

Mirosław SIERGIEJCZYK¹, Stanisław GAGO²

Politechnika Warszawska, Wydział Transportu
ul. Koszykowa 75, 00 – 662 Warszawa

¹ -mail: msi@it.pw.edu.pl

² e-mail: s.gago@wp.pl

KONCEPCJA SYSTEMU BEZPIECZEŃSTWA NA KOLEJOWYCH PRZEJŚCIACH GRANICZNYCH UE

Streszczenie:

W transporcie kolejowym, jako rozległym systemie, zagadnienie zapewnienia bezpieczeństwa publicznego wydaje się szczególnie ważne. Jednym z istotnych problemów w tym obszarze jest bezpieczeństwo publiczne na kolejowych przejściach granicznych, które są przejściami granicznymi Unii Europejskiej. W artykule dokonano identyfikacji zagrożeń bezpieczeństwa publicznego w transporcie kolejowym, w tym na kolejowych przejściach granicznych z państwami nie będącymi członkami Unii Europejskiej. Przystawiono koncepcję systemu bezpieczeństwa kolejowych przejść granicznych realizującego inteligentne scenariusze wsparcia procesów zapewnienia bezpieczeństwa na terenie przejść granicznych i pośrednio na terenie całej Unii Europejskiej.

Słowa kluczowe: bezpieczeństwo publiczne, transport kolejowy, system, monitorowanie, przejścia graniczne Unii Europejskiej

WSTĘP

Przeciwdziałaniem na coraz to powszechniejsze zagrożenia życia ludzkiego i dóbr osobistych jest budowa wszelkiego rodzaju systemów monitoringu, które w znacznej mierze przyczyniają się do wykrywania sprawców wypadków drogowych, bandyckich napadów czy też kradzieży. Systemy monitoringu powinny być przystosowane do specyfiki monitorowanych obiektów. Pewną odrębną specyfiką powinny charakteryzować się systemy monitorowania obiektów kolejowych, choćby tylko dlatego, że między innymi powinny monitorować pewne elementy infrastruktury drogi kolejowej np. mosty, głowice stacyjne, zwrotnice itp. Na terenach kolejowych istnieje wiele potencjalnych zagrożeń dla podróżnych i osób pracujących w niektórych obiektach np. na dworcach.

Transport a w szczególności transport lotniczy i transport szynowy (kolej, metro) są celami spektakularnych zamachów terrorystycznych. Jak wykazuje doświadczenie, bezpieczeństwu podróżnych zagrażają nie tylko zamachy terrorystyczne lecz również inne działania przeciwko życiu i mieniu. Zapewnienie poprawy bezpieczeństwa na dworcach i stacjach kolejowych, stacjach metra i okolicach tych obiektów należy rozpatrywać jako bezpieczeństwo systemu, który stanowią: ludzie, znajdujący się w odpowiedniej relacji – w stosunku do siebie, w stosunku do infrastruktury i środków przewozu, obiekty infrastruktury i środki transportu szynowego (kolej, metro).

W Polsce z uwagi na dotychczasową izolację i dystans do problemów światowych i europejskich zjawisko terroryzmu jest zagadnieniem niekiedy lekceważonym. Działania o charakterze terrorystycznym na świecie przybierają coraz to nowe formy i coraz to nowe obiekty narażone są na tego typu ataki. Możliwości zaistnienia takich zdarzeń na terenie

naszego kraju sprzyja obecna sytuacja geopolityczna Polski. Nasz kraj wymieniony został obok USA, Wielkiej Brytanii, Hiszpanii, Australii, Japonii i Włoch, jako miejsce potencjalnego ataku terrorystów w odwecie za wspieranie interwencji w Iraku i Afganistanie (przy czym w wymienionych pierwszych trzech krajach zamachy terrorystyczne miały miejsce).

Zagadnieniem o ostatnio szybko rosnącym znaczeniu jest wzrost zagrożenia ze strony międzynarodowych grup terrorystycznych. Taktyka ich działania nie jest przewidywalna, a zróżnicowanie metod oraz atakowanych obiektów coraz większe. Choć nie odnotowano do tej pory ataku terrorystycznego na infrastrukturę obiektów transportu publicznego naszego kraju, to z uwagi na to, że policja nie przekazuje opinii publicznej informacji operacyjnych, nie oznacza to, że nie zarejestrowano przygotowań do przeprowadzenia takiego ataku przez grupy terrorystyczne. Przykłady ataków terrorystycznych w Europie pokazują, że ataki na obiekt tego typu powodują bardzo duże straty wśród ludzi, spowodowane zarówno zamachem bezpośrednim, jak i paniką powstałą wśród podróżujących osób. a co nie mniej ważne dla terrorystów - katastrofy na dużą skalę są zdarzeniami o dużym znaczeniu medialnym.

1. ANALIZA PRAC BADAWCZYCH Z ZAKRESU MONITORINGU BEZPIECZEŃSTWA PUBLICZNEGO

W Polsce w kilku ośrodkach naukowych prowadzone są prace z zakresu inteligentnego monitorowania i przetwarzania informacji oraz automatycznego wykrywania zagrożeń oraz rozpoznawania nienormalnych zachowań lub aktów przemocy w miejscach publicznych a także identyfikacja i obserwacja obiektów ruchomych.

Projekt INDECT Inteligentny system informacyjny wspierający obserwację, wyszukiwanie i detekcję dla celów bezpieczeństwa obywateli w środowisku miejskim realizowany w AGH Kraków [7]. INDECT jest to międzynarodowy projekt badawczy mający na celu stworzenie odpowiednich narzędzi zwiększających bezpieczeństwo obywateli Unii Europejskiej oraz poufność zarejestrowanych i przechowywanych informacji. Zamierzenia projektu obejmują użycie innowacyjnych algorytmów i metod z zakresu informatyki do wykrywania i walki z terroryzmem oraz innymi działaniami przestępczymi. Są to działania zarówno w sferze wirtualnej (np. dziecięca pornografia, oprogramowanie wirusowe, rozpowszechnianie zakazanych symboli, handel ludzkimi organami) jak i rzeczywistej (np. akty terroryzmu, chuligaństwa, kradzieże). Do celów projektu INDECT zalicza się również wykrywanie potencjalnych zagrożeń (np. pożar, pozostawiony pakunek, ludzie na torach kolejowych, itp.).

Kolejnym przykładem pracy w zakresie monitorowania bezpieczeństwa publicznego jest projekt INSIGMA - Inteligentny System Informacyjny dla Globalnego Monitoringu, Detekcji i Identyfikacji Zagrożeń [8]. Celem nadrzędnym tego projektu jest opracowanie i wdrożenie złożonego systemu informacyjnego do celów kompleksowej detekcji i identyfikacji zagrożeń oraz monitoringu i identyfikacji obiektów ruchomych. Podstawowym elementem warstwy sprzętowej systemu będzie układ kamer rozmieszczonych na obszarze objętym monitoringiem, ale także za pomocą sieci sensorów, które będą w stanie wykrywać zmiany położenia obiektów, nagłe zmiany temperatury, ciśnienia oraz stężenia niebezpiecznych związków. W celu zapewnienia wysokiego poziomu ochrony, zastosowana zostanie również technika RFID służąca do zdalnej identyfikacji obiektów. Informacje na temat lokalizacji będą pozyskiwane z systemów GSM i UMTS, GPS. Dane pozyskane dzięki sieci kamer i czujników rozmieszczonych na terenie monitorowanym będą podlegały szczegółowej i automatycznej analizie w warstwie analizy kontekstowej [8].

W pracach prowadzony w ramach projektu [11] wzbogacono system monitoringu „sztuczną inteligencją” i technologiami, które pozwalają na jeszcze lepszy i dokładniejszy nadzór. System Inteligentnego Monitoringu zwraca uwagę operatora monitoringu na kamerę, która pokazuje naprawdę ważne zdarzenie. Wyjątkowość Systemu Inteligentnego Monitoringu polega na tym, że spośród obrazów, nadawanych przez setki kamer, potrafi rozpoznać np. bójkę, napaść, wyrwanie torebki, zbiegowisko, paniczną ucieczkę, porzucenie bagażu, pozostawienie auta w niedozwolonym miejscu. Usłyszy też krzyk czy wystrzał broni. Po rozpoznaniu prześle obraz na komputer operatora systemu, który będzie mógł natychmiast zareagować. Mechanizm został wyposażony w system informacji geograficznej, który zlokalizuje "gorące" miejsce na mapie i podpowie, gdzie jest najbliższy radiowóz.

Projekt systemu wspierającego bezpieczeństwo w miastach i w obiektach zakłada automatyczną identyfikację zachowań i osób oraz wykrywanie sytuacji niebezpiecznych, wykorzystujący zaawansowany monitoring miejski. Technologia monitoringu miejskiego ma m.in. pozwolić na automatyczne rozpoznawanie osoby na podstawie chodu czy ocenę stanu emocjonalnego poszczególnych osób na podstawie mimiki twarzy i gestów. Inną możliwością projektowanego systemu będzie możliwość automatycznego wykrywania nietypowych lub niebezpiecznych ruchów osoby czy grupy osób oraz typowanie sytuacji poprzedzających awantury lub akty wandalizmu. Zastosowana technologia będzie też mogła automatycznie wykryć daną osobę (lub grupę) i śledzić jej sylwetkę w sekwencjach obrazów z wielu kamer w obrębie nadzorowanych stref. W ten sposób strażnicy dowiedzą się, że np. wszczynająca awantury czy dopuszczająca się aktów wandalizmu osoba pojawiła się w innej części miasta [10].

W Polsce w kilku ośrodkach naukowych prowadzone są prace z zakresu inteligentnego monitorowania i przetwarzania informacji oraz automatycznego wykrywania zagrożeń oraz rozpoznawania nienormalnych zachowań lub aktów przemocy w miejscach publicznych a także identyfikacja i obserwacja obiektów ruchomych. Przegląd najważniejszych prac naukowo – badawczych prowadzonych przez polskie uczelnie wykazuje, że nie są prowadzone prace związane bezpośrednio z monitorowaniem transportu szynowego a już w żadnym zakresie z monitorowaniem kolejowych przejść granicznych z krajami nie będącymi członkami Unii Europejskiej.

2. 3. IDENTYFIKACJA POTRZEBY MONITOROWANIA BEZPIECZEŃSTWA NA KOLEJOWYCH PRZEJŚCIACH (STACJACH) GRANICZNYCH

Na terenach kolejowych występuje wiele potencjalnych zagrożeń podróżnych i osób pracujących np. na dworcach tj.:

- zagrożenia ludzi i infrastruktury obiektów kolejowych poprzez zamachy terrorystyczne,
- zagrożenia ze strony ludzi z marginesu społecznego (kradzieże, rozboje, wandalizm, nachalne żebractwo powodujące dyskomfort psychiczny),
- zagrożenia wynikające ze złego utrzymania obiektów kolejowych (uszkodzenia drogi kolejowej, uszkodzenia krawędzi peronowych, duże zaśmiecenie, zła ochrona przeciwpożarowa, niewystarczające oświetlenie, itp.), które mogą powodować:
 - ogólne potłuczenia podróżnych
 - kontuzje kończyn,
 - zatrucia dymem (palące się śmiecie),
 - stany lękowe,

- zagrożenia pasażerów występujące w okresie rozpoczynania oraz kończenia podróży, a w tym:
 - za wczesne lub za późne zamykanie drzwi wagonów,
 - dobieganie do odjeżdżającego pociągu,
 - upadki przy wchodzeniu lub wychodzeniu z pociągu.

Jednakże, skutki zamachów terrorystycznych są największe, najbardziej kosztowne i przynoszące najwięcej nieszczęść. Wśród krajów UE, Polska powinna stworzyć swoistą specyfikę bezpieczeństwa transportu kolejowego związaną ze szczególnie ważnymi z punktu widzenia bezpieczeństwa państwa, kolejowymi przejściami granicznymi – kolejowymi stacjami granicznymi Polski z krajami nie będącymi członkami UE. Stacje te są stacjami granicznymi Unii Europejskiej i zgodnie z Układem z Schengen oprócz służb kolejowych, policji, straży pożarnej itd. znajdują się tam wzmocnione służby Straży Granicznej, Służby Celne a także działają Inspekcja Weterynaryjna, Państwowa Inspekcja Ochrony Roślin i Nasiennictwa oraz Inspekcja Handlowa.

Ponadto ze względu na zmianę szerokości torów po drugiej stronie granicy, na tych stacjach granicznych, w zależności od rodzaju przejścia granicznego (towarowe, osobowe, towarowo-osobowe), zainstalowana jest infrastruktura do wymiany wózków wagonowych dla ruchu pasażerskiego i potężna infrastruktura do przeładunku towarów dla ruchu towarowego.

Oprócz wymienionych powyżej zagrożeń występujących w transporcie kolejowym na stacjach granicznych występują dodatkowe zagrożenia związane z przemytem ludzi i towarów, narkotyków, materiałów radioaktywnych, substancji i materiałów terrorystycznych czy też przemytu dzieł sztuki, które stanowiąc mogą dobro narodowe. Powyższe zagrożenia występują przez 24 godziny na dobę przez siedem dni w tygodniu.

Polska, granicząc z Rosją, Białorusią i Ukrainą, spośród wszystkich krajów Unii Europejskiej ma najwięcej takich stacji granicznych (14 kolejowych przejść granicznych). Obecnie praktycznie nie ma wzorca do opracowania kompleksowego systemu zapewniającego bezpieczeństwo na tego rodzaju obiektach. Analizując zagrożenia na tego typu obiektach można dojść do wniosku, że stacje graniczne powinny być wyposażone w systemy, które pozwalałyby na dokonanie kompleksowej detekcji i identyfikacji zagrożeń oraz inteligentnego monitoringu i identyfikacji obiektów ruchomych.

Systemy monitorowania obiektów stacyjno-dworcowych transportu szynowego, choćby tylko dlatego, że między innymi powinny one monitorować pewne elementy infrastruktury drogi kolejowej np. mosty, głowice stacyjne, zwrotnice itp. stanowią pewną odrębną specyfikę w stosunku do systemów monitorujących np. tereny zurbanizowane. Także i systemy monitoringu stosowane w transporcie lotniczym nie mogą stanowić pełnego rozwiązania dla transportu kolejowego a tym bardziej dla stacji granicznych.

Kolejowe przejścia (stacje) graniczne w porównaniu do innych przejść granicznych można opisać między innymi następującymi cechami:

- dużo większa, różnorodna i bardziej rozległa infrastruktura niż na innego rodzaju przejściach np. przejścia drogowe,
- w porównaniu z transportem drogowym dużo więcej towarów „przekracza granicę” w jednym środku transportu – pociąg versus samochód
- duża liczba pasażerów w jednostce transportowej (pociągu)
- inny sposób odprawy pasażerów w porównaniu z innymi środkami transportu – autokary, samochody osobowe, samoloty
- zmiana parametrów drogi kolejowej – normalnotorowa - szerokotorowa
- limitowany czas odprawy pociągów pasażerskich

- pasażerowie w zasadzie nie opuszczają pociągu podczas odprawy granicznej i z reguły zajmują pozycje siedzącą
- dostęp do obiektów dworcowych w zasadzie nie kontrolowany (nieograniczony)

Przy tworzeniu koncepcji na pewno należy korzystać zarówno z najnowszych prac prowadzonych przez światowe jak i krajowe ośrodki naukowo-badawcze. Wiele aspektów jak i rozwiązań szczegółowych prowadzonych prac będzie można wykorzystać przy tworzeniu koncepcji zapewnienia bezpieczeństwa na kolejowych przejściach (stacjach) granicznych stanowiących granice UE. Niemniej jednak wspomniana koncepcja musi uwzględnić swoistą specyfikę tego rodzaju obiektów w zakresie infrastruktury kolejowo – dworcowej, infrastruktury związanej z przeładunkiem towarów, prowadzeniem ruchu kolejowego, przewozu osób i towarów, możliwości działań nie zgodnych z prawem. Koncepcja powinna zapewnić wsparcie służb administracji państwowej, wojskowej i kolejowej by przeprowadzana kontrola była skuteczna, szybka, niezawodna i nie uciążliwa tak dla pasażerów jak i pracowników wymienionych służb zaangażowanych w obsługę kolejowego przejścia granicznego. Ponadto koncepcja powinna uwzględniać i inne zagrożenia związane z wypadkami losowymi jak i awariami poszczególnych systemów - pożary, włamania, rozboje, katastrofy, wypadki, awarie, zatrucie środowiska.

Przy tworzeniu koncepcji systemu monitoringu dla kolejowych przejść granicznych należy brać pod uwagę fakt, że każde przejście jest inne, ma swoją specyfikę, różni się one wielkością i zakresem świadczonych czynności. Kolejowe przejścia graniczne dzielą się na: osobowe, towarowe, osobowo – towarowe.

Polska ma 14 kolejowych przejść granicznych z państwami nie należącymi do Unii Europejskiej (Rosja 3 przejścia, Białoruś 5 przejść, Ukraina 6 przejść).

Na każdym przejściu granicznym panuje inny ruch pasażerski i inny ruch towarowy różniący się rodzajem i ilością przewożonych towarów. Dlatego też, w koncepcji powinno być przyjęte takie rozwiązanie, które z jednej strony będzie zapewniało bezpieczeństwo konkretnego przejścia, z drugiej zaś będzie uzasadnione ekonomicznie.

3. KONCEPCJI SYSTEMU BEZPIECZEŃSTWA KOLEJOWYCH PRZEJŚĆ GRANICZNYCH (SBKPG)

Zasadniczą funkcją systemu bezpieczeństwa kolejowych przejść granicznych (SBKPG) powinno być wspomaganie zainteresowanych Podmiotów w zakresie realizacji procesów związanych z zapewnieniem bezpieczeństwa na kolejowych przejściach granicznych, poprzez realizację inteligentnych scenariuszy. System powinien wspierać działanie służb „administracyjnych” tj. Straży Granicznej, Służb Celnej i fitosanitarnej, służb „kolejowych” tj. operatora infrastruktury kolejowej związanej z prowadzeniem ruchu oraz przewoźników pasażerskich i towarowych. Ponadto System powinien wspierać bezpieczeństwo pozostałych podmiotów działających na terenie kolejowego przejścia granicznego np. składów, magazynów, których uszkodzenie mogłoby spowodować np. skażenie środowiska. Generalnie system powinien wzmocniać procesy związane z bezpieczeństwem:

- ludzi (obywateli Unii Europejskiej poprzez zapobieganie przenikania terrorystów i materiałów terrorystycznych na teren UE, podróżnych i personelu znajdującego się na terenie przejścia granicznego),
- szeroko rozumianej infrastruktury (droga kolejowa, dworce, podstacje trakcyjne, place przeładunkowe, magazyny, itd.),
- taboru (wagony pasażerskie i towarowe, lokomotywy, pojazdy i urządzenia transportu wewnętrznego np. dźwigi, wózki widłowe, itd.)

- środowiska (np. zapobieganie zanieczyszczeniu lub skażeniu terenu lub powietrza).

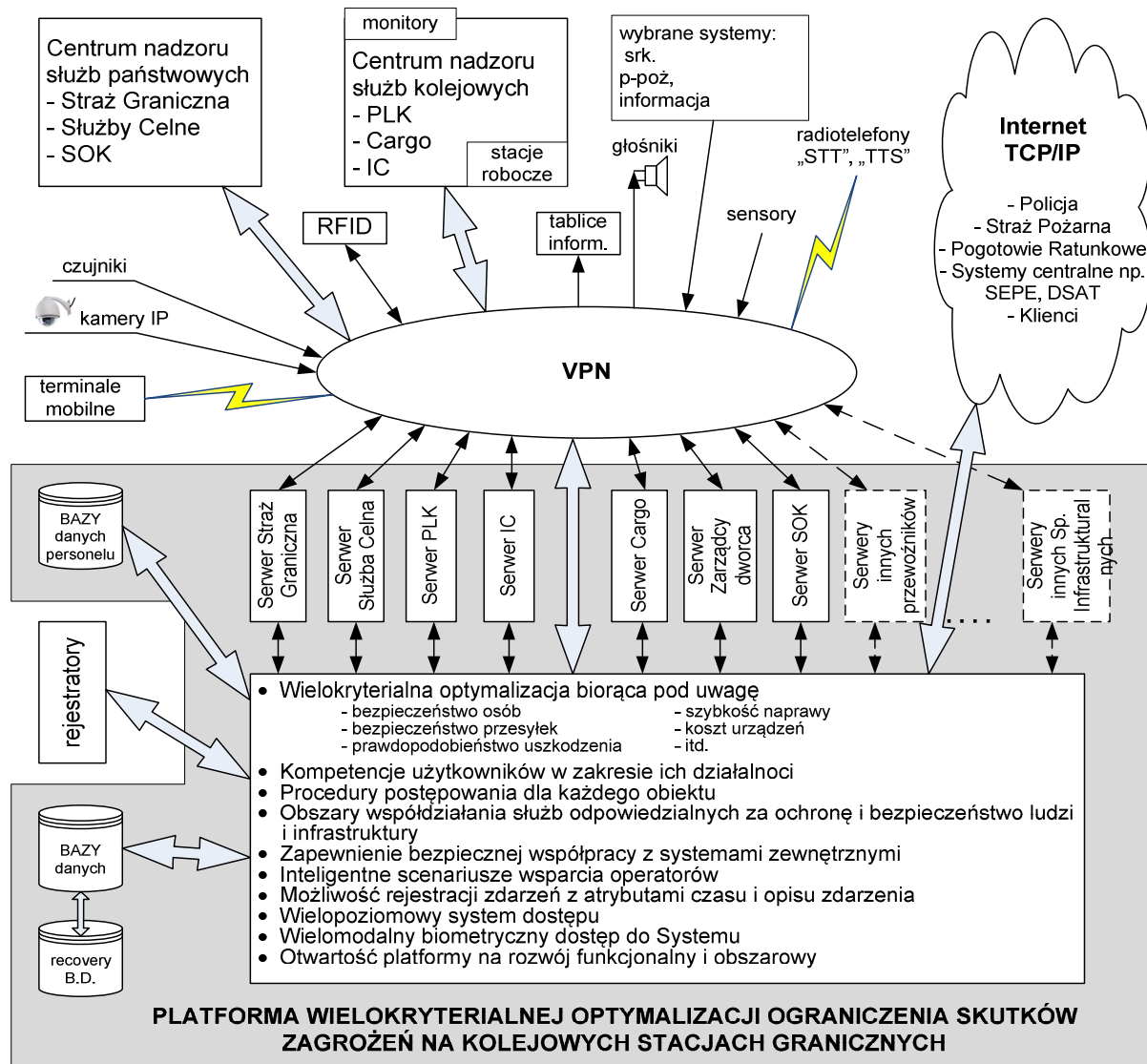
Oprócz realizacji inteligentnych scenariuszy wsparcia zainteresowanych służb, SBKPG powinien realizować funkcję rejestracji zdarzeń wraz z ich opisem i atrybutem czasu. System bezpieczeństwa kolejowych przejść granicznych (SBKPG) powinien składać się z:

- systemów monitorowania określonych obiektów i terenu kolejowego przejścia granicznego,
- systemów monitorowania infrastruktury znajdującej się na terenie przejścia granicznego,
- systemów monitorowania stanu środowiska na terenie i w otoczeniu przejścia granicznego,
- systemów monitorowania zachowań podróżnych oraz osób znajdujących się na terenie kolejowych przejść granicznych,
- inteligentnej platformy przetwarzania i analizy informacji,
- centrów monitoringu i zarządzania poszczególnych organów administracyjnych i branżowych działających na terenie kolejowych przejść granicznych,
- systemów zbierania danych i dystrybucji informacji.

Na rysunku 1 przedstawiono schematycznie koncepcję systemu bezpieczeństwa kolejowych przejść granicznych. W skład systemów monitorowania określonych obiektów i terenu kolejowego przejścia granicznego w zasadzie wchodzić będą terminale stacjonarne np. wszelkiego rodzaju kamery wizyjne IP, czujniki, sensory, tablice informacyjne, głośniki (megafony). Osobnego omówienia wymagają zaproponowane w koncepcji przenośne terminale, przeznaczone przede wszystkim dla funkcjonariuszy Straży Granicznej i Służby Celnej. Terminale te miałyby służyć do multimodalnej biometrycznej weryfikacji osób i monitoringu zachowań pasażerów przekraczających granicę znajdujących się w pociągu.

Biometryczna weryfikacja osób może być realizowana przez istniejące już systemy rozpoznawania twarzy. Główną zaletą systemów rozpoznawania twarzy jest możliwość przeprowadzania identyfikacji obrazu z urządzeń kontrolnych bez konieczności angażowania osoby rozpoznawanej. Rozpoznawanie twarzy ogranicza się jedynie do pozyskania obrazu twarzy lub ich sekwencji, po czym system sam dokonuje analizy obrazu i podejmuje decyzję czy dana osoba figuruje w bazie danych obrazów twarzy, czy też nie.

Jest kilka gotowych do wdrożenia systemów biometrycznej kontroli tożsamości. Na uwagę zasługuje firma Guardia A/S, zajmująca się biometrycznymi technologiami w systemach zabezpieczeń, oferująca system rozpoznający twarz. Guardia Control jest systemem kontroli, który skanuje twarz, tworząc jej obraz w trzech wymiarach (z dokładnością do 1 mm), mierzy temperaturę skóry (z dokładnością do 0,2°C) i tworzy trójwymiarowy model twarzy. Powstaje trójwymiarowy model wizerunku twarzy oraz trójwymiarowy model termiczny twarzy. Na podstawie tych modeli z około 300 punktów charakterystycznych ustala się wzorzec biometryczny. Skanowanie temperaturowe w zakresie podczerwieni dodatkowo może dostarczyć informacji np. o chorobie osobnika. Zaletą systemu jest to, że działa w pełni autonomicznie, nie angażując żadnych osób w proces skanowania. Urządzenia skanujące nie są narażone na zabrudzenia wynikające z kontaktu fizycznego, jak w przypadku metod skanowania odcisku palca czy dłoni (preferowanych w systemach ochrony lotnisk), i nie angażują uwagi personelu podczas procesu pobierania wzorca. Specjaliści od biometrycznego systemu kontroli Guardia twierdzą, że technologia rozpoznawania 3D jest najbardziej godna zaufania i użyteczna dla celów bezpieczeństwa na rynku, a rozpoznawanie 2D i inne biometryczne systemy znajdują tylko ograniczone zastosowanie (wyniki projektów pilotażowych prowadzonych przez Guardia A/S, w których użyto odcisków palca, rozpoznawania twarzy 2D, tęczy oka, analizy podpisu odręcznego i głosu, uwidaczniają ich niską niezawodność – pomiędzy 40% a 60% – w stosunku do zaprezentowanego systemu 3D [2]. Bardziej skomplikowanym problemem jest biometryczne



Rys. 1. Koncepcja logicznej architektury systemu bezpieczeństwa kolejowych przejść granicznych.

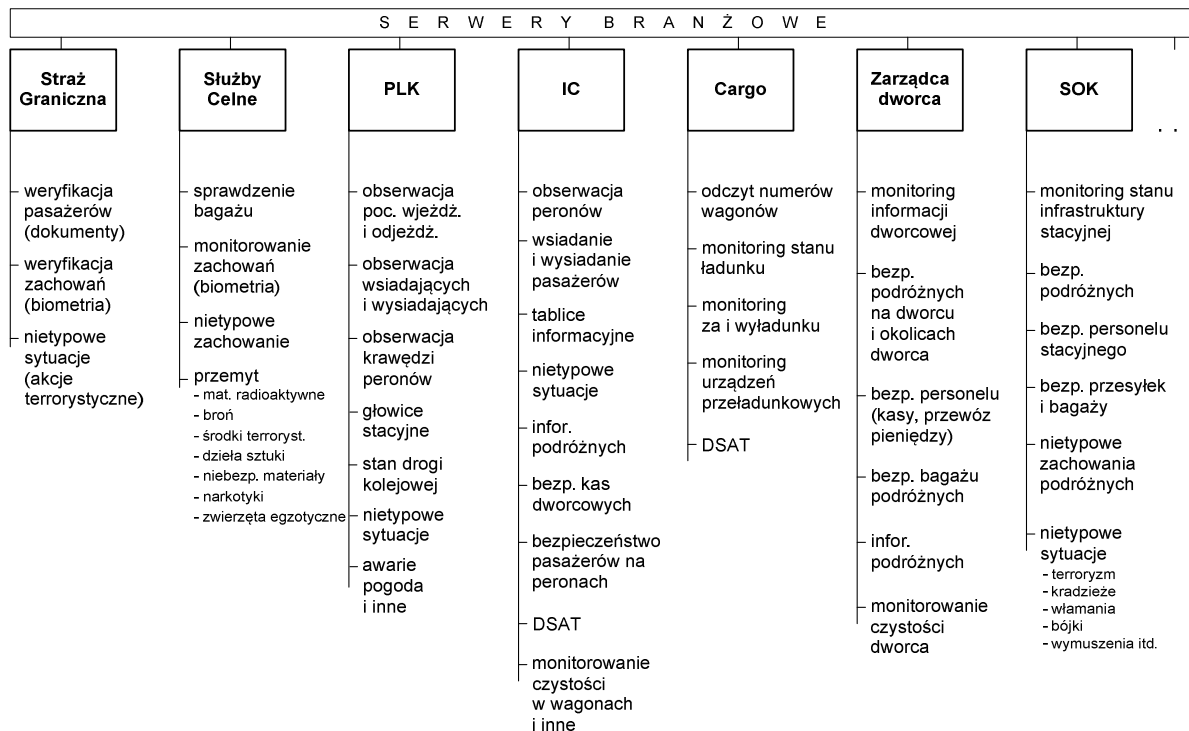
Źródło: opracowanie własne.

monitorowanie zachowań ludzi. Interesujące rozwiązanie przedstawia projekt Cogito izraelskiej firmy Suspect Detection Systems Ltd. W sierpniu 2006 r. opublikowano, że spółka opracowała biometryczny system (biometryczny wykrywacz kłamstw) do wykrywania nienaturalnych zachowań, emocji podczas odpowiedzi na serię wyselekcjonowanych pytań, na podstawie których można domniemać złe zamiary podróżnego. System, nazwany Cogito, używa technik wzorowanych na badaniach poligraficznych. W ciągu kilku minut system określa, czy pasażer może kontynuować podróż, czy też powinien być poddany dalszej i bardziej szczegółowej kontroli. *Suspect Detection* to technologia, która wykorzystuje oprogramowanie emulujące oficera dochodzeniowego, ujawniającego modus operandi sprawcy. System wyszukuje wzory zachowań, które wskazują na coś, czym można scharakteryzować wszystkich potencjalnych sprawców przestępstw (wykroczeń), a mianowicie na obawę wykrycia przez funkcjonariusza przekroczenia przepisów prawnych. System może izolować tych podejrzanych, którzy kwalifikują się do drugiego etapu badania, prowadzonego przez wytrenowanych, doświadczonych badaczy (psychologów). Badania wykazują, iż system jest w wysokim stopniu dokładny i skuteczny (najwyżej czteroprocentowe prawdopodobieństwo wystąpienia fałszywego alarmu) [2].

Na obecnym etapie rozwoju technologii można sobie wyobrazić mobilny terminal do weryfikacji twarzy pasażerów, gdzie praktycznie wystarczy minikamera IP przesyłająca dane drogą radiową do systemu, to zdecydowanie trudniej jest zrealizować mobilny (przenośny) terminal do weryfikacji biometrycznej zachowań pojedynczych pasażerów znajdujących się w przedziale wagonu. Jednakże, należy zauważyć, że prototyp izraelskiej firmy Suspect Detection Systems Ltd został zaprezentowany w lecie 2006 r., a więc pięć lat temu. Biorąc pod uwagę postęp technologiczny i techniczny w branży IT należy mniemać, że stosunkowo w niedługim czasie biometryczna weryfikacja zachowań pasażerów będzie mogła być też realizowana za pomocą terminali przenośnych.

Zdalne centra monitoringu i zarządzania będą tworzone przez poszczególne zainteresowane jednostki działające na terenie przejść granicznych np. Straż Graniczna, Służby Celne, SOK, Policja, Służby fitosanitarne, zarządca infrastruktury – PKP PLK, zainteresowani przewoźnicy itd.

Zadaniem inteligentnej platformy przetwarzania i analizy informacji będzie zbieranie, przetwarzanie, inteligentna analiza, podejmowanie decyzji i kierowanie informacją do określonych punktów zainteresowań. Punktami zainteresowań dla platformy będą serwery branżowego do których będą przesyłane dane pierwotne z określonych dla danego serwera terminali (urządzeń końcowych), następnie te dane będą przesyłane do platformy. Platforma po otrzymaniu danych od serwerów branżowych przetworzy w sposób „inteligentny” otrzymane dane i stworzy odpowiednie informacje skieruje je do poszczególnych serwerów branżowych. Informacje te będą dostępne dla uprawnionych pracowników/funkcjonariuszy według ich kompetencji. Na rysunku 2 przedstawiono przykładowe funkcje przypisane do poszczególnych serwerów branżowych.



Rys. 2. Przykładowe funkcje sprawowane przez serwery branżowe.

Źródło: opracowanie własne.

Do realizacji zadań systemów zbierania danych i dystrybucji informacji powinna być utworzona wydzielona odpowiednio zabezpieczona sieć intranetowa pracująca zgodnie z protokołami MPLS VPN. Wirtualne sieci MPLS VPN same w sobie mają silne zabezpieczenia przed nieautoryzowanym dostępem z zewnątrz sieci, ale w newralgicznych

punktach sieci powinny być stosowane dodatkowe zabezpieczenia np. zaporą sieciową (*Firewall*), które zapewniałyby bezpieczeństwo dostępu do określonych aplikacji (danych) tylko dla określonych użytkowników. Jest oczywistym, że dostęp do Systemu powinien być wielopoziomowy tzn., że każdy użytkownik Systemu będzie uprawniony tylko do określonych dla niego zadań i wynikających z tego funkcji Systemu. Zalecanym w koncepcji rozwiązaniem jest metoda dostępu "Coś, co wiesz" (ang. *Something you know*) - użytkownik zna słowo, może to być numer NIP/PIN, PESEL, hasło, ciąg znaków alfanumerycznych itd. Dostęp do aplikacji, które mają zasadniczy wpływ na działanie całego Systemu a których zamierzona lub niezamierzona modyfikacja mogłaby doprowadzić do wadliwego działania Systemu, powinien być szczególnie chroniony. Do szczególnie ważnych aplikacji można zaliczyć np. dostęp do systemu operacyjnego platformy, dostęp do rekonfiguracji sieci MPLS VPN, baz danych, serwerów branżowych czy też dostęp do rejestratorów. Dostęp do tych aplikacji powinien być weryfikowany poprzez systemy "Kim jesteś i co robisz" (ang. *Something what you are and something that you do*), które odnoszą się do niepowtarzalnych cech anatomicznych i charakterystycznych cech behawioralnych (zachowawczych), indywidualnych dla każdej osoby uprawnionej do przeprowadzenia określonej rekonfiguracji. System kontroli dostępu, w którym wykorzystuje się zasadę "Kim jesteś i co robisz", jest biometrycznym systemem kontroli dostępu. System ten w ogólności złożony jest z czytnika biometrycznego lub urządzenia skanującego, oprogramowania które konwertuje pobraną z czytnika informację do postaci cyfrowej oraz bazy danych, która przechowuje dane biometryczne tj. wzorce niezbędne do porównania z danymi pochodzącymi z czytnika. W czasie konwersji informacji pobranej w czytniku oprogramowanie identyfikuje określone punkty charakterystyczne, które następnie są przetwarzane przy użyciu wybranego algorytmu matematycznego do postaci, która może być w skuteczny sposób porównana z rekordem w bazie danych [3]. Sieć teleinformatyczna dla potrzeb SBKPG powinna być tak zaprojektowana, by każde łącze miało zapewnioną odpowiednią przepustowość zależną od ilości i pilności przesyłanych danych a każda aplikacja mogła gwarantować odpowiednią dla niej jakość usługi.

System SBKPG powinien poprzez odpowiednie interfejsy współpracować z innymi systemami zainstalowanymi na przejściu granicznym np. systemami przeciwpożarowymi czy też systemami informacji podróżnych w celu przesyłania informacji głosowych i wizualnych kierowanych do podróżnych i personelu o potencjalnych zagrożeniach. SBKPG powinien mieć możliwość połączenia się poprzez odpowiednio zabezpieczoną sieć Internetową ze „światem zewnętrznym” tj. np. z określonymi bazami danych policji, Straży Granicznej czy też bazą Służby Celnej, w celu weryfikacji wybranych osób przekraczających granicę państwa. Ponadto System powinien mieć możliwość przesyłania danych dotyczących stanu taboru, danych o ruchu pociągów do centralnych systemów przewoźników jak i operatora infrastruktury np. systemy SEPE (*System Ewidencji Pracy Eksploatacyjnej*), DSAT (*Detekcja Stanów Awaryjnych Taboru*) itp.

System bezpieczeństwa kolejowych przejść granicznych powinien charakteryzować się dużą niezawodnością co można osiągnąć poprzez odpowiednią i zaprojektowaną zgodnie ze sztuką inżynierską, redundancją sprzętową (hardware) i programową (software). Należy również pamiętać o zapewnieniu bezprzerwowego zasilania całego Systemu. Konfiguracja i wielkość poszczególnych składników SBKPG powinna być dostosowana do konkretnego przejścia granicznego. Dlatego też System powinien mieć budowę modułową (dotyczy to powinno zarówno hardware'u jak i software'u) umożliwiającą dołączanie nowych źródeł i ujść danych przez określone interfejsy np. monitoring nowych obiektów, czy też powstanie nowego zdalnego branżowego centrum monitoringu i zarządzania np. przy Komendzie Policji.

PODSUMOWANIE

Każde przejście graniczne a szczególnie przejścia graniczne Unii Europejskiej z krajami nie należącymi do Unii są miejscami narażonymi na przemyt towarów, narkotyków, dzieł sztuki, ludzi a także miejscami potencjalnie narażonymi na przenikanie grup terrorystycznych i niebezpiecznych materiałów. Dlatego też na wszystkich przejściach granicznych są prowadzone odpowiednie kontrole podróżnych i sprawdzanie ich bagażu. Technika sprawdzania i kontroli ciągle jest rozwijana i w dużej mierze zależy od środka transportu. W transporcie lotniczym choć by tylko ze względu na potencjalne zagrożenie terrorystyczne stosuje się indywidualną kontrolę każdego podróżnego i jego bagażu. W transporcie samochodowym kontrola osobista pasażerów i bagażu z różnych względów jest wyciągnięta ale przejścia te nie są narażone na zamachy terrorystyczne (zbyt mało ludzi w danym momencie czasowym i stosunkowo niewielka infrastruktura). Kolejowe przejścia graniczne mogą mieć bogatą infrastrukturę i w określonym przekroju czasowym na tych przejściach może znajdować się na niewielkim terenie stosunkowo dużo ludzi (dwa lub więcej pociągów na stacji). Ponadto na terenie kolejowego przejścia granicznego mogą znajdować się niebezpieczne związki chemiczne, których wyciek lub wybuch może spowodować duże skażenie środowiska stwarzając zagrożenie dla życia ludzi i zwierząt. Chociaż by tylko z tych powodów dla przejść tych należy opracować specjalne procedury i techniki wspierające służby kontrolne w zakresie ochrony ludzi i ich bagażu.

BIBLIOGRAFIA

- [1] Niczyporuk Z., Sienkiewicz – Małyjurek K.: Systemy monitoringu wizyjnego w bezpieczeństwie publicznym. WPS Gliwice 2008.
- [2] Niedziejko P. Krysowaty I. Z biometrią w podróży. Zabezpieczenia 6/2006. AAT Hoplding, Warszawa 2006
- [3] Niedziejko P. Krysowaty I. Biometria-Charakterystyka danych człowieka Część 1, Część 2, Część 3. Zabezpieczenia 6/2006. AAT Hoplding, Warszawa 2006.
- [4] Norman T.: Integrated security systems design. Butterworth Heinemann, 2007.
- [5] Pakulski D.: Cyfrowy monitoring wizyjny w sieciach IP, Zabezpieczenia No.II 2005.
- [6] Siergiejczyk M., Gago S.: Public Safety Issues in Rail Transport. Polish Journal of Environmental Studies. ISSN 1230-1485.Vol 17, No 3C (2008). HARD Publishing Company, Olsztyn 2008.
- [7] www.indect-project.eu
- [8] insigma.kt.agh.edu.pl
- [9] www.marchnetworks.com
- [10] bytomski.pl/viewtopic
- [11] www.trojmiasto.pl/wiadomosci/Najmadrzejszy-monitoring-na-swiecie-powstal-w-Trojmiescie-n39558.html
- [12] www.face-recognition.eu
- [13] www.cybernet.com

THE CONCEPT OF SECURITY SYSTEM ON THE RAILROAD BORDER CROSSINGS EU

Abstract:

In rail transport, as a large system, the issue to ensure the public safety seems particularly important. One of the problems in this area is public safety on the railway border crossings, which are crossing points of the European Union. In the article is made the identification of threats to public security in railway transport, including rail border crossings with non-member European Union countries (Russia, Belarus, Ukraine). There is presented the concept of the railway border crossings safety system performing intelligent scenarios support the process of ensuring security in border crossings, and indirectly on the territory of the all European Union.

Keywords: public safety, railway transport, system, monitoring, border crossings of the European Union