Hochschule
Albstadt-Sigmaringen
Albstadt-Sigmaringen University

Modulhandbuch

Fakultät Informatik
Studiengang Systems Engineering

StuPO 18.1
ab Wintersemester 2021/22
Ersteller: Prof. Dr.German Nemirovski, Studiendekan
Verantwortlich: Prof. Dr. German Nemirovski, Studiendekan

Inhaltsverzeichnis

1 Vorwort

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:
- 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, Qualitätsmanagement, 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 Investitionsgüterindustrie, 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.

2 Qualifikationsziel-Modul-Matrix

Modul-Nr.	Modulbezeichnung	Summe der Unterstützungspunkte	Praxisnahes und Fachübergreifendes Wissen	Methoden und Werkzeuge	Breites Wissen	Sicherheitskompetenz	Wissenschaftliches Niveau und ausgeprägte Anwendungsorientierung
	Qualifikationsziel (QuZ)						
51000	Eingebettete Systeme	5	1	2	1		1
52000	Virtuelle Modellierung	5		2	1		2
52500	Steuerung von Cyber Physical Systems	6		2	2		2
51500	Big Data	7	2	2	2		1
53500	Einführung Industrie 4.0	5	1	1	1	1	1
52600	Open Source Intelligenc	7	1	1	1	2	2
52700	Incident Response und MalwareDefense	5	1	2		2	
53000	WPM 1a / 1b	5	1	1	1	1	1
54000	Theoret. Informatik u. Künstl.Intelligenz	15	1	2			2
55000	Elektronik	5	2	1	1		1
55500	Security und Internet der Dinge	9	2	2	1	2	2
54500	IT-Sicherheit	6	1	1	2	2	
56500	Projekt Industrie 4.0	5	1	1	1	1	1
56000	Advanced Network and Internenet Security	7	2	2		2	1
55700	Security Analytics	6		2		2	2
56000	WPM 2a / 2b	5	1	1	1	1	1
60100	Master Theis	10	2	2	2	2	2

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

3 Studiengangs-Kompetenzmatrix

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
52000	Virtuelle Modellierung	7	7	7								
52500	Steuerung von Cyber Physical Systems	7	6	6					7			7
51500	Big Data	7	7	7						7		
53500	Einführung Industrie 4.0		7		7							
52600	Open Source Intelligenc	6	7	7	7	7			7	7		7
52700	Incident Response und MalwareDefense	7			7				7	7		
53000	WPM 1a / 1b	7	7		7		7			7		
54000	Theoret. Informatik u. Künstl.Intelligenz	7	6	7	7					6		
55000	Elektronik	7	6	7					6			6
55500	Security und Internet der Dinge	7		7			7			7		
54500	IT-Sicherheit	6	7	7						7		
56500	Projekt Industrie 4.0				7					7		7
56000	Advanced Network and Internenet Security	7	7	7	7					7		
55700	Security Analytics											
56000	WPM 2a / 2b	7	7		7		7			7		
60100	Master Theis				7					7		

4 Modulbeschreibungen

4.1 1. Semester

4.1.1 51000 –Eingebettete Systeme

Studiengang: Systems Engineering
StuPO-Version: 18.1

Semester: WS 2021/22
Letzte Bearbeitung: 20.09.21

Modul: Eingebettete Systeme						
51000	**Workload** 150 h	**Modulart** P	**Studiensemester** 1	**Dauer** 1 Semester	**Häufigkeit** WS und SS	
1	**Lehrveranstaltung(en)** Eingebettete Systeme (ES) Praktikum Eingebettete Systeme	**Sprache** Deutsch	**Kontakt-zeit** 4 SWS / 60 h	**Selbst-studium** 90	**Credits (ECTS)** 5	
2	**Lehrform(en) / SWS:** Vorlesung (2 SWS) Praktikum (2 SWS)					
3	**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, 6]* *Sozialkompetenz* Fragen während Lehrveranstaltung und Klausurvorbereitung. Präsentation der Praktikumsergebnisse vor Publikum. *[Kommunikation, 7]* *Selbstständigkeit* Selbständiges Erlernen der Komponenten und Designmethoden. *[Lernkompetenz, 7]*						
4	**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
5	**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.
6	**Prüfungsformen***:* Eingebettete Systeme: Klausur K90 (2,5 ECTS) Praktikum Eingebettete Systeme: La (2,5 ECTS) Das Praktikum beinhaltet sowohl Laborarbeit als auch Präsentation vor Publikum
7	***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.
8	***Verwendbarkeit des Moduls:*** SE-AC/SE-Industrie 4.0/Security SE
9	***Modulverantwortliche(r):*** Prof. Dr. Derk Rembold Dozenten: Prof. Dr. Derk Rembold
10	***Optionale Informationen:*** keine

4.1.2 52000 - Virtuelle Modellierung

Studiengang: Systems Engineering
StuPO-Version: 18.1

Semester: WS 2021/22
Letzte Bearbeitung: 20.09.21

Modul: Virtuelle Modellierung						
52000	**Workload** 150 h	**Modulart** P	**Studiensemester** 1	**Dauer** 1 Semester	**Häufigkeit** WS und SS	
1	**Lehrveranstaltung(en)** Vorlesung Virtuelle Modellierung Projekt Virtuelle Modellierung	**Sprache** Deutsch	**Kontakt-zeit** 4 SWS / 60 h	**Selbst-studium** 90	**Credits (ECTS)** 5	
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 /Kompetenzausprägung wählen /Niveaustufe wählen *Selbstständigkeit* Selbständiges Erstellen virtueller Modelle *Reflexivität*/Kompetenzausprägung wählen *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 (2,5 ECTS) Projekt Virtuelle Modellierung: Ha + R (2,5 ECTS)
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:*** SE-AC/SE-Industrie 4.0/Security SE
9	***Modulverantwortliche(r):*** Prof. Dr. Beisheim Dozenten: Prof. Dr. Beisheim
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

4.1.3 52500 – Steuerung von Cyber Physical Systems

Studiengang: Systems Engineering
StuPO-Version: 18.1

Semester: WS 2021/22
Letzte Bearbeitung: 20.09.21

<table>
<tr><td colspan="7">Modul: Steuerung von Cyber Physical Systems / Echtzeitsysteme (AC/I 4.0/Sec-SE</td></tr>
<tr><td colspan="2">52500</td><td>Workload
150h</td><td>Modulart
P</td><td colspan="2">Studiensemester
1</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS und SS</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
90</td><td>Credits (ECTS)
5</td></tr>
<tr><td>2</td><td colspan="7">Lehrform(en) / SWS:
Vorlesung, Umfang 15x3 = 45 SWS
Projekt, Umfang 15x1 = 15 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, 6]

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</td></tr>
</table>

	Eigenständiges Aussuchen einer Aufgabe in Kombination mit dem Modul Eingebettete Systeme. Erstellung von User Stories für Aufgabe zur Lernkontrolle.
	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
5	**Teilnahmevoraussetzungen:** Es wird empfohlen dieses Modul in Kombination zum Modul Eingebettete System zu wählen.
6	**Prüfungsformen***:* Steuerung von Cyber Physicel / Echtzeitsysteme: Klausur K90 (3,5 ECTS) Praktikum Steuerung von Cyber Physical / Praktikum Echtzeitsysteme: Laborarbeit und Präsentation vor Publikum (1,5 ECTS)
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:*** SE-AC/SE-Industrie 4.0/Security SE
9	***Modulverantwortliche(r):*** Prof. Dr. Rembold Dozenten: Prof. Dr. Rembold
10	***Optionale Informationen:*** Keine

4.1.4 52600 – Open Source Intelligence

Studiengang: Systems Engineering
StuPO-Version: 18.1

Semester: WS 2021/22
Letzte Bearbeitung: 20.09.21

<table>
<tr><td colspan="7">Modul: Open Source Intelligence</td></tr>
<tr><td colspan="2">52600</td><td>Workload
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 Open Source Intelligence
Praktikum Open Source Intelligence</td><td>Sprache
Deutsch oder Englisch (Literaturstudium in Deutsch und Englisch erforderlich)</td><td>Kontakt-zeit
60 SWS / 4 h</td><td>Selbst-studium
90</td><td>Credits (ECTS)
5</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, 6]
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 [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]

Selbstständigkeit
Nicht relevant
Studierende können neue OSINT Anwendungen eigenständig identifizieren und erforschen sowie mit der Fachcommunity diskutieren

[Eigenständigkeit/Verantwortung, 7]</td></tr>
</table>

	Aktuelle Aufgabenstellungen und Probleme aus dem OSINT Bereich können eigenständig anhand der aktuellen Forschung im Print- und Preprintbereich erschlossen werden *[Lernkompetenz, 7]*
4	**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
	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, Diskussion, benotet Laborarbeit, unbenotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Ausreichend bewertetes Referat erfolgreiche Teilnahme am Praktikum
8	***Verwendbarkeit des Moduls:*** Systems Engineering, Security

9	***Modulverantwortliche(r):*** Prof. Morgenstern Dozenten: Prof. Dr. Fein
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

4.1.5 52700 – Incident Response und Malware Defense

Studiengang: Systems Engineering
StuPO-Version: 18.1

Semester: WS 2021/22
Letzte Bearbeitung: 20.09.21

<table>
<tr><td colspan="7">Modul: Incident Response und Malware Defense</td></tr>
<tr><td colspan="2">Kennnummer
52700</td><td>Workload
150 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 Incident Response und Malware Defense
Praktikum Incident Response und Malware Defense</td><td>Sprache
Deutsch</td><td>Kontakt-zeit
60 SWS / 4 h</td><td>Selbst-studium
90</td><td>Credits (ECTS)
5</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 Kategorien der Schadsoftware und deren Auswirkung. [Wissen, 7]</td></tr>
<tr><td></td><td colspan="6">Kompetenz Fertigkeiten
Die Studierenden können Methoden entwickeln und anwenden um IT-Angriffe zu erkennen, zu analysieren, einzudämmen und zu beseitigen [Systemische Fertigkeiten, 7]</td></tr>
<tr><td></td><td colspan="6">Sozialkompetenz
Die Studierenden sind in der Lage, sich mittels dem spezifischen Vokabular auszudrücken, sich verständlich zu machen und andere zu verstehen [Kommunikation, 7]</td></tr>
<tr><td></td><td colspan="6">Selbstständigkeit
Die Studierenden sind in der Lage größere Aufgaben, deren Bearbeitung auch mehrere Tage in Anspruch nimmt, 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:

1. Der Incident Response Prozess: Preparation, Detection, Analysis, Containment, Recovery, Post Incident Activity
Veranschaulichung und Vertiefung der Phasen an Beispielen
2. Klassifikation und Taxonomie von Incidents
3. Systemsicherung: Sicherung systemwichtiger Daten
4. Spurensicherung: Netzbasierte Spuren (Netzwerkmitschnitte und Netzwerk-Komponenten), Host-basierte Spuren (persistente und nicht persistente Spuren, Arbeitsspeicher)
5. Spurenanalyse: Netzbasierte Spuren (Netzwerkmitschnitte, Log-Dateien), Host-basierte Spuren (Arbeitsspeicher, Log-Dateien, Dateisysteme)</td></tr>
</table>

	6. Detektion: Signatur-basierte und Regel-basierte Methoden 7. Methoden zur Einschränkung der Schadwirkung: Sandbox, Zugriffsschutz, Rechteüberwachung, Firewall, Proxy, Netzwerksegmentierung 8. Wiederherstellung: Backup und Systemsicherung anwenden 9. Statische Malware-Analyse: Aufbau der Malware, verwendete Bibliotheken, maliziöse Funktionen und Strukturen 10. Dynamische Malware-Analyse: Wirkungsweise der Malware, Schadwirkung lokalisieren 11. Reporting zur Malware-Analyse: Wirkungsweise, Schadenspotential, potentielle Quellen 12. Reporting zum Incident Response-Prozess 13. Post Incident Aktivitäten: Maßnahmen zur Verbesserung der Sicherheit treffen; Training von Incidents Beispiele für Projekte • Aufsetzen einer Signaturbasierten Detektion in einem System. Angriff auf das System. Incident behandeln • Aufsetzen eines Systems mit Schwachstellen (z. B. offene USB-Anschlüsse oder Mail-Clients ohne Makrovirenschutz); Eintragen einer Malware; Incident Response Prozess ausführen • Entwicklung einer Malware, die vermutete Systemschwächen ausnutzt (z. B. Keylogger, DLL-Injektor); Erproben der Malware an einem System mit Malware-Schutz; Incident Respons anwenden
	Empfohlene Literaturangaben: Alan J White (Autor), Ben Clark: Blue Team Field Manual. Create Space Independent Publishing Platform (2017) Gerard Johansen: Digital Forensics and Incident Response.Packt (2012 Johansen, Gerard. Digital Forensics and Incident Response: A practical guide to deploying digital forensic techniques in response to cyber security incidents (Kindle-Positionen14-15). Packt Publishing. Kindle-Version. Cameron H. Malin, Eoghan Casey, James M. Aquilina: Malware Forensics Guide for Windows Systems, Digital Forensics Field Guides. Elsevier (2012) Weitere Literatur, insbesondere aktuelle wissenschaftliche Artikel, werden in der Vorlesung bekannt gegeben.
5	**Teilnahmevoraussetzungen:** Die Studierenden besitzen Kenntnisse, Fertigkeiten und Erfahrungen in • Betriebssysteme • Netzwerke • Netzwerksicherheit • Programmierung in einer Hochsprache und einer Skriptsprache
6	**Prüfungsformen***:* Referat 20 min. mit Ausarbeitung, benotet Praktische Arbeit mit Präsentation 20 min. und Handout, benotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandenes Referat und bestandene Praktische Arbeit
8	***Verwendbarkeit des Moduls:*** Business and Security Analytics

9	***Modulverantwortliche(r):*** Prof. Dr. Rieger Dozenten: Prof. Dr. Rieger
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

4.1.6 51500 – Big Data

Studiengang: Systems Engineering
StuPO-Version: 18.1

Semester: WS 2021/22
Letzte Bearbeitung: 20.09.21

<table>
<tr><td colspan="8">Modul: Big Data</td></tr>
<tr><td colspan="2">51500</td><td>Workload
150h</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)
Vorlesung Big Data
Praktikum Big Data</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="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 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 komplexer 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:
Vorlesung:
- Überblick zu NO-SQL-Datenbanken</td></tr>
</table>

	- 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
	
	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: Ramon Wartala: Hadoop: Zuverlässige, verteilte und skalierbare Big-Data-Anwendungen, Open Source Press Edward Capriolo, Dean Wampler, Jason Rutherglen: Programming Hive, O'Reilly Tom White: Hadoop. The definitive Guide, O' Reilly Uni Hildesheim: MySQL Cluster, http://www.uni-hildesheim.de/rz/DOC/mysql_refman-5.1-de.html/ndbcluster.htmlTobias Trelle: MongoDB, der praktische Einstieg Edward Capriolo, et. al: Programming Hive Erhard Rahm, et. al: Verteiltes und Paralleles Datenmanagemen
5	**Teilnahmevoraussetzungen:** Kenntnisse von relationalen Datenbanken
6	**Prüfungsformen***:* Vorlesung: Klausur K 90 (2,5 ECTS) Praktikum: Labor La (2,5 ECTS)
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Am Ende des Semesters ist eine 90 minütige schriftliche Prüfung zu schreiben. Während des Semesters sind mehrere Praktukumsaufgaben zu bearbeiten.
8	***Verwendbarkeit des Moduls:*** SE-AC/SE-Industrie 4.0/Security SE
9	***Modulverantwortliche(r):*** Prof. Dr. Eppler Dozenten: Prof. Dr. Eppler
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

4.1.7 53000 - Wahlpflichtmodul 1a / 1b

Studiengang: Systems Engineering
StuPO-Version: 18.1

Semester: WS 2021/22
Letzte Bearbeitung: 20.09.21

<table>
<tr><td colspan="7">Modul: Wahlpflichtmodul 1a, Wahlpflichtmodul 1b</td></tr>
<tr><td colspan="2">Kennummer
53000 /
53100</td><td>Workload
600 h</td><td>Modulart
WPM</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)
Module aus WPM-Katalog</td><td>Sprache
Deutsch</td><td>Kontakt-zeit
16 SWS / 360 h</td><td>Selbst-studium
240</td><td>Credits (ECTS)
20</td></tr>
<tr><td>2</td><td colspan="6">Lehrform(en) / SWS:
Vorlesung, Umfang 15x16 = 240 SWS</td></tr>
<tr><td>3</td><td colspan="6">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, 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="6">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>
</table>

5	**Teilnahmevoraussetzungen:** Die geforderten Voraussetzungen sind abhängig von den gewählten Modulteilen und deren Inhalten (s.o.)
6	**Prüfungsformen***:* Siehe jeweilige Modulteilbeschreibungen
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Es gelten die Ausführungen in den Beschreibungen des WPM
8	***Verwendbarkeit des Moduls:*** SE-AC/SE-Industrie 4.0
9	***Modulverantwortliche(r):*** Prof. Dr. Nemirovski Dozenten: s. Modulbeschreibungen der jeweiligen WPM
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

4.1.8 53500 – Einführung Industrie 4.0

Studiengang: Systems Engineering
StuPO-Version: 18.1

Semester: WS 2021/22
Letzte Bearbeitung: 20.09.21

<table>
<tr><td colspan="8">Modul: Einführung Industrie 4.0</td></tr>
<tr><td colspan="2">Kennnummer
53500</td><td>Workload
150 h</td><td>Modulart
P</td><td colspan="2">Studiensemester
1</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS und SS</td></tr>
<tr><td>1</td><td colspan="3">Lehrveranstaltung(en)
Vorlesung Einführung 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="7">Lehrform(en) / SWS:
Vorlesung, 4 SWS</td></tr>
<tr><td>3</td><td colspan="7">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Die Studierenden kennen den aktuellen Forschungsstand ausgewählter Forschungsbereichte Industrie 4.0. [Wissen, 7]
Kompetenz Fertigkeiten
Die Studierenden können Forschungsfragestellungen der Industrie 4.0-Anwendungen mit geeigneten Mechanismen und Methoden in Verbindung setzen und diese zur Bearbeitung der Fragestellung anwenden. [Systemische Fertigkeiten, 7]
Sozialkompetenz
Die Studierenden sind in der Lage, sich mittels dem spezifischen Vokabular auszudrücken, sich verständlich zu machen und andere zu verstehen Kommunikation /Kompetenzausprägung wählen 7]
Selbstständigkeit
Die Studierenden sind in der Lage, komplexe Fragestellungen, deren Bearbeitung auch tiefere Recherche erfordert, zu durchdringen und zur Lösung bekannte Anätze weiterzuentwickeln Lernkompetenz /Kompetenzausprägung wählen 7]</td></tr>
<tr><td>4</td><td colspan="7">Inhalte:

Einführung in die Grundbegriffe von Industrie 4.0,
Vernetzung von Menschen, Maschinen und Prozessen,
Vergleich der verschiedenen Modelle (Industrie 4.0, Industrial Internet Consortium),
Systemlandschaft einer Smart Factory,
Schnittstellen und Technologien der Systemlandschaft,
Herausforderungen, Chancen und Risiken von Industrie 4.0,
Ausprägungen von IT-Angriffen und IT-Sichehreitskonzepten für IoT,

Empfohlene Literaturangaben:
Prof. Dr. Claudia Eckert: IT-Sicherheit: Konzepte – Verfahren – Protokolle. Oldenbourg Verlag München Wien 2014</td></tr>
</table>

5	**Teilnahmevoraussetzungen:** Grundlegende Kenntnisse zu Technischen Informatik und IT-Sicherheit
6	**Prüfungsformen***:* Klausur 90 min., benotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandene Klausur
8	***Verwendbarkeit des Moduls:*** Systems Engineering, Wahlrichtung Industrie 4.0
9	***Modulverantwortliche(r):*** Prof. Dr. Rieger, Prof. Dr. Knoblauch, Prof. Dr. Rembold Dozenten: Prof. Dr. Rieger, Prof. Dr. Knoblauch, Prof. Dr. Rembold
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

4.2 2. Semester

4.2.1 54000 – Theoret. Informatik u. Künstl. Intelligenz

Studiengang: Systems Engineering
StuPO-Version: 18.1
Semester: WS 2021/22
Letzte Bearbeitung: 20.09.21

<table>
<tr><td colspan="8">Modul: Theoret. Informatik u. Künstl. Intelligenz</td></tr>
<tr><td colspan="2">Kennnummer
54000</td><td>Workload
150</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="3">Lehrveranstaltung(en)
54010 Sprachen und Automaten
54020 Mustererkennung</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="7">Lehrform(en) / SWS:
Sprachen und Automaten, Umfang 15 x 2 = 30 SWS
Mustererkennung, Umfang 15 x 2 = 30 SWS</td></tr>
<tr><td>3</td><td colspan="7">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Studierende kennen Sprachen- und Automatentheorie mit Anwendungen im Compilerbau und die Vorgehensweise beim Entwurf Mustererkennungskomponenten und intelligenter Systeme [Wissen, 7]
Kompetenz Fertigkeiten
Studierende sind in der Lage Verfahren für industrielle Mustererkennungsprobleme zu bewerten, einzusetzen und implementieren.
[Instrumentelle Fertigkeiten, 7]
Studierende beherrschen das System des technischen Denkens [Systemische Fertigkeiten, 7]
Sozialkompetenz
Nicht relevant
Selbständigkeit
Fähigkeit Sachverhalte im Bereich der Mustererkennung und des Maschinellen Lernens eigenständig und eigenverantwortlich zu analysieren und zu beurteilen
[Eigenständigkeit / Verantwortung, 6]</td></tr>
<tr><td>4</td><td colspan="7">Inhalte:

Sprachen und Automaten:
- Einführung in die Sprachen- und Automatentheorie:
o Definition Alphabet, Wort, Satz + Beispiele
o Definition formale Grammatik + Beispiele
o Chomsky-Hierarchie (Typ-0, Typ-1, Typ-2, Typ-3 Sprachen)
o Eigenschaften der verschiedenen Sprach-Typen
o Endliche Automaten
o Syntaxdiagramme</td></tr>
</table>

	o Reguläre Ausdrücke, induktiv definiert. - Einführung in Compilerbau: o Definition arithmetischer Ausdrücke o Syntaxgerichtete Übersetzungen, semantische Regeln o Umwandlung von Infix- in Postfixschreibweise durch einen syntaxgerichteten Übersetzer o Linksrekursive vs. Rechtrekursive Grammatiken o Prädiktive Syntaxanalyse und Implementierung eines Recursive-Descent-Parsers. o Maschinencode einer abstrakten Stapelmaschine o Implementierung eines Compilers einer höheren Programmiersprache für Code der abstrakten Stapel Maschine - Einsatz gängiger Werkzeuge (z.B. lex/flex, yacc/bison) Mustererkennung: - Grundlagen der Mustererkennung und des Maschinellen Lernens - Fehlerfunktionen, Optimierung, Validierung - Unüberwachte, überwachte Lernverfahren, Reinforcement Learning - Lineare Modelle für Klassifikation und Regression - Neuronale Netze und Backpropagation Algorithmus - Techniken und Tools für Deep Neural Networks und Deep Learning - Kernel Methoden und Support Vector Machines - Graphische Probabilistische Modelle - K-Means Clustering und Mixture of Gaussians - Expectation Maximization - Selbstreferentielles Autonomes Lernen Literatur (für Sprachen und Automaten): J. R. Hopcroft: Einführung in die Automatentheorie, Formale Sprachen und Komplexitätstheorie, Pearson Studium J. R. Levine et al.: lex & yacc, O'Reilly-Verlag Aho, Sethi, Ullmann: Compilerbau, Teil 1, Oldenbourg Verlag Uwe Schöning: Ideen der Informatik: Grundlegende Modelle und Konzepte der Theoretischen Informatik, Oldenbourg, 2008 Literatur (für Mustererkennung): Bishop, C: Pattern recognition and machine learning, Springer; R. Rojas: Neural Networks – a systematic Introduction, Springer-Verlag W.McKinney: Python for Data Analysis. O'Reilly. F.Chollet: Deep Learning mit Python und Keras, MITP I.Goodfellow, Y.Bengio, A.Courville: Deep Learning, MIT Press
5	Teilnahmevoraussetzungen: Mathematik für Informatiker, Programmierkenntnisse , Grundkenntnisse in C und Python
6	Prüfungsformen: Sprachen und Automaten: Klausur 60 Min. benotet Mustererkennung : Klausur 60 Min. benotet

7	Voraussetzungen für die Vergabe von Kreditpunkten: Das bestehen von beiden Klausuren
8	Verwendbarkeit des Moduls: Systems Engineering-AC/ -Industrie 4.0
9	Modulverantwortliche(r): Prof. Dr. Knoblauch, Prof. Dr. Matecki Dozenten: Prof. Dr. Knoblauch, Prof. Dr. Matecki
10	Optionale Informationen: Studiengangsspezifische, zusätzliche Informationen zum Modul

4.2.2 54500 – IT-Sicherheit

Studiengang: Systems Engineering
StuPO-Version: 18.1

Semester: WS 2021/22
Letzte Bearbeitung: 20.09.21

Modul: IT-Sicherheit					
Kennnummer 54500	**Workload** 150 h	**Modulart** PM	**Studiensemester** 2	**Dauer** 1 Semester	**Häufigkeit** WS und SS

1	**Lehrveranstaltung(en)** 54510 Vorlesung IT-Sicherheit, 54520 Paraktikum IT-Sicherheit	**Sprache** Deutsch	**Kontakt-zeit** 4 SWS / 60 h	**Selbst-studium** 90	**Credits (ECTS)** 5
2	**Lehrform(en) / SWS:** Vorlesung, Übngen: 2 SWS Praktikum: 2 SWS				
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Studierende kennen die Bedeutung, Mechanismen und Komponenten der IT-Sicherheit in Rechnersystemen; *[Wissen, 7]* *Kompetenz Fertigkeiten* Anwenden von Schwachstellenanalyse, IT-Angriff und System-Härtung; beispielhafte Erfahrungen zu E Schwachstellenanalyse, IT-Angriff und System-Härtung im Praktikum [Instrumentelle Fertigkeiten, 7] *Sozialkompetenz* Die Studierenden sind in der Lage, sich mittels dem spezifischen Vokabular auszudrücken, sich verständlich zu machen und andere zu verstehen /Kompetenzausprägung wählen *7]* *Selbstständigkeit* Die Studierenden können im Rahmen einer eigenständigen Arbeit neue Systeme im Bereich Netzwerksicherheit entwickeln und bestehende Systeme bewerten erweitern und analysieren [Eigenständigkeit/Verantwortung, *7]*				
4	**Inhalte*:*** Grundlegende Begriffe; Bedrohungen; Sicherheitsmodelle; Kryptographie, Signaturen, Schlüssel; Authentifikation; Zugriffskontrolle; Sicherheit in Rechnernetzen; *Empfohlene Literaturangaben:* Eckert, c.: IT-Sicherheit. Oldenbourg-Verlag. Tanenbaum, A.: Betriebssysteme. Pearson Studium. Tanenbaum, A.: Computernetzwerke. Pearson Studium Werth, Th.:Die Kunst der digitalen Verteidigung. C&L-Verlag. Ruef, M.: Die Kust des Penetration Testing. C&L-Verlag.				
5	**Teilnahmevoraussetzungen:** Kenntnisse zu Rechner-Systemen in Hardware und Software auf Bachelor-Niveau				

6	**Prüfungsformen***:* Klausur 90 min., benotet Laborarbeit, unbenotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestehen die Klausur und die Laborarbeit
8	***Verwendbarkeit des Moduls:*** Systems Engineering – AC / – Industrie 4.0
9	***Modulverantwortliche(r):*** Prof. Dr. Rieger Dozenten: Prof. Dr. Rieger
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

4.2.3 55000 – Elektronik

Semester: WS 2021/22

Studiengang: Systems Engineering
StuPO-Version: 18.1

Letzte Bearbeitung: 20.09.21

<table>
<tr><td colspan="8">Modul: Elektronik</td></tr>
<tr><td colspan="2">Kennnummer
55000</td><td>Work-load
150</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="3">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
90 h</td><td>Credits (ECTS)
5</td></tr>
<tr><td>2</td><td colspan="7">Lehrform(en) / SWS:
Vorlesung Chipdesign, Umfang 15 x 2 = 30 SWS
Vorlesung Sensoren und Aktoren, Umfang 15 x 2 = 30 SWS</td></tr>
<tr><td>3</td><td colspan="7">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 gegeben 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, 6]
Sozialkompetenz
Erarbeiten der Funktionsweisen ausgesuchter Themen im Team (z.B. GPS). [Kommunikation, 6]
Selbstständigkeit
Transfer der Vorlesungsinhalte in die praktische Anwendung im Rahmen der Übungen. Selbständiges Erlernen der Vorlesungsinhalte für die Klausuren. [Lernkompetenz, 6]</td></tr>
<tr><td>4</td><td colspan="7">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</td></tr>
</table>

	- 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
	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. 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, Vertiefungsrichtungen Advanced Computing, Industrie 4.0, Security Systems Engineering
9	***Modulverantwortliche(r):*** Prof. Dr. Joachim Gerlach, Prof. Dr. Derk Rembold Dozenten: Prof. Dr. Joachim Gerlach, Prof. Dr. Derk Rembold
10	***Optionale Informationen:***

4.2.4 55500 – Security und Internet der Dinge

Studiengang: Systems Engineering
StuPO-Version: 18.1

Semester: WS 2021/22
Letzte Bearbeitung: 20.09.21

<table>
<tr><td colspan="8">Modul: Security und Internet der Dinge</td></tr>
<tr><td colspan="2">Kennnummer
55000</td><td>Workload
150 h</td><td>Modulart
P</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)
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
90</td><td>Credits (ECTS)
5</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,</td></tr>
</table>

	Projekt: - Monitoring mit MQTT, Kafka - Zeitreihenanalyseverfahren mit R z.B.: ARMA, Holt-Winters - IoT-Systeme in der IBM Cloud und Azure
	Empfohlene Literaturangaben: -
5	**Teilnahmevoraussetzungen:** Kenntnisse von relationalen Datenbanken
6	**Prüfungsformen***:* Vorlesung: Klausur K 60 (2,5 ECTS) Projekt: Ha+R (2,5 ECTS)
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.
8	***Verwendbarkeit des Moduls:*** Systems Engineering-AC/ -Industrie 4.0/Security SE
9	***Modulverantwortliche(r):*** Prof. Dr. Eppler Dozenten: Prof. Dr. Eppler
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

4.2.5 55700 – Security Analytics

Studiengang: Systems Engineering
StuPO-Version: 18.1

Semester: WS 2021/22
Letzte Bearbeitung: 20.09.21

<table>
<tr><td colspan="8">Modul: Security Analytics</td></tr>
<tr><td colspan="2">Kennnummer
52700</td><td>Workload
150</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="3">Lehrveranstaltung(en)
a. 52705 Security Analytics
b. 52720 Proj. Security Analytics</td><td>Sprache
a.,b., deutsch oder englisch</td><td>Kontakt-zeit
4 SWS/
a. 30 h
b. 30 h</td><td>Selbst-studium
90</td><td>Credits (ECTS)
5</td></tr>
<tr><td>2</td><td colspan="7">Lehrform(en) / SWS:
a. Vorlesung (2 SWS)
b. Projektarbeit (2 SWS)</td></tr>
<tr><td>3</td><td colspan="7">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="7">Inhalte:
Definition und Begriffsklärung,
Security Analytics Use Cases,
Data Souesess und Methoden der Datensammlung ,
Real time Datensammeln,
Anwendung der Security Analytics Ergebnissen und ihr Impact,
Basic security analytics Costs,
Advanced persistent threats,</td></tr>
</table>

	Security Analytics und Digitale Forensics, 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. 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), Praktische Arbeit (Projekt-Prüfung).
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandene Klausur und die praktische Arbeit
8	***Verwendbarkeit des Moduls:*** Systems Engineering – Security Systems Engineering
9	***Modulverantwortliche(r):*** Prof. Dr. German Nemirovski
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

4.2.6 56000 – Advanced Network and Internet Security

Studiengang: Systems Engineering
StuPO-Version: 18.1

Semester: WS 2021/22
Letzte Bearbeitung: 20.09.21

<table>
<tr><td colspan="8">Modul: Advanced Network and Internet Security (ANIS)</td></tr>
<tr><td colspan="2">Kennnummer
52600</td><td>Workload
150 h</td><td>Modulart
P</td><td colspan="2">Studiensemester
2</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS und SS</td></tr>
<tr><td>1</td><td colspan="3">Lehrveranstaltung(en)
Vorlesung, Seminar, Projekt</td><td>Sprache
Englisch</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="7">Lehrform(en) / SWS:
Vorlesung: 1 SWS
Seminar: 1,5 SWS
Projekt: 1,5 SWS</td></tr>
<tr><td>3</td><td colspan="7">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Die Studierenden kennen den aktuellen Forschungsstand ausgewählter Forschungsbereiche in der Netzwerksicherheit [Wissen, 7]
Kompetenz Fertigkeiten
Die Studierenden können Forschungsfragestellungen der Netzwerksicherheit mit geeigneten Mechanismen und Methoden in Verbindung setzen und diese zur Bearbeitung der Fragestellung anwenden [Instrumentelle Fertigkeiten, 7]

Die Studierenden können eine Forschungsfragestellung bearbeiten und die erzielten Ergebnisse adäquat [Systemische Fertigkeiten, 7]
Sozialkompetenz
Lernergebnisbeschreibung mit einer bestimmten Kompetenz /Kompetenzausprägung wählen /Niveaustufe wählen
Selbstständigkeit
Die Studierenden können im Rahmen einer eigenständigen Arbeit neue Systeme im Bereich Netzwerksicherheit entwickeln und bestehende Systeme bewerten erweitern und analysieren [Eigenständigkeit/Verantwortung, 7]</td></tr>
<tr><td>4</td><td colspan="7">Inhalte:
Die Vorlesung gliedert sich in drei Teile auf, die z.T. zeitlich überlappend durchgeführt werden:
- Wiederholung und Vertiefung der Grundlagen und fortgeschrittenen Aspekte der Netzwerksicherheit. Dieser Teil wird im Rahmen einer Vorlesung absolviert und dient dazu Informatik Studenten ohne spezifischen IT Security Hintergrund die Grundlagen für die Bearbeitung des Referats und des Projekts zu vermitteln.
- Ausarbeitung eines Referats über ein aktuelles Thema der Netzwerksicherheit (basierend auf aktuellen Konferenz- oder Journal Veröffentlichungen aus dem Bereich der Netzwerksicherheit). Dieser Teil dient dazu, an einem konkreten Beispiel den</td></tr>
</table>

	Aufbau einer wissenschaftlichen Arbeit zu erarbeiten und diese zu bewerten. Die Referate werden im Peer-Review Prozess von jeweils zwei Kommilitonen korrigiert und ähnlich zu einem Konferenzformat gehalten (1-tägige Blockveranstaltung). - Bearbeitung eines eigenen Projekts zu einer ausgewählten Forschungsfragestellung aus dem Bereich der Netzwerk- und Internetsicherheit. Dabei werden sowohl Ingenieursmethoden als auch analytische Methoden verwendet um die Fragestellung zu beantworten. Die Projektbearbeitung schließt mit einem Vortrag über die Ergebnisse ab (erneut im Konferenz-Format als Blockveranstaltung). Hier sollen selbständig wissenschaftliche Fragestellungen bearbeitet werden. Beispiele für die zu behandelnden Themen • Sicherheit moderner Kommunikationsprotokolle (HTTP/2, QUIC, P2P Protokolle, etc.) • Aktuelle Angriffe gegen Kommunikationsprotokolle • Protokolle zur Erreichung spezifischer Sicherheitsziele (Vertraulichkeit, Integrität, Verfügbarkeit, Anonymität, Pseudonymität) • Authentifikations- und Authorisierungsprotokolle • Sicherheit im industriellen Umfeld (Fertigung, Steuerung) • Analyse von Kommunikationsdaten zur Erkennung von Sicherheitsproblemen • Analyse verschlüsselter Verbindungen zur Klassifikation von Verkehr • Analyse von Log- Einträgen und anderweitig erfassten Ereignissen zur Erkennung und Klassifikation von Angriffen
	Empfohlene Literaturangaben: R. Anderson, Security Engineering, Wiley, 2009G. Schäfer, M. Roßberg, Netzssicherheit, dpunkt.verlag, 2014 Ausgewählte Literatur bekannter Top-Tier Konferenzen im Bereich Sicherheit und Netzwerksicherheit z.B. ACM CCS, Usenix Security, Defcon, Balckhat, etc.
5	**Teilnahmevoraussetzungen:** Kenntnisse von Netzwerken und IT Sicherheit auf Bachelor Niveau
6	**Prüfungsformen***:* Referat 20 min. mit Ausarbeitung, benotet Laborarbeit, unbenotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestehen des Referates und der Laborarbeit
8	***Verwendbarkeit des Moduls:*** Systems Engineering – Security Systems Engineering
9	***Modulverantwortliche(r):*** Prof. Dr. German Nemirovski Dozenten: Prof. Dr. German Nemirovski
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

4.2.7 56000 – Wahlpflichtmodul 2a / 2b

<table>
<tr><td colspan="8">Modul: Wahlpflichtmodul 2a, Wahlpflichtmodul 2b</td></tr>
<tr><td colspan="2">Kennnummer
56000/
56100</td><td>Workload
600 h</td><td>Modulart
WPM</td><td colspan="2">Studiensemester
1</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS und SS</td></tr>
<tr><td>1</td><td colspan="3">Lehrveranstaltung(en)
Module aus WPM-Katalog</td><td>Sprache
Deutsch</td><td>Kontakt-zeit
16 SWS / 360 h</td><td>Selbst-studium
240</td><td>Credits (ECTS)
20</td></tr>
<tr><td>2</td><td colspan="7">Lehrform(en) / SWS:
Vorlesung, Umfang 15x16 = 240 SWS</td></tr>
<tr><td rowspan="4">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]</td></tr>
<tr><td colspan="7">Kompetenz Fertigkeiten
Die Studierenden sind in Lage Konzepte und Methoden zu abstrahieren und auf neue Anwendungsfelder zu übertragen [Systemische Fertigkeiten, 7]</td></tr>
<tr><td colspan="7">Sozialkompetenz
Projekte organisieren, umsetzen, steuern und die Einhaltung nach Gesichtspunkten des Qualitätsmanagements kontrollieren, überwachen. [Team-/Führungsfähigkeit, 7]</td></tr>
<tr><td colspan="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 rowspan="2">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</td></tr>
<tr><td colspan="7">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>
</table>

7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Es gelten die Ausführungen in den Beschreibungen des WPM
8	***Verwendbarkeit des Moduls:*** SE-AC/SE-Industrie 4.0
9	***Modulverantwortliche(r):*** Prof. Dr. Nemirovski Dozenten: s. Modulbeschreibungen der jeweiligen WPM
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

4.2.8 56500 – Projekt Industrie 4.0

Studiengang: Systems Engineering **Semester**: WS 2021/22
StuPO-Version: 18.1 **Letzte Bearbeitung**: 20.09.21

<table>
<tr><td colspan="8">Modul: Projekt Industrie 4.0</td></tr>
<tr><td colspan="2">Kennnummer
56500</td><td>Workload
150 h</td><td>Modulart
P</td><td colspan="2">Studiensemester
2</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS und SS</td></tr>
<tr><td>1</td><td colspan="3">Lehrveranstaltung(en)
56510 Seminar, Übungen 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="7">Lehrform(en) / SWS:
Seminar, Übngen: 4 SWS</td></tr>
<tr><td>3</td><td colspan="7">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Programmierfähigkeit

Kompetenz Fertigkeiten
Die Studierenden sollen weitgehend selbstständig und unter Berücksichtigung betrieblicher Gegebenheiten die für die Ingineurtätigkverwenden üblichen Methoden und Techniken einsetzen [Systemische Fertigkeiten, 7]

Sozialkompetenz
Nicht relevant

Selbstständigkeit
Das Leitmotiv soll die aktive Aneignung von Wissen durch selbstständiges Lernen anhand der Verknüpfung von Wissenschaft und Praxis sein. Die Lerngelegenheiten werden durch das Industrieprojekt, welches im Unternehmen sowie an der Hochschule durchgeführt wird, gegeben (Prinzip „Forschendes Lernen“ - Wissen und Verstehen sowie Können). [Lernkompetenz, 7]

Die Studierenden sollen technische Projekte weitgehend selbständig bearbeiten [Eigenständigkeit/Verantwortung, 7]</td></tr>
<tr><td>4</td><td colspan="7">Inhalte:
Fertigungssimulation unter Berücksichtigung unternehmensrelevanter Aspekte. Zu entwickeln ist ein Konzept einer bedarfsgerechten Datenerhebung und Simulation eines Fertigungsprozesses in Kooperation mit einem Industrieunternehmen. Hierbei müssen die Prozessketten in der Fertigung/Produktion sowie im Businessbereich untersucht werden. Die ermittelten Daten sind die Grundlage des Fertigungs- und Simulationsmodells.</td></tr>
<tr><td></td><td colspan="7">Empfohlene Literaturangaben:
Eley, Michael (2012): Simulation in der Logistik. Einführung in die Erstellung ereignisdiskreter Modelle unter Verwendung des Werkzeuges "Plant Simulation"; Springer Berlin Heidelberg</td></tr>
<tr><td>5</td><td colspan="7">Teilnahmevoraussetzungen:
Programmierfähigkeit</td></tr>
</table>

6	**Prüfungsformen***:* Eine Kombination aus Hausarbeit und Referat, benotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestehen die Hausarbeit und des Referates
8	***Verwendbarkeit des Moduls:*** Systems Engineering – Industrie 4.0
9	***Modulverantwortliche(r):*** Prof. Dr. Rembold Dozenten: Herr Kliem
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

4.3 3. Semester

4.3.1 60100 – Master-Thesis

Studiengang: Systems Engineering
StuPO-Version: 18.1

Semester: WS 2021/22
Letzte Bearbeitung: 20.09.21

Modul: Master-Thesis						
Kennnummer 61000	**Workload** 750 h	**Modulart** P	**Studiensemester** 3	**Dauer** 1 Semester	**Häufigkeit** WS und SS	
1	**Lehrveranstaltung(en)** Projekt Master-Thesis Mündliche Prüfung Kolloquium	**Sprache** Deutsch (deutsches und englisches Literatur-studium erforderlich)	**Kontakt-zeit** SWS / 0h	**Selbst-studium** 750 (Präsenz & Selbst-studium)	**Credits (ECTS)** 25	
2	**Lehrform(en) / SWS:** Projekt, betreute selbständige wissenschaftliche Arbeit					
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Die Studierenden beweisen ihr Tiefgreifendes Wissen und Fachliche Kompetenz in allen bereichen, die als Qualifikationsziele des Studien gangen deklariert worden soind. *[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* Die Studierenden beweisen ihre Fertigkeit komplexe inhalte und Aufgabenstellungen schriftlich, mit hilfe fon Medien und verbal zu kommunizieren, in der Interaktion mit Betreuern und kollegen nach Lösungen zu suchen und diese nach ihrer Umsetzung in vereinbarten Zeitlichen Rahmen bekannt zu geben. *[Kommunikation, 7]* *Selbstständigkeit* Master-Thesis ist das größte Projekt im gesamten Master-Studiums, das die Studierenden nachweislich selbständig und verantwortlich ausführen. *[Eigenständigkeit/Verantwortung, 7]*					

4	**Inhalte*:*** abhängig von Thema und Inhalt der Master - Thesis
	Empfohlene Literaturangaben: Abhängig vom Thema und Inhalt der Master-Thesis
5	**Teilnahmevoraussetzungen:** Ggf. formal geregelt in der Prüfungsordnung
6	**Prüfungsformen***:* Master-Thesis (Ma.), benotet. Mündliche Prüfung 20 min., benotet Referat 30 Min, unbenotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestehen die Masterthesis (schriftliche Ausarbeitung). Bestehen die mündliche Prüfung Bestehen das Referat
8	***Verwendbarkeit des Moduls:*** Business and Security Analytics, M.Sc.
9	***Modulverantwortliche(r):*** Prof. Dr. German Nemirovski Dozenten: abhängig vom Thema und Inhalt der Master-Thesis
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

4.3.2 61010 – Mündliche Masterprüfung

Studiengang: Systems Engineering
StuPO-Version: 18.1

Semester: WS 2021/22
Letzte Bearbeitung: 20.09.21

<table>
<tr><td colspan="8">Modul: Mündliche Masterprüfung</td></tr>
<tr><td colspan="2">Kennnummer
61010</td><td>Workload
150 h</td><td>Modulart
P</td><td>Studiensemester
3</td><td colspan="2">Dauer
1 Semester</td><td>Häufigkeit
WS und SS</td></tr>
<tr><td>1</td><td colspan="3">Lehrveranstaltung(en)
61030 Mastervortrag
61020 Masterprüfung</td><td>Sprache
Deutsch (deutsches und englisches Literatur-studium erforderlich)</td><td>Kontakt-zeit
---</td><td>Selbst-studium
150 (Präsenz & Selbst-studium)</td><td>Credits (ECTS)
5</td></tr>
<tr><td>2</td><td colspan="7">Lehrform(en) / SWS:
Projekt, betreute selbständige wissenschaftliche Arbeit</td></tr>
<tr><td>3</td><td colspan="7">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Wissen in Abhängigkeit vom Thema der Masterarbeit [Wissen, 7]</td></tr>
<tr><td></td><td colspan="7">Kompetenz Fertigkeiten
Mit dem Master – Vortrag sollen die Studierenden die Ergebnisse ihrer Tätigkeit in eine anschaulichen Art einem fachlich kompetenten Hörerkreis vermitteln. Die Verteidigung soll nicht nur eine Präsentation der wissenschaftlichen Ergebnisse der Masterarbeit, sondern auch eine Präsentation der Persönlichkeit des Vortragenden sein. [Systemische Fertigkeiten, 7]</td></tr>
<tr><td></td><td colspan="7">Sozialkompetenz
Studierende sind in der Lage, sehr komplexe Inhalte in einer plausiblen und transparenten, jedoch aussagekräftigen Form in Kürzester Zeit darzustellen. [Kommunikation, 7]</td></tr>
<tr><td></td><td colspan="7">Selbstständigkeit
Insbesondere in der dem Vortrag folgenden Diskussion sollen die Studierenden Beweis von der Tiefgründigkeit und Sicherheit ihrer Kenntnisse abgeben. [Lernkompetenz, 7]</td></tr>
<tr><td>4</td><td colspan="7">Inhalte:
Ist abhängig vom Thema und Inhalt der Master-Thesis</td></tr>
<tr><td></td><td colspan="7">Empfohlene Literaturangaben:
Anleitung zurwissenschaftlichen Arbeit. Vom Kandidaten selber vorzuschlagende vertiefende Literatur.</td></tr>
<tr><td>5</td><td colspan="7">Teilnahmevoraussetzungen:
Ggf. formal beschrieben in Prüfungsordnung</td></tr>
</table>

6	**Prüfungsformen***:* Referat 30 min., benotet Mündliche Prüfung 30 min., benotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandene Referat, Bestandene mündliche Prüfung
8	***Verwendbarkeit des Moduls:*** Systems Engineering
9	***Modulverantwortliche(r):*** Prof. Dr. German Nemirovski Dozenten: abhängig vom Thema und Inhalt der Master-Thesis
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul