Systems Engineering

Master of Engineering (M.Eng.)

Modulhandbuch

Version 18.1 / Version 1.0

Vertiefungsrichtungen:

- **Advanced Computing**
- **Industrie 4.0**
- **Security Systems Engineering**

Inhalt Seite

1.Semester

2. Semester

3. Semester

Modulnummer	51000
Studiengang	SE-AC/SE-Industrie 4.0/Security SE
Modulbezeichnung	**Eingebettete Systeme**
Lehrveranstaltungen	Eingebettete Systeme (ES) Praktikum Eingebettete Systeme
Semester	1
Modulverantwortliche(r)	Prof. Dr. Rembold
Dozent(in)	Prof. Dr. Rembold
Sprache	Deutsch
Zuordnung zum Curriculum	PM in M.Eng.
Lehrform / SWS	Vorlesung, Umfang 15 x 2 = 30 SWS Praktikum, Umfang 15 x 2 = 30 SWS
Zeitaufwand	• Summe: 150 h • Vorlesung 60 h • Vor- und Nachbereitung der Vorlesung: 36 h • Bearbeitung von Übungsaufgaben: 24 h • Prüfungsvorbereitung und Prüfung: 30 h
Leistungspunkte	5 ECTS
Voraussetzungen	Kenntnisse zu technischen Systemen in Hardware und Software auf Bachelor-Niveau
Lernziele / Kompetenzen	Kennen lernen von Zweck, Funktionsweise und Komponenten von eingebetteten Systemen; Anwenden von Entwurfsverfahren für eingebettete Systeme, beispielhafte Erfahrungen zu Entwurf und Implementierung von ES im Praktikum
Inhalt	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 *Spracherkennung:* Formanten, Cepstrum, Fensterung, MEL Filter, Liftering
Studien- und Prüfungsleistungen	Eingebettete Systeme: Klausur K 90 (2,5 ECTS) Praktikum Eingebettete Systeme: La (2,5 ECTS)
Medienformen	Für Studierende: Skript, Übungsblätter, Aufgabenblätter, Arbeiten am Rechner und an Modellen Dozent: Overhead- und Beamerprojektionen, Demonstrationen am Rechner und an Modellen, Tafel
Literatur	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

Modulnummer	51500
Studiengang	SE-AC/SE-Industrie 4.0/Security SE
Modulbezeichnung	**Big Data**
Lehrveranstaltungen	Vorlesung Big Data Praktikum Big Data
Semester	1
Modulverantwortliche(r)	Prof. Dr. Eppler
Dozent(in)	Prof. Dr. eppler
Sprache	Deutsch
Zuordnung zum Curriculum	PM in M.Eng.
Lehrform / SWS	Vorlesung: 2 SWS Praktikum: 2 SWS
Zeitaufwand	• Summe: 150 h • Vorlesung: 23 h • Praktikum: 23 h • Vor- und Nachbereitung der Vorlesung: 24 h • Vor- und Nachbereitung des Praktikums: 50 h • Prüfungsvorbereitung und Prüfung: 30 h
Leistungspunkte	5 ECTS
Voraussetzungen	Kenntnisse von relationalen Datenbanken
Lernziele / Kompetenzen	**Kenntnisse** Die Studierenden • kennen Systeme und Techniken für die parallele Datenverarbeitung • kennen die Aufgabenstellungen aus dem Themengebiet von Big Data **Fertigkeiten** Die Studierenden können in-memory Datenbanken, Datenbanktechnologien Map Reduce und YARN sowie verteilte Datenbankmanagementsysteme anwenden, darunter z.B. Hadoop, MongoDB, HBase und MySQL-Cluster. **Kompetenzen** Das Modul trägt zum Erreichen der folgenden 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.
Inhalt	**Vorlesung:**

	• Überblick zu No-SQL-Datenbanken, speziell MongoDB • Überblick zu Graphendatenbanken • Architekturen für verteiltes und paralleles Datenmanagement und Datenverteilung • Verteilte Anfragebearbeitung • Clustering und die Map Reduce Funktion • Verteilte Datenbanken o Vertikale/horizontale Fragmentierung o Fragmentierungstransparenz o Transaktionskontrolle • Frameworks für Skalierung und Parallelisierung der Datenzugriffe am Beispiel von Apache Hadoop o Hadoop File System o Map Reduce o YARN o Hive, RHive, Pig, Sqoop, Spark, HBase, o Partitionierung o Graph Builder • Datenbank-Clustering am Beispiel des MySQL Cluster o Cluster einrichten o Partitionstypen o Verwaltung von Partitionen **Praktikum:** Arbeiten mit dem DBMS Hadoop • Partitionierung • SQL-Abfragen • Load von Hadoop mit unstrukturierten Daten wie Texten, Bilder, etc. • Map/Reduce-/YARN- Framework • Hive, Pig, Sqoop, Spark, HBase • BigInsight Arbeiten mit einem MySQL Cluster • Partitionierung • SQL Abfragen Arbeiten mit MongoDB Arbeiten mit Injectiontools wie Apache Nifi
Studien- und Prüfungsleistungen	Vorlesung: Klausur K 90 (2,5 ECTS) Praktikum: Labor La (2,5 ECTS)
Medienformen	Beamer, Tafel
Literatur	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.html Tobias Trelle: MongoDB, der praktische Einstieg Edward Capriolo, et. al: Programming Hive Erhard Rahm, et. al: Verteiltes und Paralleles Datenmanagement

Modulnummer	52000
Studiengang	SE-AC/SE-Industrie 4.0/Security SE
Modulbezeichnung	**Virtuelle Modellierung**
Lehrveranstaltungen	Vorlesung Virtuelle Modellierung Projekt Virtuelle Modellierung
Semester	1
Modulverantwortliche(r)	Prof. Dr. Beisheim
Dozent(in)	Prof. Dr. Beisheim
Sprache	Deutsch
Zuordnung zum Curriculum	PM in M.Eng.
Lehrform / SWS	Vorlesung, Umfang 15 x 2 = 30 SWS Projekt, Umfang 15 x 2 = 30 SWS
Zeitaufwand	• Summe: 150 h • Vorlesung: 60 h • Vor- und Nachbereitung der Vorlesung: 30 h • Bearbeitung von Übungsaufgaben: 30 h • Prüfungsvorbereitung und Prüfung: 30 h
Leistungspunkte	5 ECTS
Voraussetzungen	Für das Praktikum sind Kenntnisse der objektorientierten Modellierung, der Datenstrukturen und der Datenschnittstellen hilfreich, werden aber nicht zwingend vorausgesetzt.
Lernziele / Kompetenzen	Die Studierenden • verfügen über Kenntnisse über Verfahren, Methoden, Algorithmen und Einsatzgebiete Virtueller Modellierung. • 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. *Wissen Niveau 6, Fertigkeit Niveau 6, Selbstständigkeit Niveau 6*
Inhalt	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.
Studien-und Prüfungsleistungen	Virtuelles Modellieren: Klausur K 60 (2,5 ECTS) Projekt Virtuelle Modellierung: Ha + R(2,5 ECTS)
Medienformen	Beamer + PC, Tafel; Skripte und Übungsaufgaben sind online verfügbar
Literatur	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 Manual

Modulnummer	52500
Studiengang	SE-AC/SE-Industrie 4.0/Security SE
Modulbezeichnung	**Steuerung von Cyber Physical Systems/Echtzeitsysteme**
Lehrveranstaltungen	Steuerung von Cyber Physical Systems/Echtzeitsysteme Praktikum Steuerung von Cyber Physical Systems/Echtzeitsysteme
Semester	1.
Modulverantwortliche(r)	Prof. Dr. Rembold
Dozent(in)	Prof. Dr. Rembold
Sprache	deutsch
Zuordnung zum Curriculum	PM M.Eng.
Lehrform / SWS	Vorlesung: Umfang 15 x 3 = 45 SWS Praktikum: Umfang 15 x 1 = 15 SWS
Zeitaufwand	• Summe: 150 h • Vorlesung: 60 h • Vor- und Nachbereitung der Vorlesung: 15 h • Bearbeitung von Übungsaufgaben: 45 h • Prüfungsvorbereitung und Prüfung: 30 h
Leistungspunkte	5 ECTS
Voraussetzungen	keine
Lernziele / Kompetenzen	Verständnis für moderne echtzeitfähige und nebenläufige Softwaresysteme, Einführung in Echtzeitplanung, Vertiefung in Kommunikation und Synchronisation, Bedeutung von Echtzeitbetriebssystemen, Leistungsanalyse und Optimierung für den Entwurf von Echtzeitsystemen, Erläuterung der Begriffe und Verfahren am Beispielen der Automatisierungs- und Kommunikationstechnik.
Inhalt	**Einführung in Steuerung von Cyber Physical/ Echtzeitsysteme:** Echtzeitbetrieb, Ereignisse, Zeitanforderungen, Analyse des technischen Prozesses, Taskbegriff. **Steuerung von Cyber Physical/ Echtzeitbetriebssysteme:** Standard und Echzeitbetriebssysteme, 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 Antwortszeiten. Zeitbedarfsanalyse, Prioritätsinversion durch Unterbrechung. **Lernprojekte im Praktikum** Interruptprogrammierung Analyse eines kontinuierlichen dynamischen Systems
Studien- und Prüfungsleistungen	Steuerung von Cyber Physical/ Echtzeitsysteme: Klausur K 90 (3,5 ECTS) Praktikum Steuerung von Cyber Physical/ Praktikum Echtzeitsysteme: Laborarbeit La (1,5 ECTS)
Medienformen	Beamer, Overhead, Tafel

	Praktikum im Labor mit technischen Modellprozessen.
Literatur	[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.

Modulnummer	53500
Studiengang	SE-Industrie 4.0
Modulbezeichnung	**Einführung Industrie 4.0**
Lehrveranstaltungen	Vorlesung Einführung Industrie 4.0
Semester	1
Modulverantwortliche(r)	
Dozent(in)	Prof. Dr. Rieger/Prof. Dr. Knoblauch/Prof. Dr. Rembold
Sprache	Deutsch
Zuordnung zum Curriculum	PM in M.Eng.
Lehrform / SWS	
Zeitaufwand	• Summe: • Vorlesung und Übungen am Rechner: • Vor- und Nachbereitung der Vorlesung: • Vor- und Nachbereitung der Übungen: • Prüfungsvorbereitung und Prüfung:
Leistungspunkte	5 ECTS
Voraussetzungen	grundlegende Kenntnisse zu IT-Sicherheit
Lernziele / Kompetenzen	* Die Begrifflichkeiten der IT-Sicherheit: Schutzziele, Schwachstellen, Bedrohungen Risiken * Die häufigsten Bedrohungen durch Schadsoftware: Viren, Trojaner, * Angriffe aus dem Internet auf IoT * Die wichtigsten Sicherheitsmechanismen für IoT * Intelligente Adaptive Systeme * Methoden des Machinellen Lernens * Neuronale Netze
Inhalt	
Studien- und Prüfungsleistungen	* Einführung in die IT-Sicherheit * Einführung in IT-Angriffe * Ausprägungen von IT-Angriffen und IT-Sicherheitskonzepten für IoT
Medienformen	Skript, Beamer, Diskussion
Literatur	* Prof. Dr. Claudia Eckert: IT-Sicherheit: Konzepte – Verfahren – Protokolle. Oldenbourg Verlag München Wien 2014

Modulnummer	52600
Studiengang	Security SE
Modulbezeichnung	**Open Source Intelligence**
Lehrveranstaltungen	Vorlesung Open Source Intelligence Praktikum Open Source Intelligence
Semester	1
Modulverantwortliche(r)	Prof. Morgenstern
Dozent(in)	Prof. Morgenstern
Sprache	Englisch oder Deutsch (Literaturstudium Englisch/Deutsch erforderlich)
Zuordnung zum Curriculum	Studiengang Business and Security Analytics Wahl/Pflicht: Wahlpflicht
Lehrform / SWS	Vorlesung, Übungen, Seminar: 3 SWS Praktikum: 1 SWS
Zeitaufwand	Veranstaltung/Art — Präsenz — Eigenstudium Vorlesung,Übungen,Seminar — 45 h — 90 h Praktikum — 15 h — 30 h Summe: — 60 h — 120 h (6 * 30 Std./ECTS)
Leistungspunkte	6 ECTS
Voraussetzungen	Keine
Empfohlene Voraussetzungen	• Grundlagen Betriebssysteme und Netzwerke • Grundlagen IT Sicherheit • Programmierung in einer Skriptsprache
Lernziele / Kompetenzen	Das Modul trägt zum Erreichen der folgenden Lernergebnisse (Kompetenzen) bei: • Die Studierenden kennen OSINT Methoden und Techniken im Bereich Datensammlung, Analyse und Bewertung • Die Studierenden können OSINT Werkzeuge methodisch anwenden, weiterentwickeln oder selbstständig entwickeln • Die Studierenden kennen die relevanten OSINT Terminologien und können gewonnene Daten, Informationen und Ermittlungserkenntnisse unterscheiden, bewerten und in den jeweiligen Kontext einordnen • Die Studierenden kennen Grundzüge des relevanten rechtlichen Rahmens und können konkrete OSINT Methoden und Techniken im legalen, ethischen und moralischen Kontext würdigen • Die Studierenden kennen den aktuellen Forschungsstand ausgewählter OSINT Forschungsbereiche und können die jeweiligen Forschungsergebnisse einordnen Die Studierenden können aktuelle OSINT Forschungsfragestellungen und Thesen wissenschaftlich bearbeiten, Ergebnisse in schriftlicher und mündlicher Form adäquat präsentieren (z.B. als wissenschaftliches Poster, Paper, Talk, Journalartikel)
Inhalt	**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
Studien- und Prüfungsleistungen	Referat 20 min mit zugehörigen Ausarbeitungen und Diskussion, benotet Laborarbeit, unbenotet
Medienformen	Vorlesung/Seminar mit Beamer, Tafel, Poster, Paper physisch oder digital (über Lernplattform)
Literatur	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.

Modulnummer	52700
Studiengang	Security SE
Modulbezeichnung	**Incident Response und Malware Defense**
Lehrveranstaltungen	Vorlesung Incident Response und Malware Defense Praktikum Incident Response und Malware Defense
Semester	1
Modulverantwortliche(r)	Prof. Dr. Rieger
Dozent(in)	Prof. Dr. Rieger
Sprache	Deutsch
Zuordnung zum Curriculum	Studiengang Business and Security Analytics Wahl/Pflicht: Wahlpflicht
Lehrform / SWS	Vorlesung: 2 SWS Praktikum: 2 SWS
Zeitaufwand	Veranstaltung/Art — Präsenz — Eigenstudium Vorlesung & Übungen — 30 h — 60 h Projekt — 30 h — 60 h Summe: (6 * 30 Std./ECTS) — 60 h — 120 h
Leistungspunkte	6 ECTS
Voraussetzungen	Keine
Empfohlene Voraussetzungen	Die Studierenden besitzen Kenntnisse, Fertigkeiten und Erfahrungen in • Betriebssysteme • Netzwerke • Netzwerksicherheit • Programmierung in einer Hochsprache und einer Skriptsprache
Lernziele / Kompetenzen	Das Modul trägt zum Erreichen der folgenden Lernergebnisse (Kompetenzen) bei: • Die Studierenden kennen den aktuellen Forschungsstand zu den Themenbereichen Incident Response und Malware Analyse • Die Studierenden können den Prozess der Incident Response auf konkrete Aufgabenstellungen anwenden und mit spezifischen Methoden umsetzen. • Die Studierenden können im Incident Response Prozess Malware identifizieren, isolieren und analysieren • Die Studierenden können im Rahmen einer eigenständigen Arbeit neue Ansätze für einen Incident Response Prozess mit konkreter Aufgabenstellung entwickeln. • Die Studierenden können im Rahmen einer eigenständigen Arbeit „Trainings-Malware“ für ein Incident Response System entwickeln.
Inhalt	**Vorlesung und Projektarbeit** 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) 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
Studien- und Prüfungsleistungen	Referat 20 min mit Ausarbeitung, benotet Praktische Arbeit mit Präsentation 20 min und Handout, benotet
Medienformen	Folien im PDF-Format; Betrachtung der Implementierung konkreter Anwendungsfälle mit Beamer; Ausarbeitungen und Handouts in Papierform oder als PDF.
Literatur	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, warden in der Vorlesung bekannt gegeben.

Modulnummer	53000/53100
Studiengang	SE-AC/SE-Industrie 4.0
Modulbezeichnung	**Wahlpflichtmodul 1a**, **Wahlpflichtmodul 1b**
Lehrveranstaltungen	Module aus WPM-Katalog (extra Liste)
Semester	1 + 2
Modulverantwortliche(r)	Prof. Dr. Kurz
Dozent(in)	
Sprache	Deutsch
Zuordnung zum Curriculum	WPM in M.Eng.
Lehrform / SWS	Vorlesung, Umfang 15 x 16 = 240 SWS
Zeitaufwand	• Summe: 600 h • Vorlesung: 240 h • Vor- und Nachbereitung der Vorlesung: 120 h • Bearbeitung von Übungsaufgaben: 120 h • Prüfungsvorbereitung und Prüfung: 120 h
Leistungspunkte	20 ECTS
Voraussetzungen	Die geforderten Voraussetzungen sind abhängig von den gewählten Modulteilen und deren Inhalten (s.o.).
Lernziele / Kompetenzen	Je nach Auswahl der Modulteile vertiefen die Hörer ihre Kenntnisse in den Bereichen moderner weiterführender Konzepte der Informatik insbes. Technische Informatik, Regelungstechnik, Wirtschaft, Systementwurf. Darüber hinaus bleibt es den Hörern freigestellt aus dem Lehrangebot anderer Masterstudiengänge im Umfang von bis zu 8 SWS auf Antrag eigene Schwerpunktbildungen vorzunehmen.
Inhalt	Für die hier vorgeschlagenen Modulteile 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.
Studien- und Prüfungsleistungen	Siehe jeweilige Modulteilbeschreibungen
Medienformen	Siehe jeweilige Modulteilbeschreibungen
Literatur	Siehe jeweilige Modulteilbeschreibungen

Modulnummer	53500
Studiengang	SE-AC/SE-Industrie 4.0
Modulbezeichnung	**Theoretische Informatik und Künstliche Intelligenz**
Lehrveranstaltungen	Sprachen und Automaten (SpAu) Mustererkennung (Mu)
Semester	2 (SpAu) + 2 (Mu)
Modulverantwortliche(r)	Prof. Dr. Knoblauch, Prof. Dr. Matecki
Dozent(in)	Prof. Dr. Knoblauch, Prof. Dr. Matecki
Sprache	Deutsch
Zuordnung zum Curriculum	PM in M.Eng.
Lehrform / SWS	Vorlesung (SpAu), Umfang 15 x 2 = 30 SWS Vorlesung (Mu), Umfang 15 x 2 = 30 SWS
Zeitaufwand	• Summe: 150 h • Vorlesung: 60 h • Vor- und Nachbereitung der Vorlesung: 45 h • Bearbeitung von Übungsaufgaben: 30 h • Prüfungsvorbereitung und Prüfung: 15 h
Leistungspunkte	5 ECTS
Voraussetzungen	SpAu: Mathematik für Informatiker, Programmierkenntnisse , Grundkenntnisse in C und Python Mu: Mathematik I – III Programmierkenntnisse von Vorteil, aber nicht zwingend erforderlich
Lernziele / Kompetenzen	SpAu: Einführung in die Sprachen- und Automatentheorie mit Anwendungen im Compilerbau. Mu: Verfahren für industrielle Mustererkennungsprobleme bewerten, einzusetzen, implementieren. Vorgehensweise beim Entwurf Mustererkennungskomponenten; Entwurf intelligenter Systeme; System technisches Denken
Inhalt	SpAu: - 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 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) Mu: Grundlagen merkmalsbasierter Mustererkennung; Mustererkennungs-Verfahrensketten in der Industrie; Statistische Klassifikation; Lernende Klassifikatoren; Elementare Bausteine neuronaler Klassifikatoren; Überwacht lernende Feedforward Netze, Selbstorganisierende Netze mit ihren Lernverfahren und ihrer SW-technischen Realisierung. Optimierung lernender Mustererkennungskomponenten in industriellen Verfahrensketten; Verbesserung der Generalisierungsfähigkeit; (Kreuzvalidierung, Pruning-Verfahren).
Studien- und Prüfungsleistungen	Sprachen und Automaten (SpAu): Klausur K 60 (2,5 ECTS) Mustererkennung (Mu): Klausur K 60 (2,5 ECTS)
Medienformen	Tafel, Overhead, PC mit Beamer
Literatur	SpAu: 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 Mu: R. Rojas: Neural Networks – a systematic Introduction, Springer-Verlag J. Rogers: Object Oriented Neural Networks in C++, Academic Press A. Zell: Simulation Neuronaler Netze, 1. Auflage, Addison-Wesley-Verlag

Modulnummer	54000
Studiengang	SE-AC/SE-Industrie 4.0
Modulbezeichnung	**IT-Sicherheit**
Lehrveranstaltungen	IT-Sicherheit Praktikum IT-Sicherheit
Semester	2
Modulverantwortliche(r)	Prof. Dr. Rieger
Dozent(in)	Prof. Dr. Rieger
Sprache	Deutsch
Zuordnung zum Curriculum	PM in M.Eng.
Lehrform/SWS	Vorlesung, Umfang 15 x 2 = 30 SWS Laborarbeit, Umfang 15 x 2 = 30 SWS
Zeitaufwand	• Summe: 150 h • Vorlesung: 30 h • Vor- und Nachbereitung der Vorlesung: 30 h • Bearbeitung von Übungsaufgaben: 70 h • Prüfungsvorbereitung 20 h
Leistungspunkte	5 ECTS
Voraussetzungen	Kenntnisse zu Rechner-Systemen in Hardware und Software auf Bachelor-Niveau
Lernziele/Kompetenzen	Kennen lernen von Bedeutung, Mechanismen und Komponenten der IT-Sicherheit in Rechnersystemen; Anwenden von Schwachstellenanalyse, IT-Angriff und System-Härtung; beispielhafte Erfahrungen zu E Schwachstellenanalyse, IT-Angriff und System-Härtung im Praktikum
Inhalt	Grundlegende Begriffe; Bedrohungen; Sicherheitsmodelle; Kryptographie, Signaturen, Schlüssel; Authentifikation; Zugriffskontrolle; Sicherheit in Rechnernetzen;
Studien- und Prüfungsleistungen	IT-Sicherheit: Klausur K 90 (2,5 ECTS) Praktikum IT-Sicherheit: Laborarbeit La (2,5 ECTS)
Medienformen	Für Studierende: Skript, Übungsblätter, Aufgabenblätter, Dozent: Overhead- und Beamerprojektionen, Tafel
Literatur	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.

Modulnummer	54500
Studiengang	SE-AC/SE-Industrie 4.0
Modulbezeichnung	**Elektronik**
Lehrveranstaltungen	Chipdesign (CD) Sensoren und Aktoren (SuA)
Semester	2 (CD) + 2 (SuA)
Modulverantwortliche(r)	Prof. Dr. Gerlach/Prof. Dr. Rembold
Dozent(in)	Prof. Dr. Gerlach/Prof. Dr. Rembold
Sprache	Deutsch
Zuordnung zum Curriculum	PM in M.Eng.
Lehrform / SWS	Vorlesung (CD), Umfang 15 x 2 = 30 SWS Vorlesung (SuA), Umfang 15 x 2 = 30 SWS
Zeitaufwand	• Summe: 150 h • Vorlesung: 60 h • Vor- und Nachbereitung der Vorlesung: 40 h • Bearbeitung von Übungsaufgaben: 20 h • Prüfungsvorbereitung und Prüfung: 30 h
Leistungspunkte	5 ECTS
Voraussetzungen	CD: Grundlagen des digitalen Schaltungsentwurfs: Digitale Schaltungstechnik, Entwurf digitaler Systeme SuA: Physik, Elektrotechnik
Lernziele / Kompetenzen	CD: Überblick über Aufbau und Funktionsweise integrierter Schaltungen, theoretische und praktische Kenntnisse in Entwurf und Implementierung integrierter Schaltungen SuA: Der Studierende soll die wesentlichen Sensor- und Aktorprinzipien und ihre anwendungsspezifischen Vorteile kennen lernen. Er soll in der Lage sein entsprechend den Systemanforderungen und den Aufwendungen für die Signalgenerierung die Sensor- oder Aktortechnologie zu bewerten, auszuwählen und zu konfigurieren.
Inhalt	CD: ▪ 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 SuA: **Sensortechnik** ▪ Akkustische 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
Studien- und Prüfungsleistungen	Chipdesign: Klausur K 60 (2,5 ECTS) Sensoren u. Aktoren: Klausur K 60 (2,5 ECTS)
Medienformen	Für Studierende: Skript, Übungsblätter, Aufgabenblätter, Arbeiten am Rechner und an Modellen Dozent: Overhead- und Beamerprojektionen, Demonstrationen am Rechner und an Modellen, Tafel, PC mit Beamer, Intranet- und Internetzugriff
Literatur	Jansen, D. e. al.: Handbuch der Electronic Design Automation Hanser Verlag; Smith, M.: Application-Specific Integrated Circuits, Verlag Adison-Wesley Ashenden, P., Peterson, G., Teegarden, D.: The System Designer's Guide to VHDL-AMS, Verlag Morgan Kaufman Hoppe, B.: ASIC-Design, Springer-Verlag Hering E., Steinhart H.: Taschenbuch der Mechatronik. Niebuhr J., Lindner G.: Physikalische Messtechnik mit Sensoren

Modulnummer	55000
Studiengang	SE-AC/SE-Industrie 4.0
Modulbezeichnung	**Security und Internet der Dinge**
Lehrveranstaltungen	Security und Internet der Dinge Praktikum Security und Internet der Dinge
Semester	2
Modulverantwortliche(r)	Prof. Dr. Thomas Eppler
Dozent(in)	Prof. Dr. Thomas Eppler
Sprache	Deutsch
Zuordnung zum Curriculum	PM in M.Eng.
Lehrform / SWS	Vorlesung: 2 SWS Praktikum: 2 SWS
Zeitaufwand	• Summe: 150 h • Vorlesung : 23 h • Praktikum: 23 h • Vor- und Nachbereitung der Vorlesung: 24 h • Vor- und Nachbereitung des Praktikums: 50 h • Prüfungsvorbereitung und Prüfung: 30 h
Leistungspunkte	5 ECTS
Voraussetzungen	keine
Lernziele / Kompetenzen	**Kenntnisse** Die Studierenden • kennen Systeme und Techniken vom Systemmonitoring bis zu Auswertesystemen • kennen Technologien zur Sicherung dieser Systeme **Fertigkeiten** Die Studierenden können Monitoringtechnologien, WebServices, Datenbanksysteme und BI-Lösungen anwenden. **Kompetenzen** Das Modul trägt zum Erreichen der folgenden Lernergebnisse (Kompetenzen) bei: 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 Internet der Dinge eigenständig zu lesen und qualitative Vergleiche der gelesenen Beiträge systematisch zu präsentieren. • sind in der Lage IoT-Systeme zu analysieren und aufzubauen.
Inhalt	**Vorlesung:** • IoT-Systembeschreibungen • Monitoringtechnologien • Architekturen für verteiltes und paralleles Datenmanagement und Datenverteilung • WebServices

	• Zeitreihenanalyseverfahren, Principal Component Analysis **Praktikum:** • Monitoring mit MQTT, SNMP, Kafka • Datensammler • REST-Webservices • Regelengines • Zeitreihenanalyseverfahren mit R z.B.: ARMA, Holt-Winters • PCA in R • IoT-Systeme in der Cloud z.B. mit BigInsight und Azure
Studien- und Prüfungsleistungen	Vorlesung: Klausur K 90 (2,5 ECTS) Praktikum: Labor La (2,5 ECTS)
Medienformen	Beamer, Tafel
Literatur	keine

Modulnummer	55100
Studiengang	SE-Industrie 4.0
Modulbezeichnung	**Projekt Industrie 4.0**
Lehrveranstaltungen	Projekt Industrie 4.0
Semester	2
Modulverantwortliche(r)	Prof. Dr. Kurz
Dozent(in)	Herr Kliem
Sprache	deutsch
Zuordnung zum Curriculum	PM in M.Eng.
Lehrform / SWS	4
Zeitaufwand	• Summe: 150 h • Vorlesung und Übungen am Rechner: 30 h • Vor- und Nachbereitung der Vorlesung: 15 h • Projektbearbeitung: 70 h • Projektdokumentation: 15 h • Vorbereitung präsentation: 20 h
Leistungspunkte	5 ECTS
Voraussetzungen	
Lernziele / Kompetenzen	• 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). • Die Studierenden sollen technische Projekte und Vorhaben kennen lernen (Fachkompetenz). Sie sollen weitgehend selbstständig und unter Berücksichtigung betrieblicher Gegebenheiten ingenieurmäßig arbeiten (Methodenkompetenz).
Inhalt	• Fertigungssimulation unter Berücksichtigung unternehmensrelevanter Aspekte. • Zu entwickeln ist ein Konzept einer bedarfsgerechten Datenerhebung und Simulation eines Fertigungsprozesses in Kooperation mit einem Industrieunternehmen[1)]. Hierbei müssen die Prozessketten in der Fertigung/Produktion sowie im Businessbereich untersucht werden. Die ermittelten Daten sind die Grundlage des Fertigungs- und Simulationsmodells.
Studien- und Prüfungsleistungen	• Prüfungsvorleistung: Projektbericht + Präsentation • Prüfungsleistung: Ha + R
Medienformen	
Literatur	• Bangsow, Steffen (2008): Fertigungssimulationen mit Plant Simulation und SimTalk. 1. Aufl.: Carl Hanser Verlag GmbH & Co. KG. • Dombrowski, Uwe; Mielke, Tim (Hg.) (2015): Ganzheitliche Produktionssysteme. Aktueller Stand und zukünftige Entwicklungen. Berlin: Springer Vieweg (VDI-Buch). • Kühn, Wolfgang (2006): Digitale Fabrik. Fabriksimulation für Produktionsplaner. München, Wien: Hanser.

	• Eley, Michael (2012): Simulation in der Logistik. Einführung in die Erstellung ereignisdiskreter Modelle unter Verwendung des Werkzeuges "Plant Simulation"; Springer Berlin Heidelberg

1) Firma Mettler-Toledo (Albstadt) GmbH

Modulnummer	55600
Studiengang	Security SE
Modulbezeichnung	**Advanced Network and Internet Security**
Lehrveranstaltungen	Vorlesung Advanced Network and Internet Security Praktikum Advanced Network and Internet Security
Semester	2
Modulverantwortliche(r)	Prof. Dr. Heer
Dozent(in)	Prof. Dr. Heer
Sprache	Englisch
Zuordnung zum Curriculum	Studiengang Business and Security Analytics
Lehrform / SWS	Vorlesung: 1 SWS Seminar: 1,5 SWS Projekt: 1,5 SWS
Zeitaufwand	Veranstaltung/Art — Präsenz — Eigenstudium Vorlesung & Übungen — 10 h — 20 h Seminar — 25 h — 50 h Projekt — 25 h — 50 h Summe: — 60 h — 120 h • (6 * 30 Std./ECTS)
Leistungspunkte	6 ECTS
Voraussetzungen	keine
Empfohlene Voraussetzungen	Die Studierenden besitzen Kenntnisse, Fertigkeiten und Erfahrungen in • Betriebssysteme • Netzwerke • Netzwerksicherheit Programmierung in einer Hochsprache und einer Skriptsprache
Lernziele / Kompetenzen	Das Modul trägt zum Erreichen der folgenden Lernergebnisse (Kompetenzen) bei: • Die Studierenden kennen den aktuellen Forschungsstand ausgewählter Forschungsbereiche in der Netzwerksicherheit • Die Studierenden können Forschungsfragestellungen der Netzwerksicherheit mit geeigneten Mechanismen und Methoden in Verbindung setzen und diese zur Bearbeitung der Fragestellung anwenden • Die Studierenden können eine Forschungsfragestellung bearbeiten und die erzielten Ergebnisse adäquat präsentieren Die Studierenden können im Rahmen einer eigenständigen Arbeit neue Systeme im Bereich Netzwerksicherheit entwickeln und bestehende Systeme bewerten erweitern und analysieren
Inhalt	**Vorlesung, Projektarbeit, Referat** Die Vorlesung gliedert sich in drei Teile auf, die z.T. zeitlich überlappend durchgeführt werden: 14. Wiederholung und Vertiefung der Grundlagen und fortgeschrittenen Aspekte der Netzwerksicherheit. Dieser Teil wird im Rahmen einer Vorlesung absolviert. Informatik Studenten

	ohne spezifischen IT Security Hintergrund werden darin die Grundlagen für die Bearbeitung des Referats und des Projekts vermittelt. 15. Ausarbeitung eines Referats über ein aktuelles Thema der Netzwerksicherheit (basierend auf aktuellen Konferenz- oder Journal Veröffentlichungen aus dem Bereich der Netzwerksicherheit). Die Studierenden lernen an einem konkreten Beispiel den Aufbau einer wissenschaftlichen Arbeit. Die Referate werden im Peer-Review Prozess von jeweils zwei Kommilitonen korrigiert und ähnlich zu einem Konferenzformat gehalten (z.B. Eintägige Blockveranstaltung). 16. Bearbeitung eines eigenen kleinen 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 Autorisierungsprotokolle • 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
Studien- und Prüfungsleistungen	Referat 20 min mit Ausarbeitung/Projektarbeit, benotet
Medienformen	Folien im PDF-Format; Betrachtung der Implementierung konkreter Anwendungsfälle mit Beamer; Referate mit Beamer, Ausarbeitungen und Handouts in Papierform oder als PDF. (Materialien sind in Englisch)
Literatur	R. Anderson, Security Engineering, Wiley, 2009 G. Schäfer, M. Roßberg, Netzsicherheit, dpunkt.verlag, 2014 Ausgewählte Literatur bekannter Top-Tier Konferenzen im Bereich Sicherheit und Netzwerksicherheit z.B. ACM CCS, Usenix Security, Defcon, Balckhat, etc.

Modulnummer	55500
Studiengang	Security SE
Modulbezeichnung	**Security Analytics**
Lehrveranstaltungen	Vorlesung Security Analytics Project Security Analytics
Semester	2
Modulverantwortliche(r)	Prof. Dr. Nemirovski
Dozent(in)	Prof. Dr. Nemirovski
Sprache	Deutsch
Zuordnung zum Curriculum	Studiengang Business and Security Analytics
Lehrform / SWS	Vorlesung: 2 SWS Projekt: 2 SWS
Zeitaufwand	Veranstaltung/Art — Präsenz — Eigenstudium Vorlesung & Übungen — 30 h — 60 h Projekt — 30 h — 60 h Summe: (6 * 30 Std./ECTS) — 60 h — 120 h
Leistungspunkte	6 ECTS
Voraussetzungen	Keine
Empfohlene Voraussetzungen	Die Studierenden besitzen Kenntnisse, Fertigkeiten und Erfahrungen in • Betriebssysteme • Netzwerke • Netzwerksicherheit • Statistik
Lernziele / Kompetenzen	Das Modul trägt zum Erreichen der folgenden Lernergebnisse (Kompetenzen) bei: • Die Studierenden kennen den aktuellen Forschungsstand zu den Themenbereichen Security Analytics • Die Studierenden können die analytischen Prozesse auf konkrete Aufgabenstellungen anwenden und mit spezifischen Methoden und Tools umsetzen. • Die Studierenden können im Rahmen einer eigenständigen Arbeit neue Ansätze für einen Security Analytics Prozess mit konkreter Aufgabenstellung entwickeln.
Inhalt	**Vorlesung und Praktikum** 1. Definition und Begriffsklärung 2. Security Analytics Use Cases 3. Data Souesess und Methoden der Datensammlung 4. Real time Datensammeln 5. Anwendung der Security Analytics Ergebnissen und ihr Impact 6. Basic security analytics Costs 7. Advanced persistent threats 8. Security Analytics und Digitale Forensics 9. 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
Studien- und Prüfungsleistungen	Klausur 90 (6) benotet Praktische Arbeit mit Präsentation 20 min und Handout, benotet
Medienformen	Folien im PDF-Format; Betrachtung der Implementierung konkreter Anwendungsfälle mit Beamer; Ausarbeitungen und Handouts in Papierform oder als PDF.
Literatur	

Modulnummer	55500/55600
Studiengang	SE-AC/SE-Industrie 4.0/Sec-SE
Modulbezeichnung	**Wahlpflichtmodul 2a / Wahlpflichtmodul 2b**
Lehrveranstaltungen	Module aus WPM-Katalog (extra Liste)
Semester	1 + 2
Modulverantwortliche(r)	Prof. Dr. Kurz
Dozent(in)	
Sprache	Deutsch
Zuordnung zum Curriculum	WPM in M.Eng.
Lehrform / SWS	Vorlesung, Umfang 15 x 16 = 240 SWS
Zeitaufwand	• Summe: 600 h • Vorlesung: 240 h • Vor- und Nachbereitung der Vorlesung: 120 h • Bearbeitung von Übungsaufgaben: 120 h • Prüfungsvorbereitung und Prüfung: 120 h
Leistungspunkte	5 ECTS
Voraussetzungen	Die geforderten Voraussetzungen sind abhängig von den gewählten Modulteilen und deren Inhalten (s.o.).
Lernziele / Kompetenzen	Je nach Auswahl der Modulteile vertiefen die Hörer ihre Kenntnisse in den Bereichen moderner weiterführender Konzepte der Informatik insbes. Technische Informatik, Regelungstechnik, Wirtschaft, Systementwurf. Darüber hinaus bleibt es den Hörern freigestellt aus dem Lehrangebot anderer Masterstudiengänge im Umfang von bis zu 8 SWS auf Antrag eigene Schwerpunktbildungen vorzunehmen.
Inhalt	Für die hier vorgeschlagenen Modulteile 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.
Studien- und Prüfungsleistungen	Siehe jeweilige Modulteilbeschreibungen
Medienformen	Siehe jeweilige Modulteilbeschreibungen
Literatur	Siehe jeweilige Modulteilbeschreibungen

Modulnummer	61000
Studiengang	Systems Engineering
Modulbezeichnung	**Master-Thesis**
Lehrveranstaltungen	Master-Thesis Kolloquium
Semester	3
Modulverantwortliche(r)	Prof. Dr. Kurz
Dozent(in)	Ist abhängig vom Thema und Inhalt der Master-Thesis
Sprache	Deutsch, Englisch
Zuordnung zum Curriculum	PM in M.Eng.
Lehrform / SWS	Betreute selbstständige wissenschaftliche Arbeit: 15 x 22 = 330 SWS
Zeitaufwand	• Summe: 936 h • Vorlesung: 660 h • Vor- und Nachbereitung der Vorlesung: 138 h • Prüfungsvorbereitung und Prüfung: 138 h
Leistungspunkte	30 ECTS
Voraussetzungen	Lehrinhalte SE un d TI
Lernziele / Kompetenzen	Mit der Master–Thesis zeigt der Student, dass er unter Anleitung selbstständig 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. Im Rahmen des Kolloquiums wird der Student am Beispiel seiner Master–Thesis seine Vorgehensweise, seine Methoden und seinen Lösungsweg erläutern und begründen. In einer mündlichen Prüfung wird das erworbene Wissen des Studenten im Zusammenhang überprüft. Der Kandidat soll zeigen, dass er das im Studium erworbene Wissen zur Lösung umfassender Ingenieurprobleme anwenden kann.
Inhalt	Ist abhängig vom Thema und Inhalt der Master-Thesis
Studien- und Prüfungsleistungen	Master-Thesis: Ma (25 ECTS) Mündliche Masterprüfung: M (2,5 ECTS) Kolloquium: R (2,5 ECTS)
Medienformen	Ist abhängig vom Thema und Inhalt der Master-Thesis
Literatur	Anleitung zur wissenschaftlichen Arbeit. Projektmanagement und Dokumentation. Vom Kandidaten selber vorzuschlagende vertiefende Literatur