Technische Hochschule Ingolstadt

Module Handbook

M.Sc. SOCIOTECHNICAL CYBERSECURITY (SPO SS 26)

Faculty of Computer Science

Summer term 2026

as of: 2026-01-29

This program and module description become effective on 15.03.2026. It supplements the study and examination regulations and serves to ensure that the modules are available according to the regulation of SS 26.Additionally, it contains detailed information about modules, contents, assignments, and examinations.

Content

1 Description of Modules

1.1 Compulsory Modules

Principles of Cybersecurity and Networks			
Module abbreviation:	SOC_CSN	**SPO-No.:**	1
Curriculum:	**Program**	**Module type**	**Semester**
	Sociotechnical Cyber-security (SPO SS 26)	Einsetzungstext ist leer!	1
Module attribute:	**Language of instruction**	**Duration of module**	**Frequency of offer**
	English	1 semester	only winter term

Responsible for module:	Hutzelmann, Thomas
Credit points / SWS:	8 ECTS / 4 SWS
Workload:	Contact hours: 0 h Self study hours: 0 h Total hours: 200 h
Subjects of the module:	Principles of Cybersecurity and Networks
Lecture types:	O - Online self-study course with support from a lecturer
Usability for other study programs:	None

Examinations:

schrP90 - written exam, 90 minutes

Requirements:
None

Prerequisites according examination regulation:

None

Recommended prerequisites:

None

Objectives:

After successful completion of this module, students are able to …

- analyse and design advanced threat models for complex networked and distributed systems.
- evaluate and apply advanced risk rating and risk management approaches in technical cybersecurity contexts.
- plan, conduct and critically assess advanced security testing methods for networks, systems and applications.
- design and evaluate Zero Trust architectures and explain their implications for modern network security.
- analyse communication systems based on layered models and explain security properties across layers.

- evaluate transport- and application-layer protocols (with a focus on DNS) with respect to security properties and attack surfaces.
- analyse and assess routing mechanisms (in particular BGP) with regard to resilience and security risks.
- design and evaluate technical security controls such as IDS, firewalls, segmentation mechanisms and authentication infrastructures.
- design secure network architectures using technologies such as VLAN, IPsec, VPN and modern solutions (e.g. WireGuard) and integrate them into coherent security concepts.

Content:

- Advanced threat modeling for complex systems
- Advanced risk rating and management for complex systems
- Advanced security testing
- Zero trust architectures
- Layered model of communication
- Transport layer protocols
- Application layer protocols with focus on DNS
- Routing with focus on BGP
- Intrusion detection systems
- Firewalls including NAT as IPv4 workaround and changes introduced by IPv6
- Authentication mechanisms with focus on Kerberos
- Virtual LAN
- IPsec
- VPN and WireGuard

Literature:

- RAIS, Razi and others, March 2024. *Zero trust networks: building secure systems in untrusted networks*. Beijing: O'Reilly. ISBN 978-1-492-09656-6
- ANDERSON, Ross, 2020. *Security engineering: a guide to building dependable distributed systems* [online]. Indianapolis: Wiley PDF e-Book. ISBN 978-1-119-64468-2, 978-1-119-64283-1. Available via: https://onlinelibrary.wiley.com/doi/book/10.1002/9781119644682.
- KAUFMAN, Charlie and others, 2023. *Network Security: private Communication in a Public World*. Boston ; Amsterdam ; London: Addison-Wesley. ISBN 978-0-13-664360-9, 0-13-664360-4

Additional remarks:

None

Principles of Computer Science and Programming

Module abbreviation:	SOC_PCSP	**SPO-No.:**	2
Curriculum:	**Program**	**Module type**	**Semester**
	Sociotechnical Cyber-security (SPO SS 26)	Einsetzungstext ist leer!	1
Module attribute:	**Language of instruction**	**Duration of module**	**Frequency of offer**
	English	1 semester	only winter term

Responsible for module:	Apel, Sebastian
Credit points / SWS:	8 ECTS / 4 SWS
Workload:	Contact hours: 0 h Self study hours: 0 h Total hours: 200 h
Subjects of the module:	Principles of Computer Science and Programming
Lecture types:	O - Online self-study course with support from a lecturer
Usability for other study programs:	None

Examinations:

schrP90 - written exam, 90 minutes

Requirements:
None

Prerequisites according examination regulation:

None

Recommended prerequisites:

None

Objectives:

Nach dem Besuch des Moduls sind die Studierenden in der Lage,

- die grundlegenden Konzepte einer objektorientierten Programmiersprache zu erklären und in Python-Programmen anzuwenden
- algorithmische Probleme zu analysieren und geeignete Datenstrukturen sowie Algorithmen auszuwählen und zu implementieren
- Software-Systeme mittels UML zu modellieren und aus Modellen lauffähigen Code zu entwickeln
- Design Principles (insbesondere SOLID) zu erklären und bei der Implementierung anzuwenden
- gängige Design Patterns zu erkennen, zu erklären und situationsgerecht einzusetzen
- den Zusammenhang zwischen Kohäsion, Kopplung und Wartbarkeit zu erläutern
- die praktische Anwendung der gelernten Inhalte in einem mittelgroßen Softwareprojekt nachzuweisen

Content:

- Fundamentals of programming (variables, data types, operators, control structures, functions, modules, exception handling, file I/O)

- Object-oriented programming (classes, objects, inheritance, polymorphism, abstract classes, special methods)
- Fundamentals of computer science (number systems, bit operations, encoding, Boolean logic, concept of algorithms)
- Data structures (lists, dictionaries, sets, stacks, queues, hash tables, trees, graphs) and algorithms (searching and sorting algorithms, recursion) including their complexity
- Memory management (stack vs. heap, garbage collection, pass-by-reference)
- Software modelling with UML (class diagrams, object diagrams, sequence diagrams, levels of abstraction in modelling)
- Design principles (including cohesion and coupling, SOLID principles) and design patterns (including creational patterns, structural patterns, behavioral patterns, architectural patterns)
- Advanced topics such as version control, testing frameworks and code quality (Git, unit testing, integration testing, code reviews, refactoring, code smells, technical debt)

Literature:

Will be specified at the beginning

Additional remarks:

None

Principles of Mathematics

Module abbreviation:	SOC_PM	**SPO-No.:**	3
Curriculum:	**Program**	**Module type**	**Semester**
	Sociotechnical Cyber-security (SPO SS 26)	Einsetzungstext ist leer!	1
Module attribute:	**Language of instruction**	**Duration of module**	**Frequency of offer**
	English	1 semester	only summer term

Responsible for module:	Roegner, Katherine
Credit points / SWS:	8 ECTS / 4 SWS
Workload:	Contact hours: 0 h Self study hours: 0 h Total hours: 200 h
Subjects of the module:	Principles of Mathematics
Lecture types:	O - Online self-study course with support from a lecturer
Usability for other study programs:	None

Examinations:

schrP90 - written exam, 90 minutes

Requirements:
None

Prerequisites according examination regulation:

None

Recommended prerequisites:

None

Objectives:

After successful completion of this module, students are able to …

- explain and apply fundamental concepts of number theory in the context of computer science and cybersecurity.
- analyse and apply basic cryptographic principles based on mathematical foundations.
- apply statistical methods to analyse data sets and interpret results in a scientifically sound manner.
- use formal logic (Boolean algebra and predicate logic) to model, analyse and evaluate statements and systems.
- model real-world problems using graph-theoretical concepts and select appropriate solution approaches.
- analyse properties of graphs, including trees, paths and circuits, and classify them formally.
- evaluate algorithmic approaches to graph problems (e.g. shortest paths, traveling salesman problem) with regard to correctness and complexity.
- represent graphs using suitable data structures (e.g. adjacency matrices) and apply these representations in practical contexts.
- transfer mathematical methods to applied problems in computer science and cybersecurity.

Content:

• Fundamentals of number theory
• Fundamentals of cryptography
• Fundamentals of statistics
• Logic including Boolean algebra and predicate logic
• Graph theory
  ○ Trees and forests
  ○ Eulerian circuits
  ○ Hamiltonian circuits
  ○ Traveling salesman problem
  ○ Dijkstra algorithm
  ○ Adjacency matrices
  ○ Applications of graph theory

Literature:
Will be specified at the beginning
Additional remarks:
None

Information and Product Security Management and Communication

Module abbreviation:	SOC_IPSMC	**SPO-No.:**	4
Curriculum:	**Program**	**Module type**	**Semester**
	Sociotechnical Cyber-security (SPO SS 26)	Einsetzungstext ist leer!	1,3
Module attribute:	**Language of instruction**	**Duration of module**	**Frequency of offer**
	English	1 semester	only summer term

Responsible for module:	Gmelch, Oliver
Credit points / SWS:	6 ECTS / 4 SWS
Workload:	Contact hours: 47 h Self study hours: 104 h Total hours: 151 h
Subjects of the module:	Information and Product Security Management and Communication
Lecture types:	SU/Ü - Seminar-based teaching with exercises
Usability for other study programs:	None

Examinations:

schrP90 - written exam, 90 minutes

Requirements:
None

Prerequisites according examination regulation:

None

Recommended prerequisites:

None

Objectives:

After successful completion of this module, students are able to …

- critically analyse and compare cybersecurity management frameworks and justify their application in different organisational and product contexts.
- design and evaluate cybersecurity governance structures within corporate environments, including roles, responsibilities and decision-making processes.
- develop and apply structured threat and risk models for complex socio-technical systems and derive evidence-based risk treatment strategies.
- analyse security- and risk-related data sets and translate results into meaningful management reports for technical and non-technical stakeholders.
- assess cybersecurity maturity using established maturity models and formulate targeted improvement roadmaps.
- design business continuity concepts and evaluate organisational resilience with regard to cyber-related disruption scenarios.
- plan and implement cybersecurity awareness strategies that are appropriate for different target groups and organisational cultures.

- manage cybersecurity incidents and crisis situations, including structured communication with internal and external stakeholders.
- design and evaluate product security management processes across the lifecycle of digital and cyber-physical products.

Content:

- Cybersecurity Management Frameworks (e.g., ISO 27001, NIST CSF)
- Cybersecurity in corporate governance
- Threat and Risk Modeling and Management
- Data Analysis for Risk and Security Management/Reporting
- Cybersecurity Maturity models
- Business Continuity Management
- Cybersecurity Awareness
- Crisis Communication & Incident Management
- Product Security Management

Literature:

- EDWARDS, Jason and Griffin WEAVER, 2024. *The cybersecurity guide to governance, risk, and compliance*. Hoboken, NJ: Wiley. ISBN 9781394250196, 1394250193
- TOKGOZ, Emre, 2026. *Six Sigma for Continuous Improvement in Cybersecurity: A Guide for Students and Professionals* [online]. Cham: Springer Nature Switzerland PDF e-Book. ISBN 978-3-031-91030-2. Available via: https://doi.org/10.1007/978-3-031-91030-2.

Additional remarks:

None

Human Factors

Module abbreviation:	SOC_HF	**SPO-No.:**	5
Curriculum:	**Program**	**Module type**	**Semester**
	Sociotechnical Cyber-security (SPO SS 26)	Compulsory Sub-ject	2
Module attribute:	**Language of instruction**	**Duration of module**	**Frequency of offer**
	English	1 semester	only winter term

Responsible for module:	Sturm, Christian
Credit points / SWS:	6 ECTS / 4 SWS
Workload:	Contact hours: 47 h Self study hours: 103 h Total hours: 150 h
Subjects of the module:	Human Factors
Lecture types:	SU/Ü - Seminar-based teaching with exercises
Usability for other study programs:	None

Examinations:

schrP90-120 written examination 90-120 minutes

Requirements:
None

Prerequisites according examination regulation:

None

Recommended prerequisites:

None

Objectives:

After active participation in the course, students can…

- …explain key principles from social sciences relevant to cybersecurity
- …use behavioral and cognitive frameworks to evaluate susceptibility to social engineering
- …analyze security incidents using cognitive, social, and anthropological perspectives
- …design behavior-change interventions
- …critically assess the ethical implications of influencing human behavior in cybersecurity

Self- and social competences:
Upon completion of the module, students

- …have acquired a high level of self-awareness and reflectivity of their own positionality, actions, and reactions in relation to manipulative behavior
- ...have gained experience in shifting their viewpoints to see both the victim's and the attacker's point of view in relation to cybersecurity incidents
- ...can lead a discourse on measurements to mitigate human vulnerabilities to cyber attacks

Content:

- Foundations of human factors in cybersecurity
- Cognitive biases in security decision-making
- Attention, perception, and cognitive load
- Memory, learning, and habit formation
- Risk perception and threat Assessment
- Human error
- Embodied cognition
- Psychology of deception and social engineering
- Nudging
- Privacy and trust
- Cultural models of trust and authority
- Cross-cultural aspects of cybersecurity
- Research methods in human factors

Literature:

- EYSENCK, Michael W., 2022. *Simply psychology*. London ; New York: Routledge. ISBN 978-0-367-60785-2, 978-0-367-55015-8
- SINGH, Tarnveer, 2025. *Cybersecurity, Psychology and People Hacking* [online]. Cham: Springer Nature Switzerland PDF e-Book. ISBN 978-3-031-85994-6. Available via: https://doi.org/10.1007/978-3-031-85994-6.
- CARTWRIGHT, Edward, 2024. *Behavioral economics*. London ; New York: Routledge. ISBN 978-1-032-41410-2, 978-1-032-41412-6

Additional remarks:

None

Project Sociotechnical Cybersecurity Engagement - Preparation

Module abbreviation:	SOC_SCE_PREP	**SPO-No.:**	7
Curriculum:	**Program**	**Module type**	**Semester**
	Sociotechnical Cyber-security (SPO SS 26)	Compulsory Sub-ject	2
Module attribute:	**Language of instruction**	**Duration of module**	**Frequency of offer**
	German	1 semester	only winter term

Responsible for module:	Hof, Hans-Joachim
Credit points / SWS:	2 ECTS / 1 SWS
Workload:	Contact hours: 12 h Self study hours: 38 h Total hours: 50 h
Subjects of the module:	Project Sociotechnical Cybersecurity Engagement - Preparation
Lecture types:	Proj - project
Usability for other study programs:	None

Examinations:

Proj - project work (5-25 pages) with oral presentation (5-15 pages)

Requirements:
None

Prerequisites according examination regulation:

None

Recommended prerequisites:

None

Objectives:

After successful completion of this module, students are able to …

- develop a coherent project idea in the field of sociotechnical cybersecurity with a clear societal or community-oriented benefit.
- justify the relevance and feasibility of the project in relation to ethical, social and professional responsibilities in cybersecurity.
- identify relevant stakeholders and analyse their roles, interests and influence on the project.
- initiate professional communication with stakeholders and establish initial cooperation.
- define project objectives, scope and success criteria in coordination with the supervising professor.
- develop a structured project plan including milestones, responsibilities and timeline.
- reflect on the honorary and non-profit character of the project and align their work accordingly.

Content:

- Development of a honorary, non-profit project idea in the area of cybersecurity, ideally with high social or technical impact
- Alignment of project idea with supervising professor

- Stakeholder identification and analysis
- Communication with internal and external stakeholders
- Definition of project goals and success criteria
- Project planning and structuring
- Ethical aspects of non-profit cybersecurity engagement
- Documentation of the project concept and plan

Literature:

- SCHÜSSLER, Anne and Peter SCHÜSSLER, 2020. *Weniger schlecht Projekte managen: ohne Krise zum Projekterfolg*. Heidelberg: O'Reilly. ISBN 978-3-96010-195-6

Additional remarks:

None

Seminar Medical Cybersecurity

Module abbreviation:	SOC_MED	**SPO-No.:**	9
Curriculum:	**Program**	**Module type**	**Semester**
	Sociotechnical Cyber-security (SPO SS 26)	Compulsory Sub-ject	2
Module attribute:	**Language of instruction**	**Duration of module**	**Frequency of offer**
	German	1 semester	only winter term

Responsible for module:	Hof, Hans-Joachim
Credit points / SWS:	6 ECTS / 4 SWS
Workload:	Contact hours: 47 h Self study hours: 104 h Total hours: 151 h
Subjects of the module:	Seminar Medical Cybersecurity
Lecture types:	S - seminar
Usability for other study programs:	None

Examinations:

Seminar paper 10–20 pages, presentation 15–20 minutes

Requirements:
None

Prerequisites according examination regulation:

None

Recommended prerequisites:

None

Objectives:

After successful completion of the module, students are able to …

- independently acquire advanced subject-specific knowledge in the field of medical cybersecurity by researching, analysing and synthesising relevant academic literature and deriving well-founded conclusions.
- structure complex topics in medical cybersecurity and present them clearly and appropriately in an oral presentation using suitable media.
- critically follow and reflect on academic presentations in medical cybersecurity and engage in well-founded subject-related discussion with the presenters.
- apply and further develop their communicative and transferable skills, in particular argumentation, academic discourse and constructive feedback.
- present the content of their work in the form of a concise written academic report in a clear, structured and comprehensible manner.

Content:

- Literature review on a topic assigned by the lecturer (by allocation or selection) in the area of medical cybersecurity

- Independent research and analysis of relevant academic sources
- Writing a scientific paper on the selected topic
- Preparation of an academic presentation on the topic
- Presentation of results in the seminar
- Active participation in structured discussions
- Moderation of discussions by the lecturer based on prepared guiding questions

Literature:

- HERING, Heike, 2025. *How to Write Technical and Scientific Reports: Understandable Structure, Good Design, Convincing Presentation* [online]. Berlin, Heidelberg: Springer Berlin Heidelberg PDF e-Book. ISBN 978-3-662-69773-3. Available via: https://doi.org/10.1007/978-3-662-69773-3.
- GASTEL, Barbara, 2024. *How to write and publish a scientific paper* [online]. PDF e-Book. ISBN 978-1-009-47753-6.

Additional remarks:

None

Industrial and IoT Cybersecurity

Module abbreviation:	SOC_IIC	**SPO-No.:**	10
Curriculum:	**Program**	**Module type**	**Semester**
	Sociotechnical Cybersecurity (SPO SS 26)	Compulsory Subject	2
Module attribute:	**Language of instruction**	**Duration of module**	**Frequency of offer**
	English	1 semester	only winter term

Responsible for module:	Wamser, Markus
Credit points / SWS:	6 ECTS / 4 SWS
Workload:	Contact hours: 47 h Self study hours: 104 h Total hours: 151 h
Subjects of the module:	Industrial and IoT Cybersecurity
Lecture types:	SU/Ü - Seminar-based teaching with exercises
Usability for other study programs:	None

Examinations:

LN

Requirements:
None

Prerequisites according examination regulation:

LN of serial nos. 1, 2 and 3

Recommended prerequisites:

None

Objectives:

After successful completion of this module, students are able to …

- analyse cybersecurity challenges specific to industrial and IoT systems under resource, timing and reliability constraints.
- evaluate the suitability of lightweight cryptographic algorithms and protocols for constrained devices and environments.
- design security concepts that explicitly consider energy efficiency, computational limitations and real-time requirements.
- analyse complex security architectures for operational technology environments and distinguish them from classical IT architectures.
- assess the interaction between cybersecurity, system availability and functional safety in industrial systems.
- evaluate security risks and attack surfaces in cyber-physical systems and industrial control architectures.
- analyse the security implications of edge computing architectures in industrial and IoT environments.

- evaluate decentralised approaches such as federated learning and blockchain for trust, integrity and resilience in industrial systems.
- apply security principles to realistic industrial and IoT architectures and derive justified design decisions.

Content:

- Characteristics and constraints of industrial and IoT systems
  - Resource constraints in embedded and cyber-physical systems
  - Lightweight cryptography for constrained environments
  - Energy-efficient security mechanisms
  - Efficient security protocols for IoT and industrial communication
- Advanced principles for complex security architectures in operational technology
  - Differences between IT security architectures and OT security architectures
  - Security architectures for industrial control systems
  - Real-time requirements and their impact on cybersecurity mechanisms
  - Availability, resilience and safety as design constraints for security
- Threat models for industrial and IoT environments
  - Attack surfaces in cyber-physical systems
  - Secure communication in industrial networks
- Edge computing architectures in industrial systems
  - Security for edge-based data processing and analytics
  - Federated learning in industrial and IoT environments
- Blockchain technologies for trust and integrity in industrial systems

Literature:

- KNAPP, Eric D., 2024. *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*. Chantilly: Elsevier Science & Technology Books. ISBN 978-0-443-13738-9
- MACAULAY, Tyson and Bryan SINGER, 2012. *Cybersecurity for industrial control systems: SCADA, DCS, PLC, HMI, and SIS*. Boca Raton: CRC Press. ISBN 978-1-4398-0198-7, 1-4398-0198-3
- MARTIN , Keith M. , 2025. *Everyday Cryptography: Fundamental Principles and Applications*. ISBN 978-0198903284

Additional remarks:

None

Cybersecurity for Mobility Systems

Module abbreviation:	SOC_MOS	**SPO-No.:**	11
Curriculum:	**Program**	**Module type**	**Semester**
	Sociotechnical Cyber-security (SPO SS 26)	Compulsory Sub-ject	2
Module attribute:	**Language of instruction**	**Duration of module**	**Frequency of offer**
	English	1 semester	only winter term

Responsible for module:	Hof, Hans-Joachim
Credit points / SWS:	6 ECTS / 4 SWS
Workload:	Contact hours: 47 h Self study hours: 104 h Total hours: 151 h
Subjects of the module:	Cybersecurity for Mobility Systems
Lecture types:	SU/Ü - Seminar-based teaching with exercises
Usability for other study programs:	None

Examinations:

PF - Portfolio-Exam (all exams before the examination period)

Requirements:
None

Prerequisites according examination regulation:

LN of serial nos. 1, 2 and 3

Recommended prerequisites:

None

Objectives:

After successful completion of this module, students are able to …

- analyse and evaluate the interplay and potential conflicts between security and safety in safety-critical mobility systems.
- design security concepts for complex cyber-physical and safety-critical systems such as connected and autonomous vehicles.
- analyse architectures and attack surfaces of V2X systems and distributed automotive platforms.
- evaluate advanced threats against embedded systems and apply suitable protection mechanisms.
- design and assess secure software update mechanisms for safety-critical and highly regulated environments.
- assess risks arising from system complexity, interconnectivity and real-time constraints in mobility systems.
- apply relevant standards and regulatory frameworks (e.g. ISO 21434, UNECE R155/R156) to concrete technical scenarios.
- analyse incidents and real-world case studies from the automotive and mobility domain and derive lessons learned.

- develop holistic security architectures that integrate embedded security, communication security and system safety.

Content:

- Advanced Principles of Security & Safety for Mobility Systems
  - Architectures of connected and autonomous mobility systems
  - Attack surfaces in modern vehicle architectures
  - Interaction and conflicts between safety and security
- Complex Distributed Systems in V2X environments
  - Vehicle-to-everything communication technologies
  - Threat models for V2X and autonomous driving
  - Cybersecurity controls for V2X environments
- Advanced Embedded Systems Security
  - Hardware security for embedded systems
  - Secure boot and trusted execution environments
  - Cryptographic mechanisms in automotive ECUs
  - Secure communication in in-vehicle networks
- Security of Software-updates for safety-critical systems
  - Over-the-air update mechanisms and their trust models
  - Security testing for automotive and embedded systems
- Automotive cybersecurity standards and regulations (ISO 21434 and UNECE R155/R156)

Literature:

- MERLI, Dominik, 2024. *Engineering secure devices: a practical guide for embedded system architects and developers*. San Francisco: No Starch Press. ISBN 978-1-7185-0348-9
- OKA, Dennis Kengo, 2021. *Building secure cars: assuring the automotive software development lifecycle* [online]. Hoboken, NJ: John Wiley & Sons PDF e-Book. ISBN 1119710766, 1119710774. Available via: https://onlinelibrary.wiley.com/doi/book/10.1002/9781119710783.

Additional remarks:

None

Sociotechnical Systems

Module abbreviation:	SOC_SOS	**SPO-No.:**	12
Curriculum:	**Program**	**Module type**	**Semester**
	Sociotechnical Cyber-security (SPO SS 26)	Compulsory Sub-ject	3
Module attribute:	**Language of instruction**	**Duration of module**	**Frequency of offer**
	English	1 semester	only winter term

Responsible for module:	Sturm, Christian
Credit points / SWS:	6 ECTS / 4 SWS
Workload:	Contact hours: 47 h Self study hours: 103 h Total hours: 150 h
Subjects of the module:	Sociotechnical Systems
Lecture types:	SU/Ü - Seminar-based teaching with exercises
Usability for other study programs:	None

Examinations:

schrP90-120 written examination 90-120 minutes

Requirements:
None

Prerequisites according examination regulation:

None

Recommended prerequisites:

None

Objectives:

After active participation in the course, students can…

- … explain core principles of socio-technical systems theory and STS frameworks in relation to cybersecurity
- …describe how cybersecurity is based on interactions between human actors, technical infrastructures, organizational structures, and cultural context
- …design cybersecurity interventions (policies, controls, tools, or processes) that reflect whole-system understanding rather than technical enforcement alone
- …use participatory design approaches and stakeholder-inclusive development processes to improve system security and adoption
- …reflect on cybersecurity as an emergent property of complex adaptive socio-technical systems

Self- and social competences:
Upon completion of the module, students

- …engage stakeholders and end-users in analysis and development processes
- ...communicate complex cybersecurity topics clearly across disciplinary boundaries
- ...reflect upon societal, human, and organizational consequences of security decisions

Content:

- Sociotechnical systems foundations
- Human-centered development of secure systems
- User experience research, design and principles
- Usability engineering
- Usable security, privacy, and secure UX design
- Resilience
- Sociotechnical risk and resilience engineering
- Distributed cognition and team-based security
- Sociotechnical accidents and failures
- Technology adoption models
- Human-machine teaming in cybersecurity
- Artificial Intelligence in sociotechnical systems for cybersecurity

Literature:

- AHRENS, Volker, 2025. *Systems Engineering & Management: A generic approach to the design and control of socio-technical systems* [online]. Wiesbaden: Springer Fachmedien Wiesbaden PDF e-Book. ISBN 978-3-658-46875-0. Available via: https://doi.org/10.1007/978-3-658-46875-0.
- CRANOR, Lorrie Faith, 2005. *Security and usability: designing secure systems that people can use*. Beijing [u.a.]: O'Reilly. ISBN 0-596-00827-9, 978-0-596-00827-7
- STALLINGS, William, 2020. *Information privacy engineering and privacy by design: understanding privacy threats, technology, and regulations based on standards and best practices*. Boston, Mass.: Addison-Wesley. ISBN 978-0-13-530215-6
- LAZAR, Jonathan, FENG, Jinjuan Heidi, HOCHHEISER, Harry, 2017. *Research methods in human-computer interaction* [online]. Cambridge, MA: Morgan Kaufmann Publishers, an imprint of Elsevier PDF e-Book. ISBN 978-0-12-809343-6. Available via: https://doi.org/10.1016/B978-0-12-805390-4.09991-X.

Additional remarks:

None

Global Cybersecurity Strategy and Business

Module abbreviation:	SOC_CSB	**SPO-No.:**	13
Curriculum:	**Program**	**Module type**	**Semester**
	Sociotechnical Cyber-security (SPO SS 26)	Compulsory Sub-ject	3
Module attribute:	**Language of instruction**	**Duration of module**	**Frequency of offer**
	English	1 semester	only winter term

Responsible for module:	Hof, Hans-Joachim
Credit points / SWS:	6 ECTS / 4 SWS
Workload:	Contact hours: 47 h Self study hours: 103 h Total hours: 150 h
Subjects of the module:	Global Cybersecurity Strategy and Business
Lecture types:	SU/Ü - Seminar-based teaching with exercises
Usability for other study programs:	None

Examinations:

LN

Requirements:
None

Prerequisites according examination regulation:

None

Recommended prerequisites:

None

Objectives:

After successful completion of this module, students are able to …

- design comprehensive cybersecurity strategies aligned with organisational goals and global risk environments.
- analyse business implications of cybersecurity, including economic trade-offs, investment decisions and value contribution.
- assess and manage cybersecurity risks in complex global supply chains.
- apply methods for cybersecurity trend scouting and threat intelligence to anticipate emerging risks and technologies.
- define, select and interpret meaningful cybersecurity KPIs for management decision-making.
- communicate cybersecurity topics effectively using storytelling techniques for different stakeholder groups.
- shape cybersecurity leadership practices and foster a sustainable cybersecurity culture within organisations.
- plan and implement stakeholder engagement and advocacy strategies in cybersecurity contexts.
- design and evaluate concepts for internal and external cybersecurity community building.

Content:

- Cybersecurity strategy development
- Business implications of cybersecurity and cybersecurity economics
- Supply chain security for global supply chains
- Methods for cybersecurity trend scouting and threat intelligence
- Cybersecurity KPIs
- Storytelling for cybersecurity
- Leadership in cybersecurity and cybersecurity culture including stakeholder engagement and advocacy
- Cybersecurity community building internal and external

Literature:

- TARUN, Renee, 21. *Fight Fire with Fire: Proactive Cybersecurity Strategies for Today's Leaders*. ISBN 978-1119854272
- TRIM, Peter, . *Cyber Security Management and Strategic Intelligence* . ISBN 978-1032944661
- CARNOVALE, Steven, YENIYURT, Sengun, ©2021. *Cyber security and supply chain management: risks, challenges and solutions* [online]. New Jersey ; London ; Singapore ; Beijing ; Shanghai ; Hong Kong ; Taipei ; Chennai ; Tokyo: World Scientific PDF e-Book. ISBN 978-981-1233-12-8, 981-1233-12-8. Available via: https://doi.org/10.1142/12140.
- WILHOIT, Kyle and Joseph OPACKI, 2022. *Operationalizing Threat Intelligence: A guide to developing and operationalizing cyber threat intelligence programs*. First publishe: June 2022. edition. Birmingham, Mumbai: Packt. ISBN 978-1-80181-468-3

Additional remarks:

None

Advanced Cybersecurity

Module abbreviation:	SOC_ACybSec	**SPO-No.:**	14
Curriculum:	**Program**	**Module type**	**Semester**
	Sociotechnical Cyber-security (SPO SS 26)	Compulsory Sub-ject	3
Module attribute:	**Language of instruction**	**Duration of module**	**Frequency of offer**
	English	1 semester	only summer term

Responsible for module:	Hutzelmann, Thomas
Credit points / SWS:	6 ECTS / 4 SWS
Workload:	Contact hours: 47 h Self study hours: 103 h Total hours: 150 h
Subjects of the module:	Advanced Cybersecurity
Lecture types:	SU/Ü - Seminar-based teaching with exercises
Usability for other study programs:	None

Examinations:

schrP120 - written exam, 120 minutes

Requirements:
None

Prerequisites according examination regulation:

LN of serial nos. 1, 2 and 3

Recommended prerequisites:

None

Objectives:

After successful completion of this module, students are able to …

- analyse advanced cryptographic methods and assess their applicability in future cybersecurity architectures.
- evaluate post-quantum cryptography, quantum key exchange and privacy-preserving cryptographic techniques with regard to real-world deployment.
- assess the impact of emerging cryptographic technologies on application domains such as mobility, industrial systems and healthcare.
- apply formal methods such as model checking, abstract interpretation and formal verification to analyse the security properties of systems.
- evaluate the strengths and limitations of formal methods for different cybersecurity problem classes.
- analyse and design approaches for using artificial intelligence in cybersecurity applications such as detection, classification and response.
- assess risks, limitations and trustworthiness of AI-based security mechanisms.
- evaluate future cybersecurity trends and their implications for existing architectures, standards and infrastructures.

- transfer advanced cybersecurity concepts into concrete design recommendations for complex socio-technical systems.

Content:

- Advanced cryptographic primitives and protocols
  - Post-quantum cryptography
  - Quantum key distribution and quantum key exchange
  - Zero-knowledge proofs and privacy-preserving authentication
  - Homomorphic encryption and secure computation
  - Integration of advanced cryptography into real-world systems
- Formal methods for cybersecurity
  - Model checking for security properties
  - Abstract interpretation and static security analysis
  - Formal verification of protocols and systems
  - Limitations and challenges of formal methods
- Artificial intelligence for cybersecurity
  - Machine learning for intrusion detection and anomaly detection
  - Automated vulnerability discovery using AI
  - Threat intelligence supported by AI
  - Security challenges of AI-based security systems
- Technology foresight in cybersecurity
  - Impact of emerging technologies on application domains
- Case studies from mobility, industry and healthcare

Literature:

- KATZ, Jonathan and Yehuda LINDELL, 2025. *Introduction to modern cryptography*. Boca Raton ; London ; New York: CRC Press, Taylor & Francis Group. ISBN 978-1-040-36650-9
- TAKAGI, Tsuyoshi, WAKAYAMA, Masato, KUNIHIRO, Noboru, TANAKA, Keisuke, KIMOTO, Kazufumi, KUDO, Momonari, 2026. *Mathematical Foundations for Post-Quantum Cryptography: Crypto-Math CREST* [online]. Singapore: Springer Nature Singapore PDF e-Book. ISBN 978-981-9612-18-5. Available via: https://doi.org/10.1007/978-981-96-1218-5.

Additional remarks:

None

Master Thesis

Module abbreviation:	SOC_MAT	**SPO-No.:**	16
Curriculum:	**Program**	**Module type**	**Semester**
	Sociotechnical Cyber-security (SPO SS 26)	Compulsory Sub-ject	
Module attribute:	**Language of instruction**	**Duration of module**	**Frequency of offer**
	German	1 semester	only winter term

Responsible for module:	Hof, Hans-Joachim
Credit points / SWS:	30 ECTS / 0 SWS
Workload:	Contact hours: 0 h Self study hours: 750 h Total hours: 750 h
Subjects of the module:	16.1: Master Thesis 16.2: Master Thesis Colloquium
Lecture types:	16.1: MA - Master's Thesis 16.2: MA - Master's Thesis
Usability for other study programs:	None

Examinations:

16.1: Master-Thesis
16.2: Colloquium

Requirements:
None

Prerequisites according examination regulation:

None

Recommended prerequisites:

None

Objectives:

After successful completion of the Master's thesis, including the colloquium, students are able to …

- independently analyse a complex academic problem and systematically address it using appropriate scientific methods.
- critically evaluate requirements, alternative solution approaches and their own solution concepts, and present the results in a clearly structured, academically convincing and comprehensible written thesis.
- independently plan a comprehensive and demanding task and successfully complete it within the specified timeframe through effective time and self-management.
- present the results of their Master's thesis clearly, precisely and appropriately to the audience in an academic colloquium.
- critically reflect on subject-related questions during the colloquium, respond to them in a well-founded manner, and defend their own results with sound arguments.

Content:
• Independent work on a complex academic research question within the subject area of the degree programme • Application of scientific methods and research practices • In-depth study within the thematic focus of the thesis • Project planning and time management • Identification of the thesis topic and coordination with the primary examiner • Preparation of a thesis proposal (exposé) to structure the research project • Written documentation of the results • Presentation and defence in the colloquium
Literature:
Will be specified at the beginning
Additional remarks:
None