



30

1994 – 2024





ROLA INSTYTUTÓW W FUNKCJONOWANIU WYDZIAŁU CYBERNETYKI

**dr hab. inż. Zbigniew Tarapata, prof. WAT
dziekan**

Instytuty tworzące Wydział Cybernetyki WAT odgrywają kluczową rolę w funkcjonowaniu wydziału, zapewniając kompleksowe wsparcie w obszarze naukowym, dydaktycznym i organizacyjnym. Instytuty: Systemów Informatycznych, Matematyki i Kryptologii oraz Teleinformatyki i Cyberbezpieczeństwa współtworzą fundamenty akademickie wydziału, kształcąc specjalistów niezbędnych dla rozwoju nowoczesnej gospodarki i bezpieczeństwa państwa. Koordynują procesy dydaktyczne, dbając o wysoką jakość kształcenia i dostosowanie programów nauczania do zmieniających się potrzeb rynku i wyzwań technologicznych. Jednocześnie wspierają rozwój kadry naukowej i technologii poprzez prowadzenie badań, projektów naukowych oraz współpracę z przemysłem i instytucjami państwowymi. Dzięki swojej interdyscyplinarności wzmacniają pozycję Wydziału i Uczelni.

INSTYTUT SYSTEMÓW INFORMATYCZNYCH

struktura i misja



Instytut Systemów Informatycznych (ISI) działa od 1994 roku jako jednostka naukowo-dydaktyczna. Od 2011 roku składa się z pięciu zakładów: Inżynierii Oprogramowania, Inżynierii Systemów Informatycznych, Badań Operacyjnych i Wspomagania Decyzji, Informatycznych Systemów Zarządzania oraz Systemów Symulacyjnych i Wspomagania Dowodzenia. Kadra naukowa Instytutu to w większości absolwenci WAT, posiadający tytuły doktorskie, zatrudniani także w instytucjach publicznych i firmach prywatnych. Instytut specjalizuje się w realizacji prac badawczych i naukowych oraz kształceniu.

Kontakt:

tel.: 261 839 504, 261 837 338



INSTYTUT SYSTEMÓW INFORMATYCZNYCH

**działalność edukacyjna i infrastruktura
badawcza**

Kształcenie w Instytucie Systemów Informatycznych odbywa się w formie studiów stacjonarnych, niestacjonarnych i podyplomowych i MBA. Na kierunku Informatyka Instytut profiluje cztery specjalności w ramach inżynierii systemów: systemy informatyczne, informatyczne systemy zarządzania, analiza danych oraz modelowanie i symulacja. Na kierunku Kryptologia i cyberbezpieczeństwo odpowiada za specjalność bezpieczeństwo informacyjne. Od 2018 roku ISI prowadzi cztery specjalistyczne pracownie badawcze: Pracownia zobrazowania wielkoformatowego i symulacji rozszerzonych, Pracownia Informatycznych Systemów Symulacji Numerycznej w Systemach Wspomagania Decyzji oraz Diagnostyki Medycznej, Pracownia Informatycznych Systemów Wspomagania Decyzji oraz Pracownia Modelowania i Analizy Cyberprzestrzeni.

Kontakt:

tel.: 261 839 504, 261 837 338



INSTYTUT SYSTEMÓW INFORMATYCZNYCH osiągnięcia naukowe

Instytut współpracuje z wieloma uczelniami i ośrodkami badawczymi. Pracownicy naukowcy uczestniczą w projektach badawczych i wdrożeniowych finansowanych przez NCBiR oraz przemysł, przyczyniając się do rozwoju technologii w dziedzinie modelowania, sztucznej inteligencji i systemów zarządzania. Instytut jest również wydawcą czasopisma „Computer Science and Mathematical Modelling”, które od 2015 roku publikuje prace z zakresu informatyki i badań operacyjnych. Pracownicy i studenci odnoszą sukcesy w międzynarodowych konkursach technologicznych, takich jak Microsoft Imagine Cup, HackYeah oraz konkursy NATO, zdobywając medale na prestiżowych wystawach wynalazków.



Kontakt:

tel.: 261 839 504, 261 837 338



WYZWANIA STOJĄCE PRZED INSTYTUTEM

dr hab. inż. Tadeusz Nowicki, prof. WAT
dyrektor

W obszarze zainteresowań Instytutu Systemów Informatycznych jest rozwijanie systemów wspomagania decyzji dla zastosowań wojskowych. W szczególności, w najbliższych latach widzimy potrzebę opracowania modeli, metod i technik związanych z szeroko pojętym obszarem sztucznej inteligencji, symulacji komputerowej, grafowych baz danych, inżynierii oprogramowania itd. dla konstruowania systemów wspomagania dowodzenia na polu walki, metod oceny potencjału bojowego wojsk, algorytmizacji działań bezzałogowych statków powietrznych, systemów wspomagania diagnostyki medycznej, zastosowania sztucznych sieci neuronowych do modelowania i rozwiązywania problemów w systemach technicznych.



SYSTEM SYMULACYJNEGO WSPOMAGANIA SZKOLENIA OPERACYJNEGO PK. ZŁOCIEŃ



Wdrożenie

Wdrożony na zlecenie MON
w celu wspomagania
komputerowo (CAX) ćwiczeń
szczebla operacyjno-
strategicznego na
wszystkich etapach ćwiczeń.

System ZŁOCIEŃ symuluje działania jednostek wojskowych, uwzględniając ich zdolności operacyjne oraz warunki, w jakich działają. Architektura systemu oparta jest na rozproszonym środowisku zgodnym z High Level Architecture (HLA). Wykorzystuje serwery SUN/Solaris® oraz stacje robocze PC/Windows. Oprogramowanie symulacyjne zostało stworzone w językach: ADA, C++, PhP.





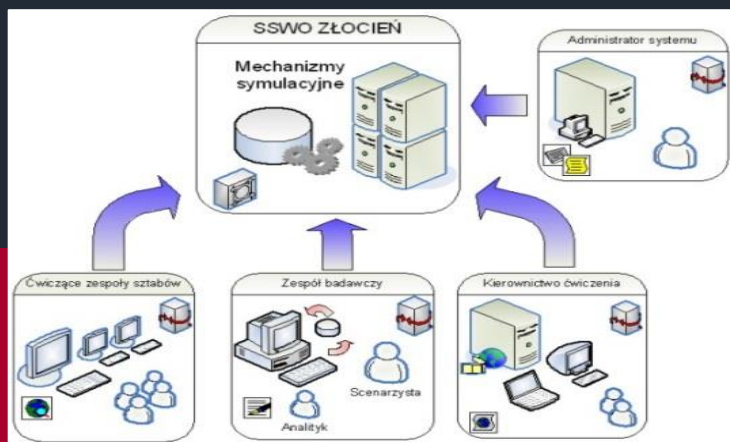
SYSTEM SYMULACYJNEGO WSPOMAGANIA SZKOLENIA OPERACYJNEGO PK. ZŁOCIEŃ

Użytkownicy

Centrum Symulacji i Komputerowych Gier Wojennych Akademii Obrony Narodowej (CSiKGW AON), uczestnicy ćwiczeń operacyjno-strategicznych, kadra wojskowa MON.

Kierownik Zespołu

dr hab. inż. Andrzej Najgebauer
prof. WAT





SYSTEM AGREGACJI RAPORTÓW – NARZĘDZIE ANALITYCZNE (SARNA)



Wdrożenie

Wdrożony podczas pandemii grypy spowodowanej wirusem A/H1N1 (wirus świńskiej grypy) na zlecenie RCB.

Spełniał ściśle określone zadania: dostępność oraz łatwość wdrażania, utrzymania i obsługi. Zbudowany w technologii klient-server. Podstawowym element stanowi serwer IIS, system zarządzania bazą danych MSSQL oraz usługi prognozowania typu web-services. Dane obrazowane były na mapach cyfrowych pakietu ESRI. Zastosowano adaptacyjną metodę „rywalizacji” między wieloma modelami prognostycznymi celem minimalizacji błędu prognozy.



SYSTEM AGREGACJI RAPORTÓW – NARZĘDZIE ANALITYCZNE (SARNA)

Użytkownicy

Szpitalne, wojewódzkie CZK, RCB

Kierownik Zespołu

dr inż. Dariusz Pierzchała
prof. WAT






SARNA

System raportowania danych o pacjentach i zasobach szpitali dla zachorowań na grypę i zachorowań grypopodobnych

Raport dotyczący osób i zasobów szpitalnych dla osób przyjętych z powodu zachorowania na grypę lub zachorowania grypopodobnego

Informacje zbiorcze za okres 24 godz. od godz. 8.00 dnia 3 grudnia 2009 r. do godz. 8.00 dnia 4 grudnia 2009 r.

Data ankiety 2009-12-03 21:07:10

	Dzieci (do 14 lat)	Dorośli (od 15 lat)
1. Liczba osób przyjętych na hospitalizację		
2. Liczba osób wypisanych po hospitalizacji		
3. Liczba zgonów osób z infekcyjną chorobą układu oddechowego		

Stan na godz. 8.00 dnia 4 grudnia 2009 r.

Data ankiety 2009-12-04 08:00:00

	Dzieci (do 14 lat)	Dorośli (od 15 lat)
4. Liczba osób hospitalizowanych		
5. Liczba osób hospitalizowanych wymagającym wspomaganie oddechu respiratorem		
6. Liczba wolnych łóżek zapewniających wspomaganie oddechu respiratorem osobom z infekcyjną chorobą układu oddechowego		

Weryfikuj dane Wyczyść dane



SYMULATOR WARIANTÓW DZIAŁAŃ BOJOWYCH WOJSK LĄDOWYCH (SWD-T)



Wdrożenie

Wdrożony w celu szybkiego przygotowania oraz wielokryterialnej oceny wariantów działań z wykorzystaniem symulacji komputerowej.



Model symulacyjny obejmuje działania ogólnowojskowe na poziomie taktycznym (obrona, natarcie, marsz), wspierające, zabezpieczające i niesymetryczne w różnych uwarunkowaniach terenowych.

Symulator składa się z edytorów: scenariuszy, bazy parametrów UiSW oraz ŚBiM i danych terenowych, modułu symulacji walki (przemieszczania, rozpoznania, oddziaływania ogniowego, modułu zobrazowania przebiegu i wyników symulacji działań).

Wykorzystuje mechanizm symulacji dyskretniej ze zmiennym tempem czasu. Wykorzystano interfejs MIP w formie bazy pośredniej JC3 oraz standard High Level Architecture (IEEE1516, STANAG 4603).

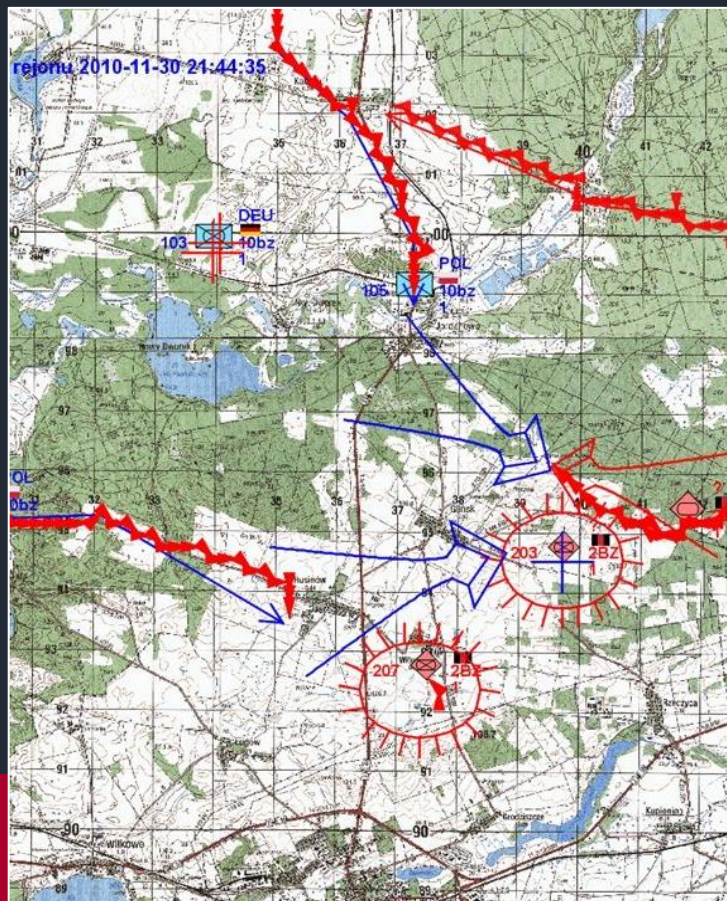
SYMULATOR WARIANTÓW DZIAŁAŃ BOJOWYCH WOJSK LĄDOWYCH (SWD-T)

Użytkownicy

Wydział Dowodzenia AON (obecnie ASZwoj); Strategiczny Przegląd
Obrony 2018

Kierownik Zespołu

dr hab. inż. Andrzej Najgebauer
prof. WAT





SYMULATOR STANOWISKA KIEROWCY WOZU BOJOWEGO PSP



Wdrożenie

Wdrożony w celu
zwiększenia skuteczności
działań ratowników
Krajowego Systemu
Ratowniczo-Gaśniczego.



Stacja szkoleniowa zwiększająca skuteczność ratowników
Krajowego Systemu Ratowniczo-Gaśniczego.

Mobilne stanowisko szkolenia kierowców straży pożarnej zostało
zaprojektowane w oparciu o kontener umożliwiający
przemieszczanie całego zestawu szkoleniowego. Stanowisko
symulatora kierowcy zostało zbudowane na bazie wskazanego
wozu bojowego straży pożarnej. Uwzględnia ono najistotniejsze
elementy przyrządów sterowniczych pojazdu. Symulator zapewnia
wizualizację sytuacji, widok przez przednią szybę oraz szyby boczne
pojazdu.

Konstrukcja symulatora umożliwia symulację ruchów pojazdu:
wstrząsy, przechylenia i wibracje we wszystkich kierunkach.

SYMULATOR STANOWISKA KIEROWCY WOZU BOJOWEGO PSP

Użytkownicy

Centrala szkolenia służb pożarniczych

Kierownik Zespołu

dr inż. Roman Wantoch-Rekowski





SYMULATOR SYSTEMU KIEROWANIA OGNIEM WIEŻY HITFIST-30P DO SYMULATORA SK-1 PLUTONU KTO ROSOMAK



Wdrożenie

Wdrożony na zlecenie
Ośrodka Badawczo-
Rozwojowego Urządzeń
Mechanicznych „OBRUM”
sp. z o.o. w Gliwicach (Bumar
ŁĄD).



Symulator został opracowany z wykorzystaniem programowalnego środowiska symulacji wirtualnej VBS2 i służy do szkolenia załóg pojazdów KTO Rosomak. Oprogramowanie współpracuje z imitatorami oprzyrządowania wieży Hitfist-30P, generując obraz na monitorach działonowego i dowódcy oraz na dziewięciu peryskopach.

System odwzorowuje pełną funkcjonalność systemu kierowania ogniem i współdziała z oprogramowaniem kierowcy, a także administratora i instruktora, umożliwiając przeprowadzenie zaawansowanych szkoleń dotyczących obsługi wieży oraz taktyki działania dowódcy i działonowego.



www.wcy.wat.edu.pl



SYMULATOR SYSTEMU KIEROWNIA OGNIEM WIEŻY HIYFIST-30P DO SYMULATORA SK-1 PLUTONU KTO ROSOMAK

Użytkownicy

Załogi pojazdów KTO Rosomak, jednostki
wojskowe prowadzące szkolenia taktyczne,
Ośrodek Badawczo-Rozwojowy Urządzeń
Mechanicznych „OBRUM”.

Kierownik Zespołu

dr hab. inż. Andrzej Najgebauer
prof. WAT





WIRTUALNY SYSTEM DOSKONALENIA TAKTYKI OCHRONY GRANICY PAŃSTWOWEJ ORAZ KONTROLI RUCHU GRANICZNEGO



Wdrożenie

Wdrożony na zlecenie
Centrum Szkolenia Straży
Granicznej w Kętrzynie.



Oba moduły umożliwiają, w warunkach wirtualnej rzeczywistości, szkolenie kadry kierowniczej. W ramach ćwiczeń, Kierownicy Działań, np. Kierownicy Zmiany mogą prowadzić wieloosobowe ćwiczenia ukierunkowane m.in. na weryfikację procedur oraz decyzji przez nich podejmowanych (Symulator Sztabowy) czy też, w przypadku Symulatora Wysokiej Rozdzielczości, odbyć szkolenie z zakresu pirotechnika w porcie lotniczym, szkolenie Kierownika Zmiany lub funkcjonariuszy I linii Kontroli Ruchu Granicznego na drogowym lub kolejowym przejściu granicznym wraz z obsługą zdarzeń kryzysowych, a nawet szkolenie kierującego działaniami blokadowymi w sytuacjach nadzwyczajnych.

www.wcy.wat.edu.pl



WIRTUALNY SYSTEM DOSKONALENIA TAKTYKI OCHRONY GRANICY PAŃSTWOWEJ ORAZ KONTROLI RUCHU GRANICZNEGO

Użytkownicy

Funkcjonariusze Straży Granicznej, kadra kierownicza Centrum Szkolenia Straży Granicznej.

Kierownik Zespołu

gen. bryg. dr inż. Mariusz Chmielewski





SYSTEM INFORMATYCZNEGO WSPARCIA ROZWOJU ZDOLNOŚCI ORAZ IDENTYFIKACJI POTRZEB OPERACYJNYCH SZRP PK. ZDOLNOŚCI



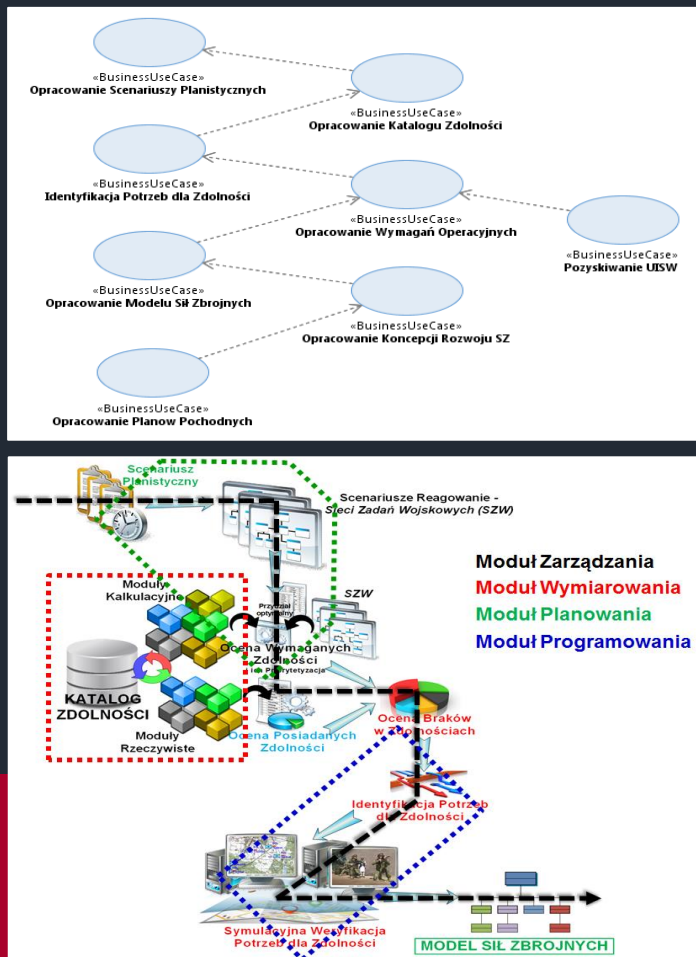
Wdrożenie

Wdrożony w celu wsparcia procesu planowania i programowania (PiP) rozwoju Sił Zbrojnych Rzeczypospolitej Polskiej.

System ZDOLNOŚCI jest kompleksowym rozwiązaniem informatycznym, które integruje różnorodne moduły funkcjonalne. Każdy z modułów odpowiada za poszczególne etapy procesu, zapewniając spójność danych i dokumentów oraz ułatwiając równoległą pracę osób funkcyjnych. Moduły funkcjonalne systemu wsparcia PiP rozwoju SZRP obejmują: Moduł Zarządzania, Moduł Wymiarowania, Moduł Planowania i Moduł Programowania (Symulator Działań Zbrojnych).



www.wcy.wat.edu.pl



SYSTEM INFORMATYCZNEGO WSPARCIA ROZWOJU ZDOLNOŚCI ORAZ IDENTYFIKACJI POTRZEB OPERACYJNYCH SZRP

Użytkownicy

Siły Zbrojne RP, Ministerstwo Obrony Narodowej,
jednostki odpowiedzialne za rozwój i utrzymanie
zdolności operacyjnych.

Kierownik Zespołu

dr hab. inż. Andrzej Najgebauer
prof. WAT





SYSTEM SEMANTYCZNEGO POSZUKIWANIA INFORMACJI I ZARZĄDZANIA WIEDZĄ W OBSZARZE ZAGINIĘĆ I POSZUKIWANIA OSÓB



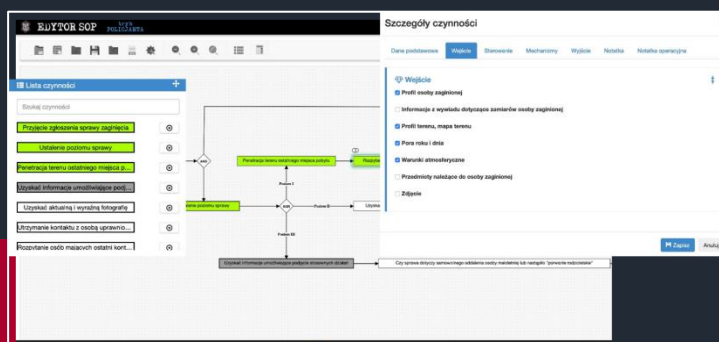
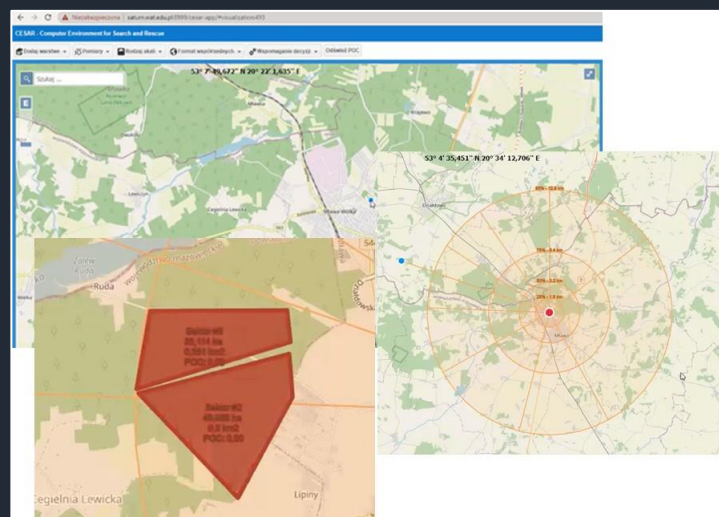
Wdrożenie

Zrealizowany przez
konsorcjum: Wyższa Szkoła
Policji w Szczytnie, Wojskowa
Akademia Techniczna oraz
Transition Technologies S.A.
Finansowany przez NCBiR
na zlecenie Komendy
Główniej Policji

Celem systemu było stworzenie centralnej bazy danych oraz narzędzia wspomagającego semantyczne poszukiwanie informacji i zarządzanie wiedzą w zakresie zaginięć i poszukiwań osób. Rozwiązanie zbudowano w architekturze wielowarstwowej, obejmującej różnorodne moduły funkcjonalne: Moduł Analizy Danych, Moduł Interfejsu Użytkownika, Moduł Obsługi Składu Danych, Moduł Wnioskowania Geo-lokalizacyjnego i Wizualizacji Przestrzennej i Moduł Planowania Poszukiwań.



www.wcy.wat.edu.pl



SYSTEM SEMANTYCZNEGO POSZUKIWANIA INFORMACJI I ZARZĄDZANIA WIEDZĄ W OBSZARZE ZAGINIĘĆ I POSZUKIWANIA OSÓB

Użytkownicy

Komenda Główna Policji

Kierownik Zespołu

dr hab. inż. Ryszard Antkiewicz
prof. WAT





SYSTEM WSPOMAGAJĄCY ĆWICZENIA SYMULACYJNE I USPRAWNIAJĄCY PROCEDURY DZIAŁANIA INSPEKTORÓW SANITARNYCH W PRZYPADKU ZATRUĆ I EPIDEMII PRZENOSZONYCH DROGĄ POKARMOWĄ



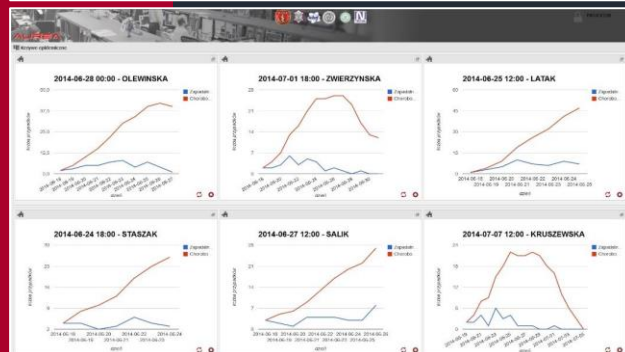
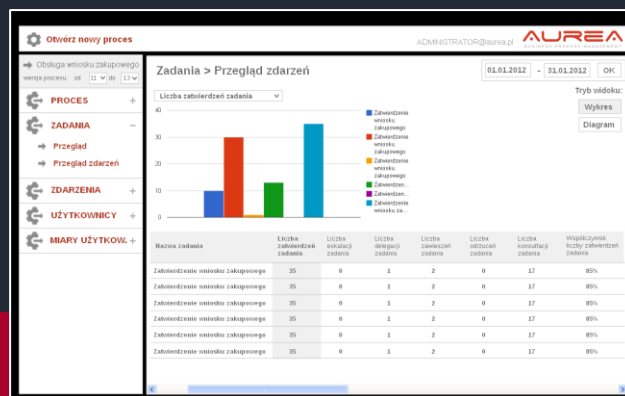
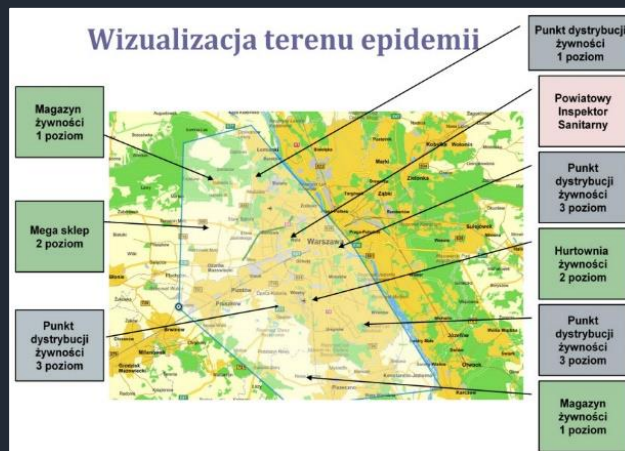
Wdrożenie

Wdrożony na potrzeby służb sanitarnych celu wspomagania organizacji ćwiczeń symulacyjnych.

Służy do modelowania i symulacji procesów oraz trenowania procedur wspomaganych komputerowo w zakresie zarządzania bezpieczeństwem żywności.

Wspomaga organizację ćwiczeń symulacyjnych dla służb sanitarnych (inspektorów Sanepid) w celu praktycznego wykorzystania i ćwiczenia procedur i działań podejmowanych po zaistnieniu informacji o możliwym zakażeniu żywności.





SYSTEM WSPOMAGAJĄCY ĆWICZENIA SYMULACYJNE I USPRAWNIAJĄCY PROCEDURY DZIAŁANIA INSPEKTORÓW SANITARNYCH W PRZYPADKU ZATRUĆ I EPIDEMII PRZENOSZONYCH DROGĄ POKARMOWĄ

Użytkownicy

Oddziały powiatowe SANEPID

Kierownik Zespołu

dr hab. inż. Tadeusz Nowicki
prof. WAT





SYSTEM WSPOMAGAJĄCY DECYZJE TERAPEUTYCZNE PACJENTÓW Z NIEWYDOLNOŚCIĄ SERCA „AMULET”



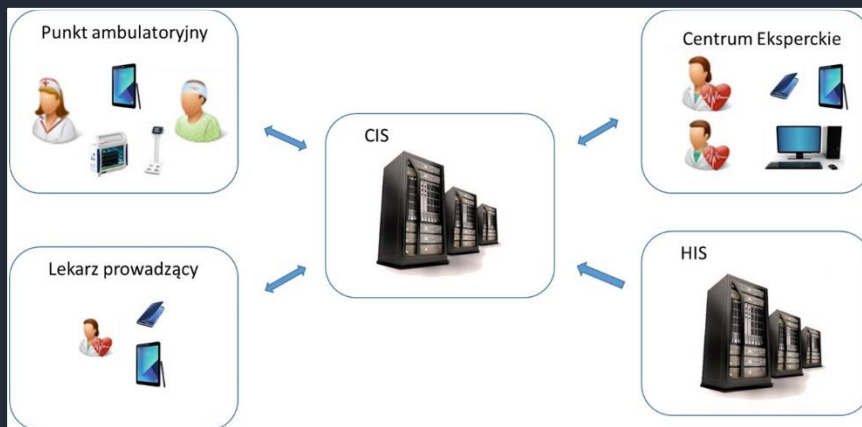
Wdrożenie

Wdrożony w celu wsparcia terapii chorób serca.
Uczestnicy projektu: WIM, WAT, UM we Wrocławiu, UM w Gdańsku, 4 Wojskowy Szpital Kliniczny we Wrocławiu, Grupa Łukasiewicz-ITAM, Grupa Casus BTL.



System wykorzystuje nowoczesne metody nieinwazyjnej oceny klinicznej. Jest odpowiedzią na potrzeby lekarzy i pacjentów. Jej podstawą jest możliwość kontroli parametrów pracy serca za pomocą wyspecjalizowanych urządzeń obsługiwanych przez personel medyczny oraz małego urządzenia mobilnego obsługiwanego przez pacjenta. Urządzenie przesyła wyniki pomiarów do systemu, do którego dostęp ma personel medyczny i pacjent.

www.wcy.wat.edu.pl



SYSTEM WSPOMAGAJĄCY DECYZJE TERAPEUTYCZNE PACJENTÓW Z NIEWYDOLNOŚCIĄ SERCA „AMULET”

Użytkownicy

Zespoły szpitalno-lecznicze

Kierownik Zespołu

Prof. dr hab. inż. Andrzej Walczak



INSTYTUT TELEINFORMATYKI I CYBERBEZPIECZEŃSTWA

struktura i misja



Instytut Teleinformatyki i Cyberbezpieczeństwa (ITC) powstał w 1994 roku. W latach 1994–2003 funkcjonował pod nazwą Instytut Automatyki i Robotyki, a od 2003 do 2019 jako Instytut Teleinformatyki i Automatyki. Wywodzi się z połączenia katedr: Budowy i Eksploatacji Systemów Komputerowych oraz Cybernetyki Technicznej, których historia sięga 1968 roku. Główne obszary działalności Instytutu to kształcenie studentów na poziomie inżynierskim, magisterskim i doktoranckim oraz prowadzenie badań naukowych. W ramach ITC działają trzy zakłady: Zakład Bezpieczeństwa Teleinformatycznego, Zakład Inteligentnych Systemów Maszynowych oraz Zakład Systemów Komputerowych, które obejmują szeroki zakres działalności naukowo-dydaktycznej.

Kontakt:

tel.: 261-838-703

INSTYTUT TELEINFORMATYKI I CYBERBEZPIECZEŃSTWA

działalność edukacyjna i infrastruktura badawcza



Działalność edukacyjna instytutu obejmuje programy studiów inżynierskich, magisterskich, doktoranckich, podyplomowych (w tym MBA) oraz udział w programie Erasmus+. Na kierunku Informatyka Instytut profiluje 4 specjalności: bezpieczeństwo systemów teleinformatycznych, sieci teleinformatyczne, internetowe technologie multimedialne oraz mobilne systemy komputerowe. Na kierunku Kryptologia i cyberbezpieczeństwo odpowiada za specjalność cyberobrona. ITC współpracuje także z globalnymi liderami technologicznymi, oferując studentom udział w programach Cisco, RedHat, Microsoft oraz Palo Alto i in.

Infrastruktura badawcza ITC obejmuje 3 zakłady (Bezpieczeństwa Teleinformatycznego, Inteligentnych Systemów Maszynowych i Systemów Komputerowych) oraz Laboratorium Teleinformatyki i Cyberbezpieczeństwa.

Kontakt:
tel.: 261-838-703

INSTYTUT TELEINFORMATYKI I CYBERBEZPIECZEŃSTWA

osiągnięcia naukowe



W ostatnich latach pracownicy instytutu brali udział w licznych międzynarodowych konferencjach naukowych, takich jak MILCOM, IEEE WFIoT czy IBIMA, prezentując wyniki swoich badań oraz zdobywając wyróżnienia za innowacyjność i jakość prezentacji.

Studenci ITC również odnoszą sukcesy, biorąc udział w prestiżowych wydarzeniach takich jak STEM CTF: Cyber Challenge czy SECCON CTF, gdzie zdobywali czołowe miejsca.

Osiągnięcia pracowników i studentów obejmują także aktywny udział w praktycznych ćwiczeniach takich jak Locked Shields czy CWIX, gdzie demonstrują swoje umiejętności w praktycznych sytuacjach związanych z cyberbezpieczeństwem i technologiami informatycznymi.

Kontakt:

tel.: 261-838-703



WYZWANIA STOJĄCE PRZED INSTYTUTEM

dr inż. Tomasz Malinowski, prof. WAT
dyrektor

Instytut Teleinformatyki i Cyberbezpieczeństwa od 30 lat rozwija się w takich dziedzinach nauk technicznych, jak cybernetyka techniczna, sztuczna inteligencja, sieci teleinformatyczne z konwergencją usług oraz cyberbezpieczeństwo. Kluczowe cele Instytutu obejmują modernizację laboratoriów, rozwój współpracy z ośrodkami badawczymi w kraju i za granicą, integrację badań z dydaktyką oraz poszerzanie oferty edukacyjnej dla przyszłych specjalistów wojska i instytucji cywilnych. Instytut koncentruje się na projektowaniu nowoczesnych i bezpiecznych systemów teleinformatycznych, rozwijaniu technik analizy danych oraz wspomagania decyzji, organizuje seminaria, konferencje oraz nowoczesne szkolenia, jednocześnie podnosząc kwalifikacje zawodowe pracowników, aby sprostać wymaganiom współczesnych technologii.



BEZPIECZNA STACJA DO ZASTOSOWAŃ SPECJALNYCH BSDZS



Wdrożenie

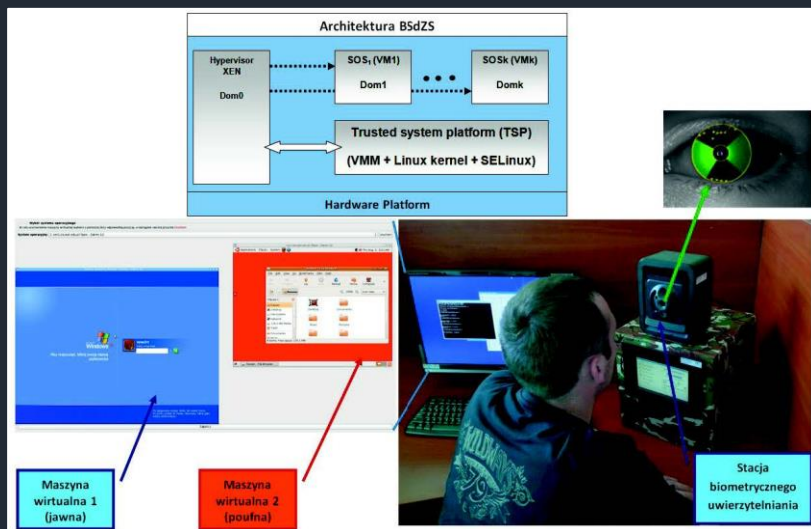
Zrealizowany przez
konsorcjum: Wydział
Cybernetyki WAT,
Filbico Sp. z o.o., Wojskowy
Instytut Łączności, NASK.



BSdZS to specjalistyczny system komputerowy, który umożliwia równoczesne uruchamianie wielu instancji systemów operacyjnych (maszyn wirtualnych) na jednym komputerze, zapewniając kontrolę dostępu, ochronę kryptograficzną i nadzór nad przepływem danych.

BSdZS obejmuje bezpieczną platformę systemową, specjalne wersje systemów Windows i Linux oraz rozwiązania do ochrony danych i bezpiecznej konfiguracji. Każda instancja systemu tworzy odrębną domenę bezpieczeństwa, pozwalając na przetwarzanie danych o różnych poziomach klasyfikacji.

www.wcy.wat.edu.pl



BEZPIECZNA STACJA DO ZASTOSOWAŃ SPECJALNYCH BSDZS

Użytkownicy

Instytucje państwowe, ministerstwa, agencje rządowe i służby, w których przetwarza się informacje niejawne

Kierownik Zespołu

dr hab. inż. Zbigniew Zieliński
prof. WAT





ZBIÓR ROZWIĄZAŃ W ZAKRESIE WIDZENIA KOMPUTEROWEGO



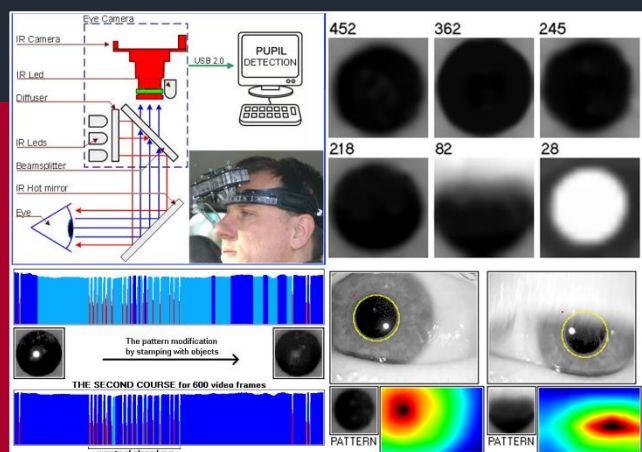
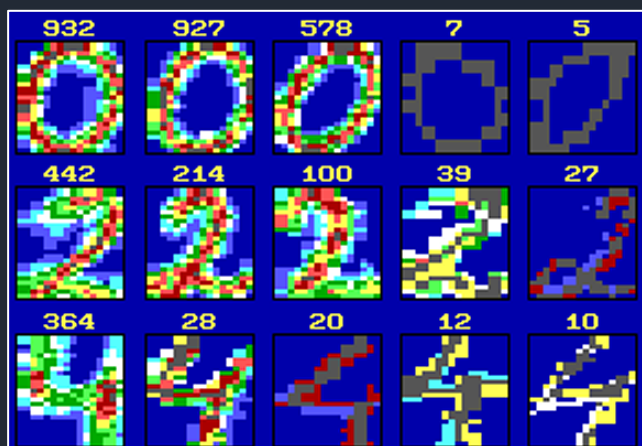
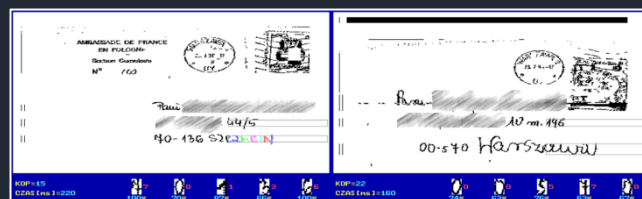
Wdrożenie

Poczta Polska – pierwsze
zastosowanie.

Widzenie komputerowe to technologia umożliwiająca komputerom rozpoznawanie i analizę obrazów przy użyciu urządzeń takich jak skanery czy kamery. Obrazy rejestrowane są przez kamerę, a następnie przetwarzane cyfrowo w celu ich analizy. Technologię tę wykorzystuje się m.in. do identyfikacji podpisu odręcznego, rozpoznawania twarzy w smartfonach oraz w medycznej analizie obrazów.



www.wcy.wat.edu.pl



ZBIÓR ROZWIĄZAŃ W ZAKRESIE WIDZENIA KOMPUTEROWEGO

Użytkownicy

Medycyna, wojsko, robotyka, systemy
monitoringu i nadzoru, logistyka, bankowość
i poczta.

Kierownik Zespołu

dr inż. Witold Żorski





CZUJNIK DO MONITOROWANIA ZABURZEŃ CZYNNOŚCI GRUCZOŁÓW MEIBOMA



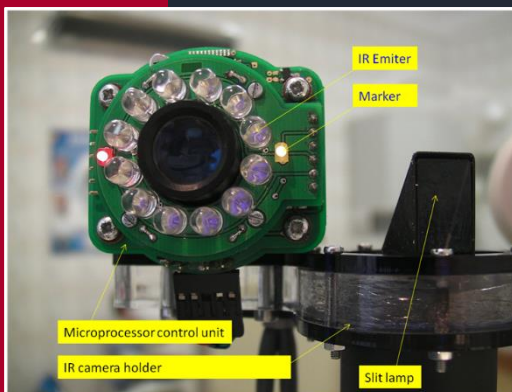
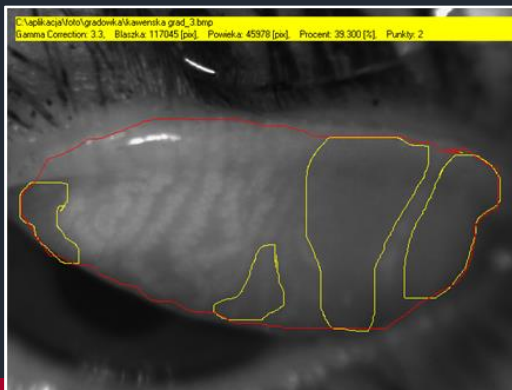
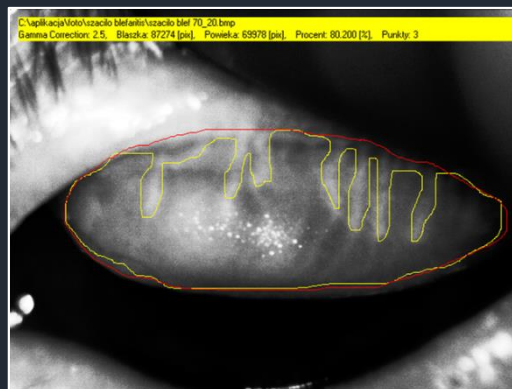
Wdrożenie

Opracowanie urządzeń
i testów diagnostycznych
wystarczających do
jednoznacznego określenia
stopnia dysfunkcji gruczołów.



Meibografia pozwala na jednoczesną ocenę liczby gruczołów mięszkowych oraz ich ukrwienia. Czujnik pozwala na bezinwazyjne badanie gruczołów rzęskowych. Konstrukcja czujnika oparta jest na algorytmach przetwarzania obrazu oraz detektorze (kamera pracująca w bliskiej podczerwieni) i precyzyjnie sterowanym oświetlaczu IR. Wykorzystując zjawisko pochłaniania przez krew ciepła generowanego przez światło w zakresie bliskiej podczerwieni, uzyskujemy obrazowanie gruczołów rzęskowych, które podlega ocenie.

www.wcy.wat.edu.pl



CZUJNIK DO MONITOROWANIA ZABURZEŃ CZYNNOŚCI GRUCZOŁÓW MEIBOMA

Użytkownicy

Kliniki okulistyczne, specjaliści zajmujący się
diagnostyką chorób oczu

Kierownik Zespołu

dr hab. inż. Krzysztof Murawski
prof. WAT





OPTYCZNY SENSOR DO OCHRONY DZIEŁ SZTUKI



Wdrożenie

Zapewnienie precyzyjnej ochrony obiektów przed nieautoryzowanym dostępem lub manipulacją.

Czujnik wykorzystuje obrazowanie laserowe realizowane w paśmie podczerwieni. Składa się z toru optycznego, miniaturowej kamery, oświetlacza laserowego, układu przetwarzania i analizy obrazu, mikrokontrolera i układu kodowania oraz transmisji danych. W efekcie powstał wizyjny, bezdotykowy i zintegrowany czujnik do indywidualnej ochrony obiektu wykonanego z materiałów takich jak: tkanina, marmur, szkło, metal, drewno, itp.



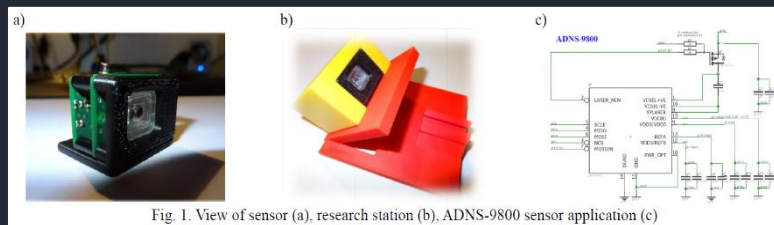


Fig. 1. View of sensor (a), research station (b), ADNS-9800 sensor application (c)

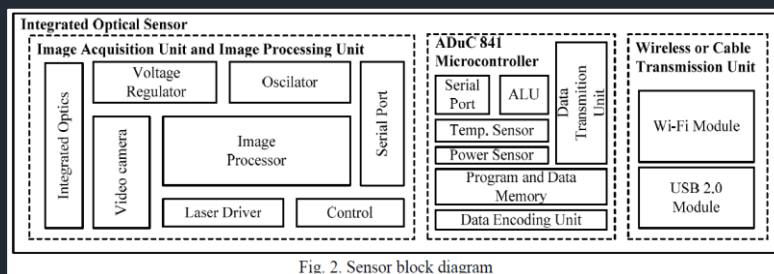


Fig. 2. Sensor block diagram

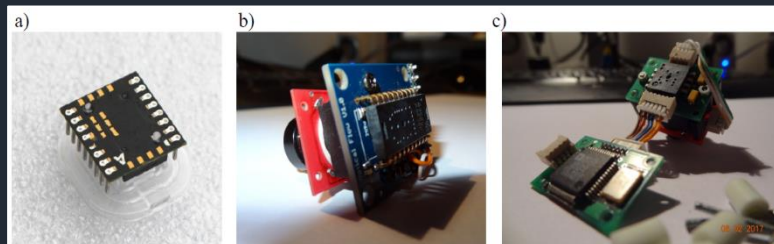


Fig. 3. View of sensor with optics: ADNS-9800 (a), ADNS-3080 (b), ADNS-5020 and ADuC841 (c)

OPTYCZNY SENSOR DO OCHRONY DZIEŁ SZTUKI

Użytkownicy

Muzea, galerie sztuki, prywatni kolekcjonerzy,
instytucje przechowujące cenne dokumenty

Kierownik Zespołu

dr hab. inż. Krzysztof Murawski
prof. WAT





TECHNIKA REKONSTRUKCJI KSZTAŁTU MEMBRANY WIOTKIEJ POMPY WSPOMAGANIA SERCA W OPARCIU O INTERPOLACJĘ PRZESTRZENNĄ

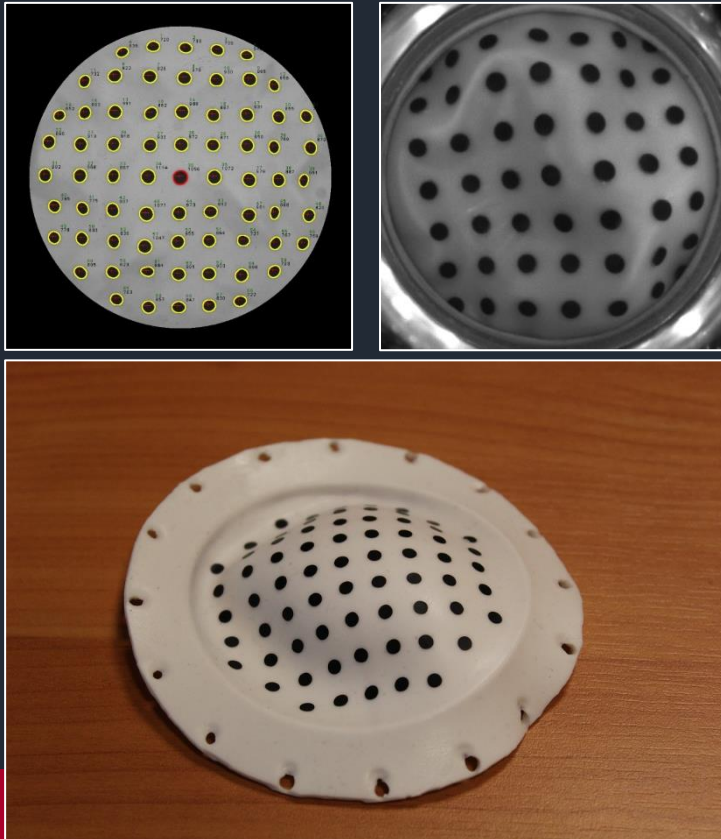


Wdrożenie

Rozwiązanie problemu
wyznaczenia chwilowej
objętości wyrzutowej krwi
z komory krwistej pompy
typu pulsacyjnego,
wspomagającej pracę serca.



W metodzie DFD chwilowa objętość wyrzutowa krwi z komory wyznaczana jest na podstawie chwilowego kształtu 3D powierzchni membrany pompującej krew. Metoda została opracowana do wizyjnego pomiaru odległości. Zastosowano ją do wyznaczania kształtu powierzchni wiotkiej membrany pozaustrojowej pulsacyjnej pompy wspomaganie serca. W celu przyspieszenia obliczeń i miniaturyzacji czujnika wizyjnego, konieczne było zastosowanie „odpornej” metody rekonstrukcji kształtu membrany opartej na interpolacji przestrzennej.



TECHNIKA REKONSTRUKCJI KSZTAŁTU MEMBRANY WIOTKIEJ POMPY WSPOMAGANIA SERCA W OPARCIU O INTERPOLACJĘ PRZESTRZENNĄ

Użytkownicy

Kliniki kardiologiczne, ośrodki badawcze
specjalizujące się w technologiach wspomaganie
pracy serca

Kierownik Zespołu

dr hab. inż. Krzysztof Murawski
prof. WAT





SYSTEM POMIARU WASKULARYZACJI ROGÓWKI



Wdrożenie

Opracowanie nowej,
specjalizowanej, techniki
segmentacji obrazu
kolorowego.

Segmentację obrazu przeprowadzano w celu optycznego wyznaczenia położenia naczyń krwionośnych na powierzchni rogówki i pomiaru stopnia jej unaczynienia (waskularyzacji). Metoda oparta jest na analizie obrazu rogówki uzyskanego w zakresie światła widzialnego. Z medycznego punktu widzenia istotne jest opracowanie wskaźnika i metody pomiaru stopnia waskularyzacji rogówki. Wskaźnik taki pozwoli oceniać rezultaty zastosowanej metody leczenia a także obiektywnie przeprowadzać diagnostykę obrazową.



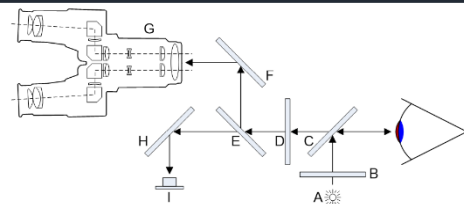


Fig. 2. System observation of fluorescence structures of the eye [14]: white light source (A); bandpass filter $\lambda_{CWL} \in [465\text{nm}, 490\text{nm}]$ (B); prism (C); bandpass filter $\lambda_{CWL} \in [520\text{nm}, 530\text{nm}]$ (D); 50R/50T plate beam splitter (E); reflecting mirror (H, F); CCD camera (I); eyepiece (G)

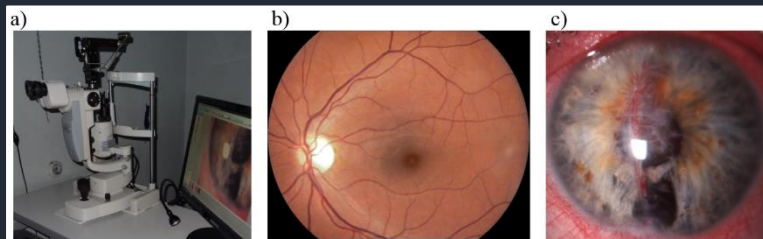


Fig. 1. Stanowisko pozyskiwania zdjęć: lampa szczelinowa z sensorem (a) naczynia krwionośne siatkówki (b), naczynia krwionośne rogówki (c).

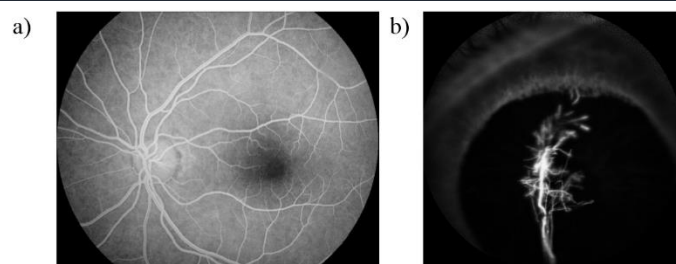


Fig. 3. Angiografia fluoresceinowa naczyń z Fig. 1: siatkówki (a), rogówki (b)

SYSTEM POMIARU WASKULARYZACJI ROGÓWKI

Użytkownicy

Kliniki okulistyczne, specjaliści zajmujący się
diagnostyką chorób oczu

Kierownik Zespołu

dr hab. inż. Krzysztof Murawski
prof. WAT





WIZYJNY SENSOR DO POMIARU OBJĘTOŚCI CIECZY

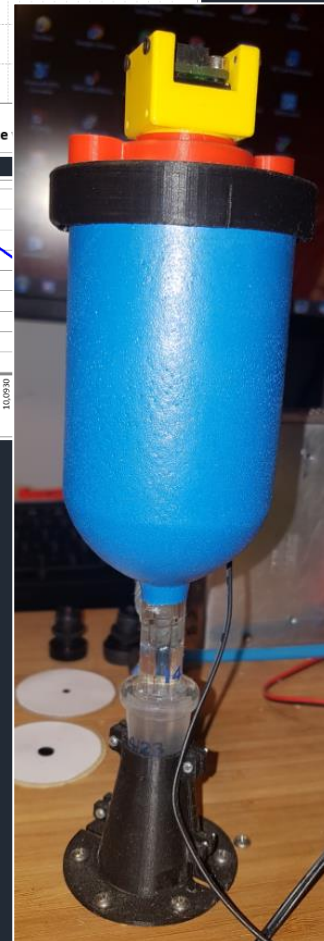


Wdrożenie

Stworzenie video-manometru i praktyczne zastosowanie nowej metody pomiaru ciśnienia, opartej na wizyjnym pomiarze zmian szerokości markera umieszczonego na powierzchni odkształcanej membrany.

Zastosowanie teorii soft-sensorów umożliwiło wykonanie czujnika, który wielkość objętości cieczy wyznacza na podstawie tylko jednego obrazu pozyskanego z miniaturowej kamery wideo. Umieszczona wewnątrz sensora kamera stanowi jednocześnie układ pomiarowy i układ umożliwiający zdalną diagnostykę sensora. Dzięki zastosowaniu układu wizyjnego sensor może pracować zarówno w dzień jak i w nocy, także przy zmiennych warunkach ciśnienia, temperatury i oświetlenia.





W medycynie, układach sterowania oraz systemach transportu gazu, charakteryzując się optymalnymi właściwościami do pracy w środowiskach zagrożonych wybuchem oraz medycznym.

dr hab. inż. Krzysztof Murawski
prof. WAT





SENSOR WIZYJNY DO MONITOROWANIA I POMIARU CIŚNIENIA GAZU



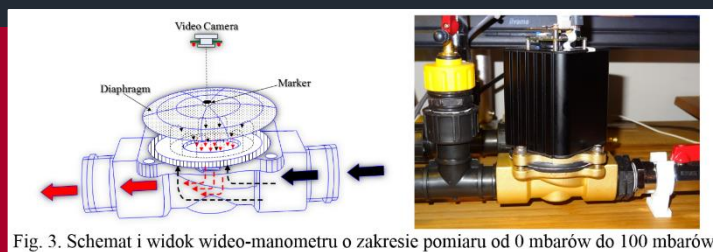
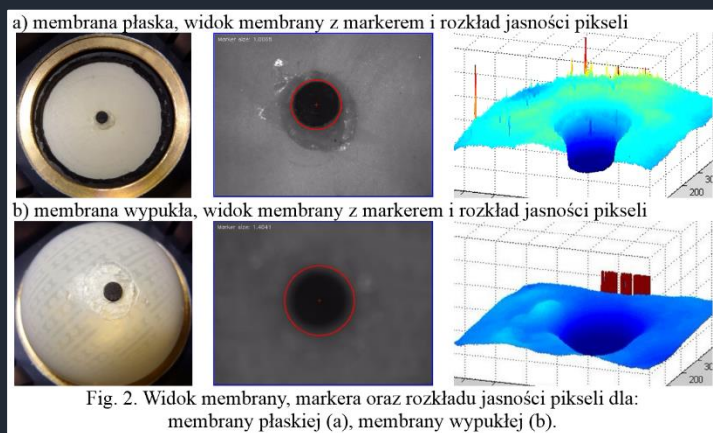
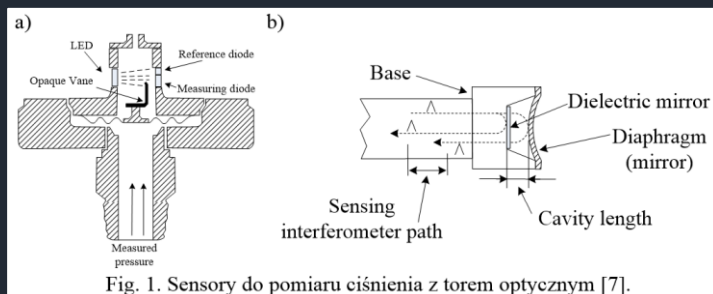
Wdrożenie

Stworzenie wideo-manometru do precyzyjnego pomiaru ciśnienia gazów poprzez wizyjny pomiar zmian szerokości markera na odkształcanej membranie.



Zaproponowana technika oferuje szereg zalet, takich jak: bezkontaktowy pomiar, izolacja galwaniczna sensora od komory ciśnienia, wysoka czułość, powtarzalność i dokładność pomiarów, odporność na zakłócenia, oraz prostota konstrukcji. Sensor jest mały, skalowalny, i może być stosowany z różnymi typami membran, co obejmuje membrany płaskie, faliste, mieszka oraz kapsuły. Dodatkowo, posiada funkcję wizyjnej autodiagnostyki w czasie rzeczywistym, co jest unikalną cechą wśród czujników ciśnienia optycznego.

www.wcy.wat.edu.pl



SENSOR WIZYJNY DO MONITOROWANIA I POMIARU CIŚNIENIA GAZU

Użytkownicy

Potencjalne zastosowania sensora obejmują medycynę, systemy sterowania oraz transport gazu. Jest również idealny do zastosowań w środowiskach wymagających odporności na wybuchy oraz w medycynie.

Kierownik Zespołu

dr hab. inż. Krzysztof Murawski
prof. WAT





WIZYJNY SENSOR DLA PRECYZYJNEJ KONTROLI PRACY VAD



Wdrożenie

Opracowanie wizyjnego sensora oraz metody określania objętości wyrzutowej (SV) pulsacyjnej, pozaustrojowej, pneumatycznej pompy wspomagania pracy serca (VAD).



Zaproponowana technika opiera się na analizie kształtu 3D powierzchni membrany wiotkiej na podstawie jednego zdjęcia, co pozwala na szybkie i precyzyjne określenie objętości wyrzutowej krwi. W badaniach użyto silikonowej membrany kompozytowej z wkładem włókniny, charakteryzującej się elastycznością i wytrzymałością. Opracowany sensor oraz metoda osiągnęły średni błąd bezwzględny pomiaru SV wynoszący 1,83 ml przy pojemności komory krwistej 120 ml i maksymalnej objętości wyrzutowej 70 ml, oraz średni błąd względny nie przekraczający 1,5% w całym zakresie pomiarowym.

www.wcy.wat.edu.pl

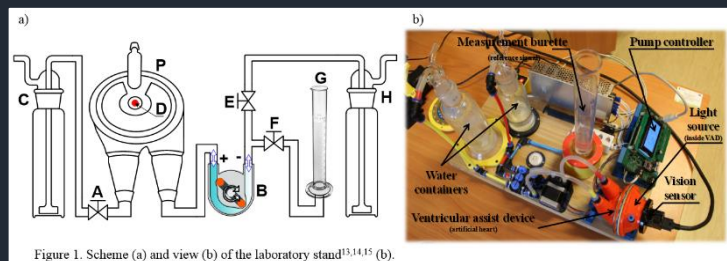


Figure 1. Scheme (a) and view (b) of the laboratory stand^{13,14,15} (b).

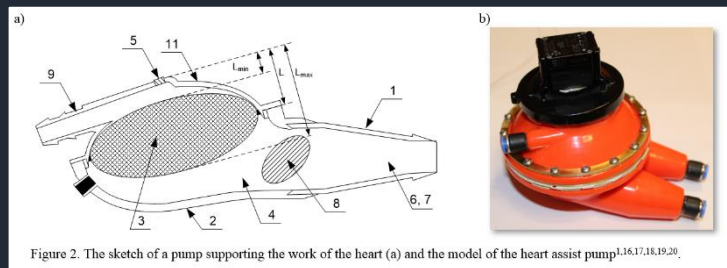


Figure 2. The sketch of a pump supporting the work of the heart (a) and the model of the heart assist pump^{1,16,17,18,19,20}.

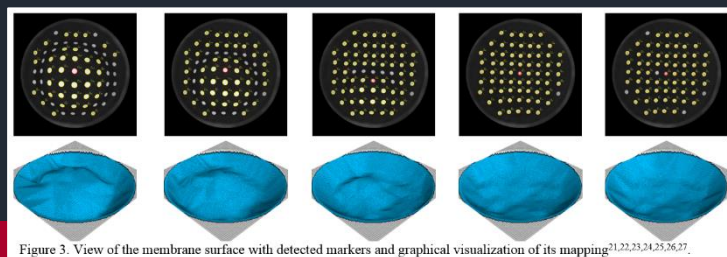


Figure 3. View of the membrane surface with detected markers and graphical visualization of its mapping^{21,22,23,24,25,26,27}.

WIZYJNY SENSOR DLA PRECYZYJNEJ KONTROLI PRACY VAD

Użytkownicy

W medycynie, umożliwiając precyzyjne monitorowanie pracy serca oraz pomiar objętości wyrzutowej krwi w czasie rzeczywistym.

Kierownik Zespołu

dr hab. inż. Krzysztof Murawski
prof. WAT





BADANIE WPŁYWU ŚWIATŁA NA WYNIK REKONSTRUKCJI 3D MEMBRANY WIOTKIEJ POMPY WSPOMAGANIA PRACY SERCA

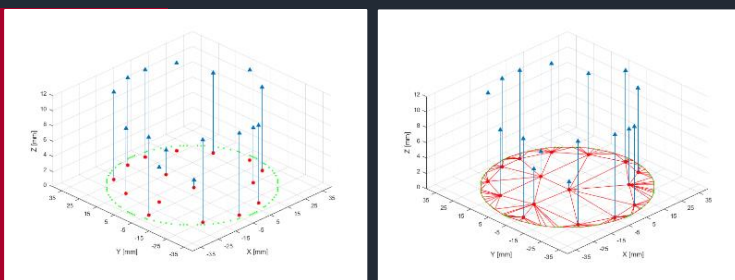
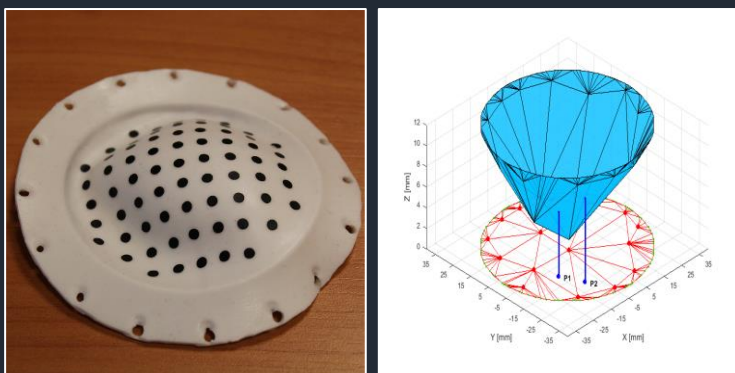
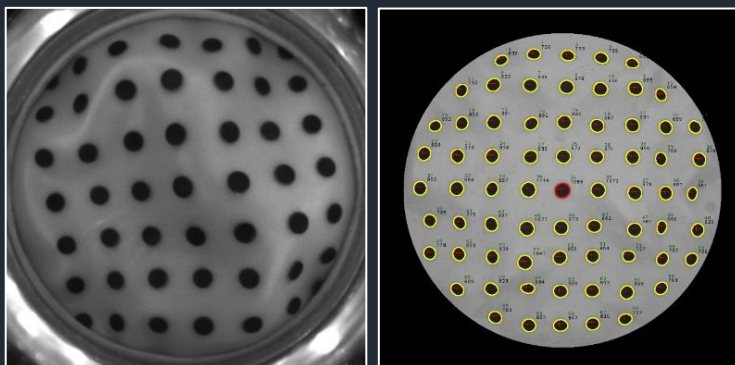


Wdrożenie

Określenie wpływu oświetlenia na wynik rekonstrukcji 3D kształtu powierzchni membrany wiotkiej pompy wspomagania pracy serca (VAD).



Badania przeprowadzono z użyciem autorskiego czujnika wizyjnego, który obserwuje ruchy membrany i rekonstruuje jej kształt na podstawie oświetlenia i obrazu z kamery. Zastosowano nowe modele pomp VAD, wykonane techniką druku przestrzennego (rys. 2) oraz odlewniczą (rys. 3), z kompozytową membraną wiotką (rys. 5, 7). Membrany są separowane pomiędzy komorą krwistą a pneumatyczną, co widoczne jest na rysunkach 6. Badania potwierdziły, że użyte oświetlenie istotnie wpływa na dokładność rekonstrukcji kształtu membrany, kluczowego dla precyzyjnego pomiaru SV i CO.



BADANIE WPŁYWU ŚWIATŁA NA WYNIK REKONSTRUKCJI 3D MEMBRANY WIOTKIEJ POMPY WSPOMAGANIA PRACY SERCA

Użytkownicy

Zastosowanie w dalszym rozwoju technologii
wspomagania pracy serca oraz w medycznych
systemach monitorowania funkcji serca.

Kierownik Zespołu

dr hab. inż. Krzysztof Murawski
prof. WAT



INSTYTUT MATEMATYKI I KRYPTOLOGII

struktura i misja



Instytut Matematyki i Kryptologii powstał w 1994 roku jako Instytut Matematyki i Badań Operacyjnych, z połączenia Katedry Matematyki, istniejącej od 1951 roku i części Katedry Badań Operacyjnych, a od 2003 roku działa pod obecną nazwą. Zatrudnia 69 nauczycieli akademickich, w tym pięciu profesorów, pięciu doktorów habilitowanych i 45 doktorów. Instytut dzieli się cztery zakłady: Zakład Analizy Matematycznej i Matematyki Stosowanej, Zakład Algebry i Teorii Liczb, Zakład Probabilistyki, Zakład Kryptologii, oraz Laboratorium Badawcze Kryptologii i Pracownia Matematyki Stosowanej.

Instytut kształci na studiach licencjackich, inżynierskich, magisterskich i doktoranckich w zakresie matematyki oraz kryptologii i cyberbezpieczeństwa.

Kontakt:

tel.: 261 838 740

INSTYTUT MATEMATYKI I KRYPTOLOGII

działalność edukacyjna i infrastruktura badawcza



Głównymi zadaniami dydaktycznymi realizowanymi przez Instytut jest nauczanie matematyki wyższej wszystkich studentów Wojskowej Akademii Technicznej oraz profilowanie specjalności systemy kryptograficzne kierunku studiów kryptologia i cyberbezpieczeństwo, współprowadzonego przez wszystkie trzy instytuty Wydziału Cybernetyki.

Instytut wykorzystuje w badaniach i nauczaniu komputery i oprogramowanie zgromadzone w Laboratorium Badawczym Kryptologii (w tym w dwóch laboratoriach dydaktycznych) oraz w dwóch laboratoriach matematyki stosowanej, a także indywidualny sprzęt pracowników.

Pracownicy Instytutu angażują się również w działania popularyzujące naukę, prowadząc wykłady dla uczniów szkół średnich oraz organizując Konkurs Matematyczny imienia gen. dyw. prof. dr hab. inż. Sylwestra Kaliskiego.

Kontakt:

tel.: 261 838 740

INSTYTUT MATEMATYKI I KRYPTOLOGII

osiągnięcia naukowe



Pracownicy Instytutu prowadzą badania w zakresie matematyki i jej zastosowań w technice oraz w zakresie kryptologii z zastosowaniami i cyberbezpieczeństwa. Regularnie publikują wyniki w międzynarodowych i krajowych czasopismach naukowych (od powstania instytutu około pięciuset artykułów) oraz prezentują je na międzynarodowych i krajowych konferencjach naukowych.

Na podstawie wyników badań uzyskują stopnie naukowe. Ich prace zostały nagrodzone wieloma medalami na polskich i międzynarodowych wystawach wynalazków.

Kontakt:

tel.: 261 838 740



WYZWANIA STOJĄCE PRZED INSTYTUTEM

dr Marek Kojdecki, prof. WAT
dyrektor Instytutu

Kontynuacja i rozwój badań w obszarze matematyki i jej zastosowań, w tym we współpracy z jednostkami badawczymi w Wojskowej Akademii Technicznej i poza nią.

Kontynuacja i rozwój badań w obszarze kryptologii i jej zastosowań, w tym prace wdrożeniowe z zastosowaniem nowych technologii, także w konsorcjach z zewnętrznymi partnerami.

Utrzymanie wysokiego poziomu nauczania matematyki i stworzenie informatycznego systemu wsparcia dla nauczycieli i studentów.

Profilowanie i aktualizowanie treści nauczania specjalności systemy kryptograficzne z wykorzystaniem najnowszej wiedzy i wyników badań w IMK.



UNIWERSALNY SYSTEM WCZESNEJ DETEKCJI I UNIESZKODLIWIANIA ZŁOŚLIWEGO OPROGRAMOWANIA TYPU RANSOMWARE



Wdrożenie

Skuteczne zwalczanie
złośliwego oprogramowania
typu ransomware.

Wykorzystuje zaawansowane technologie, aby nie tylko reagować na znane zagrożenia, lecz także przewidywać i neutralizować nowe formy ataków. Głównym celem projektu jest zapewnienie szybkiego i skutecznego reagowania na nowe, nieznane warianty ransomware, które mogą poważnie zagrażać bezpieczeństwu danych i funkcjonowania instytucji.



www.wcy.wat.edu.pl





Wojskowa Akademia Techniczna



Rzeczpospolita Polska



Narodowe Centrum Badań i Rozwoju

Wojskowa Akademia Techniczna realizuje projekt „Uniwersalny system wczesnej detekcji i unieszkodliwiania złośliwego oprogramowania typu ransomware”

AKRONIM: USEDRans

Liderem projektu jest TIMSI Sp. z o.o.

Projekt współfinansowany przez Narodowe Centrum Badań i Rozwoju w ramach Programu Badań Naukowych i Prac Rozwojowych CyberSecident – Cyberbezpieczeństwo i e-Tożsamość.

Umowa o dofinansowanie: CYBERSECIDENT/490737/IV/NCBR/2021

Wartość projektu: 4 505 360,00 zł

Wartość dofinansowania: 3 690 074,00 zł



UNIWERSALNY SYSTEM WCZESNEJ DETEKЦИИ I UNIESZKODLIWIANIA ZŁOŚLIWEGO OPROGRAMOWANIA TYPU RANSOMWARE

Użytkownicy

Społeczne zaangażowanie poprzez bezpłatne udostępnienie rozwiązań każdemu obywatelowi RP do celów niekomercyjnych.

Kierownik Zespołu

dr Michał Glet
dr Kamil Kaczyński





BUDOWA KOMPETENCJI PAŃSTWA W ZAKRESIE KRYPTOLOGII I CYBERBEZPIECZEŃSTWA – PROJEKT „ROTOR”



Wdrożenie

Konsorcjum na czele
z Wydziałem Cybernetyki
WAT (Instytut Matematyki
i Kryptologii); finansowany
przez NCBiR

Projekt niejawnny.

Jego celem była budowa kompetencji państwa w zakresie
kryptologii i cyberbezpieczeństwa.



www.wcy.wat.edu.pl



BUDOWA KOMPETENCJI PAŃSTWA W ZAKRESIE KRYPTOLOGII I CYBERBEZPIECZEŃSTWA – PROJEKT „ROTOR”

Użytkownicy

Informacja niejawna

Kierownik Zespołu

Informacja niejawna





IMPLEMENTACJA KRYPTOGRAFII POSTKWANTOWEJ -PROJEKT „ISSIP-PKI”



Wdrożenie

Realizowany przez
konsorcjum;
współfinansowany przez
NCBiR.

Realizowany w ramach programu dotyczącego obronności
i bezpieczeństwa państwa. Do prac nad projektem został powołany
specjalny zespół składający się z pracowników naukowych
Instytutu Matematyki i Kryptologii Wydziału Cybernetyki WAT.



www.wcy.wat.edu.pl



IMPLEMENTACJA KRYPTOGRAFII POSTKWANTOWEJ -PROJEKT „ISSIP-PKI”

Użytkownicy

Służby i urzędy państwa.

Kierownik Zespołu

mgr inż. Krzysztof Mańk



Wdrożenie

Współfinansowany przez
NCBiR w ramach programu
dotyczącego obronności
i bezpieczeństwa państwa,
realizowany przez
konsorcjum: WAT,
Zachodniopomorski
Uniwersytet Technologiczny
w Szczecinie, firma Unizeto
Technologies S.A.



Utworzono projekt modelu bezpiecznej architektury systemu
ochrony informacji niejawnej dla urządzeń mobilnych. Urządzenie
posiada szereg unikalnych cech, które umożliwiają zbudowanie
silnej długoterminowej przewagi konkurencyjnej na rynku
rozwiązań wspierających ochronę informacji.



**WOJSKOWA
AKADEMIA TECHNICZNA**

MOBILNE URZĄDZENIE DO OCHRONY INFORMACJI NIEJAWNEJ



Urządzenie do ochrony informacji niejawnej, realizujące funkcjonalności wynikające z wymagań modelu ORCON. Jego podstawę mają stanowić: zaawansowany moduł kryptograficzny klasy *secret protection* i polityki dostępu pozwalające na generowanie odpowiednich scenariuszy biznesowych ochrony informacji.

Kierownik projektu PBS1/B3/11/2012
Prof. dr hab. n. mat. inż. **Jerzy Gawinecki**
Instytut Matematyki i Kryptologii, Wydział Cybernetyki, WAT
Konsorcjum

Projekt dofinansowany ze środków NCBIR w latach 2012-15





Istotną cechą systemów informatycznych, którą obecnie należy brać pod uwagę podczas budowania mechanizmów ochrony informacji niejawnej jest mobilność nie tylko użytkowników informacji, ale także mobilność samej informacji. W takiej sytuacji pojawia się problem dotyczący skuteczności zabezpieczenia informacji niejawnych przechowywanych na urządzeniach mobilnych. Rozwiązanie sformułowanego problemu wymaga osiągnięcia dwóch celów: bezpieczeństwa mobilnej informacji oraz zwolnienia użytkowników z obowiązku nadzorowania każdej informacji znajdującej się w jego systemie. W praktyce oznacza to, że informacja mobilna powinna być chroniona i nadzorowana zgodnie z wymaganiami modelu kontroli dostępu ORCON. Najskuteczniejsze rozwiązanie problemu mobilności informacji w połączeniu z wymaganiami ORCON można uzyskać dzięki zastosowaniu kryptograficznych technik kontroli dostępu do zasobów, które zapewnią przechowywanie informacji na stacji w postaci zaszyfrowanej i odszyfrowanie jej tylko przez uprawnione podmioty (zgodnie z polityką dostępu). Na tym właśnie bazuje *Mobilne urządzenie do ochrony informacji niejawnej*, którego podstawę stanowią dwa elementy:

- specjalizowany moduł kryptograficzny klasy SP stanowiący źródło zaufania poprzez zapewnienie kontroli integralności kodu i danych konfiguracyjnych urządzenia.
- Struktury dostępu, które pozwolą generować odpowiednie mechanizmy ochrony informacji. Do tego celu wykorzystywane będą m.in. schematy szyfrowania grupowego, dowolnie predefiniowaną strukturą przywilejów.

Stworzone urządzenie składać się będzie z internetowej aplikacji oraz sprzętu, który swoim kształtem przypominał będzie pastylkę, która będzie podłączana do urządzenia mobilnego. To właśnie kolor tej pastylki (zielony- urządzenie bezpieczne, czerwony- urządzenie zhakowane) będzie stanowił dla użytkownika informację na temat bezpieczeństwa jego urządzenia.

Wydział Cybernetyki
Instytut Matematyki i Kryptologii
tel.: (+48 22) 683 96 87, fax: (+48 22) 683 79 19, e-mail: jgawinecki@wat.edu.pl

Military University of Technology, ul. gen. S. Kaliskiego 2, 00-908 Warszawa, POLAND
MUT Chancellor secretariat: phone: (+48 22) 683 90 03, fax: (+48 22) 683 76 60, e-mail: sekretariat.rektor@wat.edu.pl
MUT exchange: phone (+48 22) 683 90 00, fax: (+48 22) 683 99 01, www.wat.edu.pl

MOBILNE URZĄDZENIE DO OCHRONY INFORMACJI NIEJAWNEJ

Użytkownicy

Użytkownicy urządzeń mobilnych - do zapewnienia wysokiego poziomu ochrony informacji.

Kierownik Zespołu

prof. dr hab. n. mat. inż. Jerzy Gawinecki





BUDOWA OTWARTEJ PLATFORMY WIEDZY DLA SPOŁECZEŃSTWA NAUKOWEGO SYNAT



Wdrożenie

W ramach projektu SYNAT „Interdyscyplinarny system interaktywnej informacji naukowej i naukowo technicznej„.

Celem projektu było opracowanie koncepcji oraz wdrożenie sieciowej platformy hostingowej i komunikacyjnej dla zdigitalizowanej wiedzy wykorzystywanej przez badaczy, jednostki naukowe, studentów itp.



www.wcy.wat.edu.pl



BUDOWA OTWARTEJ PLATFORMY WIEDZY DLA SPOŁECZEŃSTWA NAUKOWEGO

Użytkownicy

Biblioteki uniwersyteckie

Kierownik Zespołu

prof. dr hab. n. mat. inż. Jerzy Gawinecki



Wdrożenie

Współfinansowany przez
NCBiR w ramach programu
dotyczącego obronności
i bezpieczeństwa państwa,
realizowany przez
konsorcjum: WAT, firma
ENTE Sp. z o.o.



Zwiększenie poziomu bezpieczeństwa lotniska oraz pasażerów na nim przebywających poprzez opracowanie kompleksowej platformy poprawy bezpieczeństwa lotnisk oraz monitorowanie krytycznych elementów infrastruktury lotnisk. Cechą wyróżniającą jest kompleksowość zbudowanego systemu informatycznego, integrującego w jednym miejscu informacje dotyczące różnych zdarzeń z obszaru bezpieczeństwa, pozyskiwanych z systemów dziedzinowych. W celu zwiększenia poziomu bezpieczeństwa lotniska oraz pasażerów na nim przebywających opracowano innowacyjne, w warunkach krajowych, rozwiązanie pozwalające na weryfikację tożsamości pasażerów na bazie identyfikacji cech biometrycznych.

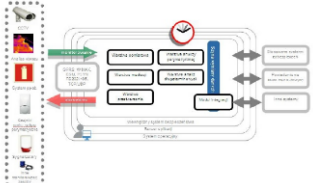


WOJSKOWA
AKADEMIA TECHNICZNA

Demonstrator Technologii Systemu Monitorowania Lotnisk

Projekt Badawczo - Rozwojowy Nr. O R00011112
OPRACOWANIE DEMONSTRATORA TECHNOLOGII NA POTRZEBY WYKONANIA
PROTOTYPU SYSTEMU MONITOROWANIA LOTNISK.

Kierownik Projektu
Dr inż. Michał Misztal
Instytut Matematyki i Kryptologii,
Wydział Cybernetyki, WAT



Konsorcjum




ENTE Sp. z o.o.
 Gliwice 44-100, ul. Gaudiego 7
 tel.: +48 32 33 82 200, fax: +48 32 33 82 210
 e-mail: ente@ente.com.pl, www.ente.com.pl

Cele projektu

Wynikiem realizacji projektu będzie demonstrator technologii systemu monitorującego krytyczne elementy infrastruktury portów lotniczych wraz z dokumentacją techniczną oprogramowania oraz procedurami bezpieczeństwa dla infrastruktury monitorującej odpowiadającymi danej technologii w celu jej optymalnego wykorzystania. System będzie zawierał moduł wspomagający działania dyspozytorskie w sytuacji wystąpienia działań kryzysowych. Moduł ten będzie obejmował integrację z systemami dyspozytorskimi Centrum Powiadomienia Ratunkowego służb mundurowych (Straż pożarna, Policja, Pogotowie). Dodatkowo, w celu zwiększenia poziomu bezpieczeństwa lotniska oraz pasażerów na nim przebywających, w ramach projektu zostanie opracowane innowacyjne w warunkach krajowych rozwiązanie pozwalające na weryfikację tożsamości pasażerów na bazie identyfikacji cech biometrycznych. Cechą wyróżniającą projektowane rozwiązanie będzie budowanie kompleksowego systemu informatycznego, integrującego w jednym miejscu informacje dotyczące różnych zdarzeń z obszaru bezpieczeństwa, pozyskiwanych z systemów dziedzicznych.

Czas realizacji: od 27.10.2010 do 27.10.2012

wydział Cybernetyki
Instytut Matematyki i Kryptologii
tel: (+48 22) 683 96 87, fax: (+48 22) 683 79 19, e-mail: jgawinecki@wat.edu.pl

Military University of Technology, ul. gen. S. Kaliskiego 2, 00-908 Warszawa, POLAND
MUT Chancellor secretariat: phone: (+48 22) 683 90 03, fax: (+48 22) 683 76 60, e-mail: sekretariat.rektora@wat.edu.pl
MUT exchange: phone (+48 22) 683 90 00, fax: (+48 22) 683 99 01, www.wat.edu.pl



DEMONSTRATOR TECHNOLOGII SYSTEMU MONITOROWANIA LOTNISK

Użytkownicy

Międzynarodowe i lokalne lotniska

Kierownik Zespołu

dr inż. Michał Misztal





UNIWERSALNY SYSTEM OCHRONY KRYPTOGRAFICZNEJ ŁĄCZNOŚCI RADIOWEJ ZT



Wdrożenie

Opracowanie
kompleksowego systemu
zapewniającego
bezpieczeństwo informacji
przesyłanych przez
radiostacje KF i UKF.

System składa się z Uniwersalnych Modułów Kryptograficznych, bloków interfejsów radiowych, oraz stanowiska generacji i dystrybucji kluczy kryptograficznych. Zapewnia ochronę urządzeń takich jak Radmor PR4G, Harris Falcon II oraz CTM RKS8000/RKP8100, umożliwiając szyfrowanie danych z prędkością do 1Gb/s oraz obsługę różnych trybów pracy radiostacji.



www.wcy.wat.edu.pl



UNIWERSALNY SYSTEM OCHRONY KRYPTOGRAFICZNEJ ŁĄCZNOŚCI RADIOWEJ ZT

Użytkownicy

Pracujący z nowoczesnymi systemami dowodzenia i zarządzania polem walki, do zapewnienia bezpieczeństwa przesyłanych informacji oraz komunikatów w krytycznych warunkach operacyjnych.

Kierownik Zespołu

prof. dr hab. n. mat. inż. Jerzy Gawinecki





KRYPTOGRAFIA WYKORZYSTUJĄCA KRZYWE ELIPTYCZNE W ZASTOSOWANIACH DO TERMINALI TELEFONICZNYCH I RADIOSTACJI IP PRZEZNACZONYCH DO PRACY W SIECIOCENTRYCZNYCH SYSTEMACH KOALICYJNYCH I NARODOWYCH



Wdrożenie

Współfinansowany przez
NCBiR w ramach programu
dotyczącego obronności
i bezpieczeństwa państwa;
realizowany przez konsorcjum:
WAT, firma Transbit Sp. z o.o.

Wykonano implementację algorytmu klucza publicznego w wersji
narodowej i koalicyjnej (NATO) oraz symetryczny algorytm służący
do szyfrowania danych. Algorytm weryfikacji podpisu oraz
ustalania klucza symetrycznego to ECMQV z krzywą eliptyczną
384 bity. Algorytm symetryczny to AES z długością klucza 256
bitów.



www.wcy.wat.edu.pl



**WOJSKOWA
AKADEMIA TECHNICZNA**

Terminal SCIP

Projekt Badawczo - Rozwojowy Nr O R00 0069 07

Kryptografia wykorzystująca krzywe eliptyczne w zastosowaniach do terminali telefonicznych i radiostacji IP przeznaczonych do pracy w sieciocentrycznych systemach koalicyjnych i narodowych



Kierownik Projektu
Dr inż. Piotr Bora
Instytut Matematyki i Kryptologii, Wydział Cybernetyki, WAT

Konsorcjum:



TRANSBIT
TRANSBIT
02-958 WARSZAWA,
UL. PRZYCZÓŁKOWA 109 A
TEL.: +48 22 550 48 00, FAX: +48 22 550 48 10
biuro@transbit.com.pl
www.transbit.com.pl

Osiągnięte cele projektu

Zaprojektowanie dwóch niezależnych systemów telekomunikacyjnych: sojuszniczego i narodowego. Oparcie systemu sojuszniczego o arytmetykę na krzywych eliptycznych nad ciałem $GF(p)$. Oparcie systemu narodowego o arytmetykę na krzywych eliptycznych nad ciałem $GF(2^n)$. Projekt powiązany jest z NATOwskim Projektem SCIP, którego wdrożenie planowane jest w 2016 roku. Zaprojektowano i wykonano sprzętowy akcelerator arytmetyki na krzywych eliptycznych, zarówno dla systemu sojuszniczego, jak i narodowego. Dla systemu narodowego dokonano wyboru parametrów domenowych, gwarantujących założony poziom bezpieczeństwa - bezpieczne krzywe eliptyczne i generatory grup odpowiednich rzędów. Wykonano w pełni funkcjonalne demonstratory, bazujące na układach programowalnych firmy XILINX.

Okres trwania projektu: 29.06.2009 - 29.06.2011

Wydział Cybernetyki
Instytut Matematyki i Kryptologii
tel: (+48 22) 683 96 87, fax: (+48 22) 683 79 19, e-mail: jgawinecki@wat.edu.pl

Military University of Technology, ul. gen. S. Kaliskiego 2, 00-908 Warszawa, POLAND

MUT Chancellor secretariat: phone: (+48 22) 683 90 03, fax: (+48 22) 683 76 60, e-mail: sekretariat.rektora@wat.edu.pl

MUT exchange: phone (+48 22) 683 90 00, fax: (+48 22) 683 99 01, www.wat.edu.pl



KRYPTOGRAFIA WYKORZYSTUJĄCA KRZYWE ELIPTYCZNE W ZASTOSOWANIACH DO TERMINALI TELEFONICZNYCH I RADIOSTACJI IP PRZEZNACZONYCH DO PRACY W SIECIOCENTRYCZNYCH SYSTEMACH KOALICYJNYCH I NARODOWYCH

Użytkownicy

Polowe systemy teleinformatyczne RSZ

Kierownik Zespołu

dr inż. Piotr Bora





DEMONSTRATOR TECHNOLOGII GENERATORA KOPROCESORA KRYPTOGRAFICZNEGO OPERUJĄCEGO NA ELEMENTACH Z CIAŁA $GF(2^N)$



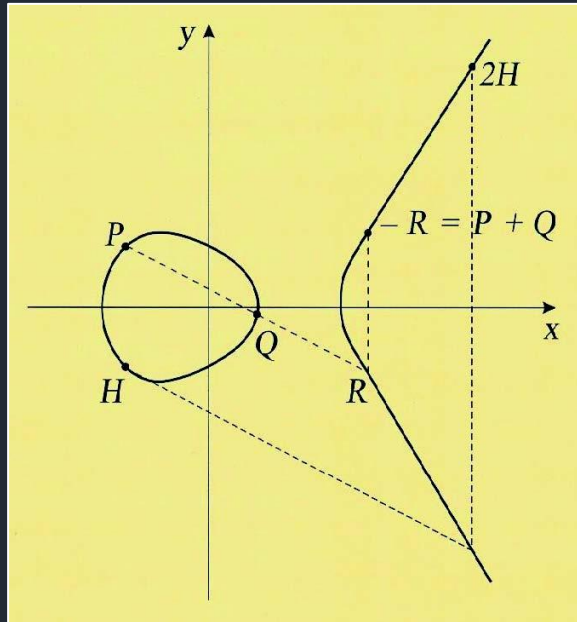
Wdrożenie

Stworzenie unikalnego narzędzia wspomagającego projektowanie systemów kryptograficznych, szczególnie implementacji rozwiązań klucza publicznego na krzywych eliptycznych oraz dla struktur FPGA i ASIC.



Umożliwia generowanie kodu VHDL i AHDL, definiującego struktury jądra kryptograficznego, oraz umożliwia obliczenia dla dowolnego wielomianu pierwotnego danego stopnia, nie wymagając zmian w koprocesorze. Innowacyjne podejście do dekompozycji układu mnożącego oraz zabezpieczenia przed atakami poboru mocy czynią ten generator rozwiązaniem unikatowym na świecie.

www.wcy.wat.edu.pl



DEMONSTRATOR TECHNOLOGII GENERATORA KOPROCESORA KRYPTOGRAFICZNEGO OPERUJĄCEGO NA ELEMENTACH Z CIAŁA $GF(2^N)$

Użytkownicy

Zastosowanie głównie w projektowaniu systemów kryptograficznych dla różnorodnych aplikacji, zapewnia efektywność i bezpieczeństwo obliczeń na krzywych eliptycznych.

Kierownik Zespołu

prof. dr hab. n. mat. inż. Jerzy Gawinecki





IMPLEMENTACJA SYSTEMU KRYPTOGRAFICZNEGO W OPARCIU O INNOWACYJNE TECHNOLOGIE PÓŁPRZEWODNIKOWE



Wdrożenie

Konsorcjum: WAT, firma WASKO S.A. w celu uzyskania wzorcowego rozwiązania sprzętowego i systemowego szyfrowania informacji.



W projekcie wykorzystywano rozwiązanie układowe budowane w oparciu o układy firmy XILINX rodziny VIRTEX 5 podrodziny FXT ze szczególnym uwzględnieniem układów oznaczonych w typoszeregu tej rodziny numerami 70 i 100. Model szyfratora zbudowano w oparciu o platformę sprzętową ML507 firmy XILINX, natomiast prototyp wykonany został w oparciu o zaprojektowany własny schemat elektroniki z układem o numerze 100. Wybór tej rodziny układów podyktowany był możliwymi do wykorzystania w ramach pojedynczej struktury zasobami ze szczególnym uwzględnieniem procesora Power PC. W układzie z oznaczeniem 100 umieszczone są dwa takie procesory.

www.wcy.wat.edu.pl



**WOJSKOWA
AKADEMIA TECHNICZNA**

SZYFRATOR NARODOWY



Projekt Badawczo – Rozwojowy Nr O R00 0031 06
IMPLEMENTACJA SYSTEMU KRYPTOGRAFICZNEGO
W OPARCIU O INNOWACYJNE TECHNOLOGIE PÓŁPRZEWODNIKOWE
Demonstrator technologii na poziomie gotowości VIII finansowany w całości ze środków
Ministerstwa Nauki i Szkolnictwa Wyższego w ramach VI konkursu Departamentu Badań na Rzecz
Bezpieczeństwa i Obronności Państwa wspierany przez Ministerstwo Obrony Narodowej.

Kierownik projektu
Prof. dr hab. n. mat. inż. Jerzy August Gawinecki
Dyrektor Instytutu Matematyki i Kryptologii, Wydział Cybernetyki WAT

Konsorcjum	WOJSKOWA AKADEMIA TECHNICZNA im. Jarosława Dąbrowskiego Wydział Cybernetyki Instytut Matematyki i Kryptologii Warszawa 00-908, Gen. S. Kaliskiego 2 tel.: +48 22 683 9687, fax: +48 22 683 7919 e-mail: jgawinecki@wat.edu.pl, www.wat.edu.pl	WASKO S.A. Gliwice 44-100, Berbeckiego 6 tel.: +48 32 33 25 500, fax: +48 32 33 25 505 e-mail: wasko@wasko.pl, www.wasko.pl
-------------------	--	---

Cel projektu
ZWIĘKSZENIE POZIOMU OBRONNOŚCI I BEZPIECZEŃSTWA PAŃSTWA POPRZEC WYTWORZENIE
OD PODSTAW NOWOCZESNEGO POLSKIEGO SZYFRATORA.
Termin realizacji projektu: od 08.12.2008 r. do 07.12. 2010 r.

Zastosowanie szyfratora
Wykorzystanie do przesyłania danych w istniejącej sieci telekomunikacyjnej:
• Cywilnej (tajemnica służbowa) – sektor bankowy, sektor przemysłu, logistyka, cywilni odbiorcy biznesowi.
• Jednostek odpowiedzialnych za strategiczno sektory gospodarki i bezpieczeństwo państwa (tajemnica państwowa) – MON, SKW, Administracja rządowa, placówki dyplomatyczne, BBN, ABW, BOR.

Cechy wyróżniające
• Dodatkowe zabezpieczenia na implementację funkcji kryptograficznych w strukturze programowej ograniczające możliwości ataku poprzez analizę ulotu elektromagnetycznego, szczególnie z uwzględnieniem ulotu przewodzonego.
• System kryptograficzny posiadający zabezpieczenia na poziomie systemowym powodujące, że atak fizyczny na urządzenie szyfrujące nie będzie opłacalny.

Wynik końcowy
• Wytworzenie od podstaw nowoczesnego polskiego szyfratora – urządzenia wykorzystującego bezpieczne, komercyjne i narodowe zaawansowane algorytmy kryptograficzne.
• Wykonanie praktycznej platformy szyfratora w oparciu o układy FPGA i procesory najnowszych generacji.

Wydział Cybernetyki
Instytut Matematyki i Kryptologii
kontakt: telefon: +48 22 6839687, fax: +48 22 6837919, e-mail: jgawinecki@wat.edu.pl

Wojskowa Akademia Techniczna, ul. gen. S. Kaliskiego 2, 00-908 Warszawa, Polska
WAT Sekretariat Rektora: telefon: (+48 22) 6839003, faks: (+48 22) 683 76 60, e-mail: sekretariat.rektora@wat.edu.pl
WAT kontakt: telefon: (+48 22) 683 90 00, faks: (+48 22) 683 99 01, www.wat.edu.pl

IMPLEMENTACJA SYSTEMU KRYPTOGRAFICZNEGO W OPARCIU O INNOWACYJNE TECHNOLOGIE PÓŁPRZEWODNIKOWE

Użytkownicy

Do ochrony danych w sieciach telekomunikacji:
cywilnych (sektor bankowy, przemysł, PKP)
i jednostkach odpowiedzialnych za strategiczne
sektory gospodarki i bezpieczeństwo Państwa.

Kierownik Zespołu

prof. dr hab. n. mat. inż. Jerzy Gawinecki





WYDZIAŁ CYBERNETYKI
ul. Gen. Sylwestra Kaliskiego 2
00-908 Warszawa 46

POMYSŁ I REALIZACJA:
KAROLINA KRAWCZYŃSKA
MAGDALENA MOSZCZYŃSKA



wcy.wat.edu.pl

facebook.com/wcywat

twitter.com/WatWcy

linkedin.com/company/wydział-cybernetyki-wat-wcy-wat

Warszawa, 2025