



Karta przedmiotu

Nazwa i kod przedmiotu	SYSTEMY ZABEZPIECZEŃ W PRZEMYŚLE, PG_00059283						
Kierunek studiów	Automatyka, robotyka i systemy sterowania						
Data rozpoczęcia studiów	luty 2026 r.		Rok akademicki realizacji przedmiotu		2026/2027		
Poziom kształcenia	II stopnia		Grupa zajęć				
Forma studiów	stacjonarne		Sposób realizacji		na uczelni		
Rok studiów	1		Język wykładowy		polski		
Semestr studiów	2		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 inż. Jacek Zawalich				
	Prowadzący zajęcia z przedmiotu		dr inż. Jacek Zawalich				
Formy zajęć	Forma zajęć	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium	RAZEM
	Liczba godzin zajęć	30.0	0.0	0.0	15.0	0.0	45
	W tym liczba godzin zajęć na odległość: 0.0						
	Adres kursu na platformie eNauczanie: https://enauczanie.pg.edu.pl/2025/course/view.php?id=914						
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	Zapoznanie studentów z metodami analizy i projektowania systemów zabezpieczeń w przemyśle.						
Efekty uczenia się przedmiotu	Efekt kierunkowy		Efekt z przedmiotu		Sposób weryfikacji i oceny efektu		
	[K7_W09] ma wiedzę z zakresu typowych systemów zabezpieczeń w warunkach przemysłowych, zna metody identyfikacji zagrożeń i projektowania systemów zabezpieczeń zgodnie z metodyką bezpieczeństwa funkcjonalnego, ma wiedzę z zakresu bezpieczeństwa informacji		Student ma wiedzę na temat identyfikacji zagrożeń i definiowania funkcji zabezpieczających do zaimplementowania w przemysłowym systemie sterowania ICS (Industrial Control System) zgodnie z koncepcją bezpieczeństwa funkcjonalnego (IEC 61508) i odpowiednich norm sektorowych z uwzględnieniem aspektów cyberbezpieczeństwa (IEC 62443).		[SW3] Ocena wiedzy zawartej w opracowaniu tekstowym i projektowym [SW1] Ocena wiedzy faktograficznej [SW2] Ocena wiedzy zawartej w prezentacji		
	[K7_U08] ma przygotowanie niezbędne do pracy w środowisku przemysłowym, prowadzenia badań, stosuje zasady bezpieczeństwa i higieny pracy		Student ma umiejętności oraz zna metody i narzędzia do implementacji funkcji bezpieczeństwa w przyrządowych systemach bezpieczeństwa SIS. Potrafi na podstawie analizy probabilistycznej zweryfikować złożoną strukturę systemu automatyki.		[SU2] Ocena umiejętności analizy informacji [SU4] Ocena umiejętności korzystania z metod i narzędzi		

Treści przedmiotu	Treści przedmiotu - wykład Przykładowe systemy zabezpieczeń w różnych sektorach gospodarki. Zaawansowane metody analizy niezawodności i bezpieczeństwa systemów technicznych. Modelowanie probabilistyczne obiektów. Mechanizmy uszkodzeń elementów w systemach zabezpieczających i modele. Analiza rodzajów, skutków i krytyczności uszkodzeń (FMECA) systemów programowalnych. Zaawansowana analiza niezawodnościowa systemów złożonych różnymi metodami: schematów blokowych niezawodności (RDB), drzewa uszkodzeń i błędów (FT), drzew zdarzeń (ET) i grafów Markowa (MG). Optymalizowanie niezawodności. Wymagania normy PN-EN 61508 i jej relacje z normami sektorowymi PN-EN 61511 i PN-EN 62061. Ryzyko indywidualne i społeczne. Identyfikacja zagrożeń, analiza i ocena ryzyka. Cele i koncepcja zarządzania bezpieczeństwem funkcjonalnym w cyklu życia. Treści przedmiotu - projekt Analiza instalacji przemysłowych metodą HAZOP. Definiowanie funkcji związanych z bezpieczeństwem. Definiowanie scenariuszy awaryjnych. Określanie wymaganego poziomu nienaruszalności bezpieczeństwa SIL na podstawie analizy i oceny ryzyka; metoda macierzy ryzyka. Potencjalne błędy systematyczne w systemach E/E/PE i unikanie błędów. Jakość oprogramowania i wymagania w cyklu życia. Ochrona sieci komputerowych. Ograniczenia architektoniczne w podsystemach E/E/PE. Weryfikacja poziomu SIL w warunkach niepewności. Uszkodzenia zależne i ich eliminowanie. Analiza warstw zabezpieczeń LOPA w nawiązaniu do PN-EN 61511. Czynniki ludzkie w analizie bezpieczeństwa funkcjonalnego i warstw zabezpieczeń; analiza funkcjonalna, projektowanie interfejsów i systemu alarmowego. Wymagania dotyczące bezpieczeństwa funkcjonalnego systemów sterowania maszyn według PN-EN 62061. Strategia testowania systemów E/E/PE.		
Wymagania wstępne i dodatkowe	Wiedza dotycząca analizy niezawodności w systemach technicznych, technologii programowalnych i systemów komputerowych w przemyśle i gospodarce.		
Sposoby i kryteria oceniania osiągniętych efektów uczenia się	Sposób oceniania (składowe)	Próg zaliczeniowy	Składowa oceny końcowej
	Kolokwium I	60.0%	50.0%
	Projekt	60.0%	50.0%
Zalecana lista lektur	Podstawowa lista lektur	1. Materiały dydaktyczne dostępne są na stronie internetowej Zespołu Technologii Sieciowych i Inżynierii Bezpieczeństwa. 2. Kosmowski K.T.(red.): Podstawy bezpieczeństwa funkcjonalnego, Wydawnictwo PG. Gdańsk, 2016-2020 (III wyd.). 3. Podstawy komputerowej aplikacji CARE (BQR). 4. Wprowadzenie do oprogramowania Pro-SIL. WEiA PG, 2010.	
	Uzupełniająca lista lektur	1. Hoyland A., Rausand M.: System Reliability Theory. Models and Statistical Methods. New York: John Wiley & Sons, Inc. 1994. 2. MIL-HDBK-217F. Reliability Prediction of Electronic Equipment. Washington, DC: U.S. Department of Defence, 1991. 3. MIL-STD-1629A. Procedures for performing a failure mode, effects and criticality analysis. Washington, DC: U.S. Department of Defence, 1980.	
	Adresy eZasobów		
Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania	Identyfikacja zagrożeń oraz ocena ryzyka ukierunkowana na określanie PL lub SIL funkcji bezpieczeństwa. Projektowanie architektury systemu zabezpieczeń instalacji przemysłowej z uwzględnieniem wymagań bezpieczeństwa funkcjonalnego. Poziom nienaruszalności bezpieczeństwa (SIL) funkcji bezpieczeństwa i kryteria probabilistyczne.		
Zajęcia praktyczne w ramach przedmiotu	Nie dotyczy		

Dokument wygenerowany elektronicznie. Nie wymaga pieczęci ani podpisu.