3</td><td colspan="6">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Die Studierenden kennen die grundlegenden Methoden des Data- und Web-Mining. Sie verstehen die Konzepte, kennen die Funktionsmechanismen der Methoden sowie die Rahmenbedingungen für deren Einsatz. [Wissen, 7]
Kompetenz Fertigkeiten
Die Studierenden sind in der Lage die Methoden des Data- und Web-Mining in realen Anwendungssituationen sinnvoll einzusetzen. Sie sind in der Lage aus eine Menge von in Frage kommenden Methoden die geeigneten auszuwählen und diese einzusetzen. [Instrumentelle Fertigkeiten, 7]

Die Ergebnisse aus der Anwendung der Methoden können eingeordnet und kritisch bewertet werden. [Beurteilungsfähigkeit, 7]
Sozialkompetenz
Die Studierenden sind in der Lage die Ergebnisse ihrer Analysen einem Fachkundigen zu erläutern. [Kommunikation, 7]
Selbstständigkeit
Die Studierenden sind in der Lage, eigenständig Datenanalysen zu konzipieren, auszuführen und die Ergebnisse verständlich darzustellen. [Eigenständigkeit/Verantwortung, 7]</td></tr>
<tr><td>4</td><td colspan="6">Inhalte:
Grundlagen das Data- und Web Mining
Prozessuale Sicht auf das Data Mining (Crisp-DM)
Data Preprocessing (Data Cleansing, Missing Values, Dimensionsreduzierung…)

Clusteranalyse (hierarchisch, partitionierend)
Klassifikation (Entscheidungsbäume, einfache Neuronale Netze, Support Vector Machines,
Assoziations Daten (A-Priori, FP-Growth)
Sequenzanalyse
Web Mining (Web Content Analyse)

Empfohlene Literaturangaben:

Han, J et al. – Data Mining – Concepts and Techniques, Elsevier – Morgan Kaufmann, 3rd edit., 2012
Thomas A. Runkler, Data Mining –Methoden und Algorithmen intelligenter Datenanalyse, Springer Vieweg, 2010
Ian H. Witten, Eibe Frank, Mark A. Hall, Data Mining: Practical Machine Learning Tools and Techniques, 3rd edit., Elsevier, 2011;
Florin Gorunescu, Data Mining: Concepts, Models and Techniques, Springer, 2011,
Markus Hofmann, Ralf Klinkenberg, Rapidminer: Data Mining Use Cases and Business Analytics Applications, Productivity Pr Inc, 2013,
Bing Liu, Web Data Mining: Exploring Hyperlinks, Contents, and Usage Data (Data-Centric Systems and Applications), Springer; 2. Auflage, 2011,
Beierle, C., Kern-Isberner, G. – Methoden wissensbasierter Systeme – Grundlagen, Algorithmen, Anwendungen, Vieweg+Teubner, 5. Aufl. 2014</td></tr>
</table>

5	**Teilnahmevoraussetzungen:** Es existieren keine Teilnahmevoraussetzungen.
6	**Prüfungsformen***:* Klausur 90 min., benotet Praktische Arbeit, unbenotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Die erfolgreiche praktische Arbeit im Praktikum wird durch Semesteraufgaben, die eigenständig zu bearbeiten sind, nachgewiesen.
8	***Verwendbarkeit des Moduls:*** Business and Security Analytics, M.Sc.
9	***Modulverantwortliche(r):*** Prof. Dr. Bernd Stauß Dozenten: Prof. Dr. Bernd Stauß, N.N.
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul
11	***Bearbeitungsstand:*** *24.01.2025*

5.3.2 Large Scale Data Analysis and Parallelization

<table>
<tr><td colspan="7">Modul: Large-Scale Data Analysis and Parallelization</td></tr>
<tr><td colspan="2">Kennnummer
51400</td><td>Workload
180 h</td><td>Modulart
P</td><td>Studiensemester
1</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS und SS</td></tr>
<tr><td>1</td><td colspan="2">Lehrveranstaltung(en)
Vorlesung Large-Scale Data Analysis and Parallelization
Praktikum Large-Scale Data Analysis and Parallelization</td><td>Sprache
Deutsch oder Englisch, wenn von den Modulteil-nehmern gewünscht (deutsches und englisches Literatur-studium erforderlich)</td><td>Kontakt-zeit
4 SWS / 60 h</td><td>Selbst-studium
120</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="6">Lehrform(en) / SWS:
Vorlesung: 2 SWS
Praktikum: 2 SWS</td></tr>
<tr><td>3</td><td colspan="6">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Die Studierenden
- kennen Systeme und Techniken für die parallele Datenverarbeitung
- kennen die Aufgabenstellungen aus dem Themengebiet von Big Data [Wissen, 7]
Kompetenz Fertigkeiten
Lernergebnisse (Kompetenzen) bei:
Die Studierenden
- sind in der Lage die Problem- und Aufgabenstellungen mit Bezug auf das Themengebiet Big Data zu erkennen, diese, basierend auf eigenem Wissen und durch die gezielte Recherche zu beschreiben, Lösungsansätze zu entwickeln und diese allein oder im Team umzusetzen.
- sind in der Lage, eine anwendungsbezogene Evaluation von Daten, –Zugriffs- und –Verwaltungstechniken sowie von den diese Techniken implementierenden Systemen auszuführen, und darauf basierend eine zielgerechte Auswahl zu treffen.
- sind in der Lage wissenschaftliche Beiträge im Themenbereich Big Data eigenständig zu lesen und qualitative Vergleiche der gelesenen Beiträge systematisch zu präsentieren. [Instrumentelle Fertigkeiten, 7]
Sozialkompetenz
Die Studierenden können im Rahmen einer eigenständigen Arbeit neue Ansätze für einen Big Data Prozess mit konkreter Aufgabenstellung entwickeln [Team-/Führungsfähigkeit, 7]</td></tr>
<tr><td></td><td colspan="6">Selbstständigkeit
Die Studierenden sind in der Lage komplexe Aufgaben verantwortungsvoll zu erfüllen, realistische Ziele zu definieren und diese konsequent zu verfolgen.
[Eigenständigkeit/Verantwortung, 7]</td></tr>
<tr><td>4</td><td colspan="6">Inhalte:
Vorlesung:
- Überblick zu No-SQL-Datenbanken
- Überblick zu Graphendatenbanken
- Architekturen für verteiltes und paralleles Datenmanagement und Datenverteilung
- Verteilte Anfragebearbeitung
- Clustering, Map Reduce, YARN, Tez
- Verteilte Datenbanken
- Vertikale/horizontale Fragmentierung
- Fragmentierungstransparenz
- Transaktionskontrolle
- Frameworks für Skalierung und Parallelisierung der Datenzugriffe am Beispiel von Apache Hadoop, Spark und verteilten RDBMS</td></tr>
</table>

	Praktikum: Arbeiten mit Apache Hadoop, Spark Clustern, IBM Cloud, Azure, IBM Data Warehouse Arbeiten mit MongoDB, Apache Cassandra, Neo4J Arbeiten mit Injectiontools wie Apache Nifi, Talend, IBM NodeRed
	Empfohlene Literaturangaben: keine
5	**Teilnahmevoraussetzungen:** keine
6	**Prüfungsformen***:* Klausur 90 min., benotet Praktische Arbeit, unbenotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Am Ende des Semesters ist eine 90-minütige schriftliche Prüfung zu schreiben. Während des Semesters sind mehrere Praktikumsaufgaben zu bearbeiten.
8	***Verwendbarkeit des Moduls:*** Business and Security Analytics, M.Sc.
9	***Modulverantwortliche(r):*** Prof. Dr. Thomas Eppler Dozenten: Prof. Dr. Thomas Eppler
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul
11	***Bearbeitungsstand:*** *24.01.2025*

5.3.3 Strategic IT Management

<table>
<tr><td colspan="7">Modul: Strategic IT Management</td></tr>
<tr><td colspan="2">Kennnummer
51500</td><td>Workload
180 h</td><td>Modulart
P</td><td>Studiensemester
1</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS und SS</td></tr>
<tr><td>1</td><td colspan="2">Lehrveranstaltung(en)
Vorlesung Strategic IT-Management
Fallstudie Strategic IT-Management</td><td>Sprache
Deutsch (deutsches und englisches Literatur-studium erforderlich)</td><td>Kontakt-zeit
4 SWS / 60 h</td><td>Selbst-studium
120</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="6">Lehrform(en) / SWS:
Vorlesung: 2 SWS
Fallstudie: 2 SWS</td></tr>
<tr><td>3</td><td colspan="6">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Die Studierenden
• kennen Zielstellung, Zielgruppen und den Aufbau von IT-Strategien
• kennen Instrumente zur Planung, Steuerung und Kontrolle von IT-Bereichen
• kennen die strategischen Herausforderungen der IT-Sicherheit im digitalen Zeitalter
• kennen die strategische Bedeutung von IT Governance, Risk and Compliance Management (IT-GRC) für Unternehmen, IT-Organisation und CIO
• kennen innovative Geschäftsmodelle der digitalen Plattformökonomie aus Sicht der IT
[Wissen, 7]
Kompetenz Fertigkeiten
Die Studierenden
• können den Einsatz der Informationstechnologie im Kontext der strategischen Ausrichtung des Unternehmens bewerten und einordnen
• können die Herausforderungen, Aufgaben und methodisches Vorgehen des IT-Management beschreiben
• können die Auswirkungen von Digitalisierung und speziell der digitalen Plattformökonomie auf das IT-Management skizzieren
• beherrschen die differenzierte Einordnung von IT-Sicherheit und IT-Governance, Risk and Compliance Management (IT-GRC) in den Kontext des IT-Managements
[Instrumentelle Fertigkeiten, 7]
Die Studierenden
• können in umfangreichen, realitätsnahen Fallstudien die Unternehmenssituation analysieren, strategische Aspekte vor dem Hintergrund von Branche sowie Unternehmensumwelt bewerten, die Herausforderungen für IT-Organisationen und das IT-Management systematisieren
• können weiterhin – durch zielgerichtete Abstraktionstechniken – Grundzüge von IT-Strategien und Maßnahmenkataloge für das IT-Management entwickeln
[Systemische Fertigkeiten, 7]
Sozialkompetenz
Die Studierenden sind in der Lage, die komplexen Fallstudien zum IT-Management – im Kontext aktueller Trends und Entwicklungen in IT und Digitalisierung – in einem Team zu bearbeiten und die Teamarbeit selbst zu organisieren
[Team-/Führungsfähigkeit, 7]

Zielgruppenorientierter Einsatz von Präsentationsmethoden und Dokumentationstechniken auf Management-Niveau
[Kommunikation, 7]
Selbstständigkeit
Die Studierenden können tiefergehende Problemstellungen auch in komplexen Fallstudien erkennen, methodisch bearbeiten, lösungs- sowie kontextbezogen recherchieren, auf das Wesentliche im Managementkontext abstrahieren und zielgerichtet lösen
[Eigenständigkeit/Verantwortung, 7]</td></tr>
<tr><td>4</td><td colspan="6">Inhalte:
• IT-Strategieentwicklung
• Rolle und Aufgaben der IT im Unternehmen</td></tr>
</table>

	• Rolle, Aufgaben und Pflichten des Chief Information Officer (CIO) im Unternehmen • Aufgaben, Rollen und Gremien im IT-Management • Aufbau von IT-Organisationen und internationale Koordination • Business-IT-Alignment mit internen und externen Kunden • IT-Sicherheit und IT Governance, Risk and Compliance Management (IT-GRC) • IT-Service- und Prozessmanagement • IT-Ressourcenmanagement • Management des IT-Applikationsportfolios • IT-Partnermanagement: Relationship Management und Sourcing-Strategien • Sourcing Strategien: Business Process Outsourcing, Application Outsourcing, IT-Infrastruktur Outsourcing und Cloud Computing • IT-Projekt- und Projektportfoliomanagement • IT-Planung und IT-Controlling • IT-Management Cockpits • Umgang mit Schatten-IT • Digitalisierung, Digitale Transformation und Digitale Plattformökonomie • Industrie 4.0 im Kontext von Industrieunternehmen • IT-Unterstützung innovativer Geschäftsmodelle in der Plattformökonomie
	Empfohlene Literaturangaben: Porter, M. E.: Wettbewerbsstrategie: Methoden zur Analyse von Branchen und Konkurrenten, 12. Auflage, campus, 2013 Porter, M. E.: Wettbewerbsvorteile: Spitzenleistungen erreichen und behaupten, 8. Auflage, campus, 2014 Malik, F.: Strategie des Managements komplexer Systeme: Ein Beitrag zur Management-Kybernetik evolutionärer Systeme, 11. Auflage, 2015 Camenzind, A./Fueglistaller, U.: Strategisches Denken in KMU und die Lehren von Clausewitz, Verlag Neue Zürcher Zeitung, 2014 Simon, H./Von der Gathen, A.: Das große Handbuch der Strategieinstrumente: Werkzeuge für eine erfolgreiche Unternehmensführung, 2. Auflage, Campus, 2010 Hofmann, J./Schmidt, W.: Masterkurs IT-Management - Grundlagen, Umsetzung und erfolgreiche Praxis für Studenten und Praktiker. 2. Auflage, Vieweg und Teubner, 2010 Tiemeyer, E.: Handbuch IT-Management: Konzepte, Methoden, Lösungen und Arbeitshilfen für die Praxis, 7. Auflage, Hanser Verlag, 2020 Oswald G./Krcmar, H.: Digitale Transformation: Fallbeispiele und Branchenanalysen (Informationsmanagement und digitale Transformation), Springer Gabler, 2018 Krcmar, H.: Informationsmanagement, 6. Auflage, Springer, 2015 Resch, O.: Einführung in das IT-Management - Grundlagen, Umsetzung, Best Practice, 4. Auflage, Erich Schmidt Verlag, 2016 Hermann, Ulrich: Digitalisierung im Industrieunternehmen: Die Chancen der digitalen Ökonomie der Dinge erkennen, entwickeln und erfolgreich umsetzen, Apprimus, 2019 Zimmermann, S.: Der Umgang mit Schatten-IT in Unternehmen: Eine Methode zum Management intransparenter Informationstechnologie Hanschke, I.: Strategisches Management der IT-Landschaft: Ein praktischer Leitfacen für das Enterprise Architecture Management, 3. Auflage, Hanser Verlag, 2013 Kersten, H./Klett, G./Reuter, J./Schröder, K.-W.: IT-Sicherheitsmanagement nach der neuen ISO 27001: ISMS, Risiken, Kennziffern, Controls, 4. Auflage, Springer Vieweg, 2019 Sowa, A.: „Management der Informationssicherheit: Kontrolle und Optimierung", Springer Vieweg, 2017 Mangiapane, M./Büchler, R.: Modernes IT-Management: Methodische Kombination von IT-Strategie und IT-Reifegrademodell, Springer Vieweg, 2015 Osterwald, A./Pigneur, Y.: Business Model Generation: Ein Handbuch für Visionäre, Spielveränderer und Herausforderer, campus, 2011 Osterwald, A./Pigneur, Y./Bernarda, G./Smith, A.: Value Proposition Design: Entwickeln Sie Produkte und Services, die Ihre Kunden wirklich wollen, campus, 2015 Gärtner, C./Heinrich. C. (Hrsg.): Fallstudien zur Digitalen Transformation: Case Studies für die Lehre und praktische Anwendung, Springer Gabler, 2017 Von Engelhardt, S./Petzold, S. (Hrsg.): Das Geschäftsmodell-Toolbox für digitale Ökosysteme, Campus, 2019 Srnicek, N.: Plattform-Kapitalismus, Hamburger Edition, 2018 Jaekel: Die Macht der digitalen Plattformen: Wegweiser im Zeitalter einer expandierenden Digitalsphäre und künstlicher Intelligenz, Springer Vieweg, 2017 Parker, G. G./Van Alstyne, M.W./Choudary, S. P.: Die Plattform-Revolution im E-Commerce: Von Airbnb, Uber, PayPal und Co. lernen: Wie neue Plattform-Geschäftsmodelle die Wirtschaft verändern, mitp, 2017 Clement, R./Schreiber, D./Bossauer, P./Pakusch, C.: Internet-Ökonomie: Grundlagen und Fallbeispiele der digitalen und vernetzten Wirtschaft, 4. Auflage, Springer Gabler, 2020

5	**Teilnahmevoraussetzungen:** Kenntnisse auf den folgenden Lehrgebieten sind hilfreich: • IT-Management, IT-Consulting und E-Business • IT-Sicherheit und IT Governance, Risk and Compliance Management (IT-GRC)
6	**Prüfungsformen***:* Seminararbeit, benotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Erfolgreich bearbeitete Seminararbeit
8	***Verwendbarkeit des Moduls:*** Business and Security Analytics, M.Sc.
9	***Modulverantwortliche(r):*** Prof. Dr. Nils Herda Dozent: Prof. Dr. Nils Herda
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul
11	***Bearbeitungsstand:*** *24.01.2025*

5.3.4 Business Process Management and Data Compliance

<table>
<tr><td colspan="7">Modul: Business Process Management and Data Compliance</td></tr>
<tr><td colspan="2">Kennnummer
52300</td><td>Workload
180 h</td><td>Modulart
P</td><td>Studiensemester
2</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS und SS</td></tr>
<tr><td>1</td><td colspan="2">Lehrveranstaltung(en)
Vorlesung Business Process Management and Data Compliance
Fallstudie Business Process Management and Data Compliance</td><td>Sprache
Deutsch (deutsches und englisches Literatur-studium erforderlich)</td><td>Kontakt-zeit
4 SWS / 60 h</td><td>Selbst-studium
120</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="6">Lehrform(en) / SWS:
Vorlesung: 2 SWS
Fallstudie: 2 SWS</td></tr>
<tr><td>3</td><td colspan="6">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen

Die Studierenden
• kennen Merkmale, Aufbau und Prinzipien von Prozessen und Geschäftsprozesse im Kontext der betrieblichen Ablauforganisationen
• kennen betriebliche Wertschöpfungsstrukturen und Anforderungen an das unternehmensweite Prozessmanagement
• kennen die gängigen Modellierungsmethoden und können diese auf Meta-Modellebene systematisieren
• kennen Kennzahlen und Kennzahlensysteme für das Monitoring von Geschäftsprozessen
• kennen den Datenbegriff und Methodiken zum Master Data Management
• kennen die Herausforderungen zum Datenschutz im Kontext der betrieblichen Erfassung, Verarbeitung und Speicherung personenbezogener Daten
• kennen Zielstellung, methodisches Vorgehen und Kontrollmechanismen zu Data Compliance, auch im digitalen Kontext [Wissen, 7]

Kompetenz Fertigkeiten

Die Studierenden
• können betriebliche Ablaufstrukturen in gängigen Modellierungsnotationen modellieren und beherrschen den Einsatz von Abstraktionstechniken
• können betriebliche Prozesse auf Automationspotenzial und Resilienzfähigkeit hin analysieren und optimieren
• können Prozesse auf Basis von Kennzahlen und Kennzahlensystemen systematisieren und vergleichen sowie Monitoring- und Reporting-Strukturen aufbauen
• können den betrieblichen Datenschutz und Data Compliance-Strukturen beschreiben und systematisieren
[Instrumentelle Fertigkeiten, 7]

Sozialkompetenz

Die Studierenden sind in der Lage, die komplexen Fallstudien zu Business Process Management and Data Compliance – im Kontext aktueller Trends und Entwicklungen in IT und Digitalisierung – in einem Team zu bearbeiten und die Teamarbeit selbst zu organisieren
[Team-/Führungsfähigkeit, 7]

Zielgruppenorientierter Einsatz von Präsentationsmethoden und Dokumentationstechniken auf Management-Niveau
[Kommunikation, 7]

Selbstständigkeit

Die Studierenden können tiefergehende Problemstellungen auch in komplexen Fallstudien erkennen, methodisch bearbeiten, lösungs- sowie kontextbezogen recherchieren, auf das Wesentliche im Managementkontext abstrahieren und zielgerichtet lösen
[Eigenständigkeit/Verantwortung, 7]</td></tr>
</table>

4	**Inhalte*:*** • Prozesse und Geschäftsprozesse • Betriebliche Kernkompetenzen und unternehmensweite Kernprozesse • Betriebliche Wertschöpfung, Wertschöpfungsstufen und Wertschöpfungsketten • Prozessmanagement und Prozessportfolio • Operatives versus strategisches Prozessmanagement • Enterprise Architecture Management und Business Architecture Management • Aufbau und Vergleich von Modellierungsmethoden für den betrieblichen Einsatz • Meta-Modelle und Meta-Meta-Modelle • Referenzmodelle und Prozesslandkarten • Kennzahlen und Kennzahlensysteme für das Monitoring von Geschäftsprozessen • Daten und Master Data Management • Datenschutz im Kontext der betrieblichen Unternehmung • Erfassung, Verarbeitung und Speicherung von Daten im Kontext gesetzlicher Vorgaben (Bundesdatenschutzgesetz und Datenschutz-Grundverordnung) • Zielstellung, methodisches Vorgehen und Kontrollmechanismen zu Data Compliance • Data Compliance im Kontext von Digitalisierung und digitaler Plattformökonomie *Empfohlene Literaturangaben:* Hofmann, J./Schmidt, W.: Masterkurs IT-Management - Grundlagen, Umsetzung und erfolgreiche Praxis für Studenten und Praktiker. 2. Auflage, Vieweg und Teubner, 2010 Tiemeyer, E.: Handbuch IT-Management: Konzepte, Methoden, Lösungen und Arbeitshilfen für die Praxis, 7. Auflage, Hanser Verlag, 2020 Hanschke, I.: Strategisches Management der IT-Landschaft: Ein praktischer Leitfacen für das Enterprise Architecture Management, 3. Auflage, Hanser Verlag, 2013 Kersten, H./Klett, G./Reuter, J./Schröder, K.-W.: IT-Sicherheitsmanagement nach der neuen ISO 27001: ISMS, Risiken, Kennziffern, Controls, 4. Auflage, Springer Vieweg, 2019 Schmelzer, Herrmann J./Sesselmann, Wolfgang: Geschäftsprozessmanagement in der Praxis: Kunden zufrieden stellen, Produktivität steigern und Wert erhöhen, Hanser, 2013 Keuper, Frank/Neumann, Fritz: Corporate Governance, Risk Management und Compliance: Innovative Konzepte und Strategien,Gabler, 2010 Nestler, D./Modi, J. (Hrsg.: Institut der Wirtschaftsprüfer in Deutschland e.V.): Leitfaden IT-Compliance: Anforderungen, Chancen und Umsetzungsmöglichkeiten, IDW, 2020. Klotz, M.: IT-Compliance: Ein Überblick, 1. Auflage, dpunkt, 2009 Rath, M.; Sponholz, R.: IT-Compliance – Erfolgreiches Management regulatorischer Anforderungen, o. A., Erich Schmidt, 2009 Sowa, A.: „Management der Informationssicherheit: Kontrolle und Optimierung", Springer Vieweg, 2017 Sowa, A./Duscha, P./Schreiber, S.: IT-Revision, IT-Audit und IT-Compliance: Neue Ansätze für die IT-Prüfung, Springer Vieweg, 2019 Hermann, Ulrich: Digitalisierung im Industrieunternehmen: Die Chancen der digitalen Ökonomie der Dinge erkennen, entwickeln und erfolgreich umsetzen, Apprimus, 2019 Gärtner, C./Heinrich. C. (Hrsg.): Fallstudien zur Digitalen Transformation: Case Studies für die Lehre und praktische Anwendung, Springer Gabler, 2017 Von Engelhardt, S./Petzold, S. (Hrsg.): Das Geschäftsmodell-Toolbox für digitale Ökosysteme, Campus, 2019 Srnicek, N.: Plattform-Kapitalismus, Hamburger Edition, 2018 Jaekel: Die Macht der digitalen Plattformen: Wegweiser im Zeitalter einer expandierenden Digitalsphäre und künstlicher Intelligenz, Springer Vieweg, 2017 Parker, G. G./Van Alstyne, M.W./Choudary, S. P.: Die Plattform-Revolution im E-Commerce: Von Airbnb, Uber, PayPal und Co. lernen: Wie neue Plattform-Geschäftsmodelle die Wirtschaft verändern, mitp, 2017 Clement, R./Schreiber, D./Bossauer, P./Pakusch, C.: Internet-Ökonomie: Grundlagen und Fallbeispiele der digitalen und vernetzten Wirtschaft, 4. Auflage, Springer Gabler, 2020
5	**Teilnahmevoraussetzungen:** Kenntnisse auf den folgenden Lehrgebieten sind hilfreich: • IT-Management, IT-Consulting und E-Business • IT-Sicherheit und IT Governance, Risk and Compliance Management (IT-GRC)
6	**Prüfungsformen*:*** Mündliche Prüfung (20 min.), benotet Referat, unbenotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Erfolgreich bearbeitete Seminararbeit

8	***Verwendbarkeit des Moduls:*** Business and Security Analytics, M.Sc.
9	**Modulverantwortliche(r):** Prof. Dr. Nils Herda Dozenten: Prof. Dr. Nils Herda, Prof. Dr. Bernd Stauß
10	**Optionale Informationen:** Studiengangsspezifische, zusätzliche Informationen zum Modul
11	**Bearbeitungsstand:** 24.01.2025

5.3.5 Advanced Statistic

<table>
<tr><td colspan="7">Modul: Advanced Statistics</td></tr>
<tr><td colspan="2">Kennnummer
52400</td><td>Workload
180 h</td><td>Modulart
P</td><td>Studiensemester
2</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS und SS</td></tr>
<tr><td>1</td><td colspan="2">Lehrveranstaltung(en)
Vorlesung & Seminar Advanced Statistics
Übungen Advanced Statistics</td><td>Sprache
Deutsch und Englisch (deutsches und englisches Literatur-studium erforderlich)</td><td>Kontakt-zeit
4 SWS / 60 h</td><td>Selbst-studium
120</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="6">Lehrform(en) / SWS:
Vorlesung & Seminar: 2 SWS
Übungen: 2 SWS</td></tr>
<tr><td>3</td><td colspan="6">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Studierende kennen die grundlegenden Begriffe der Wahrscheinlichkeitstheorie und können diese anwenden [Wissen, 7]
Kompetenz Fertigkeiten
Die Studierenden können den Stoff praktisch in der Programmiersprache R für Analysen umsetzen [Instrumentelle Fertigkeiten, 7]
Sozialkompetenz
Die Studierenden können statistische Sachverhalte anderen vermitteln. [Kommunikation, 7]
Selbstständigkeit
Die Studierenden können selbstständig Analysen mittels der Programmiersprache R durchführen. [Eigenständigkeit/Verantwortung, 7]</td></tr>
<tr><td>4</td><td colspan="6">Inhalte:
R-Grundlagen.

Stochastische Grundlagen (Wahrscheinlichkeit, Bedingte Wahrscheinlichkeit, Satz von Bayes) Zufallsvariablen, Erwartungswert, Varianz, Stichproben, Lage- und Streumaße

Bootstrapping, Konfidenzintervalle, Verteilungen (Binomialverteilung, Poisson-Verteilung, Geometrische Verteilung, Exponentialverteilung, Normalverteilung, Betaverteilung)

Signifikanz- und Hypothesentests (A/B-Tests, Permutationstests, ANOVA), Korrelationen, Maximum-Likelihood, Lineare Regression.

Empfohlene Literaturangaben:
Introduction to Statistical Thought☐ISBN: 978-1616100483
http://people.math.umass.edu/~lavine/Book/book.html
Introduction to Probability and Statistics UsingR ISBN: 978-0-557-24979-4
http://cran.r-project.org/web/packages/IPSUR/vignettes/IPSUR.pdfAn Introduction to Statistical Learning: with Applications in R Gareth James, Daniela Witten, Trevor Hastie, Robert TibshiraniSpringer Texts in Statistics, 11. Juli 2016, ISBN-10: 1461471370
Die "'offizielle"' R-Einführung☐ISBN: 978-0954612085
cran.r-project.org/doc/manuals/R-intro.pdf R-Kurs der Uni Augsburg: stats.math.uni-augsburg.de/~theus/r-kurs.pdf</td></tr>
<tr><td>5</td><td colspan="6">Teilnahmevoraussetzungen:
Grundlegende Programmierkenntnisse müssen da sein.</td></tr>
<tr><td>6</td><td colspan="6">Prüfungsformen:
Klausur 90 min., benotet
Referat, unbenotet</td></tr>
<tr><td>7</td><td colspan="6">Voraussetzungen für die Vergabe von Kreditpunkten:
Bestandene Klausur und Referat</td></tr>
</table>

8	***Verwendbarkeit des Moduls:*** Business and Security Analytics, M.Sc., Systems Engineering M.Eng.
9	***Modulverantwortliche(r):*** Prof. Dr. Nemirovski Dozenten: Prof. Dr. Nemirovski
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul
11	***Bearbeitungsstand:*** *24.01.2025*

5.3.6 Security Analytics

<table>
<tr><td colspan="7">Modul: Security Analytics</td></tr>
<tr><td>Kennnummer
52500</td><td>Workload
180</td><td>Modulart
PM</td><td colspan="2">Studiensemester
2</td><td>Dauer
1</td><td>Häufigkeit
SS</td></tr>
<tr><td>1</td><td colspan="2">Lehrveranstaltung(en)
a. 52505 Security Analytics
b. 52510 Projekt Security Analytics</td><td>Sprache
deutsch oder englisch</td><td>Kontakt-zeit
a. 30
b. 30</td><td>Selbst-studium
120</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="6">Lehrform(en) / SWS:
a. Vorlesung, b. Projektarbeit</td></tr>
<tr><td>3</td><td colspan="6">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Die Studierenden kennen den aktuellen Forschungsstand zu den Themenbereichen Security Analytics wie Malware Analytics or/and Security Network Package and Profess Analytics. [Wissen, 7]
Vertieftes Verstehen von Semantic Web -Technologien als Instrument für interoperable Wissensbeschreibung [Wissen, 7]
Kompetenz Fertigkeiten
Die Studierenden können den Analytischen Prozesse auf konkrete Aufgabenstellungen anwenden und mit spezifischen Methoden und Tools umsetzen. [Instrumentelle Fertigkeiten, 7]
Die Studierenden können im Rahmen einer eigenständigen Arbeit neue Ansätze für einen Security Analytics Prozess mit konkreter Aufgabenstellung entwickeln. [Systemische Fertigkeiten, 7]
Sozialkompetenz
Sind in der Lage komplexe Aufgaben in einem Team zu bearbeiten, die Teamarbeit zu organisieren und die Rollen effektiv zu verteilen. [Team-/Führungsfähigkeit, 7]
Selbstständigkeit
Sind in der Lage komplexe Aufgaben verantwortungsvoll zu erfüllen, realistische Ziele zu definieren und diese konsequent zu verfolgen.
[Eigenständigkeit/Verantwortung, 7]</td></tr>
<tr><td>4</td><td colspan="6">Inhalte:
Definition und Begriffserklärung,
Security Analytics Use Cases,
Data Souesess und Methoden der Datensammlung ,
Real time Datensammeln,
Anwendung der Security Analytics-Ergebnisse und ihr Impact,
Basic security analytics Costs,
Advanced persistent threats,
Security Analytics und Digitale Forensic,
Übersicht der security analytics tools and services, u.a.:
Blue Coat Security Analytics Platform,
Lancope Stealth Watch System,
Juniper Networks JSA Series Secure Analytics,
EMC RSA Security Analytics NetWitness,
FireEye Threat Analytics Platform,
Arbor Networks Security Analytics,
Click Security Click Commander,
Hexis Cyber Solutions' NeatBeat MON,
Sumo Logics' cloud service.,
Security Onion.

Empfohlene Literaturangaben:
Hitzler, P., Krötzsch, M., Rudolph, S., & Sure, Y. (2007). Semantic Web: Grundlagen. Springer-Verlag.

Dengel, Andreas, ed. Semantische Technologien: Grundlagen. Konzepte. Anwendungen. Springer-Verlag, 2011.</td></tr>
</table>

	Ege, Börteçin, Bernhard Humm, and Anatol Reibold, eds. Corporate Semantic Web: Wie semantische Anwendungen in Unternehmen Nutzen stiften. Springer-Verlag, 2015.
5	**Teilnahmevoraussetzungen:** Grundkenntnisse in formalen Logiken (DQR 3), Kenntnisse in Web Technologien und auszeichnungssprachen (DQR 5)
6	**Prüfungsformen***:* Klausur 90 Min. (Modulprüfung) benotet, Praktische Arbeit (Projekt-Prüfung) unbenotet.
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandene Klausur und die praktische Arbeit
8	***Verwendbarkeit des Moduls:*** Business und Security Analysis MSc.
9	***Modulverantwortliche(r):*** Prof. Dr. German Nemirovski
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul
11	***Bearbeitungsstand:*** *24.01.2025*

5.3.7 Master-Thesis

<table>
<tr><td colspan="7">Modul: Master-Thesis</td></tr>
<tr><td colspan="2">Kennnummer
61000</td><td>Workload
900 h</td><td>Modulart
P</td><td>Studiensemester
3</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS und SS</td></tr>
<tr><td>1</td><td colspan="2">Lehrveranstaltung(en)
Projekt Master-Thesis
Mündliche Prüfung
Kolloquium</td><td>Sprache
Deutsch (deutsches und englisches Literatur-studium erforderlich)</td><td>Kontakt-zeit
--</td><td>Selbst-studium
900 (Präsenz & Selbst-studium)</td><td>Credits (ECTS)
30</td></tr>
<tr><td>2</td><td colspan="6">Lehrform(en) / SWS:
Projekt, betreute selbständige wissenschaftliche Arbeit</td></tr>
<tr><td>3</td><td colspan="6">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Abhängig vom Thema der Masterarbeit [Wissen, 7]
Kompetenz Fertigkeiten
Mit der Master-Thesis zeigt der Student, dass er unter Anleitung selbständig umfangreiche wissenschaftliche Themen bearbeiten kann. Er wird praxisorientierte oder theoretische Themenstellungen nach wissenschaftlichen Kriterien analysieren, strukturieren und ergebnisorientiert bearbeiten. Die Master-Thesis dokumentiert seine Arbeit und erfüllt die Kriterien eines wissenschaftlichen Berichts. [Systemische Fertigkeiten, 7]
Sozialkompetenz
Abhängig vom Thema und Ort der Ausarbeitung (z.B. ein externes Unternehmen) [Team-/Führungsfähigkeit, 7]
Selbstständigkeit
Master-Thesis ist das größte Projekt im gesamten Master-Studiums, das die Studierenden nachweislich selbständig und verantwortlich ausführen. [Eigenständigkeit/Verantwortung, 7]</td></tr>
<tr><td>4</td><td colspan="6">Inhalte:
abhängig von Thema und Inhalt der Master-Thesis

Empfohlene Literaturangaben:
Abhängig vom Thema und Inhalt der Master-Thesis</td></tr>
<tr><td>5</td><td colspan="6">Teilnahmevoraussetzungen:
Ggf. formal geregelt in der Prüfungsordnung</td></tr>
<tr><td>6</td><td colspan="6">Prüfungsformen:
Master-Thesis (Ma.), benotet
Mündliche Prüfung 20 min., benotet
Referat 25 min. benotet</td></tr>
<tr><td>7</td><td colspan="6">Voraussetzungen für die Vergabe von Kreditpunkten:
Bestehen der Master-Thesis (schriftliche Ausarbeitung)
Bestehen der mündlichen Prüfung
Bestehen des Referats</td></tr>
<tr><td>8</td><td colspan="6">Verwendbarkeit des Moduls:
Business and Security Analytics, M.Sc.</td></tr>
<tr><td>9</td><td colspan="6">Modulverantwortliche(r):
Prof. Dr. German Nemirovski
Dozenten: abhängig vom Thema und Inhalt der Master-Thesis</td></tr>
<tr><td>10</td><td colspan="6">Optionale Informationen:
Studiengangsspezifische, zusätzliche Informationen zum Modul</td></tr>
<tr><td>11</td><td colspan="6">Bearbeitungsstand:
24.01.2025</td></tr>
</table>

5.4 Pflichtmodule Systems Engineering M.Eng.

5.4.1 Eingebettete Systeme

<table>
<tr><td colspan="7">Modul: Eingebettete Systeme</td></tr>
<tr><td colspan="2">51000</td><td>Workload
180 h</td><td>Modulart
P</td><td>Studiensemester
1</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS</td></tr>
<tr><td>1</td><td colspan="2">Lehrveranstaltung(en)
Eingebettete Systeme (ES)
Praktikum Eingebettete Systeme</td><td>Sprache
Deutsch</td><td>Kontakt-zeit
4 SWS / 60 h</td><td>Selbst-studium
120</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="6">Lehrform(en) / SWS:
Vorlesung (2 SWS)
Praktikum (2 SWS)</td></tr>
<tr><td>3</td><td colspan="6">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Kenntnis von Komponenten eingebetteter Systeme und Wissen über Zusammenstellung zu einem Gesamtsystem. [Wissen, 7]
Kompetenz Fertigkeiten
Erstellung eines Designs mit Auswahl von Komponenten für eingebettete Systeme. [Instrumentelle Fertigkeiten, 7]
Sozialkompetenz
Fragen während Lehrveranstaltung und Klausurvorbereitung. Präsentation der Praktikumsergebnisse vor Publikum. [Kommunikation, 7]
Selbstständigkeit
Selbständiges Erlernen der Komponenten und Designmethoden. [Lernkompetenz, 7]</td></tr>
<tr><td>4</td><td colspan="6">Inhalte:
Prozessoren:
Prozessortypen: Universalprozessoren, Mikrocontroller, Digitale Signalprozessoren, FPGSs etc.
Peripherie: Speicher, Bus, Drahtlos, Filter, Kamera
Systemanalyse, Design/Entwurf: Entkopplung, Layout, EMV, Schutzschaltung
Signalverarbeitung: Entprellung von Schalter, Drehgeber, Modellierung von Filter, Fensterfunktion, Antialiasing, Fouriertransformation, Regler, Automaten,
Neuronale Netze: Einsatz von künstlicher Intelligenz auf Embedded.
Lernprojekte im Praktikum
Eigenständige Wahl einer Aufgabe in Kombination mit dem Fach Steuerung Cyber Physical Systems. Erstellung von User Stories für die Aufgabe zur Lernkontrolle.

Empfohlene Literaturangaben:
Barr, M.: Programming Embedded Systems, Verlag O’Reiley;
Labrosse, J.: Embedded Systems Buildung Blocks, Verlag Prentice Hall;
Thaller, G.: Software Engineering für Echtzeit und Embedded Systems, Verlag bhv;
Schwebel, R.: Embedded Linux, Verlag mitp.
Bosch GmbH: Autoelektrik, Autoelektronik, Verlag Vieweg
Häuslein, A: Systemanalyse, VDE-Verlag Hruschka, P.: Agile Softwareentwicklung für Embedded Real-Time Systems mit der UML, Hanser-Verlag</td></tr>
<tr><td>5</td><td colspan="6">Teilnahmevoraussetzungen:
Kenntnisse zu technischen Systemen in Hardware und Software auf Bachelor-Niveau. Es wird empfohlen dieses Modul in Kombination zum Modul Steuerung Cyber Physical Systems zu wählen.</td></tr>
<tr><td>6</td><td colspan="6">Prüfungsformen:
Eingebettete Systeme: Klausur K90 benotet
Praktikum Eingebettete Systeme: La unbenotet
Das Praktikum beinhaltet sowohl Laborarbeit als auch Präsentation vor Publikum</td></tr>
<tr><td>7</td><td colspan="6">Voraussetzungen für die Vergabe von Kreditpunkten:
Der Studierende muss in der Lage sein, Komponenten von eingebetteten Systemen zu benennen und das Zusammenspiel erklären. Die Funktionsweise gängiger Komponenten müssen bekannt sein. Er soll aus einer Aufgabenstellung eigenständig ein Design eines eingebetteten Systems entwickeln können.
Eigenständige praktische Arbeiten müssen vor Publikum präsentiert werden können.</td></tr>
</table>

8	***Verwendbarkeit des Moduls:*** Systems Engineering M.Eng., Wahlrichtungen Advanced Computing, Security Systems, Industrie 4.0
9	***Modulverantwortliche(r):*** Prof. Dr. Derk Rembold Dozenten: Prof. Dr. Derk Rembold
10	***Optionale Informationen:*** keine
11	***Bearbeitungsstand:*** *24.01.2025*

5.4.2 Virtuelle Modellierung

Modul: Virtuelle Modellierung					
52000	**Workload** 180 h	**Modulart** P	**Studiensemester** 1	**Dauer** 1 Semester	**Häufigkeit** WS

1	**Lehrveranstaltung(en)** Vorlesung Virtuelle Modellierung Projekt Virtuelle Modellierung	**Sprache** Deutsch	**Kontakt-zeit** 4 SWS / 60 h	**Selbst-studium** 120	**Credits (ECTS)** 6

2	**Lehrform(en) / SWS:** Vorlesung (2 SWS) Projekt (2 SWS)
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Die Studierenden verfügen über Kenntnisse über Verfahren, Methoden, Algorithmen und Einsatzgebiete Virtueller Modellierung *[Wissen, 7]* *Kompetenz Fertigkeiten* Die Studierenden - beherrschen die systematische Vorgehensweise einiger spezifischer Anwendungen zur selbstständigen Erstellung Virtueller Modelle. - haben ein Verständnis für erforderliche datentechnische Einbindung von Computerwerkzeugen zur Virtuellen Modellierung und können ihre Ergebnisse unter Beachtung von Alternativen beurteilen. *[Instrumentelle Fertigkeiten, 7]* *Sozialkompetenz* Nicht relevant *Selbstständigkeit* Selbständiges Erstellen virtueller Modelle *[Reflexivität, 7]*
4	**Inhalte*:*** Virtuelle Modellierung von Produkten und Prozessen, Peripheriegeräte, Modellbildungstheorie, Systemarchitekturen, ausgewählte Algorithmen, Visibilitätsverfahren, Datenstrukturen, Informationsmodelle der virtuellen Realität, Featurebasierte Systeme, Berechnung an virtuellen Modellen, Modellbildung der objekt- und ereignisorientierten Simulation, virtuelle Erprobung, Rapid Prototyping, Virtuelle und reale Prozessketten, EDM-Systeme und Managementkonzepte für virtuelle Entwicklungs- und Produktionsstrukturen. *Empfohlene Literaturangaben:* Spur, G., Krause, F.-L.: Das virtuelle Produkt, Carl Hanser Verlag. Pahl, G.: Konstruieren mit 3D-CAD-Systemen, Springer Verlag Eigner, M., Maier, H.: Einführung und Anwendung von CAD-Systemen, Carl Hanser Verlag, München. eM-Plant, Reference Manua
5	**Teilnahmevoraussetzungen:** Für das Praktikum sind Kenntnisse der objektorientierten Modellierung, der Datenstrukturen und der Datenschnittstellen hilfreich, werden aber nicht zwingend vorausgesetzt.
6	**Prüfungsformen***:* Virtuelles Modellieren: Klausur K60 (3 ECTS) benotet Projekt Virtuelle Modellierung: Ha + R (3 ECTS) benotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Während des Semesters sind eine Hausarbeit und ein Referat zu erstellen. In den beiden Prüfungswochen ist eine 60-minütige Klausur zu schreiben.
8	***Verwendbarkeit des Moduls:*** Systems Engineering M.Eng., Wahlrichtungen Advanced Computing, Security Systems und Industrie 4.0
9	***Modulverantwortliche(r):*** Prof. Dr. Beisheim Dozenten: Prof. Dr. Beisheim
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul
11	***Bearbeitungsstand:*** *24.01.2025*

5.4.3 Steuerung von Cyber Physical Systems

<table>
<tr><td colspan="8">Modul: Steuerung von Cyber Physical Systems / Echtzeitsysteme (AC/I 4.0/Sec-SE</td></tr>
<tr><td colspan="2">52500</td><td>Workload
180h</td><td>Modulart
P</td><td colspan="2">Studiensemester
1</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS</td></tr>
<tr><td>1</td><td colspan="3">Lehrveranstaltung(en)
Steuerung von Cyber Physical Systems / Echtzeitsysteme Praktikum Steuerung von Cyber Physical Systems / Echtzeitsysteme</td><td>Sprache
Deutsch</td><td>Kontakt-zeit
4 SWS / 60 h</td><td>Selbst-studium
120</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="7">Lehrform(en) / SWS:
Vorlesung (3 SWS)
Praktikum (1 SWS)</td></tr>
<tr><td>3</td><td colspan="7">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Kenntnisse über die Algorithmen von Systemen zur Steuerung von Hardware im Rahmen von Echtzeit. [Wissen, 7]
Kompetenz Fertigkeiten
Der Studierende muss die Echtzeitfähigkeit von System über Berechnung belegen. [Instrumentelle Fertigkeiten, 7]
Sozialkompetenz
Fragen während Lehrveranstaltung und Klausurvorbereitung. Präsentation der Praktikumsergebnisse vor Publikum. [Kommunikation, 7]
Selbstständigkeit
Selbständiges Erlernen der Algorithmen zur Bestimmung der Echtzeitfähigkeit. [Lernkompetenz, 7]</td></tr>
<tr><td>4</td><td colspan="7">Inhalte:
Einführung in Steuerung von Cyber Physical/Echtzeitsysteme:
Echtzeitbetrieb, Ereignisse, Zeitanforderungen, Analyse des technischen Prozesses, Taskbegriff.
Steuerung von Cyber Physical/ Echtzeitbetriebssysteme:
Standard und Echtzeitbetriebssysteme, Unterbrechungsverwaltung, Speicherverwaltung, Nachrichtenaustausch, Zeitgeber
Echtzeitplanung: Zeitgesteuerte Verfahren, Planung nach Prioritäten, Fristen, Spielraum, Zykluszeiten – Rate Monotonic Analysis (RMA).
Kommunikation und Synchronisation:
Einseitige/mehrseitige Synchronisation, Semaphore, Prioritätsinversion.
Echtzeitnachweis: Rate Monotonic Analysis. Liu and Leyland. Schlechteste Antwortzeiten.
Zeitbedarfsanalyse, Prioritätsinversion durch Unterbrechung.
Lernprojekte im Praktikum
Eigenständiges Aussuchen einer Aufgabe in Kombination mit dem Modul Eingebettete Systeme.
Erstellung von User Stories für Aufgabe zur Lernkontrolle.</td></tr>
<tr><td></td><td colspan="7">Empfohlene Literaturangaben:
[1]Laplante, P.A.: Real-Time Systems Design and Analysis: An Engineer's Handbook; IEEE Computer Society Press 1993; ISBN 0-8186-3107-4
[2]Lauber, R.; Göhner, P.: Prozessautomatisierung I, Springer Verlag 1998, ISBN 3-540-65318-X
[3]Rembold, U.; Levi, P.:Realzeitsysteme zur Prozessautomatisierung; Carl Hanser Verlag 1994, ISBN 3-446-15713-1
[4] Klein, M.H.; Rayla, T.; Pollak, B.; Obenza, R.; Harbour, M.G.: A Practicioner’s Handbook for Real-Time Analysis: Guide to Rate Monotonic Analysis for Real-Time Systems; Kluwer Academic Publishing 1993; ISBN 0-7923-9361-9</td></tr>
<tr><td>5</td><td colspan="7">Teilnahmevoraussetzungen:
Es wird empfohlen dieses Modul in Kombination zum Modul Eingebettete System zu wählen.</td></tr>
<tr><td>6</td><td colspan="7">Prüfungsformen:
Steuerung von Cyber Physicel / Echtzeitsysteme: Klausur K90 (6 ECTS) benotet
Praktikum Steuerung von Cyber Physical / Praktikum Echtzeitsysteme: Laborarbeit und Präsentation vor Publikum unbenotet</td></tr>
</table>

7	**Voraussetzungen für die Vergabe von Kreditpunkten:** Eigenständige praktische Arbeiten müssen vor Publikum präsentiert werden können. Der Studierende muss Algorithmen zur Echtzeitsteuerung benennen können. Er soll die Echtzeitfähigkeit von Multitask-Systemen nachweisen können.
8	**Verwendbarkeit des Moduls:** Systems Engineering M.Eng., Wahlrichtungen Advanced Computing, Industrie 4.0, SE-Security Systems
9	**Modulverantwortliche(r):** Prof. Dr. Rembold Dozenten: Prof. Dr. Rembold
10	**Optionale Informationen:** Keine
11	**Bearbeitungsstand:** 24.01.2025

5.4.4 Einführung Industrie 4.0

<table>
<tr><td colspan="7">Modul: Einführung Industrie 4.0</td></tr>
<tr><td colspan="2">53500</td><td>Work-load
150 h</td><td>Modulart
P</td><td>Studiensemester
1</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS</td></tr>
<tr><td>1</td><td colspan="2">Lehrveranstaltung(en)
Vorlesung Einführung Industrie 4.0</td><td>Sprache
Deutsch</td><td>Kontakt-zeit
4 SWS / 60 h</td><td>Selbst-studium
90</td><td>Credits (ECTS)
5</td></tr>
<tr><td>2</td><td colspan="6">Lehrform(en) / SWS:
Vorlesung und Seminar (4 SWS)</td></tr>
<tr><td>3</td><td colspan="6">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Kenntnisse aus Produktion, künstlicher Intelligenz und IT Security [Wissen, 7]
Kompetenz Fertigkeiten
Berechnung von Enthropie, Bestimmung von Entscheidungsbäumen, Algorithmusherleitung, Struktur von neuronalen Netzen. Software bei IT Security Systemen [Instrumentelle Fertigkeiten, 7]
Sozialkompetenz
Vorlesung, Seminare von externen Dozenten [Kommunikation, 7]
Selbstständigkeit
Selbständige Klausurvorbereitung [Eigenständigkeit/Verantwortung, 7]</td></tr>
<tr><td>4</td><td colspan="6">Inhalte:
Vorstellung der Produktionspyramide. Präventive, Prädiktive Maintenance. IT-Security in Produktionsumgebungen. Vorstellung von Software zur Verbesserung der IT-Sicherheit. Vorstellung von künstlicher Intelligenz und Machine Learning. Anwendungen der künstlichen Intelligenz und Stand der Technik.

Empfohlene Literaturangaben:
Prof. Dr. Claudia Eckert: IT-Sicherheit: Konzepte – Verfahren – Protokolle. Oldenbourg Verlag München Wien 2014</td></tr>
<tr><td>5</td><td colspan="6">Teilnahmevoraussetzungen:
Grundlegende Kenntnisse zu IT-Sicherheit, grundlegende Kenntnisse zu künstlicher Intelligenz</td></tr>
<tr><td>6</td><td colspan="6">Prüfungsformen:
Schriftliche Klausur K90 min benotet</td></tr>
<tr><td>7</td><td colspan="6">Voraussetzungen für die Vergabe von Kreditpunkten:
Bestandene schriftliche Klausur</td></tr>
<tr><td>8</td><td colspan="6">Verwendbarkeit des Moduls:
Systems Engineering M.Eng., Wahlrichtung Industrie 4.0</td></tr>
<tr><td>9</td><td colspan="6">Modulverantwortliche(r):
Dozenten: Prof. Dr. Rembold</td></tr>
<tr><td>10</td><td colspan="6">Optionale Informationen:
Studiengangsspezifische, zusätzliche Informationen zum Modul</td></tr>
<tr><td>11</td><td colspan="6">Bearbeitungsstand:
24.01.2025</td></tr>
</table>

5.4.5 Projekt Industrie 4.0

<table>
<tr><td colspan="7">Modul: Projekt Industrie 4.0</td></tr>
<tr><td colspan="2">Kennnummer
56500</td><td>Work-load
150</td><td>Modulart
PM</td><td>Studiensemester
2.</td><td>Dauer
1</td><td>Häufigkeit
SS</td></tr>
<tr><td>1</td><td colspan="2">Lehrveranstaltung(en)
Projekt Industrie 4.0</td><td>Sprache
deutsch</td><td>Kontakt-zeit
4 SWS / 60 h</td><td>Selbst-studium
90 h</td><td>Credits (ECTS)
5</td></tr>
<tr><td>2</td><td colspan="6">Lehrform(en) / SWS:
Projekt Industrie 4.0: Project Management / 4 SWS</td></tr>
<tr><td>3</td><td colspan="6">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Aufbau von Simulationen, Kennen Projekte und Vorhaben aus der Praxis [Wissen, 7]
Kompetenz Fertigkeiten
Verfügt über spezialisierte Fachliche und konzeptionelle Fertigkeiten zur Lösung strategischer Probleme; Kann neue Ideen und Verfahren entwickeln. [Systemische Fertigkeiten, 7]
Sozialkompetenz
Teamfähig sein
Kommunikationsfähig sein; Wertschätzend agieren; Unterschiedliche Meinungen moderieren; Konflikte aushalten und beilegen; Sich angemessen durchsetzen und kooperieren;
[Team-/Führungsfähigkeit, 7
Selbstständigkeit
Für neue anwendungs- oder forschungsorientierte Aufgaben Ziele unter Reflexion der möglichen gesellschaftlichen, wirtschaftlichen und kulturellen Auswirkungen definieren, geeignete Mittel einsetzen und hierfür Wissen eigenständig erschließen. [Eigenständigkeit/Verantwortung, 7]</td></tr>
<tr><td>4</td><td colspan="6">Inhalte:
Erarbeitung der theoretischen Grundlagen für das zu bearbeitende Projektthema
• Projektplanung in Abstimmung mit beteiligtem Unternehmen
• Selbstständige Bearbeitung des Themas durch die Studierenden in Projektgruppen unter Anwendung der üblichen Projektmanagementmethoden
Es ist von allen Beteiligten eine Projektdokumentation anzufertigen, die Projektergebnisse sind zum Projektabschluss vor einem hochkarätigen Gremium zu präsentieren.</td></tr>
<tr><td></td><td colspan="6">Empfohlene Literaturangaben:
Kühn, W.: Digitale Fabrik. Fabriksimulation für Produktionsplaner. Hanser
Gorecki, P.; Pautsch, P.: Praxisbuch Lean Management. Der Weg zur operativen Excellence. Hanser
Gutenschwager, K. et al.: Simulation in Produktion und Logistik. Grundlagen und Anwendungen. Springer Berlin; Springer Vieweg
März, L. et al.: Simulation und Optimierung in Produktion und Logistik. Praxisorientierter Leitfaden mit Fallbeispielen. Springer-Verlag</td></tr>
<tr><td>5</td><td colspan="6">Teilnahmevoraussetzungen:
Wissen zur Simulation von Fertigungs-, Produktions- und Logistiksimulation</td></tr>
<tr><td>6</td><td colspan="6">Prüfungsformen:
Hausarbeit + Referat (benotet)</td></tr>
<tr><td>7</td><td colspan="6">Voraussetzungen für die Vergabe von Kreditpunkten:
Beteiligung an Projekt + Bestandene Prüfungsleistung</td></tr>
<tr><td>8</td><td colspan="6">Verwendbarkeit des Moduls:
Systems Engineering M.Eng., Wahlrichtungen Advanced Computing, Security Systems und Industrie 4.0
Pflichtmodul im Studiengang Systems Engineering M.Eng, Wahlrichtung Systems Engineering M.Eng.
Master-Studiengänge der Fakultät Engineering</td></tr>
</table>

9	***Modulverantwortliche(r):*** Prof. Dr. Bernd Stauss Dozent: Knut Kliem
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul
11	***Bearbeitungsstand:*** *24.01.2025*

5.4.6 Seminar Industrie 4.0 (1. Semester)

<table>
<tr><td colspan="7">Modul: Seminar Industrie 4.0 (1. Semester)</td></tr>
<tr><td colspan="2">Kennnummer
z.B. 15100</td><td>Work-load
60 h</td><td>Modulart
PM</td><td>Studiensemester
1</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS</td></tr>
<tr><td>1</td><td colspan="2">Lehrveranstaltung(en)
Seminar Industrie 4.0</td><td>Sprache
Deutsch und Englisch (deutsches und englisches Literaturstudium erforderlich)</td><td>Kontakt-zeit
1 SWS
15 h)</td><td>Selbst-studium
45h</td><td>Credits (ECTS)
2</td></tr>
<tr><td>2</td><td colspan="6">Lehrform(en) / SWS:
Seminar 2 SWS</td></tr>
<tr><td>3</td><td colspan="6">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Studierende kennen wissenschaftliche Herausforderungen und die fortgeschrittenen Anwendungsfälle aus dem Themengebiet Industrie 4.0 [Wissen, 7]
Kompetenz Fertigkeiten
Die Studierenden können effizient Methoden und Tools für die wissenschaftliche und akademische Recherche anwenden. [Instrumentelle Fertigkeiten, 7]
Sozialkompetenz
Die Studierenden können sehr komplexe Sachverhalte aus dem Themengebiet Industrie 4.0 vermitteln. Sie können Beispiele der angewandten Forschung aufbereiten und kompetent präsentieren. [Kommunikation, 7]
Selbstständigkeit
Die Studierenden können selbstständig Beispiele angewandter Forschung analysieren, aufbereiten und für ein kompetentes Auditorium Präsentieren.
[Eigenständigkeit/Verantwortung, 7]</td></tr>
<tr><td>4</td><td colspan="6">Inhalte:
Aktuelle Topics und Szenarien aus dem Themengebiet Industrie 4.0, darunter
IOT, Sensoren, Akteure, Protokolle, Digitale Transformation, Digitaler Zwilling, Sicherhit der IOT Systeme.

Empfohlene Literaturangaben:
Empfohlene Literaturangaben</td></tr>
<tr><td>5</td><td colspan="6">Teilnahmevoraussetzungen:
Abgeschlossene Bachelorausbildung in einem technischen Fach.</td></tr>
<tr><td>6</td><td colspan="6">Prüfungsformen:
Hausarbeit und Referat 20 Min., benotet</td></tr>
<tr><td>7</td><td colspan="6">Voraussetzungen für die Vergabe von Kreditpunkten:
Bestandene Hausarbeit und Referat</td></tr>
<tr><td>8</td><td colspan="6">Verwendbarkeit des Moduls:
Systems Engineering M. Eng., Wahlrichtung Industrie 4.0</td></tr>
<tr><td>9</td><td colspan="6">Modulverantwortliche(r):
Prof. Dr. Nemirovski</td></tr>
<tr><td>10</td><td colspan="6">Optionale Informationen:
Studiengangsspezifische, zusätzliche Informationen zum Modul</td></tr>
<tr><td>11</td><td colspan="6">Bearbeitungsstand:
24.01.2025</td></tr>
</table>

5.4.7 Seminar Industrie 4.0 (2. Semester)

<table>
<tr><td colspan="7">Modul: Seminar Industrie 4.0 (2. Semester)</td></tr>
<tr><td colspan="2">Kennnummer
z.B. 15100</td><td>Work-load
60 h</td><td>Modulart
PM</td><td>Studiensemester
2</td><td>Dauer
1 Semester</td><td>Häufigkeit
SS</td></tr>
<tr><td>1</td><td colspan="2">Lehrveranstaltung(en)
Seminar Industrie 4.0</td><td>Sprache
Deutsch und Englisch (deutsches und englisches Literaturstudium erforderlich)</td><td>Kontakt-zeit
1 SWS / 30 h)</td><td>Selbst-studium
45h</td><td>Credits (ECTS)
2</td></tr>
<tr><td>2</td><td colspan="6">Lehrform(en) / SWS:
Seminar (1 SWS)</td></tr>
<tr><td>3</td><td colspan="6">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Studierende kennen wissenschaftliche Herausforderungen und die fortgeschrittenen Anwendungsfälle aus dem Themengebiet Industrie 4.0 [Wissen, 7]
Kompetenz Fertigkeiten
Die Studierenden können effizient Methoden und Tools für die wissenschaftliche und akademische Recherche anwenden. [Instrumentelle Fertigkeiten, 7]
Sozialkompetenz
Die Studierenden können sehr komplexe Sachverhalte aus dem Themengebiet Industrie 4.0 vermitteln. Sie können Beispiele der angewandten Forschung aufbereiten und kompetent präsentieren. [Kommunikation, 7]
Selbstständigkeit
Die Studierenden können selbstständig Beispiele angewandter Forschung analysieren, aufbereiten und für ein kompetentes Auditorium Präsentieren.
[Eigenständigkeit/Verantwortung, 7]</td></tr>
<tr><td>4</td><td colspan="6">Inhalte:
Aktuelle Topics und Szenarien aus dem Themengebiet Industrie 4.0, darunter
IOT, Sensoren, Akteure, Protokolle, Digitale Transformation, Digitaler Zwilling, Sicherhit der IOT Systeme.

Empfohlene Literaturangaben:
Empfohlene Literaturangaben</td></tr>
<tr><td>5</td><td colspan="6">Teilnahmevoraussetzungen:
Abgeschlossene Bachelorausbildung in einem technischen Fach.</td></tr>
<tr><td>6</td><td colspan="6">Prüfungsformen:
Hausarbeit und Referat 20 Min., benotet</td></tr>
<tr><td>7</td><td colspan="6">Voraussetzungen für die Vergabe von Kreditpunkten:
Bestandene Hausarbeit und Referat</td></tr>
<tr><td>8</td><td colspan="6">Verwendbarkeit des Moduls:
Systems Engineering M. Eng., Wahlrichtung Industrie 4.0</td></tr>
<tr><td>9</td><td colspan="6">Modulverantwortliche(r):
Prof. Dr. Nemirovski</td></tr>
<tr><td>10</td><td colspan="6">Optionale Informationen:
Studiengangsspezifische, zusätzliche Informationen zum Modul</td></tr>
<tr><td>11</td><td colspan="6">Bearbeitungsstand:
24.01.2025</td></tr>
</table>

5.4.8 Maschinelles Lernen

<table>
<tr><td colspan="7">Modul: Maschinelles Lernen</td></tr>
<tr><td colspan="2">Kennnummer
xxxxx</td><td>Work-load
180</td><td>Modulart
PM</td><td>Studiensemester
1/2</td><td>Dauer
1 Semester</td><td>Häufigkeit
SS</td></tr>
<tr><td>1</td><td colspan="2">Lehrveranstaltung(en)
a. Vorlesung Maschinelles Lernen
b. Praktikum Maschinelles Lernen</td><td>Sprache
Deutsch</td><td>Kontakt-zeit
4SWS / 60h</td><td>Selbst-studium
120h</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="6">Lehrform(en) / SWS:
Vorlesung (2 SWS)
Praktikum (2 SWS)</td></tr>
<tr><td>3</td><td colspan="6">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Breite und tiefe Kenntnisse der Begriffe, Konzepte und Verfahren im Bereich Künstliche Intelligenz und Maschinelles Lernen [Wissen, 7]

Kompetenz Fertigkeiten
Beherrschung der Anwendung von Methoden und Verfahren der Künstlichen Intelligenz und des Maschinellen Lernens zur Implementierung intelligenter lernender Systeme [Instrumentelle Fertigkeiten, 7]

Sozialkompetenz
Fähigkeit Sachverhalte im Bereich der Künstlichen Intelligenz und des Maschinellen Lernens präzise zu kommunizieren und darüber zu argumentieren [Kommunikation, 7]

Selbstständigkeit
Fähigkeit sich selbständig neue, weiterführende bzw. noch nicht explizit behandelte Konzepte und Verfahren im Bereich der Künstlicher Intelligenz und des Maschinellen Lernens anzueignen [Lernkompetenz, 7]

Fähigkeit Sachverhalte im Bereich der Künstlicher Intelligenz und des Maschinellen Lernens mit Hilfe der beschriebenen Fertigkeiten eigenständig und eigenverantwortlich zu analysieren und zu beurteilen [Eigenständigkeit/Verantwortung, 7]</td></tr>
<tr><td>4</td><td colspan="6">Inhalte:

(1) Überblick Künstliche Intelligenz und Maschinelles Lernen: Begriff Intelligenz und Lernen, Neuronale KI, Symbolische KI, kurze Geschichte der KI
(2) Grundbegriffe und Konzepte der Künstlichen Intelligenz und des Maschinellen Lernens: Unüberwachte Lernverfahren, Überwachte Lernverfahren, Reinforcement Learning, Fehlerfunktionen und Optimierungsprinzipien, Modell-Evaluierung und -Selektion, Overfitting, Regularisierung, Hyperparameter-Optimierung und Datenaufteilung
(3) Einfache Lernmodelle: Dichteschätzung, Nearest-Neighbor-Verfahren, Entscheidungsbäume, Random Forests, Naive Bayes
(4) Maschine Learning Bibliotheken: Python/Numpy, Scikit-Learn, Tensorflow, Keras, Pytorch
(5) Lineare Modell für Regression und Klassifikation: Least Squares, Least Mean Squares, Weight Decay, Bayes'sche Lineare Regression
(6) Lernen von Funktionsgraphen, Neuronale Netze, Backpropagation Algorithmus
(7) VC-Dimension, Kernel Methoden, Suport Vektor Machine, RBF Netzwerke
(8) Deep Learning: Deep Neural Networks, Initialisierungsmethoden, Vanishing und Exploding Gradients, Weiht Sharing, Batch Normalization, Convolutional Neural Networks (CNN), DCNN-Architekturen
(9) Optimierungstechniken: Stochastischer Gradientenabstieg, Momentum, Nesterov, Adagrad, RMSprop, Adam
(10) Sequentielle Verarbeitung: Rekurrente Netzwerke, LSTM
(11) Graphische Modelle: Bayes'sche Netzwerke, Markov Netzwerke
(12) Deep-Q-Learning, Generative Adversarial Networks
(13) DNN-Architekturen für Objekt-Detektion, Semantische Segmentierung, Language
(14) Aktuelle Forschungsthemen</td></tr>
</table>

	Empfohlene Literaturangaben: Russell S., Norvig, P.: Künstliche Intelligenz, Pearson; Ertel W.: Grundkurs Künstliche Intelligenz, Springer-Vieweg; Bishop, C: Pattern recognition and machine learning, Springer; S.Raschka: Python Machine Learning. Packt Publishing; W.McKinney: Python for Data Analysis. O'Reilly. F.Chollet: Deep Learning mit Python. Knoblauch A.: Lernende Systeme. Eine fundierte Einführung in Theorie und Praxis der Künstlichen Intelligenz und des Maschinellen Lernens, Springer-Vieweg, to appear 2025 A.Knoblauch: Mathematik für Informatik und Data Science. Eine fundierte Einführung in Logik, Analysis, Lineare Algebra und Stochastik, Springer-Vieweg, 2024
5	**Teilnahmevoraussetzungen:** Grundlagen Mathematik: Analysis und Lineare Algebra, Wahrscheinlichkeitsrechnung, Mehrdimensionale Differentialrechnung (wird bei Bedarf wiederholt; bzw. Tutorial) Grundlagen Programmieren in Python/Numpy
6	**Prüfungsformen***:* Klausur, 90 min., benotet Laborarbeit, unbenotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** - Bestehen der Klausur - Bestehen des Praktikums (durch Abgabe von Praktikumsausarbeitungen)
8	***Verwendbarkeit des Moduls:*** Systems Engineering M.Eng. Wahlrichtung Advanced Computing und Industrie 4.0
9	***Modulverantwortliche(r):*** Prof. Dr. Knoblauch
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul
11	***Bearbeitungsstand:*** *25.01.2025*

5.4.9 Elektronik

<table>
<tr><td colspan="7">Modul: Elektronik</td></tr>
<tr><td colspan="2">Kennnummer
55000</td><td>Work-load
180</td><td>Modulart
P</td><td>Studiensemester
2. Semester</td><td>Dauer
1 Semester</td><td>Häufigkeit
SS</td></tr>
<tr><td>1</td><td colspan="2">Lehrveranstaltung(en)
LV 55010 Vorlesung Chipdesign
LV 55020 Vorlesung Sensoren und Aktoren</td><td>Sprache
Deutsch</td><td>Kontakt-zeit
4 SWS / 60 h</td><td>Selbst-studium
120 h</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="6">Lehrform(en) / SWS:
Vorlesung Chipdesign (2 SWS)
Vorlesung Sensoren und Aktoren (2 SWS)</td></tr>
<tr><td>3</td><td colspan="6">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Kenntnis des Entwicklungsprozesses integrierter Schaltungen. Kenntnisse von Sensoren und Aktoren technischer Systeme. [Wissen, 7]
Kompetenz Fertigkeiten
Fähigkeit zur Umsetzung einer gegebenen Problemstellung in eine Implementierung als integrierte Schaltung unter Anwendung der dafür relevanten Entwurfsmethoden und Entwurfswerkzeuge.
Designvorschläge und Angaben von Sensoren und Aktoren bei Entwicklungsarbeiten. [Instrumentelle Fertigkeiten, 7]
Sozialkompetenz
Erarbeiten der Funktionsweisen ausgesuchter Themen im Team (z.B. GPS). [Kommunikation, 7]
Selbstständigkeit
Transfer der Vorlesungsinhalte in die praktische Anwendung im Rahmen der Übungen.
Selbständiges Erlernen der Vorlesungsinhalte für die Klausuren. [Lernkompetenz, 7]</td></tr>
<tr><td>4</td><td colspan="6">Inhalte:

Chipdesign:
- Einführung in den Entwurf integrierter Schaltungen
- Die Hardwarebeschreibungssprache VHDL
- Übung: Modellierung einer Schaltungen mit VHDL, Simulation des VHDL-Modells
- Fertigungstechnologien
- Übung: Synthese des VHDL-Modells auf eine FPGA-Plattform
- Fertigungsprozess – der Schritt zum Silizium

Sensoren und Aktoren:
Sensortechnik
- Akustische Sensoren
- Chemische Sensoren
- Optische Sensoren
- Thermische Sensoren
- Analoge und digitale Messsignalverarbeitung
- Sensor/Aktor-Bussysteme
- Mechanische Sensoren
- Magnetische Sensoren
- Piezo
Aktortechnik
- Hydraulik
- Gleichstromantrieb
- Schrittmotor
- Asynchronantriebe
- Chemische Aktoren
- Piezo</td></tr>
<tr><td></td><td colspan="6">Empfohlene Literaturangaben:
- Ashenden, P.J.: The Designer’s Guide to VHDL. Morgan Kaufmann Publishers.
- Kesel, F., Bartholomä, R.: Entwurf von digitalen Schaltungen mit HDLs und FPGAs. Oldenbourg Verlag.
- Ashenden, P.J.: VHDL Cookbook.</td></tr>
</table>

	https://www.ics.uci.edu/~alexv/154/VHDL-Cookbook.pdf - Mäder, A.: VHDL-Kompakt. https://tams.informatik.uni-hamburg.de/vhdl/doc/ajmMaterial/vhdl.pdf - Hering E., Steinhart H.: Taschenbuch der Mechatronik. - Niebuhr J., Lindner G.: Physikalische Messtechnik mit Sensoren.
5	**Teilnahmevoraussetzungen:** Chipdesign: Grundlagen der digitalen Schaltungstechnik und des Entwurfs digitaler Systeme Sensoren und Aktoren: Physik, Elektrotechnik
6	**Prüfungsformen***:* Chipdesign: Klausur 60 Minuten, benotet Sensoren und Aktoren: Klausur 60 Minuten, benotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Chipdesign: Bestandene Klausur (2,5 ECTS) Sensoren und Aktoren: Bestandene Klausur (2,5 ECTS)
8	***Verwendbarkeit des Moduls:*** Systems Engineering M.Eng., Wahlrichtung Advanced Computing, Security Systems, Industrie 4.0
9	***Modulverantwortliche(r):*** Prof. Dr. Joachim Gerlach, Prof. Dr. Derk Rembold Dozenten: Prof. Dr. Joachim Gerlach, Prof. Dr. Derk Rembold
10	***Optionale Informationen:***
11	***Bearbeitungsstand:*** *24.01.2025*

5.4.10 Security Hardware Design

<table>
<tr><td colspan="7">Modul: Security Hardware Design</td></tr>
<tr><td>Kennnummer
100110</td><td>Workload
180</td><td>Modulart
P</td><td colspan="2">Studiensemester
2. Semester</td><td>Dauer
1 Semester</td><td>Häufigkeit
SS</td></tr>
<tr><td>1</td><td colspan="2">Lehrveranstaltung(en)
Vorlesung Security Hardware Design
Projekt Security Hardware Design</td><td>Sprache
Deutsch oder Englisch</td><td>Kontakt-zeit
Vorlesung
2 SWS / 30h
Projekt
2 SWS / 30h</td><td>Selbst-studium
120</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="6">Lehrform(en) / SWS:
Vorlesung Security Hardware Design (2 SWS)
Projekt Security Hardware Design (2 SWS)</td></tr>
<tr><td>3</td><td colspan="6">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Die Studierenden verstehen verschiedene Implementierungs-Strategien von sicherheitsrelevanten Algorithmen in Hardware. [Wissen, 7]
Kompetenz Fertigkeiten
Die Studierenden können sicherheitsrelevante Algorithmen effizient in Hardware umsetzen und auf bestimmte Zielvorgaben hin optimieren. [Instrumentelle Fertigkeiten, 7]

Die Studierenden können die Auswirkungen von Optimierungen auf Systeme bzgl. unterschiedlichen Kriterien, wie z.B. Gesamtsystemperformance, Kosten, oder Angriffs-Anfälligkeit beurteilen und geeignete Maßnahmen herleiten und umsetzen. [Beurteilungsfähigkeit, 7]
Sozialkompetenz
Die Studierenden können komplexe Themenfelder der Hardware-Sicherheit mit anderen Experten diskutieren und im Team weiterentwickeln. [Team-/Führungsfähigkeit, 7]
Selbstständigkeit
Die Studierenden können selbstständig und anwendungsorientiert Entscheidungen zur Optimierung komplexer Sachverhalte treffen. [Eigenständigkeit/Verantwortung, 7]</td></tr>
<tr><td>4</td><td colspan="6">Inhalte:
Vorlesung
- Einführung in die RTL-Programmierung mit VHDL
- Grundlagen zur Programmierung von FPGAs und ASICs
- Optimierungsstrategien für hochperformante, ressourcensparende, oder energiesparende Implementierungen
- Optimierungs-Strategien mit Software/Hardware Co-Design
- Anwendung der Optimierungsstrategien für unterschiedliche kryptografische Algorithmen
- Effiziente Algorithmen für Public Key Kryptografie
- Sichere Prozessorarchitekturen

Projektarbeit
- Einführung in die FPGA-Programmierung mit VHDL
- Implementierung und Optimierung eines Algorithmus auf einem FPGA
- Erprobung unterschiedlicher Optimierungsstrategien

Empfohlene Literaturangaben:
Koç, C. K. - Cryptographic Engineering, Springer-Verlag, 2010

Ashenden, J. P. - The Designer's Guide to VHDL, Morgan Kaufmann, 2010</td></tr>
<tr><td>5</td><td colspan="6">Teilnahmevoraussetzungen:
Grundlagen der Kryptologie, Programmierkenntnisse (C, optional ARM Assembly oder VHDL)</td></tr>
<tr><td>6</td><td colspan="6">Prüfungsformen:
Referat 20 min. inkl. Wissenschaftlicher Ausarbeitung zum Projekt, Diskussion benotet</td></tr>
</table>

7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Ausreichend bewertete Ausarbeitung Ausreichend bewertetes Referat
8	***Verwendbarkeit des Moduls:*** Advanced IT Security M.Sc. Systems Engineering M.Eng., Wahlrichtung Security Systems
9	***Modulverantwortliche(r):*** Prof. Dr. Bernhard Jungk
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul
11	***Bearbeitungsstand:*** *24.01.2025*

5.4.11 Security und Internet der Dinge

<table>
<tr><td colspan="7">Modul: Security und Internet der Dinge</td></tr>
<tr><td colspan="2">Kennnummer
55000</td><td>Workload
180 h</td><td>Modulart
P</td><td colspan="2">Studiensemester
2</td><td>Häufigkeit
SS</td></tr>
<tr><td>1</td><td colspan="3">Lehrveranstaltung(en)
Vorlesung Security und Internet der Dinge
Projekt Security und Internet der Dinge</td><td>Sprache
Deutsch</td><td>Kontakt-zeit
4 SWS / 60 h</td><td>Selbst-studium
120</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="7">Lehrform(en) / SWS:
Vorlesung: 2 SWS
Praktikum: 2 SWS</td></tr>
<tr><td>3</td><td colspan="7">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Die Studierenden
- kennen Systeme und Techniken vom Systemmonitoring bis zu Auswertesystemen - - - kennen Technologien zur Sicherung dieser Systeme [Wissen, 7]
Kompetenz Fertigkeiten
Die Studierenden
- sind in der Lage die Problem- und Aufgabenstellungen mit Bezug auf das Themengebiet zu erkennen, diese, basierend auf eigenem Wissen und durch die gezielte Recherche zu beschreiben, Lösungsansätze zu entwickeln und diese allein oder im Team umzusetzen.
- sind in der Lage wissenschaftliche Beiträge im Themenbereich eigenständig zu lesen und qualitative Vergleiche der gelesenen Beiträge systematisch zu präsentieren. [Instrumentelle Fertigkeiten, 7]
Sozialkompetenz
Die Studierenden können im Rahmen einer eigenständigen Arbeit neue Ansätze für einen IoT Prozess mit konkreter Aufgabenstellung entwickeln [Team-/Führungsfähigkeit, 7]
Selbstständigkeit
Die Studierenden sind in der Lage komplexe Aufgaben verantwortungsvoll zu erfüllen, realistische Ziele zu definieren und diese konsequent zu verfolgen.
[Eigenständigkeit/Verantwortung, 7]</td></tr>
<tr><td>4</td><td colspan="7">Inhalte:
IoT-Systembeschreibungen
- Monitoringtechnologien
- Monitoringprotokolle (MQTT, Kafka)
- WebServices
- Zeitreihenanalyseverfahren, Principal Component Analysis,

Projekt:
- Monitoring mit MQTT, Kafka
- Zeitreihenanalyseverfahren mit R z.B.: ARMA, Holt-Winters
- IoT-Systeme in der IBM Cloud und Azure
Empfohlene Literaturangaben:

-</td></tr>
<tr><td>5</td><td colspan="7">Teilnahmevoraussetzungen:
Kenntnisse von relationalen Datenbanken</td></tr>
<tr><td>6</td><td colspan="7">Prüfungsformen:
Vorlesung: Klausur K 60 (3 ECTS)
Projekt: Ha+R (3 ECTS)</td></tr>
<tr><td>7</td><td colspan="7">Voraussetzungen für die Vergabe von Kreditpunkten:
Am Ende des Semesters ist eine 60-minütige schriftliche Prüfung zu schreiben. Während des Semesters ist ein Projekt zu einem selbstgewählten Thema aus dem Bereits IoT zu bearbeiten und eine Präsentation zu halten.</td></tr>
</table>

8	***Verwendbarkeit des Moduls:*** Systems Engineering M.Eng., Wahlrichtungen Advanced Computing, Security Systems, Industrie 4.0
9	***Modulverantwortliche(r):*** Prof. Dr. Eppler Dozenten: Prof. Dr. Eppler
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul
11	***Bearbeitungsstand:*** *24.01.2025*

5.4.12 Master-Thesis

<table>
<tr><td colspan="7">Modul: Master-Thesis</td></tr>
<tr><td colspan="2">Kennnummer
61000</td><td>Workload
900 h</td><td>Modulart
PM</td><td>Studiensemester
3</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS und SS</td></tr>
<tr><td>1</td><td colspan="2">Lehrveranstaltung(en)
Projekt Master-Thesis
Mündliche Prüfung
Kolloquium</td><td>Sprache
Deutsch (deutsches und englisches Literatur-studium erforderlich)</td><td>Kontakt-zeit</td><td>Selbst-studium
900 (Präsenz & Selbst-studium)</td><td>Credits (ECTS)
30</td></tr>
<tr><td>2</td><td colspan="6">Lehrform(en) / SWS:
Projekt, betreute selbständige wissenschaftliche Arbeit</td></tr>
<tr><td>3</td><td colspan="6">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Abhängig vom Thema der Masterarbeit [Wissen, 7]
Kompetenz Fertigkeiten
Mit der Master-Thesis zeigt der Student, dass er unter Anleitung selbständig umfangreiche wissenschaftliche Themen bearbeiten kann. Er wird praxisorientierte oder theoretische Themenstellungen nach wissenschaftlichen Kriterien analysieren, strukturieren und ergebnisorientiert bearbeiten. Die Master – Thesis dokumentiert seine Arbeit und erfüllt die Kriterien eines wissenschaftlichen Berichts. [Systemische Fertigkeiten, 7]
Sozialkompetenz
Abhängig vom Thema und Ort der Ausarbeitung (z.B. ein externes Unternehmen).
[Team-/Führungsfähigkeit, 7]
Selbstständigkeit
Master-Thesis ist das größte Projekt im gesamten Master-Studium, das die Studierenden nachweislich selbständig und verantwortlich ausführen. [Eigenständigkeit/Verantwortung, 7]</td></tr>
<tr><td>4</td><td colspan="6">Inhalte:
Abhängig von Thema und Inhalt der Master-Thesis

Empfohlene Literaturangaben:
Abhängig vom Thema und Inhalt der Master-Thesis</td></tr>
<tr><td>5</td><td colspan="6">Teilnahmevoraussetzungen:
Ggf. formal geregelt in der Prüfungsordnung</td></tr>
<tr><td>6</td><td colspan="6">Prüfungsformen:
Master-Thesis (Ma.), benotet.
Mündliche Prüfung 20 min., benotet
Referat 25 Min, benotet</td></tr>
<tr><td>7</td><td colspan="6">Voraussetzungen für die Vergabe von Kreditpunkten:
Bestehen der Master-Thesis (schriftliche Ausarbeitung).
Bestehen der mündlichen Prüfung, Bestehen des Referats</td></tr>
<tr><td>8</td><td colspan="6">Verwendbarkeit des Moduls:
Systems Engineering M.Eng., Wahlrichtungen Advanced Computing, Security Systems und Industrie 4,0</td></tr>
<tr><td>9</td><td colspan="6">Modulverantwortliche(r):
Prof. Dr. German Nemirovski
Dozenten: abhängig vom Thema und Inhalt der Master-Thesis</td></tr>
<tr><td>10</td><td colspan="6">Optionale Informationen:
Studiengangsspezifische, zusätzliche Informationen zum Modul</td></tr>
<tr><td>11</td><td colspan="6">Bearbeitungsstand:
24.01.2025</td></tr>
</table>

5.5 Wahlpflichtmodule

Für die Übersicht der angebotenen Wahlpflichtmodule wird an dieser Stelle auf den jeweils gültigen Wahlpflichtmodulkatalog verwiesen.

5.5.5 Wahlpflichtmodul 1a / Wahlpflichtmodul 1b

<table>
<tr><td colspan="7">Modul: Wahlpflichtmodule 1a / 1b</td></tr>
<tr><td colspan="2">Kennummer
52500 / 53000</td><td>Workload
180 h</td><td>Modulart
WPM</td><td colspan="2">Studiensemester
1</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS</td></tr>
<tr><td>1</td><td colspan="3">Lehrveranstaltung(en)
Module aus WPM-Katalog (extra Liste)</td><td>Sprache
Deutsch</td><td>Kontakt-zeit
4 SWS / 60 h</td><td>Selbst-studium
120 h</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="7">Lehrform(en) / SWS:
Wird definiert durch jeweiligen Modulverantwortlichen (4 SWS)</td></tr>
<tr><td>3</td><td colspan="7">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Studierenden wenden ihr im Studium erlangtes Wissen auf den jeweiligen Bereich an. Die Studierenden können sich darüber hinaus in angemessener Zeit neue Inhalte aneignen und diese geeignet strukturieren und didaktisch aufbereiten. [Wissen, 7]
Kompetenz Fertigkeiten
Die Studierenden sind in Lage Konzepte und Methoden zu abstrahieren und auf neue Anwendungsfelder zu übertragen. [Systemische Fertigkeiten, 7]
Sozialkompetenz
Projekte organisieren, umsetzen, steuern und die Einhaltung nach Gesichtspunkten des Qualitätsmanagements kontrollieren und überwachen. [Team-/Führungsfähigkeit, 7]
Selbstständigkeit
Studierende können die Lehrinhalte selbständig aufarbeiten und strukturiert wiedergeben. Sie sind in der Lage Aufgaben im vorgegeben Zeitrahmen zu bearbeiten.
[Eigenständigkeit/Verantwortung, 7]</td></tr>
<tr><td>4</td><td colspan="7">Inhalte:
Für die hier Wahlpflichtmodulteile existieren jeweils gesonderte Modulteilbeschreibungen in diesem Modulhandbuch. Wenn Modulteile aus anderen Masterstudiengängen gewählt werden gelten die Inhaltsangaben der dort definierten Modulteilbeschreibungen. Sofern in diesen Fällen grundlegende Vorkenntnisse erforderlich sind die im bisherigen Studienverlauf der Studierenden nicht zwangsläufig erworben wurden, obliegt es dem Kandidaten diese Vorkenntnisse gesondert zu erwerben

Empfohlene Literaturangaben:
Siehe jeweilige Modulteilbeschreibungen</td></tr>
<tr><td>5</td><td colspan="7">Teilnahmevoraussetzungen:
Die geforderten Voraussetzungen sind abhängig von den gewählten Modulteilen und deren Inhalten (s.o.)</td></tr>
<tr><td>6</td><td colspan="7">Prüfungsformen:
Siehe jeweilige Modulteilbeschreibungen</td></tr>
<tr><td>7</td><td colspan="7">Voraussetzungen für die Vergabe von Kreditpunkten:
Es gelten die Ausführungen in den Beschreibungen des WPM</td></tr>
<tr><td>8</td><td colspan="7">Verwendbarkeit des Moduls:
Advanced IT Security M.Sc., Business and Security Analytics M.Sc., Systems Engineering M.Eng., Wahlrichtungen Advanced Computing und Security Systems</td></tr>
<tr><td>9</td><td colspan="7">Modulverantwortliche(r):
Prof. Dr. Nemirovski
Dozenten: s. Modulbeschreibungen der jeweiligen WPM</td></tr>
<tr><td>10</td><td colspan="7">Optionale Informationen:
Studiengangsspezifische, zusätzliche Informationen zum Modul</td></tr>
<tr><td>11</td><td colspan="7">Bearbeitungsstand:
24.01.2025</td></tr>
</table>

5.5.6 Wahlpflichtmodul 2a / Wahlpflichtmodul 2b

<table>
<tr><td colspan="7">Modul: Wahlpflichtmodule 2a / 2b</td></tr>
<tr><td colspan="2">Kennnummer
55500 / 56000</td><td>Workload
180 h</td><td>Modulart
WPM</td><td colspan="2">Studiensemester
2</td><td>Dauer
1 Semester</td><td>Häufigkeit
SS</td></tr>
<tr><td>1</td><td colspan="3">Lehrveranstaltung(en)
Module aus WPM-Katalog (extra Liste)</td><td>Sprache
Deutsch</td><td>Kontakt-zeit
4 SWS / 60 h</td><td>Selbst-studium
120</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="7">Lehrform(en) / SWS:
Wird definiert durch den jeweiligen Modulverantwortlichen (4 SWS)</td></tr>
<tr><td>3</td><td colspan="7">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Studierenden wenden ihr im Studium erlangtes Wissen auf den jeweiligen Bereich an. Die Studierenden können sich darüber hinaus in angemessener Zeit neue Inhalte aneignen und diese geeignet strukturieren und didaktisch aufbereiten. [Wissen, 7]
Kompetenz Fertigkeiten
Die Studierenden sind in Lage Konzepte und Methoden zu abstrahieren und auf neue Anwendungsfelder zu übertragen. [Systemische Fertigkeiten, 7]
Sozialkompetenz
Projekte organisieren, umsetzen, steuern und die Einhaltung nach Gesichtspunkten des Qualitätsmanagements kontrollieren und überwachen. [Team-/Führungsfähigkeit, 7]
Selbstständigkeit
Studierende können die Lehrinhalte selbständig aufarbeiten und strukturiert wiedergeben. Sie sind in der Lage Aufgaben im vorgegeben Zeitrahmen zu bearbeiten.
[Eigenständigkeit/Verantwortung, 7]</td></tr>
<tr><td>4</td><td colspan="7">Inhalte:
Für die hier Wahlpflichtmodulteile existieren jeweils gesonderte Modulteilbeschreibungen in diesem Modulhandbuch. Wenn Modulteile aus anderen Masterstudiengängen gewählt werden gelten die Inhaltsangaben der dort definierten Modulteilbeschreibungen. Sofern in diesen Fällen grundlegende Vorkenntnisse erforderlich sind die im bisherigen Studienverlauf der Studierenden nicht zwangsläufig erworben wurden, obliegt es dem Kandidaten diese Vorkenntnisse gesondert zu erwerben

Empfohlene Literaturangaben:
Siehe jeweilige Modulteilbeschreibungen</td></tr>
<tr><td>5</td><td colspan="7">Teilnahmevoraussetzungen:
Die geforderten Voraussetzungen sind abhängig von den gewählten Modulteilen und deren Inhalten (s.o.)</td></tr>
<tr><td>6</td><td colspan="7">Prüfungsformen:
Siehe jeweilige Modulteilbeschreibungen</td></tr>
<tr><td>7</td><td colspan="7">Voraussetzungen für die Vergabe von Kreditpunkten:
Es gelten die Ausführungen in den Beschreibungen des WPM</td></tr>
<tr><td>8</td><td colspan="7">Verwendbarkeit des Moduls:
Systems Engineering M.Eng., Wahlrichtung Advanced Computing, Security Systems</td></tr>
<tr><td>9</td><td colspan="7">Modulverantwortliche(r):
Prof. Dr. Nemirovski
Dozenten: s. Modulbeschreibungen der jeweiligen WPM</td></tr>
<tr><td>10</td><td colspan="7">Optionale Informationen:
Studiengangsspezifische, zusätzliche Informationen zum Modul</td></tr>
<tr><td>11</td><td colspan="7">Bearbeitungsstand:
24.01.2025</td></tr>
</table>

5.5.7 Wahlpflichtmodul 1a / Wahlpflichtmodul 1b

<table>
<tr><td colspan="7">Modul: Wahlpflichtmodule 1a / 1b - Industrie 4.0</td></tr>
<tr><td colspan="2">Kennummer
52500 / 53000</td><td>Workload
75 h</td><td>Modulart
WPM</td><td colspan="2">Studiensemester
1</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS</td></tr>
<tr><td>1</td><td colspan="3">Lehrveranstaltung(en)
Module aus WPM-Katalog (extra Liste)</td><td>Sprache
Deutsch</td><td>Kontakt-zeit
2 SWS / 30 h</td><td>Selbst-studium
45 h</td><td>Credits (ECTS)
2,5</td></tr>
<tr><td>2</td><td colspan="7">Lehrform(en) / SWS:
Wird definiert durch jeweiligen Modulverantwortlichen (2 SWS)</td></tr>
<tr><td>3</td><td colspan="7">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Studierenden wenden ihr im Studium erlangtes Wissen auf den jeweiligen Bereich an. Die Studierenden können sich darüber hinaus in angemessener Zeit neue Inhalte aneignen und diese geeignet strukturieren und didaktisch aufbereiten. [Wissen, 7]
Kompetenz Fertigkeiten
Die Studierenden sind in Lage Konzepte und Methoden zu abstrahieren und auf neue Anwendungsfelder zu übertragen. [Systemische Fertigkeiten, 7]
Sozialkompetenz
Projekte organisieren, umsetzen, steuern und die Einhaltung nach Gesichtspunkten des Qualitätsmanagements kontrollieren und überwachen. [Team-/Führungsfähigkeit, 7]
Selbstständigkeit
Studierende können die Lehrinhalte selbständig aufarbeiten und strukturiert wiedergeben. Sie sind in der Lage Aufgaben im vorgegeben Zeitrahmen zu bearbeiten.
[Eigenständigkeit/Verantwortung, 7]</td></tr>
<tr><td>4</td><td colspan="7">Inhalte:
Für die hier Wahlpflichtmodulteile existieren jeweils gesonderte Modulteilbeschreibungen in diesem Modulhandbuch. Wenn Modulteile aus anderen Masterstudiengängen gewählt werden gelten die Inhaltsangaben der dort definierten Modulteilbeschreibungen. Sofern in diesen Fällen grundlegende Vorkenntnisse erforderlich sind die im bisherigen Studienverlauf der Studierenden nicht zwangsläufig erworben wurden, obliegt es dem Kandidaten diese Vorkenntnisse gesondert zu erwerben

Empfohlene Literaturangaben:
Siehe jeweilige Modulteilbeschreibungen</td></tr>
<tr><td>5</td><td colspan="7">Teilnahmevoraussetzungen:
Die geforderten Voraussetzungen sind abhängig von den gewählten Modulteilen und deren Inhalten (s.o.)</td></tr>
<tr><td>6</td><td colspan="7">Prüfungsformen:
Siehe jeweilige Modulteilbeschreibungen</td></tr>
<tr><td>7</td><td colspan="7">Voraussetzungen für die Vergabe von Kreditpunkten:
Es gelten die Ausführungen in den Beschreibungen des WPM</td></tr>
<tr><td>8</td><td colspan="7">Verwendbarkeit des Moduls:
Systems Engineering M.Eng., Wahlrichtungen Industrie 4.0</td></tr>
<tr><td>9</td><td colspan="7">Modulverantwortliche(r):
Prof. Dr. Nemirovski
Dozenten: s. Modulbeschreibungen der jeweiligen WPM</td></tr>
<tr><td>10</td><td colspan="7">Optionale Informationen:
Studiengangsspezifische, zusätzliche Informationen zum Modul</td></tr>
<tr><td>11</td><td colspan="7">Bearbeitungsstand:
24.01.2025</td></tr>
</table>

5.5.8 Wahlpflichtmodul 2a / Wahlpflichtmodul 2b

<table>
<tr><td colspan="7">Modul: Wahlpflichtmodule 2a / 2b – Industrie 4.0</td></tr>
<tr><td colspan="2">Kennnummer
55500 / 56000</td><td>Workload
75 h</td><td>Modulart
WPM</td><td colspan="2">Studiensemester
2</td><td>Dauer
1 Semester</td><td>Häufigkeit
SS</td></tr>
<tr><td>1</td><td colspan="3">Lehrveranstaltung(en)
Module aus WPM-Katalog (extra Liste)</td><td>Sprache
Deutsch</td><td>Kontakt-zeit
2 SWS / 30 h</td><td>Selbst-studium
75</td><td>Credits (ECTS)
2,5</td></tr>
<tr><td>2</td><td colspan="7">Lehrform(en) / SWS:
Wird definiert durch den jeweiligen Modulverantwortlichen (2 SWS)</td></tr>
<tr><td>3</td><td colspan="7">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Studierenden wenden ihr im Studium erlangtes Wissen auf den jeweiligen Bereich an. Die Studierenden können sich darüber hinaus in angemessener Zeit neue Inhalte aneignen und diese geeignet strukturieren und didaktisch aufbereiten. [Wissen, 7]
Kompetenz Fertigkeiten
Die Studierenden sind in Lage Konzepte und Methoden zu abstrahieren und auf neue Anwendungsfelder zu übertragen. [Systemische Fertigkeiten, 7]
Sozialkompetenz
Projekte organisieren, umsetzen, steuern und die Einhaltung nach Gesichtspunkten des Qualitätsmanagements kontrollieren und überwachen. [Team-/Führungsfähigkeit, 7]
Selbstständigkeit
Studierende können die Lehrinhalte selbständig aufarbeiten und strukturiert wiedergeben. Sie sind in der Lage Aufgaben im vorgegeben Zeitrahmen zu bearbeiten.
[Eigenständigkeit/Verantwortung, 7]</td></tr>
<tr><td>4</td><td colspan="7">Inhalte:
Für die hier Wahlpflichtmodulteile existieren jeweils gesonderte Modulteilbeschreibungen in diesem Modulhandbuch. Wenn Modulteile aus anderen Masterstudiengängen gewählt werden gelten die Inhaltsangaben der dort definierten Modulteilbeschreibungen. Sofern in diesen Fällen grundlegende Vorkenntnisse erforderlich sind die im bisherigen Studienverlauf der Studierenden nicht zwangsläufig erworben wurden, obliegt es dem Kandidaten diese Vorkenntnisse gesondert zu erwerben

Empfohlene Literaturangaben:
Siehe jeweilige Modulteilbeschreibungen</td></tr>
<tr><td>5</td><td colspan="7">Teilnahmevoraussetzungen:
Die geforderten Voraussetzungen sind abhängig von den gewählten Modulteilen und deren Inhalten (s.o.)</td></tr>
<tr><td>6</td><td colspan="7">Prüfungsformen:
Siehe jeweilige Modulteilbeschreibungen</td></tr>
<tr><td>7</td><td colspan="7">Voraussetzungen für die Vergabe von Kreditpunkten:
Es gelten die Ausführungen in den Beschreibungen des WPM</td></tr>
<tr><td>8</td><td colspan="7">Verwendbarkeit des Moduls:
Systems Engineering M.Eng., Wahlrichtung Industrie 4.0</td></tr>
<tr><td>9</td><td colspan="7">Modulverantwortliche(r):
Prof. Dr. Nemirovski
Dozenten: s. Modulbeschreibungen der jeweiligen WPM</td></tr>
<tr><td>10</td><td colspan="7">Optionale Informationen:
Studiengangsspezifische, zusätzliche Informationen zum Modul</td></tr>
<tr><td>11</td><td colspan="7">Bearbeitungsstand:
24.01.2025</td></tr>
</table>