

# PAŃSTWOWA WYŻSZA SZKOŁA ZAWODOWA W NOWYM SĄCZU

## KARTA PRZEDMIOTU

obowiązuje studentów rozpoczynających studia w roku akademickim 2013/2014

Instytut Techniczny

Kierunek studiów: Mechatronika

Profil: Ogólnoakademicki

Forma studiów: Stacjonarne

Kod kierunku: 06.0

Stopień studiów: I

Specjalności: Mechatronika stosowana  
Mechatronika pojazdów samochodowych

### 1 PRZEDMIOT

|                      |  |
|----------------------|--|
| NAZWA PRZEDMIOTU     | Bezpieczeństwo IT w systemach mechatronicznych |
| KOD PRZEDMIOTU       | IT 06.0 AIS B25 13/14                          |
| KATEGORIA PRZEDMIOTU | Przedmioty podstawowe i kierunkowe             |
| LICZBA PUNKTÓW ECTS  | 1  |
| SEMESTRY             | 7  |

### 2 RODZAJ ZAJĘĆ, LICZBA GODZIN W PLANIE STUDIÓW

| SEMESTR | WYKŁAD | ĆWICZENIA | LABORATORIUM | PROJEKT | SEMINARIUM |
|---------|--------|-----------|--------------|---------|------------|
| 7       | 15     |           |              |         |            |

### 3 CELE PRZEDMIOTU

- Cel 1** Przedmiot służy do poznania podstaw bezpieczeństwa technologii informatycznych (IT) w systemach mechatronicznych.
- Cel 2** Zapoznanie się ze standardami i zakończonymi projektami w zakresie bezpieczeństwa IT w systemach mechatronicznych.
- Cel 3** Zapoznanie studentów z aspektami bezpieczeństwa wewnętrznej sieci systemu mechatronicznego, komponentów sieci pokładowej i interakcji wielu komponentów w obrębie sieci tego systemu.
- Cel 4** Przekazanie studentom wiedzy w zakresie infrastruktury i kryptograficznych mechanizmów bezpieczeństwa dla systemu komunikacji Car2X, oraz oceny kryptograficznych metod ochrony IT w systemach mechatronicznych.
- Cel 5** Nabycie wiedzy o usługach bezpieczeństwa i wbudowanym systemie kryptograficznym w systemach mechatronicznych.



## 4 WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I INNYCH KOMPETENCJI

- a Informatyka
- b Elektrotechnika i elektronika analogowa
- c Metrologia techniczna i systemy pomiarowe
- d Elektronika cyfrowa, optoelektronika

## 5 EFEKTY KSZTAŁCENIA

- EK1** Wiedza: Ma elementarną wiedzę w zakresie architektury systemów i sieci informatycznych oraz systemów operacyjnych opartych na standardach i zakończonych projektach (SeVeCom, Preciosa, EVITA), niezbędną do instalacji, obsługi i utrzymania narzędzi informatycznych służących do symulacji i projektowania układów, systemów i urządzeń mechatronicznych z uwzględnieniem bezpieczeństwa stosowanych w nich IT.
- EK2** Wiedza: Posiada ogólną wiedzę w zakresie bezpieczeństwa wewnętrznej sieci systemu mechatronicznego, komponentów sieci pokładowej i interakcji wielu komponentów w obrębie sieci tego systemu.
- EK3** Wiedza: Ma elementarną wiedzę dotyczącą infrastruktury i kryptograficznych mechanizmów bezpieczeństwa dla systemu komunikacji Car2X.
- EK4** Wiedza: Posiada podstawową wiedzę o usługach bezpieczeństwa i wbudowanym systemie kryptograficznym w systemach mechatronicznych.
- EK5** Umiejętności: Potrafi posłużyć się dobranymi z norm mechanizmami zabezpieczającymi do ochrony komunikacji w systemach mechatronicznych.
- EK6** Umiejętności: Potrafi ocenić przydatność i sposób funkcjonowania, istniejące rozwiązania elementów wbudowanego systemu kryptograficznego, możliwość ich zastosowania dla systemu mechatronicznego.
- EK7** Kompetencje społeczne: Ma świadomość dotyczącą swojej roli wykształconego inżyniera mechatroniki w lokalnym społeczeństwie, w szczególności dotyczącą propagacji nowoczesnych rozwiązań bezpieczeństwa IT w systemach mechatronicznych, ich wpływu na zaufanie mieszkańców regionu do nowoczesnych systemów informatycznych wraz z polepszeniem jakości życia.
- EK8** Kompetencje społeczne: Potrafi sformułować i przekazać w sposób zrozumiały dla przeciętnego obywatela nowe wyzwania dla przemysłu mechatronicznego: elektroniczne bezpieczeństwo IT.

## 6 TREŚCI PROGRAMOWE

### WYKŁAD

| LP | TEMATYKA ZAJĘĆ<br>OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH   | LICZBA GODZIN |
|----|--|---------------|
| W1 | Wprowadzenie i rozwój historyczny bezpieczeństwa IT w systemach mechatronicznych. Elektroniczne bezpieczeństwo i ochrona - nowe wyzwania dla przemysłu mechatronicznego.   | 1             |
| W2 | Bezpieczeństwo wewnętrznej sieci systemu mechatronicznego: magistrala CAN, wyzwania i zagrożenia dla bezpieczeństwa CAN, odstępstwa od norm.   | 2             |
| W3 | Bezpieczeństwo komponentów wewnętrznej sieci systemu mechatronicznego:: metodologia ataków, lokalne testowanie, testy drogowe. Interakcje wielu komponentów wewnętrznej sieci systemu mechatronicznego:: ataki kompleksowe, niwelowanie wewnętrznych sieci CAN, wykrywanie versus zapobieganie atakom oraz bezpieczeństwo. | 2             |



## WYKŁAD

| LP | TEMATYKA ZAJĘĆ<br>OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH   | LICZBA GODZIN |
|----|--|---------------|
| W4 | Infrastruktura systemu komunikacyjnego Car2X: sieć komunikacyjna, protokół komunikacyjny, aplikacje, podstawowe typy komunikatów. Usługi i możliwe mechanizmy bezpieczeństwa: usługi bezpieczeństwa, metody z kluczem publicznym, metody symetryczne, metody hybrydowe, wymagania eksploatacyjne (wydajnościowe), wymagania prywatności. Kryptograficzne mechanizmy i opcje implementacyjne standardu IEEE 1609.2: opis komponentów kryptograficznych, uzasadnienie racjonalne, zwyczajna implementacja oprogramowania na procesorze samochodowym, karty inteligentne, programowalne układy logiczne FPGA (Field Programmable Gate Array) i elektroniczne układy scalone ASIC (Application-Specific Integrated Circuit). | 2             |
| W5 | Wbudowany system kryptograficzny w systemie mechatronicznym: mechanizmy bezpieczeństwa, IT bezpieczeństwo i kryptografia, integracja funkcji kryptograficznych algorytmów symetrycznych i z kluczem publicznym z aplikacjami systemu mechatronicznego, bezpieczna implementacja a atak bocznym kanałem SCA (Side Channel Attack), wydajna implementacja, rozwiązania Eurobits (European Competence Center for IT Security) w dziedzinie IT bezpieczeństwa systemów mechatronicznych.   | 2             |
| W6 | Rozwiązania bezpieczeństwa IT w zakończonych projektach europejskich SeVeCom i Preciosa: ochrona zewnętrznej komunikacji samochodowej, ochroną prywatności w komunikacji samochodowej.   | 2             |
| W7 | Aplikacje E-bezpieczeństwa chronione pojazd przed włamaniem EVITA: wewnętrzne bezpieczeństwo pokładowe, bezpieczna komunikacja zewnętrzna pojazdu.   | 4             |
|    | RAZEM  | 15            |

## 7 METODY DYDAKTYCZNE

M1 Wykłady

M2 Prezentacje multimedialne

## 8 OBCIĄŻENIE PRACĄ STUDENTA

| FORMA AKTYWNOŚCI   | ŚREDNIA LICZBA<br>GODZIN NA<br>ZREALIZOWANIE<br>AKTYWNOŚCI |
|--|--|
| <b>Godziny kontaktowe z nauczycielem akademickim, w tym:</b>                                     |  |
| Godziny wynikające z planu studiów   | 15   |
| Konsultacje przedmiotowe   | 0  |
| Egzaminy i zaliczenia w sesji  | 0  |
| <b>Godziny bez udziału nauczyciela akademickiego wynikające z nakładu pracy studenta, w tym:</b> |  |
| Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury                               | 10   |
| Opracowanie wyników  | 0  |
| Przygotowanie raportu, projektu, prezentacji, dyskusji   | 0  |
| <b>SUMARYCZNA LICZBA GODZIN DLA PRZEDMIOTU WYNIKAJĄCA Z CAŁEGO NAKŁADU PRACY STUDENTA</b>        | <b>25</b>  |
| SUMARYCZNA LICZBA PUNKTÓW ECTS DLA PRZEDMIOTU  | 1  |



## 9 SPOSOBY OCENY

### OCENA FORMUJĄCA

**F1** Odpowiedź ustna

**F2** Aktywność na zajęciach

**F3** Referat

### KRYTERIA OCENY

| EFEKT KSZTAŁCENIA 1 |   | MIEJSCE WERYFIKACJI | OPIS WERYFIKACJI EK 1   |
|---------------------|---|---------------------|---|
| NA OCENĘ 3          | Opisuje architektury systemów i sieci informatycznych oraz systemów operacyjnych opartych na standardach i zakończonych projektach (SeVeCom, Preciosa, EVITA) z błędami.  | wykład              | Ocena z odpowiedzi ustnych, aktywności na zajęciach i referatu. |
| NA OCENĘ 4          | Posiada wiadomości na ocenę 3 a ponadto definiuje kilku narzędzi, poprawnie formułuje narzędzia i potrafi w analityczny sposób je porównać.   |                     |   |
| NA OCENĘ 5          | Posiada wiadomości na ocenę 4, a ponadto identyfikuje narzędzia potrzebne do rozwiązania zadanego problemu z jednoczesnym uzasadnieniem i nie popełnia żadnych błędów.  |                     |   |
| EFEKT KSZTAŁCENIA 2 |   | MIEJSCE WERYFIKACJI | OPIS WERYFIKACJI EK 2   |
| NA OCENĘ 3          | Określa zasady bezpieczeństwa wewnętrznej sieci systemu mechatronicznego i komponentów sieci pokładowej z błędami.  | wykład              | Ocena z odpowiedzi ustnych, aktywności na zajęciach i referatu. |
| NA OCENĘ 4          | Posiada wiadomości na ocenę 3 a ponadto formułuje kilku narzędzi, poprawnie definiuje interakcje wielu komponentów w obrębie sieci systemu mechatronicznego.  |                     |   |
| NA OCENĘ 5          | Posiada wiadomości na ocenę 4 a ponadto identyfikuje narzędzia potrzebne do rozwiązania zadanego problemu z jednoczesnym uzasadnieniem narzędzia, potrafi w analityczny sposób je porównać i nie popełnia żadnych błędów. |                     |   |
| EFEKT KSZTAŁCENIA 3 |   | MIEJSCE WERYFIKACJI | OPIS WERYFIKACJI EK 3   |
| NA OCENĘ 3          | Opisuje infrastruktury i kryptograficznych mechanizmów bezpieczeństwa dla systemu komunikacji Car2X z błędami.  | wykład              | Ocena z odpowiedzi ustnych, aktywności na zajęciach i referatu. |
| NA OCENĘ 4          | Posiada wiadomości na ocenę 3 a ponadto poprawnie formułuje mechanizmy kryptograficzne i potrafi w analityczny sposób je porównać.  |                     |   |



|                     |   |                     |   |
|---------------------|---|---------------------|---|
| NA OCENĘ 5          | Posiada wiadomości na ocenę 4 a ponadto identyfikuje infrastrukturę i kryptograficzne mechanizmy bezpieczeństwa potrzebne do rozwiązania zadanego problemu z jednoczesnym uzasadnieniem i nie popełnia żadnych błędów.  |                     |   |
| EFEKT KSZTAŁCENIA 4 |   | MIEJSCE WERYFIKACJI | OPIS WERYFIKACJI EK 4   |
| NA OCENĘ 3          | Opisuje usługi bezpieczeństwa i strukturę wbudowanego systemu kryptograficznego w systemach mechatronicznych z błędami.   | wykład              | Ocena z odpowiedzi ustnych, aktywności na zajęciach i referatu. |
| NA OCENĘ 4          | Posiada wiadomości na ocenę 3 a ponadto formułuje kilku usług bezpieczeństwa i wyznacza kilku elementów wbudowanym systemie kryptograficznym w systemach mechatronicznych, poprawnie definiuje usługi bezpieczeństwa i komponenty wbudowanego systemu kryptograficznego, oraz potrafi w analityczny sposób je porównać. |                     |   |
| NA OCENĘ 5          | Posiada wiadomości na ocenę 4 a ponadto identyfikuje usługi bezpieczeństwa i komponenty wbudowanego systemu kryptograficznego potrzebne do rozwiązania zadanego problemu z jednoczesnym uzasadnieniem i nie popełnia żadnych błędów.  |                     |   |
| EFEKT KSZTAŁCENIA 5 |   | MIEJSCE WERYFIKACJI | OPIS WERYFIKACJI EK 5   |
| NA OCENĘ 3          | Posługuje się mechanizmami zabezpieczającymi z błędami.   | wykład              | Ocena z odpowiedzi ustnych, aktywności na zajęciach i referatu. |
| NA OCENĘ 4          | Posiada umiejętności na ocenę 3 a ponadto poprawnie wykorzystuje mechanizmy zabezpieczające i potrafi w analityczny sposób je porównać.   |                     |   |
| NA OCENĘ 5          | Posiada umiejętności ocenę 4 a ponadto identyfikuje mechanizmy zabezpieczające potrzebne do rozwiązania zadanego problemu z jednoczesnym uzasadnieniem i nie popełnia żadnych błędów.   |                     |   |
| EFEKT KSZTAŁCENIA 6 |   | MIEJSCE WERYFIKACJI | OPIS WERYFIKACJI EK 6   |
| NA OCENĘ 3          | Umie oszacować przydatność i sposób funkcjonowania, oraz istniejące rozwiązania elementów wbudowanego systemu kryptograficznego z błędami.  | wykład              | Ocena z odpowiedzi ustnych, aktywności na zajęciach i referatu. |



|                     |   |                        |   |
|---------------------|---|------------------------|---|
| NA<br>OCENĘ<br>4    | Posiada umiejętności na ocenę 3 a ponadto rozumie kilku istniejących rozwiązań elementów wbudowanego systemu kryptograficznego, poprawnie ocenia sposób funkcjonowania wbudowanego systemu kryptograficznego i wykorzystuje istniejące rozwiązania jego elementów, oraz potrafi w analityczny sposób je porównać. |                        |   |
| NA<br>OCENĘ<br>5    | Posiada umiejętności ocenę 4 a ponadto identyfikuje elementy potrzebne do rozwiązania zadanego problemu z jednoczesnym uzasadnieniem i nie popełnia żadnych błędów.   |                        |   |
| EFEKT KSZTAŁCENIA 7 |   | MIEJSCE<br>WERYFIKACJI | OPIS WERYFIKACJI EK 7   |
| NA<br>OCENĘ<br>3    | Uświadamia sobie błędnie swoją rolę wykształconego inżyniera mechatronika w lokalnym społeczeństwie.  | wykład                 | Ocena z odpowiedzi ustnych, aktywności na zajęciach i referatu. |
| NA<br>OCENĘ<br>4    | Posiada kompetencje społeczne na ocenę 3 a ponadto formułuje swoją rolę, poprawnie umie propagować nowoczesne rozwiązania bezpieczeństwa IT w systemach mechatronicznych i potrafi w analityczny sposób je porównać.  |                        |   |
| NA<br>OCENĘ<br>5    | Posiada kompetencje społeczne na ocenę 4 a ponadto rozumie wpływ na zaufanie mieszkańców regionu do nowoczesnych systemów informatycznych wraz z polepszeniem jakości życia i nie popełnia żadnych błędów.  |                        |   |
| EFEKT KSZTAŁCENIA 8 |   | MIEJSCE<br>WERYFIKACJI | OPIS WERYFIKACJI EK 8   |
| NA<br>OCENĘ<br>3    | Potrafi sformułować zaledwie kilku aspektów nowego wyzwania dla przemysłu mechatronicznego: elektroniczne bezpieczeństwo IT.  | wykład                 | Ocena z odpowiedzi ustnych, aktywności na zajęciach i referatu. |
| NA<br>OCENĘ<br>4    | Posiada kompetencje społeczne na ocenę 3 a ponadto potrafi przekazać w sposób zrozumiały dla przeciętnego obywatela kilku aspektów nowego wyzwania przemysłu mechatronicznego: elektroniczne bezpieczeństwo IT, poprawnie definiuje i przekazuje nowe wyzwania, oraz potrafi w analityczny sposób je porównać.    |                        |   |
| NA<br>OCENĘ<br>5    | Posiada kompetencje społeczne na ocenę 4 a ponadto identyfikuje nowe wyzwania potrzebne do rozwiązania zadanego problemu z jednoczesnym uzasadnieniem i nie popełnia żadnych błędów.  |                        |   |

**OCENA DO INDEKSU (OCENA PODSUMOWUJĄCA)**

Średnia ważona ocen cząstkowych uzyskanych za poszczególne efekty kształcenia.

**WARUNKI ZALICZENIA PRZEDMIOTU**

a Zaliczenie na podstawie obecności i aktywnego udziału w wykładach, oraz wyników oceny napisanego referatu.

**10 MACIERZ REALIZACJI PRZEDMIOTU**

| EFEKTY<br>KSZTAŁCENIA<br>DLA<br>PRZEDMIOTU | ODNIESIENIE DO<br>EFEKTÓW<br>KIERUNKOWYCH | CELE PRZEDMIOTU | TREŚCI<br>PROGRAMOWE | METODY<br>DYDAKTYCZNE |
|--|---|-----------------|----------------------|-----------------------|
| EK1  | MT_W05                                    | Cel2            | W6, W7               | M1, M2                |
| EK2  | MT_W05                                    | Cel3            | W2, W3               | M1, M2                |
| EK3  | MT_W05                                    | Cel4            | W4                   | M1, M2                |
| EK4  | MT_W05                                    | Cel5            | W4, W5               | M1, M2                |
| EK5  | MT_W05                                    | Cel2            | W4, W6, W7           | M1, M2                |
| EK6  | MT_W05                                    | Cel5            | W5                   | M1, M2                |
| EK7  | MT_K07                                    | Cel1            | W1                   | M1, M2                |
| EK8  | MT_K07                                    | Cel1            | W1                   | M1, M2                |

**11 WYKAZ LITERATURY****LITERATURA PODSTAWOWA:**

- [1] Henniger O. — *Secure automotive on-board networks Basis for secure vehicle-to-X communication*, Darmstadt, 2010, Fraunhofer SIT ([http://www.agentschapnl.nl/sites/default/files/bijlagen/01\\_Staufrei\\_EVITA.pdf](http://www.agentschapnl.nl/sites/default/files/bijlagen/01_Staufrei_EVITA.pdf))
- [2] Karpiński M. — *Bezpieczeństwo informacji*, Warszawa, 2012, Pomiar Automatyka Kontrola
- [3] Karpiński M., Kurytnik I.P. — *Sieci komputerowe: Bezpieczeństwo. Część 1 Metody i systemy kryptograficzne*, Bielsko-Biała, 2006, ATH
- [4] Schneider B. — *Kryptografia dla praktyków. Wyd. 2 zm. i rozsz.*, Warszawa, 2002, WNT
- [5] Strebe B. — *Bezpieczeństwo sieci*, Warszawa, 2005, MIKOM

**LITERATURA UZUPEŁNIAJĄCA:**

- [1] Kargl F. — *Secure Vehicle Communication. Deliverable 2.1-App.A: Baseline Security Specification. Project Sevecom*, Ulm, Germany, 2009, <http://www.sevecom.org/>
- [2] Borowik B., Karpinsky M., Lahno V., Petrov O. — *Theory of Digital Automata*, Dordrecht Heidelberg New York London, 2013, Springer
- [3] Schaub F. — *PRivacy Enabled Capability In Co-Operative Systems and Safety Applications. Deliverable 10: Mechanisms for V2X Privacy. Project PRECIOSA*, Berlin, Germany, 2010, <http://www.preciosa-project.org/>
- [4] Schtze T. — *Automotive Security: Cryptography for Car2X Communication*, Stuttgart, Germany, 2011, Rohde & Schwarz SIT GmbH ([http://www.torsten-schuetze.de/reports/ieee1609-2\\_security.pdf](http://www.torsten-schuetze.de/reports/ieee1609-2_security.pdf))



## 12 INFORMACJE O NAUCZYCIELACH AKADEMICKICH

### OSOBA ODPOWIEDZIALNA ZA KARTĘ

prof. dr hab. inż. Mikołaj Karpiński (kontakt: mkarpinski@ath.bielsko.pl)

### OSOBY PROWADZĄCE PRZEDMIOT

prof. dr hab. inż. Mikołaj Karpiński (kontakt: mkarpinski@ath.bielsko.pl)

## 13 ZATWIERDZENIE KARTY PRZEDMIOTU DO REALIZACJI

| (miejscowość, data) | (odpowiedzialny za przedmiot) | (kierownik zakładu) | (dyrektor instytutu) |
|---------------------|-------------------------------|---------------------|----------------------|
|---------------------|-------------------------------|---------------------|----------------------|

PWSZ w Nowym Sączu

PRZYJMUJĘ DO REALIZACJI (data i podpisy osób prowadzących przedmiot)

.....