Autor*: dr hab. inż. Mariusz Rawski*

Systemy Cyfrowe (SYCY)
Digital Systems

Poziom kształcenia: I stopień
Forma i tryb prowadzenia przedmiotu: stacjonarna
Kierunek studiów: Cyberbezpieczeństwo
Specjalność:
Grupa przedmiotów:
Poziom przedmiotu: podstawowy
Status przedmiotu: obowiązkowy
Język przedmiotu: polski
Semestr nominalny (tylko dla przedmiotów obowiązkowych): 3
Minimalny numer semestru: 2
Wymagania wstępne, zalecane przedmioty poprzedzające: TECY
Limit liczby studentów: 60

Powód zgłoszenia przedmiotu: program studiów na nowym kierunku Cyberbezpieczeństwo

Cel przedmiotu:

Głównym celem przedmiotu jest zaznajomienie studentów(ek) z podstawami projektowania i realizacji sprzętowych systemów cyfrowych. Omówione zostaną metodyki projektowania takich systemów, ich optymalizacji i weryfikacji. Przedstawione zostaną sposoby modelowania kombinacyjnych i sekwencyjnych układów cyfrowych z użyciem języka HDL. Zaprezentowane zostaną koncepcje dotyczące projektowania na poziomie RTL z użyciem metodyki ASM oraz projektowania hierarchicznego. Przedstawione zostaną zagadnienia dotyczące zastosowania systemów sprzętowych w cyberbezpieczeństwie oraz projektowania sprzętowych systemów cyfrowych z uwzględnieniem cyberbezpieczeństwa.

Istotnym elementem przedmiotu jest projekt, w ramach którego zespoły projektowe będą miały za zadanie zaprojektowanie, weryfikację i uruchomienie na platformie prototypowej wyposażonej w układ programowalny sprzętowego systemu cyfrowego. Projektowany system będzie łączył zagadnienia z obszar cyberbezpieczeństwa z zagadnieniami z takich obszarów, jak DSP (Digital Signal Processing), SDR (Software-Defined Radio), SDN (Software-Defined Networking), itp. Projekt realizowany będzie etapowo, każdy etap zaliczany będzie na podstawie raportu.

Treść kształcenia:

WYKŁADY:

1. **Układy cyfrowe – klasyfikacja, technologie wytwarzania, specyfika projektowania (2 godz.)**
   Klasyfikacja układów cyfrowych (układy katalogowe, układy specjalizowane ASIC, układy programowalne (FPLD). Etapy procesu projektowego. Style projektowania układów cyfrowych. Przykład syntezy układu cyfrowego realizującego prosty algorytm. Porównanie metodologii projektowania układu cyfrowego z projektowaniem oprogramowania. Komputerowe projektowanie. Narzędzia CAD. Architektury nowoczesnych systemów cyfrowych: System on a Chip (SoC), Multiprocessor System on a Chip (MPSoC), Network on Chip (NoC). Ogólne zagadnienia związane z cyberbezpieczeństwem w kontekście procesu projektowania i wytwarzania oraz podstawowe podatności sprzętu, czyli luki w zabezpieczeniach lub niepożądane funkcjonalności (backdoory).

2. **Modelowanie systemów cyfrowych (2 godz.)**
   Sposoby reprezentacji liczb w zapisie binarnym (NKB, U2, zapis stałopozycyjny oraz zmiennopozycyjny). Podstawowe działania arytmetyczne na liczbach przedstawionych binarnie.
   Sposoby opisu i modelowania systemów cyfrowych. Diagram "Y". Cyfrowe kombinacyjne i sekwencyjne bloki funkcjonalne wykorzystywane w syntezie strukturalnej układów cyfrowych.

3. **Zasady specyfikacji układów cyfrowych – języki opisu sprzętu (2 godz.)**
   Ograniczenia tradycyjnych języków programowania. Zastosowania języków HDL (Hardware Description Language). Cechy języków HDL. Podstawowe koncepcje na przykładzie języka VHDL. Opis strukturalny. Opis behawioralny. Testbench. Konfiguracja. Elementy języka VHDL. Różne sposobów opisu projektowanego systemu.

4. **Modelowanie logiki kombinacyjnej (2 godz.)**
   Sposoby realizacji logiki kombinacyjnej z wykorzystaniem struktur języka VHDL. Sposoby implementacji podstawowych kombinacyjnych bloków funkcjonalnych, tj. multipleksery dekodery, moduły opisane tablicą prawdy i równaniami boolowskimi. Parametry czasowe układów kombinacyjnych. Pojęcie ścieżki krytycznej (topologicznej, rzeczywistej, fałszywej).

5. **Modelowanie logiki sekwencyjnej (2 godz.)**
   Wykorzystanie elementów pamięciowych. Model układu sekwencyjnego. Sposoby opisu sekwencyjnych bloków funkcjonalnych. Liczniki. Sposoby realizacji logiki sekwencyjnej z wykorzystaniem struktur języka VHDL. Sposoby implementacji podstawowych sekwencyjnych bloków funkcjonalnych, tj. rejestry, automaty, liczniki. Rejestry przesuwające jako generatory pseudolosowe.

6. **Projektowanie hierarchiczne i zaawansowane zagadnienia syntezy układów cyfrowych (4 godz.)**
   Przedstawienie metodologii projektowania hierarchicznego (bottom-up itop-down). Moduły parametryzowane. Wykorzystanie pakietów. Zaawansowane metody optymalizacji układów kombinacyjnych i sekwencyjnych FSM. Wpływ metod

optymalizacji na parametry układu (wielkość zasobów, częstotliwość pracy, pobór mocy, itp). Podstawowe informacje o atakach wykorzystujące wiedzę o parametrach układu (side-channel attack) i metodach zapobiegania im.

7. **Projektowanie układów z wykorzystaniem FSM i ASM (4 godz.)**
   Zastosowanie automatów FSM i diagramów ASM do projektowania synchronicznych układów cyfrowych. Pojęcia: ripple and/or gated clocks,clock skew, clock enable. Dystrybucja sygnału zegara. Sprzętowa realizacja protokołów komunikacyjnych na prostym przykładzie. Synchronizacja międzysymbolowa. Synchronizacja międzyramkowa. Generacja sekwencji. Sposoby współdziałania automatów w systemie cyfrowym. Obsługa portów dwukierunkowych. Wykorzystanie specjalizowanych bloków na przykładzie pamięci RAM. Domeny zegarowe i komunikacja między nimi.

8. **Sprzętowa realizacja wybranych algorytmów cyfrowego przetwarzania sygnałów i informacji (4 godz.)**
   Sprzętowa realizacja operacji MAC. Wyznaczanie wartości wybranych funkcji arytmetycznych na przykładzie pierwiastka kwadratowego. Modulacja i demodulacja cyfrowa. Kody korekcyjne.

9. **Zaawansowane metody projektowania (4 godz.)**
   Różne sposoby projektowania układów cyfrowych. Strukturalna realizacja przepływu danych. Rozwijanie pętli (loop unrolling). Układ sterujący -układ operacyjny. Diagramy ASM. Diagramy ASMD. Operacje RT realizowanew trybie Mealy'ego. Współdzielenie zasobów. Potokowanie. Synteza HLS (High-level synthesis). Kosynteza sprzętowo-programowa (Hardware/Software co-design).

10. **Sprzętowa realizacja funkcji kryptograficznych (4 godz.)**
    Realizacja podstawowych przekształceń kryptograficznych (permutacja, podstawienie). Realizacja prostego szyfru strumieniowego z wykorzystaniem generatora RNG. Realizacja szyfru blokowego na podstawie algorytmu DES. Wpływ zaawansowanych metod projektowania na wydajność szyfrowania. Integracja rdzenia DES z procesorem typu SoftCore.

ĆWICZENIA:
–

LABORATORIA:
Zajęcia laboratoryjne są wprowadzeniem do projektu realizowanego w ramach przedmiotu. Mają one za zdanie zapoznanie studentów(ek) z procesem projektowym z wykorzystaniem specjalistycznych narzędzi CAD i platform do prototypowania wyposażonych w układy programowalne FPGA. Podzielono je na 3 części tematyczne:

1. Zapoznanie z projektowaniem sprzętowych systemów cyfrowych z wykorzystaniem narzędzi CAD. Zaprojektowanie prostego układu cyfrowego, przeprowadzenie

weryfikacji funkcjonalnej z użyciem symulatora i uruchomienie na platformie do prototypowania.
2. Wykorzystanie metodyki ASM do sprzętowej realizacji algorytmów. Realizacja wybranego algorytmu z wykorzystaniem koncepcji ASMD. Realizacja układu sterującego, układu operacyjnego i ich integracja.
3. Sprzętowa realizacja algorytmu jako *Custom Instruction* i jego integracja w systemie mikroprocesorowym opartym na procesorze typu *SoftCore*.

PROJEKT:

W ramach projektu zespół 2-3 osobowy będzie miał za zadanie opracować sprzętową realizację systemu łączącego zagadnienia z obszaru cyberbezpieczeństwa z zagadnieniami z takich obszarów, jak DSP (Digital Signal Processing), SDR (Software-Defined Radio), SDN (Software-Defined Networking), itp. Realizacja zadania będzie obejmowała 4 etapy: przeprowadzenie analizy literaturowej i opracowanie koncepcji rozwiązania, opracowanie modelu referencyjnego i modelu *bit accurate*, zaprojektowanie i weryfikację funkcjonalną modelu sprzętowego z analizą efektywności oraz realizację systemu z wykorzystaniem platformy sprzętowej wyposażonej w układ FPGA. Każdy etap zaliczany będzie na podstawie raportu. Istotne będzie prowadzenie dokumentacji projektu oraz przygotowanie prezentacji wyników projektu.

ZAJĘCIA ZINTEGROWANE:

–

Treść kształcenia - streszczenie w jęz. angielskim:

The main objective of the course is to introduce students to the basics of design and implementation of hardware digital systems. The course presents design methodologies, optimization and verification methods. The methods for modeling combinational and sequential circuits using HDL will be discussed. Topics related to application of hardware digital systems in cybersecurity and design for cybersecurity will be presented.

Egzamin: NIE

Literatura i oprogramowanie:

- Slajdy do wykładu, materiały uzupełniające w postaci zadań interaktywnych oraz demonstracji obrazujących omawiane zagadnienia,

- Książki:
  1. Pong P. Chu. (2006). RTL Hardware Design Using VHDL: Coding for Efficiency, Portability, and Scalability. Wiley-IEEE Press.
  2. Uwe Meyer-Baese. (2007). Digital Signal Processing with Field Programmable Gate Arrays. 10.1007/978-3-540-72613-5.
  3. Peter J. Ashenden. (2008) Digital Design: An Embedded Systems Approach Using Verilog. Elsevier Science.

4. Richard S. Sandige. (2011). Fundamentals of Digital and Computer Design with VHDL. McGraw Hill Higher Education.

- Internet
- Oprogramowanie:
    1. Oprogramowanie CAD do projektowania układów cyfrowych
    2. Oprogramowanie do symulacji układów cyfrowych
    3. Oprogramowanie do syntezy i optymalizacji

Wymiar godzinowy zajęć:	W	C	L	P
	30	–	15	15

Przewidywane formy kształcenia i organizacja przedmiotu

Realizacja przedmiotu obejmuje następujące formy zajęć:

- wykład prowadzony w wymiarze 2 godz. tygodniowo,
- zajęcia laboratoryjne w wymiarze 1 godz. tygodniowo zorganizowane w 3 zajęcia laboratoryjne.
- zajęcia projektowe; w ramach tych zajęć student(ka), korzystając z oprogramowania (które jest dostępne w laboratorium, ale może być także zainstalowane na prywatnym komputerze studenta), wykorzystując podaną przez prowadzącego specyfikację system, opracowuje koncepcję realizacji, projektuje, przeprowadza weryfikację i optymalizację oraz wykonuje realizację systemu z wykorzystaniem jednej z dostępnych platform do prototypowania; student(ka) może ponadto uczestniczyć w prowadzonych co tydzień w wymiarze 1 godz. konsultacjach.

Sprawdzanie założonych efektów kształcenia realizowane jest przez:

- ocenę wiedzy i umiejętności związanych z realizacją zadań projektowych – ocenę sprawozdań z realizacji projektu (poszczególnych etapów projektowych),
- ocenę wiedzy i umiejętności wykazanych na egzaminie pisemnym o charakterze problemowym (na egzaminie student może korzystać z dowolnych materiałów dydaktycznych oraz komputera) oraz – w przypadkach wątpliwości co do oceny – na egzaminie ustnym,

Wymiar w jednostkach ECTS: 5 pkt.

Liczba godzin pracy studenta związanych z osiągnięciem efektów kształcenia (opis):

1. *liczba godzin kontaktowych – **65 godz.**, w tym*
    - *obecność na wykładach: **30 godz.**,*
    - *obecność na zajęciach laboratoryjnych:**15 godz.**,*
    - *udział w konsultacjach związanych z realizacją projektu: **16 godz.** (zakładamy, że student korzysta z konsultacji dotyczących zainstalowania, uruchomienia i korzystania z oprogramowania wspomagającego projektowanie, a ponadto z „regularnych” konsultacji 8 razy w semestrze),*
    - *udział w konsultacjach związanych z realizacją miniprojektów (zadań domowych), zagadnień poruszanych na wykładzie: **4 godz.***

2. *praca własna studenta – **83 godz.**, w tym*

- *analiza literatury i materiałów wykładowych związana z przygotowaniem do kolejnych wykładów, zajęć laboratoryjnych i realizacji projektów:* ***25 godz.***
- *realizacja projektu:* ***30 godz.*** *= 4 x 10 godz. (4 etapy: opracowanie koncepcji, opracowanie modelu referencyjnego i modelu bit accurate , projektowanie, weryfikacja i optymalizacja, realizacja systemu na platformie sprzętowej),*
- *przygotowanie do egzaminu:* ***10 godz.***

Łączny nakład pracy studenta wynosi 124 godz., **co odpowiada** 5 pkt. **ECTS.**

Liczba punktów ECTS na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich: 2,5 pkt. ECTS, co odpowiada 65 godz. kontaktowym.

Liczba punktów ECTS, którą student uzyskuje w ramach zajęć o charakterze praktycznym: 3 pkt. ECTS co odpowiada 83 godz. zajęć laboratoryjnych i projektowych oraz przygotowaniu do tych zajęć.

EFEKTY KSZTAŁCENIA/UCZENIA SIĘ

efekty kształcenia/uczenia się	forma zajęć/ technika kształcenia	sposób weryfikacji (oceny)*	odniesienie do efektów uczenia się dla programu
WIEDZA			
w1: ma podstawową wiedzę o etapach procesu projektowego systemów cyfrowych	wykład + projekt + laboratorium	projekt, laboratorium, kololwium	W04 W09 W10
w2: ma podstawową wiedzę o ogólnych zagadnieniach związanych z cyberbezpieczeństwem w kontekście procesu projektowania i wytwarzania oraz podstawowych podatnościach sprzętu	wykład + projekt	projekt, kololwium	W04 W09 W10
w3: ma wiedzę o sposobach modelowania systemów cyfrowych w wykorzystaniem języków HDL	wykład + projekt + laboratorium	projekt, laboratorium, kololwium	W04
w4: ma wiedzę o metodach optymalizacji i ich wpływie i na parametry układu oraz podstawową wiedzę o atakach wykorzystujących znajomość parametrów układu (side-channel attack) i metodach zapobiegania im.	wykład + projekt	projekt, kololwium	W04 W09 W10
w5: ma wiedzę o zaawansowanych metodach projektowania systemów cyfrowych	wykład + projekt	projekt, kololwium	W04
w6: ma podstawową wiedzę o sprzętowej realizacji algorytmów kryptograficznych	wykład + projekt	projekt, kololwium	W04 W09 W10
UMIEJĘTNOŚCI			
u1: potrafi przygotować środowisko pracy	wykład + laboratorium	laboratorium	U03
u2: potrafi opracować koncepcję i sprzętową realizację systemu łączącego zagadnienia z obszaru cyberbezpieczeństwa z zagadnieniami z obszarów takich, jak np. DSP, SDR, SDN, itp.	wykład + projekt + laboratorium	projekt + laboratorium	U01 U03 U08 U09
u2: potrafi przeprowadzić wersyfikację sprzętowej realizacji systemu	wykład + projekt + laboratorium	projekt + laboratorium	U03 U08 U09
u3: potrafi przygotować dokumentację sprzętowej realizacji systemu	wykład + projekt	projekt	U10
KOMPETENCJE SPOŁECZNE			
ks1: rozumie potrzebę stałego aktualizowania i wzbogacania posiadanej wiedzy	wykład + projekt + laboratorium	–	KS01

Wydziałowa Komisja Akredytacji Przedmiotów (WKAP)

Uwagi:
–

Data i podpis autora (kierownika zespołu autorskiego):