COURSE DESCRIPTION CARD - SYLLABUS

Course name
Security of industrial automation systems [N1Eltech2>PO10-BPSA]

Course

Field of study
Electrical Engineering

Year/Semester
5/9

Area of study (specialization)
–

Profile of study
general academic

Level of study
first-cycle

Course offered in
Polish

Form of study
part-time

Requirements
elective

Number of hours

Lecture
10

Laboratory classes
10

Other
0

Tutorials
0

Projects/seminars
0

Number of credit points

2,00

Coordinators

dr inż. Michał Weissenberg
michal.weissenberg@put.poznan.pl

prof. dr hab. inż. Mariusz Głąbowski
mariusz.glabowski@put.poznan.pl

Lecturers

Prerequisites

The student starting this course should have basic knowledge of ICT networks, understand the communication process between network devices, and possess basic skills in configuring network devices. Basic programming skills are also required. The student should be able to independently obtain information from technical documentation and indicated sources.

Course objective

1. To provide students with theoretical foundations of industrial automation systems and Industrial Internet of Things (IIoT) architectures. 2. To introduce security requirements for industrial automation systems across different network layers. 3. To familiarize students with methods for identifying vulnerabilities and threats in industrial and IIoT environments. 4. To present principles of designing, implementing, and maintaining secure industrial automation systems. 5. To develop practical skills in analyzing and securing IIoT infrastructure in laboratory environments.

Course-related learning outcomes

Knowledge:
The student has in-depth knowledge of industrial automation systems and IIoT architectures,
The student understands threats and vulnerabilities specific to industrial and IIoT infrastructures,
The student knows methods and mechanisms used to secure industrial automation and IIoT systems,
The student is familiar with current standards, regulations, and best practices in industrial cybersecurity,
The student possesses English terminology used in the field of industrial automation and IIoT security.

Skills:
The student can analyze industrial automation architectures from a security perspective,
The student can identify vulnerabilities in IIoT and industrial networks,
The student can configure basic security mechanisms in industrial and IIoT systems,
The student can work effectively in a team during laboratory exercises,
The student can independently expand knowledge in the area of industrial cybersecurity.

Social competences:
The student understands the responsibility associated with designing and maintaining secure industrial systems,
The student recognizes the need for continuous professional development in industrial cybersecurity,
The student is prepared to work responsibly in engineering teams.

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

Lectures: written examination verifying theoretical knowledge (pass mark: 50%; no auxiliary materials allowed).
Laboratories: continuous assessment based on task completion, laboratory reports, and practical tests verifying skills in configuring secure IIoT systems.

Programme content

The course covers issues related to the security of industrial automation systems and Industrial Internet of Things architectures. It includes models and architectures of industrial systems, communication protocols, security requirements, vulnerability and threat identification, and risk management. The course also addresses principles of designing and implementing security mechanisms, monitoring industrial systems, and applying standards, regulations, and commercial solutions for securing industrial automation and IIoT infrastructures.

Course topics

Lecture:
1. Fundamentals of industrial automation and IIoT security.
2. Architectures of industrial automation systems and IIoT.
3. Communication protocols in industrial and IIoT systems.
4. Security requirements and threat models.
5. Vulnerabilities in industrial automation and IIoT systems.
6. Risk management in industrial systems.
7. Security mechanisms for IIoT networks.
8. Advanced security features.
9. VPN technologies in industrial networks.
10. Standards, regulations, and best practices in industrial cybersecurity.
11. Overview of commercial security solutions for industrial automation systems.

Laboratory:
1. Introduction to the laboratory environment.
2. Overview of physical devices and simulation tools.
3. Analysis of IIoT and industrial network architectures.
4. Identification of security requirements.
5. Analysis of Layer 2 and Layer 3 network traffic.
6. Vulnerability detection in industrial and IIoT systems.
7. Configuration of security mechanisms.
8. Testing commercial security solutions.

9. Lifecycle management of IIoT systems from a security perspective.

Teaching methods

1. Lecture: multimedia presentation illustrated with examples.
2. Laboratory exercises: teamwork, practical tasks, configuration of devices, and use of simulation environments.

Bibliography

Basic:
1. Big Data and the Internet of Things : enterprise information architecture for a new age. Autor: Stackowiak, Robert., Licht, Art., Mantha, Venu., Nagode, Louis., Apress Media, 2015.
2. Internet of Things: global technological and societal trends. Autor: Vermesan, Ovidiu., Friess, Peter., River Publishers. River Publishers, 2011.
3. Sikorski M., Roman A. M., Internet rzeczy, PWN 2020.
4. "Cybersecurity Essentials" by Charles J. Brooks, Christopher Grow, Philip A. Craig, Jr., and Donald Short. Published by John Wiley & Sons in 2018. ISBN: 978-1-119-36239-5.
5. "Network Security Essentials: Applications and Standards" by William Stallings. Published by Pearson in 2017. ISBN: 978-0-134-52733-8.

Additional:
1. Curriculum available on the cisco.netacad.net platform as part of the Cisco Network Academy run at the Institute of Communication and Computer Networks.
2. Erik Brynjolfsson, The second machine age: work, progress and prosperity in a time of brilliant technologies; W. W. Norton & Company, 2016.
3. Gaston C. Hillar, Internet of Things with Python Paperback, Packt Publishing, 2016.

Breakdown of average student's workload

	Hours	ECTS
Total workload	55	2,00
Classes requiring direct contact with the teacher	20	0,50
Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation)	35	1,50