



Karta przedmiotu

Nazwa i kod przedmiotu	BEZPIECZEŃSTWO FUNKCJONALNE I OCHRONA INFORMACJI, PG_00062386							
Kierunek studiów	Automatyka, robotyka i systemy sterowania							
Data rozpoczęcia studiów	październik 2022 r.	Rok akademicki realizacji przedmiotu			2024/2025			
Poziom kształcenia	I stopnia - inżynierskie	Grupa zajęć						
Forma studiów	stacjonarne	Sposób realizacji			na uczelni			
Rok studiów	3	Język wykładowy			polski			
Semestr studiów	6	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		dr inż. Emilian Piesik					
	Prowadzący zajęcia z przedmiotu							
Formy zajęć i metody nauczania	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							
Dodatkowe informacje: Wykład, prezentacje i materiały pomocnicze. Projekt, instrukcje.								
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		3.0		27.0	75	
Cel przedmiotu	Przekazanie studentom podstawowej wiedzy inżynierskiej dotyczącej identyfikacji zagrożeń oraz analizy i oceny ryzyka w systemach technicznych przydatnej w projektowaniu systemów sterowania z uwzględnieniem wymagań bezpieczeństwa funkcjonalnego.							
Efekty uczenia się przedmiotu	Efekt kierunkowy		Efekt z przedmiotu			Sposób weryfikacji i oceny efektu		
	[K6_U07] potrafi budować i analizować modele układów i systemów z zakresu związanego z systemami sterowania i automatyką		Student zna podstawy metodyczne identyfikowania zagrożeń związanych z eksploatacją maszyn i linii produkcyjnych oraz instalacji przemysłowych. Posiada wiedzę jak definiować funkcje bezpieczeństwa z uwzględnieniem wyników analizy i oceny ryzyka, aby racjonalnie zmniejszać ryzyko wypadków oraz strat ludzkich, środowiskowych i materialnych. Student zna rozwiązania warstwowego systemu zabezpieczeń oraz wie jak je analizować. Student wie jak dobierać rozwiązania architektury sprzętowej realizujące funkcję bezpieczeństwa.			[SU5] Ocena umiejętności zaprezentowania wyników realizacji zadania [SU3] Ocena umiejętności wykorzystania wiedzy uzyskanej w ramach przedmiotu [SU4] Ocena umiejętności korzystania z metod i narzędzi		
	[K6_W07] ma podstawową wiedzę związaną z systemami sterowania i automatyki		Student wie jak określić wymagany poziom nienaruszalności bezpieczeństwa PLr lub SILr funkcji bezpieczeństwa oraz jak weryfikować te poziomy na podstawie modelu probabilistycznego przemysłowego systemu automatyki i sterowania w projektowaniu. Student zna podstawowe zasady cyberbezpieczeństwa dotyczące powiązanych technologii operacyjnych, informatycznych i chmurowych OT-IT-CT.			[SW1] Ocena wiedzy faktograficznej [SW3] Ocena wiedzy zawartej w opracowaniu tekstowym i projektowym		

Treści przedmiotu	<p>WYKŁAD Definicje ryzyka, ryzyko indywidualne i społeczne. Zasada ALARP, matryca ryzyka i wymagana redukcja ryzyka. Koncepcja bezpieczeństwa funkcjonalnego systemów sterowania i zabezpieczeń. Projektowanie systemów elektrycznych / elektronicznych i programowalnych elektronicznych (E/E/PE). Przykłady rozwiązań bezpieczeństwa funkcjonalnego w przemyśle. Niezawodność i bezpieczeństwo funkcjonalne systemów sterowania maszyn. Klasyfikacja systemów sterowania według norm: PN-EN 954, PN-EN 13849 i PN-EN 62061. Poziomy bezpieczeństwa PL. Analiza zagrożeń i definiowanie funkcji związanych z bezpieczeństwem. Określanie poziomu nienaruszalności bezpieczeństwa SIL na podstawie oceny ryzyka według PN-EN 61508. Pokrycie diagnostyczne DC w podsystemach. Weryfikacja SIL metodami jakościowymi i ilościowymi. Warstwy zabezpieczeniowo-ochronne według PN-EN 61511. Metoda LOPA. Projektowanie przyrządowych funkcji bezpieczeństwa SIS i systemu alarmowego AS. Ochrona informacji w systemach komputerowych. Kryteria oceny ryzyka. Określanie poziomów ochrony informacji. Metody i rozwiązania ochrony informacji w sieci: ochrona dostępu, audyt, ochrona antywirusowa i ściany zaporowe. Ochrona transmisji informacji i baz danych. Przepisy prawne, zalecenia i standardy dotyczące ochrony informacji. Przykłady systemów zabezpieczeń i ochrony informacji w przemyśle. Identyfikacja zagrożeń i ocena czynników ryzyka. Projekt: Określanie wymaganego poziomu bezpieczeństwa PL funkcji bezpieczeństwa realizowanej przez system sterowania maszyny. Realizacja techniczna i weryfikacja PL na przykładach urządzenia zabezpieczenia maszyny i kurtyny świetlnej. Określanie wymaganego SIL funkcji związanych z bezpieczeństwem. Weryfikacja poziomu SIL, projektowanie i wykonanie struktury systemu zabezpieczeń KzN. Sterowniki do zastosowań bezpieczeństwa. Warstwy zabezpieczeń (BPCS, człowiek-operator i system alarmowy, SIS/ESD).</p>											
Wymagania wstępne i dodatkowe	<p>Wiedza dotycząca rachunku prawdopodobieństwa, analizy niezawodności w systemach technicznych oraz zastosowania systemów komputerowych i programowalnych systemów sterowania w przemyśle.</p>											
Sposoby i kryteria oceniania osiągniętych efektów uczenia się	<table border="1" data-bbox="448 620 794 725"> <thead> <tr> <th>Sposób oceniania (składowe)</th> <th>Próg zaliczeniowy</th> <th>Składowa oceny końcowej</th> </tr> </thead> <tbody> <tr> <td>Projekt</td> <td>60.0%</td> <td>50.0%</td> </tr> <tr> <td>Dwa kolokwia - teoria / zadania</td> <td>60.0%</td> <td>50.0%</td> </tr> </tbody> </table>	Sposób oceniania (składowe)	Próg zaliczeniowy	Składowa oceny końcowej	Projekt	60.0%	50.0%	Dwa kolokwia - teoria / zadania	60.0%	50.0%		
Sposób oceniania (składowe)	Próg zaliczeniowy	Składowa oceny końcowej										
Projekt	60.0%	50.0%										
Dwa kolokwia - teoria / zadania	60.0%	50.0%										
Zalecana lista lektur	<p>Podstawowa lista lektur</p>	<ol style="list-style-type: none"> Kosmowski K.T. (red.): Podstawy bezpieczeństwa funkcjonalnego, Wydawnictwo Politechniki Gdańskiej, Gdańsk 2020. Kosmowski K.T. (Ed.): Functional safety management in critical systems, Fundacja Rozwoju Uniwersytetu Gdańskiego Gdańsk 2007. Liderman K.: Analiza ryzyka i ochrona informacji w systemach komputerowych. Wydawnictwo Naukowe PWN SA, Warszawa 2008. 										
	<p>Uzupełniająca lista lektur</p>	<ol style="list-style-type: none"> Andersen R.: Inżynieria zabezpieczeń. WNT, Warszawa 2005. Białas A.: Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie, WNT, Warszawa 2006. 										
	<p>Adresy eZasobów</p>	<p>Adresy na platformie eNauczanie:</p>										
Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania	<ol style="list-style-type: none"> Graf ryzyka do określania wymaganego poziomu nienaruszalności bezpieczeństwa (SIL). Jakościowa weryfikacja SIL systemu E/E/PE. Ilościowa weryfikacja SIL systemu E/E/PE. 											
Praktyki zawodowe w ramach przedmiotu	<p>Nie dotyczy</p>											