COURSE DESCRIPTION CARD - SYLLABUS

Course name
Security of Industrial IoT

Course

Field of study
Computing

Year/semester
1/2

Area of study (specialization)
Cybersecurity

Profile of study
general academic

Level of study
Second-cycle studies

Course offered in
English

Form of study
full-time

Requirements
elective

Number of hours

Lecture	Laboratory classes	Other (e.g. online)
15	15	
Tutorials	Projects/seminars	

Number of credit points

2

Lecturers

Responsible for the course/lecturer:
dr inż. Maciej Sobieraj

maciej.sobieraj@put.poznan.pl

tel: 61 665 3909

Faculty of Computing and Telecommunications
ul. Polanka 3, 60-965 Poznań

Responsible for the course/lecturer:
mgr inż. Michał Weissenberg

email: michal.weissenberg@put.poznan.pl

tel: 61 665 3946

Faculty of Computing and Telecommunications
ul. Polanka 3, 60-965 Poznań

Prerequisites

The student starting this course should have basic knowledge of cybersecurity and IoT. Moreover, the student should have basic knowledge about ICT networks, basic skills in configuring network devices and understands the communication process between network devices. Student should also have basic programming skills. The student should also have the ability to obtain information from the indicated sources.

The student should demonstrate such qualities as honesty, responsibility, perseverance, cognitive curiosity, creativity, personal culture, respect for other people, and ready to work in a group.

Course objective

1. Provide students with a theoretical foundation about Industrial IoT architecture, components, and applications.

2. Provide students with a theoretical and practical about layered security requirements from the network edge to the core and access to the applications layer.

3. Familiarizing the student with standards and regulations regarding audit requirements as well as protocols, applications, and IPv6 for IIoT.

4. Presentation of issues allowing to identify vulnerabilities and threats in IIoT.

5. Presentation of best practices in the design principles and process of securing and segmenting IIoT networks.

Course-related learning outcomes

Knowledge

A student has advanced and in-depth knowledge of widely understood methods of creating IIoT networks, theoretical foundations of their construction, and using tools to manage them.

A student knows development trends and the most important cutting edge achievements in ICT networks, and above all in the area of secure the critical infrastructure and IIoT networks.

A student knows advanced methods, techniques, and tools used to solve complex problems in secure the IoT networks and know-how to use protocols and features to ensure system security on the network devices and IIoT devices.

A student has an extensive vocabulary in English in the field of the terminology used in topics related to the Industrial Internet of Things.

Skills

A student is able to educate himself, gaining the knowledge necessary to understand and solve problems occurring in the Industrial Internet of Things security.

A student can work in a group, actively participating in the planning of the course and the implementation of laboratory classes related to the security of the Industrial Internet of Things.

A student is able to assess the suitability and the possibility of using new achievements (protocols and tools) at IIoT devices and network devices to secure the Industrial Internet of Things system.

A student is able to detect vulnerabilities in IIoT networks and eliminate them.

Social competences

A student is aware of a progress and the resulting need for continuous training in the field of the security of the Industrial Internet of Things.

A student is aware of the responsibility for joint work in teams implementing ICT projects.

A student is aware of the responsibility for the results of his work, which has a direct impact on the safety of people and devices that make up the Industrial Internet of Things.

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

Lectures: knowledge is verified by a written and/or oral test. The pass mark is 51% of the points, and it is not allowed to use any auxiliary materials during the test.

Laboratories: knowledge and skills are verified based on the assessment of the current progress in the implementation of tasks; checking the assumed learning outcomes is carried out by evaluating. Written reports on individual laboratory topics and practical tests of the skills to configure secure IIoT systems.

Programme content

Lecture:

1. Introduction - concepts, definitions, history, architectures, and frameworks of Industrial IoT networks.

2. Security requirements - introduction to Industrial IoT network security requirements.

3. Protocols - the most important information about protocols used in Industrial IoT networks.

4. Vulnerabilities - analyzing vulnerabilities and exploiting them in IIoT networks.

5. Securing - presentation and implementation of the process of securing IIoT networks.

6. Securing - presentation and implementation of the advanced security features used to secure IIoT networks.

7. VPN - describing and implementation of the VPN Solutions in IIoT networks.

8. Commercial solutions - presentation of commercial solutions within the IIoT network security.

Laboratory:

1. Introduction

2. Overview of the simulation environment and physical devices

3. Understand the components of Industrial IoT networks and identify their security requirements

4. Analysis of layer 2 and layer 3 network traffic in an Industrial IoT network

5. Resource analysis and vulnerability detection in IIoT network

6. Learning about commercial network infrastructure security solutions in IIoT network

7. IIoT lifecycle management

Teaching methods

1. Lecture: multimedia presentation illustrated with examples.

2. Laboratory exercises: carrying out the tasks given by the teacher - practical exercises, teamwork, the use of network devices, and simulation environments.

Bibliography

Basic

Literature from recognized scientific journals, standardization documents, websites of device manufacturers posted by the teacher on the eKursy platform.

Courses and materials prepared by equipment manufacturers.

Additional

Breakdown of average student's workload

	Hours	ECTS
Total workload	50	2,0
Classes requiring direct contact with the teacher	30	1,5
Student's own work (literature studies, preparation for laboratory classes, preparation for practical test on laboratory and to exam) [1]	20	0,5

[1] delete or add other activities as appropriate