Bernd Hentschel, Zbyszko Pawlak, Karol Górski
Wyższa Szkoła Logistyki

Logistyczny system namierzania, identyfikacji i monitoringu w czasie rzeczywistym osób niebezpiecznych w węzłach transportowych obszarów zurbanizowanych

Badania oraz praktyczne aplikacje systemów zarządzania logistycznego zagrożeniami terrorystycznymi stanowią do tej pory słabo rozpoznany obszar i objęły właściwie tylko problematykę bezpośredniej identyfikacji substancji radioaktywnych. Celem natomiast wprowadzenia proponowanej przez autorów nowej metody identyfikacji jest rozwiązanie kompleksowe, obejmujące różne rodzaje możliwego ataku terrorystycznego, to znaczy chemicznego, biologicznego, radiologicznego i nuklearnego, we wszelkiego rodzaju węzłach transportowych obszarów zurbanizowanych, a więc takich, jak na przykład stacje metra, dworce kolejowe i autobusowe, porty lotnicze oraz żeglugi śródlądowej i morskiej. Realizacja przyjętego celu, polegała na przeprowadzeniu badań opartych na trójstopniowym systemie informatycznym, który skonfigurowano na potrzeby niezawodnej, automatycznej identyfikacji substancji oraz osób podejrzanych o generowanie zagrożeń terrorystycznych w czasie rzeczywistym.

Współczesne wyzwania w dziedzinie bezpieczeństwa ludności wymagają harmonijnego współdziałania wszystkich instytucji państwowych, organów władzy i administracji oraz dostosowania ich metod pracy do nowych zagrożeń, z uwzględnieniem konieczności dysponowania nowoczesnymi, zintegrowanymi systemami kierowania i zarządzania na wypadek kryzysu. Pociąga to za sobą konieczność wyposażenia wszystkich służb, stojących na straży bezpieczeństwa obywatelskiego, w wyspecjalizowany sprzęt techniczny i systemy informacyjne wspomagające monitorowanie, identyfikację i przeciwdziałanie zagrożeniom bezpieczeństwa obywateli, w tym procesy informacyjno-decyzyjne ratownictwa i zarządzania kryzysowego oraz skuteczne kierowanie działaniami ratowniczymi i reagowaniem kryzysowym. Realizacja tych przedsięwzięć wymaga ciągłego doskonalenia technologii wykrywania i prognozowania rozwoju zagrożeń, teleinformatycznego przetwarzania informacji, ochrony i przeciwdziałania zagrożeniom oraz likwidacji ich skutków. Technologie te są ściśle związane z problematyką badawczą „inżynierii bezpieczeństwa" obejmującej dwa obszary: bezpieczeństwo techniczne i bezpieczeństwo cywilne. Obecnie na całym świecie podejmuje się wzmożone wysiłki w celu wypracowania i wdrożenia do eksploatacji nowych strategii i technologii w zakresie ochrony bezpieczeństwa podróżnych w formie różnego typu aplikacji praktycznych.

Nowoczesne technologie na rzecz szeroko rozumianego bezpieczeństwa obejmują przede wszystkim następujące obszary:

- ochronę przed terroryzmem (włączając tak zwany bioterroryzm oraz przypadki użycia niebezpiecznych substancji biologicznych, chemicznych, radioaktywnych, nuklearnych, wysokoenergetycznych materiałów wybuchowych i innych)
- procesy zarządzania kryzysowego
- bezpieczeństwo i ochronę systemów sieciowych
- interoperacyjność oraz integrację systemów informacyjnych i łączności
- poprawę świadomości sytuacji – wiedzy o zagrożeniach.

W obszarach tych za kluczowe uznaje się technologie dla systemów bezpieczeństwa, do których należą między innymi: technologie sensorowe, systemów obserwacji, wykrywania i śledzenia, systemów informacyjnych, modelowania i symulacji. Zakres technologii oraz nowych opracowań naukowo-badawczych mieści się w priorytetach zarówno 6, jak też 7 Programu Ramowego Unii Europejskiej oraz priorytetach technologicznych (CapTech) Europejskiej Agencji Obrony (EDA). Świadczy to o zbieżności polskich priorytetów technologicznych w zakresie bezpieczeństwa z tematyką badawczą Unii Europejskiej co stwarza możliwość rozszerzania i kontynuacji tej tematyki przy wykorzystaniu funduszy europejskich oraz przy współpracy z zagranicznymi ośrodkami badawczymi w ramach wspólnych projektów [1].

Artykuł, jest próbą odpowiedzi na aktualne zainteresowanie zagadnieniami ochrony bezpieczeństwa i implikowanymi przez nie wyzwaniami natury logistycznej. Obejmuje zatem tematycznie problematykę zarządzania zagrożeniami (*Disaster-Management*) w zakresie ataków terrorystycznych typu CBRN[1] w miejscach nasilonych przepływów pasażerskich.

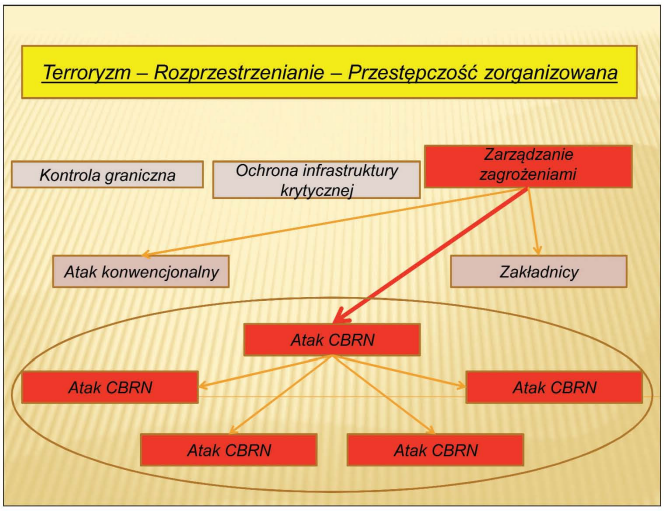
Źródła zagrożeń w węzłach transportowych obszarów zurbanizowanych

Szczególnie zagadnienia ochrony przed terroryzmem oraz wczesne wykrywanie zagrożeń ze strony osób niebezpiecznych w strefach przemieszczania się potoków pasażerskich w węzłach transportowych obszarów zurbanizowanych stanowią główne punkty ciężkości, dla których oferuje się współcześnie cały szereg rozwiązań, charakteryzujących się różnym przebiegiem procesów i czynności logistycznych. Ochrona tych elementów wymaga zastosowania zintegrowanego podejścia do

[1] Skrót CBRN opisuje rodzaje możliwych ataków terrorystycznych, odpowiednio: dla C – atak chemiczny, B – atak biologiczny, dla R – atak radiologiczny i dla N – atak nuklearny. Każda z tych form działalności terrorystycznej stanowi na całym świecie problem o najwyższym, priorytetowym znaczeniu w wymiarze zarówno krajowym, jak i międzynarodowym.

monitorowania i oceny zagrożeń, śledzenia zarówno przepływu pasażerów, jak i produktów a ponadto bezpiecznych procesów wymiany między krajami i operatorami logistycznymi, a także szybkiej i skutecznej ich kontroli.

Ogólnie rzecz biorąc można stwierdzić, że przedsięwzięcia zmierzające do poprawy bezpieczeństwa podróżującej ludności dotyczą trzech sfer. Do pierwszej przykładowo zaliczyć można punkty odpraw granicznych (*Border Control*), do następnej ochronę infrastruktury krytycznej (*Protection of Critical Infrastructure*), a do trzeciej sferę zarządzania niebezpieczeństwem (*Disaster Management*) – oczywiście w przypadku niebezpieczeństw zidentyfikowanych. Schematyczne powiązanie tych wszystkich trzech komponentów oraz niezwykłą złożoność relacji, które wynikają z przedstawionej współzależności, przedstawiono na rysunku1.



Rys. 1. Przykłady relacji pomiędzy zagrożeniami, możliwościami i technologiami. *Źródło: opracowanie własne.*

Zgodnie rodzajami zdarzeń, jakie zachodzą w przestrzeni zarządzania węzłami transportowymi obszarów zurbanizowanych, autorzy artykułu wskazują na rozwiązania przyjęte dla ochrony (*Protection*) przed substancjami niebezpiecznymi klasy CBRN, ich identyfikacji (*Detection*), unieszkodliwiania (*Decontamination*) oraz na funkcjonujące w tym zakresie systemy logistyczne, z uwzględnieniem całej ich złożoności (*Systems Interoperability*). W tym kontekście interesującym aspektem są trendy w zakresie rozwoju sfery poprawy bezpieczeństwa w węzłach transportowych ludności oraz aplikacje konkretnych rozwiązań na obszarze Niemiec. Wartościowy rozkład, przypisany poszczególnym sektorom w odniesieniu do potencjalnych zagrożeń do 2015 roku, wydaje się być bardzo znaczący (rysunek 2).

Rynek systemów bezpieczeństwa w Niemczech 2008 - 2015 (mln €)

Sektor bezpieczeństwa IT	4750 - 10640
Śledztwa i dochodzenia	800 - 920
Likwidacja niebezpieczeństw	2330 - 2370
Systemy antywłamaniowe	7130 - 9520
Identyfikacja	920 - 1720
Sprzęt specjalistyczny	2330 - 2860
Zabezpieczenia przeciwpożarowe	1610 - 2010
Materiały niebezpieczne	2330 - 2370

Rys. 2. Rynek systemów bezpieczeństwa w Niemczech. *Źródło: www.sicherheit.berlin-brandenburg.de (dostęp 18.12.2012) [2].*

Należy w związku z tym założyć, że oprogramowanie dla rozwiązań informatycznych w dziedzinie bezpieczeństwa, ich oprzyrządowanie i wyposażenie, jak również systemy identyfikacyjne mocno zaznaczą swoją obecność na rynku, a w niektórych przypadkach dojdzie do koncentracji, czy też silnego przesunięcia akcentów. Nowoczesne węzły transportowe ludności wyposażone są z reguły w szereg instalacji alarmowych oraz technicznych systemów zapewniających bezpieczeństwo ich funkcjonowania. Przykładowo systemy zarządzania bezpieczeństwem budynków (*Building Management Systems* – BMS) integrują:

- systemy bezpieczeństwa (system przeciwpożarowy, system antynapadowo-włamaniowy, system kontroli dostępu, system telewizji dozorowej)
- teleinformatyczne systemy bezpieczeństwa (system bezpieczeństwa zasobów komputerowych, system bezpieczeństwa transmisji danych, system ochrony fizycznej urządzeń teleinformatycznych)
- systemy sterujące automatyką budynku (klimatyzacja, praca wind, oświetlenie, zasilanie w media – woda, gaz, elektryczność).

BMS zapewnia techniczne narzędzia zarządzania bezpieczeństwem i komfortem pracy w budynku w warunkach codziennej eksploatacji i w sytuacjach awaryjnych. BMS nie zabezpiecza bezpieczeństwa węzłów transportowych ludności w sytuacji kryzysowej, gdy uszkodzenia infrastruktury i urządzeń technicznych spowodują dezintegrację systemu. W takich przypadkach konieczna jest pomoc z zewnątrz – w postaci zarządzania kryzysowego, które jest zespołem wcześniej opracowanych procedur postępowania, informacji wprowadzanych na bieżąco w oparciu o dane służb rozpoznania i ratownictwa oraz procedur opracowanych dla minimalizacji skutków zagrożenia terroryzmem (chemicznym, biologicznym, radiologicznym itp.). Wymaga to prowadzenia i koordynowania prac w wielu kierunkach, zarówno studiów systemowych jak też doboru i badania odpowiedniej bazy sensorów [3].

Logistyczne rozwiązania systemu namierzania, identyfikacji i monitoringu w czasie rzeczywistym osób niebezpiecznych

Wszechstronne wyposażenie służb reagowania kryzysowego w różnego rodzaju urządzenia oraz tworzenie na ich bazie systemów wykrywania i powiadamiania jest warunkiem początkowym i koniecznym wszelkich działań mających zapewnić ochronę przed skutkami zagrożeń [4]. Monitorowanie zagrożeń bezpieczeństwa można logistycznie prowadzić w stałej sieci pomiarowej lub w ruchomych punktach pomiarowych.

Metody stosowane w monitorowaniu zagrożeń CBRN, z punktu widzenia sposobu pobierania próbek do analizy, można podzielić na dwie grupy: 1) próbkowanie w miejscu występowania zagrożenia; 2) zdalna detekcja, identyfikacja i pomiar stężenia substancji niebezpiecznej. W pierwszej grupie metod, z powodu rozdzielenia w czasie i przestrzeni miejsc pobrania próbki i jej analizy, dokładność i jednoznaczność pomiarów jest mało precyzyjna. Metody zdalne pozbawione są tych wad i w zależności od zastosowanej techniki pomiarowej umożliwiają prowadzenie monitorowania środowiska nawet na bardzo dużych odległościach. W zdalnej detekcji szczególną rolę odgrywają metody i technologie optoelektroniczne, które jako bardzo precyzyjne narzędzie wykrywania i określania stężeń gazowych zanieczyszczeń atmosfery coraz częściej wypierają w monitorowaniu środowiska metody tradycyjnie stosowane (na przykład metody chemii mokrej, chromatografia). Do najważniejszych zalet metod optoelektronicznych należy zaliczyć możliwość pełnej automatyzacji pomiaru, jednoznaczność wyników, możliwość dokonywania pomiarów bez konieczności pobierania próbki, a także zintegrowanie różnych systemów elektrooptycznych w procesie zbierania, przetwarzania i transmisji danych.

Wyróżnić można 2 rodzaje systemów zdalnego monitorowania: typu „stand-off" i typu „remote" [5]. Systemy „stand-off" (na przykład czujniki optyczne) pozwalają wykrywać zagrożenia ze znacznej odległości bez kontaktu z obszarem jego występowania. Są to przykładowo aktywne systemy laserowe (*Difference Absorption Lidar*) DIAL lub pasywne systemy termowizyjne [6]. Pojedyncza stacja typu „stand-off" może pokryć znaczny obszar, którego wielkość zależy od zasięgu, pola widzenia i szybkości skanowania. Systemy typu „remote" wykorzystują różne rodzaje niewielkich czujników punktowych „in situ" (*łac.* „w miejscu" – *przyp. red.*), przy czym dane z tych czujników przesyłane są za pomocą łącz przewodowych lub bezprzewodowych do centrów alarmowych. Centra te analizują dane przychodzące z sieci czujników i określają poziom zagrożenia.

Proponowany w przeprowadzonych przez autorów badaniach projekt logistycznego rozwiązania systemu typu ROIT (*Real-time Observation, Identification and Tracking from dangerous persons in airports*), został zaprojektowany w ten sposób, że możliwa jest aplikacja trójstopniowego systemu informatycznego, skonfigurowanego na potrzeby identyfikacji, obserwacji i zabezpieczenia przed niepożądanym działaniem ze strony osób, co do których istnieje podejrzenie o generowanie zagrożeń typu CBRN. Celem praktycznej aplikacji systemu jest:

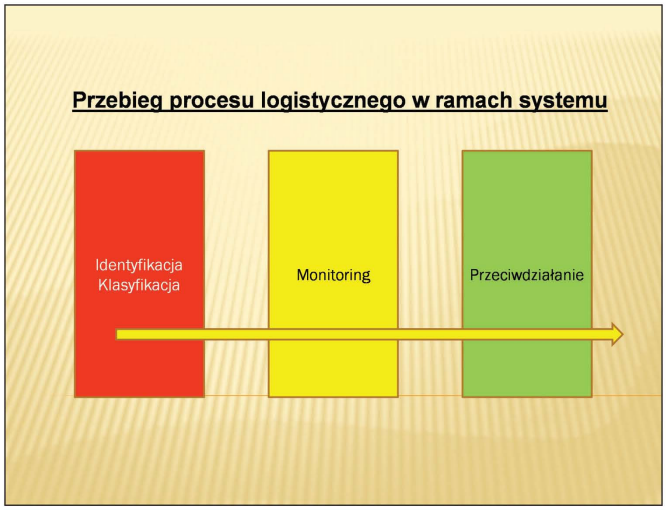
- umożliwienie niezawodnej, automatycznej identyfikacji oraz klasyfikacji potencjalnych materiałów i substancji niebezpiecznych przy powiązaniu ich z właścicielami lub dysponentami
- stworzenie możliwości równoległego przekazywania stosownych informacji do odpowiednich służb ochrony węzłów transportowych obszarów zurbanizowanych (stacji metra, dworców kolejowych i autobusowych, portów lotniczych oraz żeglugi śródlądowej i morskiej), a także zespołów ekspercckich i systemów bezpieczeństwa ogólnego (policja, wojsko)
- zagwarantowanie możliwości samodzielnej obserwacji w czasie rzeczywistym osób, co do których istnieje podejrzenie o generowanie zagrożeń typu CBRN, po zebraniu relewantnych informacji od współdziałających służb i instytucji współpracujących
- umożliwienie dyskretnej i sprawnej eliminacji tego typu osób ze strumienia przepływu pasażerów w przestrzeni węzłów transportowych obszarów zurbanizowanych po ich skutecznej i wiarygodnej identyfikacji.

Sekwencję realizacji procesów logistycznych w ramach proponowanego systemu przedstawiono na rysunku 3, natomiast poszczególne sekwencje procesu zostaną omówione oddzielnie, dla zobrazowania zakresu i zawartości produktu, który stanowi cel rozwiązania w ramach zrealizowanego projektu.

Identyfikacja / Klasyfikacja

Automatyczna identyfikacja oraz klasyfikacja osób, co do których istnieje podejrzenie o generowanie zagrożeń typu CBRN, powinna być realizowana w oparciu o inteligentny system detekcyjny. W tym celu każdy z pasażerów musi zostać poddany osobnej kontroli pod kątem ewentualnego posiadania materiałów niebezpiecznych, bez konieczności generowania nadmiernych kosztów i obciążeń zarówno po stronie pasażerów, jak również po stronie personelu. Działanie to powinno pozostawać bez wpływu na bieżącą, sprawną obsługę pasażerów, bez tworzenia zatorów, czy też innego rodzaju komplikacji.

Proces identyfikacji i klasyfikacji podróżnych pod kątem prewencji zagrożeń realizowany jest zatem niezależnie i niezauważalnie dla badanego obiektu, czy też obserwowanej osoby w oparciu o innowacyjny system detekcyjny w korelacji z odpowiednim systemem logistycznym. Sposób działania systemu można opisać następująco: sensory identyfikacyjne „dozorują" nieprzerwanie określony obszar, na który wkraczają kontrolowane osoby. Dzieje się tak w obrębie śluz spowalniających o pojedynczej przepustowości, w obrębie punktów odpraw (*check-in*) i innego typu podobnych miejsc, działających na zasadzie zwężającej się „szyjki butelki" (*bottle-necks*) – predestynowanych przez swoją konfigurację do realizacji przedmiotowych czynności. W przypadku reakcji sensorów na jeden lub więcej materiałów niebezpiecznych, system klasyfikuje je w zależności od danego poziomu działań alarmujących i uruchamia tym samym odpowiednie działania interwencyjne. Sche-



Rys. 3. Przebieg procesu logistycznego w ramach systemu.
Źródło: opracowanie własne.

mat działania systemu (rysunek 4) wyjaśnia zasadę identyfikacji, podczas której osoba (4) w sposób wymuszony musi przejść przez specjalne zwężenie w kształcie nawiązującym do „szyjki od butelki" (1). W momencie przekraczania zwężenia następuje identyfikacja w strefie aktywnej (2) w efekcie zadziałania urządzenia (3). W przypadku pozytywnego wyniku działań identyfikujących (o ile osoba jest w posiadaniu materiałów niebezpiecznych z klasy CBRN) następuje stosowana klasyfikacja i zakwalifikowanie przypadku do odpowiednich poziomów alarmowania.

W oparciu o 5 poziomów alarmowania (tabela 1) można wygenerować różne opisane działania w celu ochrony przed potencjalnym zagrożeniem, ponadto zatrzymać podejrzane osoby oraz materiały niebezpieczne w celu ich eliminacji z przestrzeni węzłów transportowych (w ramach wielopoziomowego zarządzania sytuacjami niebezpiecznymi). W oparciu o ten system zarządzania, wszystkie zainteresowane ogniwa bezpieczeństwa (policja państwowa, policja municypalna, wojsko, służby celne oraz agencje ochrony) mogą właściwie zareagować na zagrożenie i zaplanować adekwatne do sytuacji wspólne działania prewencyjne w ramach operacyjnego zarządzania sytuacjami niebezpiecznymi.

Tab. 1. Możliwe poziomy alarmowania.

Poziom alarmu	Materiał niebezpieczny
0	Nie zidentyfikowano żadnego materiału niebezpiecznego
1	Materiały trujące i odurzające
2	Materiały wybuchowe/chemiczne
3	Materiały radioaktywne
4	Materiały wybuchowe i radioaktywne

Źródło: opracowanie własne.

Monitoring

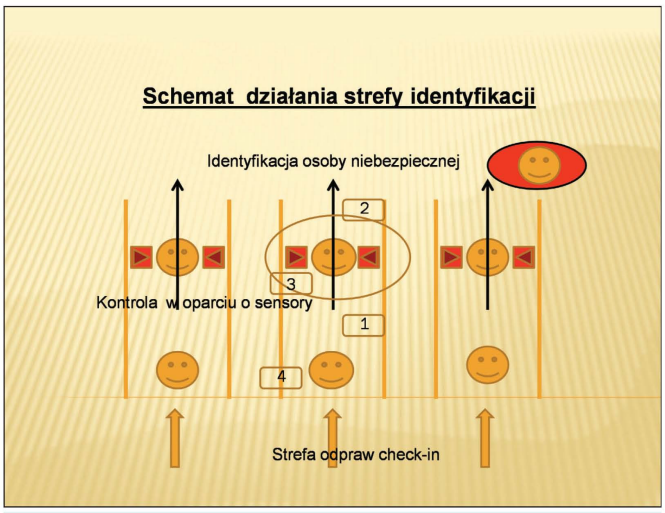
Po dokonaniu identyfikacji i klasyfikacji pojawia się zawsze zadanie dalszej, dyskretnej obserwacji danej osoby lub obiektu (poprzez skoordynowany monitoring wraz z wizualizacją w formie obrazu na monitorze). W tym celu należy zaaplikować funkcjonujący w oparciu o sensory system informatyczny, który w zależności od poziomu alarmowania w ramach procedury śledzenia na monitorze, będzie w stanie te osoby lub obiekty oznaczać i monitorować. Monitoring ekranowy służy do wizualnej identyfikacji osób i obiektów na monitorze przez personel kontrolujący. W tabeli 2 podano klasyfikację kolorystyczną, odpowiadającą każdemu proponowanemu poziomowi alarmowania.

Wszystkie obiekty noszące znamiona potencjalnego ryzyka są dalej monitorowane obrazem. Każdemu obrazowi, towarzyszą informacje dodatkowe, odpowiadające danemu poziomowi alarmowania. Ten optyczny środek pomocniczy jest niezbędny jako wyposażenie dla personelu kontrolującego,

Tab. 2. Klasyfikacja kolorystyczna w zależności od poziomu alarmowania.

Poziom alarmu	Klasyfikacja kolorystyczna
0	zielony
1	żółty
2	pomarańczowy
3	czerwony
4	fioletowy

Źródło: opracowanie własne.



Rys. 4. Schemat działania systemu identyfikacji podróżnych w obrębie punktów odpraw (check-in). *Źródło: opracowanie własne.*

ponieważ w oparciu o obraz z kamery może przesłać szerszy opis dla zainteresowanych służb ochrony bezpieczeństwa danego węzła transportowego. Rozszerzona charakterystyka osoby opiera się zatem na obrazie z kamery kontrolnej oraz zawiera wszystkie niezbędne informacje, które umożliwiają dokładną identyfikację osoby postrzeganej jako potencjalnie niebezpieczna.

Ze strony oprogramowania i oprzyrządowania informatycznego musi być zapewniona możliwość ograniczenia funkcji namierzania i obserwacji do jednego, określonego pomieszczenia. Celem tego zastrzeżenia jest uzyskanie sprzężenia zastosowanych systemów sensorycznych i oprogramowania dla procesu „wykrywania", aby można było go skonfigurować międzyoperacyjnie dla eliminacji strat informacyjnych. Poza tym, rzeczą niezmiernie ważną jest zapewnienie ciągłości łańcucha informacyjnego w celu konsekwentnej ochrony przed potencjalnymi zagrożeniami. Takie rozwiązanie powinno zostać skonfigurowane w postaci swoistego łańcucha informacyjnego, łączącego szereg pomieszczeń oraz zawierać możliwie wszystkie znane rozwiązania innowacyjne z dziedziny wykrywania i monitorowania zagrożeń. Te dwa aspekty, to znaczy „oznaczanie obiektu kontrolnego" oraz „konsekwent-

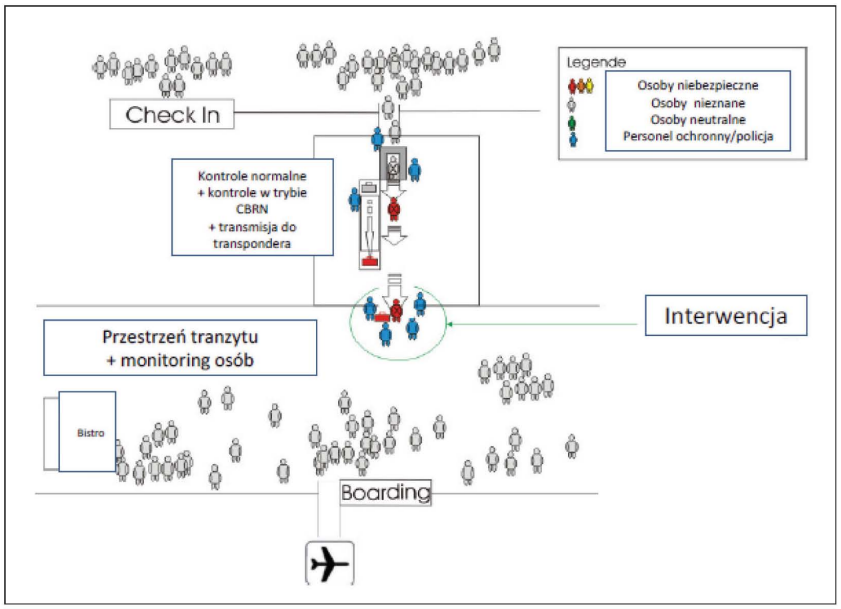
Rys. 5. Realizacja czynności „oznaczania osoby" w ramach doświadczenia laboratoryjnego. *Źródło: materiały konsorcjum Karp GmbH / Technische Hochschule Wildau / Projektlogistik GmbH.*

na kontrola istotnych dla bezpieczeństwa węzła transportowego obiektów przez kilka stref dozoru", stanowią punkt ciężkości systemu wykrywania i monitoringu potencjalnych zagrożeń. W tym zakresie opracowano już system wykrywania pod nazwą „CASTAF" (*Computer Aided Screening, Tracking and Fixing*) [7]. Rysunek 5 pokazuje czynność oznaczania obserwowanej osoby i wynik takiego oznaczania w ramach przeprowadzonego doświadczenia laboratoryjnego, zawierającego obraz całokształtu drogi poruszania się monitorowanej osoby – w tym przypadku na terenie portu lotniczego.

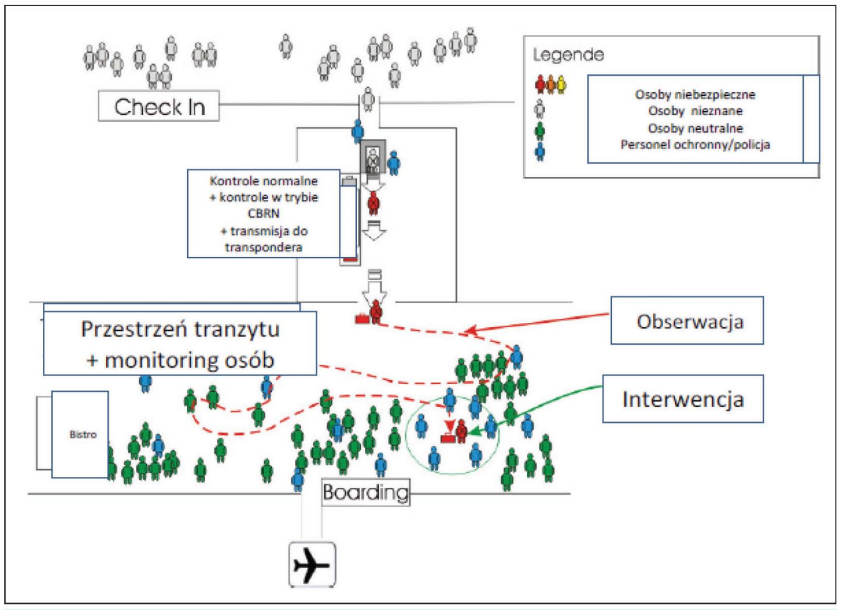
Wyodrębnienie osoby stwarzającej zagrożenie i zabezpieczenie materiału niebezpiecznego

Finalnym segmentem proponowanego systemu jest możliwość celowego wyodrębnienia osoby zidentyfikowanej jako stwarzająca potencjalne zagrożenie oraz zabezpieczenie materiału niebezpiecznego, i – tym samym – skuteczna prewencja zagrożenia. Same czynności zabezpieczenia (przejęcia) materiałów i substancji niebezpiecznych skorelowane są indywidualnie z danym poziomem alarmowania, jak również z warunkami przestrzennymi danego pomieszczenia. Na rysunku 6 (a, b, c, d) przedstawiono poszczególne scenariusze działań detekcyjnych oraz działań zabezpieczania materiałów niebezpiecznych w kolejnych wariantach, na przykładzie portu lotniczego.

Wszystkie przedstawione na rysunku 6 warianty w tym kształcie są zasadniczo możliwe do realizacji w każdego rodzaju pasażerskim węźle transportowym obszarów zurbanizowanych, aczkolwiek wykazują zarówno zalety, jak i wady. W powiązaniu z powstającym systemem detekcyjnym i wspomaganym komputerowo, za sprawą odpowiedniego oprogramowania systemem sterowania czynnościami monitoringu osób podejrzanych o posiadanie materiałów i substancji niebezpiecznych, zarysowano szerokie pole do przedmiotowych badań i rozwoju. W tym zakresie funkcjonują już także scenariusze cząstkowe, zdefiniowane poniżej.



Rys. 6 a. Wariant 1. *Źródło: opracowanie własne.*



Rys. 6 b. Wariant 2. *Źródło: opracowanie własne.*

Poziom alarmu 1: *materiały trujące i odurzające (narkotyki)*

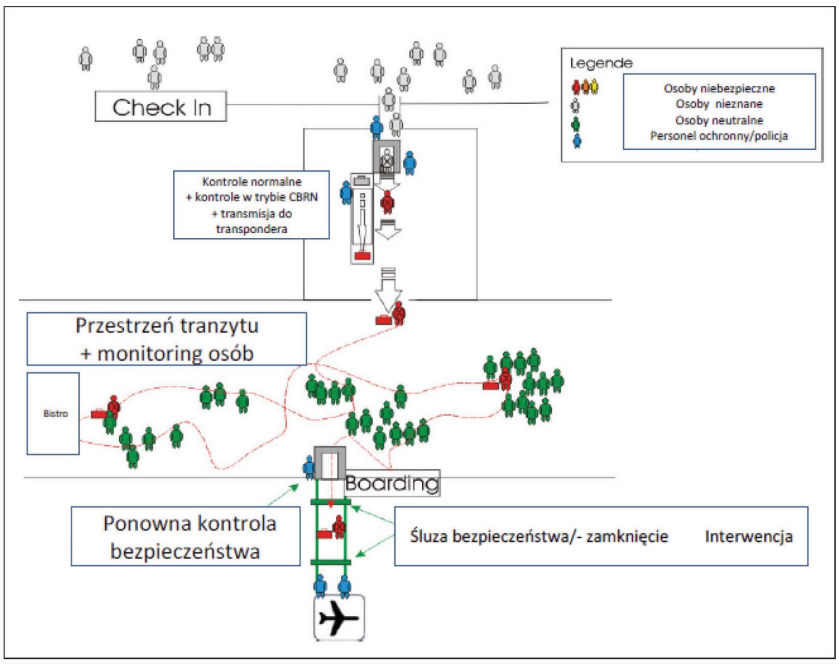
Potencjalne zagrożenie, jakie niesie ze sobą osoba przewożąca tego typu substancje, ocenia się jako niewielkie, gdyż na ogół chodzi tylko o uniemożliwienie ich dalszego transportu. Jak wynika z wieloletnich obserwacji, kurierzy narkotyków nie posiadają broni z uwagi na małe ilości przemycanych substancji. Z tego względu zabezpieczenie (przejęcie) może odbyć się w każdym miejscu.

MOŻLIWY SCENARIUSZ ZABEZPIECZENIA (PRZEJĘCIA): rozszerzona charakterystyka osoby, jej aktualna pozycja i kierunek przemieszczania zostają przekazane do służb prewencyjnych na miejscu. Odpowiedni zespół interwencyjny zbliża się w sposób dyskretny do wskazanej osoby i prosi personel kontrolny o potwierdzenie zgodności danej osoby z przedmiotem interwencji. Interwencja następuje sprawnie i w miarę możliwości dyskretnie. W najbliższym biurze służb prewencyjnych następuje przesłuchanie i przejęcie narkotyków lub innych substancji podwyższonego ryzyka.

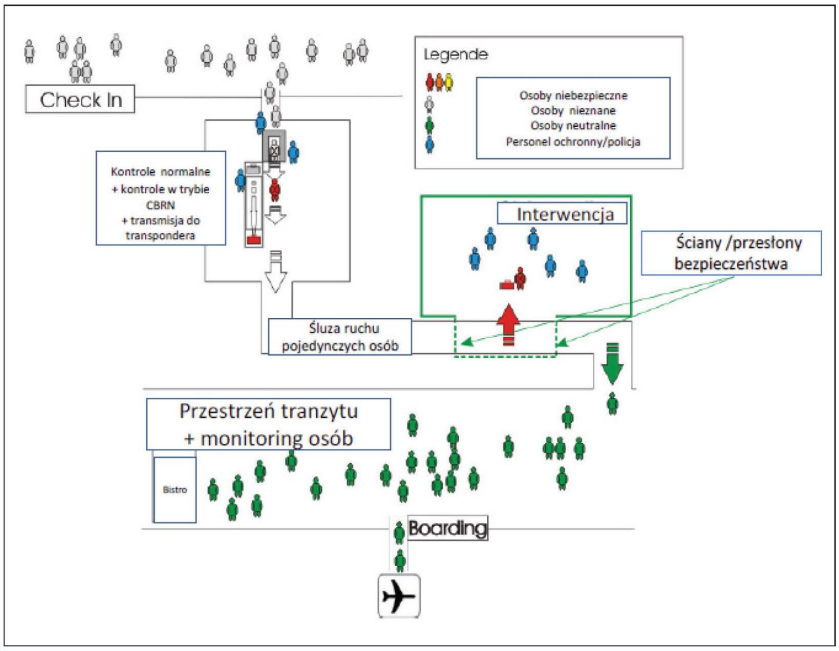
Poziom alarmu 2: *materiały wybuchowe/chemiczne/biologiczne*

Poziom ten dotyczy potencjalnie wysokiego zagrożenia dla wszystkich uczestników scenariusza wydarzeń (służby prewencji węzła transportowego, pasażerów oraz osoby powodującej zagrożenie), z uwagi na istnienie wielu ukrytych aspektów nielegalnego przewozu lub realizacji określonego zamiaru przestępczego (Czy materiał wybuchowy / chemiczny / biologiczny jest tylko przewożony? Czy materiał wybuchowy sta-

nowi już element jakiejś większej całości, na przykład bomby? W jaki sposób dojdzie do odpalenia ładunku wybuchowego?). Z uwagi choćby tylko na powyższe aspekty, służby prewencji węzła transportowego muszą wychodzić zawsze z poziomu scenariusza dla najgorszego możliwego przypadku („*Worst-Case-Scenario*") i do tego scenariusza dostosować wszystkie działania. Podstawowym elementem tych działań jest tworzenie śluzy w formie sztucznej „szyjki butelki", która powinna umożliwiać oddzielenie obiektu potencjalnego ryzyka od ogólnie dostępnej przestrzeni węzła transportowego, a tym samym eliminacji źródła zagrożenia z otoczenia.



Rys. 6 c. Wariant 3. *Źródło: opracowanie własne.*



Rys. 6 d. Wariant 4. *Źródło: opracowanie własne.*

MOŻLIWY SCENARIUSZ ZABEZPIECZENIA (PRZEJĘCIA): Sensem i celem instalacji śluz typu „szyjka butelki" jest oddzielenie źródła zagrożenia, a zarazem obiektu niosącego potencjalne ryzyko, od otoczenia. Aby to oddzielenie efektywnie zrealizować, osoba / obiekt muszą zostać wyodrębnione z szerszej grupy pasażerów. Zespół interwencyjny organu prewencji węzła transportowego otrzymuje informacje dotyczące poziomu alarmu, rozszerzonej charakterystyki osoby, jak również pozycji obiektu potencjalnego ryzyka. Z uwagi na fakt, że śluzy w formie „szyjki butelki" stanowią elementarną część koncepcji ochrony bezpieczeństwa pasażerów na obszarze praktycznie wszystkich węzłów transportowych, wyodrębniony i monitorowany obiekt musi przez taką śluzę przejść. W międzyczasie członkowie brygady antyterrorystycznej zajmują pozycje w określonej uprzednio śluzie bezpieczeństwa i przylegającej do niej przestrzeni izolacyjnej. Zarówno śluza bezpieczeństwa, jak również przestrzeń izolacyjna muszą w przypadku eksplozji być w stanie zaabsorbować powstające przy wybuchu naciski i siły tak, aby w możliwie największym stopniu stłumić skutki detonacji. Interwencja w miarę możliwości nie powinna zakłócić bieżącej obsługi ruchu pasażerskiego.

***Poziom alarmu 3:** materiały radioaktywne*

W zasadzie scenariusz postępowania w tym przypadku bazuje na zasadach podobnych do dotyczących poziomu alarmu 1. Ze względu na to, że zidentyfikowana zostaje obecność materiału radioaktywnego, wychodzi się z założenia, że sprawa dotyczy tylko czystego przemytu. Tym samym zagrożenie skupia się w zasadzie tylko na promieniowaniu radioaktywnym. W uzupełnieniu do reguł postępowania jak przy poziomie alarmu 1, interweniujący funkcjonariusze muszą być wyposażeni w elementy ochronne, przy czym ich kontakt z materiałem radioaktywnym powinien być sprowadzony do niezbędnego minimum. Typ przeprowadzanych działań należy określić przy zabezpieczaniu i przejęciu materiału radioaktywnego, a to zależy każdorazowo od kierownictwa akcji na miejscu zdarzenia.

***Poziom alarmu 4:** materiały wybuchowe i radioaktywne*

Kombinacja materiałów wybuchowych z materiałami radioaktywnymi (*dirty bomb*), jak również w kombinacji z materiałami biologicznymi, stanowi najwyższy stopień zagrożenia terrorystycznego przede wszystkim z uwagi na fakt, że eksplozja powoduje szerokie rozproszenie materiału radioaktywnego / biologicznego, a tym samym powoduje wysokie skażenie otoczenia. Powstają przy tym znaczne szkody towarzyszące eksplozji. Na potrzeby ochrony przed tego typu zagrożeniem należy zaadaptować tryb postępowania, jak w przypadku poziomu alarmu 2, aczkolwiek rozszerzony o dodatkowe przedsięwzięcia ochronne dla personelu z oddziałów prewencji węzła trans-

portowego oraz samych pasażerów. Dla zminimalizowania zagrożenia należy doprowadzić do częściowego zatrzymania względnie spowolnienia napływającego strumienia innych pasażerów – jednakże w ramach tych działań nie może powstać u osoby monitorowanej wrażenie, że ona sama i zamiary jej działania zostały rozpoznane.

Podsumowanie

Proponowana nowa metoda gwarantuje możliwość kompleksowej obserwacji w czasie rzeczywistym osób, co do których istnieje podejrzenie o generowanie zagrożeń typu CBRN. Dodatkowo system umożliwia dyskretną i sprawną eliminację tego typu osób ze strumienia przepływu pasażerów w przestrzeni węzłów transportowych na wszelkiego typu w obszarach zurbanizowanych, po ich skutecznej i wiarygodnej identyfikacji.

Rozwój nowoczesnych technologii, wspomagających zarówno służby prewencyjne szczebla państwowego, jak i municypalnego w realizacji strategicznych zadań ochrony przed zagrożeniami terrorystycznymi, ma charakter interdyscyplinarny i obejmuje wiele sektorów społecznych i gospodarczych. W zakresie logistycznego wspomagania procesów informacyjno-decyzyjnych zarządzania kryzysowego, wyselekcjonowane technologie, na rozwoju których powinien zostać skoncentrowany wysiłek badawczy, powinny być wspierane przez wieloletnie programy finansowane przez administrację państwową oraz przemysł. W oparciu o wnioski płynące z międzynarodowych doświadczeń w zakresie generowanych zagrożeń typu CBRN w różnego typu węzłach transportu pasażerskiego, zostały przedstawione w niniejszym artykule różne scenariusze z zakresie identyfikacji, monitorowania i zatrzymywania osób niebezpiecznych. Rozwijany obecnie w sposób kompleksowy system prewencji, wraz ze wspierającym go systemem logistycznym stanowią aktualnie główny punkt ciężkości badań i praktycznych aplikacji, podejmowanych w tym zakresie w wielu państwach.

Streszczenie

W artykule poddane zostały analizie zagadnienia problematyki zarządzania logistycznego zagrożeniami (*Disaster-Management*), w zakresie ataków terrorystycznych typu CBRN (C – atak chemiczny, B – atak biologiczny, dla R – atak radiologiczny i dla N – atak nuklearny) w węzłach transportowych obszarów zurbanizowanych (stacje metra, dworce kolejowe i autobusowe, porty lotnicze oraz żeglugi śródlądowej i morskiej). Każda z wymienionych form działalności terrorystycznej stanowi na całym świecie problem o najwyższym i priorytetowym znaczeniu w transporcie pasażerskim. Proponowany w przeprowadzonych przez autorów badaniach projekt nowego logistycznego rozwiązania systemu typu ROIT (*Realtime Observation, Identification and Tracking from dangerous persons in airports*), został zaprojektowany w ten sposób, że możliwa jest aplikacja trójstopniowego systemu informatycznego, skonfigurowanego na potrzeby identyfikacji, obserwacji i zabezpieczenia przed niepożądanym działaniem ze strony osób, co do których istnieje podejrzenie o generowanie zagrożeń typu CBRN. Celem praktycznej aplikacji systemu w różnych scenariuszach jest: umożliwienie niezawodnej, automatycznej identyfikacji oraz klasyfikacji potencjalnych materiałów i substancji niebezpiecznych przy powiązaniu ich z właścicielami lub dysponentami, stworzenie możliwości równoległego przekazywania stosownych informacji do odpowiednich służb ochrony węzłów transportowych obszarów zurbanizowanych oraz zespołów eksperckich i systemów bezpieczeństwa ogólnego (policja, wojsko), zagwarantowanie możliwości samodzielnej obserwacji w czasie rzeczywistym osób, co do których istnieje podejrzenie o generowanie zagrożeń typu CBRN oraz umożliwienie dyskretnej i sprawnej eliminacji tego typu osób ze strumienia przepływu pasażerów w węzłach transportowych, po ich skutecznej i wiarygodnej identyfikacji.

A logistics system of realtime observation, identification and tracking from dangerous persons in transport junction of urban areas

Summary

The topic scrutinized in the following article concerns the Disaster Management and concentrates particularly on terrorist attacks of CBRN type (C – chemical attack/weapon, B – biological attack/weapon, R – radiological attack/weapon, N – nuclear attack/weapon) in transport junction of urban areas (metro stations, railway and bus stations, airports and harbours). Each of the aforementioned is an issue of great importance and high priority for the passenger transport. The ROIT project (Realtime Observation, Identification and Tracking from dangerous people in airports) has been designed in a way that enables the application of the three-steps computer system. The programme has been configured to identify, observe and protect from undesired actions of people suspected of involvement in CBRN. The main aims of applying the device in different scenarios are: enabling reliable automatic identification and classification of potentially hazardous materials and substances, association of the materials with their owners or distributors and simultaneous alerting the transport junction security of urban areas, expert team and general security systems (police, military forces). Further purposes involve the independent opportunity to observe the suspects as well as to eliminate them secretly and quickly from the rest of passengers flow in transport junction, after thorough and credible identification.

Literatura / Bibliography

1. www.eda.europa.eu/publications/12-04-04/EDA_2011_Annual_Report (dostęp 28.02.2013).
2. www.sicherheit.berlin-brandenburg.de (dostęp 18.12.2012).
3. Valera M., Velastin S. A., Intelligent distributed surveillance systems: a reviev, Vision, Image and Signed Processing, IEE Proceedings, vol. 152 (2), 2005, pp. 192-204.
4. Jane's NBC Protection Equipment 2001-2002, Jane's Defence Data, 2001.
5. Harig R., Matz G., Toxic Cloud imaging by Infrared Spectrometry: A Scanning FTIR System for Identification and Visualization, Field analytical Chemistry and Technology 5 (1-2), 2001, pp. 75-90.
6. Kovalev V. A., Eichinger W. E., Elastic Lidar. Theory, Practice and Analysis Methods, J. Wiley Interscience Publication, 2004, pp. 65-67.
7. www.zlur.de/zentrum-lur/projekte/ (dostęp 20.12.2012)