SYLLABUS

1. Data about the program of study

1.1 Institution	The Technical University of Cluj-Napoca
1.2 Faculty	Faculty of Automation and Computer Science
1.3 Department	Automation
1.4 Field of study	System's Engineering
1.5 Cycle of study	Master
1.6 Program of study / Qualification	Cyber Physical Systems
1.7 Form of education	Full time

2. Data about the subject

2.1 Subject name	***Cyber-Physical Systems' Security***			Subject code	**10.00**
2.2 Course responsible / lecturer	Prof.dr.ing. Ovidiu Petru Stan – Ovidiu.stan@aut.utcluj.ro				
2.3 Teachers in charge of seminars / Laboratory / project	Drd.ing. Draghici Bogdan				
2.4 Year of study	1	2.5 Semester	2	2.6 Type of assessment (E - exam, C - colloquium, V – verification)	E
2.7 Subject category	Formative category: DA – advanced, DS – speciality, DC – complementary				DA
	Optionality: DI – imposed, DO – optional (alternative), DF – optional (free choice)				DI

3. Estimated total time

3.1 Number of hours per week	3	of which:	Course	1	Seminars	0	Laboratory	1	Project	0
3.2 Number of hours per semester	42	of which:	Course	28	Seminars	0	Laboratory	14	Project	0
3.3 Individual study:										
(a) Manual, lecture material and notes, bibliography										20
(b) Supplementary study in the library, online and in the field										20
(c) Preparation for seminars/laboratory works, homework, reports, portfolios, essays										13
(d) Tutoring										2
(e) Exams and tests										3
(f) Other activities:										0

3.4 Total hours of individual study (suma (3.3(a)…3.3(f)))	58
3.5 Total hours per semester (3.2+3.4)	100
3.6 Number of credit points	4

4. Pre-requisites (where appropriate)

4.1 Curriculum	• Mathematical Algebra, Special Mathematics, Probability • Programming in a high-level object language
4.2 Competence	Computer usage basics

5. Requirements (where appropriate)

5.1. For the course	Classroom with, video projector, blackboard, Internet connection
5.2. For the applications	Laboratory attendance is mandatory

6. Specific competence

6.1 Professional competences	• Applies the principles of scientific ethics and integrity in research activities • Communicates scientific findings • Conducts literature research • Develops professional networks with researchers • Disseminates results to the scientific community • Perform quality control • Manage interoperable and reusable data that is accessible and easy to find • Models and simulates hardware • Performs data analysis • Writes scientific and academic papers and technical documentation • Tests hardware • Analyzes software specifications • Develops software prototypes • Uses software libraries
6.2 Cross competences	• Show initiative • Think analytically • Apply scientific, technological, and engineering knowledge • Work in teams

7. Expected Learning Outcomes

Knowledge	The student will know: • advanced concepts, principles, and methodologies in systems engineering, automation, and cyber-physical systems • techniques, methods, and technologies for the analysis, design, implementation, and optimization of applications based on programmable equipment and embedded systems • principles of design, operation, and evaluation for complex control systems, industrial networks, and related hardware and software components • standards, best practices, and regulations for quality, safety, security, and ethical conduct in professional and research activities • the principles of scientific ethics, academic integrity, and responsible management of research and experimental data • interdisciplinary concepts from mathematics, signal processing, automation, control theory, and computer science applicable to the design and optimization of complex systems
Skills	The student will be able to: • conduct scientific and interdisciplinary research, analyze data, and communicate results effectively to professional and academic audiences • analyze technical data, evaluate alternatives, and apply problem-solving strategies to complex engineering challenges • apply ethical principles, academic integrity, and responsible research practices in professional activities • integrate multidisciplinary knowledge to design, optimize, implement, and evaluate innovative solutions for complex control systems and industrial networks
Responsibilities and autonomy	• The student will be responsible for carrying out professional or research projects in compliance with quality, safety, and security standard • The student will be responsible for ensuring ethical conduct, academic integrity, and proper management of research and experimental data • The student will be responsible for promoting collaboration, teamwork, knowledge transfer, and innovation within professional and research environments

8. Discipline objective (as results from the *key competences gained*)

8.1 General objective	• Identify and master the main modern techniques in security in the current technological context of the CPS and Internet of Things • This course aims to introduce students to the concept of CPS & IoT and its impact on our daily lives, make them understand the architecture and components of CPS & IoT and address the challenges and solutions of implementing.

	• Students will learn how to link and exchange communication costs and computing power, as well as hardware and software. In addition, digital security is a critical design issue for CPS systems. From this course, students will become aware of the issues of cyber-security issues raised by IoT and will gain knowledge about related security techniques. Students will also gain hands-on experiences about building IoT devices and implementing security techniques through team projects.
8.2 Specific objectives	• Use of specific algorithms/methods to secure data through encryption • Identification of vulnerabilities • Security assessment of smart devices • Understanding the impact of CPS & IoT technologies • Knowledge of emerging CPS & IoT technologies • Developing critical thinking skills

9. Contents

9.1 Lectures	Hours	Teaching methods	Notes
Course logistics + Security basics + IoT/CPS architecture and threat models	4	Presentation and reading from course notes and references, case studies, questions and answers face-to-face and online, case studies.	
Cyber threats: risk landscape and real attack case studies	4		
Program analysis for IoT/CPS (static/dynamic analysis, symbolic execution) + Binary analysis building blocks (program slicing, taint tracking, rewriting) + binary hardening	4		
Side-channel attacks (types, threat models, case studies) + defense strategies (static/dynamic enforcers)	4		
Formal verification and model checking (LTL/MTL) + data-driven verification for autonomous systems	4		
Machine learning for perception and decision making (sensor fusion, Kalman filter) + security of ML systems	4		
Security protocols verification + Trusted/Confidential Computing (TCC) + Cost-efficient hybrid hardening for DNNs + EU regulations (NIS2, CRA) + Cybersecurity assessments	4		

Bibliography:

- Ross Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems 3rd Edition, ISBN 978-1119642787, Chapters 1, 2, 3
- Trent Jaeger, Operating System Security, ISBN: 978-3-031-02333-0, Chapter 1
- Greer, C. , Burns, M. , Wollman, D. and Griffor, E. (2019), Cyber-Physical Systems and Internet of Things, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.SP.1900-202
- Anders Møller, Michael I. SchwartzbachStatic Program Analysis, https://cs.au.dk/~amoeller/spa/spa.pdf Chapter 1
- Compilers, Principles, Techniques and Tools (Dragon Book), Chapter 10
- Celik et al., Program Analysis of Commodity IoT Applications for Security and Privacy: Challenges and Opportunities, https://arxiv.org/pdf/1809.06962.pdf
- What is soundness (in static analysis) https://tinyurl.com/749mt8n8
- Shoshitaishvili et al., (State of) The Art of War: Offensive Techniques in Binary Analysis, https://sites.cs.ucsb.edu/~vigna/publications/2016_SP_angrSoK.pdf
- Mathias Payer, Software Security Principles, Policies, and Protection (Book), Chapter 4 (Memory and Type Safety), https://nebelwelt.net/SS3P/softsec.pdf
- Manes et al., The Art, Science, and Engineering of Fuzzing: A Survey (Paper), https://arxiv.org/pdf/1812.00140.pdf
- Klees et al., Evaluating Fuzz Testing (Paper), https://cseweb.ucsd.edu/~dstefan/cse227-spring20/papers/klees:evaluating.pdf
- Kapinski et al., Simulation-Based Approaches for Verification of Embedded Control Systems, https://viterbi-web.usc.edu/~jdeshmuk/teaching/cs699-fm-for-cps/Papers/B1.pdf
- Michael Huth, Mark Ryan, Logic in Computer Science, Modelling and Reasoning about Systems, Chapter 3 (Verification by Model Checking), http://staff.ustc.edu.cn/~huangwc/book/LogicInCS.pdf
- Yurtsever et al., A Survey of Autonomous Driving: Common Practices and Emerging Technologies (Paper), https://arxiv.org/pdf/1906.05113.pdf
- Spreitzer et al. Systematic Classification of Side-Channel Attacks: A Case Study for Mobile Devices, https://arxiv.org/pdf/1611.03748.pdf

- Lentzsch et al., Hey Alexa, is this Skill Safe? Taking a Closer Look at the Alexa Skill Ecosystem, https://anupamdas.org/paper/NDSS2021.pdf
- Blanchet et al., Modeling and Verifying Security Protocols with the Applied Pi Calculus and ProVerif, https://bblanche.gitlabpages.inria.fr/publications/BlanchetFnTPS16.pdf
- Cremers et al., A Comprehensive Symbolic Analysis of TLS 1.3, https://acmccs.github.io/papers/p1773-cremersA.pdf
- Cerdeira et al., SoK: Understanding the Prevailing Security Vulnerabilities in TrustZone-assisted TEE Systems, https://www.cs.purdue.edu/homes/pfonseca/papers/sp2020-tees.pdf
- Stan, O.P.; Enyedi, S.; Corches, C.; Flonta, S.; Stefan, I.; Gota, D.; Miclea, L. Method to Increase Dependability in a Cloud-Fog-Edge Environment. Sensors 2021, 21, 4714. https://doi.org/10.3390/s21144714
- Ovidiu Stan, Szilard Enyedi, Marius Misaros, Liviu Miclea, Introducere in dependabilitatea sistemelor - Vol1, UTPRESS, 2022, 978-606-737-597-8

9.2 Applications - Seminars/Laboratory/Project	Hours	Teaching methods	Notes
01. Cryptography foundations for CPS: Hashes and Message Authentication; Asymmetric & Symmetric Cryptography	2	Hands-on experiments + analysis	
02. Crypto and Crypto Protocols: User Authentication; Key Management; Authentication Protocols	2		
03. Network Security in CPS/IoT: Networking Background and TCP Attacks; Transport Layer Security; Routing Security; DNS Security; Firewalls and Tunnels; Intrusion Detection Systems	2		
04. Topic: Systems Security: Software Vulnerabilities; Access Control; Operating System Security	2		
05. Topic: Systems Security: Web Security; Mobile Security; IoT Security	2		
06. Machine Learning for Security Applications: Attacks on the Machine Learning Pipeline: Poisoning attacks, model theft attacks, adversarial examples, recovery of sensitive training data, and physical-world attacks; Threat Models: White Box, Black Box, and Grey Box; Transferability; Types of Defenses: Pre-processing, and robust optimization; Introduction to Privacy in Machine Learning: Membership inference and model inversion attacks	2		
07. Security of Machine Learning Systems (adversarial attacks + defenses)	2		

Bibliography

1. Ross Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems 3rd Edition, ISBN 978-1119642787, Chapters 1, 2, 3
2. Trent Jaeger, Operating System Security, ISBN: 978-3-031-02333-0, Chapter 1
3. Greer, C. , Burns, M. , Wollman, D. and Griffor, E. (2019), Cyber-Physical Systems and Internet of Things, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.SP.1900-202
4. Anders Møller, Michael I. SchwartzbachStatic Program Analysis, https://cs.au.dk/~amoeller/spa/spa.pdf Chapter 1
5. Compilers, Principles, Techniques and Tools (Dragon Book), Chapter 10
6. Celik et al., Program Analysis of Commodity IoT Applications for Security and Privacy: Challenges and Opportunities, https://arxiv.org/pdf/1809.06962.pdf
7. What is soundness (in static analysis) https://tinyurl.com/749mt8n8
8. Shoshitaishvili et al., (State of) The Art of War: Offensive Techniques in Binary Analysis, https://sites.cs.ucsb.edu/~vigna/publications/2016_SP_angrSoK.pdf
9. Mathias Payer, Software Security Principles, Policies, and Protection (Book), Chapter 4 (Memory and Type Safety), https://nebelwelt.net/SS3P/softsec.pdf

10. Manes et al., The Art, Science, and Engineering of Fuzzing: A Survey (Paper), https://arxiv.org/pdf/1812.00140.pdf
11. Klees et al., Evaluating Fuzz Testing (Paper), https://cseweb.ucsd.edu/~dstefan/cse227-spring20/papers/klees:evaluating.pdf
12. Kapinski et al., Simulation-Based Approaches for Verification of Embedded Control Systems, https://viterbi-web.usc.edu/~jdeshmuk/teaching/cs699-fm-for-cps/Papers/B1.pdf
13. Michael Huth, Mark Ryan, Logic in Computer Science, Modelling and Reasoning about Systems, Chapter 3 (Verification by Model Checking), http://staff.ustc.edu.cn/~huangwc/book/LogicInCS.pdf
14. Yurtsever et al., A Survey of Autonomous Driving: Common Practices and Emerging Technologies (Paper), https://arxiv.org/pdf/1906.05113.pdf
15. Spreitzer et al. Systematic Classification of Side-Channel Attacks: A Case Study for Mobile Devices, https://arxiv.org/pdf/1611.03748.pdf
16. Lentzsch et al., Hey Alexa, is this Skill Safe?: Taking a Closer Look at the Alexa Skill Ecosystem, https://anupamdas.org/paper/NDSS2021.pdf
17. Blanchet et al., Modeling and Verifying Security Protocols with the Applied Pi Calculus and ProVerif, https://bblanche.gitlabpages.inria.fr/publications/BlanchetFnTPS16.pdf
18. Cremers et al., A Comprehensive Symbolic Analysis of TLS 1.3, https://acmccs.github.io/papers/p1773-cremersA.pdf
19. Cerdeira et al., SoK: Understanding the Prevailing Security Vulnerabilities in TrustZone-assisted TEE Systems, https://www.cs.purdue.edu/homes/pfonseca/papers/sp2020-tees.pdf
20. Stan, O.P.; Enyedi, S.; Corches, C.; Flonta, S.; Stefan, I.; Gota, D.; Miclea, L. Method to Increase Dependability in a Cloud-Fog-Edge Environment. Sensors 2021, 21, 4714. https://doi.org/10.3390/s21144714
21. Ovidiu Stan, Szilard Enyedi, Marius Misaros, Liviu Miclea, Introducere in dependabilitatea sistemelor - Vol1, UTPRESS, 2022, 978-606-737-597-8

Se vor preciza, după caz: tematica seminariilor, lucrările de laborator, tematica și etapele proiectului.

9. Bridging course contents with the expectations of the representatives of the community, professional associations and employers in the field

The course is essential in cyber-physical systems and familiarizes students with the basic security problems and solutions. The material is continuously adapted to the requirements of potential employers and to the feedback of already employed graduates.

10. Evaluation

Activity type	Assessment criteria	Assessment methods	Weight in the final grade
Course	Method of analysis, synthesis and integration of theoretical information	Exam	30%
Seminar	-	-	-
Laboratory	Method of analysis, synthesis and integration of theoretical information	Project	40%
	Problem solving corresponding to laboratory meetings	Presentation of solutions, answers to questions	5%
	Scientific paper	1. Organization - adherence to IEEE format and structure; concordance and flow of work 2. Content - relevance and comprehensive coverage of subject matter; application of concepts presented in the course; reflection of critical thinking skills 3. Inclusion of a minimum of 10 references	15%

Project			

Minimum standard of performance:

- Attend laboratory meetings and complete all assignments
- Concurrent conditions for passing the exam
  - Minimum of 5 points from the exam
  - Minimum 5 points from project + scientific paper

Date of filling in: 01.09.2025	**Responsible**	**Title First name Last name**	**Signature**
	Course	Prof.dr.ing. Ovidiu Petru Stan	
	Applications	Drd.ing. Draghici Bogdan	

Date of approval in the department of Automation _____	Head of department, Prof.dr.eng. Honoriu VĂLEAN
Date of approval in the Faculty of Automation and Computer Science Council _____	Dean, Prof.dr.eng. Vlad MUREȘAN