SYLLABUS

1. Program Information

1.1 Higher education institution	Technical University of Cluj-Napoca
1.2 Faculty	Faculty of Automation and Computer Science
1.3 Department	Department of Automation
1.4 Field of study	Automation, Applied Informatics and Intelligent Systems
1.5 Cycle of studies	Bachelor
1.6 Study Programme/Qualification	Intelligent Automation Systems (dual, in English language)
1.7 Form of education	IF – full-time education
1.8 Course code	50.00

2. Course information

2.1 Course title	**Cybersecurity for Industrial Automation**					
2.2 Course lecturer	*Conf.dr.ing. Adrian Colesa – adrian.colesa@cs.utcluj.ro*					
2.3 Seminar / Laboratory / Project Lecturer	*Dr.ing.Ievgen Babeshko (Emerson)* *Ing. Sebastian Ciceu (Emerson)*					
2.4 Year of study	4	2.5 Semester	1	2.6 Type of assessment		E
2.7 Course status	Formative category *(DF, DS, DC)*					DS
	Optionality *(DOB, DOP, DFac)*					DOB

3.Total estimated time

3.1 Number of hours per week	4	of which:	HEI	Lecture	2	Seminar	0	Laboratory	0	Project	0
			CO		0		0		2		0
3.2 Number of hours per semester	56	of which:	HEI	Lecture	28	Seminar	0	Laboratory	0	Project	0
			CO		0		0		28		0

3.3 Distribution of time allocation (hours per semester) for:	HEI	CO
(a) Study based on textbook, course support, bibliography, and notes	14	
(b) Additional documentation in library, specialized electronic platforms, and fieldwork		14
(c) Preparation of seminars/laboratories, assignments, papers, portfolios and essays		14
(d) Tutoring	5	5
(e) Examinations	3	14
(f) Other activities:		
3.4 Total individual study hours (sum (3.3(a)... 3.3(f)))	22	47
3.5 Total hours per semester (3.2+3.4)	50	75
3.6 Number of credits per semester	2	3

(HEI = Higher Education Institution, CO = Company)

4. Prerequisites (where applicable)

4.1 Curriculum Prerequisites	• Computer Programming and Algorithm Design • Computer Architecture, Operating Systems and Fundamentals of Computer Networking
4.2 Competency Prerequisites	

5. Conditions (where applicable)

5.1. Course Organization Conditions	• Course lectures will be delivered using presentations, visual aids, and discussions to foster understanding of cybersecurity principles in industrial environments.
5.2. Seminar / Laboratory / Project organization conditions	• The laboratory environment will include industrial control systems (ICS), virtualization environments (Hyper-V), SIEM solutions, and data protection systems.

	• Students will have access to real hardware (servers, workstations, networking equipment) used in industrial automation. • Activities will be supported by dedicated software tools (e.g., DeltaV Cybersecurity Manual, threat monitoring tools, endpoint protection solutions). • Guided supervision will be provided by experienced professionals during in-company sessions.

6. Specific Competencies Acquired

Professional Competencies	• PC01 Adjust engineering designs • PC03 Approve engineering design • PC06 Define technical requirements • PC07 Demonstrate disciplinary expertise • PC09 Design prototypes • PC26 Use information technology tools • PC29 Come up with solutions to problems • PC32 Perform data analysis
Transversal Competencies	• TC01 Apply knowledge of science, technology and engineering • TC02 Think analytically • TC03 Demonstrate responsibility

7. Learning outcomes

Knowledge:	• The student will be able to describe key concepts of cybersecurity in the context of industrial automation and control systems (ICS). • The student will be able to identify and explain differences between IT and OT security requirements and architectures. • The student will be able to summarize European cybersecurity directives (NIS2, CRA) and their impact on industrial environments.
Skills:	• The student will be able to implement cybersecurity best practices for OT environments, including endpoint protection, application whitelisting, and system hardening. • The student will be able to apply procedures for data protection, resilience, and incident response in industrial control systems. • The student will be able to conduct basic cybersecurity assessments, identify risks, and suggest mitigation strategies.
Responsibility and autonomy:	• The student will be able to work independently and in teams to analyze cyber threats and propose countermeasures for OT environments. • The student will be able to demonstrate a responsible approach in applying cybersecurity solutions within industrial automation projects. • The student will be able to adapt to evolving security standards and proactively seek updates in the field of OT cybersecurity.

8. Course Objectives

8.1 General objective of the course	• To provide students with fundamental and applied knowledge about cybersecurity in industrial environments, equipping them with skills to identify, evaluate, and mitigate cybersecurity risks in OT systems.
8.2 Specific objectives	• To introduce students to differences between IT and OT security and their implications in industrial environments.

	• To familiarize students with network typologies and cybersecurity best practices in OT environments, with a focus on DeltaV and other industrial platforms. • To develop practical skills in implementing endpoint protection, application whitelisting, and patch management for industrial control systems. • To enable students to understand and apply data protection and resilience strategies. • To guide students in conducting cybersecurity assessments, gap analyses, and incident response for OT systems. • To expose students to current European cybersecurity regulations and understand their implications for industrial environments.

9. Contents

9.1 Lectures	No. of hours	Teaching methods	Obs.
1. Introduction to OT Cybersecurity	2	Blackboard illustrations and explanations, beamer presentations, discussions, short challenges	
2. IT vs. OT	2		
3. Network Typology and best practices (DeltaV Cybersecurity Manual)	2		
4. Data Protection and Data Resilience	2		
5. DeltaV Cybersecurity Administration: Endpoint Protection, Application Whitelisting, System Patching	6		
6. Advanced OT Cybersecurity Solutions: Secured Remote Access, SIEM Solution (Security Information and Event Management), Threat Monitoring Solutions and Hardening	6		
7. European Cybersecurity Directives and Regulations: NIS2 and CRA (Cyber Resilience Act)	2		
8. Cybersecurity Assessments: Basic Cybersecurity Assessment, Cyber Security Management System, Gap Analysis	2		
9. Cyber Threats: Risks and case studies of cyber-attacks	2		
10. Incident Response in OT Cybersecurity	2		

Bibliography

1. DeltaV Cybersecurity Manual
2. Security Information and Event Management
3. Cyber Resilience Act, https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act
4. Gheorghe-Romeo Andreica, Iustin-Alexandru Ivanciu, Daniel Zincă, Virgil Dobrotă, Integration of the Suricata Intrusion Detection System and of the Wazuh Security Information and event management for real-time denial-of-service and data tampering detection and alerting, Acta Technica Napocensis, U.T.Press ISSN 1221-6542, vol. 64(2024)
5. Eric Cole, Ronald Krutz, James W. Conley, Network security bible, Wiley Publishing (29), 2009
6. Andrei Luţas, Bogdan Sîrb, Adrian Coleşa, VMI-based protection and control of a Linux VM running security-sensitive applications, Mediamira, 2018

9.2 Seminar / laboratory / project	Hours HEI	Hours CO	Teaching methods	Obs.
1. OT Cybersecurity & IT vs. OT Differences		4		
2. Network Typology and DeltaV Best Practices		4		
3. Data Protection, Resilience & Endpoint Protection		4		
4. Application Whitelisting and System Patching		4		
5. Secured Remote Access & SIEM Integration		4		
6. Threat Monitoring & European Cybersecurity Directives (NIS2, CRA)		4		

7. Cybersecurity Assessments, Gap Analysis & Incident Response Simulation		4		

Bibliography

1. DeltaV Cybersecurity Manual
2. Security Information and Event Management
3. Cyber Resilience Act, https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act
4. Gheorghe-Romeo Andreica, Iustin-Alexandru Ivanciu, Daniel Zincă, Virgil Dobrotă, Integration of the Suricata Intrusion Detection System and of the Wazuh Security Information and event management for real-time denial-of-service and data tampering detection and alerting, Acta Technica Napocensis, U.T.Press ISSN 1221-6542, vol. 64(2024)
5. Eric Cole, Ronald Krutz, James W. Conley, Network security bible, Wiley Publishing (29), 2009
6. Andrei Luţas, Bogdan Sîrb, Adrian Coleşa, VMI-based protection and control of a Linux VM running security-sensitive applications, Mediamira, 2018

10. Correlation of course content with the expectations of the epistemic community representatives, professional associations, and major employers in the field related to the program

The course content is designed to align with current industry standards and best practices as recommended by professional organizations and employers in the field of industrial automation and cybersecurity.

11. Evaluation

Activity Type	Evaluation criteria	Evaluation methods	Weight in final grade
11.1 Lecture	Understanding and applying cybersecurity concepts; clarity of explanations	Written exam, including online quiz tests (e.g. on Moodle platform)	50%
11.2 Seminar/ Laboratory/Project	Practical execution skills; implementation of cybersecurity solutions; troubleshooting and debugging; adherence to procedures	Continuous in-lab evaluation + final report	50%

11.3 Minimum Performance Standard

- Final exam >=5
- Lab grade>=5 mandatory to be able to take the final exam

50% Final exam + 50% Lab Grade > 5

Date of completion: 15.09.2025	Lecturers		Signature
	Course	Conf.Dr.Ing. Adrian Colesa	

Date of approval by the Department of Automation Council 24.11.2025	Director of the Department of Automation Prof.dr.ing. Honoriu VĂLEAN
Date of approval by the Faculty of Automation and Computer Science Council 28.11.2025	Dean Prof.dr.ing. Vlad MUREȘAN