SYLLABUS

Name: ***IoT Networks (InfAAu-IOT>SM1IOTN19)***
Name in Polish:
Name in English: ***IoT Networks***

Information on course:

Course offered by department: Faculty of Automatic Control, Electronics and Computer Science
Course for department: Silesian University of Technology

Default type of course examination report:

ZAL

Language:

English

Course homepage:

https://platforma2.polsl.pl/rau2/course/view.php?id=999

Short description:

The objective of the course is to deliver to the students the latest and up-to-date knowledge on advanced networking and communication technologies within the Internet of Things world, covering low and high-level protocols. That includes theoretical and practical approaches.

Description:

Lectures
• detailed program content:
Network protocols used in Internet of Things systems: WiFi, Bluetooth, Bluetooth Low Energy, 6LOWPAN, LoRa, MQTT, CoAP
• teaching methods used, including distance learning methods and techniques:
Lecture supported by a multimedia presentation. Film materials available on the remote education platform.

Lectures are not compulsory.

Laboratory:
A number of laboratory scenarios will be given to students to solve real-life networking problems. We mostly use remote labs (https://iot.aeu.polsl.pl)

The laboratory is implemented on real devices of the Internet of Things. Laboratory instructions are available on the remote education platform.

ECTS: 2
Total: 60h (contact hours 30h / self study 30h)
Lecture 15h
Labs 15h
Self study: self-paced learning via PZE, report writing, literature and documentation study

Bibliography:

[1] Sell, Raivo, Rim Puks, Mallor Kingsepp, Agris Nikitenko, Karlis Berkolds, Anete Vagale, Rudolfs Rumba, et al. 2025. Introduction to the IoT (Internet of Things). Coursebook. Riga: RTU Press. https://iot-open.eu/introduction-to-the-iot-coursebook-2nd-edition/.
[2] “ITU Internet Reports 2005: The Internet of Things.” http://www.itu.int/osg/spu/publications/internetofthings/
[3] “Special Report: The Internet of Things”, in “the institute”, IEEE 2014, http://theinstitute.ieee.org/static/special-report-the-internet-of-things
[4] “Towards a definition of the Internet of Things (IoT)”, IEEE 2015
[5] Standard for an Architectural Framework for the Internet of Things (IoT) http://grouper.ieee.org/groups/2413/
[6] Ovidiu Vermesan, Peter Friess (eds.): Digitizing the Industry, Internet of Things Connecting the Physical, Digital and Virtual Worlds, River Publishers Series in Communications, 2016
[7] Vision and Challenges for Realising the Internet of Things, CERP-IoT 2010, http://www.internet-of-things-research.eu/pdf/IoT_Clusterbook_March_2010.pdf
[8] Salim Elbouanani, My Ahmed El Kiram, Omar Achbarou: “Introduction To The Internet Of Things Security. Standardization and research challenges”, 2015 11th International Conference on Information Assurance and Security (IAS), IEEE 2015
[9] On-line study module IOTOPENEU E4: IoT Communication and Networking, https://multiasm.eu/mooc/course/view.php?id=4
[10] IOTOPENEU M2: IoT Architectures, inc. Networks, https://multiasm.eu/mooc/course/view.php?id=7

Learning outcomes:

The student understands the theoretical foundations of security in IoT systems, including authentication, encryption, and access control mechanisms, and can explain how they relate to general principles of computer security. K2A_W03 (exam, labwork grade/report grade)

The student has in-depth knowledge of IoT-specific security threats (e.g. device spoofing, firmware attacks, side-channel attacks) and is familiar with advanced protection mechanisms tailored for resource-constrained IoT devices and networks. K2A_W06 (exam, labwork grade/report grade)

The student knows the architecture of typical IoT networks (e.g. LoRaWAN, Zigbee, NB-IoT) and is able to select and apply appropriate data transmission technologies and communication protocols depending on the requirements of a given IoT application. K2A_W14 (laboratory report, self evaluation on-line quiz)

The student is able to design and carry out experiments using IoT devices and tools for analyzing and simulating IoT networks, interpret the obtained results (e.g. latency, range, packet loss), and formulate conclusions regarding the efficiency of network solutions. K2A_U07 (laboratory report)

The student effectively collaborates in a project team while carrying out tasks related to the design, testing, and analysis of IoT network operation, and is also capable of taking on the role of team leader, coordinating the work across various project stages. K2A_U15 (laboratory report)

Assessment methods and assessment criteria:

Passing the quizzes on the IOTOPENEU E4 and IOTOPENEU M modules (online) is mandatory. Lectures are not compulsory.

The credit is obtained on the basis of graded reports from each of the laboratory exercises. Attendance at laboratory classes is compulsory.
The obtained grade is the arithmetic mean of the grades obtained from all laboratory reports. The student's activity during classes may influence the grade.

Final grade is a weighted average of the laboratory work (LAB) and on-line-based Quizzes (Q), evaluating theory:

final grade = 0.7*LAB + 0.3*Q

where LAB is calculated as an average of all laboratory exercises given to the student to implement.

Laboratory work is evaluated based on the performance of the student during the labs and based on the report provided.

The syllabus is valid from academic year 2025/2026 and its content cannot be changed during the semester.

Course credits in various terms:

Informatics, full-time master degree studies 3 sem. (InfAAu-SM3)			
Type of credits	Number	First term	Last term
European Credit Transfer System (ECTS)	2	2020/2021-Z	