fiw.thws

Faculty of Computer Science and Business Information Systems

Technical University of Applied Sciences Würzburg-Schweinfurt

Module Handbook

Bachelor Information Security (B. Sc.)

Summer semester 2026
Winter semester 2025

Contents

1. semester

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 6810040
Algebra

Module profile

Exam number
6810040

Duration
1 semester

Frequency
Every winter semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar-style instruction

Language of instruction
German

Organisation

Responsible lecturer
Prof. Dr. Andreas Keller

Lecturer(s)
Prof. Dr. Andreas Keller

Applicability	BISD
Semester according to SPO	1. semester
Type of module	Compulsory module

Required prerequisites for the participation in the module according to the SPO
none

Recommended prerequisites for the participation in the module
School maths

Content
General principles:
- Body of real numbers
- Principle of complete induction
- Introduction to the field of complex numbers

Linear algebra:
- Vector spaces (linear independence, basis and dimension)
- Matrices (calculating with matrices, trace and determinant, rank of a matrix)
- Linear systems of equations
- Gaussian algorithm
- Linear mappings

Elementary number theory:
- Residual representation of integers, ggT
- Extended Euclidean algorithm
- Modulo calculus
- Calculating with remainder classes
- Linear congruence equations
- Modular exponentiation

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Written exam (sP) according to § 23 APO

Examination - length/format
90 minutes

The concrete length/format of the examination will be determined in the study plan.

Language of examination
German

Condition for the award of credit points
None

Learning outcomes
1. students remember basic mathematical concepts and procedures relevant to computer science.
2. students understand the principles of algebraic and geometric mathematics and their application in computer science contexts.
3. students apply mathematical techniques to solve problems in computer science and develop solution strategies.
4. students analyse mathematical problems and identify suitable solution approaches taking into account various mathematical theories.
5. students evaluate different solution strategies for their efficiency and appropriateness in computer science.
6. students create mathematical models to abstract and solve complex problems in computer science.

Literature
Bartholomé, Andreas; Rung, Josef; Kern, Hans: Number Theory for Beginners. Vieweg+Teubner, Wiesbaden, 2013.
Beutelspacher, Albrecht; Zschiegner, Marc-Alexander: Discrete mathematics for beginners. Vieweg+Teubner, Wiesbaden, 2014.
Gramlich, Günter: Linear Algebra - An Introduction. Fachbuchverlag Leipzig in the Carl Hanser Verlag, 2021.
Hartmann, Peter: Mathematics for computer scientists. Vieweg +Teubner, Wiesbaden, 2020.
Papula, Lothar: Mathematics for Engineers and Scientists Volumes 1 and 2. Vieweg+Teubner, Wiesbaden, 2018.
Pommersheim, James E.; Marks, Tim K.; Flapan, Erica L.: Number Theory: A Lively Introduction with Proofs, Applications, and Stories. John Wiley & Sons. 2010.
Schubert, Matthias: Mathematics for Computer Scientists. Vieweg +Teubner, Wiesbaden, 2012.
Strang, Gilbert: Linear Algebra. Springer-Verlag, Berlin/Heidelberg/ New York, 2003.

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 5101620,6810030 Databases

Module profile

Exam number
5101620,6810030

Duration
1 semester

Frequency
Every winter semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar-style instruction, Exercise

Language of instruction
German

Organisation

Responsible lecturer
Prof. Dr. Frank-Michael Schleif

Lecturer(s)
Michael Rott

Applicability	BIN, BISD
Semester according to SPO	1. semester
Type of module	Compulsory module

Required prerequisites for the participation in the module according to the SPO
bZv

Recommended prerequisites for the participation in the module
none

Content
The module teaches the basic concepts and techniques of database development. The relational data model and the relational algebra are introduced as theoretical foundations. One focus is on database modelling, in particular the creation of entity-relationship models (ER models) and their conversion into relational schemas, taking normal forms into account. Introduction to the SQL language, including data manipulation, data queries and the definition of schemas and transaction management. Database development and administration is practised in practical exercises and semester-long projects.

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Written exam (sP) according to § 23 APO

Examination - length/format
90 minutes

The concrete length/format of the examination will be determined in the study plan.

Language of examination
German

Condition for the award of credit points
None

Learning outcomes

- Students can explain basic concepts of data persistence and the differences between persistent and non-persistent data.
- Students can define the central terms of relational databases, such as relation, primary key, foreign key and normalisation.
- Students understand relational algebra and can apply simple operations to it.
- Students can explain the connection between conceptual, logical and physical data modelling and justify their importance for database development.
- Students are able to create entity-relationship models (ERM) for given use cases and convert these into relational schemas.
- Students can formulate and execute SQL queries for data manipulation (DML) and schema definition (DDL).
- Students can analyse existing database schemas and evaluate them with regard to redundancy, consistency and normal forms.
- Students are able to analyse technical information requirements and derive suitable data structures and queries from them.

Literature

- Michael Kofler (2024). Database Systems - The Comprehensive Textbook (2nd edition). Bonn: Rheinwerk Verlag GmbH
- Kemper, A., & Eickler, A. (2015). Database systems - An introduction (10th edition). Munich: De Gruyter Oldenbourg Verlag
- Elmasri, R., & Navathe, S. B. (2015). Fundamentals of database systems (7th edition). Munich: Pearson Studium
- Garcia-Molina, H., Ullman, J. D., & Widom, J. (2013). Database Systems: The Complete Book (2nd ed.). Upper Saddle River, NJ: Pearson
- Saake, G., Sattler, K.-U., & Heuer, A. (2011). Databases - Concepts and Languages (3rd ed.). Munich: Pearson Studium

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 5111010,6810010
Basics of Algorithms and Data Structures

Module profile

Exam number
5111010,6810010

Duration
1 semester

Frequency
Every winter semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar-style instruction, Exercise

Language of instruction
German

Organisation

Responsible lecturer
Prof. Dr. Frank Deinzer

Lecturer(s)
Prof. Dr. Frank Deinzer,
Prof. Dr. Dominik Seuß

Applicability	BIN, BISD
Semester according to SPO	1. semester
Type of module	Compulsory module

Required prerequisites for the participation in the module according to the SPO
none

Recommended prerequisites for the participation in the module
none

Content
Theoretical topics
- Recursion: end-recursive/non-end-recursive, linear recursion/tree recursion
- Complexity: O-notation, runtime complexity, memory complexity
- Higher order functions
- (Anonymous) lambda functions
- Abstraction mechanisms: procedural abstraction, abstraction with data
- Representation of complex data structures
- Sorting and searching

Practical topics
- Numerical algorithms
- Algorithms on lists
- Algorithms on trees
- Algorithms on fields
- Algorithms on symbolic data
- Algorithms on strings
- Algorithms on sets
- Algorithms on queues

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Other exam (soP) according to §§ 26, 27 APO

Examination - length/format
Portfolio

The concrete length/format of the examination will be determined in the study plan.

Language of examination
German

Condition for the award of credit points
None

Learning outcomes
Students develop an understanding of the stylistics and aesthetics of programming at the beginning of their training.
Students understand the basic techniques for algorithmic problem solving.
Students generalise the appropriate application of important techniques for mastering complex systems.
Students apply concepts in the areas of recursion and abstraction.
Students apply standard solution techniques to algorithmic problems.

Literature
Abelson, Sussman: Structure and interpretation of computer programs. Springer Verlag, 4th edition, 2014
Wagenknecht: Programming paradigms: An introduction based on Scheme. Vieweg+Teubner, 2013

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 6810050
Foundations of Information Security

Module profile

Exam number
6810050

Duration
1 semester

Frequency
Every winter semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar-style instruction

Language of instruction
German

Organisation

Responsible lecturer
Prof. Dr.-Ing. Sebastian Biedermann

Lecturer(s)
Prof. Dr.-Ing. Sebastian Biedermann

Applicability	BISD
Semester according to SPO	1. semester
Type of module	Compulsory module

Required prerequisites for the participation in the module according to the SPO
none

Recommended prerequisites for the participation in the module
none

Content
In this module, topics that are fundamental for further modules in the Information Security degree programme are explained in the necessary technical depth.
The basics of operating systems, applications, computer networks and programming are always taught with a focus on information security issues.
Different types of attackers, their motivation and their business models are discussed using well-known scenarios from the past as examples.
Furthermore, the various job profiles, the associated tasks and possible career options in the field of information security are presented.

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Written exam (sP) according to § 23 APO

Examination - length/format
90 minutes

The concrete length/format of the examination will be determined in the study plan.

Language of examination
German

Condition for the award of credit points
None

Learning outcomes
Students...

- understand the basic protection goals of information security
- know popular strategies of digital attacks, the motivations and/or business models behind them
- understand the functioning of operating systems and their security mechanisms and security problems
- understand the basic sequence of programmes and processes and the associated security-relevant interactions
- know the basics of digital communication, computer networks and the internet
- are familiar with various job profiles and the associated tasks in the field of information security
- can write simple programmes in a scripting language

Literature
Jason Andress, Foundations of Information Security, 2019
Andrew S. Tanenbaum, Modern Operating Systems, 4th edition, 2016
Andrew S. Tanenbaum, Computer Networks, 5th updated edition, 2019
Justin Seitz & Tim Arnold, Black Hat Python, 2nd edition, 2021

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 6820020
Programming in Python

Module profile

Exam number
6820020

Duration
1 semester

Frequency
Every winter semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar-style instruction, Exercise

Language of instruction
German

Organisation

Responsible lecturer
Prof. Dr. Tristan Wimmer

Lecturer(s)
Prof. Dr. Tristan Wimmer, Christine Zilker

Applicability	BISD
Semester according to SPO	1. semester
Type of module	Compulsory module

Required prerequisites for the participation in the module according to the SPO
none

Recommended prerequisites for the participation in the module
none

Content
This module aims to teach students the basics of programming using the Python programming language. It introduces the basic concepts of programming languages and programming paradigms and creates the basis for further modules in the Software Engineering degree programme.
The following topics are covered:

- Elementary data types, data structures and operators
- Control structures: loops and conditional statements
- Programming with functions
- Introduction to object-orientated programming
- Introduction to the concept of inheritance
- Introduction to exception handling

In addition to these topics, this module demonstrates the appropriate structuring options for code, as well as documentation options for a clean and readable programming style. Furthermore, students are shown how best to encounter and solve problems.

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Written exam (sP) according to § 23 APO

Examination - length/format
90 minutes

The concrete length/format of the examination will be determined in the study plan.

Language of examination
German

Condition for the award of credit points
None

Learning outcomes
After successfully completing the module, students will be able to identify and name the basic data types, data structures and operators and apply them in the Python programming language.

- Students will be able to explain how control structures such as loops and conditional statements control the flow of programmes and how these are implemented in Python.
- After successfully completing the module, students will be able to write simple Python programmes that use functions and parameter passing to solve specific tasks, applying the principle of divide and conquer.
- Students will be able to apply object-oriented programming to improve the structure and maintainability of a programme through encapsulation.
- After successfully completing the module, students will be able to design and implement an object-oriented programme in Python for a specific requirement using the basic principles of inheritance.
- After successfully completing the module, students will be able to apply exception handling for incorrect inputs and data type incompatibilities.

Literature
Häberlein, Tobias. Programming with Python: An Introduction to Procedural, Object-Oriented and Functional Programming. 1st ed. 2024. Berlin, Heidelberg: Springer Berlin Heidelberg, 2024. https://doi.org/10.1007/978-3-662-68678-2.

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 6810060
Social Engineering and Security Awareness

Module profile

Exam number
6810060

Duration
1 semester

Frequency
Every winter semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar-style instruction

Language of instruction
English

Organisation

Responsible lecturer
Prof. Dr. Kristin Weber

Lecturer(s)
Prof. Dr. Kristin Weber,
Andreas Schütz

Applicability	BISD
Semester according to SPO	1. semester
Type of module	Compulsory module

Required prerequisites for the participation in the module according to the SPO
none

Recommended prerequisites for the participation in the module
none

Content
The module Social Engineering and Security Awareness focuses on the human factor of information security. People make a decisive contribution to information security in companies with their behaviour - they are an important security factor. Due to this influence, they are increasingly targeted by cyber criminals. The module primarily looks at these two aspects - security factor and victim - of the human factor in information security.

Information security awareness describes the sensitisation of employees for information security (security factor). The module contains the following contents on awareness:
- Concept and models, psychological understanding of awareness
- Practical examples of awareness measures
- Promoting and measuring awareness

Social engineering is the targeted manipulation of people in order to seduce them into unintentional actions (victims). The following contents, among others, are dealt with in social engineering:
- Basics and forms
- Psychological tricks
- Phishing and phishing simulations

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Written exam (sP) according to § 23 APO

Examination - length/format
90 minutes

The concrete length/format of the examination will be determined in the study plan.

Language of examination
English

Condition for the award of credit points
None

Learning outcomes
Students see people as a solution and not as a problem for information security.
They explain the role of the human factor in information security using examples.
The students know and identify the principles of social engineering and can explain them using examples.
They name different forms of phishing and can discuss the advantages and disadvantages of phishing simulations.
They understand what information security awareness means and know methods to enhance the different aspects of awareness.
Students can create awareness measures in a targeted and individualised way.

Literature
Beißel, S.: Security Awareness, De Gruyter, 2019.
Cialdini, R.: Influence - The Psychology of Persuasion, Collins Business, 2007.
Hadnagy, C. (with Schulman, S.): Human Hacking - Win Friends, Influence People, and Leave Them Better Off for Having Met You, Harper Business, 2021.
Helisch, M.; Pokoyski, D. (eds.): Security Awareness - New Ways to Successfully Sensitise Employees, Vieweg+Teubner, 2010.
Schroeder, J.: Advanced Persistent Training, Apress, 2017.
Verplanken, B. (Ed.): The Psychology of Habit - Theory, Mechanisms, Change, and Context, Springer, 2018.
Weber, K.: Humans and Information Security, Hanser, 2024.
Weber, K.; Schütz, A.; Fertig, T.: Fundamentals and Application of Information Security Awareness, SpringerVieweg, 2019.
Take Aware Sec&Life Magazine, https://www.take-aware-events.com/news-post/magazinesecandlife

2. semester

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 9999999
General Compulsory Elective

Module profile

Exam number
9999999

Duration
1 semester

Frequency
Every semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar

Language of instruction
German/English

Organisation

Responsible lecturer
Prof. Dr. Jochen Seufert

Lecturer(s)
Beate Wassermann

Applicability	BEC, BISD, BDGD
Semester according to SPO	2. semester
Type of module	AWPM

Required prerequisites for the participation in the module according to the SPO
As a rule, none; exceptions are determined and announced by the Faculty of Natural Sciences and Humanities.

Recommended prerequisites for the participation in the module
none

Content
Selection of two general science electives (AWPF) (2 x 2 SWS) or one AWPF (1 x 4 SWS) from the range of subjects offered by the Faculty of Applied Natural Sciences and Humanities (FANG).

Range of subjects offered by the FANG in the areas of
- languages
- cultural studies
- Natural sciences and technology
- Politics, law and economics
- Education, psychology and social sciences
- Soft skills
- Creativity and art.

Courses whose content is already part of or directly related to parts of other modules of the degree programme are excluded from the FANG catalogue. The corresponding courses are marked with a blocking note in the FANG subject catalogue.
The contents of the individual AWPFs are published on the FANG faculty's own homepage.

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Written exam (sP) according to § 23 APO

Examination - length/format
90 minutes

The concrete length/format of the examination will be determined in the study plan.

Language of examination
German/English

Condition for the award of credit points
None

Learning outcomes
The subject-specific learning objectives depend on the AWPF selected.
The students

- also acquire knowledge and competences that are not subject-specific but may be important for the desired career goal, such as special knowledge of foreign languages, natural sciences or social sciences
- analyse a wide variety of issues
- categorise subject-specific knowledge in an interdisciplinary context
- transfer what they have learnt to their current training
- have expanded their key competences and, where applicable, foreign language skills, which supports their personal development, including in intercultural terms
- are aware of their personal, social and ethical responsibilities.

Literature
depending on the selected AWPFs

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 6810100
Basics of Cryptography

Module profile

Exam number
6810100

Duration
1 semester

Frequency
Every summer semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar-style instruction, Exercise

Language of instruction
German

Organisation

Responsible lecturer
Prof. Dr. Andreas Keller

Lecturer(s)
Prof. Dr. Andreas Keller

Applicability	BISD
Semester according to SPO	2. semester
Type of module	Compulsory module

Required prerequisites for the participation in the module according to the SPO
none

Recommended prerequisites for the participation in the module
Module "Algebra"

Content
- Mathematical basics
- Block ciphers
- DES and AES
- The RSA method
- Cryptographic hash function
- Discrete logarithms and the ElGamal method

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Written exam (sP) according to § 23 APO

Examination - length/format
90 minutes

The concrete length/format of the examination will be determined in the study plan.

Language of examination
German

Condition for the award of credit points
None

Learning outcomes
After completing the module, students will be able to

- name mathematical concepts of number theory and linear algebra that are relevant to cryptographic procedures.
- describe and differentiate between basic cryptographic methods such as symmetric and asymmetric encryption.
- explain the functionality of selected cryptographic algorithms (e.g. RSA, Diffie-Hellman, AES) using mathematical principles.
- analyse the security of cryptographic procedures using mathematical criteria (e.g. prime factorisation, discrete logarithm).
- critically evaluate the applicability of cryptographic methods with regard to key lengths, computational effort and known attack scenarios.
- recognise and explain the limits of cryptographic methods, especially with regard to theoretical and practical attacks.
- work on cryptographic tasks independently and in a structured manner.
- use logical thinking to develop suitable solutions for cryptographic problems and justify them mathematically.
- reflect on the importance of mathematical structures for the security of encryption methods.

Literature
Beutelspacher, Wolfenstetter: Cryptography in Theory and Practice, Vieweg+Teubner Verlag | Springer Fachmedien Wiesbaden GmbH, Wiesbaden 2010
Delf, Knebl: Introduction to Cryptography, Springer Berlin, Heidelberg, 2016
Ertel: Applied Cryptography, Hanser Verlag, 2018

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 6810120
ISM-Standards and Processes

Module profile

Exam number
6810120

Duration
1 semester

Frequency
Every summer semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar-style instruction

Language of instruction
English

Organisation

Responsible lecturer
Prof. Dr. Kristin Weber

Lecturer(s)
Prof. Dr. Kristin Weber,
Aaron Kutzner

Applicability	BISD
Semester according to SPO	2. semester
Type of module	Compulsory module

Required prerequisites for the participation in the module according to the SPO
none

Recommended prerequisites for the participation in the module
Social Engineering and Security Awareness

Content
The module Information Security Management (ISM) Standards and Processes deals with the holistic design of information security management in companies and organisations. Information security does not only mean implementing technical measures to protect the IT infrastructure. Rather, organisational, technical, physical and personnel security measures must be coordinated with each other and with the objectives of the organisation. Effective security concepts are developed, implemented, audited, and continuously improved on the basis of established frameworks, taking into account effectiveness, usability and cost efficiency.

Against this background, the module ISM Standards & Processes covers, among others, the following topics:

- Structure and content of information security management (ISM) standards and frameworks (e.g., ISO27001, BSI IT-Grundschutz, CISIS12)
- Creation of holistic information security concepts
- Organisational security measures, e.g., guidelines for information security, classification concept for information
- Metrics and maturity models for information security
- Incident response and business continuity management
- Audits of security concepts and measures

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Written exam (sP) according to § 23 APO

Examination - length/format
90 minutes

The concrete length/format of the examination will be determined in the study plan.

Language of examination
English

Condition for the award of credit points
None

Learning outcomes
Students know the content and structure of ISMS standards and frameworks and select these depending on the situation.
Students create organisational security measures such as information security guidelines.
Students adapt processes such as incident response and business continuity management to organisation-specific requirements.
Students understand the relationship between effectiveness, efficiency, and usability for the selection and implementation of information security measures.
Students know concepts for the evaluation, auditing, and continuous improvement of ISMS.

Literature
Green, J.: Information Security Management Principles, 4th Ed., BCS, 2024
Harich, T.: IT Security Management - The Comprehensive Practical Handbook, 4th Ed., mitp, 2025
Kersten, H.; Schröder, K.: ISO 27001: 2022/2023 - Management of information security according to the current standards, SpringerVieweg, 2023
Lang, M.; Löhr, H: IT Security - Technologies and Best Practices for Implementation in Organisations, 2nd Ed., HANSER, 2025
Sowa, A.: Management of information security - control and optimisation, Springer Vieweg, Wiesbaden, 2017
Weber, K.: People and information security, Hanser, 2024
Whitman, M.; Mattord, H.: Management of Information Security, Cengage Learning, 6th ed., 2019

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 5111120,6810070
Internet Communication

Module profile

Exam number
5111120,6810070

Duration
1 semester

Frequency
Every summer semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar-style instruction

Language of instruction
German

Organisation

Responsible lecturer
Prof. Dr. Christian Bachmeir

Lecturer(s)
Prof. Dr. Christian Bachmeir

Applicability	BIN, BISD
Semester according to SPO	2. semester
Type of module	Compulsory module

Required prerequisites for the participation in the module according to the SPO
none

Recommended prerequisites for the participation in the module
none

Content
Rough structure:
1) Introduction to communication networks
2) Theoretical basics of communication technology
3) Practical basics of Internet communication
4) Introduction to IT security
5) Basics of cryptography

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Written exam (sP) according to § 23 APO

Examination - length/format
90 minutes

The concrete length/format of the examination will be determined in the study plan.

Language of examination
German

Condition for the award of credit points
None

Learning outcomes
1. students remember the basic concepts of communication systems on the Internet and their technical foundations.
2. students understand the functioning of wireless communication technology and its effects on data transmission.
3. students apply modern cryptographic methods to ensure the security of Internet communication.
4. students analyse the performance, possibilities and limitations of communication systems on the Internet in order to make well-founded decisions when developing distributed systems.
5. students understand and evaluate the necessity of cryptographic procedures in different application scenarios of everyday operations.
6. students create concepts for the implementation of security mechanisms in Internet communication systems based on cryptographic techniques they have learnt.

Literature
Patrick Schnabel, Communication Technology Primer, Kindle eBooks
Kurose, Ross: Computer Networks, The Top-Down Approach, Publisher: Pearson Studium; Edition: 6th, updated edition, 2019
Tanenbaum, Wetherall: Computer Networks, Publisher: Pearson Studium; Edition: 5th, updated edition, 2013
Schmeh: Cryptography: Methods - Protocols - Infrastructures (iX-Edition) Publisher: dpunkt.verlag GmbH; Edition: 5th, updated edition, 2013

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 5101820,6810220
Computer Architecture

Module profile

Exam number
5101820,6810220

Duration
1 semester

Frequency
Every summer semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar-style instruction, Exercise

Language of instruction
German

Organisation

Responsible lecturer
Prof. Dr. Christian Bachmeir

Lecturer(s)
Prof. Dr. Christian Bachmeir

Applicability	BIN, BISD
Semester according to SPO	2. semester
Type of module	Compulsory module

Required prerequisites for the participation in the module according to the SPO
none

Recommended prerequisites for the participation in the module
Fundamentals of Computer Engineering

Content
- Historical development
- Calculator classifications (Flynn, Händler, Giloi)
- Computer arithmetic (representation of characters and numbers, IEEE 745, basic arithmetic operations, Booth algorithm)
- Microcomputer core with control and arithmetic unit (pipeline concept, dependencies and their resolution, dynamic scheduling: scoreboard, Tomasulo)
- Machine instructions (ISA, addressing types, assembler programming)
- x86 assembler (nasm, Linux/Ubuntu)
- RISC / CISC concepts (resource conflicts, µprogramming)
- Memory (structure of DRAM, SRAM, caches, coherence protocols)
- I/O and peripherals (external memory, buses)
- Parallel computers and multithreading
- Performance evaluation (basic terms, benchmarks)

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Written exam (sP) according to § 23 APO

Examination - length/format
90 minutes

The concrete length/format of the examination will be determined in the study plan.

Language of examination
German

Condition for the award of credit points
None

Learning outcomes
Students gain an understanding of the structure and operation of computer systems,
and the operation of different computer architectures.
They also acquire basic knowledge in the field of embedded systems.
.
Students are able to

- visualise basic components of simple computers,
- explain different forms of realisation of complex circuits,
- describe relevant memory technologies,
- analyse the structure and programming of processors,
- implement simple assembler programmes and take into account specific characteristics of a computer when programming,
- evaluate the performance of computers,
- design subcomponents of a simple computer.

Literature
Hennessy, John L.; Patterson, David A.: Computer Architecture: A Quantitative Approach. Edition: 2025 (7th edition).
Hennessy, John L.; Patterson, David A.: Computer Organisation and Design. - Edition: 2020 (6th edition).
Brinkschulte, Uwe; Ungerer, Theo: Microcontrollers and Microprocessors - 2nd edition: 2010.
Tanenbaum, Andrew S.: Structured Computer Organisation. - Edition: 2012 (6th edition).
Coy, Wolfgang: Structure and operation of computer systems, 2013.
Hermann, Peter: Computer Architecture, 2013.
Bähring, Heinz: Microcomputer systems, 2013.
Märtin, C.: Introduction to computer architectures, 2003.
Malz, H.: Computer Architecture, 2004.
Oberschelp, W.; Vossen, G.: Rechneraufbau und Rechnerstrukturen, 2006.
Bundschuh, B.; Sokolowsky, P.: Rechnerstrukturen und Rechnerarchitekturen, 1988.
Austin, Todd; Tanenbaum, Andrew S.: Computer Architecture: From Digital Logic to Parallel Computing. Pearson, 2014.
Hennessy, John L.; Patterson, David A.: Computer Organisation and Design: The Hardware/Software Interface. Morgan Kaufmann Publishers, year 2021 (6th edition). Homeister, Matthias: Understanding Quantum Computing: Fundamentals-Applications-Perspectives. Springer-Verlag, 2022.
Vossen, Gerhard; Oberschelp, Werner: Computer Architecture. Oldenbourg-Verlag, 2006.
Slomka, Frank; Glaß, Michael: Fundamentals of Computer Architecture. Springer, 2023.
Ernst, Norbert; Schmidt, Inge; Beneken, Johann: Grundkurs Informatik. Springer, 2023.

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 6820110
Web Exploitation

Module profile

Exam number
6820110

Duration
1 semester

Frequency
Every summer semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar-style instruction

Language of instruction
German/English

Organisation

Responsible lecturer
Prof. Dr.-Ing. Sebastian Biedermann

Lecturer(s)
Prof. Dr.-Ing. Sebastian Biedermann

Applicability	BISD
Semester according to SPO	2. semester
Type of module	Compulsory module

Required prerequisites for the participation in the module according to the SPO
none

Recommended prerequisites for the participation in the module
None

Content
Students learn the professional role and methodological workflow of web penetration testers, including legal and ethical frameworks. Techniques for identifying and exploiting common web vulnerabilities (e.g., OWASP Top Ten) in frontends, backends and APIs are taught. Web post-exploitation scenarios (e.g., web shells, session hijacking, API abuse) and related containment considerations are practised in isolated labs. Finally, students train structured reporting and target-audience appropriate presentation of findings.

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Written exam (sP) according to § 23 APO

Examination - length/format
90 minutes

The concrete length/format of the examination will be determined in the study plan.

Language of examination
German/English

Condition for the award of credit points
None

Learning outcomes
After completing the module, students can:

- describe the professional role of web penetration testers and their responsibilities within IT security.
- outline the typical workflow of a web penetration test (reconnaissance → enumeration → exploitation → post-exploitation → reporting).
- name legal constraints, scope boundaries and ethical considerations and incorporate them into test planning.
- identify common web vulnerabilities (e.g., injection, XSS, CSRF, authentication issues) in test applications and produce reproducible proofs of concept.
- perform web post-exploitation techniques (e.g., session takeover, web shells, API abuse) in a lab context and analyse their effects.
- assess discovered vulnerabilities in terms of exploitability and business impact (e.g., using CVSS criteria) and set remediation priorities.
- document the results of a web penetration test in a structured report and present key findings in a target-appropriate manner.

Literature
The Web Application's Hackers Handbook (Dafydd Stuttart et al.), 2023
Penetration Testing - a Hands-On Introduction to Hacking (Georgia Weidman), 2014
Hacking, The Next Generation (Nitesh Dhanjani et al.), 2021

3. semester

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 5111160,6810140
Backend Systems

Module profile

Exam number
5111160,6810140

Duration
1 semester

Frequency
Every winter semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 30 hrs

Self-study: 120 hrs

Total: 150 hrs

Teaching format
Seminar-style instruction

Language of instruction
English

Organisation

Responsible lecturer
Prof. Dr. Peter Braun

Lecturer(s)
Prof. Dr. Peter Braun

Applicability	BIN, BISD
Semester according to SPO	3. semester
Type of module	Compulsory module

Required prerequisites for the participation in the module according to the SPO
None

Recommended prerequisites for the participation in the module
Programming 1 and Programming 2

Content

- Introduction to distributed systems, client-server, and peer-to-peer systems.
- Software architectures for backend systems (3-tier, hexagonal, monolithic vs. micro-service, event-driven)
- Frameworks to implement backend systems (e.g. Spring)
- Advanced database techniques, scalability, replication, sharding, ORM-tools, query caching, CAP theorem
- Protocols for remote procedure call, for example, GraphQL and Google RPC.
- Basics of the HTTP protocol and application in the form of Web APIs.
- Comprehensive introduction to the REST architecture principle: resources, URLs, CRUD, hypermedia, caching, security.
- Configuration of Web servers (Apache), load balancer, and public caches (nginx)
- Testing of backend systems, performance testing using JMeter, monitoring and logging
- Security aspects of network protocol and backend systems

In the traditional degree programme, the lecturer provides or agrees with the topics of the practical examples for the examination. In the BIN dual study programme, the lecturer consults with the company on a task, ensuring practical relevance and feedback from the company.

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Other exam (soP) according to §§ 26, 27 APO

Examination - length/format
Portfolio

The concrete length/format of the examination will be determined in the study plan.

Language of examination
English

Condition for the award of credit points
None

Learning outcomes

- The students understand the fundamental concepts and differences of distributed systems, including their architecture and communication models.
- The students analyse various software architectures for backend systems and evaluate their suitability for different use cases.
- The students apply advanced database techniques such as replication and sharding to enhance data availability and performance.
- The students implement a backend system using a framework like Spring, following best practices for configuration, deployment, and security.
- The students compare different protocols for remote procedure calls, such as GraphQL and Google RPC, assessing their strengths and limitations.
- The students design RESTful APIs by applying the principles of the REST architecture, focusing on resources, URLs, CRUD operations, and security strategies.
- The students evaluate the security aspects of network protocols and backend systems, proposing improvements based on best practices.

Literature

- Coulouris, J. Dollimore, and T. Kindberg, Distributed Systems: Concepts and Design (4th Edition) (International Computer Science). Boston, MA, USA: Addison-Wesley Longman Publishing Co, Inc, 2005.
- N. Biswas, Practical GraphQL: Learning Full-Stack GraphQL Development with Projects. Berkeley, CA: Apress, 2023.
- J. Webber, S. Parastatidis, and I. Robinson, REST in practice: hypermedia and systems architecture, 1st ed. in Theory in practice. Beijing Cologne: O'Reilly, 2010.
- L. Richardson and M. Amundsen, RESTful Web APIs, First edition, Second release. Beijing Cambridge Farnham Cologne Sebastopol Tokyo: O'Reilly, 2015.
- I. Dominte, Web API Development for the Absolute Beginner: A Step-by-step Approach to Learning the Fundamentals of Web API Development with .NET 7. Berkeley, CA: Apress, 2023.

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 6810180
Governance, Risk, Compliance and Ethics

Module profile

Exam number
6810180

Duration
1 semester

Frequency
Every winter semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar-style instruction

Language of instruction
German

Organisation

Responsible lecturer
Prof. Dr. Kristin Weber

Lecturer(s)
Prof. Dr. Kristin Weber,
Prof. Dr. Markus Oermann

Applicability	BISD
Semester according to SPO	3. semester
Type of module	Compulsory module

Required prerequisites for the participation in the module according to the SPO
none

Recommended prerequisites for the participation in the module
ISM Standards & Processes

Content
Many people and units inside and outside organisations are involved in the management of information security. Governance regulates how transparency, accountability and efficiency are ensured by defining structures, responsibilities and framework conditions, while at the same time safeguarding the interests of all stakeholders. This module shows which stakeholders are involved in information security management, how responsibilities are defined, decisions are made and optimal framework conditions for maximum information security are created.

The identification and assessment of IT risks helps organisations to deal with threats to information security in a targeted and structured manner. The risk-oriented approach is pursued in many ISMS frameworks (information security management system). The module teaches the basics of IT risk management, such as measures for identifying, analysing, assessing and handling IT risks in a structured risk management process.

In the section on ethics, essential conceptual foundations of moral philosophy are explained. On the basis of established schools of ethics, the normative justification of (information) security as a value and guiding principle is examined. The consideration of models for the integration of ethical considerations in development and system design processes builds a bridge to the application of ethical principles in practice. Questions of compliance with the applicable data protection law are also of particular relevance here. After an overview of its basic structures, the focus is on the requirements for technical and organisational data protection as well as the enforcement and consequences of legal violations. Finally, the basics of the reformed information security law are explained.

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Written exam (sP) according to § 23 APO

Examination - length/format
90 minutes

The concrete length/format of the examination will be determined in the study plan.

Language of examination
German

Condition for the award of credit points
None

Learning outcomes
After completing the module, students will be able to

- name and specifically design basic governance mechanisms (e.g. responsibilities, guidelines, decision-making processes, committees) in the context of information security.
- describe relevant roles and participants in information security management within and outside of organisations and differentiate between their tasks.
- explain the importance and function of IT risk management for information security and illustrate this using practical examples.
- identify and describe the organisational framework conditions for effective IT risk management.
- understand, apply and document a simple, structured IT risk management process.
- recognise ethical challenges in dealing with digital systems with security relevance and develop solutions for integrating ethical principles into work processes.
- explain the basic structures of data protection law and answer fundamental questions about data protection compliance.
- describe the main contents of information security law and assess their relevance for operational practice.
- communicate in a targeted manner with legal or regulatory experts on issues relating to data protection and information security law.
- reflect on the relationships between governance, risk and compliance management and ethics in security-critical IT environments.

Literature
Harich, T.: IT-Sicherheitsmanagement: das umfassende Praxis-Handbuch für IT-Security und technische Datenschutz nach ISO 27001. 3rd edition, MITP, 2021.
Johannsen, A.; Kant, D.: IT Governance, Risk and Compliance Management (IT-GRC) - A competence-orientated approach for SMEs. In: HMD - Praxis der Wirtschaftsinformatik, 57, 2020, pp. 1058-1074. https://doi.org/10.1365/s40702-020-00625-8
Kersten, H. et al: IT security management according to the new ISO 27001 - ISMS, risks, indicators, controls. 2nd, updated edition, SpringerVieweg, 2020.
Lang, M.; Löhr, H.: IT-Sicherheit - Technologien und Best Practices für die Umsetzung in Unternehmen. 2nd, revised edition, Hanser, 2024.
Lewinski/Rüpke/Eckhardt (2022): Data protection law. 2nd edition. Munich, C.H. Beck.

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 5003230,6810160
IT Project Management

Module profile

Exam number
5003230,6810160

Duration
1 semester

Frequency
Every winter semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar-style instruction, Exercise

Language of instruction
German

Organisation

Responsible lecturer
Prof. Dr.-Ing. Anne Heß

Lecturer(s)
Prof. Dr. Eva Wedlich,
Prof. Dr.-Ing. Anne Heß

Applicability	BISD, BWI
Semester according to SPO	3. semester
Type of module	Compulsory module

Required prerequisites for the participation in the module according to the SPO
none

Recommended prerequisites for the participation in the module
none

Content

- Introduction to project and project management
- Project organisation
- Project planning process
- Project costing
- Project control and monitoring
- Project completion
- Personnel management and project marketing
- IT product management
- Core activities in IT projects (analysis, design, implementation, integration and stabilisation)
- Quality management and quality assurance
- Configuration management (rudimentary)
- Process models (phase models vs. iterative / incremental / agile process models)
- Agile project management / Scrum

In the non-dual study programme, the lecturer determines the topics of the practical examples for seminar teaching and examination. In the dual study programme, students can work on practical examples from the company in seminar lessons and examinations.

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Written exam (sP) according to § 23 APO

Examination - length/format
90 minutes

The concrete length/format of the examination will be determined in the study plan.

Language of examination
German

Condition for the award of credit points
None

Learning outcomes

- Students learn project management skills, in particular the necessary knowledge for project managers. Project management methods, processes and tools are covered.
- Students are familiarised with relevant core activities of software development and their objectives
- Students can assign and describe relevant sub-activities, input requirements and result types to the core activities
- Students can describe various process models (waterfall model, V-model, Scrum), including their respective advantages and disadvantages, and can describe and assign activities in the process models
- Students understand the characteristic features and differences between phase-orientated process models and iterative/ incremental process models and can select suitable process models for a given project context and justify their selection
- Students know the basic principles, roles, artefacts, ceremonies and practices of agile projects (using Scrum as an example) and can find their way around an agile project as a team member
- Students understand the importance and relevance of software quality
- Students know the key concepts of quality management and quality assurance and can describe the relevant tasks and skills (soft skills) of quality managers
- Students know the main objectives, concepts and activities of configuration management, including the basic functionalities of tools to support configuration management

Literature

- Johannsen, A. and Kramer, A.: Basiswissen für Softwareprojektmanager, dpunkt.verlag, 2017.
- Olfert, K.: Projektmanagement, NWB Verlag, 11th edition 2019.
- Sterrer, C. and Winkler, G.: setting milestones. Project management (methods, processes, tools), Goldegg Verlag, 2010.
- Sterrer, C.: pm k.i.s.s.: Keep it short and simple, Goldegg Verlag, 2011.
- Tiemeyer, E: Handbuch IT-Projektmanagement, Hanser 2018
- Ziegler, Michael : Agile project management with Scrum for beginners, ISBN-13: 979-8751100346 , 2021
- Gundlach, Marco: Agile Project Management - Successfully Navigating with Scrum and Kanban: A Comprehensive Guide for Beginners and Experts, ISBN-13: 979-8392911936, 2023

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 6810170
Security Engineering

Module profile

Exam number
6810170

Duration
1 semester

Frequency
Every winter semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar-style instruction

Language of instruction
German/English

Organisation

Responsible lecturer
Prof. Dr.-Ing. Sebastian Biedermann

Lecturer(s)
Prof. Dr. Benjamin Weggenmann,
Prof. Dr. Minal Moharir

Applicability	BISD
Semester according to SPO	3. semester
Type of module	Compulsory module

Required prerequisites for the participation in the module according to the SPO
none

Recommended prerequisites for the participation in the module
none

Content
Students acquire knowledge and skills for designing and analysing secure IT systems using modern cryptographic methods. The focus is on the practical application of basic cryptographic concepts such as symmetric and asymmetric encryption as well as hashing algorithms for the development of secure applications. In addition, students deal with the functionality and security-relevant aspects of central protocols such as TLS, PGP, Kerberos, VPN/IPSec and the anonymisation network TOR. Current developments such as post-quantum cryptography (e.g. Merkle Signature Scheme), zero-knowledge proofs as well as biometric and multi-factor authentication methods are also covered. Another focus is on the principle of "security by design" and the systematic identification of security-critical vulnerabilities in system architectures. Students learn to analyse security-relevant requirements and use them to design robust (distributed) systems in accordance with current standards. The module thus teaches both conceptual and technical skills for developing secure information systems in complex environments.

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Written exam (sP) according to § 23 APO

Examination - length/format
90 minutes

The concrete length/format of the examination will be determined in the study plan.

Language of examination
German/English

Condition for the award of credit points
None

Learning outcomes
After completing the module, students will be able to

- Describe basic cryptographic concepts (e.g. symmetric/asymmetric encryption, hashing) and use them specifically in security-relevant application scenarios.
- explain the functionality of security-relevant protocols such as TLS, Kerberos, VPN/IPSec, PGP or TOR and analyse security-critical vulnerabilities.
- assess modern authentication methods such as multi-factor authentication, biometric methods and their security-related strengths and weaknesses.
- explain the basics of current cryptographic developments such as post-quantum cryptography (e.g. Merkle Signature Scheme) and assess their potential.
- analyse requirements for secure (distributed) systems and systematically translate them into a secure system design.
- Integrate cryptographic procedures into the design of secure systems and protocols, taking into account current standards and best practices.
- recognise potential threats in the design of security-relevant systems and design suitable technical countermeasures.
- Systematically consider and evaluate security properties (e.g. confidentiality, integrity, authenticity) in system designs.
- reflect on the relationship between technical implementation, cryptographic principles and secure system design.

Literature
Security Engineering: A Guide to Building Dependable Distributed Systems, Ross Anderson, 2020
Applied Cryptography: Protocols, Algorithms and Source Code in C, Bruce Schneider, 1996
Bulletproof TLS and PKI, Second Edition: Understanding and Deploying SSL/TLS and PKI to Secure Servers and Web Applications, Ivan Ristic, 2022

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 5003031
Software industry, education and economy in India

Module profile

Exam number
5003031

Duration
1 semester

Frequency
Every winter semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar

Language of instruction
English

Organisation

Responsible lecturer
Prof. Dr. Isabel John

Lecturer(s)
Prof. Dr. Isabel John,
Prof. Dr.-Ing. Erik Schaffernicht

Applicability	BDGD, BEC, BIN, BISD, BWI
Semester according to SPO	3. semester
Type of module	FWPM

Required prerequisites for the participation in the module according to the SPO
Good knowledge of English

Recommended prerequisites for the participation in the module
none

Content
Introduction to India and our partner university Christ University in Bangalore
Selection of topics for the intercultural presentations (e.g. politics, religion, IT industry) in preparation for the excursion.
Presentation of methods for developing presentations in terms of topic selection, structure and slide design.
Introduction to the topic for the joint projects with Christ University students, which will be worked on in small groups from October.

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Other exam (soP) according to §§ 26, 27 APO

Examination - length/format
Portfolio

The concrete length/format of the examination will be determined in the study plan.

Language of examination
English

Condition for the award of credit points
None

Learning outcomes
Students recall basic facts about India and its importance in information technology.
Students analyse and evaluate differences between Germany and India.
Students use an image-orientated, free presentation style in their presentations.
Students apply basic communication techniques in the intercultural field using India as an example.
Students demonstrate successful co-operation with students from the partner university in the context of a technical project.

Literature
Will be announced in the seminar depending on the topics.

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 6810150
Business and IT Law

Module profile

Exam number
6810150

Duration
1 semester

Frequency
Every winter semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar-style instruction

Language of instruction
German

Organisation

Responsible lecturer
Prof. Dr. Oliver Ehret

Lecturer(s)
Prof. Dr. Oliver Ehret

Applicability	BISD
Semester according to SPO	3. semester
Type of module	Compulsory module

Required prerequisites for the participation in the module according to the SPO
none

Recommended prerequisites for the participation in the module
none

Content
General contract law
Special contract law with regard to IT, special types of contracts Basic principles of copyright law
Overview of relevant areas of intellectual property law Internet law
Data protection law

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Written exam (sP) according to § 23 APO

Examination - length/format
90 minutes

The concrete length/format of the examination will be determined in the study plan.

Language of examination
German

Condition for the award of credit points
None

Learning outcomes
Categorise law, basic legal concepts of our legal system and its basic structures; provide an overview of the role that law plays for IT specialists. Understand the basic principles of general private and public law; understand and classify IT law terms; gain an overview of the main IT-relevant legal areas and contractual areas; recognise, assess and limit legal risks; develop practical skills in dealing with IT-relevant legal problems and know basic types of contracts in the IT sector; acquire basic knowledge of copyright law, especially in the area of software and databases; understand the principles of data protection, especially in the IT sector.
The importance of data protection law, especially in an international context, is emphasised. Emphasis is also placed on conveying how closely computer science, the architecture of IT systems, information security and data protection are interlinked.

Literature
Köhler, Bürgerliches Gesetzbuch, dtv, 89th edition 2022
Schneider: IT and computer law, 15th edition, Beck dtv, Munich 2022.
Kallwass, Abels: Private Law, Verlag Franz Vahlen Munich, 24th edition, 2021
Hoeren: IT Contract Law, 2nd edition, Verlag Otto Schmidt, Cologne 2012.
Marly: Praxishandbuch Softwarerecht, 7th edition, C.H.Beck, Munich 2018.
Härting: Internetrecht, 7th edition, Verlag Otto Schmidt, Cologne 2022.
Hoeren: Skript Internetrecht Uni Münster, as of April 2020
Haug: Basic knowledge of internet law, Verlag W. Kohlhammer, 3rd edition, 2016
Redeker: IT law, C.H.Beck, 7th edition, 2020
Schneider: Handbook, IT law, Otto Schmidt, 5th edition, 2017
Kühling, Sack, Hartmann: Data protection law, 5th edition C.F.Müller, 2021

4. semester

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 6810240
Expertise and Communication

Module profile

Exam number
6810240

Duration
1 semester

Frequency
Every summer semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 30 hrs

Self-study: 120 hrs

Total: 150 hrs

Teaching format
Seminar

Language of instruction
German/English

Organisation

Responsible lecturer
Prof. Dr. Kristin Weber

Lecturer(s)
Prof. Dr. Kristin Weber,
Prof. Dr. Benjamin Weggenmann

Applicability	BISD
Semester according to SPO	4. semester
Type of module	Compulsory module

Required prerequisites for the participation in the module according to the SPO
Module 6810060

Recommended prerequisites for the participation in the module
none

Content
In this seminar, students work independently on current topics from all areas of information security and related topics, such as data protection. The lecturers provide a selection of topics from which the students choose a topic or suggest a different topic. The chosen topic is worked on independently by the students comprehensively and according to scientific principles and documented in a term paper. The accompanying seminar teaches writing and creativity techniques as well as the basics of academic research and work. In addition, students present their topics in a presentation for a non-specialist audience in order to test their ability to present technical topics in a way that is appropriate for the target group.

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Other exam (soP) according to §§ 26, 27 APO

Examination - length/format
Practical study achievement

The concrete length/format of the examination will be determined in the study plan.

Language of examination
German/English

Condition for the award of credit points
None

Learning outcomes
After successfully completing this module,

- students will know how to familiarise themselves independently with information security topics and expand their knowledge.
- be familiar with other current issues relating to information security and related topics, e.g. data protection.
- are able to apply the basics of scientific work.
- are able to show, document and discuss interim results and know what role feedback plays in scientific discourse.
- are able to produce a written paper that fulfils scientific standards.
- are able to prepare, communicate and present scientific and technical topics in a way that is appropriate for the target group.
- are familiar with writing and creativity techniques and can apply them depending on the situation.

Literature
Aengenheyster, S.; Dörr, K. (eds.): Practical Handbook of IT Communication. SpringerGabler, 2019.
Kirchem, S.; Waack, J.: Personas entwickeln für Marketing, Vertrieb und Kommunikation - Grundlagen, Konzept und praktische Umsetzung. SpringerGabler 2021.
Lubienetzki, U.; Schüler-Lubienetzki, H.: Was wir uns wie sagen und zeigen - Psychologie der menschlichen Kommunikation. Springer, 2020.

Module: 5111230,6810200
Frontend Systems

Module profile

Exam number
5111230,6810200

Duration
1 semester

Frequency
Every summer semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar-style instruction, Exercise

Language of instruction
English

Organisation

Responsible lecturer
Prof. Dr. Peter Braun

Lecturer(s)
Prof. Dr. Peter Braun

Applicability	BIN, BISD
Semester according to SPO	4. semester
Type of module	Compulsory module

Required prerequisites for the participation in the module according to the SPO
none

Recommended prerequisites for the participation in the module
Backend Systems

Content

- Introduction to Web Technologies: Basic building blocks of web development, including HTML for structuring web content, CSS for styling and layout, and JavaScript for adding interactivity and dynamic behaviour to web pages.
- Advanced JavaScript and Modern ES6+ Features: More details about JavaScript, exploring modern ES6+ features such as let, const, arrow functions, template literals, modules, promises, and async/await, and learn how to apply these in real-world scenarios.
- Fundamentals of React: Core concepts of React, including its component-based architecture, JSX syntax, and the use of state and props to manage data within components, enabling the creation of dynamic and interactive user interfaces.
- Advanced React Techniques: Advanced topics in React, such as the Context API for state management across the application, React hooks for managing state and side effects in functional components, and performance optimisation strategies.
- IT Security in Frontend Development: Principles of IT security as they relate to frontend development, including securing user input, preventing cross-site scripting (XSS) and cross-site request forgery (CSRF), and ensuring secure communication between frontend and backend systems. Introduction to the Open Web Application Security Project Top Ten list.
- Project Development and Deployment: Setting up development environments, following best practices in code organisation and documentation, and deploying and maintaining frontend applications in a production environment.

In the traditional degree programme, the lecturer provides or agrees with the topics of the practical examples for the examination. In the BIN dual study programme, the lecturer consults with the company on a task, ensuring practical relevance and feedback from the company.

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Other exam (soP) according to §§ 26, 27 APO

Examination - length/format
Portfolio

The concrete length/format of the examination will be determined in the study plan.

Language of examination
English

Condition for the award of credit points
None

Learning outcomes

- The students understand the foundational principles of HTML, CSS, and JavaScript to build and style basic web pages effectively.
- The students apply modern web frameworks like React and Svelte to develop dynamic and responsive user interfaces.
- The students analyse different state management techniques, such as React hooks and the context API, to manage complexity in web applications.
- The students design cross-platform mobile user interfaces using Flutter, focusing on user experience and performance.
- The students implement best practices in frontend development, including version control, testing, and secure deployment processes.
- The students create a comprehensive frontend project from scratch, integrating all learned concepts into a fully functional application.
- The students evaluate different frameworks and tools for frontend development to make informed decisions based on specific project requirements.

Literature

Marijn Haverbeke: Eloquent JavaScript: A Modern Introduction to Programming. 4th edition, 2024.
Alex Banks, Eve Porcello: Learning React: Modern Patterns for Developing React Apps. O'Reilly, 2020.
Thomas Bailey, Alessandro Biessek: Flutter for Beginners: Cross-platform mobile development from Hello, World! to app release with Flutter 3.10+ and Dart 3.x. Packt, 2023.
Andrew Hoffman: Web Application Security: Exploitation and Countermeasures for Modern Web Applications. O'Reilly, 2024.

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 6100930,6810190
Innovation Management and Entrepreneurship

Module profile

Exam number
6100930,6810190

Duration
1 semester

Frequency
Every summer semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar-style instruction

Language of instruction
German

Organisation

Responsible lecturer
Prof. Dr. Michael Müßig

Lecturer(s)
Prof. Dr. Michael Müßig

Applicability	BEC, BISD
Semester according to SPO	4. semester
Type of module	Compulsory module

Required prerequisites for the participation in the module according to the SPO
none

Recommended prerequisites for the participation in the module
none

Content
Intro: Motivation, innovation, company, founding a company, startup and a look at economic history
Definitions: Management, ... and all terms relating to innovation and types of innovation
Processes and correlations: Adoption and diffusion, acceptance
Prediction: Gartner's hypecycle and the three horizons
Innovation in the company, Schumpeter and the innovator's dilemma, disruption
Startup ecosystems
End-to-end: design thinking, personas and value proposition, business model canvas, lean startup and customer development, MVP and prototyping
The business plan, founding team
Growth and change, growth hacking
Founding, financing, designing and evaluating companies
Open and crowd innovation, Jugaad, frugal and sustainability in founding and innovation

CASE studies (alternating): Tesla, Kodak and digital photography, Fashion and TEC, Scoutbee, Vogel Communications

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Written exam (sP) according to § 23 APO

Examination - length/format
90 minutes

The concrete length/format of the examination will be determined in the study plan.

Language of examination
German

Condition for the award of credit points
None

Learning outcomes
After successfully completing the module, students will be able to

- Present and explain the terminology in the field of innovation management as well as business creation and management
- assess statements on regional and company-internal ecosystems for innovation and intra- and entrepreneurship
- Understand the importance of teams and team processes in the field of innovation development and business creation and be able to apply team-building methods
- Students learn the basics of a business plan in terms of its structure and creation and are able to develop and create one independently
- Identify the key tax, legal and economic building blocks of a successful business start-up and analyse their significance
- They will be able to present and design their own business model ideas using the methodical approaches of design thinking, value proposition and business modelling

Literature
Mandatory:
Hess, Thomas: Strategically managing digital transformation. Springer Fachmedien Wiesbaden GmbH, 2019
Osterwalder, Alexander; Pigneur, Yves et al: Business Model Generation, campus Verlag, 2013 (and more recent editions)
Ries, Eric: Lean Startup, 4th ed. Reline-Verlag Munich 2015
Kotsemir, M.; Abroskin, A.; Meissner, D.: Innovation Concepts and Typology - an evolutionary
Discussion. Basic Research Programme, Working papers, SERIES: SCIENCE, TECHNOLOGY AND INNOVATION WP BRP 05/STI/2013

Supplementary:
Christensen, Clayton M.: The Innovators Dilemma, Harvard Business Review Press (1997 and current editions, also available in German)
Burkhardt, Christoph: Thinking error innovation; SpringerGabler 2017

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 6820220
OS Exploitation

Module profile

Exam number
6820220

Duration
1 semester

Frequency
Every summer semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar-style instruction

Language of instruction
German/English

Organisation

Responsible lecturer
Prof. Dr. Benjamin Weggenmann

Lecturer(s)
Prof. Dr. Benjamin Weggenmann

Applicability	BISD
Semester according to SPO	4. semester
Type of module	Compulsory module

Required prerequisites for the participation in the module according to the SPO

•

Recommended prerequisites for the participation in the module
IT Security Fundamentals (IT Security Fundamentals)

Content
OS Exploitation provides a practice-oriented introduction to software vulnerabilities and exploitation techniques on modern operating systems. Students learn relevant OS architecture fundamentals (kernel and user space, privilege rings, process and memory management, calling conventions, system calls, access control) as a basis for understanding how typical vulnerabilities such as buffer and heap overflows, integer overflows, format string bugs, and race conditions arise in real-world software. Building on this foundation, the module covers userland and kernel exploitation (including shellcode and privilege escalation), the use of the Metasploit framework (e.g. Meterpreter, privilege escalation), and the analysis of malware families, business models, detection and evasion techniques, with a particular focus on API hooking and endpoint detection and response (EDR/XDR) concepts.

Students apply static and dynamic analysis methods such as disassembly, reverse engineering, debugging, fuzzing, and sandboxing/emulation to identify and assess vulnerabilities in binaries and to select and use suitable exploits. The module discusses compiler-, OS- and hardware-based defence mechanisms (e.g. bounds checking, stack canaries, ASLR, non-executable memory, secure boot) as well as advanced attack techniques such as Return-Oriented Programming to illustrate how such protections can be bypassed. On completion, students understand common vulnerability classes and mitigation techniques in contemporary operating systems, can judge the exploitability and severity of discovered weaknesses, interpret and write simple detection rules, and are familiar with basic threat intelligence sharing concepts.

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Written exam (sP) according to § 23 APO

Examination - length/format
90 minutes

The concrete length/format of the examination will be determined in the study plan.

Language of examination
German/English

Condition for the award of credit points
None

Learning outcomes

- Students understand common forms of software vulnerabilities.
- They can apply static and dynamic analysis techniques to analyse binaries to discover and identify vulnerabilities.
- They are able to assess the severity of discovered vulnerabilities based on their exploitability.
- They are able to select and apply suitable exploits to discovered vulnerabilities.
- Students understand mitigation techniques implemented in modern OSes and, where applicable, novel attack strategies that may circumvent them.
- Students understand how malware works and the methods it uses to avoid detection. They can apply simple evasion techniques themselves.
- Students know about threat intelligence sharing and can interpret and write simple detection rules.

Literature
Will be announced in the lecture.

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 5100240,6810210
Programming Project

Module profile

Exam number
5100240,6810210

Duration
1 semester

Frequency
Every semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 12 hrs

Self-study: 138 hrs

Total: 150 hrs

Teaching format
Seminar

Language of instruction
German

Organisation

Responsible lecturer
Prof. Dr. Peter Braun

Lecturer(s)
Prof. Dr. Peter Braun

Applicability	BISD, BIN
Semester according to SPO	4. semester
Type of module	Compulsory module

Required prerequisites for the participation in the module according to the SPO
BIN: Programming I and Programming II
BISD: Programming I

Recommended prerequisites for the participation in the module
Programming I + II
Databases I
Software Engineering I

Content
The students should realise their own application in groups. An application could, for example, be a game, a three-tier web application or a comparable application. Possible parts of the application could be a graphical user interface (including a web interface), database connection including schema design, network communication, AI, etc. The students also create documentation (general overview, various use cases, the most important activity and sequence diagrams, etc.).

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Other exam (soP) according to §§ 26, 27 APO

Examination - length/format
Practical study achievement

The concrete length/format of the examination will be determined in the study plan.

Language of examination
German

Condition for the award of credit points
None

Learning outcomes
After successfully completing the module, students will be able to

- develop a first larger application in a team of 4-6 people
- carry out and implement project planning
- carry out and implement a task distribution
- apply their knowledge of software design
- apply programming concepts they have learnt
- look up required content themselves using suitable literature
- break down a task into sub-problems.

Literature
None

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 6810230
Security Operations

Module profile

Exam number
6810230

Duration
1 semester

Frequency
Every summer semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar-style instruction

Language of instruction
German/English

Organisation

Responsible lecturer
Prof. Dr. Benjamin Weggenmann

Lecturer(s)
Dr.-Ing. Rodrigo Daniel do Carmo,
Prof. Dr. Benjamin Weggenmann

Applicability	BISD
Semester according to SPO	4. semester
Type of module	Compulsory module

Required prerequisites for the participation in the module according to the SPO
none

Recommended prerequisites for the participation in the module
none

Content
Students learn how to secure networks and IT systems using technical protective measures. The focus is on central security components such as firewalls, proxies and intrusion detection systems (IDS). Students acquire practical knowledge of how to set up, configure and use these systems in realistic scenarios. The content is based on the typical requirements of a corporate environment and established security standards such as those of the National Institute of Standards and Technology (NIST). A special focus is placed on the topic of security monitoring: students learn to identify, correlate and analyse security-relevant information from various sources in a targeted manner. They develop and implement case-specific detection rules for attack detection and deal with the tasks and processes of a Security Operations Centre (SOC), including logging, incident detection and response. The module thus provides a practical understanding of the operation of IT security systems in modern corporate environments.

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Other exam (soP) according to §§ 26, 27 APO

Examination - length/format
Practical study achievement

The concrete length/format of the examination will be determined in the study plan.

Language of examination
German/English

Condition for the award of credit points
None

Learning outcomes

- Students know the functions of firewalls, proxies and intrusion detection systems and can set them up
- Students can develop and implement case-specific rules for recognising attacks
- Students can identify and collate security-relevant information for security monitoring
- Students know the tasks of a Security Operations Centre (SOC)

Literature

Defensive Security Handbook: Best Practices for Securing Infrastructure, Lee Brotherston and Amanda Berlin, 2017
Zero Trust Security: An Enterprise Guide, Jason Garbis and Jerry W. Chapman, 2021
Security Operations Centre: Building, Operating and Maintaining Your SOC, Joseph Muniz and Gary McIntyre, 2015

5. semester

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 6810250
Supervised Internship

Module profile

Exam number
6810250

Duration
1 semester

Frequency
Every semester

Credit hours (SWS)
1

ECTS-Credits (CP)
30.0

Workload
Guided study time:
Presence time: 15 hrs

Self-study: 885 hrs

Total: 900 hrs

Teaching format
Practice

Language of instruction
German/English

Organisation

Responsible lecturer
Michael Rott

Lecturer(s)
Michael Rott

Applicability	BISD
Semester according to SPO	5. semester
Type of module	Compulsory module

Required prerequisites for the participation in the module according to the SPO
> 90 ECTS points. 55 ECTS from 1st year

Recommended prerequisites for the participation in the module
none

Content

- As part of a larger IT project, you will be required to work independently in as many project phases as possible (system analysis, system planning, implementation, system introduction and testing). This project should last at least 12 weeks.
- Ideally, the intern will familiarise themselves with various departments and areas of the company prior to the project in order to gain a rough understanding of other departments and the company as a whole.

The contact person/supervisor at the FHWS is the representative for the supervised practical phase, Prof. Dr Tobias Aubele

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Other exam (soP) according to §§ 26, 27 APO

Examination - length/format
Documentation, Presentation

The concrete length/format of the examination will be determined in the study plan.

Language of examination
German/English

Condition for the award of credit points
None

Learning outcomes
The trainee should

- acquire relevant, practice-orientated knowledge of operational processes
- learn (through guidance) to work independently and autonomously in IT projects.
- combine competences acquired during their studies with practical experience.
- learn to understand problems and requirements (e.g. customer requirements).
- learn to design and implement solutions to problems (e.g. for company processes and/or IT projects).
- experience working in a team.
- get to know and experience embedding in the company, its processes and organisational procedures.
- get to know and experience the IT profession.
- learn to approach the right people when problems arise.
- learn about the unconditional will to successfully and professionally realise projects.
- experience excellence and professionalism.
- experience how employees are captivated.
- recognise and feel the meaning of their work.

Literature
No general literature recommendation possible

6. semester

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 5003180
Advanced Database Techniques

Module profile

Exam number
5003180

Duration
1 semester

Frequency
Every semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar

Language of instruction
German

Organisation

Responsible lecturer
Prof. Dr. Peter Braun

Lecturer(s)
Michael Rott

Applicability	BIN, BWI, BISD
Semester according to SPO	6. semester
Type of module	FWPM

Required prerequisites for the participation in the module according to the SPO
none

Recommended prerequisites for the participation in the module
Databases, Databases I, Backend Systems

Content
As part of this module, students acquire practical and interdisciplinary skills in the field of modern database management. The content taught is designed to combine technological fundamentals with current requirements from practice and research.

The following aspects are covered in particular:

- In-depth examination of the CAP theorem, taking into account real distributed database systems.
- Systematic selection of suitable database management systems (DBMS) on the basis of concrete application scenarios. This includes both relational (e.g. PostgreSQL, MySQL, SQL Server, Oracle) and non-relational systems (e.g. MongoDB, Redis, Riak).
- Use of a data modelling tool (e.g. erwin Data Modeler) to create conceptual and physical data models.
- Use and evaluation of monitoring and performance tools, in particular with regard to load distribution, system monitoring and analysis of query execution plans.
- Investigating different fragmentation strategies for the efficient storage and management of large amounts of data in distributed database systems.

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Other exam (soP) according to §§ 26, 27 APO

Examination - length/format
Portfolio

The concrete length/format of the examination will be determined in the study plan.

Language of examination
German

Condition for the award of credit points
None

Learning outcomes

- Students recognise basic concepts, terms and architectures of relational database systems.
- Students understand the structure and functionality of various database management systems (DBMS).
- Students apply relational modelling techniques to create conceptual data models (e.g. ER diagrams).
- Students analyse requirements for database systems in order to select suitable technical solutions.
- Students evaluate simple database designs with regard to freedom from redundancy, normalisation and performance.
- Students create relational database schemas using suitable modelling and implementation tools.

Literature

Kofler, Michael: Datenbanksysteme - Das umfassende Lehrbuch; 2nd edition; Rheinwerk Verlag; Bonn, 2024
Heuer, Andreas; Saake, Gunter: Databases - Concepts and Languages; 6th ed.; MITP-Verlag; Bonn, 2018
Rahm, Saale, Sattler: Distributed and Parallel Data Management; Springer Vieweg; Berlin Heidelberg, 2015

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 5003859
Agentic AI: Enabling Autonomous and Goal-Driven Intelligence

Module profile

Exam number
5003859

Duration
1 semester

Frequency
Every summer semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar

Language of instruction
English

Organisation

Responsible lecturer
Prof. Dr. Frank-Michael Schleif

Lecturer(s)
Manikanda Kumar

Applicability	BIN, BWI, BEC, BISD
Semester according to SPO	6. semester
Type of module	FWPM

Required prerequisites for the participation in the module according to the SPO
none

Recommended prerequisites for the participation in the module
Python programming, Fundamentals of AI/ML.

Content
This course is designed to introduce next-generation AI systems capable of autonomous decision-making, planning, reasoning, and self-improvement to students. Unlike traditional reactive AI models, Agentic AI systems can initiate actions, perform multi-step tasks, collaborate with other agents, and adapt to dynamic environments. This course equips learners with both theoretical foundations and hands-on experience in building autonomous AI agents.
The learners will explore agent architectures, cognitive models, memory systems, tool-use capabilities, multi-agent collaboration frameworks, and practical agent deployment workflows. Through lab exercises using modern frameworks such as Flowise, LangChain, AutoGen Studio, CrewAI, and AgentOps, students will build goal-driven agents, evaluators, planners, and multi-agent systems. Real-world applications from business automation, sustainability, smart systems, and software engineering will be emphasised throughout.
The course ends with a practical assessment where participants design, implement, and demonstrate a functional autonomous agent. By integrating theory, hands-on experimentation, and evaluation, this course provides a strong foundation for applying Agentic AI in academic, industrial, and research environments aligned with the green digital transformation.

1 Foundations of Agentic AI
Agentic AI - Autonomous AI vs Traditional AI - Agent lifecycle and capabilities - Types of autonomy in AI systems - Rule-based agents vs LLM-driven agents - Real-world examples of agents - maturity levels of autonomous systems - Application domains aligned to sustainability & green digital transition.
Interactive brainstorming: Where can agents be used in business?
2. agent architectures, memory, and planning
Cognitive architecture: perception, reasoning, memory, action - Memory systems in agents: short-term memory, episodic memory, vector-store memory, long-term memory - Planning systems: task decomposition, tree of thought, planner-executor architecture - Tool-calling & API integration - Evaluator-planner loops - Safety layers & guardrails.
3. building autonomous agents and tool-using systems

Agent capabilities: tool-use, retrieval augmentation, action loops - Safety, guardrails, and constraints, Using frameworks: LangChain Agents, AutoGen Studio, CrewAI worker-manager roles - Hands-on use cases: Research automation agents - Business workflow agents.

4. multi-agent systems, collaborations, and workflows

Multi-agent systems: roles & communication, Manager-worker architecture, Planner-agent-reviewer loops, Collaboration strategies: parallel, sequential, cooperative, Real-world MAS applications (smart grids, supply chain, robotics)

5. deployment, monitoring, ethics

Deployment workflows (local, cloud) - Logging, monitoring, and evaluation of agents - Safety, ethical issues & governance of autonomous systems - Responsible AI principles for autonomous systems - Real-world challenges: hallucination, error handling, misuse.

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Other exam (soP) according to §§ 26, 27 APO

Examination - length/format
Practical study achievement

The concrete length/format of the examination will be determined in the study plan.

Language of examination
English

Condition for the award of credit points
None

Learning outcomes
1. understand and explain the principles, architecture, and lifecycle of Agentic AI systems and compare them with traditional AI models.
2. design and implement autonomous agents using modern frameworks with capabilities such as planning, memory, tool-use, and reasoning.
3. evaluate and deploy single-agent and multi-agent systems for real-world applications related to sustainability, automation, and intelligent digital ecosystems.

Literature
Text Books:
Martin Ford "Architects of Intelligence: The truth about AI from the people building it" 2018.
Stuart J. Russell, Peter Norvig, "Artificial Intelligence: A Modern Approach", Prentice Hall Series in Artificial Intelligence, 2009
Reference Books:
Kence Anderson, "Designing Autonomous AI: A Guide for Machine Teaching", O'Reilly Media, Inc., 2022

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 6322190
Augmented Reality

Module profile

Exam number
6322190

Duration
1 semester

Frequency
Every summer semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar-style instruction, Exercise

Language of instruction
German

Organisation

Responsible lecturer
Stefan Sauer

Lecturer(s)
Stefan Sauer

Applicability	BEC, BIN, BWI, BISD, BDGD
Semester according to SPO	6. semester
Type of module	FWPM

Required prerequisites for the participation in the module according to the SPO
none

Recommended prerequisites for the participation in the module
none

Content
The event is organised by the Faculty of Polymer Engineering and Surveying (FKV):
(https://geo.thws.de/studium/bachelor-geovisualisierung/studienablauf/modulhandbuch-bgv-ab-ws-202223/)

For scheduling see: https://geo.thws.de/studium/aktuelle-lehrveranstaltungsplaene/

Augmented and mixed reality and their applications
- Realisation of marker-based applications
- Realisation of image-based applications
- Realisation of LBS applications

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Other exam (soP) according to §§ 26, 27 APO

Examination - length/format
Portfolio

The concrete length/format of the examination will be determined in the study plan.

Language of examination
German

Condition for the award of credit points
None

Learning outcomes
1. students know the basic concepts of augmented reality (AR) and mixed reality (MR) and their areas of application.
2. students understand the differences between marker-based, image-based and location-based applications (LBS) in AR technology.
3. students use appropriate services to plan and realise AR applications.
4. students analyse requirements and possible uses for AR applications in relation to various content-based approaches.
5. students evaluate the effectiveness of different techniques for visualising content relative to spatial objects and markers.
6. students independently create AR applications that are both marker-based and image-based and can successfully publish them.
7. understand concepts for integrating AR applications into existing systems and services.

Literature
Dörner, R.; Broll, W.; Grimm, P.; Jung, B.: Virtual and Augmented Reality (VR/AR): Fundamentals and Methods of Virtual and Augmented Reality. 2nd edition, Springer-Verlag Berlin, Heidelberg, 2019. ISBN 978-3-662-58860-4.
Vetter, M. & Olberding, H.: E-learning material on geovisualisation, [online] smart.vhb.org, 2019/2020.

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 5003836
BSI BCM Practitioner and BSI Incident Practitioner

Module profile

Exam number
5003836

Duration
1 semester

Frequency
Every summer semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar

Language of instruction
German

Organisation

Responsible lecturer
Prof. Dr. Alexander Schinner

Lecturer(s)
Liane Kiesewalter,
Tobias Kasch

Applicability	BIN, BWI, BEC, BISD, BDGD
Semester according to SPO	6. semester
Type of module	FWPM

Required prerequisites for the participation in the module according to the SPO
none

Recommended prerequisites for the participation in the module
none

Content
BCM practitioner
- Introduction to BCM
- BCM process and stage model
- Standards and regulatory principles
- Initiation, planning and set-up
- Structure and empowerment of the BAO
- BIA pre-filter and BIA
- Risk analysis
- Emergency planning (BC strategies, CFPs and WAPs)
- Practising and testing
- Performance review and key figures

Incident practitioner
- Introduction to the cyber security network including framework conditions for digital first responders, incident practitioners and incident experts
- Summary of the content of the basic course
- Behaviour on the phone incl. non-technical measures
- Threats and forms of attack and overview of the current threat situation
- Sequence of standard procedures
- Handling of IT security incidents
- Remote support
- Incident handling for IT systems "away from the usual office environment"
- "After the incident is before the incident" preventive measures

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Other exam (soP) according to §§ 26, 27 APO

Examination - length/format
Portfolio

The concrete length/format of the examination will be determined in the study plan.

Language of examination
German

Condition for the award of credit points
None

Learning outcomes

- Teaching the BCMS process in accordance with BSI Standard 200-4 with practical relevance
- Effective detection, analysis and management of security incidents in accordance with BSI standards
- Preparation for the relevant BSI audits as part of the cyber security network (CSN)

Literature
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/Schulungen-zum-BCM-Praktiker/Schulungen_zum_BCM_Praktiker_node.html
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber-Sicherheitsnetzwerk/Qualifizierung/Vorfall_Praktiker/Vorfall_Praktiker.html

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 5003816
Behavioural Pricing

Module profile

Exam number
5003816

Duration
1 semester

Frequency
Every summer semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar

Language of instruction
German

Organisation

Responsible lecturer
Prof. Dr. Tobias Aubele

Lecturer(s)
Juliane Richter

Applicability	BEC, BWI, BISD, BDGD
Semester according to SPO	6. semester
Type of module	FWPM

Required prerequisites for the participation in the module according to the SPO
none

Recommended prerequisites for the participation in the module
none

Content
Students learn about the influence of prices on consumer behaviour from a psychological perspective. They understand the intrapersonal processes of perception, evaluation and storage of price information and can apply price psychological effects themselves.

Contents:
Basics of price management
- Introduction to the price management process
- Basic models of business price theory
- Starting points for price determination

Introduction to behavioural pricing
- Behavioural pricing as a branch of behavioural economics
- Psychological processes and constructs for processing price information
- Behavioural science theories on price perception, assessment and storage

Behavioural pricing in practice
- Design of price information from the supplier's perspective
- Price psychological effects and application examples
- Use of behavioural pricing in various industries

Possibilities and limitations of (behavioural) pricing
- Empirical price research
- Innovative (digital) pricing approaches from a practical and theoretical perspective
- Ethical and legal aspects of (behavioural) pricing

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Written exam (sP) according to § 23 APO

Examination - length/format
90 minutes

The concrete length/format of the examination will be determined in the study plan.

Language of examination
German

Condition for the award of credit points
None

Learning outcomes
General learning objectives:
You are familiar with the methodological and ethical aspects of pricing and can assess pricing approaches from a business and behavioural economics perspective

Sub-objectives:
1. students understand the behavioural pricing approach and know the theoretical principles of the psychological effect of price information.
a. Professional competence: Students know the basics of behavioural pricing management. They understand the psychological effect of price information in different phases of the purchasing process.
b. Problem-solving and assessment skills: Students understand the approach of behavioural pricing as a sub-discipline of behavioural economics and how it differs from classical price theory.
c. Methodological competence: Students practise interpreting behavioural and psychological models and applying them to price management.
d. Communication skills: Students are able to discuss the concepts and models presented in the lecture in a precise and technically correct manner.
e. Self-competence: Students can deepen their knowledge independently with specific specialised articles.

2. students can apply price psychological effects themselves and are familiar with various areas of application.
a. Professional competence: Students understand the influence of different pricing parameters on price perception and consumer behaviour.
b. Problem-solving and assessment skills: Students can assess price-psychological measures in different contexts and explain them on the basis of the relevant theory. They can independently derive suitable price-psychological measures and apply them to specific practical cases.
c. Methodological competence: Students are able to transfer the effects demonstrated in the lecture to price-related issues in practice.
d. Communication skills: Students are able to contribute to discussions on price-psychological measures and present their own approaches. In doing so, they communicate precisely, effectively and correctly using technical language.
e. Social competence: Students work together effectively in a team as part of a practical case.
f. Self-competence: Students work independently, creatively and use feedback for their personal development.

3. students are familiar with the business principles of pricing policy.
a. Professional competence: Students understand the significance and decision-making areas of pricing policy. They are familiar with the classic concepts of pricing theory and the starting points for determining prices.

b. Problem-solving and judgement skills: Students can correctly classify the concepts and approaches of price management and apply them to case studies.
c. Methodological competence: Students know empirical methods for price determination, understand their challenges and can apply selected survey methods themselves.
d. Self-competence: Students are able to expand on the fundamentals covered by studying the literature independently.

4. students critically analyse current trends in price management and innovative, digital pricing approaches.

Literature

Beck, H. (2014). Behavioural Economics - An introduction (focus on chapters 1, 4-6). Wiesbaden: Springer Gabler.
Diller, H., Müller, S., Ivens, B., & Beinert, M. (2021). Pricing: Principles and processes of corporate pricing policy. Stuttgart: Kohlhammer.
Holzwarth et al (2020). Applying behavioural science to health and financial decisions. In: Behavioural Economics Guide 2020.
Kopetzky, M. (2015). Price psychology: four steps to optimised pricing. Wiesbaden: Springer Gabler.
Krämer, A. (2020). Dynamic and individual prices from a company and consumer perspective. In R. Kalka & A. Krämer (Eds.), Price communication. Wiesbaden: Springer Gabler.
Mazumdar, T., Raj, S. P., & Sinha, I. (2005). Reference price research: Review and propositions. Journal of Marketing, 69(4), 84-102.
Meehan, B., Rosenberg, S., & Duke, C. (2018). How to double savings rates: A case study for nudging for good. In: Behavioural Economics Guide 2018.
Pechtl, H. (2014). Price policy: Behavioural pricing and pricing systems. Constance: UVK Verlagsgesellschaft mbH.
Pechtl, H. (2004). The price knowledge of consumers: a theoretical-conceptual analysis (No. 01/2004). Economic Discussion Papers.
Simon, H. (2015). Confessions of the pricing man. Wiesbaden: Springer Gabler.
Simon, H. & Fassnacht, M. (2016). Price management: strategy - analysis - decision - implementation. Wiesbaden: Springer Gabler.

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 100000
Business Intelligence and Reporting

Module profile

Exam number
100000

Duration
1 semester

Frequency
Every summer semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 0 hrs

Self-study: 150 hrs

Total: 150 hrs

Teaching format
Lecture

Language of instruction
German

Organisation

Responsible lecturer
Prof. Dr. Frank-Michael Schleif

Lecturer(s)

Applicability	BIN, BWI, BISD, BDGD
Semester according to SPO	6. semester
Type of module	FWPM

Required prerequisites for the participation in the module according to the SPO
This is an offer of the Virtual University of Bavaria. Further information can be found at https://kurse.vhb.org/VHBPORTAL/kursprogramm/kursprogramm.jsp?kDetail=true&COURSEID=20177,83,1508,1

Recommended prerequisites for the participation in the module
This is an offer of the Virtual University of Bavaria. Further information can be found at https://kurse.vhb.org/VHBPORTAL/kursprogramm/kursprogramm.jsp?kDetail=true&COURSEID=20177,83,1508,1

Content
This is an offer of the Virtual University of Bavaria. Further information can be found at https://kurse.vhb.org/VHBPORTAL/kursprogramm/kursprogramm.jsp?kDetail=true&COURSEID=20177,83,1508,1

The module is mandatory for students of the specialisation: << Business Technology >> in BWI
and is used as a substitute for the module BI specialisation I. For the participants of the BI specialisation
will also be offered 2-3 course parts by Prof. Schleif at SHL in summer semester 2025, especially on BI topics
and supplemented by an enrichment lecture. Please also refer to the timetable.

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Written exam (sP) according to § 23 APO

Examination - length/format
90 minutes

The concrete length/format of the examination will be determined in the study plan.

Language of examination
German

Condition for the award of credit points
None

Learning outcomes
This is an offer of the Virtual University of Bavaria. Further information can be found at https://kurse.vhb.org/VHBPORTAL/kursprogramm/kursprogramm.jsp?kDetail=true&COURSEID=20177,83,1508,1

Literature
This is an offer of the Virtual University of Bavaria. Further information can be found at https://kurse.vhb.org/VHBPORTAL/kursprogramm/kursprogramm.jsp?kDetail=true&COURSEID=20177,83,1508,1

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 5003856
CANVA – Branding with AI

Module profile

Exam number
5003856

Duration
1 semester

Frequency
Irregular

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar

Language of instruction
German

Organisation

Responsible lecturer
Prof. Dr. Christina Völkl-Wolf

Lecturer(s)
Verena Rempel

Applicability	BWI, BEC, BISD, BDGD
Semester according to SPO	6. semester
Type of module	FWPM

Required prerequisites for the participation in the module according to the SPO
none

Recommended prerequisites for the participation in the module
Own laptop, installation of the Pro version/test access to the CANVA programme.

Content
1. corporate identity - strategic
Understanding the terms
CI, CD, brand
Best practice examples from different industries, analysis of international brands
Positioning, brand values
Mission & vision
Identity models (e.g. Golden Circle)
Target group profile (e.g. persona)
Brand personality (mood board, archetype)
Tonality and language style

2.corporate design - visual
Derive a design system
From brand essence to visual system (design with Canva)
Logo
Colour scheme
Typography
Visual language
Layout principles (grid, white space, composition)

3. branding of a brand
Creation of social media content for the brand
Colour management and colour effect
Fonts and font design
Photo editing, graphics
Video, reels, stories

Development of a brand cosmos:
Creation of digital media and print media such as website, social media content, audio-visual content, business cards, etc.

Usage scenarios / application:
Self-employment/freelancing: A consistent CD helps with professional external image and differentiation.
Application folder/portfolio: Your own branding as a "common thread" creates recognition and demonstrates strategic thinking.

Start-ups & student initiatives: A clear brand identity simplifies communication, fundraising and community building.
Agency work: CI/CD expertise is a key qualification for strategic design processes on behalf of clients.
Research & science: Scientific projects also benefit from a coherent, comprehensible image.

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
none

Examination - type
Other exam (soP) according to §§ 26, 27 APO

Examination - length/format
Portfolio

The concrete length/format of the examination will be determined in the study plan.

Language of examination
German

Condition for the award of credit points
none

Learning outcomes
The students develop a complete corporate identity and corporate design
Concept for a real own project or a fictitious project / start-up including visual realisation with the help of Canva and AI applications. The aim is to design a consistent, professional brand image for a later real application. Confident use of CANVA as design software is a prerequisite.

Students will recognise key concepts of corporate identity and corporate design.
Students understand the importance of strategic brand management for digital communication media.
Students analyse CI/CD systems with regard to target groups, differentiation and use of media.
Students evaluate design solutions in the context of user experience, media formats and communication goals.
Students apply the content they have learnt and create a complete corporate identity concept including a cross-media design system for their own or a fictitious project.

Literature
https://www.canva.com/de_de/

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 5003823
Computer Networks and Cyber Security

Module profile

Exam number
5003823

Duration
1 semester

Frequency
Every summer semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar

Language of instruction
English

Organisation

Responsible lecturer
Prof. Dr.-Ing. Sebastian Biedermann

Lecturer(s)
Siavosh Haghighi Movahed

Applicability	BIN, BWI, BISD
Semester according to SPO	6. semester
Type of module	FWPM

Required prerequisites for the participation in the module according to the SPO
none

Recommended prerequisites for the participation in the module
none

Content
This module is designed to provide students with the knowledge and skills necessary to design, implement, and manage secure computer networks.
In this module, students will gain a solid foundation in establishing and maintaining robust network infrastructures. Simultaneously, the module addresses the critical aspect of securing these networks against potential threats, ranging from cyberattacks to data breaches. Through a combination of theoretical concepts and practical exercises, students will develop the expertise needed to identify vulnerabilities, implement security measures, and formulate strategies to safeguard information assets in the interconnected world of computer networks. In addition to providing a broad range of fundamental computer networking and security knowledge for all IT careers, this module will also provide students with an opportunity to further self-study and gain conceptual knowledge and practical skills required for 200-301 Cisco® Certified Network Associate (CCNA®) exam.

Indicative content:
- Fundamentals of enterprise campus network design
- Network protocols and models
- Fundamentals of IP routing and switching
- IP addressing (IPv4/IPv6)
- Network security concepts and principals
- Configure and verify secure Inter-switch connectivity
- Implementing, optimising, and securing switched networks
- Implementing secure device access and access control systems
- Define key security concepts (threats, vulnerabilities, exploits, and mitigation techniques)
- Firewall Technologies

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Written exam (sP) according to § 23 APO

Examination - length/format
90 minutes

The concrete length/format of the examination will be determined in the study plan.

Language of examination
English

Condition for the award of credit points
None

Learning outcomes
By engaging successfully with this module, students will be able to:
1. Explain the fundamentals of computer network and cyber security.
2. design, implement, configure, and troubleshoot high available secure scalable network infrastructures.
3. implement network security and access control solutions using routers, switches, and firewalls.
4. explain how vulnerabilities, threats, and exploits can be mitigated to enhance network security.

Literature
1. the students know the fundamentals of computer networks and cyber security principles.
2. the students understand the importance of securing network infrastructures against potential threats and vulnerabilities.
3. the students apply best practices in designing, implementing, configuring, and troubleshooting high-availability, secure, and scalable network infrastructures.
4. the students understand how threats and exploits can undermine network security and identify measures to mitigate these risks.
5. the students evaluate network security solutions, including access control measures implemented through routers, switches, and firewalls.
6. the students create comprehensive strategies to secure information assets and maintain robust network infrastructures based on theoretical knowledge and practical exercises.
7. the students develop the practical skills needed to prepare for the 200-301 Cisco® Certified Network Associate (CCNA®) exam, applying their learning to real-world scenarios.

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 5003861
Computer Networks for Practical Engineers

Module profile

Exam number
5003861

Duration
1 semester

Frequency
Irregular

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar

Language of instruction
English

Organisation

Responsible lecturer
Prof. Dr. Rolf Schillinger

Lecturer(s)
Bishnu Prasad Gautam

Applicability	BIN, BWI, BEC, BISD, BDGD
Semester according to SPO	6. semester
Type of module	FWPM

Required prerequisites for the participation in the module according to the SPO
none

Recommended prerequisites for the participation in the module
none

Content
This course provides students with practical knowledge and skills in computer networks, focusing on how networks are constructed, configured, and operated by computer network engineers. The course begins at the physical layer with hands-on construction of LAN (Ethernet) cables, and then introduces fundamental concepts such as classful and classless IP addressing, switching, and routing.
Students will learn static routing as a foundation, followed by dynamic routing protocols including RIP, OSPF, and BGP through practical laboratory exercises. The course also introduces essential network security concepts, with particular attention to firewalls and basic network protection mechanisms required in real network environments.
In the final part of the course, students are introduced to next-generation networking paradigms, such as IoT, Software-Defined Networking (SDN), and Quantum Networks, providing insight into future network evolution. In addition to delivering a broad foundation in computer networking for IT and engineering careers, this course also supports self-study towards the 200-301 Cisco Certified Network Associate (CCNA) exam by developing relevant conceptual understanding and practical skills.

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Written exam (sP) according to § 23 APO

Examination - length/format
90 minutes

The concrete length/format of the examination will be determined in the study plan.

Language of examination
English

Condition for the award of credit points
None

Learning outcomes

- The students understand the fundamentals of computer networking, including LAN construction, network components, and basic communication principles used in modern information systems.
- The students apply IP addressing, VLAN configuration, and routing concepts to design and configure small- to medium-scale networks using both static and dynamic routing methods.
- The students analyse and compare dynamic routing protocols such as RIP, OSPF, and BGP, and explain their operational principles, use cases, and performance characteristics.
- The students design and implement practical network topologies by integrating routers, switches, and end devices, and verify connectivity through hands-on configuration and testing.
- The students understand emerging and future network systems, including IoT, Software-Defined Networking (SDN), and quantum networks, and evaluate their potential impact on security, scalability, and next-generation communication infrastructures.

Literature
Will be provided at start of module.

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 5003817
Computer Vision: Artificial Intelligence Applied

Module profile

Exam number
5003817

Duration
1 semester

Frequency
Every summer semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar

Language of instruction
English

Organisation

Responsible lecturer
Prof. Dr.-Ing. Pascal Meißner

Lecturer(s)
Prof. Dr.-Ing. Pascal Meißner

Applicability	BIN, BWI, BISD
Semester according to SPO	6. semester
Type of module	FWPM

Required prerequisites for the participation in the module according to the SPO
None

Recommended prerequisites for the participation in the module
None

Content
Have you ever wondered how self-service checkouts scan items, self-driving cars recognise pedestrians, computers detect skin cancer, and 3D models of iconic places like the Colosseum are scanned?

This module aims to answer these questions and many more by

- Giving an overview of the problems and approaches in computer vision, for applications as diverse as automation, robotics, medical imaging, and photogrammetry.
- Introducing the fundamentals of neural networks, required for constructing artificial systems with human-level perception capabilities.

The module spans from selecting the appropriate equipment for visual inspection tasks to image classification with convolutional neural networks and image retrieval with bag-of-visual-words models. The topics covered are:

01. introduction - nomenclature, history, state of the art, module logistics
02. image acquisition & digitisation - image sensors & representations, A/D conversion, Fourier transform
03. image enhancement - point operations, contrast adjustment, smoothing filters
04. feature extraction - edge detection, detection and description of local features
05 Segmentation and Morphology - Region growing, Hough transform, morphology operators
06. camera modelling - 3-D transformations, pinhole camera model, camera calibration
07. stereo vision - epipolar geometry, correlation methods, triangulation
08 Classification - Classifier evaluation, generalisation, nearest-neighbor, decision trees
09. ensemble methods - boosting and bagging, random forests, AdaBoost
10. neural networks - multi-layer perceptron, gradient descent, backpropagation

11. convolutional neural networks - Convolution and pooling layers, example architectures
12. bag-of-visual words - K-means clustering, TF-IDF, histogram comparison

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Other exam (soP) according to §§ 26, 27 APO

Examination - length/format
Colloquium

The concrete length/format of the examination will be determined in the study plan.

Language of examination
English

Condition for the award of credit points
None

Learning outcomes
By the end of the module, students should be able to:

- Select appropriate camera systems and convert image representations, as well as discuss causes and avoidance of aliasing
- Implement and apply smoothing and morphology operators, edge detectors, and segmentation techniques
- Differentiate between contrast adjustment methods and compare the various approaches to detect and describe local features
- Determine and compute rigid body transformations. Specify camera models and project image and scene points.
- Determine epipolar geometries and lines. Calculate and discuss different correlation methods
- Assess and implement the various techniques for visualising and cleaning data for training classifiers
- Apply feature engineering and selection to classification tasks
- Differentiate between the quantities in the bias-variance problem and apply it to classifiers
- Assess, implement, and train neural networks and discuss their application to vision tasks

This module will be taught in English and delivered online and on campus. All sessions will be recorded. Colloquia can be done in English or German.

Literature

- Digital Image Processing, Rafael C. Gonzalez and Richard E. Woods, 4th ed. Pearson, 978-0133356724, 2017
- Learning OpenCV 3: Computer Vision in C++ with the OpenCV Library, Adrian Kaehler and Gary Bradski, O'Reilly Media, 978-1491937990, 2017
- Introduction to Machine Learning, Ethem Alpaydin, 4th ed. MIT Press, 978-0262043793, 2020

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 5003862
Data Analytics

Module profile

Exam number
5003862

Duration
1 semester

Frequency
Irregular

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar

Language of instruction
English

Organisation

Responsible lecturer
Prof. Dr. Tobias Aubele

Lecturer(s)
Dr. Jaani Väisänen

Applicability	BIN, BWI, BEC, BISD, BDGD
Semester according to SPO	6. semester
Type of module	FWPM

Required prerequisites for the participation in the module according to the SPO
none

Recommended prerequisites for the participation in the module
No coding required. Install Altair AI Studio before the course; a university student licence is available via https://web.altair.com/altair-student-edition.

Content
This course gives business students a practical, no coding introduction to data analytics using Altair AI Studio. You'll learn to build an end to end analytics workflow-from importing and preparing data to selecting variables, building models, evaluating performance, and interpreting results for business decisions.

- Course kickoff, AI Studio workflow basics, and practical data preparation for modelling
- Regression

o Concept: what regression explains
o Hands on workflow: build a regression model in AI Studio
o Validation and model goodness: simple train/validation/test incorporating key fit metrics

- Clustering

o Concept: grouping similar cases
o Hands on workflow: prepare data and create clusters in AI Studio
o Validation and model goodness: choosing a useful number of clusters for the business question

- Tree models

o Concept: classification and interpretable drivers
o Hands on workflow: build and read a decision tree in AI Studio
o Validation and model goodness: cross validation and practical classification metrics

- Association analysis:

o Concept: co-occurrence and recommendations
o Hands on workflow: create association rulesets in AI Studio
o Validation and model goodness: support, confidence, and lift

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Other exam (soP) according to §§ 26, 27 APO

Examination - length/format
Portfolio

The concrete length/format of the examination will be determined in the study plan.

Language of examination
English

Condition for the award of credit points
None

Learning outcomes
Upon successful completion of this course, students will be able to:
1. construct end-to-end analytics workflows (Apply/Create): Independently design and execute complete data mining processes within Altair AI Studio-from data import and cleansing to model generation-without relying on programming code.
2. analyse and select Appropriate Methodologies (Analyze): Diagnose specific business problems to determine the most suitable analytical technique (Regression, Clustering, Decision Trees, or Association Analysis) based on the structure of the data and the desired business outcome.
3. evaluate model performance and robustness (Evaluate): Critically assess the quality of analytical models by interpreting quantitative validation metrics (such as R^2, Lift, Confidence, and Cross-Validation scores) to distinguish between statistical noise and reliable patterns.
4. synthesise data into business strategy (Create): Translate technical model outputs into actionable business insights and formulate data-driven strategic recommendations for management.

Literature
will be specified in the lecture.

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 5003135
Design Thinking & Innovation

Module profile

Exam number
5003135

Duration
1 semester

Frequency
Every summer semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar

Language of instruction
German

Organisation

Responsible lecturer
Prof. Dr. Michael Müßig

Lecturer(s)
Lisa Straub

Applicability	BEC, BIN, BWI, BDGD, BISD
Semester according to SPO	6. semester
Type of module	FWPM

Required prerequisites for the participation in the module according to the SPO
none

Recommended prerequisites for the participation in the module
- Interest in creative but challenging problem-solving approaches
- Entrepreneurial thinking
- Willingness to rigorously put your own ideas to the test

Content
In this course, the basic principles and background of innovation management and especially design thinking are explained and illustrated with clear examples. It is particularly important to convey to the participants that today's innovation processes place people at the centre and attempt to harmonise their customer needs with technical feasibility and economic efficiency. The students are given the first tools to organise and carry out simple design thinking innovation processes independently.
They need to understand which basic elements an innovation or design thinking process is based on and how these can be skilfully run through exercises. This makes it clear in a practical way what differences there are to the classic development process and what advantages a customer-centred approach offers, but also what disadvantages are associated with the DT approach.
The course is divided into two main modules:
1. a brief introduction to innovation management
Participants will gain an insight into common innovation models and processes, as well as the background and basic concepts of innovation research.
2. learning and going through Design Thinking yourself
Design Thinking is based on an iterative, customer-centred and playful problem-solving process that makes it possible to think outside the box in order to realise or strive for the previously unconsidered, seemingly impossible, possibly illogical and unattainable. In the course of this course, participants will go through a design thinking process and develop their own ideas as a project. The course is therefore designed to be interactive, which is why a high degree of proactive participation is expected. In return, participants can expect a course full of creativity, interesting discussions and crazy ideas.

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Other exam (soP) according to §§ 26, 27 APO

Examination - length/format
Portfolio, Presentation

The concrete length/format of the examination will be determined in the study plan.

Language of examination
German

Condition for the award of credit points
None

Learning outcomes
1. students know the basic components of the design thinking process and can name them.
2. students understand the role of design thinking in the context of other innovation models and processes and can categorise them.
3. students apply methods of effective problem definition to identify relevant challenges in the innovation process.
4. students analyse the basics of user studies in the design thinking process and can explain their significance for solution development.
5. students evaluate innovation-relevant assumptions and hypotheses in order to be able to (de)construct them effectively.
6. students organise and conduct brainstorming sessions to generate creative ideas.
7. students create prototyping processes, describe them conceptually and can explain their practical application.

Literature
Wobser, Gunther (2022): Agile innovation management: overcoming dilemmas, mastering ambidexterity and achieving long-term success with innovations. Springer Gabler. 978-3662645147
Hasso Plattner Institute (A): What is Design Thinking. https://hpi-academy.de/en/design- thin- king/what-is-design-thinking.html.
Hasso Plattner Institute (B): The six steps in the Design Thinking innovation process. https://hpi.de/school-of-design-thinking/design-thinking/hintergrund/design-thinking- process.html.
Ideo: Design Thinking. https://designthinking.ideo.com/?page_id=1542.
d.School: An Introduction to Design Thinking. PROCESS GUIDE. Institute of Design at Stanford. https://dschool-old.stanford.edu/sandbox/groups/designresources/wiki/36873/ attach- ments/74b3d/ModeGuideBOOTCAMP2010L.pdf.
Brown, Tim (2009): Change by Design. How Design Thinking Transforms Organisations and Inspires Motivation. 1st edition. Harper Business. 978-006176608-4.
Lewrick, Michael; Link, Patrick; Larry, Leifer (2017): The Design Thinking Playbook. With traditional, current and future success factors. Verlag Franz Vahlen GmbH. 978-3039097050.
Uebernickel, Falk; Brenner, Walter; Pukall, Britta; Naef, Therese; Schindholzer, Bernhard (2015): Design Thinking. The handbook. 1st edition. Frankfurter Allgemeine Buch. 978-3956010651.
Wobser, Gunther: Reinventing yourself: What SMEs can learn from Silicon Valley. BESHU BOOKS. 978-3982195025

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 6810300
IT Forensics

Module profile

Exam number
6810300

Duration
1 semester

Frequency
Every summer semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar-style instruction

Language of instruction
German

Organisation

Responsible lecturer
Prof. Dr. Alexander Schinner

Lecturer(s)
Prof. Dr. Alexander Schinner,
Jan Starke

Applicability	BISD
Semester according to SPO	6. semester
Type of module	Compulsory module

Required prerequisites for the participation in the module according to the SPO
none

Recommended prerequisites for the participation in the module
none

Content
Basics of forensics
o Introduction to digital forensics and its significance
o Legal framework and ethical considerations
Collection of evidence
o Fundamentals and best practices of evidence handling
o Chain of custody: traceability and integrity of evidence
o Live response: first steps and collection of volatile data
Data carrier forensics
o Analysing file systems and hidden data
o Recovery of deleted files and partitions
Network forensics
o Monitoring and analysing network protocols
o Anomaly detection and traffic analyses
Memory forensics
o Techniques for collecting and analysing volatile memory data
o Tools and frameworks for working with RAM images
Artefact analysis
o Identification and analysis of digital artefacts
o Timestamp and metadata analysis
Reversing
o Introduction to reverse engineering and analysis methods
o Techniques such as sandboxing, static analysis and deobfuscation
Phishing analysis
o Basics of phishing prevention and detection
o Analysing mail headers and phishing URLs
OSINT (Open Source Intelligence)
o Overview and legal aspects of open sources
o Tools such as Virustotal, Shodan, and additionally Maltego
Hunting
o Introduction to threat hunting
o Use of YARA rules, EDR systems and tools such as Velociraptor and Sigma rules
Threat intelligence
o Basics of threat analysis and intelligence lifecycle
o Mitre ATT&CK framework and TLP protocol for classification
Reporting and documentation
o Structure and creation of a professional report

o Communication and presentation of results for different target groups

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Other exam (soP) according to §§ 26, 27 APO

Examination - length/format
Portfolio

The concrete length/format of the examination will be determined in the study plan.

Language of examination
German

Condition for the award of credit points
None

Learning outcomes
After completing the module, students will be able to

- describe the structure and process of the Business Continuity Management System (BCMS) in accordance with BSI Standard 200-4 and apply it in practice.
- systematically carry out the individual phases of the BCM stage model (e.g. initiation, BIA, risk analysis, emergency planning, testing).
- name regulatory and normative principles of BCM and explain their relevance for implementation in organisations.
- carry out a business impact analysis (BIA) and derive suitable business continuation and recovery plans (CFPs, WAPs) from this.
- identify and interpret suitable key figures for evaluating the effectiveness of BCM measures.
- explain the structure and objectives of the BSI Cyber Security Network (CSN) and differentiate between the roles of digital first responders, incident practitioners and incident experts.
- recognise and analyse typical IT security incidents and handle them according to standardised procedures.
- take non-technical immediate measures in initial contact with those affected and conduct conversations about IT security incidents in a structured and empathetic manner (e.g. on the phone).
- record and prioritise security-relevant information in the event of incidents and prepare it for further analysis - even in non-standardised IT environments.
- identify preventive measures to avoid future incidents and integrate them into existing security concepts.
- prepare professionally and methodically for audits and certifications within the framework of the CSN.

Literature
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-undZertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/Schulungen-zum-BCMPraktiker/Schulungen_zum_BCM_Praktiker_node.html
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationenund-Empfehlungen/Cyber-Sicherheitsnetzwerk/Qualifizierung/Vorfall_Praktiker/Vorfall_Praktiker.html

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 5003852
Digital Sovereignty - Operational Concepts and Technologies

Module profile

Exam number
5003852

Duration
1 semester

Frequency
Irregular

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar

Language of instruction
German

Organisation

Responsible lecturer
Prof. Dr.-Ing. Tobias Fertig

Lecturer(s)
Prof. Dr. Michael Müßig,
Prof. Dr.-Ing. Tobias Fertig,
Andreas Schütz

Applicability	BIN, BWI, BEC, BISD, BDGD
Semester according to SPO	6. semester
Type of module	FWPM

Required prerequisites for the participation in the module according to the SPO
None

Recommended prerequisites for the participation in the module
None

Content
The module teaches basic concepts of digital sovereignty with a focus on the operational and technical implementation level.
After an introduction to key terms (e.g. dependencies on platform providers, data sovereignty, vendor lock-in, open source, open standards), specific technical alternatives and tools are considered.

Topics covered include
- Open source software vs. proprietary solutions
- Full stack open source (OS): in e-commerce, IT security, knowledge management, ERPs, ...
- Digital sovereignty at all levels: From hardware to payment flows (PayPal, ApplePay, GooglePay vs. digital euro, GNU Taler, Wero, etc.)
- Cloud alternatives (self-hosting, European cloud providers)
- Open standards and interoperability
- Data protection, encryption and data storage
- Practical examples from administration, education and companies

In the project-oriented part, students work in teams on specific application scenarios (e.g. digital infrastructure of a university, an SME or a municipality).
The aim is to develop realistic technical concepts to improve digital sovereignty.
The results are presented and reflected upon at the end of the semester as part of a transfer conference with a public audience and jury.

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Other exam (soP) according to §§ 26, 27 APO

Examination - length/format
Practical study achievement

The concrete length/format of the examination will be determined in the study plan.

Language of examination
German

Condition for the award of credit points
None

Learning outcomes

- Students can name key terms, players and motivations of digital sovereignty.
- Students can explain how technical dependencies arise through software, cloud services and platforms.
- Students can select suitable open source and open alternative solutions for specific application scenarios.
- Students can analyse existing digital infrastructures with regard to dependencies, risks and sovereignty deficits.
- Students can compare technical solutions in terms of costs, maintainability, security and sustainability.
- Students can design and present an operational concept for improving digital sovereignty for a defined scenario.

Literature

- https://link.springer.com/book/10.1007/978-3-031-69994-8
- https://direct.mit.edu/books/monograph/3504/The-StackOn-Software-and-Sovereignty
- https://link.springer.com/article/10.1007/s44206-024-00146-7

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 5003846
Ethical AI Hacking

Module profile

Exam number
5003846

Duration
1 semester

Frequency
Irregular

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar

Language of instruction
English

Organisation

Responsible lecturer
Prof. Dr. Benjamin Weggenmann

Lecturer(s)
Paulius Baltrušaitis

Applicability	BIN, BWI, BEC, BISD, BDGD
Semester according to SPO	6. semester
Type of module	FWPM

Required prerequisites for the participation in the module according to the SPO
None

Recommended prerequisites for the participation in the module
Python, ML/AI basics

Content
This course provides a comprehensive understanding of Artificial Intelligence (AI) security,
with a focus on ethical hacking principles, attacks on ML models and data, and defence strategies and techniques.

Students will gain theoretical and practical knowledge of key threats such as evasion, model extraction, model inversion, data extraction, data poisoning, backdoor attacks. How to provide attacks for testing purposes and what detection and protection techniques to use and how to use them.

Machine learning models such as Linear Regression, Support Vector Regression, K-Nearest Neighbours, Logistic Regression, Support Vector Machines (SVM), Decision Trees will be used.

Red and blue team scenarios will be used for practical exercises. Each student will play a role on both sides. The course will use several different scenarios for different attacks and machine learning models.

There is an example of a scenario for a red and blue team exercise focused on data poisoning and detection:
The company is developing a machine learning model to predict customer churn. The red team wants to reduce the accuracy of the logistic regression model by poisoning the data with label flipping. The goal of the blue team is to detect and mitigate the attack.
Red team tasks: Analyse the data set, develop the poisoning strategy, execute the attack, document the attack. The success of the red team is measured by the degree to which they degrade the performance of the model.
Blue team tasks: Establish a baseline (train a baseline model and evaluate the model's performance), Implement detection mechanisms - use techniques such as outlier detection (e.g. Isolation Forest), Mitigate the attack, Document the defence. The Blue Team's success is measured by their ability to detect and mitigate the attack and restore the model's performance.
Both teams will be judged on the clarity and thoroughness of their documentation and presentation of their findings to the whole group

of students, showing and commenting on their Python code and explaining their strategies.
Tools for coding: Jupyter Notebook environment for Python (scikit-learn, pandas, numpy, matplotlib, seaborn), e.g. Google Colab.

By the end of the course, students will work in teams to formulate responsible AI security testing methodologies that meet ethical and legal standards. They will discuss and evaluate the ethical implications of AI vulnerabilities and develop a set of ethical guidelines for AI security and ethical hacking.

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Written exam (sP) according to § 23 APO

Examination - length/format
90 minutes

The concrete length/format of the examination will be determined in the study plan.

Language of examination
English

Condition for the award of credit points
None

Learning outcomes
1 Understand basic AI security concepts, ethical hacking principles, and key machine learning threats.
2 Identify and classify AI-specific attacks, including evasion, model extraction, and data poisoning.
3 Simulate red team (attacker) and blue team (defender) AI security scenarios.
4. apply ethical hacking techniques to assess and exploit vulnerabilities in AI models.
5. evaluate AI attack detection and protection strategies to improve security.
6. investigate AI security breaches and analyse countermeasures.
7. develop ethical guidelines for responsible AI security testing and vulnerability disclosure.

Literature
To be clarified during lessons

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 5003863
International Digital Marketing

Module profile

Exam number
5003863

Duration
1 semester

Frequency
Irregular

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar

Language of instruction
English

Organisation

Responsible lecturer
Prof. Dr. Christina Völkl-Wolf

Lecturer(s)
Sami Lanu

Applicability	BIN, BWI, BDGD, BISD
Semester according to SPO	6. semester
Type of module	FWPM

Required prerequisites for the participation in the module according to the SPO
none

Recommended prerequisites for the participation in the module
None

Content
- Digital Marketing Strategies
- Digital marketing channels (owned, earned, paid)
- Search Engine Optimisation
- Digital marketing target group segmentation
- Social media marketing (including TikTok)
- Digital marketing targets, analytics and metrics

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Other exam (soP) according to §§ 26, 27 APO

Examination - length/format
Portfolio

The concrete length/format of the examination will be determined in the study plan.

Language of examination
English

Condition for the award of credit points
None

Learning outcomes
After the module/course students will:
1. remember & understand:
- explain the role of marketing in e-commerce and in digital society.
- describe fundamental concepts of search engine optimisation (SEO).
- outline key digital marketing metrics and analytical tools.

2. apply
- plan and implement digital marketing campaigns at an international level.
- conduct target group segmentation using Meta and Google Ads tools.
- manage social media marketing activities.
- use digital analytics and tracking tools to monitor campaign performance.

3. analyse
- analyse and select appropriate digital marketing channels (owned, earned, and paid media) for different business objectives.
- evaluate campaign results based on relevant performance indicators.

4. evaluate
- assess the effectiveness and efficiency of digital marketing strategies.
- compare and critically evaluate different digital marketing approaches and channels.

5. create
- develop integrated digital marketing strategies for international markets.
- design data-driven optimisation plans for digital marketing campaigns.

Literature
Marketing 4.0 by Philip Kotler etc. (Lecturer will provide pdf's of the needed part of the book)
Digital Marketing Trends 2026 by Brandwatch(Lecturer will provide pdf's of the needed part of the book)
Latest Meta and Google Ads best practices (Lecturer will provide pdf's)

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 5003837
Introduction to Artificial Intelligence

Module profile

Exam number
5003837

Duration
1 semester

Frequency
Every summer semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar

Language of instruction
English

Organisation

Responsible lecturer
Prof. Dr. Andreas Lehrmann

Lecturer(s)
Prof. Dr. Andreas Lehrmann

Applicability	BIN, BWI, BEC, BISD, BDGD
Semester according to SPO	6. semester
Type of module	FWPM

Required prerequisites for the participation in the module according to the SPO
none

Recommended prerequisites for the participation in the module
Basic knowledge in programming (Python) and mathematics (linear algebra, analysis).

Content
Over the last few years, artificial intelligence (AI) has profoundly changed the way we process information and make decisions, both in our personal and professional lives. A thorough understanding of the principles underlying AI is therefore a critical skill in many industries.

This course serves as a broad introduction to AI and its subfields. We are going to discuss - from scratch - the design, training, and operation of an AI system. Motivated by intuitive concepts and visual insights, we are going to introduce a technical framework that allows us to express the fundamental building blocks of an intelligently operating system (e.g., an autonomous robot). Such a system needs to:

- Organise task-dependent data and use this data to make predictions.
- Understand its environment by connecting sensory information to physical location.
- Interact with its environment by planning routes and manipulating objects.

The course will be accompanied by small coding projects in Python that demonstrate the application of these concepts in a series of practical scenarios.

In particular, the course covers the following topics:

[The State of AI] Historical developments, emerging trends, and open questions
[Tools & Techniques] AI-assisted productivity & creativity
[The AI Pipeline] From hard-coded rules to learned decisions
[Data] Collection, representation, and analysis of data
[Hello World] Algebraic, analytical, and statistical foundations of AI
[Supervised Learning I] Data-driven models of reality: classification and regression
[Supervised Learning II] Data-driven models of reality: model complexity and regularisation

[Unsupervised Learning] Finding patterns without annotations
[From Perception to Action I] Visual AI: understanding information in images
[From Perception to Action II] Visual AI: localising information in images
[From Perception to Action III] Embodied AI: manipulating environments
[From Perception to Action IV] Embodied AI: navigating environments
[Guest Lecture] Industrial applications of AI in the automotive industry
[AI & U] Working with and contributing to the future of AI

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Written exam (sP) according to § 23 APO

Examination - length/format
90 minutes

The concrete length/format of the examination will be determined in the study plan.

Language of examination
English

Condition for the award of credit points
None

Learning outcomes

- The students understand the structure of the AI landscape, including its different subfields and how they are connected.
- They can express industry tasks as learning problems (supervised, unsupervised, reinforcement) and select an appropriate AI framework for the type of data at hand.
- They are familiar with the individual components of the selected AI framework - (1) data acquisition and representation; (2) model specification and optimisation; and (3) performance evaluation and analysis - and can set up and execute this pipeline.
- The students understand the role of embodied AI and the challenges and solutions that come with it, such as perception, kinematics, and navigation.

Literature
W. Ertel: Introduction to Artificial Intelligence, Springer, 2024.
C. Bishop: Pattern Recognition and Machine Learning, Springer, 2016.

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 5003069
Mobile Applications

Module profile

Exam number
5003069

Duration
1 semester

Frequency
Every summer semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 50 hrs

Self-study: 100 hrs

Total: 150 hrs

Teaching format
Seminar

Language of instruction
English

Organisation

Responsible lecturer
Prof. Dr. Peter Braun

Lecturer(s)
Prof. Dr. Peter Braun

Applicability	BEC, BIN, BWI, BISD
Semester according to SPO	6. semester
Type of module	FWPM

Required prerequisites for the participation in the module according to the SPO
Good programming skills (e.g. from Programming 1 and 2, Web Programming 1 to 3) or similar.

Recommended prerequisites for the participation in the module
none

Content
This module introduces software development of mobile devices. The Android operating system and/or iOS will be used in the course. The development environment will be Flutter on Android Studio or VS Code. Dart will be used as the programming language. No prior knowledge of Dart programming is expected, but a good understanding of other languages (e.g., Java, Python, or JavaScript) is required.

Introduction to Dart Programming
- Short Overview of Flutter: History, advantages, and architecture.
- Introduction to Dart programming language.
- Setting up the development environment.

Introduction to Flutter - Flutter GUI development
- Understanding widgets and basic UI elements.
- Understanding Stateful and Stateless widgets.
- Layout widgets: Row, Column, Stack, etc.
- Basic interaction elements: Buttons, sliders, and switches.

Navigation and State Management
- Navigation patterns: push/pop navigation, named routes.
- State management basics: setState, Provider.
- Implementing forms and user input handling.

Working with External Data
- Fetching data from the internet (APIs).
- JSON serialisation and deserialisation.
- Firebase

Integrating Device APIs like Location and Camera
- Introduction to Device APIs in Flutter.
- Implementing location services: getting and using GPS data.
- Accessing and using the camera: taking pictures and video recording.
- Permissions handling for location and camera.

Testing Advanced Features and Best Practices

- Animations and transitions.
- Using custom fonts and assets.
- Best practices in Flutter development.
- Testing Flutter Apps

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Other exam (soP) according to §§ 26, 27 APO

Examination - length/format
Portfolio

The concrete length/format of the examination will be determined in the study plan.

Language of examination
English

Condition for the award of credit points
None

Learning outcomes

- The students understand the fundamentals of mobile application development using Flutter for Android and iOS, focusing on professional programming practices.
- The students apply concepts of asynchronous programming and thread management to handle complex tasks in mobile applications efficiently.
- The students analyse architecture concepts for mobile solutions, including the distribution between client and server and communication protocols for mobile devices.
- The students design mobile user interfaces based on reusable software components, ensuring an intuitive and consistent user experience.
- The students implement mobile applications that integrate sensor data evaluation and server communication, following best practices in mobile development.
- The students evaluate different mobile architecture approaches and technologies to choose the most suitable solutions for specific application requirements.
- The students create a fully functional mobile application for Android or iOS, including publishing and deployment.

Literature
Dieter Meiller: Modern App Development with Dart and Flutter 2: A comprehensive introduction to Flutter. De Gruyter Oldenbourg, 2021.

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 5003809
Principles of Autonomous Drones

Module profile

Exam number
5003809

Duration
1 semester

Frequency
Every summer semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar

Language of instruction
English

Organisation

Responsible lecturer
Prof. Dr. Frank Deinzer

Lecturer(s)
Marcel Kyas

Applicability	BIN, BWI, BISD, BDGD
Semester according to SPO	6. semester
Type of module	FWPM

Required prerequisites for the participation in the module according to the SPO
none

Recommended prerequisites for the participation in the module
none

Content
You will learn the fundamental methods for endowing aerial autonomous drones with perception, planning, and decision-making capabilities. You will learn algorithmic approaches for robot perception, localisation, and simultaneous localisation and mapping, as well as the control of non-linear systems, learning-based control, and aerial drone motion planning. You will learn methodologies for reasoning under uncertainty.

On day one, you will learn to describe the basic control loop of an autonomous robot. You will explain the basics of drone locomotion and kinematics (how drones move). On day two, you will learn to enumerate the purpose of sensors on a drone. You will explain the structure and applications of Bayesian filters. On day three, you will learn to implement a simple localisation system. On day four, you will learn to explain behavior trees as a formalism to describe drone behaviour. You will learn to define principles of planning algorithms (Dijkstra's Algorithm, A* Search, D* Search). You will apply reinforcement learning to solve drone planning problems.

You will design a simulation in Robot Operating System 2 (ROS2) for demonstrations and hands-on activities.

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Other exam (soP) according to §§ 26, 27 APO

Examination - length/format
Colloquium

The concrete length/format of the examination will be determined in the study plan.

Language of examination
English

Condition for the award of credit points
None

Learning outcomes
1. the students know the fundamental principles of motion control applied to aerial autonomous drones.
2. the students understand basic concepts of perception, distinguishing between classic approaches and deep learning methods for robot perception.
3. the students can explain principles of localisation and Simultaneous Localization and Mapping (SLAM), including their importance for autonomous navigation.
4. the students analyze navigation algorithms, focusing on planning and decision-making processes necessary for effective drone operation.
5. the students apply algorithmic approaches for robot perception, localisation, and planning in practical scenarios.
6. the students implement learning-based control techniques for aerial drones to enhance their motion planning capabilities.
7. the students utilize the Robot Operating System (ROS) in demonstrations and hands-on activities, reinforcing the theoretical concepts covered in the course.

Literature
Roland Siegwart, Illah Reza Nourbakhsh, and Davide Scaramuzza. Introduction to Autonomous Mobile Robots, second edition. 2011, The MIT Press
Sebastian Thrun, Wolfram Burgard, and Dieter Fox. Probabilistic Robotics. 2005, The MIT Press

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 6810310
Project Work

Module profile

Exam number
6810310

Duration
1 semester

Frequency
Every semester

Credit hours (SWS)
4

ECTS-Credits (CP)
10.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 240 hrs

Total: 300 hrs

Teaching format
Project

Language of instruction
German/English

Organisation

Responsible lecturer
Prof. Dr.-Ing. Sebastian Biedermann

Lecturer(s)
Prof. Dr. Arndt Balzer,
Prof. Dr. Peter Braun,
Prof. Dr. Frank Deinzer,
Prof. Dr. Steffen Heinzl,
Prof. Dr. Isabel John,
Prof. Dr. Frank-Michael Schleif,
Prof. Dr. Christian Bachmeir,
Prof. Dr.-Ing. Sebastian Biedermann

Applicability	BISD
Semester according to SPO	6. semester
Type of module	Compulsory module

Required prerequisites for the participation in the module according to the SPO
100 ECTS points

Recommended prerequisites for the participation in the module
none

Content
The project work is usually teamwork (at least three students). It involves either end-to-end software development according to the rules of software engineering or another task from the IT field (e.g. software comparison, software selection, software introduction). Each project is supervised by a professor from the Faculty of Computer Science and Business Informatics. In the course of the project work, the techniques and methods learned in computer science are practised in a practical professional context (teamwork; project organisation; practical tasks).
The topics of the practical examples for the examination are provided by or agreed with the lecturer in the traditional degree programme. In the BIN dual study programme, a practical task is worked on in consultation with the lecturer. This ensures practical relevance and feedback from the company.
Students are instructed to independently develop software and create documentation consisting of the following parts:

- Software development
- Requirements specification, in which the requirements for the project work are compiled (with milestones/schedule)
- Technical design using appropriate methods
- IT design
- Listing
- User manual
- Appendix (literature used; list of abbreviations, glossary, etc.)
- For other tasks:
- Project description in which the requirements for the project work are summarised (with milestones/schedule)
- Further contents to be specified by the supervising professor, which result from the individual character of the respective assignment
- Appendix (literature used; list of abbreviations, glossary, etc.)

The topics of the practical examples for the examination are provided by or agreed with the lecturer in the traditional degree programme. In the dual study programme variant, a practical assignment is worked on in consultation with the lecturer.

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Other exam (soP) according to §§ 26, 27 APO

Examination - length/format
error

The concrete length/format of the examination will be determined in the study plan.

Language of examination
German/English

Condition for the award of credit points
None

Learning outcomes
Students can methodically process and solve comprehensive tasks.
Students can develop and implement suitable solution strategies in a team.
They know how team processes work and how they can contribute their own personality.
Students can independently set up, implement, support and present a small IT project in a team. They can identify and use appropriate development technologies and test and document their code.

Literature
depending on the respective project work

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 5003865
Quantum Computing

Module profile

Exam number
5003865

Duration
1 semester

Frequency
Every summer semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar

Language of instruction
English

Organisation

Responsible lecturer
Prof. Dr. Frank-Michael Schleif

Lecturer(s)
Divya Rani

Applicability	BIN, BWI, BEC, BISD, BDGD
Semester according to SPO	6. semester
Type of module	FWPM

Required prerequisites for the participation in the module according to the SPO
none

Recommended prerequisites for the participation in the module
Basic Linear Algebra and Python Programming

Content
This course provides a comprehensive introduction to the principles, mathematical foundations, hardware concepts, and programming tools of quantum computing. Students will explore qubits, superposition, entanglement, quantum gates, algorithms, noise models, error correction, and real-world applications. Hands-on sessions using Qiskit enable learners to construct and simulate quantum circuits and run programs on IBM Quantum devices.

1. foundations of quantum computing
Classical vs Quantum computation, Qubits and quantum states, Superposition and entanglement, Dirac notation (bras & kets),Bloch sphere representation, Quantum measurement and collapse, Physical implementations of qubits: Superconducting, Ion traps, Photonic systems.
2. quantum gates and quantum circuits
Single-qubit gates: Pauli-X, Y, Z, Hadamard (H), Phase, S, T, Multi-qubit gates: CNOT, Swap, Controlled phase, Building quantum circuits, Reversible computing principles, Quantum circuit simulation tools, IBM Qiskit basics, Circuit construction & visualisation, Noise, error sources & decoherence.
3. quantum algorithms
Quantum parallelism, Deutsch-Jozsa algorithm, Grover's search algorithm, Shor's factoring algorithm Quantum Fourier Transform (QFT), Phase estimation, Variational Quantum Algorithms (VQA): VQE, QAOA
4. quantum hardware, noise & error correction
NISQ (Noisy Intermediate-Scale Quantum) era systems, Quantum noise models: Bit flip, Phase flip, Depolarising noise, Quantum error correction basics: Shor code, Steane code, Surface code (overview), Fault-tolerant quantum computation, Quantum supremacy claims (Google, IBM).
5. applications, future trends & quantum programming
Quantum cryptography (BB84, QKD), Post-Quantum Cryptography (PQC), Quantum Machine Learning (QML) basics, Quantum optimization (QAOA use cases), Quantum simulation in chemistry & physics Hands-on Qiskit programming: Creating circuits, executing on simulators, Running on IBM Quantum systems.

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Written exam (sP) according to § 23 APO

Examination - length/format
90 minutes

The concrete length/format of the examination will be determined in the study plan.

Language of examination
English

Condition for the award of credit points
None

Learning outcomes
On successful completion of the course the students shall be able to
1. explain the fundamental concepts of qubits, superposition, entanglement, and quantum measurement.
2. construct and simulate quantum circuits using quantum gates and operators.
3. analyse the working of major quantum algorithms and identify their computational advantages.
4. understand hardware constraints, quantum noise, and basic quantum error correction techniques.
5. implement quantum programs using Qiskit and evaluate applications of quantum computing across domains.

Literature
Textbook(s):
1 Nielsen, M., & Chuang, I. Quantum Computation and Quantum Information, Cambridge University Press, 2010.
2. Yanofsky, N., & Mannucci, M. Quantum Computing for Computer Scientists, Cambridge University Press, 2008.
References:
1. IBM Quantum Documentation - https://quantum-computing.ibm.com
2. Qiskit Textbook - https://qiskit.org/learn
3 Preskill, J. Quantum Computing in the NISQ Era.
4. Arun P. Quantum Computing: An Applied Approach, Springe
Online Resources (e-books, notes, ppts, video lectures etc.):
1. Qiskit Tutorials: https://qiskit.org/tutorials
2. Quantum Algorithms Zoo: https://quantumalgorithmzoo.org
3. MIT OCW - Quantum Computation
4. IBM Quantum Lab (free cloud access).

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 5003067
Requirements Engineering

Module profile

Exam number
5003067

Duration
1 semester

Frequency
Every summer semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar

Language of instruction
English

Organisation

Responsible lecturer
Prof. Dr. Isabel John

Lecturer(s)
Prof. Dr. Isabel John,
Dr. Anne Heß,
Dr.-Ing. Benedikt Kämpgen

Applicability	BEC, BIN, BWI, BISD, BDGD
Semester according to SPO	6. semester
Type of module	FWPM

Required prerequisites for the participation in the module according to the SPO
none

Recommended prerequisites for the participation in the module
Software Engineering /Software Development

Content
This module focuses on the crucial initial phase of the software development lifecycle, where the needs and constraints of the system are gathered, analysed, and documented. Similarly, machine learning (ML) system development projects benefit from RE. So this module covers requirements engineering techniques for traditional systems as well as for ML systems.

Basics of Requirements Engineering
Task Oriented, Goal Oriented RE
Elicitation Techniques
Analysis techniques
Specification / Modelling techniques
Validation techniques
RE in User Experience Engineering
RE Skills
Case Studies and Applications of Requirements Engineering
Requirements Engineering for machine learning systems
Requirements Engineering in the age of ChatGPT / generative artificial intelligence

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Other exam (soP) according to §§ 26, 27 APO

Examination - length/format
Portfolio

The concrete length/format of the examination will be determined in the study plan.

Language of examination
English

Condition for the award of credit points
None

Learning outcomes
The students remember fundamental RE models, methods, and their relevance in the software development process.
The students understand the importance of requirements engineering, including stakeholder analysis, in diverse project contexts, including international and AI-driven projects.
The students apply requirements elicitation techniques and modelling methods, such as UML, use cases, user stories, and non-functional requirements, to real-world scenarios.
The students analyze requirements through negotiation, prioritisation, and validation against quality criteria to ensure completeness and clarity.
The students evaluate different RE approaches and adapt techniques suited for specific domains like machine learning and generative AI systems.
The students create comprehensive requirements specifications and models that address the needs of complex, modern software systems, including AI applications.
The students are able to adapt requirements engineering techniques for generative artificial intelligence based systems

Literature
Cockburn, Writing Effective Use Cases, Addison Wesley, 2016
Hull, Requirements engineering, Springer Verlag, 2019
Berenbach, Software & Systems Requirements Engineering: In Practice, McGraw Hill, 2017
Chris Rupp & the SOPHISTs , Requirements Engineering (in German), Hanser, 2022
Huyen, Chip. Designing machine learning systems. " O'Reilly Media, Inc.", 2022.

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 5003857
Seminar Smart Systems

Module profile

Exam number
5003857

Duration
1 semester

Frequency
Every summer semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar

Language of instruction
German

Organisation

Responsible lecturer
Prof. Dr. Arndt Balzer

Lecturer(s)
Prof. Dr. Arndt Balzer

Applicability	BIN, BWI, BEC, BISD, BDGD
Semester according to SPO	6. semester
Type of module	FWPM

Required prerequisites for the participation in the module according to the SPO
none

Recommended prerequisites for the participation in the module
Courses in the field of computer engineering

Content
Contents: In the specialisation module, students work independently on topics from the field of smart systems. Solutions (hardware and software) are developed and presented.
Topics from previous years (selection): AI based checkout, Braille Reader, Inverse Pendulum, Kalman Filtering, Pathfinding with Turtlebot, Quadrocopter, Radar + Lidar, ROS (Robot Operating System), SDR (Software Defined Radio), SLAM (Mapping, Localisation, Navigation), Supervised Learning, Reinforcement Learning, Rock-Paper-Scissors on Pepper, WIFI Indoor Localisation, ...
The seminar is organised under a regularly updated umbrella topic, for which individual topics are assigned. The topics are determined at the beginning of the seminar and are based on current developments. Actuators and sensors, low performance systems through to smartphones, their programming and evaluation of prototype implementations are always of interest.

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Other exam (soP) according to §§ 26, 27 APO

Examination - length/format
Multimedia presentation, Colloquium

The concrete length/format of the examination will be determined in the study plan.

Language of examination
German

Condition for the award of credit points
None

Learning outcomes
Learning objectives: By dealing with a selected topic, the ability to deal with challenging topics is deepened.

- The students acquire mathematical and technical basics
- Derive the specialised knowledge required for their specific topic or area of application
- Implement this knowledge using the methods they have learnt and acquire additional confidence in their application

The findings are documented and the results are presented at the end of the seminar

- Students acquire the skills to document and present results in a comprehensible manner.
- Students apply methods of scientific work including (literature) research.
- Students generalise their ability to independently expand existing knowledge and quickly familiarise themselves with the topics of others (fellow students)

Literature

- Will be announced in each case.

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 6820270
Secure Blockchain Technologies

Module profile

Exam number
6820270

Duration
1 semester

Frequency
Every winter semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar-style instruction

Language of instruction
German

Organisation

Responsible lecturer
Prof. Dr.-Ing. Tobias Fertig

Lecturer(s)
Prof. Dr.-Ing. Tobias Fertig

Applicability	BISD
Semester according to SPO	6. semester
Type of module	Compulsory module

Required prerequisites for the participation in the module according to the SPO
none

Recommended prerequisites for the participation in the module
none

Content
In this module, students gain in-depth insights into the technical foundations and security-relevant aspects of modern blockchain systems. To begin with, they learn about the basic functioning of blockchains, including the data structure, cryptographic security and decentralised consensus building. Building on this, a practical deep dive into Ethereum-based blockchains is carried out, whereby the underlying cryptographic concepts, in particular Elliptic Curve Cryptography (ECC), are also discussed. A central component of the module is working with smart contracts. Students are introduced to the architecture of the Ethereum Virtual Machine (EVM) and learn how to write, test and deploy their own smart contracts and evaluate them in terms of security. The focus is not only on the technical implementation, but also on securing smart contracts. To deepen their knowledge, students deal with typical security vulnerabilities and attack scenarios. In practical exercises, they analyse common exploits and learn about reverse engineering methods to examine existing smart contracts and identify security-critical vulnerabilities. The aim of the module is to provide a comprehensive understanding of the responsible use of blockchain technologies and the secure development of decentralised applications.

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Other exam (soP) according to §§ 26, 27 APO

Examination - length/format
Portfolio

The concrete length/format of the examination will be determined in the study plan.

Language of examination
German

Condition for the award of credit points
None

Learning outcomes
After completing the module, students will be able to

- Describe the basic principles and functioning of blockchain technologies.
- explain the structure and functionality of Ethereum-based blockchains and the Ethereum Virtual Machine (EVM).
- understand basic concepts of Elliptic Curve Cryptography (ECC) in the context of blockchain systems.
- compare different consensus mechanisms (e.g. Proof of Work, Proof of Stake) and evaluate their suitability for specific use cases.
- identify typical application scenarios for blockchain technologies and analyse their potential benefits.
- independently implement, test and deploy smart contracts in a blockchain environment.
- recognise security-critical aspects in the development of smart contracts and implement appropriate protective measures.
- practically understand known vulnerabilities and exploits in smart contracts and analyse how they work
- apply basic reverse engineering techniques to analyse and evaluate existing smart contracts
- reflect on risks and challenges in the development and use of blockchain-based systems.

Literature
https://www.rheinwerk-verlag.de/blockchain-the-comprehensive-guide-to-blockchain-development-ethereum-solidity-and-smart-contracts/
https://book.getfoundry.sh/
https://www.harpercollins.com.au/9780008562809/proof-of-stake-the-making-of-ethereum-and-the-philosophy-of-blockchains/
https://www.campus.de/buecher-campus-verlag/wirtschaft-gesellschaft/wirtschaft/mehr_als_geld-17528.html

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 5003098
Social Media in the business world

Module profile

Exam number
5003098

Duration
1 semester

Frequency
Every summer semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 40 hrs

Self-study: 110 hrs

Total: 150 hrs

Teaching format
Seminar

Language of instruction
German

Organisation

Responsible lecturer
Prof. Dr. Christina Völkl-Wolf

Lecturer(s)
Tobias Tellers,
Philipp Oberkalkofen

Applicability	BEC, BDGD, BISD
Semester according to SPO	6. semester
Type of module	FWPM

Required prerequisites for the participation in the module according to the SPO
none

Recommended prerequisites for the participation in the module
- Basic knowledge of social media, use of internet applications
- Interest in corporate communications

Content
The module focuses on the professional development and implementation of social media strategies. Students learn to define strategic goals and analyse target groups in a differentiated manner. They receive a comprehensive overview of relevant social media channels and their targeted use, in particular blogs, Facebook, X (formerly Twitter), YouTube, Instagram and professional networks such as XING and LinkedIn. Another focus is on the sensible combination and linking of these platforms and their integration into overarching marketing strategies.

In addition, methods of monitoring, measuring success and social media controlling are taught. Particular attention is paid to community management as a key factor for successful communication in social networks. This includes the development of a community strategy, the basics of online dialogue, dealing with challenges such as trolls or shitstorms and the basic principles of crisis communication. Students also learn how community engagement can be specifically promoted and positively influenced by psychological factors. The range of topics is supplemented by the development of a content strategy, the use of social customer service and suitable methods for monitoring the success of community measures.

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Other exam (soP) according to §§ 26, 27 APO

Examination - length/format
Portfolio

The concrete length/format of the examination will be determined in the study plan.

Language of examination
German

Condition for the award of credit points
None

Learning outcomes
After successfully completing the module, students will be able to:
Students will identify key terms, building blocks and technical foundations of social media strategies in a corporate context.
Students categorise social media platforms, target groups and communication formats and explain their respective application possibilities.
Students use the principles of community management in practical situations to activate, moderate and maintain online communities.
Students distinguish between typical dialogue situations and challenges in social media dialogue and structure corresponding interaction and reaction patterns.
Students assess the success of social media measures using basic monitoring and analysis tools and derive well-founded recommendations for action.
Students develop a complete social media strategy including objectives, channel selection, content planning and integration into overarching marketing goals.

Literature
Appel, G., Grewal, L., Hadi, R., & Stephen, A. T. (2020). The future of social media in marketing. Journal of the Academy of Marketing Science, 48(1), 79-95.
Rana, N. P., Slade, E. L., Dwivedi, Y. K., & Tajvidi, M. (Eds.). (2020). Digital and Social Media Marketing: Emerging Applications and Theoretical Development. Springer.
Wolff, C. (2024). Social media strategies for B2B companies. Springer Gabler.
Tajvidi, M., Wang, Y., Hajli, N., & Love, P. E. D. (2021). Brand value co-creation in social commerce: The role of interactivity, social support, and relationship quality. International Journal of Information Management, 57.
Kapoor, K. K., Tamilmani, K., Rana, N. P., Patil, P., Dwivedi, Y. K., & Nerur, S. (2018). Advances in social media research: Past, present and future. Information Systems Frontiers, 20, 531-558.
Opresnik, M. O., & Hollensen, S. (2023). Social Media Marketing: A Practitioner Guide. Springer.

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 5003810
Software Testing

Module profile

Exam number
5003810

Duration
1 semester

Frequency
Every summer semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar

Language of instruction
English

Organisation

Responsible lecturer
Prof. Dr. Peter Braun

Lecturer(s)
Pascal Moll

Applicability	BEC, BIN, BWI, BISD
Semester according to SPO	6. semester
Type of module	FWPM

Required prerequisites for the participation in the module according to the SPO
None

Recommended prerequisites for the participation in the module
Programming I or backend programming or programming in Python or basic programming; object-orientated programming in Java
Participants will receive a virtual machine, the functionality of which should be tested before the course begins.

Content
This module deals with different types of tests and their application in software development. The SOLID principles and the 4-layer concept for test architectures are taught. It also covers the automated testing of interfaces and APIs as well as the use of mocking. Another focus is on behaviour-driven development with Cucumber. Exploratory testing and the integration of automated tests into a DevOps life cycle are also discussed. The module includes practical content for which a virtual machine is provided. The prerequisite for this is the installation of VirtualBox.

- Fundamentals of testing (test coverage, test paths, black box, white box, grey box, functional and non-functional tests, test pyramid)
- Test automation (goals, success factors, differences between different types, test framework JUnit, annotations, assertions, exception testing, parameterisation, test types, record replay, scripted testing, keyword-driven testing)
- Test architecture (SOLID principles, 4-layer concept, test modelling layer, test definition, test execution, test adaptation, interfaces, design and development, important design patterns for testing)
- Testing of graphical user interfaces (introduction to Selenium, drivers, PageObject patterns, identifiers, waits, cookies)
- Mocking (Wiremock)
- Behaviour Driven Development (Feature Files & Step Files, Cucumber & Gherkin, Parameters, Data Tables, Scenario Outlines and Background, Runner Classes)
- Exploratory testing (methods and techniques)
- Build Server (Jenkins basics & DevOps basics, gPipelines, DevOps process from a testing perspective)

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Other exam (soP) according to §§ 26, 27 APO

Examination - length/format
Portfolio

The concrete length/format of the examination will be determined in the study plan.

Language of examination
English

Condition for the award of credit points
None

Learning outcomes

- Students define test objectives for software.
- Students analyse test objectives and define suitable test types.
- Students translate test types into automated tests.
- Students decide on the use of design patterns in testing and apply design patterns.
- Students explain Behaviour Driven Development.
- Students set up and configure a build server for testing.

Literature
Essentials of Software Testing by Ralf Bierig, Stephen Brown, Edgar Galván, Joe Timoney, 2021, Cambridge University Press

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 5003858
Smart Systems

Module profile

Exam number
5003858

Duration
1 semester

Frequency
Every summer semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar

Language of instruction
German

Organisation

Responsible lecturer
Prof. Dr. Arndt Balzer

Lecturer(s)
Prof. Dr. Arndt Balzer

Applicability	BIN, BWI, BISD, BDGD
Semester according to SPO	6. semester
Type of module	FWPM

Required prerequisites for the participation in the module according to the SPO
none

Recommended prerequisites for the participation in the module
Programming I + II, Fundamentals of Computer Engineering, Computer Architecture, Operating Systems, Algorithms & Data Structures

Content
- Introduction to C for programmers
- Specifics of programming microcontrollers (ESP32, 32-bit microcontroller family from Espressif)
- Memory model, interrupt concept, ...
- Hardware structure and programming of common interfaces for communication and control of peripherals such as U(S)ART, SPI (Four Wire), I²C (Two Wire), OneWire, CAN
- Programming of peripheral devices such as digital sensors: IMU (10-axis), digital thermometers, ultrasound and actuators: displays, servos, loudspeakers, ...
- Programming of wireless interfaces (RF) such as Bluetooth and WiFi to control applications such as servos, etc. using smartphones
- Implementation of small AI models (image recognition using USB cam)
- Introduction to a current, application-based development environment ESP-IDF (Espressif IoT Development Framework)

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Other exam (soP) according to §§ 26, 27 APO

Examination - length/format
Colloquium, Practical study achievement

The concrete length/format of the examination will be determined in the study plan.

Language of examination
German

Condition for the award of credit points
None

Learning outcomes
Students are able to

- explain the specific programming of controllers and their interfaces,
- assess historically grown interfaces,
- use a software development environment that makes efficient use of innovative and application-optimised peripheral functions,
- develop hardware-related software in the C programming language for various applications.

Literature

- Kernighan, Ritchie: The C programming language, 2nd Edition (ANSI)
- Udo Brandes: Microcontroller ESP32 - The comprehensive manual
- Dausmann, et. al.: C as the first programming language, Vieweg, 2011, ebook
- Wolf: C from A to Z, Galileo Computing, openbook

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 6810290
Threat Intelligence

Module profile

Exam number
6810290

Duration
1 semester

Frequency
Every summer semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar-style instruction

Language of instruction
English

Organisation

Responsible lecturer
Prof. Dr. Christian Bachmeir

Lecturer(s)
Prof. Dr. Christian Bachmeir

Applicability	BISD
Semester according to SPO	6. semester
Type of module	Compulsory module

Required prerequisites for the participation in the module according to the SPO
none

Recommended prerequisites for the participation in the module
none

Content
Students acquire a sound understanding of the background to digital attacks and the systematic analysis of threat information. They learn about various cybercrime scenarios and analyse the underlying strategies, motivations and business models of attackers. A particular focus is on the detection and analysis of malware. Students deal with the functionalities of popular malware families and the development of corresponding detection methods, in particular using indicators of compromise (IoCs). Both static and dynamic analysis methods are taught in a practical manner. In addition, students are given an overview of publicly available sources of information on the threat situation, for example from CERTs, threat feeds or open source platforms. They learn how to research and evaluate these sources and integrate them into technical applications. Tools and standards such as YARA signatures, dashboards and threat intelligence platforms are also used. The aim of the module is to develop an application-oriented understanding of how to handle threat information and recognise its added value for information security.

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Other exam (soP) according to §§ 26, 27 APO

Examination - length/format
Portfolio

The concrete length/format of the examination will be determined in the study plan.

Language of examination
English

Condition for the award of credit points
None

Learning outcomes

- Students know the strategies, motivations and business models behind digital attacks
- Students understand the popular detection methods of malware
- Students can analyse unknown files for suspicious behaviour (static vs. dynamic analysis)
- Students can use and integrate freely available sources of information

Literature

Incident Response with Threat Intelligence: Practical insights into developing an incident response capability through intelligence-based threat hunting, Roberto Martínez, 2022
Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software, Michael Sikorski and Andrew Honig, 2012
Practical Cyber Threat Intelligence: Gather, Process, and Analyse Threat Actor Motives, Targets, and Attacks with Cyber Intelligence Practices, Erdal Ozkaya, 2023

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 100002
Usability for Engineers and Computer Scientists

Module profile

Exam number
100002

Duration
1 semester

Frequency
Every summer semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 0 hrs

Self-study: 150 hrs

Total: 150 hrs

Teaching format
Lecture

Language of instruction
German

Organisation

Responsible lecturer
Prof. Dr. Isabel John

Lecturer(s)

Applicability	BIN, BWI, BISD, BDGD
Semester according to SPO	6. semester
Type of module	FWPM

Required prerequisites for the participation in the module according to the SPO
This is an offer of the Virtual University of Bavaria. Further information can be found at https://kurse.vhb.org/VHBPORTAL/kursprogramm/kursprogramm.jsp?kDetail=true&COURSEID=19832,83,816,1

Recommended prerequisites for the participation in the module
none

Content
This is an offer of the Virtual University of Bavaria. Further information can be found at https://kurse.vhb.org/VHBPORTAL/kursprogramm/kursprogramm.jsp?kDetail=true&COURSEID=19832,83,816,1
In our highly technical and networked world, the usability of products, services and interactive systems is becoming an increasingly important feature for users and users on the one hand and a competitive advantage for manufacturers on the other. With a comparable range of functions, many products are being offered at increasingly favourable prices in global competition. The user has a choice and will opt for the advantages of a product that has been tested and optimised for usability and user experience. By using usability engineering methods, manufacturers can meet these requirements and develop unique selling points for their products. Usability and user experience objectives should therefore be considered as early as possible in the development process and implemented using suitable methods, among other things to avoid costly misdevelopments and increase the benefits for customers. Prospective engineers and computer scientists must be able to recognise this problem and know in which phases of product development suitable methods are used.

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Written exam (sP) according to § 23 APO

Examination - length/format
90 minutes

The concrete length/format of the examination will be determined in the study plan.

Language of examination
German

Condition for the award of credit points
None

Learning outcomes
This is an offer of the Virtual University of Bavaria. Further information can be found at https://kurse.vhb.org/VHBPORTAL/kursprogramm/kursprogramm.jsp?kDetail=true&COURSEID=19832,83,816,1
Naming the content of the analysis phase in usability engineering.

- Independent application of analysis methods and techniques of usability engineering
- Application-specific identification of relevant parts of the DIN/ISO 9241 series of standards
- Describe and apply terms (usability) and principles (dialogue design)
- Describe and apply a process for designing usable interactive systems
- Describe the essential aspects of cognitive psychology and industrial psychology
- Identify and name criteria for evaluating colour design in order to identify and name associated usability problems.
- Describe fundamental aspects of contrasts and their use in design.
- Recognise in which development phases design laws must be observed and how these simple laws help to identify usability problems
- Apply design laws in a targeted manner in the context of usability evaluations
- Describe the typical procedure in interface and interaction design.
- Name different types of prototypes and describe their function in usability engineering
- Describe and apply usability metrics from the areas of \"Usability Performance Metrics\" and \"Usability Issue based Metrics\".

Literature
see course

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 6322200
Virtual Reality

Module profile

Exam number
6322200

Duration
1 semester

Frequency
Every summer semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar-style instruction, Exercise

Language of instruction
German

Organisation

Responsible lecturer
Stefan Sauer

Lecturer(s)
Stefan Sauer

Applicability	BEC, BIN, BWI, BISD, BDGD
Semester according to SPO	6. semester
Type of module	FWPM

Required prerequisites for the participation in the module according to the SPO
none

Recommended prerequisites for the participation in the module
none

Content
The event is organised by the Faculty of Polymer Engineering and Surveying (FKV):
(https://geo.thws.de/studium/bachelor-geovisualisierung/studienablauf/modulhandbuch-bgv-ab-ws-202223/)

For scheduling: https://geo.thws.de/studium/aktuelle-lehrveranstaltungsplaene/

- Creation of 3D models for transfer to game engines
- Dealing with game engines
- Rendering pipeline
- Integration of VR functionalities in game engines
- Creation of fully functional 3D models in game engines
- Realisation of virtual tours

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Written exam (sP) according to § 23 APO

Examination - length/format
90 minutes

The concrete length/format of the examination will be determined in the study plan.

Language of examination
German

Condition for the award of credit points
None

Learning outcomes
After participating in the module, students can independently plan, realise and set up VR applications or publish them using appropriate services.

Game engines are used to create VR environments. Students therefore learn the basics of importing and operating geodata in game engines, as well as the settings for rendering and preparing the data for VR applications, including programming controllers and the interface to VR glasses.

Literature
Akenine-Möller, T.; Haines, E.; Hoffman, N.; Pesce, A.; Iwanicki, M.; Hillaire, S.: Real-Time Rendering, 2018, 4th edition, Milton: Chapman and Hall/CRC, London, ISBN: 9781138627000 Edler, D.; Husar, A.; Keil, J.; Vetter, M. & Dickmann, F.: Virtual Reality (VR) and Open Source Software: A Workflow for Constructing an Interactive Cartographic VR Environment to Explore Urban Landscapes, 2018. In: Kartographische Nachrichten, Journal of Cartography and Geographic Information, 68(1), p. 5-13, ISSN: 2524-4965
Edler, D.; Kühne, O.; Jenal, C.; Vetter, M.; Dickmann, F.: Potentials of spatial visualisation in virtual reality (VR) for social constructivist landscape research, 2018. In: Kartographische Nachrichten, Journal of Cartography and Geographic Information, 68(5), p. 245-254, ISSN: 2524-4965
Vetter, M.: Technical Potentials for the Visualisation in Virtual Reality, 2020. in D. Edler, C. Jenal, & O. Kühne (Eds.), Modern Approaches to the Visualisation of Landscapes, 2020, Wiesbaden: Springer VS, ISBN: 978-3-658-30956-5

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 1000010
Web Programming

Module profile

Exam number
1000010

Duration
1 semester

Frequency
Every semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 0 hrs

Self-study: 150 hrs

Total: 150 hrs

Teaching format
Lecture

Language of instruction
German

Organisation

Responsible lecturer
Prof. Dr. Rolf Schillinger

Lecturer(s)

Applicability	BWI, BISD, BDGD
Semester according to SPO	6. semester
Type of module	FWPM

Required prerequisites for the participation in the module according to the SPO
This is an offer of the Virtual University of Bavaria. Further information can be found at https://kurse.vhb.org/VHBPORTAL/kursprogramm/kursprogramm.jsp?kDetail=true&COURSEID=20179,83,1218,2

Recommended prerequisites for the participation in the module
This is an offer of the Virtual University of Bavaria. Further information can be found at https://kurse.vhb.org/VHBPORTAL/kursprogramm/kursprogramm.jsp?kDetail=true&COURSEID=20179,83,1218,2

Content
This is an offer of the Virtual University of Bavaria. Further information can be found at https://kurse.vhb.org/VHBPORTAL/kursprogramm/kursprogramm.jsp?kDetail=true&COURSEID=20179,83,1218,2

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Written exam (sP) according to § 23 APO

Examination - length/format
90 minutes

The concrete length/format of the examination will be determined in the study plan.

Language of examination
German

Condition for the award of credit points
None

Learning outcomes
This is an offer of the Virtual University of Bavaria. Further information can be found at https://kurse.vhb.org/VHBPORTAL/kursprogramm/kursprogramm.jsp?kDetail=true&COURSEID=20179,83,1218,2

Literature
This is an offer of the Virtual University of Bavaria. Further information can be found at https://kurse.vhb.org/VHBPORTAL/kursprogramm/kursprogramm.jsp?kDetail=true&COURSEID=20179,83,1218,2

7. semester

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 5003198
Green IT (Blended Intensive Program)

Module profile

Exam number
5003198

Duration
1 semester

Frequency
Irregular

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar-style instruction

Language of instruction
English

Organisation

Responsible lecturer
Prof. Dr. Peter Braun

Lecturer(s)
Prof. Dr. Peter Braun,
Prof. Dr. Frank-Michael Schleif

Applicability	BIN, BWI, BEC, BISD, BDGD
Semester according to SPO	7. semester
Type of module	FWPM

Required prerequisites for the participation in the module according to the SPO
None

Recommended prerequisites for the participation in the module
None

Content
This module explores how sustainability principles can be integrated into the design, development, deployment, and management of IT systems. It offers a multidisciplinary perspective on the environmental, economic, and societal implications of information technology. Through lectures, case studies, and collaborative international projects, students gain both theoretical foundations and practical experience in Green IT strategies. Partnering with universities in the Czech Republic, Germany, and Iceland, the module includes cross-border collaboration and comparative analysis of regional IT sustainability approaches. This module contains a compulsory study trip to Prague, the Czech Republic.

- Introduction to Green IT: Definition, significance, and global relevance; real-world applications in industry and academia
- Environmental Impact of IT: Carbon footprint, e-waste, lifecycle analysis, and Green Computing standards
- Sustainable Software Engineering: Design principles and code optimisation for energy efficiency
- Green Algorithms and Data Structures: Techniques to reduce energy consumption and benchmark software for efficiency
- AI and Machine Learning for Green IT: Optimisation of energy use, environmental monitoring, and ethical implications
- Green IT Strategies in Mobile and Distributed Systems: Sustainable design and management of mobile technologies and data centres
- Life Cycle Assessment (LCA): Application of LCA in IT hardware and software development
- Education and Training for Green IT: Curriculum development, capacity building, and case studies
- Regulatory and Compliance Aspects: Overview of international standards, compliance practices, and green certifications

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Other exam (soP) according to §§ 26, 27 APO

Examination - length/format
Portfolio

The concrete length/format of the examination will be determined in the study plan.

Language of examination
English

Condition for the award of credit points
None

Learning outcomes
Upon successful completion of this module, students will be able to:

- Remember key concepts and terminology related to Green IT, including sustainability goals, environmental impacts, and regulatory frameworks
- Understand the ecological footprint of hardware and software systems and explain how IT contributes to global sustainability challenges
- Apply principles of sustainable software engineering, energy-efficient algorithms, and lifecycle assessments to practical use cases
- Analyse and compare national and regional Green IT strategies and regulatory approaches across Germany, Iceland, and the Czech Republic
- Evaluate the sustainability impact of IT systems and development practices using recognised metrics and standards
- Create innovative, practical solutions to real-world Green IT challenges by working on interdisciplinary, cross-national projects

Literature
It will be announced in class