GDAŃSK UNIVERSITY OF TECHNOLOGY

Subject card

| | | | |
|---|---|---|---|
| Subject name and code | , PG_00070257 | | |
| Field of study | INTELIGENTNE SIECI ENERGETYCZNE (Smart Grid) | | |
| Date of commencement of studies | February 2025 | Academic year of realisation of subject | 2025/2026 |
| Education level | second-cycle studies | Subject group | |
| Mode of study | Full-time studies | Mode of delivery | at the university |
| Year of study | 2 | Language of instruction | Polish<br>No comments. |
| Semester of study | 3 | ECTS credits | 3.0 |
| Learning profile | general academic profile | Assessment form | assessment |
| Conducting unit | Department of Control Engineering -> Faculty of Electrical and Control Engineering -> Faculties of Gdańsk University of Technology | | |
| Name and surname of lecturer (lecturers) | Subject supervisor | dr hab. inż. Marcin Śliwiński | |
| | Teachers | | |

**Lesson types**

| Lesson type | Lecture | Tutorial | Laboratory | Project | Seminar | SUM |
|---|---|---|---|---|---|---|
| Number of study hours | 15.0 | 0.0 | 30.0 | 0.0 | 0.0 | 45 |

E-learning hours included: 0.0

**Learning activity and number of study hours**

| Learning activity | Participation in didactic classes included in study plan | Participation in consultation hours | Self-study | SUM |
|---|---|---|---|---|
| Number of study hours | 45 | 5.0 | 25.0 | 75 |

**Subject objectives**

The aim of the course is to provide a comprehensive overview of smart grid management issues, with particular emphasis on the role of telecommunications components and services. In terms of learning objectives, the course aims to provide students with practical skills and experience in managing modern power grids, in particular knowledge in the areas of telecommunications and cyber security, especially in solving communication problems in an environment of real technical threats.

## Learning outcomes

| Course outcome | Subject outcome | Method of verification |
|---|---|---|
| [K7_W03] has an extended and deepened knowledge of the field related to electrical power systems and electrical equipment | The student has advanced knowledge in the field of operation of intelligent electrical power devices (disconnectors, reclosers, network parameter analysers, cable connectors, automation and control devices for MV and LV) and operation of SCADA systems and telemetry data management. They have in-depth knowledge of troubleshooting problems related to interference, overloads and loss of communication in telecommunications systems and the configuration of telecommunications terminal equipment. | [SW1] Ocena wiedzy faktograficznej<br>[SW3] Ocena wiedzy zawartej w opracowaniu tekstowym i projektowym |
| [K7_K02] is aware of the impact of engineering activities on the environment, understands the the non-technical effects of those activities | The student understands the key aspects of network configuration and operation of private LTE/5G telecommunications networks, with particular emphasis on factors affecting the effective use of telecommunications services. They are aware of the impact of potential threats in terms of responding to cybersecurity incidents and deliberate attacks on telecommunications services, as well as making operational decisions in the event of a mass failure. | [SK1] Ocena umiejętności pracy w grupie<br>[SK5] Ocena umiejętności rozwiązywania problemów występujących w praktyce |
| [K7_U08] e able to carry out tests on electrical power equipment, analyse disturbances in electrical power systems, record and assess the quality of electricity in the power network | The student has the skills and knows the methods and tools for assessing the functioning of Smart Grid systems in various operating conditions: from ideal conditions, through emergency situations, to deliberate sabotage targeting telecommunications and power infrastructure. | [SU1] Ocena realizacji zadania<br>[SU4] Ocena umiejętności korzystania z metod i narzędzi<br>[SU5] Ocena umiejętności zaprezentowania wyników realizacji zadania |

## Subject contents

Course content – lecture

The lecture will comprehensively present issues related to the management of smart grids, with particular emphasis on the role of telecommunications components and services. In the context of educational objectives, the lecture will enable students to acquire practical skills and experience in the management of modern power grids, in particular knowledge in the areas of telecommunications and cyber security, especially in the field of solving communication problems in an environment of real technical threats. The problems of modern electricity metering based on smart electricity meters will be presented (bidirectional energy flow measurements on the high-voltage and low-voltage sides, energy measurements from renewable sources).

Course content – laboratory

The following scenarios will be simulated in the laboratory:

Reference Scenario (ideal conditions). A scenario presenting the operation of the Smart Grid system in ideal conditions, in which the SCADA system, communication modules and telecommunications services function correctly and without any disruptions.

Mass Failure Scenario (Blackout). This scenario aims to realistically reflect the technical difficulties that arise when managing a Smart Grid network in the event of a widespread system failure (Blackout). A power failure results in the loss or serious disruption of common telecommunications services.

Sabotage Scenario (deliberate communication disruptions, selected cybersecurity threats)

The aim of this scenario is to familiarise students with the problems resulting from deliberate, malicious actions leading to the denial of telecommunications services in a Smart Grid environment. This scenario includes elements such as:

- deliberate disruption of radio communication systems (LTE/5G)
- deliberate overloading of communication channels (DoS attacks)
- local denial of access to services caused by the illegal use of radio signal repeaters
- interference with satellite navigation systems (GNSS) that are essential for time synchronisation in LTE/5G base stations

This scenario allows for the simulation of attacks and the assessment of the impact of such actions on the security and continuity of Smart Grid systems.The laboratory will present the problems of remote energy measurement.

<table>
<tr><td>Prerequisites and co-requisites</td><td colspan="3">Student has basic knowledge of the construction of telecommunications networks, electrical circuits, automation and electrical engineering.</td></tr>
<tr><td>Assessment methods and criteria</td><td colspan="3"><table><tr><th>Subject passing criteria</th><th>Passing threshold</th><th>Percentage of the final grade</th></tr><tr><td></td><td>60.0%</td><td>50.0%</td></tr><tr><td></td><td>60.0%</td><td>50.0%</td></tr></table></td></tr>
<tr><td rowspan="3">Recommended reading</td><td>Basic literature</td><td colspan="2">• Billewicz K.: Smart power grids selected aspects, 2016.<br>• Energy law. Regulation on the principles of operation of the metering system, 2024.<br>• IT systems in the energy sector SIWE conference materials PTPIRE.<br>• IEC 62443.: Security for industrial automation and control systems.<br>• European Directive 2014/32/EU Measuring Instruments Directive (MID).<br>• NIS/NIS2 Directive on cybersecurity.</td></tr>
<tr><td>Supplementary literature</td><td colspan="2">• Hoyland A., Rausand M.: System Reliability Theory. Models andStatistical Methods. New York: John Wiley & Sons, Inc. 2015<br>• MIL-HDBK-217F. Reliability Prediction of Electronic Equipment.Washington, DC: U.S. Department of Defence.<br>• MIL-STD-1629A. Procedures for performing a failure mode, effectsand criticality analysis. Washington, DC: U.S. Department of Defence.</td></tr>
<tr><td>eResources addresses</td><td colspan="2"></td></tr>
<tr><td>Example issues/ example questions/ tasks being completed</td><td colspan="3">What defence mechanisms against cyber attacks on critical infrastructure do you know?<br><br>What bidirectional energy measurement systems do you know?<br><br>How do we calculate energy losses in the power grid?<br><br>How do we filter out excess alarm signals in the SCADA system?</td></tr>
<tr><td>Practical activites within the subject</td><td colspan="3">Not applicable</td></tr>
</table>

Document generated electronically. Does not require a seal or signature.