MATERIAL SAFETY AND RELIABILITY

1. GENERAL

SCHOOL	ENGINEERING		
SECTION	INFORMATICS AND COMPUTER ENGINEERING		
LEVEL OF STUDIES	UNDERGRADUATE		
COURSE CODE		**SEMESTER OF STUDY**	8th
COURSE TITLE	HARDWARE SECURITY AND RELIABILITY		
INDEPENDENT TEACHING ACTIVITIES *in case the credits are awarded in distinct parts of the course e.g. Lectures, Laboratory Exercises, etc. If the credits are awarded uniformly for the entire course indicate the weekly teaching hours and the total number of credits*		**WEEKLY HOURS TEACHING**	**CREDIT UNITS**
Lectures		3	
Laboratory exercises		1	
Add rows if needed. The organization of teaching and the Teaching methods used are described in detail in 4.		**4**	**5**
COURSE TYPE *Background, General Knowledge, Scientific Area, Development Skill*	Scientific Area, Skills Development		
PREREQUISITES COURSES:			
LANGUAGE OF INSTRUCTION and EXAMINATION:	Greek		
THE COURSE IS OFFERED TO ERASMUS STUDENTS	Yes (in English)		
ONLINE COURSE PAGE (URL)			

2. LEARNING OUTCOMES

Learning Outcomes

The learning outcomes of the course are described, the specific knowledge, skills and abilities of an appropriate level that students will acquire after the successful completion of the course.

Consult Appendix A

- *Description of the Level of Learning Outcomes for each course of study according to the European Higher Education Area Qualifications Framework*
- *Descriptors of Levels 6, 7 & 8 of the European Qualifications Framework for Lifelong Learning and Annex B*
- *Summary Guide for writing Learning Outcomes*

The aim of the course is to complete the students' knowledge in the field of safety and material reliability.

Upon completion of the course the student will be able to:

- designs digital circuits for cryptographic applications
- design circuits containing built-in test structures for easy controllability
- checks circuits for defects or harmful hardware trojans
- describes the concepts of reliable and energy-efficient computing and the requirements that the respective systems must meet.
- formulates reliability requirements for a system.
- describe the types of errors, failures and risks in a system and ways to deal with them, and choose appropriate responses .
- describe and apply reliability analysis methods.
- describe and be able to apply reliability assessment methods.
- understand the energy requirements of a system
- understand the main sources of a system's energy consumption
- describe and apply energy/power optimization techniques to the hardware
-

General Skills

Taking into account the general competencies that the graduate must have acquired (as listed in the Diploma Supplement and listed below) which of them is the subject aimed at?	
Search, analysis and synthesis of data and information, using the necessary technologies *Adapting to new situations Decision making* *Autonomous work* *Teamwork* *Working in an international environment Working in an interdisciplinary environment* *Generating new research ideas*	*Project planning and management* *Respect for diversity and multiculturalism Respect for the natural environment* *Demonstrate social, professional and ethical responsibility and sensitivity to gender issues Criticism and self-criticism* *Promotion of free, creative and inductive thinking*

3. COURSE CONTENT

- Autonomous Work
- Teamwork
- Introduction to fault tolerance and reliability
- Basic reliability concepts
- Reliability assessment techniques
- Reliability requirements
- Reliability analysis
- Hardware redundancy
- Information redundancy
- Time redundancy
- Troubleshooting errors
- Reliability rating
- Introduction to low-power design
- Basic techniques for designing low-power digital circuits
- Energy efficient processor architectures
- Energy efficient memories and caches
- Energy efficient operating systems compilers and application software
- Low power graphics processors
- Introduction to cryptography & data security
- Data encryption standards (DES, AES) & block ciphers
- Introduction to public-key cryptography & RSA cryptosystem
- Hardware metering & digital watermarking
- Security based on physically unclonable functions (PUFs)
- Physical attacks, side-channel attacks and countermeasures
- System-level energy optimization techniques for embedded systems
- Hardware Trojan
- True random number generators & hardware security in contactless tokens
- Hardware-based security architectures & trusted platform module

4. TEACHING AND LEARNING METHODS - ASSESSMENT

HOW TO DELIVER *Face-to-face, Remote education , etc.*	Face-to-face (in class)
USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES *Use of ICT in Teaching, in Laboratory Training, in Communication with students*	Support of the learning process through the electronic platform of the University

TEACHING ORGANIZATION *The way and methods of teaching* are described *in detail.* *Lectures, Seminars, Laboratory Exercise, Field Exercise, Bibliography* Study & Analysis, *Tutorial, Practice* (placement), *Clinical Practicum, Art Workshop, Interactive teaching, Educational visits, Project preparation, Writing of work / assignments, Artistic creation, etc.* *Indicate the student's study hours for each learning activity as well as* the *hours of unguided study so that the total workload at semester level corresponds to ECTS standards.*	**Activity** / **Workload Semester** Lectures: 39 Laboratory Exercises: 13 Project: 20 Independent Study: 53 **Course Total** (25 hours of load working per credit unit): **125**
STUDENT EVALUATION *Description of the evaluation process* *Assessment Language, Assessment Methods, Formative or Inferential, Multiple Choice Test, Short Answer Questions, Essay Development Questions, Problem Solving, Written Assignment,* Report */Report, Oral Exam, Public Presentation, Laboratory Work, Clinical Patient Examination, Artistic Performance,* Other / *Other* *Explicitly defined* assessment *criteria* are indicated and *if and where they are accessible to students.*	I. Written final exam (80%) including : - Multiple choice questions - Short answer questions - Solving problems related to the design of digital systems - II. Project/Laboratory exercises (20%) For successful completion, a grade of at least 5/10 in the Written Final Exam is required.

5. RECOMMENDED-BIBLIOGRAPHY

- Suggested Bibliography :

1. Digital Design with VHDL, Peter Ashenden, New Technologies Publications 2010
2. Introduction to Hardware Security and Trust, First Edition, Mohammad Tehranipoor and Cliff Wang (Ed.) (2012), Springer, ISBN-13: 978-1-4419-8079-3 or ISBN-10: 1- 4419-8079-2 or e-ISBN: 978-1-4419-8080-9.
3. Towards Hardware-Intrinsic Security, First Edition, Ahmad-Reza Sadeghi and David Naccache (Eds.) (2010), Springer, ISBN-13: 978-3-642-14451-6 or ISBN-10: 3-642-14451-9 or e-ISBN: 978-3-642-14452-3.
4. Fault-Tolerant Systems, First Edition, Israel Koren and C. Mani Krishna (2007), Elsevier Morgan Kaufmann Publishers, ISBN-13: 978-0-12-088525-1 or ISBN-10: 0-12-088525-5
5. Fundamentals of Dependable Computing for Software Engineers, John Knight, CRC press, 2012.
6. Fault-Tolerant Design, Elena Dubrova, Springer, 2013
7. Building Dependable Distributed Systems, Wenbing Zhao, Willey publications
8. Developing Green Software, Dr. Bob Steigerwald and Abhishek Agrawal, Intel Corporation
9. Dependability benchmarking for Computer Systems, Karama Kanoun and Lisa Spainhower (eds), Willey publications & IEEE Computer Society
10. Dependable Computing: Design and Assessment, Ravishankar K. Iyer, Zbigniew T. Kalbarczyk, Nithin M. Nakka, Wiley, 2016

11. Dependable computer systems, Assen V. Krumov, CreateSpace Independent Publishing Platform, 2013
12. Computer Architecture Techniques For Power-Efficiency, Stefanos Kaxiras and Margaret Martonosi, Morgan & Claypool, 2008
13. System-Level Design Techniques For Energy-Efficient Embedded Systems, Marcus T. Schmitz, Bashir M. Al-Hashimi and Petru Eles, Springer 2009
14. Power-efficient System Design, Preeti Ranjan Panda, B. V. N. Silpa, Aviral Shrivastava, Krishnaiah Gummidipudi, Springer 2010
15. Low power design essentials, J. Rabaey, Springer 2009