

Tomasz HEJCZYK, Leszek ALEKSANDER, Marcin WILCZEK

ENTE Sp. z o.o.
ul. Gaudiego 7, 44-100 Gliwice, Poland

System perymetryczny do wizualizacji dynamicznych zmian na terenie lotniska

Dr inż. Tomasz HEJCZYK

Absolwent Wydziału Informatyki, Automatyki, Elektroniki Pol. Śląskiej w 1999 r. Projektant i kierownik systemu radiowego: Centrum Ratownictwa Gliwice, Centrum Powiadomienia Ratunkowego w Katowicach, systemu CPR w Nowym Sączu. Projektant, kierownik wdrożenia radiolinii i światłowodów w Południowym Koncernie Węglowym S.A. Menedżer wdrożenia oddziałów ALIOR BANK S.A. w całej Polsce. Zainteresowania naukowe: czujniki gazów SAW, metody numeryczne, algorytmy genetyczne.

e-mail: t.hejczyk@wasko.pl



Mgr inż. Marcin WILCZEK

Absolwent Wydziału Nawigacja Akademii Morskiej w Gdyni. Kierownik projektu „Opracowanie demonstratora technologii na potrzeby wykonania prototypu systemu monitorowania lotnisk”. Zainteresowania naukowe: Inteligentne Systemy Transportowe, Smart Cities. Współautor projektów współfinansowanych ze środków budżetu państwa i UE. Pionier w dziedzinie projektów Inteligentnych Systemów Transportowych w Polsce. Obecnie pracuje na stanowisku głównego specjalisty ds. projektów badawczo-rozwojowych.

e-mail: m.wilczek@ente.com.pl



Mgr inż. Leszek ALEKSANDER

Absolwent Wydziału Elektrycznego oraz Organizacji i Zarządzania Pol. Śląskiej. Certyfikowany Menedżer zarządzania innowacjami MI TÜV Nord Polska oraz kierownik projektów PRINCE2®. Ekspert zewnętrzny Narodowego Programu Foresight Polska 2020 realizowanego przez Institute for International Research. Analityk biznesowy oraz współtwórca wielu projektów badawczo-rozwojowych. Wieleletni menedżer rozwiązań systemów z rodziny SCADA, MES oraz automatyki specjalizowanej.

e-mail: l.aleksander@ente.com.pl



Streszczenie

Artykuł przedstawia innowacyjny system perymetryczny, umożliwiający monitorowanie mierzalnych parametrów z systemów bezpieczeństwa. Wynikiem realizacji projektu jest demonstrator technologii, który kontroluje na bieżąco krytyczne elementy infrastruktury portów lotniczych. System zawiera moduły, wspomagające działania dyspozytorskie w sytuacji wystąpienia działań kryzysowych, które można integrować z istniejącymi już systemami dyspozytorskimi (SWD). Taka integracja w pełni gwarantuje współpracę z Centrami Powiadomienia Ratunkowego. Dodatkowo stworzono aplikację, pozwalającą na weryfikację tożsamości pasażerów na bazie identyfikacji unikalnych cech biometrycznych. W ramach projektu powstał kompleksowy system informatyczny, zbierający dane o zdarzeniach z monitorowanego obszaru bezpieczeństwa oraz innych systemów dziedzinowych.

Słowa kluczowe: System wspomagania dowodzenia (SWD), cechy biometryczne, moduł integracyjno-komunikacyjny AWIATOR, Centralny System Demonstratora (CSD), komunikacja szfrowana.

The perimetric system for the visualization of the dynamic changes in the airport area

Abstract

The article presents an innovative perimetric system that enables monitoring the measurable parameters from security systems. The result of the project realisation was the technology demonstration that keeps track of the critical elements of the airport infrastructure. The system embraces the modules that support the dispatcher actions in the case of critical situations. It will be possible to integrate these modules with already existent dispatch systems (SWD). That integration guarantees full cooperation with Emergency Call Centers. Additionally, a module for verification of passengers' identity, based on the identification of their biometric unique characteristics was created. During the project a complex information system was developed. This system collects data about events within the monitored protection area and from other domain systems.

Keywords: supervision support system (SWD), biometric features, integration – communication module AWIATOR, The Central System of Demonstration (CSD), the coded communication.

1. Wstęp

Ostatnia dekada oraz lata to seria wielu poważnych zagrożeń i konfliktów, które wytworzyły dobre praktyki w zakresie prowadzenia działań, poprawiających bezpieczeństwo. Doświadczenia te doprowadziły do stworzenia nowych reguł prowadzenia polityki bezpieczeństwa zarówno w zakresie fizycznym jak i informatycznym, lecz przede wszystkim o charakterze zapobiegawczym. Rozwój telekomunikacji, elektroniki i teleinformatyki stworzył nowe możliwości, dotyczące automatyzacji procesów podejmowania decyzji przy wykorzystaniu rozbudowanych systemów informatycznych. Kluczowe znaczenie odgrywa tu prawidłowe podejmowanie decyzji operatorskich. Ich skuteczność, szczególnie w sytuacjach o charakterze nietypowym, zależy w stopniu istotnym od dostępności informacji i jej sprawnej selekcji, w tym sygnalizowania zdarzeń, wymagających szczególnej koncentracji uwagi ochrony oraz jej ukierunkowania na identyfikację źródeł zagrożeń, zainicjowania procedur diagnostycznych lub podjęcia decyzji w trybie pilnym.

Opisywany system dedykowany jest dla portów lotniczych, wchodząc w skład infrastruktury krytycznej lotniska [1, 2], i wpisuje się w program ochrony portu lotniczego przed atakami bezprawnej ingerencji. Zastosowanie teleinformatycznego systemu integrującego daje możliwość ustalenia łańcucha powiadomienia i automatycznych procesów reakcji a także umożliwia śledzenie pracy urzędów i uwydatnianie anomalii, umożliwiając bezzwłoczną reakcję operatorów [3]. Zastosowanie technologii biometrycznych, do których, m.in. nawiązuje niniejsza publikacja, stwarza nowe możliwości kontroli agentów Handlingowych, identyfikacji pasażera, itp.

2. Cele projektu

W ramach zrealizowanego projektu, zbudowano kompleksowy system informatyczny, integrujący w jednym miejscu informacje dotyczące różnych zdarzeń, pochodzących z systemów dziedzinowych, zainstalowanych w portach lotniczych.



Rys. 1. Fragment obwodowej ochrony perymetrycznej
Fig. 1. The fragment of the district perimetric protection

Główne zakresy zdarzeń, podzielono na następujące grupy:

- zagrożenia, związane z bezpośrednim atakiem fizycznym (np. wandalizm, nieautoryzowane wejście na teren płyty lotniska, terroryzm, sabotaż),
- zagrożenia związane ze zdarzeniami losowymi (np. pożar, włamanie, wichury, itp.),
- zagrożenia związane z usterkami technicznymi (np. zużycie technologiczne, brak redundancji).

Podczas projektu powstały inteligentne moduły komunikacyjne, umożliwiające przekazywanie i pozyskiwanie informacji z monitorowanych urządzeń (rys. 2) i systemów dziedzinowych do Centralnego Systemu Demonstratora (CSD). Ich zastosowanie umożliwi separację pomiędzy dedykowanymi systemami dziedzinowymi a systemem nadrzędnym jako autonomiczną jednostką informacji a gwarancją działania poszczególnych, już działających Systemów Ochrony Technicznej (SOT), systemu Kontroli Dostępu (KD), itp.

Podczas realizacji projektu pozyskano informacje, m.in. z następujących podsystemów:

- systemu Obwodowej Ochrony Perymetrycznej (rys. 1),
- systemu Sygnalizacji Włamania i Napadu (SSWiN),
- systemu Identyfikacji Pracowników oraz Pasażerów¹,
- systemu Sygnalizacji Pożaru,
- systemu Telewizji Przemysłowej (CCTV),
- sygnały Stanu Urządzeń Dziedzinowych,
- monitoringu wizyjnego infrastruktury,
- systemu prewencyjnego przeciwdziałania zagrożeniom terrorystycznym poprzez weryfikację cech biometrycznych,
- niepublicznych elementów systemów bezpieczeństwa².

Opracowano innowacyjne w warunkach krajowych rozwiązanie pozwalające na weryfikację tożsamości pasażerów na bazie identyfikacji cech biometrycznych. Zidentyfikowano elementy krytyczne w porcie lotniczym, objętym projektem. Opracowano i zastosowano mechanizmy kryptograficzne [4] w niewrażliwych elementach systemu.

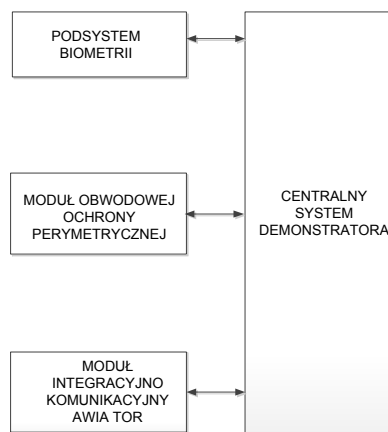


Rys. 2. Monitoring oświetlenia pasów lotniska

Fig. 2. The monitoring of the airport runway lighting system

3. Opis architektury systemu

Charakterystykę demonstratora technologii w postaci schematu blokowego przedstawia rys. 3. Centralną jednostką komunikacyjną stanowi serwer aplikacji, będący integralną częścią systemu demonstratora, zintegrowany z bazą danych. Dostęp do danych jest możliwy za pomocą aplikacji graficznych, tzw. klientów GUI (ang. *Graphical User Interface*).



Rys. 3. Schemat blokowy i wzajemne powiązania demonstratora technologii

Fig. 3. The block diagram and interrelationships of the technology demonstrator

Dane są pozyskiwane za pomocą programowych modułów komunikacyjnych, czyli aplikacji informatycznych, umożliwiających i realizujących zaawansowaną obsługę różnego rodzaju łącz komunikacyjnych oraz zapewniających lokalne gromadzenie danych. Moduł komunikacyjny może pracować jako autonomiczna i samowystarczalna jednostka. Zastosowanie wielowarstwowej architektury o charakterze centralno-rozproszonym, projektowanego centralnego systemu informatycznego, zapewnia oczekiwaną skalowalność całego rozwiązania. System demonstratora jest zasilany danymi, które pochodzą z dedykowanych podsystemów. Dane wejściowe, z monitorowanych systemów, przekazywane są przez sieć transmisji danych GSM/GPRS i mają odzwierciedlenie w panelu analitycznym systemu. W ramach systemu można zintegrować czujniki i sensory [5], które wykorzystuje się do detekcji gazów toksycznych a także do wykrywania materiałów wybuchowych i gazów bojowych. Poniżej scharakteryzowano podsystem biometryczny.

4. Podsystem biometryczny

Innowacyjnym elementem projektu było zastosowanie technik biometrycznych na potrzeby działań prewencyjnych z zakresu zarządzania bezpieczeństwem lotnisk. Zaprojektowany i wykonany podsystem biometryczny umożliwia realizację następujących celów:

- wsparcie obsługi pasażerów w zakresie identyfikacji kart pokładowych w określonych miejscach, znajdujących się na terenie portu lotniczego,
- kontrola dostępu do wydzielonych pomieszczeń obsługi technicznej portu.



Rys. 4. Testy urządzeń, badających cechy biometryczne a) pobranie wzorca biometrycznego palca w postaci układu naczyń krwionośnych

b) przypisanie kodu

Fig. 4. Biometric appliance tests a) scanning blood vessel pattern from finger b) corresponding code

¹ Zrealizowano w warunkach laboratoryjnych ze względu na aktualnie obowiązujące regulacje oraz procedury wdrożeniowe, zgodnie z dyrektywami ULC.

² Zrealizowano tylko w warstwie możliwych koncepcji rozwiązań, bez integracji.

Do budowy podsystemu wykorzystano moduł integracyjno-komunikacyjny AWIATOR w celu wytworzenia szyfrowanego kanału transmisji danych. W skład podsystemu wchodzi stanowisko rejestracji, na którym system identyfikuje pasażera i drukuje kartę pokładową. Stanowiska weryfikacji umożliwiają ponowne odczytanie i powiązanie karty pokładowej, na której jest wydrukowany kod 2D (rys. 4b). Kolejny krok to jego powiązanie z biometrycznym odciskiem palca (rys. 4a). W ramach projektu przeprowadzono kompleksową analizę różnych cech biometrycznych (np. odcisk palca, układ naczyń krwionośnych, układ twarzy, itp.) pod kątem skuteczności ich wykorzystania w projekcie.

5. Detekcja zagrożeń

W projekcie dokonano identyfikacji zagrożeń oraz określono ich wagi jednostkowe. Zidentyfikowano i zanalizowano zdarzenia, zagrażające funkcjonowaniu portu lotniczego. Połączono razem dwie kwestie: zdefiniowano źródła zagrożenia oraz odbiorców zdarzenia. Łącząc każdego z odbiorców ze zidentyfikowanymi źródłami zagrożeń przypisano dla każdego z nich wagę zdarzenia. Odpowiednim wagom zdarzeń odpowiada ich ocena. Informacje o stanie otoczenia portu lotniczego są zbierane przez system, a następnie przetwarzane zgodnie z krosową macierzą analityczną. Osobno dla każdego z pięciu zdefiniowanych odbiorców informacji (np. kierownik Pionu Bezpieczeństwa, pracownik Centrum Monitoringu, itp.) zsumowano wagi wszystkich zaistniałych zdarzeń. Na tej podstawie określano stan bezpieczeństwa, panujący na terenie portu lotniczego z punktu widzenia danego odbiorcy. Stopień zagrożenia określono za pomocą poniższego wzoru.

$$\bigwedge_{T=1}^5 S_T = k_T \sum_{k=0}^n i_k w_k \quad (1)$$

gdzie:

- S_T – stan zagrożenia z punktu widzenia odbiorcy T ,
- i_k – wystąpienie lub nie zdarzenia k (1 lub 0),
- w_k – waga zdarzenia k ,
- k_T – współczynnik skalujący dla odbiorcy T .

Do wyznaczenia stopnia zagrożenia z punktu widzenia konkretnego odbiorcy wykorzystywano współczynnik skalujący, wyznaczony empirycznie dla każdego z pięciu odbiorców. Za ogólny stopień zagrożenia portu lotniczego przyjęto średnią arytmetyczną, dla każdego z odbiorców informacji, wg poniższego wzoru.

$$S_0 = \sum_{T=1}^n \frac{S_T}{n} \quad (2)$$

gdzie:

- S_0 – ogólny stan zagrożenia dla portu lotniczego,
- S_T – stan zagrożenia z punktu widzenia odbiorcy T ,
- n – ilość odbiorców informacji, dla których wyznaczono stan zagrożenia.

Wzrost stanu zagrożenia ponad założony poziom bezpieczeństwa skutkuje automatycznym powiadomieniem określonych służb ratunkowych w modelu demonstratora.

6. Wnioski

W ramach projektu zbudowano demonstrator technologii systemu, monitorującego krytyczne elementy infrastruktury wybranego portu lotniczego, wraz z opracowaniem wzorców analitycznych w zakresie procedur bezpieczeństwa dla infrastruktury monitorującej.

Opisane rozwiązanie wyróżnia się spośród istniejących systemów ochrony ze względu na jego specyficzną budowę, wykorzystującą kompleksowy system informatyczny, integrujący w jednym miejscu dane, pozyskane z systemów dziedzinowych. W celu zwiększenia poziomu bezpieczeństwa obiektów lotniska opracowano innowacyjne rozwiązanie, pozwalające na weryfikację tożsamości pasażerów na bazie ich cech biometrycznych. W najbardziej newralgicznych miejscach systemu wykorzystano szyfrowanie danych. Wykonano testy w warunkach laboratoryjnych oraz w warunkach zbliżonych do rzeczywistych. Do tego celu praktycznie wykorzystano część ogrodzenia, otaczające lądowisko dla helikopterów, znajdującego się na terenie firmy ENTE Sp. z o.o. a także zainstalowano pilota systemu w Międzynarodowym Porcie Lotniczym „Katowice” w Pyrzowicach, umożliwiającemu monitoring parametrów w czasie rzeczywistym i określanie stopnia zagrożenia na podstawie algorytmu analitycznego w przyjętym modelu. System dodatkowo posiada moduł wsparcia działań dyspozytorskich w sytuacji wystąpienia zdarzeń kryzysowych, z możliwością zintegrowania z systemami dyspozytorskimi Centrum Powiadomienia Ratunkowego.

Wyróżnikiem zaprojektowanego systemu jest możliwość analizy pozyskiwanych danych, a w szczególności analizy obrazu z kamer systemów CCTV w powiązaniu z informacjami pozyskiwanymi z innych elementów systemu, np. sensorów dźwięku, systemów bezpieczeństwa. Wśród stosowanych sensorów stosowane są różne typy urządzeń ze względu na sposób umieszczenia: podziemne, powierzchniowe i ogrodzeniowe. W przypadku zastosowanej obwodowej ochrony perymetrycznej, opartej o innowacyjny system MOOP mamy do czynienia z otwartą architekturą, w której uniezależniamy konstrukcję systemu od stosowania specjalistycznych urządzeń a wykorzystujemy wyłącznie elementy ogólnodostępne. Przedstawiono zagadnienie detekcji zagrożeń, prezentując wzory, zaimplementowane w oprogramowaniu systemu demonstratora.

Powyższy demonstrator technologii systemu, monitorującego lotniska, brał udział w Targach Concours Lepine 2012 w Paryżu i otrzymał Srebrny Medal oraz certyfikat innowacyjności.

Wdrożenie wyników projektu przyniesie wymierne skutki dla podniesienia bezpieczeństwa na lotniskach poprzez zapewnienie sprawniejszego, szybszego reagowania na zagrożenia i zdecydowanie ułatwi proces podejmowania decyzji.

Powyższa publikacja jest wynikiem współpracy firmy ENTE Sp. z o.o. i Wojskowej Akademii Technicznej, które wspólnie realizowały projekt rozwojowy z obszaru obronności i bezpieczeństwa państwa, pt „Opracowanie demonstratora technologii na potrzeby wykonania prototypu systemu monitorowania lotnisk”. Praca naukowa finansowana przez Narodowe Centrum Badań i Rozwoju ze środków na naukę w latach 2010-2012 jako projekt rozwojowy.

7. Literatura

- [1] Stec K.: Wybrane prawne narzędzia ochrony infrastruktury krytycznej w Polsce. Bezpieczeństwo Narodowe nr 19, III -2011.
- [2] Ochrona cywilnego ruchu lotniczego w Polsce, jako element bezpieczeństwa lotnictwa cywilnego. Nr Ewid. 113/2012/P/11/062/KIN.
- [3] Zieliński M.: Bezpieczeństwo w porcie lotniczym. Zeszyty Naukowe Akademii Marynarki Wojennej ROK LI NR 4 (183) 2010.
- [4] Bora P., Gawinecki J., Miernik R., Misztal M., Szmidt J.: Kryptograficzne metody ochrony sieci teleinformatycznych. Biuletyn Wojskowej Akademii Technicznej, vol. 4 [596] 2002 r.
- [5] Hejczyk T., Urbańczyk M., Witula R., Maciak E.: SAW sensors for detection of hydrocarbons. Numerical analysis and experimental results. Bulletin of the Polish Academy of Sciences, Technical Sciences, Vol. 60, No. 3, (2012).

otrzymano / received: 15.04.2013

przyjęto do druku / accepted: 01.11.2013

artykuł recenzowany / revised paper