POLITECHNIKA GDAŃSKA

Karta przedmiotu

Nazwa i kod przedmiotu	Bezpieczeństwo systemów, PG_00048278		
Kierunek studiów	Informatyka		
Data rozpoczęcia studiów	luty 2023 r.	Rok akademicki realizacji przedmiotu	2022/2023
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	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	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 dr inż. Katarzyna Łukasiewicz	

Formy zajęć i metody nauczania	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_W03] zna i rozumie w pogłębionym stopniu budowę i zasady działania komponentów i systemów związanych z kierunkiem studiów, w tym teorie, 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_U06] potrafi analizować działanie elementów, układów i systemów związanych z kierunkiem studiów oraz mierzyć ich parametry i badać charakterystyki techniczne, interpretować uzyskane wyniki i wyciągać wnioski	Student potrafi wykonać analizę bezpieczeństwa systemu lub urządzenia	[SU1] Ocena realizacji zadania
[K7_W43] zna i rozumie w pogłębionym stopniu formalne, techniczne i społeczne aspekty działania złożonych systemów informatycznych w społeczeństwie informacyjnym i w globalnej infrastrukturze informacyjnej	Student zna mechanizmy występowania awarii i wypadków systemów technicznych zawierających oprogramowanie. Student potrafi wykonać analizę bezpieczeństwa systemu technicznego.	[SW1] Ocena wiedzy faktograficznej
[K7_W41] zna i rozumie w pogłębionym stopniu standardy, metody wytwarzania, cykl życia i trendy rozwojowe oprogramowania oraz systemów i aplikacji informacyjnych	Student zna podstawowe standardy w zakresie bezpieczeństwa systemów.	[SW1] Ocena wiedzy faktograficznej
[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.	[SU4] Ocena umiejętności korzystania z metod i narzędzi [SU1] Ocena realizacji zadania

Treści przedmiotu

1. Systemy zwiazane 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. Kncepcja poziomów nienaruszalności bezpieczeństwa (SIL) 10. Wymagania IEC61508 wzgledem 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 osiąganych efektów uczenia się

Sposób oceniania (składowe)	Próg zaliczeniowy	Składowa oceny 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 wymagan
Adresy eZasobów	Adresy na platformie eNauczanie:

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