

---

Technische Hochschule Augsburg

---

Fakultät für Elektrotechnik

---

---

**Masterstudiengang**

---

**Industrielle Sicherheit (M.Sc.)**

---

Modulhandbuch

---

**SoSe 2025**

*Stand: 4. November 2024*

Inhaltsverzeichnis	Seite
<b>A Crossoverbereich</b>	
<u>Datenkommunikation</u>	4
<u>Industrieanlagen, Automatisierung und Steuerung</u>	6
<u>Data Literacy and Business Intelligence</u>	10
<u>IT-Sicherheit</u>	14
<u>Industrial Security Basics</u>	16
<u>Human Recource and Organisation Management</u>	20
<b>B Pflichtbereich</b>	
<u>Introduction to Safety and Human Machine Interaction</u>	23
<u>Cryptography and Security</u>	28
<u>Master Seminar</u>	32
<u>Major Project</u>	34
<b>B.1 Zusätzliche Pflichtmodule für Schwerpunkt International</b>	
<u>Deutsch B2.1</u>	37
<u>Deutsch B2.2</u>	39
<b>B.2 Zusätzliche Pflichtmodule für Schwerpunkte Safety und Security</b>	
<u>Management, Mitarbeiterführung und IT-Recht</u>	41
<u>Zertifizierungsmodul</u>	45
<b>C Wahlpflichtbereich</b>	
<b>C.1 Wahlpflichtbereich 1</b>	
<u>Advanced Security Testing</u>	48
<u>Einführung in die IT-Forensik</u>	51

<u>Embedded Security</u>	53
<u>Network Penetration Testing</u>	56
<u>Project IT-Security</u>	58
<u>Project Safety</u>	60
<u>Safety</u>	62
<u>Sichere Geschäftsprozesse</u>	66
<u>Sichere Implementierung auf Microcontrollern</u>	70

## **C.2 Wahlpflichtbereich 2**

<u>Wahlpflichtbereich 2 für den Schwerpunkt International</u>	72
<u>Wahlpflichtbereich 2 für die Schwerpunkte Safety und Security</u>	73

## **D Masterarbeit**

<u>Master Thesis</u>	74
----------------------	----

### Datenkommunikation

Kürzel	IS1C1
Modulbereich	Crossover
Modul- verantwortliche:r	Prof. Dr. Rolf Winter
Pflicht/Wahl	Wahlpflicht
Turnus	Sommersemester, jährlich
Dauer	1 Semester
Lehr- veranstaltung	Datenkommunikation
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	keine
Verwendbarkeit	Wahlpflichtmodul zur Erlangung der notwendigen Leistungs- punkte lt. SPO
Lehrsprache	Deutsch
Lehr-/Lern- methoden	Seminaristischer Unterricht, Übung

## Datenkommunikation

---

Inhalte	<p>Die Vorlesung führt in die Funktionsweise und den Aufbau des Internets ein und berücksichtigt dabei die Architektur des Internets, seine Prinzipien und die eingesetzten Schlüsselprotokolle. Behandelt werden insbesondere:</p> <ul style="list-style-type: none"><li>- Protokolle der Anwendungsschicht (wie HTTP und DNS)</li><li>- Transport-Protokolle (wie TCP und UDP)</li><li>- Routing-Protokolle (link state und distance vector)</li><li>- Protokolle der Sicherungsschicht (z.B. Ethernet und WLAN)</li><li>- Arbeitsweise von Kernkomponenten des Internets (Switches, CDNs, NAT, uvm.)</li><li>- Schlüsselprinzipien des Internets (Zuverlässige Datenübertragung, Staukontrolle etc.)</li><li>- Umgang mit Standardwerkzeugen (Software) aus dem Bereich Netzwerke</li></ul>
Qualifikationsziele	<p>Die Studierenden kennen die Schlüsselprotokolle des Internets und können deren Aufgaben und Funktionsweise im Detail erklären. Sie wissen welche Funktionen der Internet-Architektur wie und wo im Netz implementiert sind. Auch die komplexen Zusammenhänge zwischen Protokollen und Mechanismen im Internet können Studierende beschreiben. Darüber hinaus können die Studierenden ihr erlerntes Wissen auch praktisch bei der Entwicklung von vernetzten Anwendungen oder der Einrichtung und Wartung von Netzen einsetzen. Das Praktikum befähigt Studierende mit Standardwerkzeugen Anwendungen und Netze zu analysieren und einzurichten.</p>
Literatur	<p>Computer Networking: A Top-Down Approach, Global Edition Taschenbuch -- Internationale Ausgabe, 10. Juni 2021, 8th Edition</p>

---

### Industrieanlagen, Automatisierung und Steuerung

Englische Modulbezeichnung	Industrial Plants, Automation and Control
Kürzel	IS1C3
Modulbereich	Crossover
Modulverantwortliche:r	Prof. Dr. Wolfgang Zeller
Pflicht/Wahl	Wahlpflicht
Turnus	Sommersemester
Dauer	1 Semester
Lehrveranstaltung	Industrieanlagen, Automatisierung und Steuerung
CP / SWS	5 CP, 4 SWS
Arbeitsaufwand	Gesamtaufwand 5 CP x 25 h = 125 h davon Präsenzzeit 45 h, Selbststudium 80 h
Prüfungsform	laut SPO und Studienplan
Benotung	gemäß §20 der APO in der jeweils gültigen Fassung
Empfohlene Voraussetzungen	keine
Verwendbarkeit	Modul zur Erlangung der notwendigen Leistungspunkte lt. SPO
Lehrsprache	Deutsch
Lehr-/Lernmethoden	Seminaristischer Unterricht, Übung

## Industrieanlagen, Automatisierung und Steuerung

---

Inhalte	<p><b>Einführung in Industrieanlagen, Automatisierungs- und Steuerungstechnik</b></p> <ul style="list-style-type: none"><li>- Ursprung, heutige Bedeutung, Zielsetzung, Anforderungen</li><li>- mechanische, fluidische und elektrische Steuerungen</li></ul> <p><b>Funktionen und Komponenten der Steuerungstechnik</b></p> <ul style="list-style-type: none"><li>- Elektronische programmierbare Steuerungen</li><li>- Schnittstellen zwischen Prozess und Steuerung</li><li>- Anwendung industrieller Kommunikationssysteme</li><li>- Feldbussysteme und Industrielle Ethernet-basierte Kommunikations-Systeme</li><li>- Bedienung und Beobachtung</li><li>- Leitstandstechnik und Betriebsdatenerfassung</li></ul> <p><b>Programmierkonzepte und standardisierte SPS-Programmiersprachen</b></p> <ul style="list-style-type: none"><li>- grundlegende Sprachelemente textueller und graphischer Programmiersprachen</li><li>- Organisation von SPS-Programmen und Steuerungsentwurf</li></ul> <p><b>Methoden und Werkzeuge zur Handhabung von Steuerungssoftware und zur Beherrschung der Komplexität von Steuerungssystemen</b></p> <ul style="list-style-type: none"><li>- Softwareentwicklung für industrielle Anwendungen</li><li>- Inbetriebnahme, Service und Wartung von Steuerungssystemen</li></ul>
---------	--

---

## Industrieanlagen, Automatisierung und Steuerung

---

Qualifikations-  
ziele

**Kenntnisse:**

- Studierende kennen die besonderen Gegebenheiten der Steuerung von ereignisdiskreten Systemen und die grundlegenden Komponenten der Automatisierungstechnik.
- Sie können industrielle Kommunikationssysteme und automatisierungstechnische Komponenten zum Bedienen Beobachten und Diagnostizieren von technischen Prozessen erläutern.

**Fertigkeiten:**

- Studierende können industrielle Steuerungen nach der jeweils gegebenen Aufgabenstellung und dem jeweils gegebenen Einsatzzweck planen.
- Sie können industrielle Steuerungen nach technischen zugleich wirtschaftlichen Gesichtspunkten beurteilen.
- Sie können SPS-Programme nach modernen Methoden der Software-Entwicklung auf Basis standardisierter Programmiersprachen erstellen.

**Kompetenzen:**

- Sie können die für den technischen und organisatorischen Gesamtkontext geeignetsten Automatisierungs-komponenten und SPS-Programmiersprachen auswählen und die Auswahl argumentativ vertreten.
  - Studierende können automatisierungstechnische Problemstellungen eigenständig beurteilen.
  - Sie können sich Informationen aus bereit gestellten Quellen beschaffen und diese kritisch auch in schriftlicher Form vergleichend bewerten.
-



## Industrieanlagen, Automatisierung und Steuerung

---

- Literatur
- Lückenskript zur Vorlesung
  - 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
  - Normen
  - Softwarepakete
-

### Data Literacy and Business Intelligence

Kürzel	IS1C3
Modulbereich	Crossover
Modul- verantwortliche:r	Prof. Dr. Peter Richard
Pflicht/Wahl	Wahlpflicht
Turnus	Sommer- und Wintersemester, jährlich
Dauer	1 Semester
Lehr- veranstaltung	Data Literacy and Business Intelligence
CP / SWS	5 CP, 4 SWS
Arbeitsaufwand	Gesamtaufwand 5 CP x 25 h = 125 h davon Präsenzzeit 60 h, Selbststudium 63,5 h, Prüfungszeit 1,5 h
Prüfungsform	laut SPO und Studienplan
Benotung	gemäß §20 der APO in der jeweils gültigen Fassung
Empfohlene Voraussetzungen	keine
Verwendbarkeit	Modul zur Erlangung der notwendigen Leistungspunkte lt. SPO
Lehrsprache	Deutsch
Lehr-/Lern- methoden	Seminaristischer Unterricht, Übung

## Data Literacy and Business Intelligence

---

- Inhalte
- Die Studierende bekommen in einem ersten Seminarblock die Grundlagen der Data-Literacy vermittelt.
  - Im Rahmen von Analysen mit BI-Werkzeugen fertigen die Studierenden Auswertungen an und hinterfragen die Ergebnisse.
  - So soll ein Bewusstsein für die Komplexität von Datenquellen, -analysen und Interpretation geschaffen werden.
  - Die Studierenden tauschen sich anhand vorgegebener Themen über den Grad der Digitalisierung und Data-Literacy in ihren verschiedenen Unternehmen aus und reflektieren die Unterschiede.
  - Ergänzt wird die Reflektion durch Gastvorträge und weiterer Übungen an BI-Werkzeugen.
-

## Data Literacy and Business Intelligence

---

**Qualifikationsziele**

Übergreifendes Ziel dieses Seminars die Stärkung und Entwicklung einer grundlegenden Datenkompetenz der Teilnehmenden Die Entwicklung zu einer digitalen Gesellschaft zeigt sich auf politischer Ebene durch die Datenstrategie der Bundesregierung und mit der Berliner Erklärung zur Digitalen Gesellschaft. Aus dieser Entwicklung ergibt sich, dass Datenkompetenzen für alle Menschen in dieser zunehmend digitalisierten Welt erforderlich sind. Die Notwendigkeit dieser Kompetenzen wird von der Data-Literacy-Charta unterstrichen, welche die Datenkompetenzen als wichtigen Bestandteil der Bildung unterstreicht. Die Studierenden sollen auf Grundlage von Daten, Entscheidungen treffen können und auf der anderen Seite Risiken durch Fehlinterpretationen der Daten erkennen können. Die Datenkompetenzen werden durch Themen im Umfeld der Business Intelligence vertieft. Hier werden Daten mit Instrumenten der Business Intelligence verarbeitet dargestellt und interpretiert. Die Vermittlung ist dabei unabhängig von einem spezifischen betriebswirtschaftlichen Fachgebiet.

### **Kenntnisse**

Die Studierenden kennen und verstehen

- grundlegende statistische Kenntnisse bei der Interpretation von Daten
- typische Verzerrungen bei der Interpretation von Daten
- Einsatzgebiete von Business Intelligence

### **Fertigkeiten**

Die Studierenden sind in der Lage,

- Daten mit einem neutralen Blick zu interpretieren
- Daten und Interpretation von Daten kritisch zu trennen
- Entscheidungsvorschläge auf Datenbasis zu erstellen
- einfache Data Pipelines umsetzen
- Berechtigungskonzepte erstellen

### **Kompetenzen**

Die Studierenden können

- interdisziplinär Erkenntnisse aus Daten gewinnen
- Daten in einem Team analysieren
- Daten kritisch bewerten und interpretieren

## Data Literacy and Business Intelligence

---

- Literatur
- 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-Sicherheit

Englische Modulbezeichnung	IT Security
Kürzel	ISCO.ITSICH
Modulbereich	Crossover
Modulverantwortliche:r	Prof. Lothar Braun
Pflicht/Wahl	Pflicht
Turnus	Winter- und Sommersemester, jährlich
Dauer	1 Semester
Lehrveranstaltung	IT-Sicherheit
CP / SWS	5 CP, 4 SWS
Arbeitsaufwand	Gesamtaufwand 5 CP x 25 h = 125 h davon Präsenzzeit 45 h, Selbststudium 80 h
Prüfungsform	laut SPO und Studienplan
Benotung	gemäß §20 der APO in der jeweils gültigen Fassung
Empfohlene Voraussetzungen	keine
Verwendbarkeit	Modul zur Erlangung der notwendigen Leistungspunkte lt. SPO
Lehrsprache	deutsch
Lehr-/Lernmethoden	Seminaristischer Unterricht, Übung
Inhalte	Die Lehrveranstaltung gibt einen Überblick über die Teilgebiete der IT-Sicherheit aus Sicht eines Anwenders. Dazu zählen relevante Standards, typische Angriffe, Sicherheitsprozesse und die Analyse von Bedrohungen und Risiken. Kryptographische Bausteine wie Verschlüsselung, Signatur und Hashfunktionen werden aus Sicht des Programmierers/Anwenders eingeführt. Grundlegende Aspekte der Sicherheit von eingebetteten Systemen, von Netzen und Web-Anwendungen werden besprochen.

## IT-Sicherheit

---

Qualifikations- ziele	<p>Nach erfolgreicher Teilnahme am Modul sind die Studierenden in der Lage:</p> <ul style="list-style-type: none"><li>- Grundbegriffe der IT-Sicherheit zu erklären.</li><li>- typische Angriffe zu beschreiben.</li><li>- die Methodik der Bedrohungs- und Risikoanalyse auf ein einfaches Szenario anzuwenden.</li><li>- die Grundlagen kryptographischer Algorithmen darzustellen.</li><li>- einfache kryptographische Anwendungen zu implementieren.</li><li>- einfache Sicherheitseigenschaften von Netzwerken, Geräten und Web-Anwendungen zu analysieren.</li><li>- einfache Sicherheitsmaßnahmen für Netzwerke, Geräte und Web-Anwendungen zu planen.</li></ul>
--------------------------	---

---

Literatur	Wird in der Vorlesung bekannt gegeben.
-----------	--

---

### Industrial Security Basics

ID	ISB
Study section	Crossover
Responsible lecturer	Prof. Dr. Helia Hollmann
Mandatory/elective	elective
Rotation	Sommer term, annually
Duration	1 term
Course	Industrial Security Basics
CP / SWS	5 CP, 4 SWS
Workload	Total 5 CP x 25 h = 125 h thereof attendance 45 h, self-study 79 h, exam 1 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



## Industrial Security Basics

---

Contents	<p>Students will develop a foundational understanding of the essential terms, technologies, and components of IT and OT security within digitalized production environments. This encompasses a thorough comprehension of the threat landscape necessary for evaluating a company's risk profile. Furthermore, students will gain comprehensive knowledge of both technical and organizational measures. On a technical front, these measures encompass adherence to fundamental principles of network security as per ISO 62443 standards. Practical implementation of security measures mandated by the standard will be executed using the BSI basic protection framework. Standard network analysis tools will be employed, alongside network segmentation and secure configuration of switches and firewalls. Backup strategies and patch management are discussed. On an organizational level, students will be introduced to Information Security Management Systems (ISMS) along with threat and risk analysis methodologies. They will learn to enact policies through rights and role management and become acquainted with tools for identifying network anomalies such as Security Information and Event Management (SIEM) systems and Intrusion Detection Systems (IDS). Hands-on exercises will reinforce the practical aspects of the curriculum.</p>
----------	--

---

## Industrial Security Basics

---

Module objectives

**Knowledge:**

- Students acquire a basic understanding of the relevant terminology, technologies and elements of IT/OT security.
- Students learn about the special features of industrial networks and protocols and their impact on IT/OT security.
- Students know standard tools for network analysis and can carry out a network analysis.

**Skills:**

- They are proficient in network segmentation and configuration of switches and firewalls.
- They can configure automation components securely.
- They are capable of conducting threat and risk analyses using straightforward scenarios.
- The knowledge acquired enables students to secure networks in accordance with ISO 62443.
- They are able to implement recommendations of the BSI basic protection.

**Competences:**

- Students can evaluate a cryptographic software library in a specific project and select a suitable one.
-

## Industrial Security Basics

---

- Literature
- Skript by lecturer
  - Documentations of Hardware components and Software libraries
  - BSI: ICS-Security -Kompendium, 11/2014, available under <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, VDE Verlag.2024
  - Singh, G.D.: The Ultimate Kali Linux Book: Perform advanced penetration testing using Nmap, Metasploit, Aircrack-ng, and Empire, 2/2022, ISBN 978-1801818933
-

### **Human Recource and Organisation Management**

Study section	Crossover
Responsible lecturer	Prof. Dr. Sarah Hatfield
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	<ul style="list-style-type: none"> <li>- Organisational Management Orientations</li> <li>- Organisational Diagnosis and Design Theories</li> <li>- Organisational Development &amp; Transformation</li> <li>- Organisational Behaviour &amp; Leadership</li> <li>- Organisation of Talent Management</li> <li>- Organisation of Innovation &amp; Performance Management</li> </ul>

## Human Resource 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 responsibilities 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 Resource 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.
-

### Introduction to Safety and Human Machine Interaction

ID	IS1G1
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	IS1G2
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	IS1G4
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	<ul style="list-style-type: none"> <li>- Methods for scientific writing and presentation</li> <li>- Independent in-depth research into a current topic</li> <li>- Writing of report in the style of a research paper</li> <li>- Review of other students` reports</li> <li>- Revision of own report based on reviews</li> <li>- Presentation of reports</li> </ul>



## 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	IS2S1
Study section	Pflichtbereich / Mandatory area
Responsible lecturer	Prof. Dr. Helia Hollmann
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	<p>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.</p> <p>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.</p>

## 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.

---

### Deutsch B2.1

Englische Modulbezeichnung	German B2.1
Kürzel	IS1SP1
Modulbereich	Pflichtbereich International
Modulverantwortliche:r	Maria Lena Weinkam
Pflicht/Wahl	Pflicht
Turnus	Sommersemester, jährlich
Dauer	1 Semester
Lehrveranstaltung	Deutsch B2.1
CP / SWS	5 CP, 4 SWS
Arbeitsaufwand	Gesamtaufwand 5 CP x 25 h = 125 h davon Präsenzzeit 60 h, Selbststudium 63,5 h, Prüfungszeit 1,5 h
Prüfungsform	laut SPO und Studienplan
Benotung	gemäß §20 der APO in der jeweils gültigen Fassung
Empfohlene Voraussetzungen	Deutsch B1.2
Verwendbarkeit	Modul zur Erlangung der notwendigen Leistungspunkte lt. SPO
Lehrsprache	deutsch
Lehr-/Lernmethoden	Seminaristischer Unterricht, Übung

## Deutsch B2.1

---

Inhalte	<p>Dieser Kurs schließt an den B1.2.-Kurs an. Er festigt und vertieft grammatische Strukturen für den alltäglichen Einsatz. Kommunikative Übungen verbessern die spontane Anwendung korrekter Grammatik und Redemittel. Folgende grammatische Strukturen werden im Kurs behandelt:</p> <ul style="list-style-type: none"><li>- Satzbau und Negation</li><li>- zweiteilige Konnektoren</li><li>- Relativsätze</li><li>- Passiv und Passiversatzformen</li><li>- Reflexivpronomen</li><li>- Modalsätze</li><li>- Wortbildung</li></ul>
Qualifikationsziele	<p><b>Kenntnisse:</b> Das Modul vermittelt die alltagspragmatischen, produktiven und rezeptiven Kompetenzen auf dem Referenzniveau B2.1 des Gemeinsamen Europäischen Referenzrahmens.</p> <p><b>Fertigkeiten:</b></p> <ul style="list-style-type: none"><li>- Studierende können Hauptinhalte komplexerer Texte verstehen.</li><li>- Sie können sich in Standardsituationen fließend in der Lernsprache verständigen.</li></ul> <p><b>Kompetenzen:</b> Sie werden befähigt, ein Studium, ein Praktikum, einen Projekt- oder Forschungsaufenthalt in einem deutschsprachigen Land erfolgreich zu bewältigen.</p>
Literatur	Kompass DaF B2.1, Kurs- und Arbeitsbuch, Klett Verlag

---

### Deutsch B2.2

Englische Modulbezeichnung	German B2.2
Kürzel	IS2SP2
Modulbereich	Pflichtbereich International
Modulverantwortliche:r	Maria Lena Weinkam
Pflicht/Wahl	Pflicht
Turnus	Wintersemester, jährlich
Dauer	1 Semester
Lehrveranstaltung	Deutsch B2.2
CP / SWS	5 CP, 4 SWS
Arbeitsaufwand	Gesamtaufwand 5 CP x 25 h = 125 h davon Präsenzzeit 60 h, Selbststudium 63,5 h, Prüfungszeit 1,5 h
Prüfungsform	laut SPO und Studienplan
Benotung	gemäß §20 der APO in der jeweils gültigen Fassung
Empfohlene Voraussetzungen	Deutsch B2.1
Verwendbarkeit	Modul zur Erlangung der notwendigen Leistungspunkte lt. SPO
Lehrsprache	deutsch
Lehr-/Lernmethoden	Seminaristischer Unterricht, Übung

## Deutsch B2.2

---

Inhalte	<p>Dieser Kurs festigt und vertieft aufbauend auf B2.1 grammatische Strukturen für den alltäglichen Einsatz. Kommunikative Übungen verbessern die spontane Anwendung korrekter Grammatik und Redemittel.</p> <p>Folgende grammatische Strukturen werden im Kurs behandelt:</p> <ul style="list-style-type: none"><li>- Modalsätze - Vertiefung</li><li>- Indefinitpronomen</li><li>- Adjektivdeklination</li><li>- Genitivattribute / Genitivobjekte</li><li>- komplexe Sätze</li><li>- Wortbildung</li></ul>
Qualifikationsziele	<p><b>Kenntnisse:</b> Das Modul vermittelt die allgemeinsprachigen, produktiven und rezeptiven Kompetenzen auf dem Referenzniveau B2.1 des Gemeinsamen Europäischen Referenzrahmens.</p> <p><b>Fertigkeiten:</b></p> <ul style="list-style-type: none"><li>- Studierende können Hauptinhalte komplexerer Texte verstehen.</li><li>- Sie können sich in Standardsituationen fließend in der Lernsprache verständigen.</li></ul> <p><b>Kompetenzen:</b> Sie werden befähigt, ein Studium, ein Praktikum, einen Projekt- oder Forschungsaufenthalt in einem deutschsprachigen Land erfolgreich zu bewältigen.</p>
Literatur	Kompass DaF B2.2, Kurs- und Arbeitsbuch, Klett Verlag

---



### **Management, Mitarbeiterführung und IT-Recht**

Englische Modulbezeichnung	Management, Leadership & IT-Legislation
Kürzel	IS1G3
Modulbereich	Pflichtbereich Safety und Security
Modulverantwortliche:r	Prof. Dr. Sarah Hatfield
Pflicht/Wahl	Pflicht
Turnus	Sommersemester, jährlich
Dauer	1 Semester
Lehrveranstaltung	Management, Mitarbeiterführung und IT-Recht
CP / SWS	5 CP, 4 SWS
Arbeitsaufwand	Gesamtaufwand 5 CP x 25 h = 125 h davon Präsenzzeit 45 h, Selbststudium 78,5 h, Prüfungszeit 1,5 h
Prüfungsform	laut SPO und Studienplan
Benotung	gemäß §20 der APO in der jeweils gültigen Fassung
VORAUSSETZUNG	keine
Verwendbarkeit	laut SPO und Studienplan
Lehrsprache	deutsch
Lehr-/Lernmethoden	Seminaristischer Unterricht, Übung

## Management, Mitarbeiterführung und IT-Recht

---

- Inhalte
- Grundlagen und grundlegende Methoden des Managements (Aufbauorganisation und Betriebsorganisation) und der Mitarbeiterführung
  - Spiegelung der Sicherheitsaspekte auf betriebswirtschaftliche Bedeutung von Daten und Informationen
  - Bewertung der Sicherheitsrelevanz von Daten und Informationen aus Managementsicht
  - Entscheidungs-Eskalationswege und darauf ausbauende Zugriffs- bzw. Rechtevergabe in Organisationen (Businessrules)
  - Entwicklung und Einführung/Kommunikation und Durchsetzung von Leitlinien und Regularien zur internen und externen Absicherung (Abwehr von Social-Engineering)
  - Entwicklung und Einführung von Schulungskonzepten bezogen auf unterschiedliche Sicherheitsklassen.
  - Entwicklung von umfänglichen Konzepten zur Sicherung von Daten und Informationen.
  - Privatrecht
    - Rechtsgeschäfte
    - Allgemeines und Besonderes Schuldrecht
    - Sachenrecht
  - Internetrecht
    - Schutz von Domains
    - Electronic Commerce
    - Schadensersatzhaftung und Haftungsbeschränkung
  - Urheberrecht/Wettbewerbsrecht
    - Grundbegriffe
    - Schutz und Haftung
    - Schadensersatzansprüche
  - Datenschutz
    - Merkmale und Grundbegriffe
    - Anwendbare Rechtsvorschriften
    - Telekommunikationsdatenschutz
  - Rechtliche Aspekte der IT-Forensik
-

## Management, Mitarbeiterführung und IT-Recht

---

Qualifikations-  
ziele

### **Kenntnisse:**

- Studierende kennen die Bedeutung von Daten- und Informationssicherheit aus betriebswirtschaftlicher Sicht.
- Sie kennen die sicherheitsrelevanten Aspekte der Aufbauorganisation, Betriebsorganisation und Mitarbeiterführung.
- Sie kennen Methoden und Maßnahmen des Managements und der Mitarbeiterführung, die Sicherheitskonzepte ermöglichen und unterstützen (z.B. Eskalationswege, Rechtevergabe, (Kommunikations-)Leitlinien, Businessrules, Schulungen).
- Sie kennen Grundzüge des Privatrechts und Grundzüge des DV-Rechts mit der Bedeutung des Datenschutzes sowie die praktische Bedeutung.

### **Fertigkeiten:**

- Studierende können für betriebliche insb. auch betriebswirtschaftlich relevante Abläufe sicherheitsrelevante Daten und Informationen identifizieren.
- Sie können die Sicherheitsrisiken/Bedrohungen die sich aus Aufbauorganisation, Betriebsorganisation und Mitarbeiterkreisen identifizieren.
- Sie können Methoden anwenden, um die Sicherheitsrisiken und Bedrohungen zu reduzieren
- Sie können in Grundzügen Betriebsvorfälle im Sinne einer juristischen Fallbearbeitung im Vertragsrecht bearbeiten

### **Kompetenzen:**

- Studierende sind in der Lage Sicherheitsrisiken/Bedrohungen aus Aufbauorganisation, Betriebsorganisation und Mitarbeiterführung einzuschätzen und geeignete Gegenmaßnahme zu entwickeln/zu bewerten.
- Sie sind in der Lage rechtliche Rahmenbedingungen einzuschätzen und die juristische Bedeutung von Sicherheitsrisiken/Bedrohungen bei der Ausarbeitung von Maßnahmen zu berücksichtigen.

## Management, Mitarbeiterführung und IT-Recht

---

### Literatur

#### 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, Stand Juni 2023, abrufbar im Internet:  
[https://www.itm.nrw/wp-content/uploads/Skript\\_IT-Vertragsrecht\\_Stand\\_Juni\\_2023.2.pdf](https://www.itm.nrw/wp-content/uploads/Skript_IT-Vertragsrecht_Stand_Juni_2023.2.pdf)
  - Beck Texte im dtv, IT- und Computerrecht, 16. Auflage 2023
  - Redeker, IT-Recht, 8. Aufl. 2023
  - Erben/Günther, Gestattung und Management von IT-Verträgen, 4. Aufl. 2023
-

### Zertifizierungsmodul

Englische Modulbezeichnung	Certification Module
Kürzel	IS2S1
Modulbereich	Pflichtbereich Safety und Security
Modulverantwortliche:r	Prof. Dr. Helia Hollmann
Pflicht/Wahl	Pflicht
Turnus	Wintersemester, jährlich
Dauer	1 Semester
Lehrveranstaltung	Zertifizierungsmodul
CP / SWS	5 CP, 4 SWS
Arbeitsaufwand	Gesamtaufwand 5 CP x 25 h = 125 h davon Präsenzzeit 45 h, Selbststudium 78,5 h, Prüfungszeit 1,5 h
Prüfungsform	laut SPO und Studienplan
Benotung	gemäß §20 der APO in der jeweils gültigen Fassung
Empfohlene Voraussetzungen	Introduction to Safety and Human Machine Interaction
Verwendbarkeit	Modul zur Erlangung der notwendigen Leistungspunkte lt. SPO
Lehrsprache	Deutsch
Lehr-/Lernmethoden	Seminaristischer Unterricht, Übung

## Zertifizierungsmodul

---

Inhalte	<p>Die Lehrveranstaltung behandelt die Themen funktionale Sicherheit, Informations-Sicherheits-Managementsysteme (ISMS) und Datenschutz. Der Schwerpunkt der Lehrveranstaltung liegt auf der funktionalen Sicherheit. Die Studierenden erwerben grundlegende Kenntnisse der funktionalen Sicherheit und können Risikoanalysen durchführen sowie Sicherheitsmaßnahmen umsetzen. Sie beherrschen den Sicherheitslebenszyklus und die Managementprozesse für eine sichere Entwicklung. Darüber hinaus wenden sie grundlegende Techniken der Hardware- und Softwareentwicklung für funktionale Sicherheit an und bewerten Sicherheitsarchitekturen. Die Lehrveranstaltung umfasst Grundlagen des ISMS, einschließlich Definition und betrieblichem Nutzen. Es werden Facetten des ISMS behandelt wie Sicherheitsregelwerke und Asset-Klassifizierung. Auch wird diskutiert, welche Akteure einzubinden sind und welche Sicherheitszertifizierungen existieren. Im Datenschutzbereich werden die Vorgaben der Datenschutz-Grundverordnung erläutert, die Unternehmen einhalten müssen, um gesetzeskonform zu agieren. Anschließend wird eine Übersicht über die internationalen Datenschutzerfordernungen gegeben und diskutiert, wie Unternehmen diesen gerecht werden können.</p>
---------	--

---

## Zertifizierungsmodul

---

Qualifikations-  
ziele

**Kenntnisse:**

- Studierende kennen die Hintergründe eines risikobasierten Informationssicherheitsmanagementsystems (ISMS) und können die grundlegenden Begriffe benennen und an Beispielen erklären.
- Studierende können die grundlegenden Begriffe der funktionalen Sicherheit verstehen und erklären und kennen qualitative und quantitative Techniken und Maßnahmen zur Erreichung der funktionalen Sicherheit.

**Fertigkeiten:**

- Studierende haben das Rüstzeug, sich mit normativer Literatur auseinander zu setzen.
- Studierende können den entsprechend der funktionalen Sicherheit geforderten Sicherheitslebenszyklus von Erstellung des Konzepts, über Gefährdungs- und Risikobeurteilung mit Erstellung einer Sicherheitsanforderungsspezifikation und nachfolgender HW und SW Entwicklung bis hin zur Außerbetriebnahme anwenden.
- Studierende verfügen über das Wissen, was zum Aufbau einer ISMS Struktur auf Vorgaben der ISO 27001 notwendig ist. Studierende kennen die Datenschutz-Grundverordnung an Unternehmen in Deutschland und Europa.

**Kompetenzen:**

- Die Studierenden haben grundlegende Kenntnisse in der Sicherheitstechnik und können die Grundlagen anwenden.

---

Literatur

- Vortragsfolien, Begleit- und Übungsmaterial 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

Kürzel	ISWP.AST
Modulbereich	Wahlpflichtbereich 1 Security
Modul- verantwortliche:r	Dr. Matthias Niedermaier
Pflicht/Wahl	Wahlpflicht
Turnus	Sommersemester, jährlich
Dauer	1 Semester
Lehr- veranstaltung	Advanced Security Testing
CP / SWS	5 CP, 4 SWS
Arbeitsaufwand	Gesamtaufwand 5 CP x 25 h = 125 h davon Präsenzzeit 45 h, Selbststudium 78,5 h, Prüfungszeit 1,5 h
Prüfungsform	laut SPO und Studienplan
Benotung	gemäß §20 der APO in der jeweils gültigen Fassung
Empfohlene Voraussetzungen	Kenntnisse in IT-Sicherheit unabdingbar
Verwendbarkeit	Wahlpflichtmodul zur Erlangung der notwendigen Leistungs- punkte lt. SPO
Lehrsprache	deutsch
Lehr-/Lern- methoden	Seminaristischer Unterricht, Übung



## Advanced Security Testing

---

Inhalte	<p>Standards bei Security Tests</p> <ul style="list-style-type: none"><li>- Berichterstellung</li><li>- Verwenden von Tools</li><li>- Auszug nicht komplett: Nessus, OpenVAS, Metasploit, binwalk, Firmwaremodification kit, ZAP, Checkstyle, CCP Check, burp suite</li><li>- Erstellung eigener Skripte um aktuelle IT-Sicherheitsaspekte zu beleuchten</li><li>- Vorgehen bei Softwaretests</li><li>- Vorgehen bei Produkttests / Hardwaretests</li><li>- Vorgehen beim Testen von IT Landschaften</li><li>- Aktueller Stand von Technik und Forschung in Bezug auf IT-Sicherheit wird vermittelt</li></ul> <p>Vorgehen</p> <ul style="list-style-type: none"><li>- Im Rahmen der Vorlesung werden folgende Themenbereiche der IT-Sicherheit beleuchtet:<ul style="list-style-type: none"><li>- Netzwerksicherheit</li><li>- Hardwaretests</li><li>- Softwaretestmethoden</li></ul></li><li>- Es werden Schwachstellen und Schutzmaßnahmen praktisch an aktuellen Geräten und Software durchgeführt.</li><li>- Die Studierenden müssen in Projektgruppen eine wissenschaftliche Fragestellung bearbeiten, hier werden Themenfelder vertieft und der Stand der Forschung aufgegriffen.</li></ul>
---------	---

---

## Advanced Security Testing

---

Qualifikations-  
ziele

**Kenntnisse:**

- In der Vorlesung soll mit praxisnahen Fragestellungen die Planung, das Vorgehen und der Abschluss von Security Tests besprochen werden. Um die Vorlesung möglichst nahe an der beruflichen Praxis zu halten, wird ein vielfältiges Spektrum an Tools/Werkzeugen verwendet.
- Es wird Wert auf eine möglichst breite Themenvielfalt in diesem Bereich gelegt. Das Aufspüren von Softwareschwachstellen im Source Code, Testen von ganzen Netzwerken sowie Hardwarenahe Fragestellungen gehören dazu.

**Fertigkeiten:**

- Durchführen von klassischen Security Produkttests
- Durchführen von Netzwerksicherheitstests
- Angriffe und Verteidigung auf Hardware
- Durchführen von Softwaretests

**Kompetenzen:**

- Die Studierenden können Penetrationstests u.a. mit Hilfe von Tools durchführen
- Sie können sich in neue Thematiken im Rahmen von Sicheren Architekturen einarbeiten
- Studierende sind in der Lage Produkte grundlegend auf ihr IT-Sicherheitsniveau zu prüfen

---

Literatur

- 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.
  - Skript
-

### Einführung in die IT-Forensik

Englische Modulbezeichnung	Basics of IT Forensics
Kürzel	ISWP.ITFORE
Modulbereich	Wahlpflichtbereich 1 Security
Modulverantwortliche:r	Dr. Kay Werthschulte
Pflicht/Wahl	Wahlpflicht
Turnus	Wintersemester, jährlich
Dauer	1 Semester
Lehrveranstaltung	Einführung in die IT-Forensik
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	Vorlesung IT Sicherheit wünschenswert, aber nicht Ausschlusskriterium
Verwendbarkeit	Wahlpflichtmodul zur Erlangung der notwendigen Leistungspunkte lt. SPO
Lehrsprache	deutsch
Lehr-/Lernmethoden	Seminaristischer Unterricht, Übung
Inhalte	<ul style="list-style-type: none"><li>- Einführung in die Digitale Forensik</li><li>- Vorgehensmodelle</li><li>- Sicherstellung digitaler Spuren</li><li>- Analyse digitaler Spuren</li><li>- Festplattenforensik</li><li>- Windows Forensik</li><li>- Arbeitsspeicherforensik</li><li>- Netzwerkforensik</li><li>- Mobile Forensik</li><li>- Malware Analyse</li></ul>

### Einführung in die IT-Forensik

---

**Qualifikationsziele** Die Vorlesung Digitale Forensik befasst sich mit der Sicherstellung, Analyse und Präsentation digitaler Spuren nach einem Vorfall. Die Studierenden bekommen dabei einen Überblick über forensische Vorgehensweisen, über IT Angriffe sowie über die zugrundeliegenden Technologien. Da es sich um eine integrierte Vorlesung handelt, wird das Gehörte direkt in der Vorlesung umgesetzt, wodurch eine enge Kopplung zwischen Theorie und Praxis erreicht wird. Die Teilnehmer sollten nach der Vorlesung in der Lage sein, festzustellen ob ein Angriff stattgefunden hat und wissen wie man digitale Beweise sicherstellt und analysiert.

---

**Literatur**

- 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	IS2S4
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
    - Cryptographic 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

Kürzel	ISWP.NETP
Modulbereich	Wahlpflichtbereich 1 Security
Modul- verantwortliche:r	Dr. Lothar Braun
Pflicht/Wahl	Wahlpflicht
Turnus	Sommersemester, jährlich
Dauer	1 Semester
Lehr- veranstaltung	Network Penetration Testing
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	- Modul IT-Sicherheit - Modul Datenkommunikation
Verwendbarkeit	Wahlpflichtmodul zur Erlangung der notwendigen Leistungs- punkte lt. SPO
Lehrsprache	deutsch
Lehr-/Lern- methoden	Seminaristischer Unterricht, Übung



## Network Penetration Testing

---

Inhalte	<ul style="list-style-type: none"><li>- Planung von Penetration Tests für Netzwerke</li><li>- Erstellung von Berichten</li><li>- Informationsgewinnung im Netzwerk<ul style="list-style-type: none"><li>- Techniken zur Erkennung von Maschinen und Diensten in Netzwerken mit gängigen Werkzeugen</li><li>- Untersuchung von Angriffsoberflächen von Netzwerkdiensten</li><li>- Identifikation von potentiellen Schwachstellen in Netzwerkdiensten</li></ul></li><li>- Angriffe auf Netzwerkdienste<ul style="list-style-type: none"><li>- Passwortangriffe</li><li>- Angriffe auf Web-Anwendungen</li><li>- Analyse, Anpassung und Verwendung von Exploits</li><li>- Buffer-Overflow Exploits</li><li>- Entwicklung von Scripten zur Durchführung von Angriffen</li></ul></li></ul>
Qualifikationsziele	<ul style="list-style-type: none"><li>- Die Studierenden erwerben Kenntnisse über die Durchführung von Penetration Tests in Computernetzwerken.</li><li>- Studierende lernen die Anwendung von Techniken zur Informationsgewinnung im Netzwerk. Sie kennen die relevanten Techniken zur Identifikation von Schwachstellen.</li><li>- Die Studierenden lernen die Techniken zur Durchführung von Angriffen zur Demonstration gefundener Schwachstellen kennen, um sie in der Lage diese mittels bekannter Tools anzuwenden. Sie sind in der Lage Handlungsempfehlungen zur Beseitigung der Schwachstellen zu geben.</li></ul>
Literatur	Wird in der Vorlesung bekannt gegeben.

---

### Project IT-Security

ID	ISWP.ITS-P
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	IS2S3.P
Study section	Wahlpflichtbereich 1 International und Safety / Compulsory elective area 1 International and Security
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

Kürzel	IS2S3
Modulbereich	Wahlpflichtbereich 1 Safety
Modul- verantwortliche:r	Prof. Dr. Wolfgang Zeller
Pflicht/Wahl	Wahlpflicht
Turnus	Wintersemester, jährlich
Dauer	1 Semester
Lehr- veranstaltung	Safety
CP / SWS	5 CP, 4 SWS
Arbeitsaufwand	Gesamtaufwand 5 CP x 25 h = 125 h davon Präsenzzeit 45 h, Selbststudium 78,5 h, Prüfung 1,5 h
Prüfungsform	laut SPO und Studienplan
Benotung	gemäß §20 der APO in der jeweils gültigen Fassung
Empfohlene Voraussetzungen	Introduction to Safety, Security and Human Machine Interac- tion
Verwendbarkeit	Modul zur Erlangung der notwendigen Leistungspunkte lt. SPO
Lehrsprache	Deutsch
Lehr-/Lern- methoden	Seminaristischer Unterricht

## Safety

---

### Inhalte

#### **Einführung**

- Anwendungsbeispiele, heutige Bedeutung, Zielsetzung

#### **Mathematische Grundlagen**

- Zufallsereignisse und Wahrscheinlichkeitsrechnung
- Ausfallverhalten technischer Systeme und Verteilungsfunktionen
- Markov Modellierung

#### **Methoden der Risikoanalyse und -bewertung**

- FMEA und FMEDA
- Fehlerbäume

#### **Sicherheitsrelevante Systemarchitekturen und deren Berechnung**

- ein- und mehrkanalige Systeme
- Berechnung charakteristische Größen zur Beschreibung von Ausfallwahrscheinlichkeit und Diagnosedeckungsgrad

#### **Methoden zur Vermeidung von Fehlern gemeinsamer Ursache**

- technische und organisatorische Maßnahmen
- Eingang in die Berechnung des Ausfallverhaltens

#### **Entwicklung sicherheitsrelevanter Steuerungssoftware**

- Grundlegende Verfahren zur Vermeidung von systematischen Fehlern
- Eingang in die methodische Entwicklung und den Nachweis sicherheitsrelevanter Steuerungssysteme

#### **Methoden der Verifikation und Validierung**

- Grundlagen des Testens und zum Nachweis der Eigenschaften sicherheitsrelevanter Steuerungen
- rechnerunterstützte Methoden

#### **Exemplarische Anwendung der mathematischen und methodischen Grundlagen**

- Produktionsmaschinen (Betriebsarten)
- Industrieroboter (Mensch-Maschine-Kollaboration)
- Kraftfahrzeugtechnik (autonomes Fahren)

## Safety

---

Qualifikations-  
ziele

### **Kenntnisse:**

- Studierende kennen die mathematischen und theoretischen Grundlagen der Wahrscheinlichkeitsrechnung und des Ausfallverhaltens technischer System.
- Sie können das methodische Vorgehen zur Gestaltung von Sicherheitsfunktionen anhand relevanter Basis-Normen skizzieren.

### **Fertigkeiten:**

- Studierende können die funktionale Sicherheit von Steuerungen gemäß gesetzlicher wie normativer Anforderungen rechnerisch nachzuweisen.
- Darauf aufbauend sind Studierende in der Lage, Verfahren zum methodischen Vorgehen und zum Nachweis der Eigenschaften von sicherheitsrelevanten Systemen gezielt anzuwenden.

### **Kompetenzen:**

- Anhand praktischer Anwendungsfälle aus verschiedenen Bereichen erlangen Studierende die Fähigkeit, das Basiswissen auf branchenspezifischen Fragestellungen erfolgreich zu übertragen.
  - Sie können funktionale Sicherheit von Steuerungen nach technischen und auch wirtschaftlichen Gesichtspunkten eigenständig beurteilen.
-



## Safety

---

### Literatur

- Vortragsfolien, Begleit- und Übungsmaterial in moodle
  - Goble, W.: Control Systems Safety Evaluation and Reliability, 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 Straightforward 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.
-

### Sichere Geschäftsprozesse

Englische Modulbezeichnung	Secure Business Processes
Kürzel	IS2S2
Modulbereich	Wahlpflichtbereich 1 Safety
Modulverantwortliche:r	Prof. Dr. Jana Görmer-Redding
Pflicht/Wahl	Wahlpflicht
Turnus	Wintersemester, jährlich
Dauer	1 Semester
Lehrveranstaltung	Sichere Geschäftsprozesse
CP / SWS	5 CP, 4 SWS
Arbeitsaufwand	Gesamtaufwand 5 CP x 25 h = 125 h davon Präsenzzeit 60 h, Selbststudium 90 h
Prüfungsform	laut SPO und Studienplan
Benotung	gemäß §20 der APO in der jeweils gültigen Fassung
Empfohlene Voraussetzungen	keine
Verwendbarkeit	Wahlpflichtmodul zur Erlangung der notwendigen Leistungspunkte lt. SPO
Lehrsprache	Deutsch, englische Anteile
Lehr-/Lernmethoden	Seminaristischer Unterricht, Übung

## Sichere Geschäftsprozesse

---

**Inhalte** Im Kontext der wachsenden Digitalisierung in allen Bereichen gewinnt IT-Sicherheit (auch IT-Security) entscheidend an Bedeutung und stellt Unternehmen vor weitreichende Herausforderungen. In der Veranstaltung werden die Studierenden sich mit entscheidenden Aspekten von sicheren Geschäftsprozessen in einer digitalisierten Welt auseinandersetzen. Die Veranstaltung ist in zwei Hauptteile unterteilt: Einerseits erlernen die Studierenden im Teil „Grundlagen der IT-Sicherheit für Geschäftsprozesse“, wie in der Anwendung Geschäftsprozesse in der SAP-ERP Software korrekt und sicher abgebildet werden können. Andererseits verdeutlicht der zweite Teil der Veranstaltung „Risikomanagement und Chancen der Digitalisierung“, welche Maßnahmen und Werkzeuge zur Identifikation, Analyse, Bewertung und Steuerung von IT-Security Risiken angewendet werden können. Das spezifische Wissen wird mit externen Vorträgen angereichert und mit Übungen und Fallstudien, bzw. Ausarbeitungen zu den Teilthemenbereichen für die Anwendung unterstützt.

### **Teil 1: Grundlagen der IT-Sicherheit für Geschäftsprozesse**

- *Einführung in die digitale Transformation:* Die Studierenden lernen die grundlegenden Konzepte und Trends der digitalen Transformation kennen und verstehen deren Auswirkungen auf Geschäftsprozesse.
- *Sicherheitsgrundlagen für Geschäftsprozesse:* Dieser Teil behandelt die wichtigsten Sicherheitsprinzipien und -konzepte, die bei der Gestaltung und Implementierung sicherer Geschäftsprozesse berücksichtigt werden sollten.
- *Sicherheit in SAP-ERP:* Die Studierenden vertiefen ihr Verständnis für die Sicherheit von Geschäftsprozessen in der SAP-ERP-Software. Dies beinhaltet den Schutz von Daten, Zugriffskontrollen und die sichere Konfiguration von SAP-Systemen.

Keywords: Rahmen und Sicherheitsanforderungen im Kontext der Verwendung von SAP, SAP Autorisierung, SAP ABAP Autorisierung, SAP GRC Access Control, SAP Identity Management System (IdM), SAP HANA Database

### **Teil 2: Risikomanagement und Chancen der Digitalisierung**

- *Chancen und Risiken der Digitalisierung:* In diesem Abschnitt werden die Chancen und Herausforderungen der Digitalisierung für Unternehmen diskutiert. Dabei liegt ein besonderer Schwerpunkt auf den damit verbundenen Sicherheitsrisiken.
- *Identifikation und Analyse von IT-Security Risiken:* Die Studierenden lernen, wie man potenzielle Risiken für Geschäftsprozesse identifiziert und analysiert.

## Sichere Geschäftsprozesse

---

### Qualifikations- ziele

#### **Kenntnisse:**

- Nach erfolgreicher Teilnahme an diesem Modul verstehen die Studierenden die ökonomischen und informationstechnischen Grundlagen der Digitalisierung und der damit einhergehenden Chancen und Risiken für Geschäftsmodelle und -prozesse.
- Darüber hinaus lernen die Studierenden verschiedene Arten von Risiken kennen und wie sie diese voneinander abgrenzen können. Aus Sicht der IT-Sicherheit wird dabei diskutiert, wie sich die Bedrohungslandkarte durch die voranschreitende Digitalisierung verändert, welche Sicherheitsrisiken einer IT-Lösung (Security, Compliance, Zuverlässigkeit) zu beachten sind und wie diese Risiken bewertet und gesteuert werden können.
- Studierende lernen Methoden zur Identifikation, Quantifizierung, Steuerung und Überwachung von Risiken anhand des Risikomanagementkreislaufs.
- Die Studierenden wissen, wie Risiken insbesondere im Bereich der IT-Sicherheit mit Hilfe von verschiedenen, quantitativen Risikomaßen zu bewerten sind und können diese ökonomisch interpretieren. Sie lernen risikoadjustierte Bewertungsansätze zur Evaluierung und Priorisierung von IT-Sicherheitsmaßnahmen kennen und wenden diese anhand praktischer Beispiele an.

#### **Fertigkeiten:**

- Studierende können die Chancen und Risiken der digitalen Transformation von Unternehmen identifizieren, bewerten, steuern und überwachen.
- Studierende können dieses Wissen auf praktische Anwendungsfälle übertragen.

#### **Kompetenzen:**

- Die Studierenden erlernen wichtige betriebswirtschaftliche Grundlagen eines integrierten Chancen- und Risikomanagements im Kontext einer sicheren Industrie 4.0.
- Diese Kompetenzen tragen zum interdisziplinären Ausbildungsziel des Studiengangs bei, da auch Spezialisten für industrielle Sicherheit Chancen und Risiken einschätzen und u.a. Investitionsentscheidungen im Bereich Cyber Security treffen und priorisieren können müssen.
- Case Study: Durch die Koordination der Teammitglieder und die Verteilung von Aufgaben innerhalb des Teams lernen die Studierenden auch

## Sichere Geschäftsprozesse

---

- Literatur
- 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](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>)
-

### Sichere Implementierung auf Microcontrollern

Englische Modulbezeichnung	Secure Implementation on Microcontrollers
Kürzel	IS2S5
Modulbereich	Wahlpflichtbereich 1 Security
Modulverantwortliche:r	Prof. Dr. Helia Hollmann
Pflicht/Wahl	Wahlpflicht
Turnus	Sommer- und Wintersemester, jährlich
Dauer	1 Semester
Lehrveranstaltung	Sichere Implementierung auf Microcontrollern
CP / SWS	5 CP, 4 SWS
Arbeitsaufwand	Gesamtaufwand 5 CP x 25 h = 125 h davon Präsenzzeit 45 h, Selbststudium 78,5 h, Prüfungszeit 1,5 h
Prüfungsform	laut SPO und Studienplan
Benotung	gemäß §20 der APO in der jeweils gültigen Fassung
Empfohlene Voraussetzungen	IT-Sicherheit, Programmierkenntnisse, Cryptography and Security
Verwendbarkeit	vertiefendes Wahlpflichtmodul zur Erlangung der notwendigen Leistungspunkte lt. SPO
Lehrsprache	Deutsch
Lehr-/Lernmethoden	Seminaristischer Unterricht, Praktikum

## Sichere Implementierung auf Microcontrollern

---

Inhalte	<p>Der Schutz eingebetteter Systeme gegenüber Angriffen Dritter auf gespeicherte Daten und Implementierungen stellt eine immer wichtigere, jedoch auch durch zunehmende Vernetzung herausfordernde Aufgabe dar. In dieser Lehrveranstaltung soll fundiertes Wissen über Angriffsmöglichkeiten auf Mikrocontroller vermittelt werden und es werden die Möglichkeiten untersucht, Mikrocontroller mittels Softwareimplementierungen zu schützen. In praktischen Übungen soll dieses Wissen selbstständig in Kleingruppen umgesetzt werden und Angriffe können mit Hilfe bereitgestellter ChipWhisperer® durchgeführt werden, um implementierte Gegenmaßnahmen auf die Probe zu stellen.</p>
Qualifikationsziele	<p><b>Kenntnisse:</b></p> <ul style="list-style-type: none"><li>- Die Studierenden lernen invasive und nicht invasive Angriffe auf Microcontroller kennen.</li></ul> <p><b>Fertigkeiten:</b></p> <ul style="list-style-type: none"><li>- Sie erlernen Techniken um Microcontroller gegen Angriffe abzusichern.</li><li>- Sie lernen, welche Möglichkeiten es gibt, Systeme mit Software zu schützen.</li></ul> <p><b>Kompetenzen:</b></p> <ul style="list-style-type: none"><li>- Die Studierenden entwickeln sicheren Code für Microcontroller</li><li>- Sie verstehen, was ein sicheres System ausmacht.</li><li>- Sie können beurteilen, inwieweit Kryptographie gegen Angriffe schützt.</li></ul>
Literatur	<ul style="list-style-type: none"><li>- Mangard, S., Oswald, E., Popp, T. (2007). Power Analysis Attacks: Revealing the Secrets of Smart Cards. Niederlande: Springer US.</li><li>- Woudenberg, J. v., O'Flynn, C. (2021). The Hardware Hacking Handbook: Breaking Embedded Security with Hardware Attacks. USA: No Starch Press.</li></ul>

---

### **Wahlpflichtbereich 2 für den Schwerpunkt International**

Es kann jedes Modul "Deutsch als Fremdsprache" des Bereichs "Deutsch Vertiefung" des Zentrums für Sprachen und Interkulturelle Kommunikation belegt werden.

---



### **Wahlpflichtbereich 2 für die Schwerpunkte Safety und Security**

Es kann jedes Modul mit technischem oder informationstechnischem Schwerpunkt für Masterstudiengänge der TH Augsburg belegt werden.

---

**Master Thesis**

ID	IS3A1
Study section	Semester 3
Responsible lecturer	Prof. Dr. Helia Hollmann
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 produce 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 write 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.

---