



Catalogue of Modules

Master Course in

Security Management

Index of contents:

1	Security Management.....	3
1.1	Introduction to Security Management.....	3
1.2	Security- and Crisis Management in the International Context.....	4
1.3	Building and Workplace Safety	5
2	IT Security	6
2.1	Network Security	6
2.2	Enterprise IT Security Solutions with a Focus on IAM.....	8
2.3	Development of Secure IT Systems.....	10
3	Mathematical and Physical Basics	12
3.1	Introduction to Communication Security.....	12
3.2	Cryptology	14
4	Law and Business Administration	16
4.1	Law.....	16
4.2	Corporate Governance, Human Resource and Conflict Management.....	18
5	Miscellaneous Modules.....	19
5.1	Semester Paper 1 and 2	19
6	Elective Modules and Projects.....	21
6.1	Project	21
6.2	Elective Modules 1, 2 and 3	23
7	General Modules.....	24
7.1	Master Seminar	24
7.2	Master Thesis	26
7.3	Master- Colloquium	27

1 Security Management

1.1 *Introduction to Security Management*

Title of course	Introduction to Security Management
Teaching aims	NN
Contents	NN
Type of course (Compulsory, Specialization, etc.)	Compulsory
Semester	1. Semester
ECTS-Credits	6 (Workload: 180 hours = 65 h contact hours - and 115 h self studies)
Module co-ordinator	Prof. Dr. Sachar Paulus
Lecturer	Prof. Dr. Sachar Paulus; Prof. Dr. Friedrich-L. Holl
Type of examination/methods	Semester paper and presentation/ oral examination
Entrance requirements	Basic knowledge in business administration
Recommended literature (Teaching and learning materials, literature)	Klaus-Rainer Müller: Handbuch Unternehmenssicherheit, Vieweg, Wiesbaden, 2005
Teaching and learning methods	Lectures with various media (digital projector, and overhead projector), Exercises in small groups, business games, presentations.
Type of examination/methods	Presentation and project report, Presentation of Business Case Proposals, term paper.
Language of instruction	German
Special remarks (i.e. online-segments, practical visits, guest speakers)	

1.2 **Security- and Crisis Management in the International Context**

Title of course	Security- and Crisis Management in the International Context
Teaching aims	Consolidation of basics in Security Management, in particular practice in a practice-related context
Contents	<ul style="list-style-type: none"> - Security management in global Organisations - Aspects of communication between security teams, definition of competence - Crisis management: How to cope with crisis in practice - Crisis communication: principles and approaches of communication in case of a crisis - Individual competencies for security- and crisis management, e.g. for call centres - External impacts and relations in the area of security - Development of a public relations campaign for security management topics
Type of course (Compulsory, Specialization, etc.)	Compulsory
Semester	2. Semester
ECTS-Credits	6 (Workload: 180 hours = 65 h contact hours and 115 h self studies)
Module co-ordinator	Prof. Dr. Sachar Paulus
Lecturer	Prof. Dr. Sachar Paulus; Prof. Dr. Friedrich-L. Holl
Type of examination/methods	Term paper and presentation/ oral examination
Entrance requirements	Basics in Security Management
Recommended literature (Teaching and learning materials, literature)	Will be presented in course
Teaching and learning methods	Lectures with various media (digital projector, and overhead projector), Exercises in small groups, business games, presentations.
Type of examination/methods	Presentation and project report, Presentation of Business Case Proposals, semester paper.
Language of instruction	German
Special remarks (i.e. online-segments, practical visits, guest speakers)	

1.3 Building and Workplace Safety

Title of course	Building and Workplace Safety
Teaching aims	NN
Contents	NN
Type of course (Compulsory, Specialization, etc.)	Compulsory
Semester	2. Semester
ECTS-Credits	3 (Workload: 90 hours = 30 h contact hours and 60 h self studies)
Module co-ordinator	Ralph Wölpert
Lecturer	Ralph Wölpert, Thorsten Weller, Ralf Dahmer, Thomas Koch
Type of examination/methods	Written examination, and/ or oral examination
Entrance requirements	
Recommended literature (Teaching and learning materials, literature)	Journals: kes, IT-Management, IT-Director, LANline, Der Sicherheitsberater, S&I,
Teaching and learning methods	Lectures with various media (digital projector, and overhead projector), Exercises with PCs in small groups (maximal 10 students)
Type of examination/methods	Questions/ answers in lectures, Written examination at the end of the course, 60 min.
Language of instruction	German
Special remarks (i.e. online-segments, practical visits, guest speakers)	

2 IT Security

2.1 Network Security

Title of course	Network Security
Teaching aims	Students learn about security in IP based Networks. They analyse risks and dangers. Students learn operations and strategies of attacks in a practice-related context.
Contents	<ul style="list-style-type: none"> - Extended basics of IP Networks (TCP/IP- Protocol, ISO/OSI, Routing, active components, Cryptology) - Risks at operation of IT, Categories of threats, Vulnerabilities and threats - Security management, Security audits with tools, Network monitoring und Network logging - Attacks and counteractive measures - cryptography applications (encrypted communication, VPN-Protocols, certificates) - WEB-Server-Security, E-Mail-Security - Project, f.e. Firewalls, Honneypots und Intrusion-Detection-Systems, WLAN-security and VPNs
Code der Lehrveranstaltung	
Type of course (Compulsory, Specialization, etc.)	Compulsory
Semester	1. Semester
ECTS-Credits	6 (Workload: 180 hours = 65 h contact hours and 115 h self studies)
Module co-ordinator	Dietmar Hausmann
Lecturer	Dietmar Hausmann; E. v. Faber
Type of examination/methods	Project paper + presentation and/ or oral examination
Entrance requirements	Basics in internet networks, operating systems and cryptology.
Recommended literature (Teaching and learning materials, literature)	<p>Alexander Michael: Netzwerke und Netzwerksicherheit - Das Lehrbuch, Hüthing Verlag, 2006.</p> <p>Plötner Johannes, Wendzel Steffen: Praxishandbuch Netzwerk-Sicherheit, Galileo Computing, 2005.</p> <p>Wätjen Dietmar: Kryptographie. Grundlagen, Algorithmen, Lehrbuch Protokolle, Spektrum Akademischer Verlag, 2004.</p> <p>Peikari, Cyrus and Chuvakin, Anton: Kenne deinen Feind - Fortgeschrittene Sicherheitstechniken, O'Reilly Verlag, 2004.</p> <p>Scambray Joel, McClure Stuart, Kurtz George - Das Anti-Hacker-Buch, mitp Verlag, 2004.</p> <p>Special literature (VPN, IPSEC, IDS, Firewalls)</p> <p>Scripts and other material will be delivered during the lectures and on BSCW</p>
Teaching and learning methods	Lectures and exercises
Type of examination/methods	Project paper and presentation
Language of instruction	German

Special remarks (i.e. online-segments, practical visits, guest speakers)	
---	--

2.2 *Enterprise IT Security Solutions with a Focus on IAM*

Title of course	Enterprise IT Security Solutions with a Focus on IAM
Teaching aims	(i) Knowledge about structure and key figures of the enterprise security market as well as all important solutions including aim, major functions and specifics; the following solution categories are considered: Secure Content Management, Firewall und VPN, Intrusion Detection and Prevention, Security and Vulnerability Management as well as the complex Identity and Access Management (IAM). (ii) Gain detailed knowledge and insights in the area of "Identity and Access Management (IAM)"; basic terms, architectures and technologies for corporate use and in complex supply chains.
Contents	A) Solutions for system and network security (categories as above), B) Basic terms of IAM (all terms from identification through accounting), C) Authorization (access management): role, usage and limitations; strategies (DAC, MAC, RBAC, IF); realization (groups, roles, ACL, capabilities); alternatives; trends and perspectives including enterprise DRM, D) Authentication (identity verification): types, methods, technologies; problems and solutions; architectures and distributed systems (e.g. LDAP, RADIUS, Kerberos, ESSO, Single sign-on, federation), E) IAM architectures (the whole picture): Identity Management (administration including password management, UP, RME and directories) and Access Management (authenticate, authorize) or RME, UP, SOD and RAA; and interfaces to ITSM, SIEM etc. F) Public Key Infrastructures (PKI): challenges and solutions; certificates; roles and tasks CA and RA; enrolment and verification of certificates; architectures; applications.
Type of course (Compulsory, Specialization, etc.)	Compulsory
Semester	2. Semester
ECTS-Credits	3 (workload: 90 hours = 30 h contact hours and 60 h self-study)
Module co-ordinator	Dr. Eberhard von Faber
Lecturer	Dr. Eberhard von Faber
Entrance requirements	Basic understanding and knowledge of business processes and enterprise organization; basic knowledge of information technology: applications, systems and networks as well as underlying and related technologies.
Recommended literature (Teaching and learning materials, literature)	[1] Walter Fumy and Jörg Sauerbrey (Hrsg.): Enterprise Security, Publicis Verlag, 2006 [2] Michael Richter: Identity Management, Integration der Benutzerverwaltung in heterogene Systemlandschaft, Vdm Verlag Dr. Müller, 2007 [3] Claudia Eckert: IT-Sicherheit, Konzepte-Verfahren-Protokolle, Oldenburg Verlag, 2006 [4] Hans-Peter Königs: IT-Risiko-Management mit

	System, Von den Grundlagen bis zur Realisierung. Ein praxisorientierter Leitfaden, Vieweg, 2005 Scripts and other material will be delivered during the lectures
Teaching and learning methods	Lectures using multimedia
Type of examination/methods	Seminar paper
Language of instruction	German
Special remarks (i.e. online-segments, practical visits, guest speakers)	

2.3 Development of Secure IT Systems

Title of course	Development of Secure IT Systems
Teaching aims	<p>Based on skills gained in the courses Network Security and Cryptology, this course is an introduction to „Security Engineering,“ a new field of engineering sciences. Students will learn methods for the ascertainment of relevant system properties, protection requirement determination, threat and risk assessment techniques for the design of IT-systems, as well as the design and implementation of security strategies and security architectures on the basis of generally common phase oriented models of system development. Furthermore, methods, techniques and tools for the development of software used in critical application areas will be introduced, and there prospects and boundaries will be tested.</p> <p>Thus, students will gain a comprehensive hands-on insight into modern methods of the design of security-sensitive applications. With these skills in a highly complex field of IT-security, students will qualify for a career in the free economy as well as in research and development.</p>
Contents	<ul style="list-style-type: none"> • Software-Engineering, programming and hardware-design • Security-Engineering <ul style="list-style-type: none"> – Development process, phase oriented models and principles of construction – Structure analysis and protection requirement determination – Risk assessment – security strategies and security architectures and validation • Security aspects of the implementation of IT-systems <ul style="list-style-type: none"> – Programming mistakes as security risks – Security aspects of programming – Programming languages and operating systems – Development tools – User-oriented design of interactive IT-security systems, Human-Computer-Interaction • Evaluation of IT-security systems <ul style="list-style-type: none"> – Test procedures and methods, e.g. Junit – semiformal and formal Verification of IT-systems
Type of course (Compulsory, Specialization, etc.)	Compulsory
Semester	2. Semester
ECTS-Credits	6 (Workload: 180 hours = 65 h contact hours and 115 h self studies)
Module co-ordinator	Prof. Dr. Vielhauer
Lecturer	Prof. Dr. Vielhauer
Entrance requirements	Basic knowledge of Software Engineering: object oriented modelling and programming
Recommended literature (Teaching and learning materials, literature)	N. Leveson: Safeware: System Safety and Computers, Addison-Wesley Longman, Amsterdam, 1995.

	<p>S. J. Powell, R. C. Linger, J. H. Poore: Cleanroom Software Engineering: Technology and Process, Addison-Wesley Professional, 1999.</p> <p>G. J. Myers: Methodisches Testen von Programmen, Oldenbourg, Auflage: 7., Aufl., 2001</p> <p>Peter Liggesmeyer: Software-Qualität, Testen, Analysieren und Verifizieren von Software, Spektrum Akademischer Verlag, 2002.</p> <p>Andrew Hunt, David Thomas: Pragmatisch Programmieren Uni-Tests mit Junit, Hanser Fachbuchverlag; Auflage: 1, 2005.</p> <p>Elfriede Dustin, Jeff Rashka, John Paul: Software Automatisch Testen, Springer, Berlin, 1. Aufl., 2001.</p>
Teaching and learning methods	
Type of examination/methods	<p>Practical work: Successful development of a secure software system</p> <p>Written final exam/oral exam, graded</p> <p>Final grade will be the average of the practical work and the final exam</p>
Language of instruction	German
Special remarks (i.e. online-segments, practical visits, guest speakers)	

3 Mathematical and Physical Basics

3.1 *Introduction to Communication Security*

Title of course	Introduction to Communication Security
Teaching aims	Being familiar with the basic toolset of an security analyzer / security designer; constantly considering both attacks and defences; usage of analogies and models; design and use of attack scenarios; developing the capabilities to design, implement and assess security mechanisms and solutions; concept tamper-proof and its implementation; understand many security measures even being implemented in hardware as well as specific attacks
Contents	Payment systems: mapping direct interaction onto electronic (virtual) processes, the necessity of security modules (e.g. as key storage); potentials and limitations of electronic communication, key management, processes and systems; fundamental threat models with indirect/direct attacks and covered channels; logical versus physical security, basic concepts and security design criteria; embedded systems: threat model; security elements and mechanisms; life-cycle and device management; smart cards: classification, types and characteristics, life-cycle; production processes including personalization; how a „computer“ works internally, smart cards: architecture, programming and realization; threat and attack model; attacks like DFA, DPA, reverse engineering, chip manipulation etc.; tools and techniques being used; countermeasures and how to surmount or assess them in practice; the concept of assurance, security evaluation and certification.
Type of course (Compulsory, Specialization, etc.)	Compulsory
Semester	1. Semester
ECTS-Credits	3 (workload: 90 hours = 30 h contact hours and 60 h self-study)
Module co-ordinator	Dr. Eberhard von Faber
Lecturer	Dr. Eberhard von Faber
Entrance requirements	Understanding the relevance of IT security and its role in the practice; basic knowledge of electrical engineering, cryptography and industrial processes and/or the willingness and ability to get familiar with
Recommended literature (Teaching and learning materials, literature)	<p>[1] Anderson, Ross: Security Engineering, A Guide to Building Dependable Distributed Systems; John Wiley & Sons, Inc.; 2001</p> <p>[2] FIPS PUB 140-2, Security Requirements for Cryptographic Modules; National Institute of Standards and Technology; 2002; http://csrc.nist.gov/cryptval/</p> <p>[3] Common Criteria for Information Technology Security Evaluation (also ISO15408), Part 1: Introduction and general model, Part 2: Security functional requirements,</p>

	<p>Part 3: Security assurance requirements http://www.bsi.de/cc/index.htm or http://www.commoncriteriaportal.org (and: CEM)</p> <p>[4] BSI-PP-0002, Smartcard Integrated Circuit Platform Protection Profile; Version 1.0, July 2001 (E. von Faber main technical editor); Smartcard Integrated Circuit Augmentations; Version 1.0, March 2002; http://www.bsi.bund.de/cc/pplist/pplist.htm</p> <p>[5] Rankl, Wolfgang and Effing, Wolfgang: Smart Card Handbook; John Wiley & Sons, 2003</p> <p>Scripts and other material will be delivered during the lectures</p>
Teaching and learning methods	Lecture using multimedia
Type of examination/methods	Written examination; exceptionally oral examination
Language of instruction	German
Special remarks (i.e. online-segments, practical visits, guest speakers)	

3.2 *Cryptology*

Title of course	Cryptology
Teaching aims	This course introduces and explains the mathematical foundations of secure communication. In this sense it covers information theory but also cryptography and cryptanalysis.
Contents	<p>The main topics of the course include methods for hiding information, for ensuring data integrity, and for achieving user authentication in digital communication networks. The students should deal with common cryptographic protocols in order to get a deep understanding of their strengths and weaknesses, where the focus lies on methods to ensure secure electronic business transactions.</p> <p>In the exercises the students learn to deal with cryptographic applications. They also investigate how cryptographic applications are designed and implemented.</p> <p>Beyond that, the students are expected to write a semester paper (approx. 20 pages) about a specific topic from the field of cryptology.</p>
Type of course (Compulsory, Specialization, etc.)	Compulsory
Semester	1. Semester
ECTS-Credits	3 (workload: 90 hours = 30 h contact hours and 60 h self-study)
Module co-ordinator	Prof. Dr. Michael Syrjakow
Lecturer	Prof. Dr. Michael Syrjakow
Entrance requirements	
Recommended literature (Teaching and learning materials, literature)	<p>Beutelspacher, Kryptologie, Vieweg, 2005</p> <p>J. Daemen – V. Rijmen, The Design of Rijndael.AES, Springer, 2001</p> <p>C. A. Deavours – L. Kruh, Machine Cryptography and Modern Cryptanalysis, Artech House Publishers, 1985</p> <p>D. E. Knuth, The Art of Computer Programming 2, Seminumerical Algorithms, Addison-Wesley, 1998</p> <p>A. J. Menezes - P. van Oorschoot - S. Vanstone, Handbook of Applied Cryptography, CRC, 1996</p> <p>M. Rosing, Implementing Elliptic Curve Cryptography, Manning Publications, 1998</p> <p>B. Schneier, Angewandte Kryptographie, Pearson Studium, 2005</p> <p>A. Sinkov, Elementary Cryptanalysis, The Mathematical Association of America, 1998</p> <p>M. Welschenbach, Cryptography in C and C++, Apress, 2005</p> <p>J. Bamford, Body of Secret: Anatomy of the Ultra-Secret National Security Agency, Anchor, Reprint Edition, 2002</p>
Teaching and learning methods	Lectures with various media (digital projector, and overhead

	projector), Exercises with PCs in small groups (maximal 10 students)
Type of examination/methods	Written examination at the end of the course, 90 minutes, graded
Language of instruction	German
Special remarks (i.e. online-segments, practical visits, guest speakers)	The e-learning program CrypTool http://www.cryptool.de/ is used

4 Law and Business Administration

4.1 Law

Title of course	Law
Teaching aims	Regulatory Framework of Security Measures
Contents	<p>1. Liability law</p> <p>1. Insolvency law Contractual basic principles, strict liability in tort, law of torts, preconditions and procedure (company/consumer insolvency proceedings and exemption from remaining debt proceedings)</p> <p>2. Telecommunications law System and content in TKG regulations 2001/21/EG;2002/19/EG, 2002/22/EG, TKV, TKÜV (telecommunications media law)</p> <p>3. Legal basis for the surveillance of telecommunications systems</p> <p>Basis of liability law (civil and strict liability in tort in telecommunications systems) and aspects of criminal law and procedural law in regard to surveillance measures</p> <p>4. Data protection laws Basics of telecommunications media law, state broadcasting contract, BGB –Info V(German Civil Code) from the perspective of right to information and its obligations as well as their legal enforcement</p> <p>5. Legal regulations on signature law and ordinance regarding digital signature</p> <p>Preconditions and procedure, particularly with regard to electronic declaration of intent and objective and subjective burden of proof as regulated by §126 a BGB</p> <p>6. Industrial property rights Copyright law/digital copyright law; patent/protection of utility patents; trade marks/domain law, protection of registered designs; aspects of competition law</p> <p>7. Company health and safety regulations Basic contractual prerequisites, general laws governing equal opportunities, labour protection laws, law governing company medical officers, security engineers and specialists for workplace safety: Health and Safety at Work Act; Ordinance on Industrial Safety and Health; German national ordinance governing VDU workplaces, Ordinance on dangerous substances</p> <p>8. Weapons law Rules of weapon law: need, reliability, purchase of firearms, storage, illegal weapons, ammunition notification and illegal or legal use of weapons from the perspective of civil and criminal law</p>
Type of course	Compulsory
Semester	1 st semester

ECTS-Credits	6 ECTS credits Workload: 180 hours 65 contact hours 115 self-study hours
Module co-ordinator	Prof. Dr. Michaela Schröter
Lecturer	Prof. Dr. Michaela Schröter, Prof. Dr. Macke, Herr Nitschke (patent agent)
Entrance requirements	
Recommended literature	
Teaching and learning methods	Lecture using a variety of media. Students will prepare the topic of the following session by reading up relevant laws and current literature on the subject. This results in an active and focused preparation and a means to cope with the considerable amount of material to be covered. Work on industrial property rights will be followed by a discussion with a patent agent on the application of law in this field. Topical examples of legal practice will be discussed and examined.
Type of examination/methods	Term paper and presentation and/or oral examination
Language of instruction	German
Special remarks	

4.2 Corporate Governance, Human Resource and Conflict Management

Title of course	Corporate Governance, Human Resource and Conflict Management
Teaching aims	Students will use their basic knowledge in business administration and have to solve complex challenges in doing advanced business decisions.
Contents	<ul style="list-style-type: none"> • Goals of Corporate Governance (Development of strategies, code of conduct, business objectives, corporate culture, staff management) • Ethical aspects of management (Anti-corruption strategies etc.) • Risk management • Crisis management (Theories, Detection and identification of a crisis, legal aspects) • Conflict management (Diagnosis, types of conflicts, strategies of conflict handling, de-escalation strategies)
Type of course (Compulsory, Specialization, etc.)	Compulsory
Semester	2. Semester
ECTS-Credits	3 (workload: 90 hours = 30 h contact hours and 60 h self-study)
Module co-ordinator	Prof. Dr. Robert U. Franz
Lecturer	Prof. Dr. Robert U. Franz
Entrance requirements	
Recommended literature (Teaching and learning materials, literature)	K. Macharzina: Unternehmensführung T. Hutzschenreuther: Krisenmanagement F. Glasl: Konfliktmanagement Case Studies and Hand outs
Teaching and learning methods	Lecture with project work and business games
Type of examination/methods	Project work+ presentation and/or oral examination
Language of instruction	German
Special remarks (i.e. online-segments, practical visits, guest speakers)	Case studies, business games, guest speakers

5 Miscellaneous Modules

5.1 Semester Paper 1 and 2

Title of course	Semester Paper 1 and 2
Teaching aims	Students shall improve and broaden their skills in the independent scientific discussion of questions in the field of Security Management and so do preparatory work for a top level Master's thesis. Both term papers may have topics based on each other; topics may be taken from commercial practice.
Contents	<ol style="list-style-type: none"> 1. Method of collecting data (statistics, Interviews, primary/secondary sources) 2. Strengthening of discussion skills: research, reading, reviewing 3. Creative techniques and individual organization 4. situational styles of writing (Advertising, press releases, scientific papers ...) 5. Scientific methods of writing 6. Writing a synopsis 7. Methodical structuring of science papers 8. Raisons d'être of scientific work groups 9. Phases of the scientific work <ol style="list-style-type: none"> 1. Research and collection of sources and materials 2. Review of sources/materials and their selection 3. Work on sources/materials and topic 10. Correct quotation
Type of course (Compulsory, Specialization, etc.)	Compulsory
Semester	1. and 2. Semester
ECTS-Credits	3 (workload: 90 hours = 30 h contact hours and 60 h self-study)
Module co-ordinator	Prof. Dr. Friedrich-L. Holl
Lecturer	Prof. Dr. Friedrich-L. Holl Holl and other lectures
Entrance requirements	
Recommended literature (Teaching and learning materials, literature)	<p>DIN 1421 (Gliederung und Benummerung in Texten)</p> <p>Eco, U. (2005): Wie man eine wissenschaftliche Abschlussarbeit schreibt - Doktor-, Diplom- und Magisterarbeit in den Geistes- und Sozialwissenschaften, Müller, Heidelberg, 11. unveränd. Aufl. d. dt. Ausg.</p> <p>Theisen, Manuel R.: Wissenschaftliches Arbeiten - Technik Methodik, Form, 2000.</p> <p>Peterßen, Wilhelm H.: Wissenschaftliche(s) Arbeiten - Eine</p>

	Einführung für Schule und Studium, 1999.
Teaching and learning methods	Exercises in small groups
Type of examination/methods	Semester paper and presentation
Language of instruction	German
Special remarks (i.e. online-segments, practical visits, guest speakers)	

6 Elective Modules and Projects

6.1 *Project*

Title of course	Project
Teaching aims	<p>On the basis of a complex assignment (project), students shall learn the handling of problems/tasks with multiple contexts. Work which may have been begun in the compulsory optional subject possibly can be continued.</p> <p>Aim of the course is to develop awareness for the essential importance of integral thinking in the context of security. In addition to the methods mentioned below, which are an essential part of the project, course contents will depend on the actual practical tasks chosen by students.</p> <p>Project example 1: Cyber-crime: During the past years, internet crime, or cyber-crime, has increased rapidly. Problems in this field range from dialers and mock lotteries to damage from viruses and worms and to unconstitutional content, fraud in online auctions and violations of data protection laws. During the project, students will deal with a subject from the huge field of cyber-crime on a scientific level mostly independently and present their results.</p> <p>Project example 2: Application system: In this project, students will have the opportunity to deal in laboratories under conditions close to reality with the choice, configuration, and adaptation of application software with regard to aspects of security. Possible examples for software-systems to be worked with are for instance database servers, database applications, and software products for the planning and control of companies (e.g. ERP-Systems). During the project, students will deal with a specific subject mostly independently and present their results at the end of the semester.</p> <p>Project example 3: Complex Security Scenario (Luggage management on airports, protection of large areas, protection of storages with goods of high value etc): Students will explore the state of the art in the relevant technologies, for example through visits at companies and/or users of such security solutions, analyze the systems, look for flaws, and develop concepts of how such scenarios might work in the future. Special attention will be payed to developing innovative ideas for security solutions and on this basis draft applications for research and development projects. The goal of such a plan is to build a base for research-oriented master's theses.</p>
Contents	<p>Problem recognition and definition: - scientific definition of the „state of the art“</p>

	<ul style="list-style-type: none"> - Integration into the current practical context - General conditions of the adoption - Application of various analysis methods, like for instance interviews, questionnaires, Delphi Method, formulation of the document-context relating to the analyzed field etc. <p>Analysis of weaknesses:</p> <ul style="list-style-type: none"> - Comparison of the existing Applications/ conditions with possible developments <p>Target concept:</p> <ul style="list-style-type: none"> - scientific development of a practice oriented method of resolution - Adoption of creative methods - Cost-benefit analysis - Development of the general conditions of the application / service <p>Prototyping:</p> <ul style="list-style-type: none"> - development of a software prototype - Implementation in the company/organization <p>The entire course will be organized according to the principles of project management.</p>
Type of course (Compulsory, Specialization, etc.)	Compulsory
Semester	2. Semester
ECTS-Credits	6 (Workload: 180 hours = 60h contact hours and 120 h self-study)
Module co-ordinator	Prof. Dr. Friedrich-L. Holl
Lecturer	Prof. Dr. Friedrich-L. Holl and other lecturers
Entrance requirements	required knowledge and skills from compulsory optional subject, depending on the project's topic
Recommended literature (Teaching and learning materials, literature)	Depends on project
Teaching and learning methods	Project work in groups of up to 7 participants, in cooperation with companies/organizations, documentation of results in accordance to scientific methods.
Type of examination/methods	Project report at the end of the semester which will be presented to and defended before the participating company/organization.
Language of instruction	German
Special remarks (i.e. online-segments, practical visits, guest speakers)	High orientation on companies and organizations

6.2 *Elective Modules 1, 2 and 3*

Title of course	Elective Modules 1, 2 and 3
Teaching aims	NN
Contents	NN
Type of course (Compulsory, Specialization, etc.)	Elective
Semester	1. or 3. Semester
ECTS-Credits	3 (Workload: 90 hours = 30h contact hours and 60 h self-study)
Module co-ordinator	Prof. Dr. Friedrich-L. Holl
Lecturer	
Entrance requirements	
Recommended literature (Teaching and learning materials, literature)	NN
Teaching and learning methods	Lectures and exercises in small groups
Type of examination/methods	Graded term paper and presentation
Language of instruction	German
Special remarks (i.e. online-segments, practical visits, guest speakers)	In enterprises and organisations

7 General Modules

7.1 Master Seminar

Title of course	Master Seminar
Teaching aims	<ul style="list-style-type: none"> • Methodological qualification for internationally focused research and conferences • Know-how to link academic state-of-the-art with the results of the project • Acquisition of skills to derive at academic results while training scientific methodology
Contents	<ul style="list-style-type: none"> • High-level academic working techniques including scientific language standards (English) • Standards of academic case work • Dealing with discussion papers and papers for international conferences (writing and discussion) • Simulation of a paper review process • Training of academic commentary techniques
Type of course (Compulsory, Specialization, etc.)	Compulsory
Semester	3. Semester
ECTS-Credits	Work load: 90h: 30 contact hours, 60h self-study, paper preparation Ratio: 30 h/ ECTS-Credit -> 3 ECTS-Credits
Module co-ordinator	A. Erhardt Ewert
Lecturer	All professors
Entrance requirements	
Recommended literature (Teaching and learning materials, literature)	<p>Booth, W. C. et a. (1995). The draft of research. Chicago London</p> <p>Brown, S. R. et al. (1990) Experimental Design and Analysis. London</p> <p>Cialdini, R. B. (2001). Influence, Science and Proctice. Bosten, M.A.</p> <p>Hussley, J., Hussley, R. (1997). Business Research. A practical guide for undergraduate and postgraduate students</p> <p>Karmasin, M. et al. (1999). Die Gestaltung wissenschaftlicher Arbeiten: ein Leitfaden für Haus-, Seminar- und Diplomarbeiten sowie Dissertationen. Wien</p> <p>Pyrzczak, S. et. Al. (1998). Writing empirical Research Reports. Los Angeles. C.A.</p> <p>Seale, C. (1999). The quality of quantitative research. London</p> <p>Trachim, W. M. K. (2000). The Research Knowledge Base. Cincinetti. Ohio</p>
Teaching and learning methods	Presentations, active participation of the students in discussions and working groups
Type of examination/methods	Not meant to be graded
Language of instruction	English, German
Special remarks (i.e. online-segments,	

practical visits, guest speakers)	
-----------------------------------	--

7.2 Master Thesis

Title of course	Master Thesis
Teaching aims	The Master thesis demonstrates the student's ability to self-responsibly analyse a challenging topic in security management. The candidate has to prove that she/he can fulfil scientific quality standards and can derive at relevant practice-oriented solutions.
Contents	The Master thesis is a degree paper worth of 21 credits that is succeeded by a colloquium. The maximal amount of time for executing the thesis is 4 months.
Type of course (Compulsory, Specialization, etc.)	Compulsory
Semester	3. Semester
ECTS-Credits	The Master work includes at least 60 pages. The processing time is 4 months). The effort represents 21 CP incl. colloquium.
Module co-ordinator	A. Erhardt Ewert
Lecturer	All professors
Entrance requirements	Only if there are no academic achievements outstanding.
Recommended literature (Teaching and learning materials, literature)	Booth, W. C. et a. (1995). The draft of research. Chicago London Brown, S. R. et al. (1990) Experimental Design and Analysis. London Cialdini, R. B. (2001). Influence, Science and Proctice. Bosten, M.A. Hussley, J., Hussley, R. (1997). Business Research. A practical guide for undergraduate and postgraduate students Karmasin, M. et al. (1999). Die Gestaltung wissenschaftlicher Arbeiten: ein Leitfaden für Haus-, Seminar- und Diplomarbeiten sowie Dissertationen. Wien Pyrzczak, S. et. Al. (1998). Writing empirical Research Reports. Los Angeles. C.A. Seale, C. (1999). The quality of quantitative research. London Trachim, W. M. K. (2000). The Research Knowledge Base. Cincinatti. Ohio
Teaching and learning methods	Independent scientific work
Type of examination/methods	For the final grade the written paper is to be weighted with 0,75 and the colloquiums is to be weighted with 0,25.
Language of instruction	German or English, other languages can be accepted by board of examiners
Special remarks (i.e. online-segments, practical visits, guest speakers)	

7.3 **Master- Colloquium**

Title of course	Master- Colloquium
Teaching aims	The aim of the module is to present the Master thesis which is a key element of the curriculum. The candidate presents and defends his or her master thesis according to scientific standards.
Contents	Exam preparation, presentation, oral exam and discussion
Type of course (Compulsory, Specialization, etc.)	Compulsory
Semester	3. Semester
ECTS-Credits	90 h (3 CP)
Module co-ordinator	A. Erhardt Ewert Prof. Dr. Bettina Burger-Menzel
Lecturer	All professors
Entrance requirements	A colloquium on Master's thesis can take place only if there are no academic achievements outstanding..
Recommended literature (Teaching and learning materials, literature)	Birkenbihl, V.: Kommunikationstraining, Landsberg am Lech 1998. Motamedi, S.: Präsentation - Ziele, Konzepte, Durchführung, Heidelberg 1998. Motamedi, S.: Rede und Vortrag, Weinheim/Basel 1993. Schilling; G.: Angewandte Rhetorik und Präsentationstechnik, Berlin 1998. Müller-Schwarz, U.; Weyer, B.: Präsentationstechnik - Mehr Erfolg durch Visualisierung bei Vortrag und Verkauf, Wiesbaden 1991. Bernstein, D.: Die Kunst der Präsentation, Frankfurt/M 1992. Hierhold, E.: Sicher präsentieren – wirksam vortragen, Wien 1994. Seifert, J. W.: Visualisieren, Präsentieren, Moderieren, Gabal; Edmüller, A.; Wilhelm, T.: Moderation: Haufe
Teaching and learning methods	Presentation and discussion
Type of examination/methods	For the final grade the written paper is to be weighted with 0,75 and the colloquiums is to be weighted with 0,25.
Language of instruction	German or English
Special remarks (i.e. online-segments, practical visits, guest speakers)	