



Karta przedmiotu

Nazwa i kod przedmiotu	SYSTEMY ZABEZPIECZEŃ W PRZEMYŚLE, PG_00038323						
Kierunek studiów	Automatyka, robotyka i systemy sterowania						
Data rozpoczęcia studiów	październik 2023 r.	Rok akademicki realizacji przedmiotu			2024/2025		
Poziom kształcenia	II stopnia	Grupa zajęć			Grupa zajęć fakultatywnych Grupa zajęć powiązanych z prowadzonymi badaniami naukowymi w dziedzinie nauki związanej z kierunkiem - profil ogólnoakademicki		
Forma studiów	niestacjonarne	Sposób realizacji			na uczelni		
Rok studiów	2	Język wykładowy			polski		
Semestr studiów	3	Liczba punktów ECTS			3.0		
Profil kształcenia	ogólnoakademicki	Forma zaliczenia			zaliczenie		
Jednostka prowadząca	Wydział Elektrotechniki i Automatyki -> Katedra Automatyki						
Imię i nazwisko wykładowcy (wykładowców)	Odpowiedzialny za przedmiot	prof. dr hab. inż. Kazimierz Kosmowski					
	Prowadzący zajęcia z przedmiotu						
Formy zajęć i metody nauczania	Forma zajęć	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium	RAZEM
	Liczba godzin zajęć	10.0	0.0	10.0	0.0	0.0	20
	W tym liczba godzin zajęć na odległość: 0.0						
Adresy na platformie eNauczanie:							
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	20	10.0	45.0	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 [SW2] Ocena wiedzy zawartej w prezentacji [SW1] Ocena wiedzy faktograficznej		
	[K7_U07] potrafi wykorzystać metody analityczne, symulacyjne i eksperymentalne do formułowania i rozwiązywania zadań inżynierskich i prostych problemów badawczych z zakresu automatyki i robotyki	Student zna zasady wyznaczania poziomów: PL (Performance Level) i SIL (Safety Integrity Level) funkcji bezpieczeństwa na podstawie zdefiniowanych matryc ryzyka oraz metody weryfikacji tych poziomów z uwzględnieniem wyników modelowania probabilistycznego systemu sterowania o danej architekturze.			[SU4] Ocena umiejętności korzystania z metod i narzędzi [SU3] Ocena umiejętności wykorzystania wiedzy uzyskanej w ramach przedmiotu [SU2] Ocena umiejętności analizy informacji		
[K7_W13] ma wiedzę o działaniu podstawowych urządzeń systemów sygnalizacji włamania i napadu, zna zasady projektowania prostych układów alarmowych	Student potrafi zaprojektować i zweryfikować funkcję bezpieczeństwa wraz z interfejsem użytkownika na stanowisku laboratoryjnym.			[SW3] Ocena wiedzy zawartej w opracowaniu tekstowym i projektowym [SW1] Ocena wiedzy faktograficznej			

Treści przedmiotu	<p>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. 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 maczyzy 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.</p>		
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
	Laboratory	60.0%	50.0%
	Kolokwium I	60.0%	50.0%
Zalecana lista lektur	Podstawowa lista lektur	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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	<p>Identyfikacja zagrożeń oraz ocena ryzyka ukierunkowana na określanie PL lub SIL funkcji bezpieczeństwa.</p> <p>Projektowanie architektury systemu zabezpieczeń instalacji przemysłowej z uwzględnieniem wymagań bezpieczeństwa funkcjonalnego.</p> <p>Poziom nienaruszalności bezpieczeństwa (SIL) funkcji bezpieczeństwa i kryteria probabilistyczne.</p>		
Praktyki zawodowe w ramach przedmiotu	Nie dotyczy		