



Karta przedmiotu

Nazwa i kod przedmiotu	Bezpieczeństwo systemów, PG_00048278						
Kierunek studiów	Informatyka						
Data rozpoczęcia studiów	luty 2027 r.	Rok akademicki realizacji przedmiotu			2026/2027		
Poziom kształcenia	II stopnia	Grupa zajęć			Grupa zajęć fakultatywnych Grupa zajęć specjalnościowych Grupa zajęć powiązanych z prowadzonymi badaniami naukowymi w dziedzinie nauki związanej z kierunkiem - profil ogólnoakademicki		
Forma studiów	stacjonarne	Sposób realizacji			na uczelni		
Rok studiów	1	Język wykładowy			polski		
Semestr studiów	1	Liczba punktów ECTS			2.0		
Profil kształcenia	ogólnoakademicki	Forma zaliczenia			zaliczenie		
Jednostka prowadząca	Wydziały Politechniki Gdańskiej -> Wydział Elektroniki, Telekomunikacji i Informatyki -> Katedra Inżynierii Oprogramowania						
Imię i nazwisko wykładowcy (wykładowców)	Odpowiedzialny za przedmiot	dr inż. Andrzej Wardziński					
	Prowadzący zajęcia z przedmiotu	dr inż. Andrzej Wardziński					
Formy zajęć	Forma zajęć	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium	RAZEM
	Liczba godzin zajęć	15.0	0.0	0.0	15.0	0.0	30
	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	30		4.0		16.0	50
Cel przedmiotu	Rozwinięcie zrozumienia roli i zakresu wymagań i związanych z nimi gwarancji dotyczących systemów uwarunkowanych bezpieczeństwem Pozyskanie wiedzy na temat podstawowych metod i technik projektowania i analizy takich systemów Praktykowanie technik analizy ryzyka dotyczącego wybranego systemu związanego z bezpieczeństwem						

Efekty uczenia się przedmiotu	Efekt kierunkowy	Efekt z przedmiotu	Sposób weryfikacji i oceny efektu
	[K7_U12] potrafi w pogłębionym stopniu analizować działanie elementów, układów i systemów związanych z kierunkiem studiów oraz mierzyć ich parametry i badać charakterystyki techniczne, a także planować i przeprowadzać eksperymenty związane z kierunkiem studiów, w tym symulacje komputerowe, interpretować uzyskane wyniki i wyciągać wnioski	Student zna mechanizmy występowania awarii w systemach technicznych zawierających oprogramowanie. Student potrafi wykonać analizę bezpieczeństwa systemu technicznego oraz zaplanować prace zapewnienia wymaganego poziomu bezpieczeństwa.	[SU4] Ocena umiejętności korzystania z metod i narzędzi
	[K7_W11] zna i rozumie w pogłębionym stopniu ogólne zasady tworzenia i rozwoju form indywidualnej przedsiębiorczości oraz ekonomiczne, prawne i inne uwarunkowania różnych rodzajów działań związanych z nadaną kwalifikacją, w tym zasady ochrony własności przemysłowej i prawa autorskiego	Student zna podstawy procesu kwalifikacji systemów technicznych pod względem bezpieczeństwa ich zastosowania.	[SW1] Ocena wiedzy faktograficznej
	[K7_W03] zna i rozumie w pogłębionym stopniu budowę i zasady działania komponentów i systemów związanych z kierunkiem studiów, w tym teorii, metody i złożone zależności między nimi oraz wybrane zagadnienia szczegółowe – właściwe dla programu kształcenia	Student zna mechanizmy występowania awarii i wypadków systemów technicznych zawierających oprogramowanie. Student potrafi wykonać analizę bezpieczeństwa systemu technicznego.	[SW3] Ocena wiedzy zawartej w opracowaniu tekstowym i projektowym
[K7_U04] potrafi wykorzystywać posiadaną wiedzę z zakresu metod i technik programowania oraz dobrać i zastosować właściwe metody i narzędzia programistyczne w tworzeniu oprogramowania komputerów albo programowania urządzeń lub sterowników wykorzystujących mikroprocesory albo elementy lub układy programowalne, charakterystycznych dla danego kierunku studiów, dokonując oceny i krytycznej analizy wykonanego oprogramowania, a także syntezy i twórczej interpretacji prezentowanych za jego pomocą informacji	Student zna mechanizmy występowania awarii systemów komputerowych. Student potrafi określić architekturę systemu spełniającą określone wymagania bezpieczeństwa.	[SU1] Ocena realizacji zadania [SU4] Ocena umiejętności korzystania z metod i narzędzi	
Treści przedmiotu	Treści przedmiotu - wykład 1. Systemy związane z bezpieczeństwem - definicje, przykłady 2. Zasady projektowania: różnorodność, zarządzanie hazardami, redukcja ryzyka 3. Studium przypadku rakiety Arian 5 4. Teoria niezawodności; nadmiarowość i jej wpływ na niezawodność i bezpieczeństwo 5. Zasada różnorodności i jej zastosowanie do oprogramowania 6. Wpływ różnorodności na niezawodność i bezpieczeństwo 7. Standard IEC 61508 - definicje i zakres 8. Standard IEC 61508 zasada ALARP 9. Koncepcja poziomów nienaruszalności bezpieczeństwa (SIL) 10. Wymagania IEC61508 względem oprogramowania i procesu wytwórczego 11. Błąd człowieka 12. Dowody zaufania i dowody bezpieczeństwa: cele i zakres 13. Metody analizy ryzyka: Hazard Analysis, HAZOP, ETA 14. Metody analizy ryzyka: FTA, FMEA, FMECA, CCA 15. Metody analizy ryzyka: FMECA, CCA		
Wymagania wstępne i dodatkowe	Nie ma wymagań		
Sposoby i kryteria oceniania osiągniętych efektów uczenia się	Sposób oceniania (składowe)	Próg zaliczeniowy	Składowa ocena końcowej
	Projekt	50.0%	50.0%
	Theoria	50.0%	50.0%
Zalecana lista lektur	Podstawowa lista lektur	J Gorski, High Integrity Systems, Lecture notes,2010 E. Hollnagel, D. D Woods, N. Leveson, Resilience Engineering, Concepts and Precepts, TJ International, 2008 Nancy Leveson, SAFEWARE: System Safety and Computers, published by Addison Wesley, 1994 Peter Neumann, Computer Related Risks, published by ACM Press, New York, 1995 Tom Anderson and Peter Lee, Fault Tolerance: Principles and Practice, published by Springer-Verlag, New York, 1990 Trust-IT Framework, http://kio.eti.pg.gda.pl/trust_case/	
	Uzupełniająca lista lektur	Nie ma wymagań	
	Adresy eZasobów		

Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania	- metody anality hazardów - ocena ryzyka, ALARP - metody ograniczania ryzyka
Zajęcia praktyczne w ramach przedmiotu	Nie dotyczy

Dokument wygenerowany elektronicznie. Nie wymaga pieczęci ani podpisu.