COURSE DESCRIPTION CARD - SYLLABUS

Course name
Cybersecurity in vehicles [S2Elmob1>CwP]

Course

Field of study
Electromobility

Year/Semester
2/3

Area of study (specialization)
Alternative Fuels and Energy Storage

Profile of study
general academic

Level of study
second-cycle

Course offered in
Polish

Form of study
full-time

Requirements
compulsory

Number of hours

Lecture
15

Laboratory classes
0

Other
0

Tutorials
0

Projects/seminars
0

Number of credit points

1,00

Coordinators

dr inż. Anna Grocholewska-Czuryło
anna.grocholewska-czurylo@put.poznan.pl

Lecturers

Prerequisites

The student has structured and theoretically founded knowledge of advanced vehicle data communication systems, computer aided design of electronic circuits and methods of data collection and analysis and visualisation of results. The student has a structued and theoretically grounded knowledge of the fundamentals of data communications, protocols and services in telecomunicationsnetworks. The student is able to obtain information from literature, databases and other sources; is able to integrate the obtained information, interpret it, as well as draw conclusions and formulate and justify opinions. The student is able to work individually and cooperate in a team. The student is aware of the importance and understands the non-technical aspects and effects of the activity of an IT engineer and the related responsibility for the decisions made. He should also understand the need to expand his competences. In addition, in terms of social competences, the student must present attitudes such as honesty, responsibility, perseverance, cognitive curiosity, creativity, personal culture, respect for other people.

Course objective

As part of the course, students learn about the issues of ICT security management in a company or institution, i.e., based on norms and standards, methods of risk analysis and appropriate selection of security (minimizing the probability and / or effects of threats), methods of responding to incidents and restoring the system information technology to the state before the incident.

Course-related learning outcomes

Knowledge:
Student has a basic knowledge of data protection, information systems secuity, risk analysis and threat modelling in vehicle information systems.

Skills:
Student is able, when formulating and solving engineering tasks, to take into account unpredictable conditions, the given technical specyfication and non-technical criteria ensuring the saving of raw materials and energy and the security of IT vehicle systems.

Social competences:
Student understands that in the technical field knowledge and skills devolve rapidly, requiring constant updating.
He/she is aware of the importance of the latest scientific and technical developments in solving research and practical problems and of the need to be supported by expert opinions when necessary.

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

lecture - the knowledge acquired during the lectures is verified during the final test. The test passing threshold is 50%. The correctness of the answers and the student's understanding of the problem are assessed.

Programme content

The program includes the following issues:
1. Introduction to Information Security
2. Risk Management. Legal and Regulatory Requirements.
3. Risk Assessment Methods
4. Threats and Threat Modeling
5. Operational Security Management of Systems

Course topics

The lecture program covers the following issues:
-Basic concepts: threat, vulnerability, risk, security breach, authentication vs. authorization.
-Basic principles of Security (including the principle of least privilege, the principle of security continuity, principles of the proper selection of cryptographic measures, principles of password usage). System functionality and level of security.
-Basic stages of the Security Process (prevention, detection, response, testing).
-Threat Modelling
-Risk Analysis and Management (risk model, process stages, quantitative and qualitativerisk analysis methods, risk mitigation methods, factors determining acceptable residual risk).
-System documentation (elements of documentation, legal requirements)
-Organizational Structure of the company and hierarchy of entities responsible for data security. Responsibilities of individuals and entities related to security management
-Economic aspects of security in IT systems (financial consequences of security breaches, cost of security)
-IT tools supporting security management processes, including the use of artificial intelligence in data protection.
-Certification of information systems (including ISO 15408). Security evaluation criteria.

Teaching methods

Lecture: lecture conducted in an interactive way with the formulation of questions to a group of students or to specific students indicated, the activity of students during classes is considered when giving the final grade, initiating a discussion during the lecture.

Bibliography

Basic:
1. Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie, Białas A. WNT, Warszawa 2017.
2. Risk Management Framework for Information Systems and Organizations A System Life Cycle Approach for Security and Privacy, NIST 800-37 rev.2, 2018

Additional:
1. ISO standards (13335, 2700x).

Breakdown of average student's workload

	Hours	ECTS
Total workload	30	1,00
Classes requiring direct contact with the teacher	17	0,50
Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation)	13	0,50