



Karta przedmiotu

Nazwa i kod przedmiotu	INTELIGENTNE SIECI ENERGETYCZNE (Smart Grid), PG_00070257						
Kierunek studiów	Elektrotechnika, Energetyka, Automatyka, robotyka i systemy sterowania, Energetyka, Energetyka						
Data rozpoczęcia studiów	luty 2025 r.		Rok akademicki realizacji przedmiotu		2025/2026		
Poziom kształcenia	II stopnia		Grupa zajęć				
Forma studiów	stacjonarne		Sposób realizacji		na uczelni		
Rok studiów	2		Język wykładowy		polski Brak.		
Semestr studiów	3		Liczba punktów ECTS		3.0		
Profil kształcenia	ogólnoakademicki		Forma zaliczenia		zaliczenie		
Jednostka prowadząca	Wydziały Politechniki Gdańskiej -> Wydział Elektrotechniki i Automatyki -> Katedra Automatyki						
Imię i nazwisko wykładowcy (wykładowców)	Odpowiedzialny za przedmiot		dr hab. inż. Marcin Śliwiński				
	Prowadzący zajęcia z przedmiotu						
Formy zajęć	Forma zajęć	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium	RAZEM
	Liczba godzin zajęć	15.0	0.0	30.0	0.0	0.0	45
	W tym liczba godzin zajęć na odległość: 0.0						
Aktywność studenta i liczba godzin pracy	Aktywność studenta	Udział w zajęciach dydaktycznych, objętych planem studiów		Udział w konsultacjach		Praca własna studenta	RAZEM
	Liczba godzin pracy studenta	45		5.0		25.0	75
Cel przedmiotu	Celem przedmiotu jest kompleksowe przedstawienie zagadnień zarządzania inteligentnymi sieciami energetycznymi (Smart Grid), ze szczególnym uwzględnieniem roli komponentów i usług telekomunikacyjnych. Pomiary energii elektrycznej w celu zarządzania jej przepływami (średniego, wysokiego napięcia, czterokwadrantowe), wraz z charakterystyką przyrządów pomiarowych i otoczenia prawnego. W kontekście celów kształcenia przedmiot ma pozwolić studentom na zdobycie praktycznych umiejętności oraz doświadczenia w zarządzaniu nowoczesnymi sieciami elektroenergetycznymi, w szczególności dotyczy to zdobycia wiedzy w obszarach związanych z telekomunikacją i cyberbezpieczeństwem - szczególnie w zakresie rozwiązywania problemów komunikacyjnych w środowisku rzeczywistych zagrożeń technicznych.						

Efekty uczenia się przedmiotu	Efekt kierunkowy	Efekt z przedmiotu	Sposób weryfikacji i oceny efektu
	[K7_W03] ma rozszerzoną i pogłębioną wiedzę z zakresu związanego z systemami i urządzeniami elektroenergetycznymi	Student posiada zaawansowaną wiedzę z obszaru eksploatacji inteligentnych urządzeń elektroenergetycznych (rozłączniki, reklozery, analizatory parametrów sieciowych, złącza kablowe, urządzenia automatyki oraz kontroli SN i NN) oraz obsługi systemów SCADA i zarządzania danymi telemetrycznymi. Posiada pogłębioną wiedzę w zakresie rozwiązywania problemów związanych z zakłóceniami, przeciążeniami oraz utratą komunikacji w systemach telekomunikacyjnych oraz konfiguracji telekomunikacyjnych urządzeń końcowych.	[SW1] Assessment of factual knowledge [SW3] Assessment of knowledge contained in written work and projects
	[K7_K02] ma świadomość wpływu działalności inżynierskiej na środowisko, rozumie pozatechniczne skutki tej działalności	Student rozumie kluczowe aspekty z konfiguracji sieci i eksploatacji prywatnych sieci telekomunikacyjnych LTE/5G, ze szczególnym uwzględnieniem czynników wpływających na efektywne korzystanie z usług telekomunikacyjnych. Ma świadomość wpływu potencjalnych zagrożeń w zakresie reagowania na incydenty związane z cyberbezpieczeństwem i celowymi atakami na odmowę usług telekomunikacyjnych oraz podejmowania decyzji operacyjnych w warunkach Awarii Masowych.	[SK1] Assessment of group work skills [SK5] Assessment of ability to solve problems that arise in practice
	[K7_U08] potrafi przeprowadzić badania urządzeń elektroenergetycznych, analizować zakłócenia w układach elektroenergetycznych, rejestrować i oceniać jakość energii elektrycznej w sieci elektroenergetycznej	Student ma umiejętność oraz zna metody i narzędzia do oceny funkcjonowania systemów Smart Grid w różnych warunkach pracy: od idealnych, przez sytuacje awaryjne, aż po celowe działania sabotażowe skierowane na infrastrukturę telekomunikacyjną i elektroenergetyczną.	[SU1] Assessment of task fulfilment [SU4] Assessment of ability to use methods and tools [SU5] Assessment of ability to present the results of task

Treści przedmiotu	Treści przedmiotu - wykład Na wykładzie zostaną kompleksowo przedstawione zagadnienia zarządzania inteligentnymi sieciami energetycznymi (Smart Grid), ze szczególnym uwzględnieniem roli komponentów i usług telekomunikacyjnych. W kontekście celów kształcenia wykład ma pozwolić na zdobycie praktycznych umiejętności oraz doświadczenia w zarządzaniu nowoczesnymi sieciami elektroenergetycznymi, w szczególności dotyczy to zdobycia wiedzy w obszarach związanych z telekomunikacją i cyberbezpieczeństwem - szczególnie w zakresie rozwiązywania problemów komunikacyjnych w środowisku rzeczywistych zagrożeń technicznych. Przedstawione zostaną problemy współczesnych pomiarów energii elektrycznej w oparciu o inteligentne liczniki elektrycznej (pomiar dwukierunkowe przepływów energii po stronie wysokiego napięcia, niskiego napięcia, pomiary energii ze źródeł odnawialnych). Treści przedmiotu - laboratoria W ramach laboratorium zasymulowane zostaną scenariusze: Scenariusz Referencyjny (warunki idealne). Scenariusz przedstawiający działanie systemu Smart Grid w warunkach idealnych, w których system SCADA, moduły komunikacyjne oraz usługi telekomunikacyjne funkcjonują poprawnie i bez żadnych zakłóceń. Scenariusz Awarii Masowej (Blackout). Scenariusz ten ma na celu realistyczne odwzorowanie trudności technicznych, jakie pojawiają się podczas zarządzania siecią Smart Grid w przypadku rozległej awarii systemowej (Blackout). Awaria zasilania skutkuje brakiem lub poważnymi zakłóceniami powszechnych usług telekomunikacyjnych. Scenariusz Sabotażu (celowe zakłócenia łączności wybrane zagrożenia cyberbezpieczeństwa) Celem tego scenariusza jest zapoznanie studentów z problemami wynikającymi z celowego, złośliwego działania prowadzącego do odmowy usług telekomunikacyjnych w środowisku Smart Grid. Scenariusz ten obejmuje takie elementy jak: • celowe zakłócanie systemów łączności radiowej (LTE/5G) • celowe przeciążanie kanałów komunikacyjnych (ataki DoS) • lokalna odmowa dostępu do usług spowodowana nielegalnym użyciem repeaterów sygnałów radiowych • zakłócanie systemów nawigacji satelitarnej (GNSS), które są istotne dla synchronizacji czasu w stacjach bazowych LTE/5G Scenariusz ten pozwala na symulację ataków oraz ocenę wpływu takich działań na bezpieczeństwo oraz ciągłość działania systemów Smart Grid. W ramach laboratorium zostaną także przedstawione problemy zdalnego pomiaru energii elektrycznej wraz z wykorzystaniem nowoczesnych układów pomiarowych.		
Wymagania wstępne i dodatkowe	Student ma podstawową wiedzę z budowy sieci teleinformatycznych, obwodów elektrycznych, automatyki i elektrotechniki.		
Sposoby i kryteria oceniania osiągniętych efektów uczenia się	Sposób oceniania (składowe)	Próg zaliczeniowy	Składowa oceny końcowej
	Laboratorium	60.0%	50.0%
	Wykład	60.0%	50.0%
Zalecana lista lektur	Podstawowa lista lektur	• Billewicz K.: Inteligentne sieci elektroenergetyczne - wybrane aspekty, 2016. • Prawo energetyczne. Rozporządzenie w sprawie zasad funkcjonowania systemu pomiarowego, 2024. • Systemy Informatyczne w Energetyce SIWE - materiały konferencyjne PTPIRE. • EC 62443 norma cyberbezpieczeństwa sieci przemysłowych. • Dyrektywa Europejska 2014/32/UE Dyrektywa urządzeń pomiarowych MID. • Dyrektywa NIS/NIS2 z zakresu cyberbezpieczeństwa.	
	Uzupełniająca lista lektur	• Hoyland A., Rausand M.: System Reliability Theory. Models and Statistical Methods. New York: John Wiley & Sons, Inc. 2015 • MIL-HDBK-217F. Reliability Prediction of Electronic Equipment. Washington, DC: U.S. Department of Defence. • MIL-STD-1629A. Procedures for performing a failure mode, effects and criticality analysis. Washington, DC: U.S. Department of Defence.	
	Adresy eZasobów		

Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania	Jakie znasz mechanizmy obrony przed cyberatakami na infrastrukturę krytyczną? Jakie znasz układy pomiaru energii dwukierunkowej? W jaki sposób obliczmy straty energii w sieci energetycznej? W jaki sposób odfiltrować nadmiar sygnałów alarmowych w systemie SCADA?
Zajęcia praktyczne w ramach przedmiotu	Nie dotyczy

Dokument wygenerowany elektronicznie. Nie wymaga pieczęci ani podpisu.