Modulhandbuch

Industrielle Sicherheit

Master (M. Sc.)

WiSe 2024/25

Stand 04.10.2024

Degree course	Industrielle Sicherheit			
	Kürzel	IS1G1	**Kürzel**	n
Moduldescription	***Introduction to Safety and Human Machine Interaction***			
Course				
Term	**2**	**Mandatory/Elective**	**optional**	
	Rotation Semesterzyklus		**Duration** 1 Semester	
Responsable lecturer				
Lecturer	Prof. Dr. Helia Hollmann, Prof. Dr. Claudia Meitinger, Prof. Dr. Wolfgang Zeller, N.N.			
Teaching language	Englisch			
Teaching method / SWS	Lecture, Tutorial		**ECTS-Credits** 5	
workload/ attendance: 45 h	**Preparation:** 90 h including examination		**Exercises:** 15 h (1 SWS)	
Assessment and contribution to module mark	**Assessment** By formal examination, coursework with group design projects and assignments **Coursework 1:** Coursework exercises and lab experiments pass/requirement for coursework 2 **Coursework 2:** Mini project: design, presentation and report 50% **Examination:** The examination paper will be of 1.5 hours duration and consist of 6 questions worth 20 marks each; the student will be required to answer 5 of these.			
Prerequisites:	none			
Recommended Prerequisites	none			
This module is a precondition for module	none			
Assesment and contribution to module mark	**Aims:** The students are provided with the knowledge of special requirements of production plants to safety and security. The			

	students become familiar with hardware components and methods that can be used to achieve the necessary level of safety and security. 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 and security 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 inter-action 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, security and human machine interaction I2 Critically evaluate choices of safety and security functions I3 Recognise aspects of safety and security in practice **PROFESSIONAL/PRACTICAL SKILLS** P1 Design a system considering relevant aspects of safety, security and human machine interaction based on legal regulations, norms and scientific findings P2 Analyse an existing system using the work system model P3 Develop and improve systems according to the human-centered design process **TRANSFERABLE SKILLS** T1 Improve oral and written communication skills T2 Work effectively in a team T3 Be able to think and work on different levels of abstraction
Content	**Content** **1) Introduction to safety, security 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 speed variable drive systems • Verification and validation (effectiveness, experimental and model based proof test) **4) Security for industrial automation and control systems** • Fundamental terms of the security for industrial automation and control systems (IACS) • Overview of the ISO/IEC 62443 • Security requirements and security levels • Security program requirements for providers of integration and maintenance services for IACS **5) 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)
Teaching method	
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 Hauke, M.; Schaefer, M.; Apfeld, R.; Bömer, T.; Huelke, M.; Borowski, T.; Büllesbach, K.-H.; Dorra, M.; Foermer-Schaefer, H.-G.; Grigulewitsch, W.; Heimann, K.D.; Köhler, B.; Krauß, M.; Kühlem, W.; Lohmaier, O.; Meffert, K.; Pilger, J.; Reuß, G.; Schuster, U.; Seifen, T.; Zilligen, H.: Functional safety of machine controls - Application of EN ISO 13849. BGIA-Report 2/2008e. German Social Accident Insurance (DGUV), Berlin 2009. ISBN: 978-3-88383-793-2 Müller, Klaus-Rainer: Handbuch der Unternehmenssicherheit, Vieweg 2005, ISBN: 978-2658101503 Informationssicherheit und IT-Grundschutz, BSI-Standards 100-1, 100-2 und 100-3, ISBN 978-3887849153 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

Studiengang	Industrielle Sicherheit			
	Kürzel	IS1G2	**Kürzel**	
Modulbezeichnung	***Cryptography and Security***			
Lehrveranstaltung	Cryptography and Security			
Studiensemester	**1**	**Pflicht/Wahl**	**Wahl**	
	Turnus Sommersemester		**Dauer** 1 Semester	
Modulverantwortlicher	Prof. Dr. Hollmann			
Dozent(in)	Prof. Dr. Hollmann Prof. Dr. Werthschulte			
Arbeitssprache	Englisch			
Lehrform / SWS	Seminaristischer Unterricht, Präsentation		**ECTS-Credits** 5	
Arbeitsaufwand/ Präsenzzeit 60 h (15 x 4 SWS)	**Eigenständige Vor-und Nachbereitungszeit** 90 h		**Gelenkte Vor- und Nachbereitung / Übung**	
Studien-/Prüfungs-leistungen/ formen	formal examination, duration 90 minutes			
Voraussetzungen nach Prüfungsordnung	None			
Empfohlene Voraussetzungen	None			
Als Vorkenntnis empfohlen für Module	None			
Modulziele/ angestrebte Lernergebnisse	**Knowledge**: • students know the basic cryptographic algorithms and their purpose • students are able to name and explain the differences between symmetric and asymmetric cryptographic algorithms • students are able to describe common attacks on embedded systems • students know the low level mechanisms of x86/ARM architectures for handling security • students know how executables can be manipulated and how to protect against it **Skills**: • students are able to analyze threats and risks of given systems • students are able to derive requirements for the application of cryptographic algorithms			

	• students are able to analyse common industrial communication systems • students are able to analyse code and find deficiencies concerning security **Competences**: 1. students are able to develop secure communication and key management concepts 2. students are able to justify security measures in devices and networks 3. students are able to criticize and defend security concepts 4. students can analyse basic attacks on systems and name countermeasures
Inhalt	1) Cryptography a) Symmetric Cryptographic b) Algorithms c) Asymmetric Cryptographic Algorithm d) Digital Signature Algorithms e) Key Exchange Protocols f) Authentication Protocols g) Secure Hash Algorithms 2) Security a) Basic terms b) Protection goals and attack classification c) Critical infrastructures d) Communication protocols i) IT-networks ii) Field bus systems iii) Examples of network attacks e) Attacks on device level i) Introduction controlling units (x86/ARM) ii) Memory protection mechanisms iii) Runtime behaviour and memory management iv) Examples of attacks on device level • 3) Basics of the ISO/IEC 62443 •
Medienformen	Projector, blackboard, pc-based examples
Literatur	• M. Howard, S. Lipner: ”The Security Development Lifecycle”, Microsoft Press, 2006 • Shostack: ”Threat Modeling: Designing for Security”, Wiley, 2014 • Paar, J. Pelzl: ”Understanding Cryptography: A Textbook for Students and Practitioners”, Springer, 2010 • 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, 2001 • G. Schell, B. Wiedemann (Ed.): „Bussysteme in der Automatisierungs- und Prozesstechnik". Springer, 2019 • R.C.Detmer: „Introduction to 80x86 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

Studiengang	Industrielle Sicherheit (Master)			
	Kürzel	IS1G3	**Kürzel**	
Modulbezeichnung	***Management und Mitarbeiterführung***			
Lehrveranstaltung	Management und Mitarbeiterführung			
Studiensemester	**1**	**Pflicht/Wahl**	**Pflicht**	
	Turnus Jährlich, Sommersemester		**Dauer** 1 Semester	
Modulverantwortliche(r)	Prof. Dr. Richard			
Dozent(in)	Prof. Dr.'s Krupp, Richard, Waibel			
Arbeitssprache	Deutsch			
Lehrform / SWS	Vorlesung (2 SWS)		**ECTS-Credits**: **3**	
Arbeitsaufwand/ Präsenzzeit: 30 h Vorlesung	**Eigenständige Vor- und Nachbereitungszeit** 30 h Vor- und Nachbereitung, 30 h Prüfungsvorbereitung und Prüfung		**Gelenkte Vor- und Nachbereitung/ Übung**	
Studien-/Prüfungs-leistungen/ -formen	Schriftliche Prüfung, 90 Minuten			
Voraussetzungen nach Prüfungsordnung:	-			
Empfohlene Voraussetzungen:	-			
Als Vorkenntnis empfohlen für:	-			
Modulziele/ angestrebte Lernergebnisse	**Lernergebnisse/Qualifikationsziele** **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.
Inhalt	• 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 o Rechtsgeschäfte o Allgemeines und Besonderes Schuldrecht o Sachenrecht • Internetrecht o Schutz von Domains o Electronic Commerce o Schadensersatzhaftung und Haftungsbeschränkung • Urheberrecht/Wettbewerbsrecht o Grundbegriffe o Schutz und Haftung o Schadensersatzansprüche

	• Datenschutz
	  ○ Merkmale und Grundbegriffe
	  ○ Anwendbare Rechtsvorschriften
	  ○ Telekommunikationsdatenschutz
	• Rechtliche Aspekte der IT-Forensik

Medienformen	Beamer, Ergänzung durch Tafelarbeit
Literatur	• Horst Steinmann; Georg Schreyögg (2013) „Management: Grundlagen der Unternehmensführung Konzepte - Funktionen – Fallstudien“, Springer Gabler. • Heinrich Kersten, Gerhard Klett (2015): „Der IT Security Manager: Aktuelles Praxiswissen für IT Security Manager und IT-Sicherheitsbeauftragte in Unternehmen und Behörden“, Springer Vieweg. • Klaus Macharzina; Joachim Wolf (2010) „Unternehmensführung: Das internationale Managementwissen Konzepte – Methoden – Praxis“, Gabler. • Thomas W. Harich (2015) „IT-Sicherheit im Unternehmen“, MITP. • Uwe Schirmer; Sabine Woydt (2016) „Mitarbeiterführung“, Springer Gabler.

Studiengang	Industrielle Sicherheit			
	Kürzel	IS1G4	**Kürzel**	
Modulbezeichnung	***Seminar***			
Lehrveranstaltung	Seminar			
Studiensemester	**1**	**Pflicht/Wahl**	**Pflicht**	
	Turnus Sommersemester		**Dauer** 1 Semester	
Modulverantwortliche(r)	Prof. Dr. Merli			
Dozent(in)	Prof. Dr. Merli Prof. Dr. Hollmann Prof. Dr. Kerber Prof. Dr. Meitinger Prof. Dr. Zeller Prof. Dr. Krupp Prof. Dr. Richard			
Arbeitssprache	Englisch			
Lehrform / SWS	Seminaristischer Unterricht, Präsentation, Seminararbeit		**ECTS-Credits** 5	
Arbeitsaufwand/ Präsenzzeit 60 h (15 x 4 SWS)	**Eigenständige Vor- und Nachbereitungszeit** 90 h inkl. Prüfungsvorbereitung und Prüfung		**Gelenkte Vor- und Nachbereitung/ Übung**	
Studien-/Prüfungs-leistungen/ -formen	examination consists of three parts: • scientific report (8-10 pages, 50%) • presentation (20-30 minutes, 30%) • two written reviews (1-2 pages each, 20%)			
Voraussetzungen nach Prüfungsordnung	none			
Empfohlene Voraussetzungen	none			
Als Vorkenntnis empfohlen für Modul:	none			
Modulziele/ angestrebte Lernergebnisse	**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 for 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
Inhalt	1. Methods for scientific writing and presentation 2. Independent in-depth research into a current topic 3. Writing of report in the style of a research paper 4. Review of other students‘ reports 5. Revision of own report based on reviews 6. Presentation of reports
Medienformen	• projector • blackboard
Literatur	• lecture slides and notes

Studiengang	Industrielle Sicherheit			
	Kürzel	IS1C1	**Kürzel**	
Modulbezeichnung	***Systemarchitektur und Netzwerktechnik***			
Lehrveranstaltung	SANT			
Studiensemester	**1**	**Pflicht/Wahl**	**Pflicht**	
	Turnus Semesterzyklus		**Dauer** 1 Semester	
Modulverantwortliche(r)	Prof. Dr. Alexander von Bodisco Dr. Dominik Merli			
Dozent(in)				
Arbeitssprache	Englisch			
Lehrform / SWS	Integrierte Vorlesung, Praktikum		**ECTS-Credits** 5	
Arbeitsaufwand/ Präsenzzeit 30 h (2 SWS)	**Eigenständige Vor- und Nachbereitungszeit** 90 h		**Gelenkte Vor- und Nachbereitung/ Übung** 30 h (2 SWS)	
Studien-/Prüfungsleistungen/ Prüfungsformen	Schrift. Prüfung; Dauer 90 Minuten			
Voraussetzungen nach Prüfungsordnung	keine			
Empfohlene Voraussetzungen	keine			
Als Vorkenntnis empfohlen für:	keine			
Modulziele/ angestrebte Lernergebnisse	**Kompetenzen** Die Studierenden verstehen den Aufbau von Rechnernetzen und deren Komponenten. Sie kennen Verfahren zur Untersuchung von Netzen und verstehen die Funktionsweise wichtiger Kommunikationsprotokolle und können deren Verhalten interpretieren.			
Inhalt	**Inhalte** 1. Grundlagen der Datenkommunikation • OSI- TCP/IP Modell, Netzwerkgrundlagen • Durchsatz- und Latenzberechnungen 2. Einführung Systemarchitektur • Grundbegriffe • Referenzmodelle • Netzwerkprotokolle • Netzstrukturen 3. Netzwerksicherheit • Firewall-Arten und -Architekturen, IDS/IPS, Honeypots, Network Security Monitoring			

	4. Kanalzugriffsverfahren
Medienformen	Beamer und Tafelanschrift
Literatur	Claudia Eckert, „IT-Sicherheit – Konzepte – Verfahren – Protokolle“, 9te Auflage, De Gruyter Oldenbourg, ISBN-13: 978-3486200003 James Kurose und Keith Ross, "Computernetzwerke - Der Top-Down Ansatz", 6te Auflage, Pearson IT, ISBN-13: 978-3-86894-237-8. Andrew S. Tanenbaum, "Computernetzwerke", 5te Auflage, Pearson Studium, ISBN-13: 978-3-8689-4137-1. Martin Sauter, "Grundkurs Mobile Kommunikationssysteme: UMTS, HSPA und LTE, GSM, GPRS, Wireless LAN und Bluetooth", 5te Auflage, Springer Vieweg, ISBN-13: 978-3-6580-1460-5.

Studiengang	Industrielle Sicherheit			
	Kürzel	IS1C3	**Kürzel**	
Modulbezeichnung	***Industrieanlagen, Automatisierung und Steuerung***			
Lehrveranstaltung	IS1C2			
Studiensemester	**1**	**Pflicht/Wahl**	**Pflicht**	
	Turnus Sommersemester		**Dauer** 1 Semester	
Modulverantwortliche(r)	Prof. Dr. Wolfgang Zeller			
Dozent(in)	Prof. Dr. Benjamin Danzer Prof. Dr. Wolfgang Zeller			
Arbeitssprache	Deutsch			
Lehrform / SWS	Vorlesung, Übung		**ECTS-Credits** 5	
Arbeitsaufwand/ Präsenzzeit 39 h (3 SWS)	**Eigenständige Vor- und Nachbereitungszeit** 98 h		**Gelenkte Vor- und Nachbereitung/ Übung** 13 h (1 SWS)	
Studien-/Prüfungs-leistungen/ -formen	Schrift. Prüfung; Dauer 90 Minuten Schriftl. Ausarbeitung; 10 Seiten			
Voraussetzungen nach Prüfungsordnung	keine			
Empfohlene Voraussetzungen	keine			
Als Vorkenntnis empfohlen für Modul:	keine			
Modulziele/ angestrebte Lernergebnisse	**Lernergebnisse/Qualifikationsziele** **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 Bedienens 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.
Inhalt	**Inhalte** **Einführung in Industrieanlagen, Automatisierungs- und Steuerungstechnik** ▪ Ursprung, heutige Bedeutung, Zielsetzung, Anforderungen ▪ mechanische, fluidische und elektrische Steuerungen **Funktionen und Komponenten der Steuerungstechnik** ▪ Elektronische programmierbare Steuerungen ▪ Schnittstellen zwischen Prozess und Steuerung ▪ Anwendung industrieller Kommunikationssysteme ▪ Feldbussysteme und Industrielle Ethernet-basierte Kommunikations-Systeme ▪ Bedienung und Beobachtung ▪ Leitstandstechnik und Betriebsdatenerfassung **Programmierkonzepte und standardisierte SPS-Programmiersprachen** ▪ grundlegende Sprachelemente textueller und graphischer Programmiersprachen ▪ Organisation von SPS-Programmen und Steuerungsentwurf **Methoden und Werkzeuge zur Handhabung von Steuerungs-software und zur Beherrschung der Komplexität von Steuerungssystemen** ▪ Softwareentwicklung für industrielle Anwendungen ▪ Inbetriebnahme, Service und Wartung von Steuerungssystemen
Medienformen	Skript, Laptop und Beamer, Filmsequenzen
Literatur	• Lückenskript zur Vorlesung, Begleit- und Übungsmaterial in moodle • Seitz, M.: Speicherprogrammierbare Steuerungen für die Fabrik- und Prozessautomation, 4. Auflage, Carl Hanser Verlag, München, 2015. ISBN: 978-3446442733 (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

	• Wellenreuther, G. u. Zastrow, D.: Automatisieren mit SPS - Theorie und Praxis, 6. Auflage, Springer Vieweg, 2015. ISBN 978-3834825971 • Softwarepakete

Studiengang	Industrielle Sicherheit			
	Kürzel	IS1C3	**Kürzel**	
Modulbezeichnung	***Informationsmanagement und Geschäftsprozesse***			
Lehrveranstaltung	Informationsmanagement und Geschäftsprozesse			
Studiensemester	**1**	**Pflicht/Wahl**	Pflicht	
	Turnus Jedes 2. Semester		**Dauer** 1 Semester	
Modulverantwortliche(r)	Prof. Dr. Richard			
Dozent(in)	Prof. Dr. Richard, Prof. Dr. Krupp			
Arbeitssprache	Deutsch			
Lehrform / SWS	Vorlesung (3 SWS), Praktikum (1 SWS)		**ECTS-Credits**: **5**	
Arbeitsaufwand/ Präsenzzeit: 45 h Vorlesung	**Eigenständige Vor- und Nachbereitungszeit** 60 h Vor- und Nachbereitung, 30 h Prüfungsvorbereitung und Prüfung		**Gelenkte Vor- und Nachbereitung/ Übung** 15 h Praktikum	
Studien-/Prüfungs-leistungen/ -formen	Schriftliche Prüfung, 90 Minuten			
Voraussetzungen nach Prüfungsordnung:	-			
Empfohlene Voraussetzungen:	-			
Als Vorkenntnis empfohlen für Modul:	-			
Modulziele/ angestrebte Lernergebnisse	**Lernergebnisse/Qualifikationsziele** **Kenntnisse:** • Studierenden kennen die Grundlagen des Geschäfts-prozessmanagements. • Sie kennen die Bedeutung der Bereitstellung von Informationen in Geschäftsprozessen in einem globalen Zusammenhang. • Sie kennen die Rahmenbedingungen für das Informations- und Geschäftsprozessmanagement • Sie kennen den Zusammenhang aber auch Unterschied von Geschäftsprozessen, Informationsprozessen und IT-Systemen/IT-Landschaften. **Fertigkeiten:** • Studierende sind in der Lage, Geschäftsprozesse und zugehörige Informationsprozesse mittels geeigneter Werkzeuge (z.B. Prozessmapping, Visualisierung, Referenzmodelle, Ablaufdiagramme, Kennzahlenanalyse) zu analysieren, zu strukturieren und zu bewerten.			

	• Sie können mit dem Ziel der Analyse, Strukturierung und Bewertung geeignete Werkzeuge (vgl. oben) beispielhaft anwenden. • Sie können aus Geschäftsprozessen Bedarfe an Informationsprozesse ableiten. **Kompetenzen:** • Studierende können die Eignung von Geschäftsprozessen hinsichtlich deren Zielsetzung einschätzen. • Sie können Geschäftsprozesse in übergeordnete Strukturen einfügen und hier deren Eignung einschätzen. • Sie können die Wechselwirkung zwischen Informationsprozessen und Geschäftsprozessen hinsichtlich deren Eignung und Güte einschätzen und strukturiert bewerten. • Sie können die Abbildung von Informationsprozessen und Geschäftsprozessen in IT-Systemen und IT-Landschaften nachvollziehen.
Inhalt	• Einführung in das Geschäftsprozessmanagement • Definition und Beschreibung von Zielsetzung und Durchführung von Geschäftsprozessen • Definition und Beschreibung von Zielsetzung und Durchführung von zugehörigen Informationsprozessen • Beschreibung von Bedarfen und Anforderungen die Sich aus Geschäftsprozessen an Informationsprozesse ergeben • Zusammenhang von Informationsprozessen mit Effizienz und Effektivität von Prozessen sowie die daraus folgende Abbildung in Kennzahlen • Übertragung der genannten Inhalte auf IT-Systeme und IT-Landschaften (Definition von nötigem Informationsumfang, nötiger Informationsbereitstellung und Informationsabgleichen zwischen realem Geschäftsprozess und IT-Systemen/Landschaften)
Medienformen	Beamer, Ergänzung durch Tafelarbeit, Prozessmodellierungstools
Literatur	• Krcmar, H.: Informationsmanagement, 5. Auflage, Berlin: Springer Verlag, 2009 • Gadatsch, A.: Grundkurs Geschäftsprozess-Management: Methoden und Werkzeuge für die IT-Praxis, Wiesbaden: Vieweg und Teubner, 2012

Studiengang	Industrielle Sicherheit			
	Kürzel	IS2S1	**Kürzel**	
Modulbezeichnung	***Zertifizierungsmodul***			
Lehrveranstaltung				
Studiensemester	**2**	**Pflicht/Wahl**	**Pflicht**	
	Turnus Wintersemester		**Dauer** 1 Semester	
Modulverantwortliche(r)	Prof. Dr. Helia Hollmann			
Dozent(in)	Krupke, Zeh, Heinritz			
Arbeitssprache	Deutsch			
Lehrform / SWS	Vorlesung, Seminar		**ECTS-Credits** 5	
Arbeitsaufwand/ Präsenzzeit 15 h (1 SWS)	**Eigenständige Vor- und Nachbereitungszeit** 90h		**Gelenkte Vor- und Nachbereitung/ Übung** 45 h (3 SWS)	
Studien-/Prüfungs-leistungen/ -formen	Schriftliche Prüfung; Dauer 90 Minuten			
Voraussetzungen nach Prüfungsordnung	keine			
Empfohlene Voraussetzungen	Introduction to Safety, Security and Human Machine Interaction			
Als Vorkenntnis empfohlen für Modul	keine			
Modulziele/ angestrebte Lernergebnisse	**Lernergebnisse/Qualifikationsziele** **Kenntnisse:** ▪ Studierende können die grundlegenden Begriffe eines ISMS nach DIN EN ISO/IEC 27001 benennen und an Beispielen erklären. ▪ Studierende kennen die Hintergründe eines risikobasierten Informationssicherheitsmanagementsystems (ISMS) und erwerben fachsprachliche Kenntnisse. ▪ Studierende können die grundlegenden Begriffe der Funktionalen Sicherheit verstehen und erklären. ▪ Studierende kennen qualitative und quantitative Techniken und Maßnahmen zur Erreichung der Funktionalen Sicherheit. **Fertigkeiten:** ▪ Studierende können geeignete Modelle aufstellen und anhand dieser eine geordnete Gefährdungs- und Bedrohungsanalyse durchführen. ▪ Studierende haben das Rüstzeug, sich mit normativer Literatur auseinander zu setzen und sich so weitere Lerninhalte zu erarbeiten.			

	▪ Studierende können die zur sicheren Entwicklung notwendigen Managementprozesse verstehen. ▪ 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 können grundlegende Techniken und Maßnahmen bei der HW und SW-Entwicklung zur Erreichung der Funktionalen Sicherheit anwenden. ▪ Sie können Sicherheitsarchitekturen erstellen und qualitativ, sowie quantitativ beurteilen **Kompetenzen:** ▪ Die Studierenden haben grundlegende Kenntnisse in der Sicherheitstechnik und können die Grundlagen anwenden.
Inhalt	**Inhalte** **Security** ▪ IT-Sicherheit für Kritische Infrastrukturen: Funktionsweise und Aufbau von Netzleit- und Fernwirktechnik sowie Primär- und Sekundärtechnik in Energieversorgungsnetzen; Gesetzliche Grundlagen: IT-Sicherheitsgesetz, BSIG, BSI-KritisV, EnWG, EU NIS-Rahmenverordnung ▪ Grundlagen ISMS und DIN EN ISO/IEC 27001: Normative Grundlagen zur Normenreihe DIN EN ISO/IEC 27001; Grundbegriffe, Aufbau, Betrieb, Umsetzung und kontinuierliche Verbesserung im Rahmen eines ISMS, PDCA-Zyklus; ▪ Risikomanagement: Risikobasierter Ansatz in der Informationssicherheit, Strukturanalyse und Schutzbedarfsfeststellung, Vulnerability Assessments nach BSI Durchführungskonzept, Bedrohungs- und Gefährdungsanalyse, Risikoassessment nach Assets oder nach Bedrohungen (G0, STRIDE, Thread Modelling) ▪ Incident Response und Business Continuity Management: Business Impact Analysis, Grundlagen Notfallmanagement und Notfallvorgehen für IT-Vorfälle ▪ Zertifizierung eines ISMS nach DIN EN ISO/IEC 27001: Vorteile einer Zertifizierung,Akkreditierung, Ablauf und Durchführung, Auditierung **Safety** ▪ Rechtliche Grundlagen: Ziele der Funktionalen Sicherheit und die Rolle des Produkthaftungsgesetzes ▪ Management der Funktionalen Sicherheit: Produkt Lebenszyklus, Verifikation und Validierung, Dokumentation, Konfigurationsmanagement, Änderungsmanagement, Kompetenzmanagement, Lieferantenmanagement

	▪ Gefahren und Risiko-Analyse: Grundbegriffe, Beispiele und praktische Übung. ▪ Anforderungsspezifikation: Grundbegriffe, Anforderungen und Beispiele **Hardware-Entwicklung** ▪ Einführung: V-Modell, Grundbegriffe, HW-Sicherheitslebenszyklus, Anforderungsspezifikation ▪ Architekturen: Unterschiedliche Sicherheitsarchitekturen (MooN), Integrität, Diagnose, Techniken und Maßnahmen, systematische Integrität ▪ Berechnung von Ausfallwahrscheinlichkeiten: FMEDA, Markov, Ausfallraten, SFF, DC, PFDavg, FMEDA Beispiel ▪ Schnittstellen: Black/White-Channel, CRC, Ausfallwahrscheinlichkeit, Fehlerbetrachtung ▪ Umsetzung: Elementen-Entwurf, Implementierung, Inbetriebnahme und Test, Änderungsmanagement ▪ V&V Aktivitäten: EMV Test, Umwelttest, Fault Insertion Tests **Software-Entwicklung** ▪ Einführung: V-Modell, Grundbegriffe, SW-Sicherheitslebenszyklus, Normenaufbau ▪ Spezifikation der Software-Sicherheitsanforderung: Grundbegriffe, Nachvollziehbarkeit, Beispiele und praktische Übung ▪ Architekturen: Einführung, Anforderungen, Hardware und Software Betrachtung ▪ Systementwurf: Modulentwurf, Unabhängigkeit von Softwaremodulen, Diagnosen ▪ Implementierung: Coding Guideline, MISRA, Dokumentation, Software Reviews, Software-Metriken ▪ V&V Aktivitäten: Modultest, Integrationstest und Validierung der Sicherheitsfunktionen ▪ Tool-Qualifizierung: Tool Klassifizierung, Validierung und Dokumentation ▪ Änderungsmanagement: Prozess-Modell, Impaktanalyse und praktische Durchführung ▪ Security for Safety: Normenbezug, Grundlagen, Risiko-Analyse, und Vorgehensweise **Spezielle Betrachtungen** ▪ Betriebsbewährtheit: Systematische Eignung, Architekturen, Restfehlerwahrscheinlichkeit, Fehlerdiagnosen und Beispielrechnungen ▪ Sicherheitslebenszyklus: Aktivitäten nach der Entwicklung ▪ Berechnung von Sicherheitskreisen: Theorie und Praxis mit Rechenbeispiele ▪ TÜV-Aktivitäten: Safety-Assessment, Checklisten, Zertifizierung, Besichtigungen von Fertigungsstätten
Medienformen	Skript, Laptop und Beamer, Filmsequenzen

Literatur	• Vortragsfolien, Begleit- und Übungsmaterial in moodle • Norm, IEC 61508:2010 Teil1-7, Beuth Verlag, 2011. • David Smith.: Safety Critical System Handbook, Butterworth Heinemann 2010. • Dirk W. Hoffmann: Software Qualität, Springer-Verlag Berlin Heidelberg, 2013. • Helmut Balzert: Lehrbuch der Softwaretechnik, Spektrum Akademischer Verlag Heidelberg, 2009. • Berhard Fechner: Transiente Fehler in Mikroprozessoren, Vieweg+Teubner Verlag, 2011. • BSI IT-Grundschutz: Gefährdungskatalog G0, Grundschutz Baustein 100-4 (Notfallmanagement). • DIN EN ISO/IEC 27001 • NIST SP800-61, • NIST SP800-86 • Shostack, A.: Threat Modeling: Designing for Security, Wiley Verlag, 2014.

Degree course	Industrielle Sicherheit			
	Code	IS2S1	**Subhead**	
Moduldescription	***Major Project***			
Course	IS2S6			
Term	**2**	**Mandatory/Elective**		
	Rotation Winter Term		**Duration** 1	
Responsable lecturer	Dr. Hollmann			
Lecturer	Drs. Braun, Hollmann, Richard, Zeller			
Teaching language	English			
Teaching method / SWS			**ECTS-Credits**: **15**	
workload/ attendance:	**Preparation**		**Exercise:**	
Assessment and contribution to module mark	The project assessment will be based on the combined assessment of a final report (80%) and the performance of the student in a presentation of his/her work (20%). The student hast to pass the Kickoff seminar.			
Prerequisites:	Content of the modules IS1C1, IS1C2, IS1C3			
Recommended Prerequisites	IS1G1, IS1G2, IS1G3			
This module is a precondition for module	none			
Assesment and contribution to module mark	**Learning outcomes:** A successful student will be able to **KNOWLEDGE AND UNDERSTANDING** 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 **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.
Content	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. **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.
Teaching method	The students work in teams in an industrial environment or lab. The students meet the project supervisors on a regular basis to discuss progress, strategy and plans for the subsequent period of work. The module is web supplemented.
Literature	Will be given during the course depending on the industrial machine or plant to be worked on.

Studiengang	Industrielle Sicherheit			
	Kürzel	IS2S2	**Kürzel**	
Modulbezeichnung	***Sichere Geschäftsprozesse***			
Lehrveranstaltung	Sichere Geschäftsprozesse			
Studiensemester	**2**	**Pflicht/Wahl**	**Wahl**	
	Turnus Jedes 2. Semester		**Dauer** Blockveranstaltung	
Modulverantwortliche(r)	Prof. Dr. Jana Görmer-Redding			
Dozent(in)	Prof. Dr. Jana Görmer-Redding			
Arbeitssprache	Deutsch, englische Anteile			
Lehrform / SWS	Vorlesung (2 SWS), Übung 2 SWS		**ECTS-Credits**: **5**	
Arbeitsaufwand/ Präsenzzeit: 30 h Vorlesung	**Eigenständige Vor- und Nachbereitungszeit** 60 h Vor- und Nachbereitung, 30 h Prüfungsvorbereitung inkl. Prüfung		**Gelenkte Vor- und Nachbereitung/ Übung** 30 h Übung	
Studien-/Prüfungs-leistungen/ -formen	Schriftliche Prüfung, 90 Minuten (bei mehr als 10 Teilnehmenden)			
Voraussetzungen nach Prüfungsordnung:	-			
Empfohlene Voraussetzungen:	-			
Als Vorkenntnis empfohlen für Module:	-			
Modulziele/ angestrebte Lernergebnisse	**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 Zeitmanagement sowie Zuverlässigkeit gegenüber den anderen Teammitgliedern. • Case Study: Durch die Vorstellung der Ergebnisse vor den Kommilitonen erlernen die Studierenden zusätzlich Präsentationstechniken sowie den sinnvollen Einsatz moderner IT.
Inhalt	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. Dies umfasst Bedrohungsanalysen, Schwachstellenbewertungen und Risikobewertungsmethoden. • Steuerung und Sicherheitsmaßnahmen: Dieser Abschnitt behandelt Strategien und Werkzeuge zur Steuerung und Minimierung von IT-Security Risiken. Hierzu gehören Security-Frameworks, Sicherheitsrichtlinien, Compliance-Anforderungen und aktuelle Sicherheitspraktiken. • Krisenmanagement und Incident Response: Die Studierenden erfahren, wie sie auf Sicherheitsvorfälle reagieren und effektive Maßnahmen zur Wiederherstellung der Sicherheit in Geschäftsprozessen ergreifen können. Keywords: Allgemeine Chancen und Risiken der Digitalisierung, Industrie 4.0, Integriertes Chancen- und Risikomanagement, Quantifizierungsmethoden, Risikomanagement in IT-Projekten, Fallstudie und Übung
Medienformen	Beamer, Ergänzung durch Tafelarbeit, Prozessmodellierungstools
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) • 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)

Studiengang	Industrielle Sicherheit			
	Kürzel	IS2S3	**Kürzel**	
Modulbezeichnung	***Safety***			
Lehrveranstaltung				
Studiensemester	**2**	**Pflicht/Wahl**	**Pflicht**	
	Turnus Wintersemester		**Dauer** 1 Semester	
Modulverantwortliche(r)	Prof. Dr. Wolfgang Zeller			
Dozent(in)	Prof. Dr. Helia Hollmann Prof. Dr. Wolfgang Zeller			
Arbeitssprache	Deutsch			
Lehrform / SWS	Vorlesung, Seminar		**ECTS-Credits** 5	
Arbeitsaufwand/ Präsenzzeit 60 h (15 x 4 SWS)	**Eigenständige Vor- und Nachbereitungszeit** 90 h inkl. Prüfungsvorbereitung und Prüfung		**Gelenkte Vor- und Nachbereitung/ Übung**	
Studien-/Prüfungs-leistungen/ -formen	Schriftliche Prüfung; Dauer 90 Minuten			
Voraussetzungen nach Prüfungsordnung	-			
Empfohlene Voraussetzungen	Introduction to Safety, Security and Human Machine Interaction			
Als Vorkenntnis empfohlen für Modul:	-			
Modulziele/ angestrebte Lernergebnisse	**Lernergebnisse/Qualifikationsziele** **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.
Inhalt	**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)
Medienformen	• Folien-Vortrag mit Skript, Laptop und Beamer, Filmsequenzen, Übungen in Form von Gruppenarbeiten

Literatur	• Vortragsfolien, Begleit- und Übungsmaterial in moodle • Goble, W.: Control Systems Safety Evaluation and Reliabilty, Instrument Society of America, 2010, ASIN: B017R2U3LO • 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.

Studiengang	Industrielle Sicherheit			
	Kürzel	IS2S4	**Kürzel**	
Modulbezeichnung	***Embedded Security***			
Lehrveranstaltung	Embedded Security			
Studiensemester	**2**	**Pflicht/Wahl**	**Optional**	
	Turnus Wintersemester		**Dauer** 1 Semester	
Modulverantwortliche(r)	Prof. Dr. Merli			
Dozent(in)	Prof. Dr. Merli			
Arbeitssprache	Englisch			
Lehrform / SWS	Seminaristischer Unterricht, praktische Übungen		**ECTS-Credits** 5	
Arbeitsaufwand/ Präsenzzeit 60 h (15 x 4 SWS)	**Eigenständige Vor- und Nachbereitungszeit** 90 h		**Gelenkte Vor- und Nachbereitung/ Übung**	
Studien-/Prüfungs-leistungen/ -formen	formal examination, duration 90 minutes			
Voraussetzungen nach Prüfungsordnung	-			
Empfohlene Voraussetzungen	basic knowledge about cryptography and IT security			
Als Vorkenntnis empfohlen für:	-			
Modulziele/ angestrebte Lernergebnisse	**Knowledge** • Students know the basic building blocks of embedded security implementations. • Students are able to name and explain the advantages and disadvantages of different cryptographic implementations. • Students are able to describe several physical attack vectors. **Skills** • Students are able to derive security requirements for embedded systems. • Students are able to analyze cryptographic implementations. • Students are able to execute practical attacks on 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.			

Inhalt	1) Fundamental Building Blocks a. Basic Structure of Embedded Systems b. Physical Unclonable Functions (PUFs) c. True Random Number Generators (TRNGs) d. Cryptographic Implementations 2) Physical Attacks a. Simple Power Analysis (SPA) b. Differential Power Analysis (DPA) c. Fault Analysis 3) Embedded Security Concepts a. Firmware and Data Protection b. Secure Microcontrollers
Medienformen	• projector • blackboard • practical exercises with embedded systems
Literatur	• D. Mukhopadhyay, R. S. Chakraborty: ”Hardware Security: Design, Threats, and Safeguards”, Chapman and Hall/CRC, 2014 • S. Mangard, E. Oswald, T. Popp: ”Power Analysis Attacks: Revealing the Secrets of Smart Cards”, Springer, 2007 • C. Paar, J. Pelzl: ”Understanding Cryptography: A Textbook for Students and Practitioners”, Springer, 2010 • C. K. Koc (Ed.): ”Cryptographic Engineering”, Springer, 2009

Studiengang	Industrielle Sicherheit			
	Kürzel	IS2S5	**Kürzel**	
Modulbezeichnung	***Sichere Konzepte und Protokolle***			
Lehrveranstaltung	SKUP			
Studiensemester	**2**	**Pflicht/Wahl**	**Pflicht**	
	Turnus Semesterzyklus		**Dauer** 1 Semester	
Modulverantwortliche(r)	Prof. Dr. Alexander von Bodisco			
Dozent(in)	Prof. Dr. Alexander von Bodisco			
Arbeitssprache	Englisch			
Lehrform / SWS	Vorlesung, Praktikum		**ECTS-Credits** 5	
Arbeitsaufwand/ Präsenzzeit 30 h (15 x 2 SWS)	**Eigenständige Vor- und Nachbereitungszeit** 90 h		**Gelenkte Vor- und Nachbereitung/ Übung** 30 h (15 x 2 SWS)	
Studien-/Prüfungsleistungen/ Prüfungsformen	Schriftl. Prüfung; Dauer 90 Minuten			
Voraussetzungen nach Prüfungsordnung	keine			
Empfohlene Voraussetzungen	keine			
Als Vorkenntnis erforderlich/empfohlen für/ Module	keine			
Modulziele/ angestrebte Lernergebnisse	Die Studierenden kennen und verstehen die relevanten Aspekte von Sicherheitskonzepten und Protokollen. Sie können Sicherheitskonzepte vergleichen und hinsichtlich Schwachstellen analysieren.			
Inhalt	Inhalte 1. Sicherheitsmodelle Modell-Klassifikation, Zugriffskontrollmodelle, Informationsflussmodelle 2. Schlüsselmanagement Zertifizierung, Schlüsselerzeugung und -aufbewahrung, Schlüsselaustausch. Schlüsselrückgewinnung 3. 3.Authentifikation Authentifikation durch Wissen, Biometrie, verteilte Systeme 4. Sicherheit in Netzen Firewall-Technologie, OSI-Sicherheitsarchitektur, sichere Kommunikation, IPSec, SSL/TLS 5. 5. Sichere mobile und drahtlose Kommunikation GSM, UMTS, Term Evolution (LTE) und SAE, WLAN, Bluetooth			
Medienformen				
Literatur	Claudia Eckert, „IT-Sicherheit – Konzete – Verfahren – Protokolle“, 9te Auflage, De Gruyter Oldenbourg, ISBN-13: 978-3486200003			

	James Kurose und Keith Ross, "Computernetzwerke - Der Top-Down Ansatz", 6te Auflage, Pearson IT, ISBN-13: 978-3-86894-237-8. Andrew S. Tanenbaum, "Computernetzwerke", 5te Auflage, Pearson Studium, ISBN-13: 978-3-8689-4137-1. Martin Sauter, "Grundkurs Mobile Kommunikationssysteme: UMTS, HSPA und LTE, GSM, GPRS, Wireless LAN und Bluetooth", 5te Auflage, Springer Vieweg, ISBN-13: 978-3-6580-1460-5.

Studiengang	Master Industrielle Sicherheit			
	Kürzel	IS3A2	**Kürzel**	
Modulbezeichnung	***Incident Response***			
Lehrveranstaltung				
Studiensemester		**Pflicht/Wahl**	**Wahl**	
	Turnus: Jährlich (WS)		**Dauer:** **1 Semester**	
Modulverantwortliche(r)	Thomas Hanka			
Dozent(in)	Thomas Hanka, Pierre Kroma			
Arbeitssprache	deutsch			
Lehrform / SWS	Seminaristischer Unterricht mit praktische Übungen zur Anwendung und Vertiefung der erworbenen Kentnisse. 4 SWS		**ECTS-Credits**: 5	
Arbeitsaufwand/ Präsenzzeit: 60 h (15 x 4)	**Eigenständige Vor- und Nachbereitungszeit** 90 h		**Gelenkte Vor- und Nachbereitung/ Übung**	
Studien-/Prüfungsleistungen/ Prüfungsformen	Praktische Prüfung			
Voraussetzungen nach Prüfungsordnung:	keine			
Empfohlene Voraussetzungen:	IT-Sicherheit			
Als Vorkenntnis erforderlich/empfohlen für/ Module:				
Modulziele/ angestrebte Lernergebnisse	• Die Studierenden lernen die wichtigsten Grundlagen und Funktionen eines Cyber Defense Centers (CDCs) kennen. • Die Studierenden können anhand von Eventinformationen Indikatoren für Angriffe identifizieren. • Sie verstehen die einzelnen Schritte eines Angriffs und können diese anhand von Systeminformationen belegen. • Sie können die identifizierten Ereignisse strukturiert beurteilen und dokumentieren.			
Inhalt	• Grundlagen der IT-Sicherheit ○ Grundbegriffe ○ Typische Angriffe ○ Sicherheitsprozess ○ Analyse von Bedrohungen und Risiken ○ Gegenmaßnahmen • - Netzwerksicherheit ○ OSI Modell ○ Paketanalyse ○ Überblick zu relevanten Protokollen • - Grundlagen zum Cyber Defense Center ○ Funktion eines CDC ○ Rollen in einem CDC ○ Verwendete Tool ○ Analyse von Logdaten			

	○ Erfassung und Bestimmungen eines Incidents
Medienformen	
Literatur	C. Eckert: ”IT-Sicherheit: Konzepte - Verfahren - Protokolle”, Oldenbourg, 2012 P. Kraft, A. Weyert: "Network Hacking", Franzis, 2014 ENISA: "Good practice guide for incident management", 2010

Studiengang	Industrielle Sicherheit			
	Kürzel	IS3A1		
Modulbezeichnung	***Master Thesis***			
Lehrveranstaltung				
Studiensemester	**3**	**Pflicht/Wahl**	**optional**	
	Turnus Semesterzyklus		**Dauer** 1 Semester	
Modulverantwortliche(r)	Helia Hollmann			
Dozent(in)	Various supervisors			
Arbeitssprache	English			
Lehrform / SWS	lecture, tutorial, independent study		**ECTS-Credits** 20	
Arbeitsaufwand/ Präsenzzeit	**Eigenständige Vor- und Nachbereitungszeit**		**Gelenkte Vor- und Nachbereitung/ Übung**	
Studien-/Prüfungsleistungen/ Prüfungsformen	**Assessment** The project assessment will be based on the final reports as well as overall project value assessment, and the performance of the student in a viva voce examination. All elements will be assessed using a criterion-based marking scheme and the final report will be assessed blindly by both the project supervisor and the project moderator. If the marks for any element cannot be reconciled between the supervisor and the moderator then the module co-ordinator			
Voraussetzungen nach Prüfungsordnung	none			
Empfohlene Voraussetzungen	none			
Als Vorkenntnis empfohlen für Modul	none			
Modulziele/ angestrebte Lernergebnisse	**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.			

	LEARNING OUTCOMES A successful student will be able to: 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 tools for the specification, design, implementation and critical evaluation and implementation of an industrial safety and security project. TRANSFERABLE SKILLS T1 Communicate effectively ideas, proposals, and/or designs to a range of audiences, using rational and reasoned arguments, either orally, written or electronically.

	T2 Be able to assess the progress of work against a plan and demonstrate good practice in project organisation and management. T3 Effectively use information technology and associated skills. T4 Develop the facility for independent learning, open-mindedness, and the spirit of critical enquiry.
Inhalt	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.
Medienformen	A series of related lectures will introduce the student to learning resources, technical writing, dissertation presentation and project management. The student will meet with the project supervisor at least once per week to discuss progress, strategy and plans for the subsequent week. The module is web supplemented.
Literatur	Rosenberg, B J, 2005, *Spring into Technical Writing: For Engineers and Scientists*, 1stEd, USA, Addison Wesley. Van Emden, J, 2005, *Writing for Engineers*, 3rd Ed., USA, Palgrave. Lock, D, 2007, *Project Management,* 9th Ed., UK, Gower Publishing Ltd. Barker S and Cole, R, 2009, *Brilliant Project Management,* Revised Ed., UK, Pearson Education Limited.