Technical University of Applied Sciences Augsburg

Faculty of Electrical Engineering

Master Program

Industrial Safety and Security (M.Sc.)

Module Catalogue

WiSe 2025/26

created: September 29, 2025

Table of Contents **Page**

C.2 Required Elective Modules 2

D Master's Thesis

Automation	
ID	AUT
Study section	MEE, MME: Catalogue I MIS: Crossover
Responsible lecturer	Prof. Dr. Benjamin Danzer
Mandatory/elective	Elective
Rotation	Summer term, annually
Duration	1 term
Course	Automation
CP / SWS	5 CP, 4 SWS
Workload	Total 5 CP x 25 h = 125 h thereof attendance 47 h, self-study 78 h
Study/Examination Performance	according to Syllabus and Examination Regulations and Record of Examinations Schedule
Marking	according §20 APO in its relevant version
Prerequisites	none
Applicability	Module to obtain essential credit points
Teaching language	English
Teaching/Learning method	Seminar-like lecture, exercise

Automation

Contents	- Petri Net basics, timed models, application in programming tools for programmable controllers. - Introduction to stochastic systems, discrete- and continuous-time Markov chains. - Review of the programming concept for PLCs according to the norm IEC 61131-3. - Connectivity between SoftPLCs, Input/Output devices and commercial applications, e.g. visualisation based on OPC or industrial ethernet. - Design and verification of safety related programmable control systems according to European standards. - Modelling of nonlinear characteristics of temperature, magnetic, optic and chemical sensors. - Modelling of dynamic effects and limitations of sensors, e.g. cut-off frequency and parasitic elements

Automation

Module objectives

Learning outcomes

- Become familiar with discrete event systems as the basis for modelling automation problems.
- Be able to treat random effects in automation problems.
- Perceive the principles of PLC networks.
- Understand the principles and limitations of sensors and sensor systems.

Knowledge Targets

- Use simulation software to analyse the behaviour of a discrete event system.
- Use PLC programming tools based on a graphical description of a discrete event system.
- Configure a network of Programmable Logic Controllers connected via fieldbus and /or Ethernet.
- Develop controller software according to the rules of IEC 61131-3.
- Simulate sensors and circuits (e.g. with PSPICE or LabView)
- Analyze data sheets & select appropriate components for automation & control systems

Capabilities

- Appreciate the value of formal description methods as the basis for problem solving.
- Know the benefits and limitations of simulation as an engineering tool.
- Perform effectively within a group in the conduct of a practical project.

Automation

Literature

- Cassandras, Lafortune: Introduction to Discrete Event Systems, Kluwer Academic Press 1999
- David, Alla: Discrete, Continuous and Hybrid Petri Nets, Springer 2005
- Tornambe: Discrete-Event System Theory, World Scientific 1995
- John, Tiegelkamp: IEC 61131-3: Programming Industrial Automation Systems, Springer 2010
- Iwanitz, Lange, Burke: OPC : From Data Access to Implementation and Application, Hüthig 2010
- Hauke, et al.: Functional safety of machine controls -- Application of EN ISO 13849, DGUV 2009
- Fitzpatrick: Analogue Design and Simulation Using Orcad Capture and Pspice, Newnes 2011
- Bishop: LabVIEW 2009 Student Edition, Prentice Hall 2009

Data Communication	
ID	IS1C1
Study section	Crossover
Responsible lecturer	Prof Dr Rolf Winter
Mandatory/elective	Elective
Rotation	Summer semester, annually
Duration	1 semester
Course	Data communication
CP / SWS	5 CP, 4 CREDIT HOURS
Workload	Total workload 5 CP x 25 h = 125 h of which attendance time 45 h, self-study 79 h, examination time 1 h
Study/Examination Performance	according to SPO and list of course assessments
Marking	according to §20 of the APO in the currently valid version
Prerequisites	none
Applicability	Required elective module to obtain the necessary credit points according to the SPO
Teaching language	German
Teaching/Learning method	Seminar-based teaching, exercise course

Data Communication	
Contents	The lecture introduces the functioning and structure of the internet, taking into account the architecture of the internet, its principles and the key protocols used. It deals in particular with - Application layer protocols (such as HTTP and DNS) - Transport protocols (such as TCP and UDP) - Routing protocols (link state and distance vector) - protocols of the data link layer (e.g. Ethernet and WLAN) - Operation of core components of the Internet (switches, CDNs, NAT, etc.) - Key principles of the Internet (reliable data transmission, congestion control, etc.) - Use of standard tools (software) in the field of networks
Module objectives	Students know the key protocols of the Internet and can explain their tasks and functionality in detail. They know which functions of the Internet architecture are implemented how and where in the network. Students can also describe the complex relationships between protocols and mechanisms on the Internet. In addition, students can apply the knowledge they have learnt in practice when developing networked applications or setting up and maintaining networks. The internship / lab course enables students to use standard tools to analyse and set up applications and networks.
Literature	Computer Networking: A Top-Down Approach, Global Edition Taschenbuch -- Internationale Ausgabe, 10. Juni 2021, 8th Edition

Human Recource and Organisation Management	
Kürzel	MIS1C6
Study section	Crossover
Responsible lecturer	Prof. Dr. Carolin Palmer
Mandatory/elective	Elective
Rotation	Summer term, annually
Duration	1 term
Course	Human Recource and Organisation Management
CP / SWS	5 CP (3 CP lecture + 2 CP project work), 4 SWS
Workload	Total 5 CP x 25 h = 125 h therof attendance 30 h, self-study 94 h, exam 1,0 h
Study/Examination Performance	according to Syllabus and Examination Regulations and Record of Examinations Schedule
Marking	according §20 APO in its relevant version
Prerequisites	none
Applicability	Module to obtain essential credit points
Teaching language	English
Teaching/Learning method	Seminar-like lecture, exercise
Contents	- Organisational Management Orientations - Organisational Diagnosis and Design Theories - Organisational Development & Transformation - Organisational Behaviour & Leadership - Organisation of Talent Management - Organisation of Innovation & Performance Management

Human Recource and Organisation Management

Module objectives

The students shall

- Understand management and leadership tasks of industrial engineers related to teams, individual staff, peers and further stakeholders.
- Be aware of the interdependency of organizational culture, strategy, processes, technology and structure.
- Differentiate current management orientations, e.g. hybrid organisations, purpose driven organisations, etc.
- Understand different approaches to leadership.
- Know the main tasks of Talent Management as well as how to support innovation and performance of individuals and teams.

The students will

- Establish fundamentals of organisational diagnosis and design based on the socio-technical theory.
- Know and explain theoretical concepts from organizational and behavioral sciences with respect to different task contexts in organisations.
- Identify different needs for organisational transformation and know theoretical concepts of change management.
- Know the main attributes and assumptions underlying innovation and performance management
- Discuss where their future responsibilies as Industrial Engineers within Talent Management may lie.

The students are able to

- Analyse case studies of specific organizational challenges and propose solutions for improved outcomes
- Combine theoretical concepts of organizational and behavioral sciences in order to solve real life tasks of industrial engineers with leadership responsibility.
- Discuss and reflect upon different approaches for promoting innovation and performance.
- Reflect upon behavioural options for leadership tasks and roles in promoting talent development.

Human Recource and Organisation Management

Literature	- Scripts by lecturer - Daft, R. L., Murphy, J.; Wilmott, H. (2020) Organization Theory and Design: An International Perspective. 4th edition. Cengage - Waddel, D. M.; Creed, A.; Cummings T. G.; Worley, C.G. (2019) Organisational Change: Development and Transformation. Cengage.

Industrial Plants, Automation and Control	
ID	IS1C3
Study section	Crossover
Responsible lecturer	Prof Dr Wolfgang Zeller
Mandatory/elective	Elective
Rotation	Summer term
Duration	1 semester
Course	Industrial Plants, Automation and Control
CP / SWS	5 CP, 4 CREDIT HOURS
Workload	Total workload 5 CP x 25 h = 125 h of which attendance time 45 h, self-study 80 h
Study/Examination Performance	according to SPO and list of course assessments
Marking	according to §20 of the APO in the currently valid version
Prerequisites	none
Applicability	Module for obtaining the necessary credit points according to SPO
Teaching language	German
Teaching/Learning method	Seminar-based teaching, exercise course

Industrial Plants, Automation and Control

Contents

Introduction to industrial plants, automation and control technology

- Origin, current significance, objectives, requirements
- Mechanical, fluidic and electrical control systems

Functions and components of control technology

- Electronic programmable control systems
- Interfaces between process and control system
- Application of industrial communication systems
- Fieldbus systems and industrial Ethernet-based communication systems
- Operation and monitoring
- Control centre technology and production data acquisition

Programming concepts and standardised PLC programming languages

- Basic language elements of textual and graphical programming languages
- Organisation of PLC programs and control system design

Methods and tools for handling control software and mastering the complexity of control systems

- Software development for industrial applications
- Commissioning, service and maintenance of control systems

Industrial Plants, Automation and Control

Module objectives

Knowledge:

- Students are familiar with the special features of controlling discrete-event systems and the basic components of automation technology.
- They can explain industrial communication systems and automation technology components for operating, monitoring and diagnosing technical processes.

Skills:

- Students can plan industrial control systems according to the given assignment and the given purpose.
- They can assess industrial control systems from a technical and economic point of view.
- They can create PLC programs using modern methods of software development on the basis of standardised programming languages.

Competences:

- They can select the most suitable automation components and PLC programming languages for the overall technical and organisational context and argue for their selection.
- Students can independently assess automation technology problems.
- They are able to obtain information from provided sources and to critically and comparatively assess them in written form.

Industrial Plants, Automation and Control

Literature	- Scriptum - Wellenreuther, G; Zastrow, D.: Automatisieren mit SPS -- Theorie und Praxis, 6. Auflage, Springer Vieweg 2015. ISBN 978-3834825971 - Seitz, M.: Speicherprogrammierbare Steuerungen in der Industrie 4.0: Objektorientierter System- und Programmentwurf, Motion Control, Sicherheit, Industrial IoT. 5. Aufl. Hanser. München 2021. ISBN: 978-3446465794 (e-book in Bibliothek) - John, K. H. u. Tiegelkamp, M.: IEC 61131-3: Programming Industrial Automation Systems: Concepts and Programming Languages, Requirements for Programming Systems, Decision-Making Aids, 2nd edition, Springer, 2014. ASIN: B01G0M6HU8 - norms - software packages

Data Literacy and Business Intelligence	
ID	IS1C3
Study section	Crossover
Responsible lecturer	Prof Dr Peter Richard
Mandatory/elective	Elective
Rotation	Summer and winter semester, annually (starting winter term 2025/26)
Duration	1 semester
Course	Data Literacy and Business Intelligence
CP / SWS	5 CP, 4 CREDIT HOURS
Workload	Total workload 5 CP x 25 h = 125 h of which attendance time 60 h, self-study 63.5 h, examination time 1.5 h
Study/Examination Performance	according to SPO and list of course assessments
Marking	according to §20 of the APO in the currently valid version
Prerequisites	none
Applicability	Module for obtaining the necessary credit points according to SPO
Teaching language	German
Teaching/Learning method	Seminar-based teaching, exercise course

Data Literacy and Business Intelligence

Contents	- In the first seminar block, students are taught the basics of data literacy. - As part of analyses with BI tools, students prepare evaluations and scrutinise the results. - The aim is to create an awareness of the complexity of data sources, analyses and interpretation. - Students discuss the degree of digitalisation and data literacy in their various companies based on predefined topics and reflect on the differences. - The reflection is supplemented by guest lectures and further exercise courses on BI tools.

Data Literacy and Business Intelligence

Module objectives	The overarching aim of this seminar is to strengthen and develop the participants' basic data skills The development towards a digital society is evident at a political level through the German government's political level through the German government's data strategy and the Berlin Declaration on the Digital Society. This development means that data skills are necessary for everyone in this increasingly digitalised world. The need for these skills is underlined by the Data Literacy Charter, which emphasises data skills as an important part of education. Students should be able to make decisions based on data and, on the other hand, recognise the risks of misinterpreting data. Data skills are deepened through topics in the field of business intelligence. Here, data is processed, visualised and interpreted using business intelligence tools. The teaching is independent of a specific business administration specialism. **Knowledge** Students know and understand - basic statistical knowledge in the interpretation of data - typical distortions in the interpretation of data - areas of application of business intelligence **Skills** Students are able to - interpret data with a neutral view - Critically separate data and interpretation of data - create decision proposals based on data - implement simple data pipelines - create authorisation concepts **Competences** The students can - gain interdisciplinary insights from data - analyse data in a team - critically assess and interpret data

Data Literacy and Business Intelligence

Literature	- Densmore, James: Data Pipelines. Pocket Reference. Moving and Processing Data for Analytics, Beijing u. a.: O'Reilly, 2021. - Foreman, John W.: Data Smart. Using Data Science to Transform Information into Insight, Indianapolis and simultaneously in Canada: Wiley, 2013. - Lang, Michael (Hrsg.): Handbuch Business Intelligence. Potenziale, Strategien und Best Practices, Düsseldorf: Symposion, 2015.

IT Security	
ID	ISCO.ITSICH
Study section	Crossover
Responsible lecturer	Prof Lothar Braun
Mandatory/elective	Compulsory
Rotation	Winter and summer semester, annually
Duration	1 semester
Course	IT Security
CP / SWS	5 CP, 4 CREDIT HOURS
Workload	Total workload 5 CP x 25 h = 125 h of which attendance time 45 h, self-study 80 h
Study/Examination Performance	according to SPO and list of course assessments
Marking	according to §20 of the APO in the currently valid version
Prerequisites	none
Applicability	Module for obtaining the necessary credit points according to SPO
Teaching language	German
Teaching/Learning method	Seminar-based teaching, exercise course
Contents	The course provides an overview of the sub-areas of IT Security from a user's perspective. This includes relevant standards, typical attacks, security processes and the analysis of threats and risks. Cryptographic building blocks such as encryption, signatures and hash functions are introduced from the perspective of the programmer/user. Fundamental aspects of the security of embedded systems, networks and web applications are discussed.

IT Security	
Module objectives	After successfully completing the module, students will be able to - explain basic concepts of IT Security. - describe typical attacks. - apply the methodology of threat and risk analysis to a simple scenario. - present the basics of cryptographic algorithms. - implement simple cryptographic applications. - analyse simple security features of networks, devices and web applications. - plan simple security measures for networks, devices and web applications.
Literature	will be announced in the lecture

Industrial Security Basics	
Kürzel	ISB
Modulbereich	EIT, ME: Vertiefungsphase IWI: Vertiefungsmodule Technik
Modul-verantwortliche:r	Prof. Dr. Helia Hollmann
Pflicht/Wahl	Wahlpflicht
Turnus	Sommersemester, jährlich
Dauer	1 Semester
Lehr-veranstaltung	Industrial Security Basics
CP / SWS	5 CP, 4 SWS
Arbeitsaufwand	Gesamtaufwand 5 CP x 25 h = 125 h davon Präsenzzeit 45 h, Selbststudium 79 h, Prüfungszeit 1 h
Prüfungsform	laut SPO und Studienplan
Benotung	gemäß §20 der APO in der jeweils gültigen Fassung
Empfohlene Voraussetzungen	Programmieren, Automatisierungstechnik 1
Verwendbarkeit	vertiefendes Wahlpflichtmodul zur Erlangung der notwendigen Leistungspunkte lt. SPO
Lehrsprache	deutsch, englisch
Lehr-/Lern-methoden	Seminaristischer Unterricht, Praktikum

Industrial Security Basics

Inhalte

- Netzwerkgrundlagen - Hardware und Protokolle: Endgeräte, Hubs, (un-)managed Switche, Router, Firewall, ISO/OSI Schichtenmodell, UDP, TCP/IP (inkl. VLAN und QOS) IPv4 und IPv6, arp
- Netzwerkgrundlagen - Topologie, Routing, Absicherung: Baumstruktur, IP-Adressen, Subnetze und Subnetzmasken, Gateways, DNS, Proxy, NAT, http/s und TLS, Firewall/OPNSense, OpenWRT, PiHole
- Besonderheiten ethernetbasierter industrieller Netzwerke und Protokolle
- Sichere Fernzugänge: Ipsec, Wireguard, OpenVPN
- Grundlagen der Kryptographie auf eingebetteten Systemen
  - symmetrische und asymmetrische Verschlüsselungsverfahren, SHA, CA's
  - Vermittlung und Diskussion von Vor- und Nachteilen moderner kryptographischer Verfahren (u.a. AES, SHA, RSA, TLS)
  - Analyse von Angriffspunkten vernetzter Systeme
- Softwareentwicklung auf Mikrocontrollern in einer gängigen Hochsprache
  - Techniken der Softwareentwicklung
  - Dokumentation von Code
  - Softwareentwicklung mit Hilfe einer modernen IDE
  - Entwicklung von Software in vernetzten Systemen mit mehreren Microcontrollern
  - Nutzung von kryptographischen Bibliotheken auf Mikrocontrollern
- Praktische Implementierung von Funktionalitäten an einer konkreten Aufgabenstellung
- Analyse von und Angriff auf IT-Systeme, Updateverfügbarkeit und -management, Angriffsvektoren (Phishing) Auswirkungen und Gegenmaßnahmen, Statistiken, Hackerparagraf
- Netzwerksicherheit im Unternehmen

Industrial Security Basics

Qualifikations-ziele

Kenntnisse:

- Studierende kennen die Eigenschaften wichtiger kryptographische Verfahren.
- Studierende kennen ausgewählte sicherheitskritische Aspekte von Mikrocomputern in vernetzten Systemen und kryptographische Schutzmaßnahmen.
- Studierende erwerben ein grundlegendes Verständnis der relevanten Begrifflichkeiten, Technologien und Elemente der IT/OT-Sicherheit.
- Studierende lernen die Besonderheiten industrieller Netzwerke und Protokolle und deren Auswirkung auf die IT-Security kennen.
- Sie erarbeiten sich ein fundiertes Verständnis für die Vulnerabilität von IT-Systemen im Unternehmensumfeld.

Fertigkeiten:

- Studierende kennen Standardtools zur Netzwerkanalyse.
- Sie beherrschen die Netzwerksegmentierung und Konfiguration von Switchen und Firewalls.
- Sie können Automatisierungskomponenten sicher konfigurieren.
- Studierende können gängige Methoden der Softwareentwicklung für eingebettete Systeme anwenden.

Kompetenzen:

- Studierende können eine kryptographische Softwarebibliotheken in einem konkreten Projekt bewerten und eine geeignete auswählen.
- Studierende können ein bestehendes Softwareprojekt für einen Mikrocontroller erweitern (Fokus: Ressourcenbeschränkung, miteinander kommunizierende Einheiten).
- Das erlangte Wissen befähigt Studierende Netzwerke nach ISO 62443 abzusichern.
- Sie sind in der Lage Empfehlungen des BSI Grundschutzes umzusetzen.
- In einem Gesamtsystem können sie die umzusetzenden IT-Security Maßnahmen priorisieren.
- Sie haben die Fähigkeit mit Netzwerkspezialisten im Unternehmen zu interagieren und gegenüber fachfremden Personen Wissen zu vermitteln.

Industrial Security Basics

Literatur	- Vorlesungsunterlagen - Dokumentation verwendeter Hardwarekomponenten und Softwarebibliotheken - BSI: ICS-Security -Kompendium, 11/2014, erhältlich unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS - Knapp, E. D., Langill, J.: Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems, 12/2014, ISBN 978-0124201149 - Kobes, P.: Leitfaden Industrial Security - IEC 62443 einfach erklärt, 7/23, ISBN 978-3800753031 - Kurose, J.F./ Ross, K.W.: Computernetzwerke, 6. Auflage, Pearson Studium, 3/2014, ISBN 978-3-8689-4237-8 - Singh, G.D.: The Ultimate Kali Linux Book: Perform advanced penetration testing using Nmap, Metasploit, Aircrack-ng, and Empire, 2/2022, ISBN 978-1801818933

Introduction to Safety and Human Machine Interaction	
ID	MIS1G1
Study section	Pflichtbereich / Mandatory area
Responsible lecturer	Prof. Dr. Wolfgang Zeller
Mandatory/elective	mandatory
Rotation	Summer term, annually
Duration	1 Semester
Course	Introduction to Safety and Human Machine Interaction
CP / SWS	5 CP, 4 SWS
Workload	Total 5 CP x 25 h = 125 h thereof attendance 60 h, self-study 63,5 h, exam 1,5 h
Study/Examination Performance	according to Syllabus and Examination Regulations and Record of Examinations Schedule
Marking	according §20 APO in its relevant version
Prerequisites	none
Applicability	Module to obtain essential credit points
Teaching language	English
Teaching/Learning method	Seminar-like lecture, practical exercises

Introduction to Safety and Human Machine Interaction

Contents

1. Introduction to safety and human machine interaction

- Fundamental terms
- Real-world examples
- Relevance of the topics

2. Legal regulations and standards

- European guidelines and recommendations
- Safety related standards
- Human factors design guidelines

3. Terms, components and methods of safety

- Fundamental terms of functional safety for industrial control systems
- Components of safety related electric, electronic and programmable electronic control systems
- Safety related communication via industrial bus systems (incl. safety profiles)
- Functional safety of machine controls (ISO 13849 and IEC 62061)
- Functional safety of speed variable drive systems

4. Terms and methods of human machine interaction

- Human-centered design process (ISO 9241-210)
- Analysis of the context of use of technical systems (work system, manual and supervisory control, methods for task analysis, taskload/workload/performance)
- Specification of user requirements
- Implementation and evaluation of prototypes
- Characteristics of human operators (perception, information processing, action execution, human error)

Introduction to Safety and Human Machine Interaction

Module objectives

Aims:

- The students are provided with the knowledge of special requirements to safety of production plants.
- The students become familiar with hardware components and methods that can be used to achieve the necessary level of safety.
- The students know legal regulations and normative basics of safety engineering and can apply them to real plants.
- The students are enabled to design and implement safety related control systems as well as other software components of the plant and consider aspects of safety in all components.
- The students are taught characteristics of humans that are relevant for the design of safety related human machine interaction as well as processes and methods for the design of the interaction and can apply these processes to real problems.
- The students have a fundamental understanding of the design of safety related human machine interaction and of safety related drive systems.
- The design and proof testing is done according to relevant current regulations, guidelines, European directives and European standards.

Learning Outcomes:
A successful student will be able to show that he/she can:

- KNOWLEDGE AND UNDERSTANDING
  - K1 Know fundamental terms, functions and components
  - K2 Know models of human perception, information processing, action execution and human error
  - K3 Know about problems that can arise in human machine systems with complex automation
  - K4 Know relevant regulations and standards
- INTELLECTUAL QUALITIES
  - I1 Read and comprehend scientific literature on safety and human machine interaction
  - I2 Critically evaluate choices of safety functions
  - I3 Recognise aspects of safety in practice
- PROFESSIONAL/PRACTICAL SKILLS
  - P1 Design a system considering relevant aspects of safety and human machine

Introduction to Safety and Human Machine Interaction

Literature

- Ridley, John; Pearce, Dick: Safety with Machinery, 2nd. Edition, Routledge, London and New York, 2011. ISBN: 978-0750667807
- Macdonald, M. Dave: Machinery Safety, Elsevier, Oxford, 2004, ISBN 978-0750662703
- Jespen, Torben: Risk Assessments and Safe Machinery - Ensuring Compliance with the EU Directives. Springer, 2016, ISBN: 978-3-319-31361-0
- Hauke, Michael et al: Functional safety of machine controls - Application of EN ISO 13849. BGIA-Report 2/2017e. German Social Accident Insurance (DGUV), Berlin, 2019. ISBN: 978-3-86423-232-9
- Kaiser, Stephanie et al: Guide for Safe Machinery - SIX STEPS TO A SAFE MACHINE. Sick AG, Waldkirch, 2024.
- Regulation (EU) 2023/1230 of the European Parliament and of the Council of 14 June 2023 on machinery and repealing Directive 2006/42/EC of the European Parliament and of the Council and Council Directive 73/361/EEC
- Müller, Klaus-Rainer: Handbuch der Unternehmenssicherheit, Vieweg 2005, ISBN: 978-2658101503
- ISO/IEC 15408 Teil 1,2,3, Beuth Verlag
- ISO/IEC 62443-3-3, Beuth Verlag
- ISO/IEC 62443-2-4, Beuth Verlag
- Beisel, Wilhelm, Ebert, Frank, Foerster, Wolfgang: Lehrbuch für den Werkschutz und private Sicherheitsdienste, Boorberg 2004, ISBN 978-3415033948
- ISO 9241-210:2010. Ergonomics of human-system interaction -- Part 210: Human-centred design for interactive systems.
- Badke-Schaub, Petra, Hofinger, Gesine, Lauche, Kristina: Human Factors -- Psychologie sicheren Handels in Risikobranchen, Springer 2012, ISBN: 978-3642198861
- Schlick, Christopher M., Bruder, Ralph, Luczak, Holger: Arbeitswissenschaft, Springer 2010, ISBN: 978-3-540-78333-6
- Cranor, Lorrie, Garfinkel, Simson: Security and Usability, O'Reilly 2005, ISBN: 0596008279

Introduction to Safety and Human Machine Interaction

Cryptography and Security	
ID	MIS1G2
Study section	Pflichtbereich / Mandatory area
Responsible lecturer	Prof. Dr. Helia Hollmann
Mandatory/elective	mandatory
Rotation	Summer term, annually
Duration	1 Semester
Course	Cryptography and Security
CP / SWS	5 CP, 4 SWS
Workload	Total 5 CP x 25 h = 125 h thereof attendance 45 h, self-study 78,5 h, exam 1,5 h
Study/Examination Performance	according to Syllabus and Examination Regulations and Record of Examinations Schedule
Marking	according §20 APO in its relevant version
Prerequisites	IT Security (Crossover)
Applicability	Module to obtain essential credit points
Teaching language	English
Teaching/Learning method	seminar-like lecture, practical exercises

Cryptography and Security

Contents

1. Cryptography The mathematical foundations for encryption algorithms are taught. Furthermore, symmetric and asymmetric encryption algorithms, digital signature algorithms, key exchange and authentication protocols are explained mathematically, including their security and efficiency. Also blockchain technology, quantum cryptography and quantum computing are introduced.
2. Security The lecture starts with a brief introduction of security aspects and points out the importance of security in different fields. During the lecture requirements for security mechanisms of protocols for automation industry as well as in IT-networks are covered. Covering the broader range of some attacks it gives a first glance into attacks on device level as well.
3. Basics of the ISO/IEC 62443

Cryptography and Security

Module objectives

Knowledge:

- students know basic cryptographic algorithms and their purpose in detail, including mathematical aspects concerning the security
- students know how to implement the algorithms efficiently
- students are able to describe common attacks on IT and embedded systems
- students know basics on handling security for end-devices
- students know how executables can be manipulated and how to protect against it

Skills:

- students are able to derive requirements for the application of cryptographic algorithm
- students are able to analyse threats and risks of given systems
- students are able to analyse common industrial communication systems
- students are able to analyse code and find deficiencies concerning security

Competences:

- students are able to develop secure communication and key management concepts
- students are able to justify security measures in devices and networks
- students are able to criticize and defend security concepts
- students can analyse basic attacks on systems and name countermeasures

Cryptography and Security

Literature

Cryptography

- C. Paar, J. Pelzl, T. Güneysu: "Understanding Cryptography: From Established Symmetric and Asymmetric Ciphers to Post-Quantum Algorithms, Springer 2024
- A. J. Menezes, P. C. van Oorschot, S. A. Vanstone: "Handbook of Applied Cryptography", CRC Press, 2018, ISBN 978-1138385979
- K. Mainzer: "Quantencomputer -- Von der Quantenwelt zur Künstlichen Intelligenz", Springer 2020
- H.-G. Fill, A. Meier: "Blockchain -- Grundlagen, Anwendungsszenarien und Nutzungspotenzial", Springer 2020

Security

- Shostack: "Threat Modeling: Designing for Security", Wiley, 2014
- Ristic: "Bulletproof SSL and TLS", Feisty Duck, 2015
- P. Engebretson: "The Basics of Hacking and Penetration Testing", Elsevier, 2011
- A. J. Menezes, P. C. van Oorschot, S. A. Vanstone:"Handbook of Applied Cryptography", CRC Press, 2018, ISBN 978-1138385979
- G. Schell, B. Wiedemann (Ed.): „Bussysteme in der Automatisierungs- und Prozesstechnik``. Springer, 2019
- R.C.Detmer: „Introduction to 80×86 Assembly Language and Computer Architecture``, Jones & Bartlett Learning, 2014.
- D.L.Russel, P.C.Arlow: ``Industrial security : managing security in the 21st century", Wiley, 2015

Master Seminar	
ID	MIS1G3
Study section	Pflichtbereich / Mandatory area
Responsible lecturer	Prof. Dr. Jana Görmer-Redding
Mandatory/elective	Mandatory
Rotation	Summer term, annually
Duration	1 Semester
Course	Master Seminar
CP / SWS	5 CP, 4 SWS
Workload	Total 5 CP x 25 h = 125 h thereof attendance 45 h, self-study 80 h
Study/Examination Performance	according to Syllabus and Examination Regulations and Record of Examinations Schedule
Marking	according §20 APO in its relevant version
Prerequisites	none
Applicability	Module to obtain essential credit points
Teaching language	English
Teaching/Learning method	Seminar
Contents	- Methods for scientific writing and presentation - Independent in-depth research into a current topic - Writing of report in the style of a research paper - Review of other students` reports - Revision of own report based on reviews - Presentation of reports

Master Seminar	
Module objectives	**Knowledge** - students know in-depth information about a research topic - students are able to name and explain the fundamental parts of scientific reports - students are able to describe the sequence of well-prepared scientific presentations **Skills** - students are able to investigate the current state of research in a specific area - students are able to interpret research results - students are able to illustrate research results to their peers **Competences** - students are able to structure information obtained from different scientific sources - students are able to prepare a presentation of research results - students are able to criticize and defend research results
Literature	- lecture slides and notes

Major Project	
ID	MIS2S1
Study section	Pflichtbereich / Mandatory area
Responsible lecturer	Prof. Dr. Kay Werthschulte
Mandatory/elective	Mandatory
Rotation	Winter term, annually
Duration	1 Semester
Course	Major Project
CP / SWS	15 CP, 10 SWS
Workload	Total 15 CP x 25 h = 375 h thereof attendance 200 h, self-study 173,5 h, exam 1,5 h
Study/Examination Performance	according to Syllabus and Examination Regulations and Record of Examinations Schedule
Marking	according §20 APO in its relevant version
Prerequisites	Crossover modules, Master Seminar, knowledge of automation and networks
Applicability	Module to obtain essential credit points
Teaching language	English
Teaching/Learning method	Seminar-like lecture, practical exercises
Contents	The students work in teams on Industrial Security and Safety to protect an industrial machine or plant. This includes the security management which leads to the definition of security measures depending on risks identified. They coordinate and perform the organizational and technical measures to ensure safety and security of the network and the system. A project kick-off event is included. In a soft skills seminar the basics of teamwork and project management are taught. Among other things, the students deal with project meetings, the roles in a team and the tasks of a team leader. Their skills in communication, cooperation and conflict resolution are trained, which contributes to personal and team development.

Major Project

Module objectives

Aims:

- To equip the student with the skills necessary to carry out a complex project from conception through to completion; to plan, monitor, implement and to communicate his/her work in a team
- To give the student an opportunity to carry out a significant investigation into a subject area cognate to the aims of the course.
- To develop the ability to work independently and produce solutions demonstrating innovation, initiative and originality.
- To provide a measure of integration of the various topics studied on the course.

Learning outcomes:

- K1 Understand the processes involved in analysis of the problem and problem solving;
- K2 Understand the mechanisms for effective project work; planning review and management

Competencies:

- INTELLECTUAL QUALITIES
  - I1 Apply knowledge gained in an innovative, original way and show initiative;
  - I2 Design, implement, and evaluate industrial machine or plants which are safe and secure up to a certain level.
- PROFESSIONAL/PRACTICAL SKILLS
  - P1 Use resources effectively;
  - P2 Identify and develop any specific skills needed to ensure a successful project outcome.
- TRANSFERABLE SKILLS
  - T1 Demonstrate the appropriate written and oral skills necessary to effectively communicate project work;
  - T2 Be able to assess the progress of work against a plan and demonstrate good practice in project organisation and management.

Major Project	
Literature	Will be given during the course depending on the industrial machine or plant to be worked on.

German B2.1	
ID	IS1SP1
Study section	Mandatory area International
Responsible lecturer	Maria Lena Weinkam
Mandatory/elective	Compulsory
Rotation	Summer semester, annually
Duration	1 semester
Course	German B2.1
CP / SWS	5 CP, 4 CREDIT HOURS
Workload	Total workload 5 CP x 25 h = 125 h of which attendance time 60 h, self-study 63.5 h, examination time 1.5 h
Study/Examination Performance	according to SPO and list of course assessments
Marking	according to §20 of the APO in the currently valid version
Prerequisites	German B1.2
Applicability	Module for obtaining the necessary credit points according to SPO
Teaching language	German
Teaching/Learning method	Seminar-based teaching, exercise course

German B2.1	
Contents	This course follows on from the B1.2. course. It consolidates and deepens grammatical structures for everyday use. Communicative exercise courses improve the spontaneous use of correct grammar and idioms. The following grammatical structures are covered in the course: - Sentence structure and negation - two-part connectors - relative clauses - Passive voice and passive forms - Reflexive pronouns - modal sentences - Word formation
Module objectives	**Knowledge:** The module teaches general language, productive and receptive skills at reference level B2.1 of the Common European Framework of Reference for Languages (CEFR). **Skills:** - Students can understand the main content of complex texts. - They can communicate fluently in standard situations in the language of instruction. **Competences:** You will be able to successfully complete a degree programme, internship / lab course, project or research stay in a German-speaking country.
Literature	Kompass DaF B2.1, Kurs- und Arbeitsbuch, Klett Verlag

German B2.2	
ID	IS2SP2
Study section	Mandatory area International
Responsible lecturer	Maria Lena Weinkam
Mandatory/elective	Compulsory
Rotation	Winter semester, annually
Duration	1 semester
Course	German B2.2
CP / SWS	5 CP, 4 CREDIT HOURS
Workload	Total workload 5 CP x 25 h = 125 h of which attendance time 60 h, self-study 63.5 h, examination time 1.5 h
Study/Examination Performance	according to SPO and list of course assessments
Marking	according to §20 of the APO in the currently valid version
Prerequisites	German B2.1
Applicability	Module for obtaining the necessary credit points according to SPO
Teaching language	German
Teaching/Learning method	Seminar-based teaching, exercise course
Contents	This course builds on B2.1 to consolidate and deepen grammatical structures for everyday use. Communicative exercise courses improve the spontaneous use of correct grammar and idioms. The following grammatical structures are covered in the course: - Modal sentences - consolidation - Indefinite pronouns - Adjective declension - Genitive attributes / genitive objects - Complex sentences - Word formation

German B2.2	
Module objectives	**Knowledge:** The module teaches general language, productive and receptive skills at reference level B2.1 of the Common European Framework of Reference for Languages (CEFR). **Skills:** - Students can understand the main content of complex texts. - They can communicate fluently in standard situations in the language of instruction. **Competences:** You will be able to successfully complete a degree programme, internship / lab course, project or research stay in a German-speaking country.
Literature	Kompass DaF B2.2, Kurs- und Arbeitsbuch, Klett Verlag

Management, Leadership and IT Law	
ID	IS1G3
Study section	Mandatory area of safety and security
Responsible lecturer	Prof Dr Sarah Hatfield
Mandatory/elective	Compulsory
Rotation	Summer semester, annually
Duration	1 semester
Course	Management, Leadership and IT Law
CP / SWS	5 CP, 4 CREDIT HOURS
Workload	Total workload 5 CP x 25 h = 125 h of which attendance time 45 h, self-study 78.5 h, examination time 1.5 h
Study/Examination Performance	according to SPO and list of course assessments
Marking	according to §20 of the APO in the currently valid version
EN VORAUSSETZUNGEN	none
Applicability	according to SPO and curriculum
Teaching language	German
Teaching/Learning method	Seminar-based teaching, exercise course

Management, Leadership and IT Law

Contents

- Fundamentals and basic methods of management (organisational structure and operational organisation) and employee management
- Reflection of security aspects on the business significance of data and information
- Assessment of the security relevance of data and information from a management perspective
- Decision escalation paths and the resulting assignment of access and rights in organisations (business rules)
- Development and introduction/communication and enforcement of guidelines and regulations for internal and external protection (defence against social engineering)
- Development and introduction of training concepts relating to different security classes.
- Development of comprehensive concepts for securing data and information.
- Private law
  - Legal transactions
  - General and special law of obligations
  - Property law
- Internet law
  - Protection of domains
  - Electronic Commerce
  - Liability for damages and limitation of liability
- Copyright law/competition law
  - Basic concepts
  - Protection and liability
  - Claims for damages
- Data protection
  - Characteristics and basic concepts
  - Applicable legal provisions
  - Telecommunications data protection
- Legal aspects of IT forensics

Management, Leadership and IT Law

Module objectives

Knowledge:

- Students know the importance of data and information security from a business perspective.
- They know the security-relevant aspects of organisational structure, operational organisation and employee management.
- They know methods and measures of management and employee leadership that enable and support security concepts (e.g. escalation paths, assignment of rights, (communication) guidelines, business rules, training).
- They know the basic principles of private law and the basic principles of IT law with the importance of data protection and its practical significance.

Skills:

- Students can identify security-relevant data and information for operational processes, especially those relevant to business management.
- They can identify the security risks/threats arising from the organisational structure, company organisation and employee groups.
- You can apply methods to reduce security risks and threats
- You will be able to process basic operational incidents in the sense of legal case processing in contract law

Competences:

- Students are able to assess security risks/threats from organisational structure, operational organisation and employee management and develop/assess suitable countermeasures.
- They are able to assess legal framework conditions and take into account the legal significance of security risks/threats when developing measures.

Management, Leadership and IT Law

Literature

Management und Mitarbeiterführung

- Kaudela-Baum, S., Nagel, E., Bürkler, P. & Glanzmann, V. (2018). Führung lernen: Fallstudien zu Führung, Personalmanagement und Organisation (2., überarb. u. erw. Aufl. 2018). Springer Gabler.
- Rosenstiel, L. v., Regnet, E. & Domsch, M. E. (2020). Führung von Mitarbeitern: Handbuch für erfolgreiches Personalmanagement (8. aktualisierte und überarbeitete Auflage 2020). Schäffer-Poeschel.
- Schirmer, U. & Woydt, S. (2022). Mitarbeiterführung (BA KOMPAKT) (4. Aufl. 2022). Springer Gabler.
- Kersten, H.; Klett, G.; Reuter, J.; Schröder, K.-W. (2020): IT-Sicherheitsmanagement nach der neuen ISO 27001 (2. Auflage 2020). Springer.

IT-Recht

- Hoeren, Skript IT-Vertragsrecht, June 2023, available under https://www.itm.nrw/wp-content/uploads/Skript_IT-Vertragsrecht_Stand_Juni_2023.2.pdf
- Beck Texte im dtv, IT- und Computerrecht, 16. Aufl. 2023
- Redeker, IT-Recht, 8. Aufl. 2023
- Erben/Günther, Gestaltung und Management von IT-Verträgen, 4. Aufl. 2023

Certification Module	
ID	IS2S1
Study section	Mandatory area of safety and security
Responsible lecturer	Prof Dr Kay Werthschulte
Mandatory/elective	Compulsory
Rotation	Winter semester, annually
Duration	1 semester
Course	Certification Module
CP / SWS	5 CP, 4 CREDIT HOURS
Workload	Total workload 5 CP x 25 h = 125 h of which attendance time 45 h, self-study 78.5 h, examination time 1.5 h
Study/Examination Performance	according to SPO and list of course assessments
Marking	according to §20 of the APO in the currently valid version
Prerequisites	Introduction to Safety and Human Machine Interaction
Applicability	Module for obtaining the necessary credit points according to SPO
Teaching language	German
Teaching/Learning method	Seminar-based teaching, exercise course

Certification Module

Contents	The course covers the topics of functional security, information security management systems (ISMS) and data protection. The course focuses on functional safety. Students acquire basic knowledge of functional security and are able to carry out risk analyses and implement security measures. They master the security life cycle and the management processes for secure development. In addition, they apply basic hardware and software development techniques for functional safety and assess safety architectures. The course covers the basics of ISMS, including definition and operational benefits. Facets of ISMS such as security regulations and asset classification are covered. It also discusses which stakeholders need to be involved and which security certifications exist. In the area of data protection, the requirements of the General Data Protection Regulation are explained, which companies must comply with in order to act in accordance with the law, followed by an overview of international data protection requirements and a discussion of how companies can fulfil them.

Certification Module

Module objectives	**Knowledge:** - Students know the background of a risk-based information security management system (ISMS) and can name the basic terms and explain them using examples. - Students can understand and explain the basic concepts of functional safety and know qualitative and quantitative techniques and measures to achieve functional safety. **Skills:** - Students have the tools to deal with normative literature. - Students can apply the safety life cycle required by functional safety, from the creation of the concept, hazard and risk assessment with the creation of a safety requirement specification and subsequent hardware and software development through to decommissioning. - Students have the knowledge required to set up an ISMS structure in accordance with ISO 27001. Students are familiar with the General Data Protection Regulation for companies in Germany and Europe. **Competences:** - Students have basic knowledge of security technology and can apply the basics.
Literature	- Lecture slides, accompanying and exercise material in moodle - Norm, IEC 61508:2010 Teil1-7, Beuth Verlag, 2011. - D. J.Smith, K. G. L. Kenneth: The Safety Critical Systems Handbook, Butterworth-Heinemann Inc., 5th Edition, 2020. - DIN EN ISO/IEC 27001

Advanced Security Testing	
ID	ISWP.AST
Study section	Compulsory elective area 1 Security
Responsible lecturer	Dr. Matthias Niedermaier Florian Fischer
Mandatory/elective	Elective
Rotation	Summer semester, annually
Duration	1 semester
Course	Advanced Security Testing
CP / SWS	5 CP, 4 CREDIT HOURS
Workload	Total workload 5 CP x 25 h = 125 h of which attendance time 45 h, self-study 78.5 h, examination time 1.0 h
Study/Examination Performance	according to SPO and list of course assessments
Marking	according to §20 of the APO in the currently valid version
Prerequisites	Knowledge of IT Security is essential
Applicability	Required elective module to obtain the necessary credit points according to the SPO
Teaching language	German
Teaching/Learning method	Seminar-based teaching, exercise course

Advanced Security Testing

Contents

- Report creation (project work and penetration test report)
- Using tools - incomplete list: OpenVAS, Metasploit, binwalk, Firmware Modification Kit, ZAP, Burp Suite, MITRE ATT&CK, Wireshark
- Developing custom scripts to analyze current IT security aspects
- Approach to software testing of embedded systems
- Approach to product testing / hardware testing
- Approach to testing Industrial Internet of Things (IIoT) environments
- Current state of technology and research
- IoT and IIoT devices and specific aspects in the field of Operational Technology (OT)
  - Pentesting of IIoT devices and OT networks
  - Microchip manufacturing, decapsulation, fault injection attacks
  - Reverse engineering of software/binary files
  - General approach
  - Static code analysis
  - Dynamic code analysis
  - Tools: Code inspection tools (strings, nm, file, objdump), disassemblers (radare2, cutter, ghidra), debuggers (gdb)
- Vulnerability management: Introduction to relevant metrics and models
- Attack detection:
  - Background on IDS/IPS, SIEM, and SOC in relation to embedded systems
  - Technical insight into relevant concepts and tools such as YARA, Zeek, Suricata
  - Tools: YARA/Strelka, Zeek, Suricata, ELK-Stack, Security Onion
- Governance, Risk, and Compliance: Introduction to security processes, risk assessment, and compliance requirements
- Relevant policies, standards, and guidelines in the cybersecurity context:
  - IEC 62434 standards series: Introduction and practical relevance to security testing
  - NERC CIP
  - NIST Special Publications (SP), Cybersecurity Framework (CSF)
  - BSI IT-Grundschutz
  - ISO 27000 series
- Current legal cybersecurity requirements (focus on OT): NIS-2, EU-MVO, CRA, TRBS1115 Part 1

Advanced Security Testing

Module objectives

Knowledge:

- The lecture will use practical questions to discuss the planning, procedure and completion of security tests. In order to keep the lecture as close as possible to professional practice, a wide range of tools will be used.
- Emphasis is placed on the broadest possible range of topics in this area. This includes detecting software vulnerabilities in source code, testing entire networks and hardware-related issues.

Skills:

- Carrying out classic security product tests
- Performing network security tests
- Attacks and defence on hardware
- Performing software tests

Competences:

- Students can carry out penetration tests with the help of tools, among other things
- They can familiarise themselves with new topics in the context of secure architectures
- Students are able to fundamentally test products for their IT security level

Advanced Security Testing

Literature

- HUANG, Andrew Bunnie. The Hardware Hacker: Adventures in Making and Breaking Hardware. 2017.
- HUANG, Andrew. Hacking the XBox: An Introduction to Reverse Engineering. 2002.
- ERICKSON, Jon. Hacking: The Art of Exploitation. No Starch Press, 2008.
- Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets & Solutions ISBN-10: 1259589714
- The Hardware Hacking Handbook: Breaking Embedded Security with Hardware Attacks ISBN-10: 1593278748
- Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems ISBN-10: 0443137374
- Skript

Basics of IT Forensics	
ID	ISWP.ITFORE
Study section	Compulsory elective area 1 Security
Responsible lecturer	Dr. Kay Werthschulte
Mandatory/elective	Elective
Rotation	Winter semester, annually
Duration	1 semester
Course	Introduction to IT forensics
CP / SWS	5 CP, 4 CREDIT HOURS
Workload	Total workload 5 CP x 25 h = 125 h of which attendance time 45 h, self-study 79 h, examination time 1 h
Study/Examination Performance	according to SPO and list of course assessments
Marking	according to §20 of the APO in the currently valid version
Prerequisites	Lecture IT Security desirable, but not an exclusion criterion
Applicability	Required elective module to obtain the necessary credit points according to the SPO
Teaching language	German
Teaching/Learning method	Seminar-based teaching, exercise course
Contents	- Introduction to digital forensics - Procedure models - Securing digital traces - Analysing digital traces - Hard drive forensics - Windows forensics - Memory forensics - Network forensics - Mobile forensics - Malware analysis

Basics of IT Forensics

Module objectives	The Digital Forensics lecture deals with securing, analysing and presenting digital traces after an incident. Students are given an overview of forensic procedures, IT attacks and the underlying technologies. As this is an integrated lecture, students will apply what they have learnt directly in the lecture, thus achieving a close link between theory and practice. After the lecture, participants should be able to determine whether an attack has taken place and know how to secure and analyse digital evidence.
Literature	- Dan Farmer, Wietse Venema: Forensic Discovery, Addison-Wesley Longman, Amsterdam; Auflage: illustrated edition (13. Januar 2005) - Brian Carrier: File System Forensic Analysis, Addison-Wesley Longman, Amsterdam (7. April 2005) - Harlan Carvey: Windows Forensic Analysis DVD Toolkit, Second Edition, Syngress; 2 edition (June 11, 2009) - Lee Reiber: Mobile Forensic Investigations, McGraw-Hill Education, Auflage: 2., 2019

Embedded Security	
ID	MIS2SSec3
Study section	Wahlpflichtbereich 1 International und Security / Compulsory elective area 1 International and Security
Responsible lecturer	Prof. Dr. Dominik Merli
Mandatory/elective	Elective
Rotation	Winterterm, annually
Duration	1 Semester
Course	Embedded Security
CP / SWS	5 CP, 4 SWS
Workload	Total 5 CP x 25 h = 125 h thereof attendance 45 h, self-study 78,5 h, exam 1,5 h
Study/Examination Performance	according to Syllabus and Examination Regulations and Record of Examinations Schedule
Marking	according §20 APO in its relevant version
Prerequisites	basic knowledge about cryptography and IT security
Applicability	Module to obtain essential credit points
Teaching language	English
Teaching/Learning method	Seminar-like lecture, practical exercises

Embedded Security

Contents

1. Introduction, Standards and Processes
   - Standards for Secure Components
   - Secure Development Process
2. Fundamental Embedded Security Building Blocks
   - Random Number Creators
   - Cryprographic Implementations
   - Confidential Data Storage and Secure Memory
   - Secure Device Identity
   - Secure Communication
3. Advanced Embedded Security Concepts
   - Secure Boot and System Integrity
   - Secure Firmware Update
   - Robust Device Architecture
   - Access Control and Management
   - System Monitoring

Embedded Security

Module objectives	**Knowledge** - Students know the basic building blocks of embedded security implementations. - Students are able to name and explain the advantages and disadvantages of different security countermeasures. - Students are able to describe typical embedded security concepts. **Skills** - Students are able to derive security requirements for embedded systems. - Students are able to analyze embedded security concepts. - Students are able to draft practical security concepts for embedded systems. **Competences** - Students are able to structure embedded system architectures according to different security needs. - Students are able to justify embedded security measures. - Students are able to criticize and defend embedded security concepts.
Literature	- D. Mukhopadhyay, R. S. Chakraborty: "Hardware Security: Design, Threats, and Safeguards", Chapman and Hall/CRC, 2014 - C. Paar, J. Pelzl: "Understanding Cryptography: A Textbook for Students and Practitioners", Springer, 2010 - C. K. Koc (Ed.): "Cryptographic Engineering", Springer, 2009

Network Penetration Testing	
ID	ISWP.NETP
Study section	Compulsory elective area 1 Security
Responsible lecturer	Dr Lothar Braun
Mandatory/elective	Elective
Rotation	Summer semester, annually
Duration	1 semester
Course	Network Penetration Testing
CP / SWS	5 CP, 4 CREDIT HOURS
Workload	Total workload 5 CP x 25 h = 125 h of which attendance time 45 h, self-study 79 h, examination time 1 h
Study/Examination Performance	according to SPO and list of course assessments
Marking	according to §20 of the APO in the currently valid version
Prerequisites	- IT Security module - Data communication module
Applicability	Required elective module to obtain the necessary credit points according to the SPO
Teaching language	German
Teaching/Learning method	Seminar-based teaching, exercise course

Network Penetration Testing	

Contents	- Planning penetration tests for networks
	- Creation of reports
	- Information gathering in the network
	  - Techniques for detecting machines and services in networks using common tools
	  - Investigation of attack surfaces of network services
	  - Identification of potential vulnerabilities in network services
	- Attacks on network services
	  - Password attacks
	  - Attacks on web applications
	  - Analysing, adapting and using exploits
	  - Buffer overflow exploits
	  - Development of scripts to carry out attacks

Module objectives	- Students acquire knowledge about the implementation of penetration tests in computer networks. - Students learn how to use techniques to obtain information in the network. They know the relevant techniques for identifying vulnerabilities. - Students learn the techniques for carrying out attacks to demonstrate vulnerabilities found and are able to apply these using familiar tools. They are able to make recommendations for action to eliminate the vulnerabilities.
Literature	will be announced in the lecture

Project IT-Security	
ID	MIS2SSec5
Study section	Wahlpflichtbereich 1 International und Security / Compulsory elective area 1 International and Security
Responsible lecturer	Prof. Dr. Dominik Merli
Mandatory/elective	Elective
Rotation	Winter and summer term, annually
Duration	1 term
Course	Project IT-Security
CP / SWS	5 CP, 4 SWS
Workload	Total 5 CP x 25 h = 125 h thereof attendance 25 h, self-study 98,5 h, exam 1,5 h
Study/Examination Performance	according to Syllabus and Examination Regulations and Record of Examinations Schedule
Marking	according §20 APO in its relevant version
Prerequisites	basic knowledge about cryptography and IT security
Applicability	Module to obtain essential credit points
Teaching language	English
Teaching/Learning method	Practical exercises
Contents	Students work on newer scientific questions independently, e.g. prototype development, laboratory setups.

Project IT-Security	
Module objectives	**Learning outcomes** Depends on the project **Knowledge Targets** Deeper Understanding in IT-Security **Capabilities** - Plan and implement an IT-Security project in terms of time, effort and resources. - Independently learn methods and procedures. - Analysing and evaluating methods with regard to the project objectives. - Document project results in an understandable and appealing way.
Literature	Project-specific literature will be announced by the supervisor before the start of the project.

Project Safety	
ID	MIS2SSaf2
Study section	Wahlpflichtbereich 1 International und Safety / Compulsory elective area 1 International and Safety
Responsible lecturer	Prof. Dr. Kay Werthschulte, Prof. Dr. Wolfgang Zeller
Mandatory/elective	Elective
Rotation	Winter term, annually
Duration	1 term
Course	Project Safety
CP / SWS	5 CP, 4 SWS
Workload	Total 5 CP x 25 h = 125 h thereof attendance 45 h, self-study 78,5 h, exam 1,5 h
Study/Examination Performance	according to Syllabus and Examination Regulations and Record of Examinations Schedule
Marking	according §20 APO in its relevant version
Prerequisites	basic knowledge about safety
Applicability	Module to obtain essential credit points
Teaching language	English
Teaching/Learning method	Seminar-like lecture, practical exercise
Contents	Students work on newer scientific questions independently, e.g. prototype development, laboratory setups.

Project Safety	
Module objectives	**Learning outcomes** Depends on the project **Knowledge Targets** Deeper Understanding in Safety **Capabilities** - Plan and implement an Safety project in terms of time, effort and resources. - Independently learn methods and procedures. - Analysing and evaluating methods with regard to the project objectives. - Document project results in an understandable and appealing way.
Literature	Project-specific literature will be announced by the supervisor before the start of the project.

Safety	
ID	IS2S3
Study section	Compulsory elective area 1 Safety
Responsible lecturer	Prof Dr Wolfgang Zeller
Mandatory/elective	Elective
Rotation	Winter semester, annually
Duration	1 semester
Course	Safety
CP / SWS	5 CP, 4 CREDIT HOURS
Workload	Total workload 5 CP x 25 h = 125 h of which attendance time 45 h, self-study 78.5 h, examination 1.5 h
Study/Examination Performance	according to SPO and list of course assessments
Marking	according to §20 of the APO in the currently valid version
Prerequisites	Introduction to Safety, Security and Human Machine Interaction
Applicability	Module for obtaining the necessary credit points according to SPO
Teaching language	German
Teaching/Learning method	Seminar-based teaching

Safety

Contents

Introduction

- Examples of use, current significance, objectives

Mathematical basics

- Random events and probability theory
- Failure behaviour of technical systems and distribution functions
- Markov modelling

Methods of risk analysis and assessment

- FMEA and FMEDA
- Fault trees

Safety-relevant system architectures and their calculation

- Single and multi-channel systems
- Calculation of characteristic variables to describe the probability of failure and diagnostic coverage

Methods for avoiding common cause failures

- Technical and organisational measures
- Included in the calculation of the failure behaviour

Development of safety-relevant control software

- Basic procedures for avoiding systematic faults
- Input into the methodical development and proof of safety-relevant control systems

Methods of verification and validation

- Fundamentals of testing and proof of the properties of safety-relevant control systems
- Computer-aided methods

Exemplary application of mathematical and methodological principles

- Production machines (operating modes)
- Industrial robots (human-machine collaboration)
- Automotive engineering (autonomous driving)

Safety

Module objectives	**Knowledge:** - Students know the mathematical and theoretical principles of probability calculation and the failure behaviour of technical systems. - They can outline the methodical procedure for designing safety functions using relevant basic standards. **Skills:** - Students are able to mathematically prove the functional safety of control systems in accordance with legal and normative requirements. - Building on this, students are able to apply procedures for the methodical approach and proof of the properties of safety-relevant systems in a targeted manner. **Competences:** - Students acquire the ability to successfully transfer their basic knowledge to industry-specific issues based on practical use cases from various areas. - They are able to independently assess the functional safety of control systems from a technical and economic point of view.
Literature	- Presentation, exercises in moodle - Goble, W.: Control Systems Safety Evaluation and Reliabilty, Instrument Society of America, 2010, ASIN: B017R2U3LO - Börcsök, Josef: Funktionale Sicherheit - Grundzüge sicherheitstechnischer Systeme, 5. überarb. Aufl., VDE Verlag, Berlin, 2021. ISBN 978-3800753574 - Smith, David u. Simpson, Kenneth G. L.: Safety Critical Systems Handbook - A Straightfoward Guide to Functional Safety, IEC 61508 and Related Standards, 3rd edition, Elsevier, 2010. ISBN 978-0080967813 - IEC 61508: Funktionale Sicherheit sicherheitsbezogener elektrischer / elektronischer / programmierbarer elektronischer Systeme, Teil 1 bis 7, Beuth 2011.

Secure Business Processes	
ID	IS2S2
Study section	Compulsory elective area 1 Safety
Responsible lecturer	Prof Dr Jana Görmer-Redding
Mandatory/elective	Elective
Rotation	Winter semester, annually
Duration	1 semester
Course	Secure Business Processes
CP / SWS	5 CP, 4 CREDIT HOURS
Workload	Total workload 5 CP x 25 h = 125 h thereof attendance 60 h, self-study 90 h
Study/Examination Performance	according to SPO and list of course assessments
Marking	according to §20 of the APO in the currently valid version
Prerequisites	none
Applicability	Required elective module to obtain the necessary credit points according to the SPO
Teaching language	German, English parts
Teaching/Learning method	Seminar-based teaching, exercise course

Secure Business Processes

Contents

In the context of growing digitalisation in all areas, IT Security is becoming increasingly important and presents companies with far-reaching challenges. In this course, students will deal with crucial aspects of secure business processes in a digitalised world. The course is divided into two main parts: On the one hand, in the ``Fundamentals of IT Security for Business Processes'' part, students will learn how business processes can be mapped correctly and securely in SAP ERP software in the application. On the other hand, the second part of the course, ``Risk management and opportunities of digitalisation'', illustrates which measures and tools can be used to identify, analyse, assess and control IT security risks. The specific knowledge is enriched with external presentations and supported with exercise courses and case studies, or elaborations on the sub-topic areas for application.

Part 1: Fundamentals of IT Security for Business Processes

- Introduction to digital transformation:* Students learn about the fundamental concepts and trends of digital transformation and understand their impact on business processes.
- Security fundamentals for business processes:* This part covers the key security principles and concepts that should be considered when designing and implementing secure business processes.
- *Security in SAP ERP:* Students will deepen their understanding of the security of business processes in SAP ERP software. This includes the protection of data, access controls and the secure configuration of SAP systems.

Keywords: Framework and security requirements in the context of using SAP, SAP Authorisation, SAP ABAP Authorisation, SAP GRC Access Control, SAP Identity Management System (IdM), SAP HANA Database

Part 2: Risk management and opportunities of digitalisation

- Opportunities and risks of digitalisation:* This section discusses the opportunities and challenges of digitalisation for companies. Particular emphasis is placed on the associated security risks.
- Identification and analysis of IT security risks:* Students learn how to identify and analyse potential risks to business processes. This includes threat analyses, vulnerability assessments and risk assessment methods.
- Management and security measures:* This section covers strategies and tools for managing and minimising IT security risks. This includes security frameworks, security policies, compliance

Secure Business Processes

Module objectives

Knowledge:

- After successfully completing this module, students will understand the economic and IT fundamentals of digitalisation and the associated opportunities and risks for business models and processes.
- In addition, students learn about different types of risks and how they can differentiate between them. From an IT Security perspective, they will discuss how the threat map is changing as a result of advancing digitalisation, which security risks of an IT solution (security, compliance, reliability) need to be considered and how these risks can be assessed and managed.
- Students learn methods for identifying, quantifying, controlling and monitoring risks using the risk management cycle.
- Students know how to assess risks, particularly in the area of IT Security, using various quantitative risk measures and can interpret these economically. They learn about risk-adjusted assessment approaches for evaluating and prioritising IT security measures and apply these using practical examples.

Skills:

- Students can identify, assess, manage and monitor the opportunities and risks of the digital transformation of companies.
- Students can transfer this knowledge to practical use cases.

Competences:

- Students learn important business fundamentals of integrated opportunity and risk management in the context of a secure Industry 4.0.
- These skills contribute to the interdisciplinary educational goal of the degree program, as industrial security specialists must also be able to assess opportunities and risks and, among other things, make and prioritise investment decisions in the area of cyber security.
- Case study: By coordinating team members and distributing tasks within the team, students also learn time management and reliability towards other team members.
- Case study: By presenting the results to their fellow students, the students also learn presentation techniques and the sensible use of modern IT.

Secure Business Processes

Literature

- Aichele C., Schönberger M. (2014) Grundlagen des Projektmanagements. In: IT-Projektmanagement. essentials. Springer Vieweg, Wiesbaden (ebook: https://link.springer.com/book/10.1007/978-3-658-08389-2)
- Kaufman C., Perlman, R., Speciner, M., Perlner, R. (2023) Network Security Private Communication in a Public World. Third Edition. Person Addison-Wesley
- Urbach N., Röglinger M. (2017) Digitalization Cases. Springer (ebook: https://link.springer.com/book/10.1007/978-3-319-95273-4 UND https://link.springer.com/book/10.1007/978-3-030-80003-1)
- Sackmann, S., Kundisch, D. & Ruch, M. HMD (2008) CRM, Kundenbewertung und Risk-Return-Steuerung im betrieblichen Einsatz (Zeitschriften-Aufsatz in HMD Praxis der Wirtschaftsinformatik, elektronisch abrufbar: https://link.springer.com/article/10.1007/BF03341171) Brandes U. (2010) Graphentheorie. In: Stegbauer C., Häußling R. (eds) Handbuch Netzwerkforschung. VS Verlag für Sozialwissenschaften (Ebook-Kapitel elektronisch abrufbar: https://link.springer.com/chapter/10.1007/978-3-531-92575-2_31)
- Purdy, G. 2010. ``ISO 31000:2009--Setting a new standard for risk management,'' Risk analysis: an official publication of the Society for Risk Analysis (30:6), pp. 881--886 (Zeitschriften-Aufsatz elektronisch abrufbar: https://web.s.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=0&sid=92817660-ef9e-4ba5-98d7-0c55c0fa9c6e%40redis)

Secure Implementation on Microcontrollers	
ID	IS2S5
Study section	Compulsory elective area 1 Security
Responsible lecturer	Prof Dr Kay Werthschulte
Mandatory/elective	Elective
Rotation	Summer and winter semester, annually
Duration	1 semester
Course	Secure implementation on microcontrollers
CP / SWS	5 CP, 4 CREDIT HOURS
Workload	Total workload 5 CP x 25 h = 125 h of which attendance time 45 h, self-study 78.5 h, examination time 1.5 h
Study/Examination Performance	according to SPO and list of course assessments
Marking	according to §20 of the APO in the currently valid version
Prerequisites	IT Security, Programming skills, Cryptography and Security
Applicability	In-depth required elective module to obtain the necessary credit points according to the SPO
Teaching language	German
Teaching/Learning method	Seminar-based teaching, internship / lab course
Contents	The protection of embedded systems against attacks by third parties on stored data and implementations is an increasingly important but also challenging task due to increasing networking. This course aims to provide in-depth knowledge of possible attacks on microcontrollers and to examine the possibilities of protecting microcontrollers using software implementations. In practical exercise courses, this knowledge will be implemented independently in small groups and attacks can be carried out using the ChipWhisperer® provided in order to put implemented countermeasures to the test.

Secure Implementation on Microcontrollers

Module objectives	**Knowledge:** - Students learn about invasive and non-invasive attacks on microcontrollers. **Skills:** - They learn techniques to secure microcontrollers against attacks. - They learn about the possibilities of protecting systems with software. **Competences:** - Students develop secure code for microcontrollers - They understand what constitutes a secure system. - They can assess the extent to which cryptography protects against attacks.
Literature	- Mangard, S., Oswald, E., Popp, T. (2007). Power Analysis Attacks: Revealing the Secrets of Smart Cards. Niederlande: Springer US. - Woudenberg, J. v., O'Flynn, C. (2021). The Hardware Hacking Handbook: Breaking Embedded Security with Hardware Attacks. USA: No Starch Press.

Required Elective Modules 2 for Focus *International*

You can take any module ``German as a Foreign Language'' from the ``German Advanced'' section of the Center for Languages and Intercultural Communication.

Required Elective Modules 2 for Focuses *Safety* and *Security*

Any module with a technical or information technology focus can be taken for master's degree programs at TH Augsburg.

Master Thesis	
ID	MIS3MT
Study section	Masterarbeit
Responsible lecturer	Prof. Dr. Kay Werthschulte
Mandatory/elective	mandatory
Rotation	Summer and winter term, annually
Duration	1 Semester
CP / SWS	20 CP
Workload	Total 25 CP x 25 h = 625 h
Study/Examination Performance	according to SPO and list of course assessments
Marking	according to §20 of the APO in the currently valid version
Prerequisites	Master Seminar
Applicability	Module to obtain essential credit points
Teaching language	English
Teaching/Learning method	lecture, tutorial, independent study
Contents	The project will integrate the underlying course material in order to apply industrial safety and security knowledge to the design of a practical industrial safety and security product or system. There should be opportunities within each project to develop experimental and theoretical work and most of the areas contained within the project should be relevant to topics studied as part of the course. It should integrate one or more of the following aspects into the solution, as appropriate: research, design, quality, implementation, evaluation, reliability, production, and marketing.

Master Thesis

Module objectives

AIMS

- To equip the student with the skills necessary to carry out a project from conception through to completion of a type relevant to an industrial safety and security environment;
- To plan, monitor, implement and communicate his/her project work.
- To give the student an opportunity to carry out a significant investigation into a subject area cognate to the aims of the course.
- To develop the ability to work independently and producce solutions demonstrating innovation, initiative and originality.
- To provide a measure of integration of the various topics studied on the course.

KNOWLEDGE AND UNDERSTANDING

- K1 Understand the processes involved in design and problem solving
- K2 Understand the mechanisms for effective project work; planning review and management.
- K3 Develop a comprehensive knowledge of an industrial safety and security project area.

INTELLECTUAL QUALITIES

- I1 Apply knowledge gained in an innovative, original way and show initiative.
- I2 Recognise and analyse criteria and specifications appropriate to a specific problem and plan strategies for its solution.
- I3 Integrate aspects of engineering, computer science or economics in theory and practice.
- I4 Demonstrate creativity and innovation in the solution of an industrial safety and security project problem and in the development of designs, products and systems.
- I5 Design, implement, and evaluate an industrial safety and security product or system which is safe and secure.
- I6 Analyse the extent to which a developed industrial safety and security product or system meets the criteria defined for its current deployment and future evolution.

PROFESSIONAL/PRACTICAL SKILLS

- P1 Use resources effectively;
- P2 Identify and develop any specific skills needed to ensure a successful project outcome.
- P3 Employ effectively modern methodologies and

Master Thesis

Literature	- S. B. Heard: The Scientist`s Guide to Writing -- How to wirte More Easily and Effectively throughout Your Scientific Career, Princeton University Press, 2022 - K. L. Turabian: A Manual for Writers of Research Papers, Theses, and Dissertations, University of Chicago Pr., 2018 - M. Zaumanis: Research Data Visualization and Scientific Graphics for Papers, Presentations and Proposals, Independently published , 2021, ISBN 979-8541959321 Additionally, apart from the general academic literature on writing, presentation skills, and scholarly work listed, it is crucial to consult subject-specific literature for the Master's thesis. The choice of literature will vary depending on the specific topic being researched.