



## KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu

Bezpieczeństwo funkcjonalne

### Przedmiot

Kierunek studiów

Rok/semestr

Informatyka

1/1

Studia w zakresie (specjalność)

Profil studiów

Cyberbezpieczeństwo

ogólnoakademicki

Poziom studiów

Język oferowanego przedmiotu

drugiego stopnia

angielski

Forma studiów

Wymagalność

stacjonarne

obligatoryjny

### Liczba godzin

Wykład

Laboratoria

Inne (np. online)

30

15

Ćwiczenia

Projekty/seminaria

### Liczba punktów ECTS

4

### Wykładowcy

Odpowiedzialny za przedmiot/wykładowca:

Odpowiedzialny za przedmiot/wykładowca:

dr hab. inż. Mariusz Żal

mariusz.zal@put.poznan.pl

tel: 61 665 39 26

Wydział Informatyki i Telekomunikacji

Instytut Sieci Teleinformatycznych

### Wymagania wstępne

Student rozpoczynający ten przedmiot powinien mieć podstawową wiedzę z zakresu sieci komputerowych, systemów operacyjnych Windows i Linux. Powinien również znać przynajmniej jeden język programowania (C, C++, Java lub C#). Powinien również posiadać umiejętność pozyskiwania informacji ze wskazanych źródeł oraz mieć gotowość do podjęcia współpracy w ramach zespołu.

### Cel przedmiotu

Przekazanie studentom szczegółowej wiedzy teoretycznej i praktycznej z zakresu bezpieczeństwa funkcjonalnego, wykrywania zagrożeń, analizy i oceny ryzyka oraz oszacowania kosztów wdrażania bezpiecznych systemów sterowania komputerowego. W ramach przedmiotu zostaną również omówione zasady tworzenia i zarządzania odpornymi systemami komputerowymi.



### Przedmiotowe efekty uczenia się

#### Wiedza

Ma uporządkowaną i podbudowaną teoretycznie wiedzę ogólną związaną z bezpieczeństwem funkcjonalnym, analizą i oceną ryzyka.

Ma zaawansowaną wiedzę szczegółową dotyczącą wybranych zagadnień z zakresu bezpiecznych systemów sterowania komputerowego.

Ma zaawansowaną i szczegółową wiedzę o procesach zachodzących w cyklu życia odpornych systemów komputerowych.

Zna zaawansowane metody, techniki i narzędzia stosowane przy identyfikacji zagrożeń, analizie i ocenie ryzyka, jak również zna metody modelowania probabilistycznego systemów E/E/EP.

#### Umiejętności

Potrafi pozyskiwać informacje z literatury, baz danych oraz innych źródeł takich, jak zalecenia i standardy (w języku polskim i angielskim) na temat bezpieczeństwa funkcjonalnego, integrować je, dokonywać ich interpretacji i krytycznej oceny, wyciągać wnioski oraz formułować i wyczerpująco uzasadniać opinie.

Potrafi planować i przeprowadzać eksperymenty, w tym pomiary i symulacje komputerowe, interpretować uzyskane wyniki i wyciągać wnioski oraz formułować i weryfikować hipotezy związane ze złożonymi problemami w zakresie bezpieczeństwa funkcjonalnego.

Potrafi wykorzystać do formułowania i rozwiązywania zadań inżynierskich i prostych problemów badawczych w zakresie analizy i oceny ryzyka oraz kosztów wprowadzania bezpieczeństwa metody analityczne, symulacyjne oraz eksperymentalne

Potrafi dokonać krytycznej analizy istniejących metod oceny ryzyka oraz zaproponować ich ulepszenia.

Potrafi współdziałać w zespole, przyjmując w nim różne role

Potrafi określić kierunki dalszego uczenia się i zrealizować proces samokształcenia, w obszarze bezpieczeństwa funkcjonalnego.

#### Kompetencje społeczne

Rozumie, że w zakresie bezpieczeństwa funkcjonalnego wiedza i umiejętności bardzo szybko stają się przestarzałe.

Rozumie znaczenie wykorzystywania najnowszej wiedzy z zakresu bezpieczeństwa funkcjonalnego w rozwiązywaniu problemów badawczych i praktycznych.

Ma świadomość konieczności profesjonalnego podejścia do rozwiązywanych problemów bezpieczeństwa funkcjonalnego i podejmowania odpowiedzialności za proponowane przez siebie projekty.

### Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:



Wiedza zdobyta w ramach wykładu weryfikowana jest przez egzamin w formie pisemnej lub ustnej. W formie pisemnej studenci muszą udzielić odpowiedzi na 7 - 10 pytań (testowych i otwartych) różnie punktowanych. Są trzy lub cztery grupy punktowe. Natomiast w przypadku egzaminu ustnego student losuje po jednym pytaniem z każdej grupy punktowej. W formie ustnej, do każdego wylosowanego pytania, student może otrzymać dodatkowe pytanie (związane z wylosowanym pytaniem). Ocena pytania (obejmuje odpowiedź zarówno na pytanie wylosowane jak i pytanie dodatkowe) obejmuje zakres odpowiedzi oraz głębię zrozumienia zagadnienia. Do każdego egzaminu przygotowanych jest 50 - 60 pytań. Warunkiem pozytywnego zaliczenia egzaminu otrzymanie minimum 50% punktów możliwych do zdobycia.

Umiejętności nabyte w ramach zajęć laboratoryjnych weryfikowane są na bieżąco. Na każdym zajęciach laboratoryjnych oceniana jest poprawność wykonania ćwiczeń w skali od 0 do 10 punktów. Warunkiem pozytywnego zaliczenia ćwiczeń laboratoryjnych jest otrzymanie minimum 50% punktów możliwych do zdobycia.

liczba punktów	ocena
<=50 %	2,0
51% - 60%	3,0
61% - 70%	3,5
71% - 80%	4,0
81% - 90%	4,5
91% - 100%	5,0

### Treści programowe

Tematyka wykładów:

- Znaczenie integralności bezpieczeństwa
- Założenia konstrukcyjne, błędy sprzętowe oraz tolerancja na błędy
- Zalecenia dotyczące bezpieczeństwa funkcjonalnego IEC 61508, IEC 61511 i pokrewne
- Cele integralności bezpieczeństwa, zarządzanie bezpieczeństwem funkcjonalnym
- Wpływ człowieka na bezpieczeństwo funkcjonalne
- Wymagania stawiane systemom E/E/EP w odniesieniu do bezpieczeństwa funkcjonalnego
- Bezpieczeństwo funkcjonalne w systemach komunikacyjnych
- Bezpieczeństwo funkcjonalne w układach cyfrowych i sterownikach PLC
- Metody identyfikacji zagrożeń oraz analiza i ocena ryzyka, analiza warstw i pierścieni zagrożeń
- Modelowanie probabilistyczne systemów E/E/EP dla celów analizy i oceny ryzyka
- Analiza kosztów i efektów zmniejszenia ryzyka
- Normy dotyczące inżynierii systemów, bezpieczeństwa komputerowych systemów sterowania oraz oprogramowania
- Normy dotyczące zarządzania jakością, środowiskiem oraz bezpieczeństwem informacji
- Odporne systemy komputerowe:
  - Ogólny algorytm tolerancji błędów.
  - Testowanie, sprawdzanie i oznaki uszkodzeń sprzętu



- Algorytmy odzyskiwania oraz przygotowanie do odzyskiwania danych,
- Języki programowania dla krytycznych systemów bezpieczeństwa,
- Zasady pisania programów w języku C w krytycznych systemach (MISRA-C).

Tematyka laboratoriów:

Zgodna z treściami wykładów

### Metody dydaktyczne

Wykład informacyjny: prezentacja multimedialna, ilustrowana przykładami podawanymi na tablicy.

Ćwiczenia laboratoryjne: ćwiczenia praktyczne w grupach, z wykorzystaniem urządzeń sieciowych oraz środowisk zwirtualizowanych.

### Literatura

Podstawowa

1. David J Smith, Kenneth G L Simpson: The Safety Critical Systems Handbook: A Straightforward Guide to Functional Safety: lec 61508 (2010 Edition), lec 61511 (2015 Edition) and Related Guidance, Butterworth-Heinemann, 2020,
2. Schagaev Igor., Kaegi-Trachsel Thomas: Software Design for Resilient Computer Systems, Springer International Publishing, 2016.

Uzupełniająca

1. Josef Börcsök: Functional Safety: Basic Principles of Safety-related Systems, Vde Verlag GmbH, 2021.
2. Harvey T. Dearden: Functional Safety In Practice (3rd Edition), Independently Published, 2020.

### Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	100	4,0
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	45	2,0
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwium/egzaminu) <sup>1</sup>	55	2,0

<sup>1</sup> niepotrzebne skreślić lub dopisać inne czynności