VI KONFERENCJA ŁĄCZNOŚCI

Ewolucja wojskowych systemów teleinformatycznych oraz Lessons Learned w świetle misji pokojowych i stabilizacyjnych

PRACA ZBIOROWA

15 SBWD

SIERADZKIE CENTRUM KULTURY

Sieradz 2015

VI KONFERENCJA ŁĄCZNOŚCI

ŚWIATOWY ZWIĄZEK POLSKICH ŻOŁNIERZY ŁĄCZNOŚCI,
15 SIERADZKA BRYGADA WSPARCIA DOWODZENIA
STOWARZYSZENIE PRZYJACIÓŁ 15 SBWD

EWOLUCJA WOJSKOWYCH SYSTEMÓW TELEINFORMATYCZNYCH ORAZ LESSONS LEARNED W ŚWIETLE MISJI POKOJOWYCH I STABILIZACYJNYCH

22-23.04.2015 r.

REDAKCJA NAUKOWA:
ppłk dr inż. Mariusz FRĄCZEK

SIERADZ 2015

RECENZENCI:
prof. dr hab. inż. Józef JANCZAK
płk prof. dr hab. inż. Jan POSOBIEC

REDAKCJA NAUKOWA:
ppłk dr inż. Mariusz FRĄCZEK

KOMITET NAUKOWY:
płk dr hab. inż. Piotr DELA
płk dr inż. Maciej MARCZYK
ppłk dr inż. Mariusz FRĄCZEK
ppłk dr inż. Bartosz BIERNACIK

KOMITET ORGANIZACYJNY:
płk Roman Januszewski
Światowy Związek Polskich Żołnierzy Łączności
Stowarzyszenie Przyjaciół 15 SBWD
płk dr hab. inż. Piotr DELA
płk dr inż. Maciej MARCZYK
ppłk dr inż. Mariusz FRĄCZEK
ppłk dr inż. Bartosz BIERNACIK
mjr mgr inż. Radosław URYCKI
Beata MICHALSKA
Andrzej DURSKI
Piotr CYRANOWICZ

PROJEKT OKŁADKI:
Beata MICHALSKA

Książka sfinansowana z dotacji Ministerstwa Obrony Narodowej

Opracowanie zawiera materiały zaprezentowane podczas konferencji.
Forma i treść przedstawienia materiałów odpowiada wersji przekazanej przez autorów.

ISBN 978-83-940387-1-7

SPIS TREŚCI

WSTĘP

Rozwój nowoczesnych środków komunikacji znajduje naturalne odzwierciedlenie w środkach łączności i informatyki coraz częściej eksploatowanych w Siłach Zbrojnych Rzeczypospolitej Polskiej. Stopniowe wyposażenie w nie jednostek dowodzenia poziomu taktycznego oraz Pułku Dowodzenia i Brygad Wsparcia Dowodzenia powoduje, iż stawiane zadania są realizowane na wysokim poziomie, skutecznie zapewniając wierność, skrytość oraz terminowość wymiany informacji. Z kolei wzrost znaczenia informacji dla działań wojsk wymusił dostosowywanie ich systemów dowodzenia oraz kierowania i sterowania środkami walki do kolejnych wyzwań w zakresie szeroko rozumianej teleinformatyki.

Miasto Sieradz jest od wielu lat związane z Wojskami Łączności i Informatyki. Jest miejscem, w którym dostrzeżono potrzebę dokonywania analiz oraz cyklicznych spotkań i dyskusji w gronie ekspertów oddanych sprawom rozwoju telekomunikacji oraz informatyki na potrzeby wojsk. Zatem odzwierciedleniem powyższego stała się kolejna, tym razem szósta edycja Konferencji Łączności pod hasłem: *„Ewolucja wojskowych systemów teleinformatycznych oraz lessons learned w świetle misji pokojowych i stabilizacyjnych"*. Gospodarzem kolejnej edycji konferencji jest Dowództwo 15 Sieradzkiej Brygady Wsparcia Dowodzenia, natomiast jej współorganizatorem tradycyjnie jest także Światowy Związek Polskich Żołnierzy Łączności, Stowarzyszenie Przyjaciół 15 SBWD oraz obecni od początku jej powstania przedstawiciele Akademii Obrony Narodowej reprezentowani przez Zakład Teleinformatyki i Bezpieczeństwa Cyberprzestrzeni (który jest spadkobiercą tradycji wszystkich wcześniejszych komórek organizacyjnych zajmujących się w swej działalności naukowo-dydaktycznej obszarem łączności i informatyki).

Powyższe stało się przyczynkiem, iż w dniach 22-23 kwietnia 2015 roku zorganizowano, pod patronatem Szefa Zarządu Kierowania i Dowodzenia P6 - SG WP kolejną - tym razem już VI Konferencję Łączności.

Tegorocznym celem konferencji pozostało przedstawienie przeobrażeń mających miejsce w obrębie wojskowych systemów łączności i informatyki, a szczególne zwrócono uwagę na kierunki zmian w wojskowych systemach teleinformatycznych w świetle doświadczeń z misji pokojowych i stabilizacyjnych. Zwrócono również uwagę na przewidywane kierunki przeobrażeń oraz oferty polskiego przemysłu zbrojeniowego w zakresie nowoczesnych rozwiązań technicznych mogących znaleźć zastosowanie w wojskach łączności, co znalazły swoje odzwierciedlenie w poszczególnych sesjach tematycznych.

VI Konferencję Łączności w Sieradzu rozpoczął Zastępca dowódcy 15 Sieradzkiej Brygady Wsparcia Dowodzenia płk Andrzej POCHOPIEŃ, który przywitał przybyłych gości oraz przedstawił cel konferencji. Następnie, w wystąpieniu otwierającym konferencję głos zabrał płk Piotr BLONKA, który w imieniu Szefa P-6 zaprezentował perspektywy rozwoju systemów dowodzenia i łączności w prezentacji na temat: *„Główne kierunki zmian w wojskowych systemach teleinformatycznych w świetle doświadczeń z misji pokojowych i stabilizacyjnych"*.

Tematyka poruszana w czasie konferencji była podzielona na sesje tematyczne nad którymi czuwał Szef S-6 15 SBWD – Pan mjr Radosław Urycki. Na szczególną uwagę czytelników zasługują niżej wymienione tematy znajdujące się w opracowaniu pokonferencyjnym:

a) główne kierunki zmian w wojskowych systemach teleinformatycznych w świetle doświadczeń z misji pokojowych i stabilizacyjnych;
b) walka informacyjna w nowych uwarunkowaniach przestrzennych;
c) wykorzystanie systemów teleinformatycznych SZ RP w reagowaniu kryzysowym;
d) informatyzacja sił zbrojnych RP – przespane szanse?

e) perspektywy i możliwości zapewnienia bezprzewodowej łączności szerokopasmowej w systemach szczebla taktycznego;
f) bezpieczeństwo wymiany danych w systemie sieciocentrycznym opartym o pozahoryzontowe linie radiowe;
g) wstępna koncepcja waveformu bazowego dla systemu narodowego;
oraz
h) komponent bezpieczeństwa systemów niejawnych wykorzystujących heterogeniczne sieci telekomunikacyjne opierające się o protokół SCIP. akronim: BSWD.

Wymiana poglądów oraz liczne dyskusje podczas konferencji pozwalały na dogłębne omówienie szczegółów tematów oraz zagadnień zaprezentowanych przez jej uczestników podczas wystąpień. Ważnym dodatkiem do prowadzonych konwersacji była możliwość zapoznania się z wybranymi rozwiązaniami technicznymi, które były prezentowane przez polski przemysł obronny.

Za istotne uznano ponownie nadmienić, że wszyscy uczestnicy zgodnie podkreślili walory organizacji konferencji oraz gościnny 15 Sieradzkiej Brygady Wsparcia Dowodzenia.

ppłk dr inż. Mariusz Frączek

dr inż. Łukasz APIECIONEK, *lapiecionek@teldat.com.pl*
inż. Wojciech MAKOWSKI, *wmakowski@teldat.com.pl*
mgr inż. Marcin WOŹNIAK, *mwozniak@teldat.com.pl*

AUTOMATYZACJA WYMIANY INFORMACJI NA POTRZEBY CLOSE AIR SUPPORT – ROZWIĄZANIE PRAKTYCZNE

Niniejsza publikacja przedstawia ***jedno z ważnych i gotowych do użycia rozwiązań*** *praktycznych* ***w zakresie automatyzacji*** *procesu* ***pozyskiwania i szerokiego dystrybuowania informacji na potrzeby Close Air Support*** *- bliskiego wsparcia powietrznego. Stanowi ono implementację systemu CID JAŚMIN, która wraz z modyfikacją systemu w samolotach MiG-29, umożliwia m.in. zwiększenie świadomości sytuacyjnej pilota na współczesnym polu walki.*

Prezentowany ***system w sposób efektywny wykorzystuje standardowe protokoły NATO,*** *dotyczące wymiany informacji pomiędzy jednostkami powietrznymi, lądowymi i/lub morskimi w celu zwiększenia ich świadomości o położeniu jednostek w rejonie działań.* ***Potrafi*** *on* ***w sposób automatyczny*** *pobierać dane z obszaru działania, dokonać ich analizy według zdefiniowanego algorytmu, a następnie przesłać je do wszystkich jednostek biorących udział w wykonywanej misji, w czasie zbliżonym do rzeczywistego.*

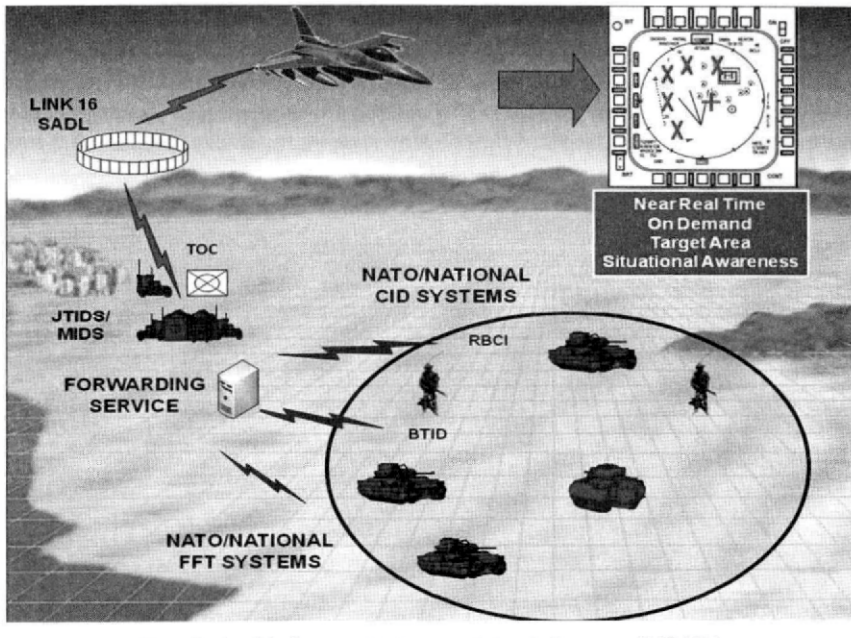
I. WSTĘP

CAS (*ang. Close Air Support*) to pojęcie określające bliskie wsparcie lotnicze, obejmujące działania jednostek lotniczych (*samolotów i śmigłowców*) przeciwko wrogim celom, które są blisko sojuszniczych wojsk lądowych i/lub morskich. Główną ideą CAS jest sprawne i precyzyjne pozyskiwanie oraz automatyczna wymiana szczegółowych informacji, m.in. o ruchu i ostrzale jednostek biorących udział w każdej misji powietrznej.

Czynnikiem decydującym o sukcesie misji z wykorzystaniem CAS jest głównie pełna integracja systemów wojskowych używanych podczas jej realizacji, zmierzająca do pozyskiwania bardziej precyzyjnych informacji (*niż dotychczas*) o położeniu jednostek w rejonie działań. Główne zadania dla CAS:

a) precyzyjne wsparcie dla wojsk własnych, w tym osłona ich działań, także na terenach zurbanizowanych;
b) skuteczna obrona kluczowych obiektów sojuszniczych (*np. baz lotniczych*), w tym patrolowanie przestrzeni powietrznej wokół nich;
c) efektywna ochrona przed siłami wroga poprzez atakowanie celów przeciwnika.

Architektura koncepcji wymiany informacji dla CAS według NATO została przedstawiona na rysunku 1.



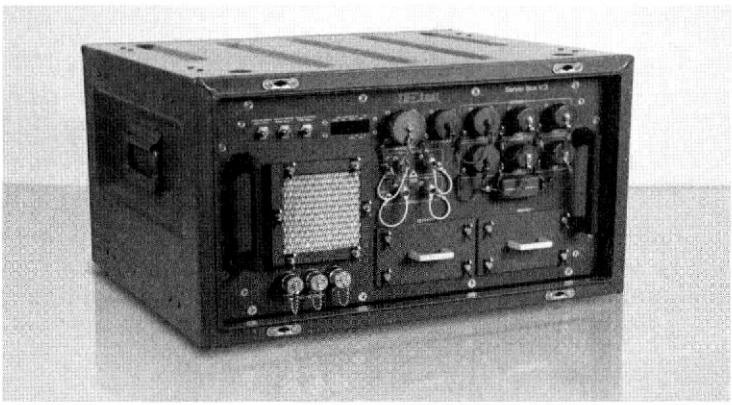
Rys. 1. Architektura CAS na podstawie koncepcji NATO

II. KONCEPCJA CID JAŚMIN

CID JAŚMIN jest serwerem identyfikacji bojowej. Produkt ten stanowi o wiele szerszą niż w oryginalnej koncepcji NATO implementację założeń tego typu serwera [1], [2]. Pełni on rolę **innowacyjnego integratora** istotnie podnoszącego głównie poziom: identyfikacji obiektów wojsk własnych i sojuszniczych, wymiany danych w tym zakresie między rodzajami sił zbrojnych oraz bezpieczeństwa wojsk i tym samym efektywności ich działań.

Rys. 2. Zastosowanie CID JAŚMIN w zakresie wsparcia procesów decyzyjnych dla systemów C3IS

Podstawowym komponentem sprzętowym rozwiązania CID JAŚMIN jest Server Box, wchodzący w skład Sieciocentrycznej Platformy Teleinformatycznej JAŚMIN. Pełni on rolę niezawodnego i wydajnego serwera, wykonanego w technologii militarnej (*o zwiększonej odporności mechaniczno-klimatycznej*), zapewniającego wysokie parametry i ponadnormatywne wymagania jakościowe, stawiane m.in. przez NATO dla tego typu urządzeń wojskowych.



Rys. 3. Server Box

III. AUTOMATYZACJA WYMIANY INFORMACJI POMIĘDZY SERWEREM CID JAŚMIN A SAMOLOTEM MiG-29

Automatyzacja wymiany informacji pomiędzy serwerem CID JAŚMIN a samolotem MiG-29 wymaga wykorzystania unikalnych i efektywnych możliwości zaimplementowanych w przedmiotowym serwerze. W tym celu wykorzystywane są specjalnie dobrane protokoły.

Do wymiany informacji o jednostkach własnych wykorzystywane są **protokoły NFFI i FFI**. Ich podstawowymi mechanizmami komunikacyjnymi są IP1 (*ang. Interoperability Profile 1*) oraz IP2 (*ang. Interoperability Profile 2*). IP1 bazuje na protokole TCP (*ang. Transmission Control Protocol*), natomiast IP2 wykorzystujący do transmisji danych protokół UDP (*ang. User Datagram Protocol*). Mechanizmy te polegają na wysyłaniu raportów dotyczących lokalizacji, a także – opcjonalnie – stanu operacyjnego przyjacielskich jednostek [3]. Rozwiązania te są bardzo korzystne z punktu widzenia zasilania informacjami serwera danych CID JAŚMIN, gdyż odbiorca wiadomości nie musi kontrolować, jakie dane zostają do niego transmitowane. Oddziałuje to wprost na szybkość działania systemu, ponieważ takie zastosowanie nie zawiera dodatkowego narzutu czasowego, potrzebnego na negocjacje pomiędzy nadawcą a odbiorcą informacji.

Protokół VMF (*ang. Variable Message Format*) pozwala na wymianę informacji w postaci sformalizowanych komunikatów. Informacje te mogą być wysyłane pomiędzy dowolnymi jednostkami na różnych szczeblach dowodzenia, od centrum dowodzenia do pojedynczego żołnierza. Wiadomości VMF, w przeciwieństwie do ADatP-3, są przesyłane w formie bitowej. Taka forma danych powoduje, że są one nieczytelne dla człowieka, jednak dzięki temu można znacznie zmniejszyć liczbę danych koniecznych do przesłania. Rozmiar wiadomości ma ogromne znaczenie w przypadku nisko przepustowych łącz radiowych typu KF.

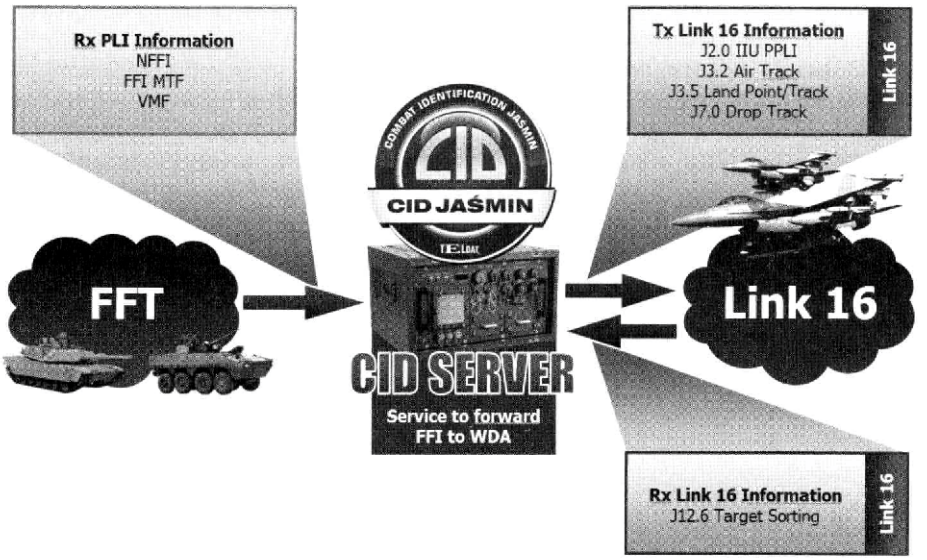
Niewątpliwie, **atutem** systemu **CID JAŚMIN** jest **możliwość wizualizacji sytuacji operacyjnej** za pomocą aplikacji Webowej, która zasilana jest danymi transmitowanymi poprzez protokół **NVG** (*ang. NATO Vector Graphics*). Takie rozwiązanie pozwala na użycie

gotowych komponentów dostępnych natywnie w systemie operacyjnym, co wyklucza konieczność instalowania dodatkowych aplikacji klienckich.

Protokołem stworzonym do celu transmisji raportów powietrznych drogą radiową jest **Link-16** [4]. Meldunki te mogą dotyczyć między innymi informacji na temat pozycji własnej oraz zauważonych obiektów (*np. sprzętu, instalacji, jednostek, itp.*). Do wykorzystania tej technologii niezbędna jest transformacja komunikatów przy pomocy dodatkowych protokołów: **JREAP-C** (*ang. Joint Range Extension Applications Protocol*) lub **SIMPLE** (*ang. The Standard Interface for Multiple Platform Link Evaluation*). Link-16 pozwala na przesyłanie raportów cykliczne, automatyczne lub na żądanie odbiorcy. To właśnie ostatni z trybów doskonale nadaje się do pobierania danych przez jednostki powietrzne z systemu CID JAŚMIN.

Mechanizm **SIP3** (*ang. Service Interoperability Profile 3*), który jest bardziej zaawansowany od IP1 i IP2, użyty w protokołach NFFI i FFI pozwala odbiorcy zdefiniować kryteria danych, które muszą spełniać informacje zanim zostaną do niego wysłane [5]. Zastosowanie tego filtra dopuszcza nie tylko określenie obszaru geograficznego ale nawet charakterystyki jednostek. Użycie tego mechanizmu umożliwia także pobranie określonej liczby ostatnich raportów dotyczących wybranych jednostek, co pozwala np. na wizualizację trasy ich przemieszczania się. Powyższe cechy SIP3 dowodzą, iż jest on, obok Link-16, wydajnym narzędziem, służącym do eksploracji bazy danych systemu CID JAŚMIN, co jest istotne zwłaszcza w sytuacji, gdy przetwarza on dużą liczbę informacji w tym samym czasie. SIP3 może także służyć do pobierania danych z systemu CID JAŚMIN nie tylko przez jednostki powietrzne, ale także lądowe, co czyni go alternatywnym rozwiązaniem dla protokołu Link-16.

Standard **NATO ADatP-37** [6], [7], zgodnie z którym CID JAŚMIN może zostać użyty, zawiera szczegółowe informacje na temat bliskiego wsparcia lotniczego. Dokument ten wyjaśnia zasady wymiany informacji pomiędzy jednostkami naziemnymi oraz dowództwem. Za pomocą protokołów NFFI, FFI lub VMF jednostki naziemnie raportują sobie wzajemnie oraz dowództwu wszystkie niezbędne informacje, wymagane do efektywnego wykonania misji. Wsparcie powietrzne może zostać udzielone, gdy inne jednostki prześlą prośbę do dowództwa o udzielenie takowego. Aby uniknąć przypadkowego uszkodzenia własnych jednostek konieczne jest przekazanie w sposób automatyczny bardzo precyzyjnych informacji o ich położeniu. W tym celu nadlatujący samolot automatycznie wysyła komunikat typu J12.6 za pomocą protokołu Link-16. Komunikat ten żąda od systemu CID informacji dotyczących położenia najbliższych mu jednostek. Odpowiedzią może być komunikat J3.5, który zawiera oczekiwane dane. Dzięki wiedzy na temat lokalizacji własnych obiektów, możliwy jest atak na wrogie jednostki przy jednoczesnym uniknięciu „ognia przyjacielskiego".



Rys. 4. Przykładowy przepływ informacji pomiędzy CID JAŚMIN i MiG-29

CID JAŚMIN to dotychczas jedyne polskie rozwiązanie, które w okresie 28.04 – 23.05.2014 r. **było z dużym powodzeniem eksploatowane w ćwiczeniu BOLD QUEST 2014** w USA **oraz odniosło znaczący sukces**. W tym zakresie:

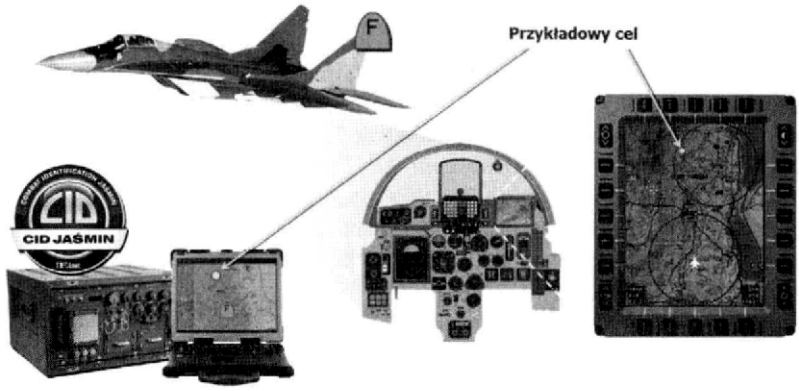
a) bez jakichkolwiek problemów uzyskał akredytację podłączenia do sieci niejawnej tego ćwiczenia;
b) pozytywnie zakończył testy z systemami wojsk NATO, m.in. USA, Danii i Włoch oraz pośredniczył w wymianie danych, np. z samolotami A10 (*symulator*), B1, F15, F16, F18D oraz F18E-Super Hornet, w zakresie m.in.: wizualizacji sytuacji operacyjnej i dostępności danych z serwera CID JAŚMIN w postaci tekstowej na terminalu pilota oraz śledzenia pozycji wymienionych samolotów;
c) przeszedł również pozytywnie testy obciążeniowe;
d) współpracował z systemem obrony przeciwlotniczej PATRIOT w przedmiocie wymiany informacji o sytuacji powietrznej.

CID JAŚMIN był i jest także z powodzeniem wykorzystywany (*w tym wiarygodnie badany i testowany*) w trakcie wielu ważnych przedsięwzięć wojskowych, m.in. w ramach kolejnych edycji ćwiczeń **NATO CWIX** 2012, 2013 i 2014.

Główne wymagania i założenia innowacyjnej współpracy CID JAŚMIN z MiG-29 [8]:

a) przygotowanie zmodernizowanych samolotów MiG-29 do pełnej implementacji prezentowanego rozwiązania;
b) montaż Konwertera Danych Telemetrycznych, zapewniającego wymianę informacji, w tym: odbiór, deszyfrację i selekcję nieautoryzowanych wiadomości w samolocie;
c) zapewnienie wysokiego poziomu bezpieczeństwa wymiany informacji poprzez zastosowanie m.in.: szyfrowanej transmisji, bram separujących [9], a także mechanizmów autoryzacyjnych;
d) wykorzystanie oprogramowania zapewniającego bieżący obraz na polu walki poprzez zastosowanie kluczowych protokołów, np.: NFFI, FFI, VMF oraz Link 16;
e) możliwość pozyskiwania bieżących informacji z: wewnętrznych systemów i sensorów dostępnych na pokładzie samolotu oraz systemów: klasy BFT, AWCIES, a także wsparcia dowodzenia wojsk własnych i sojuszniczych.

Interfejs samolotu po przetworzeniu otrzymanych danych, wysyła je do komputera misji znajdującego się na pokładzie, w celu ich zobrazowania na wyświetlaczu MFCD [8].



Rys. 5. Przykład współpracy CID JAŚMIN w zakresie automatycznej wymiany informacji dla MiG-29

IV. PODSUMOWANIE

Unikalne **zalety** CID JAŚMIN, jako **jedynego tego typu polskiego rozwiązania** to:

a) interoperacyjność z systemami NATO przy wykorzystaniu standardów zaimplementowanych w platformie JAŚMIN;
b) zaimplementowane kluczowe międzynarodowe protokoły komunikacyjne oraz możliwość transformacji komunikatów przesyłanych za ich pośrednictwem;
c) fakt, że wykorzystuje wydajne i niezawodne oprogramowanie, potwierdzone wiarygodnymi i wieloletnimi badaniami w trakcie wielu ważnych przedsięwzięć wojskowych;
d) sprawdzona i potwierdzona dużą ilością testów obciążeniowych zdolność współpracy m.in. z samolotami bojowymi, takimi jak: B1, F15, F16, F18D i F18E-Super Hornet;
e) łatwość jego wdrożenia – nie wymaga znacznych modyfikacji w strukturze naziemnej oraz na pokładzie samolotów;
f) możliwość szybkiego rozwoju, np. o moduł precyzyjnego naprowadzania samolotu na cel.

O jakości i innowacyjności **CID JAŚMIN** świadczy fakt, iż **zdobył** on **nagrodę pierwszego stopnia AirFair 2014, za pierwszy polski innowacyjny integrator istotnie zwiększający skuteczność** wymiany danych Sił Powietrznych, Marynarki Wojennej i Wojsk Lądowych oraz **bezpieczeństwo obiektów latających**.

LITERATURA:

[1] D.J. Bryant, D.G. Smith, *Impact of Uncertain Cues on Combat Identification Judgments*, Defence R&D Canada, Technical Report 2009.

[2] *Rethink Combat Identification Systems, Strengthened Management Efforts Needed to Ensure Required Capabilities*, United States General Accounting Office, June 2001.

[3] Apiecionek Ł., Romantowski M., Śliwa J., Jasiul B., Goniacz R., *Safe Exchange of Information for Civil-Military Operations*, MCC 2011: Military Communications and Information Systems Conference, Amsterdam, 17-18.10.2011, w: Military Communications and Information Technology: A Comprehensive Approach Enabler. Pod redakcją Marka Amanowicza. Warszawa: Redakcja Wydawnictw Wojskowej Akademii Technicznej, 2011, ISBN 978-83-62954-20-9, s. 39-50 (MK-312).

[4] *STANAG 5516, Edition 6, TACTICAL DATA EXCHANGE – LINK 16*, NSA
[5] *V. de Sortis, NFFI Service Interoperability Profile 3 (SIP3) Technical Specifications (VERSION 1.1.5)*, NC3A, 2011.
[6] *ADatP-37 (Draft) – NATO Standard For Services To Forward Friendly Force Information To Weapon Delivery Assets, Version 2.6*, NC3B, May 2013.
[7] *STANAG 5527 NATO Friendly Force Information Standard for Interoperability of Force Tracking Systems*, NSA.
[8] Biernat D., Łukasik M., Kosowski T., Woźniak M., *Możliwości adaptacji samolotów typu MiG-29 znajdujących się na wyposażeniu Sił Powietrznych RP do standardów NATO w obszarze zwiększania świadomości sytuacyjnej pilota*, Monografia Ogólnopolskiej Konferencji Naukowej pt. Modernizacja połączonych Rodzajów Sił Zbrojnych RP w nowych uwarunkowaniach geopolitycznych pod redakcją K. Czupryńskiego, P. Soroka, Wojskowa Akademia Techniczna, 2014, s. 213-223.
[9] Apiecionek Ł., Romantowski M., *Secure IP Network Model*, Computational Method in Science and Technology 19(4) 209-213 (2013), DOI:10.12921/cmst.2013.19.4.209-216.

***dr inż. Łukasz APIECIONEK**, lapiecionek@teldat.com.pl*
***inż. Wojciech MAKOWSKI**, wmakowski@teldat.com.pl*
***mgr inż. Marcin WOŹNIAK**, mwozniak@teldat.com.pl*

AUTOMATYZACJA PROCESU POZYSKIWANIA I DYSTRYBUOWANIA INFORMACJI SENSORYCZNEJ NA POLU WALKI

*Niniejsza **publikacja prezentuje jedno z ważnych i gotowych do użycia rozwiązań** praktycznych **w zakresie automatyzacji** procesu **pozyskiwania i rozległego dystrybuowania informacji sensorycznej na polu walki**. Stanowi ono **integrację Sieciocentrycznej Platformy Teleinformatycznej JAŚMIN** (unikalnego Systemu Systemów, w zakresie wspomagania dowodzenia i łączności) □ produktu firmy TELDAT i **Automatycznego Sygnalizatora Skażeń PROMETHEUS** □ wyrobu spółki Pimco. **Rozwiązanie to dostarcza w trybie automatycznym i ciągłym informacje o niezwykle groźnych zagrożeniach związanych z użyciem broni masowego rażenia** (CBRN), zgodnie z dyrektywami NATO. Realizacja tego była możliwa wyłącznie dzięki modułowej budowie (w tym systemom funkcjonalnym) wchodzącym w skład wymienionej platformy teleinformatycznej oraz implementacji modułu integrującego jej BMS z wskazanym także innowacyjnym i unikalnym sygnalizatorem skażeń. Powstałe w wyniku tej integracji rozwiązanie umożliwia przekazywanie sygnalizowanych zdarzeń na bieżąco w rozległym systemie, praktycznie do wszystkich szczebli dowodzenia, od najwyższego do żołnierza spieszonego włącznie.*

I. WSTĘP

Agencja Standaryzacyjna Organizacji Traktatu Północnoatlantyckiego wprowadza wiele ustaleń normalizujących między innymi: postępowanie komunikacyjne, oznaczenia na mapach, a także procedury techniczne dotyczące wyposażenia wojsk sojuszniczych.

Szczególnymi publikacjami w doktrynie wojskowej NATO są **standardy AEP-45(C)** (*ang. Allied Engineering Publication*) **oraz ATP-45(D)** (*ang. Allied Tactical Publication*). Normalizują one bowiem wszelkie zagadnienia dotyczące zagrożeń: biologicznych, chemicznych, radiologicznych i nuklearnych (*ang. Chemical, Biological, Radiological and Nuclear* □ *CBRN*). Potrzeba ich wprowadzenia i aktualizacji wynikała i wynika głównie z faktu, iż:

a) użycie broni CBRN może mieć katastrofalne skutki i obejmować bardzo duży obszar oraz stwarzać istotne zagrożenie dla ogromnej ilości ludzi;
b) broń CBRN oraz sposoby jej użycia i transportu są ciągle rozwijane i udoskonalane, podobnie jak skutki, jakie się wiążą z wykorzystaniem tych środków;
c) na poziomie indywidualnym konsekwencje użycia broni masowego rażenia są do siebie bardzo zbliżone. Podobnie zresztą jak środki ochrony;
d) w ostatnich latach zmienił się również charakter operacji wojskowych, do czego częściowo doprowadziła zmiana postrzegania przez społeczeństwo dopuszczalnego ryzyka oraz zwiększenie obawy o zagrożenia dla środowiska naturalnego.

W świetle powyższego **NATO dokonało** przywołanej na wstępie **standaryzacji niniejszych zagrożeń** w jednym pojęciu. **Ma ona na celu** [1]:

a) **wykrywanie** i informowanie sojuszników o zagrożeniach CBRN;
b) **raportowanie** wszystkich ataków chemicznych, biologicznych lub radiologicznych i nuklearnych oraz zanieczyszczeń powstałych w wyniku wybuchów;
c) **przewidywanie i ostrzeganie** o strefach zagrożonych bronią CBRN;
d) **współpracę** nad oceną CBRN, w celu uzupełnienia Połączonego Obrazu Sytuacji Operacyjnej - POSO (*ang. Common Operational Picture - COP*) dla dowództwa;
e) **ostrzeganie o sojuszniczych atakach** nuklearnych oraz przechwytywanie pocisków przeciwnika;

f) **nadawanie** zaawansowanych **ostrzeżeń o potencjalnym zagrożeniu** CBRN lub uwolnieniu toksycznych materiałów przemysłowych (*ang. Toxic Industrial Materials - TIM*).

Omawiane publikacje definiują także pięć podstawowych zasad obrony przed zagrożeniami ze strony czynników CBRN [2]:

1. **Oszacowanie wywiadu**: Wyczerpująca i dokładna ocena potencjalnego zagrożenia CBRN i TIM w obszarze wspólnych działań (*ang. Joint Operations Area - JOA*) zapewnia niezbędny fundament dla wszystkich innych środków obrony. Ocena ta musi być regularnie aktualizowana.
2. **Skuteczność przygotowania**: Wspólne siły (*ang. Joint Force*) muszą być dobrze przygotowane do obrony przed CBRN w zakresie odpowiedniej doktryny, sprzętu, procedur, organizacji i szkolenia. Te środki obrony muszą być przygotowane przed rozlokowaniem jednostek tak, aby konieczna zdolność operacyjna była obecna i możliwa na bieżąco. Takie przygotowania mają również na celu odstraszenie ewentualnych przeciwników od użycia broni CBRN lub TIM.
3. **Zarządzanie ryzykiem**: Całkowita odpowiedzialność za szeroki zakres potencjalnych zagrożeń CBRN jest nierealna. Ryzyko musi zostać przewidziane, zaplanowane, rozeznane i zarządzane tak, aby została utrzymana swoboda działania na obszarze JOA.
4. **Elastyczność, integracja i koordynacja**: Zagrożenie ze strony CBRN może być zróżnicowane, więc odpowiedź ze strony wspólnych sił powinna być kompleksowa, elastyczna i skoordynowana. Ponadto podstawowa obrona przed CBRN musi być spójna we wszystkich oddziałach wspólnych sił NATO.
5. **Wytrwałość**: Incydenty z użyciem CBRN mogą mieć dodatkowe wpływy na wytrwałość wspólnych sił NATO. Obrona przed CBRN wymaga dodatkowego zaplecza logistycznego natomiast ataki mogą obniżać funkcjonowanie łańcucha dostaw. Plan logistyczny wspólnych sił musi być odporny na zagrożenie ze strony CBRN, poprzez zastosowanie ochrony na liniach komunikacji.

Zdarzenia z użyciem broni CBRN i wynikające z nich zanieczyszczenia mogą wywierać znaczny wpływ na wiele operacji wojskowych, prowadzonych: na lądzie, w powietrzu oraz na morzu. Mają one również decydujący wpływ m.in. na decyzje dowódców różnych szczebli. Dlatego też **niezbędna jest możliwość wczesnego wykrycia takich zagrożeń, szybkiego pozyskania i dystrybuowania informacji na ich temat. Zapewnia to**:

a) zastosowanie zintegrowanego narzędzia, jakim jest **bezpośrednie połączenie** systemu zarządzania walką szczebla taktycznego – **BMS JAŚMIN i** sygnalizatora skażeń **PROMETHEUS**;
b) pełna **integracja i kompatybilność tego rozwiązania z innymi systemami funkcjonalnymi** platformy **JAŚMIN**.

II. PRZEDSTAWIENIE BMS JAŚMIN I SYGNALIZATORA PROMETHEUS ORAZ ICH USYTUOWANIE W PLATFORMIE JAŚMIN

BMS JAŚMIN jest systemem zarządzania walką szczebla taktycznego (*ang. Battlefield Management System – BMS*). Jest **jednym z głównych komponentów Sieciocentrycznej Platformy Teleinformatycznej JAŚMIN**, nazywanej także SPT JAŚMIN lub JAŚMIN, zaliczanej do systemów klasy C4ISR (*ang. Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance*). Jest ona Zintegrowanym Systemem Informacyjnym – **Systemem Systemów** posiadającym duży zbiór specjalistycznych komponentów, do których należą: systemy, podsystemy, urządzenia i oprogramowanie. Większość z nich może być używana autonomicznie. SPT JAŚMIN zapewnia nie tylko automatyzację procesów dowodzenia, ale także wsparcie

teleinformatyczne dla działań wojskowych, od szczebla operacyjnego do spieszonego żołnierza włącznie. Ponadto, charakteryzuje się: bardzo dużą kompleksowością, a jednocześnie uniwersalnością i spójnością □ technologiczną, sprzętową, programową i komponentową, wszechstronnością i wiarygodnością sprawdzenia, skalowalnością, gotowością do użycia, w wielu aspektach unikalnością, referencyjnością także w skali międzynarodowej. Rozwiązanie to m.in. zdobywa wysokie oceny w kraju i za granicą, również w państwach należących do NATO.

Opisywana platforma teleinformatyczna między innymi [3]:

- gwarantuje interoperacyjność z systemami sojuszniczymi poprzez zastosowanie sprawdzonych standardów obowiązujących w NATO;
- umożliwia uzyskanie przewagi informacyjnej i zwiększenie świadomości sytuacyjnej;
- pozwala na skuteczne i niezależne od usytuowania geograficznego monitorowanie położenia wojsk własnych i sprzymierzonych oraz zobrazowanie sytuacji operacyjnej na wszystkich szczeblach dowodzenia;
- zwiększa zdolności ekspedycyjne wojsk;
- zapewnia bezpieczną wymianę informacji z wykorzystaniem kryptografii IP (*ang. Internet Protocol*);
- eliminuje opóźnienia w pozyskiwaniu, obiegu i obrazowaniu informacji;
- usprawnia i automatyzuje procesy dowodzenia wojskami i sterowania systemami uzbrojenia, poprzez zastosowanie scentralizowanego portalu, umożliwiającego efektywną współpracę organów dowodzenia szczebla operacyjnego i taktycznego, w tym równoczesną ich pracę na wspólnych dokumentach;
- zapewnia sprawne rozwijanie oraz nowoczesne zabezpieczenie funkcjonowania stacjonarnych i mobilnych stanowisk oraz punktów dowodzenia z wykorzystaniem dostępnych urządzeń łączności przewodowej i bezprzewodowej;
- posiada zdolność do integracji systemów wsparcia teleinformatycznego, sensorów oraz efektorów stosowanych w siłach zbrojnych oraz tworzenia POSO;
- zwiększa bezpieczeństwo komponentów wojskowych i elementów wchodzących w ich skład, w tym żołnierzy oraz pojazdów;
- zapewnia kompleksowość, jednorodność i wzajemną spójność rozwiązań, modułową budowę oraz skalowalność systemu z zachowaniem najwyższych natowskich standardów technicznych i jakościowych.

Sieciocentryczna Platforma Teleinformatyczna JAŚMIN to system o architekturze zorientowanej usługowo, zgodnie z koncepcją SOA (*ang. Service-Oriented Architecture*), zawartą w założeniach NNEC (*ang. NATO Network Enable Capability*). Model ten zaleca tworzenie systemów informatycznych realizujących i wykorzystujących usługi zorientowane na funkcjonalności z punktu widzenia i na poziomie użytkownika. Zakłada też tworzenie zamkniętych interfejsami komponentów, spełniających biznesowe wymagania i umożliwiających wielokrotne wykorzystanie ich na wyższych poziomach funkcjonalnych. Zalecane przez tę koncepcję usługi udostępniają z założenia niezmienne punkty dostępowe i jednocześnie ukrywają wewnętrzne sposoby implementacji. Ponadto poszczególne komponenty porozumiewają się ze sobą dzięki wspólnemu medium komunikacyjnemu i mają do niego dostęp niezależny od sprzętu i oprogramowania, na którym działają [4].

Zgodnie z założeniami NNEC komponenty sprzętowe i programowe SPT JAŚMIN zostały zaprojektowane tak, aby mogły pracować na wszystkich poziomach działań. Były one m.in. z powodzeniem wykorzystane i przetestowane podczas wyjątkowo dużej ilości ważnych ćwiczeń krajowych i międzynarodowych, w których potwierdzono i sprawdzono szeroki zakres usług tej platformy teleinformatycznej [4]. Więcej informacji na jej temat–można znaleźć w [5], [6], [7], [8], [9], [10].

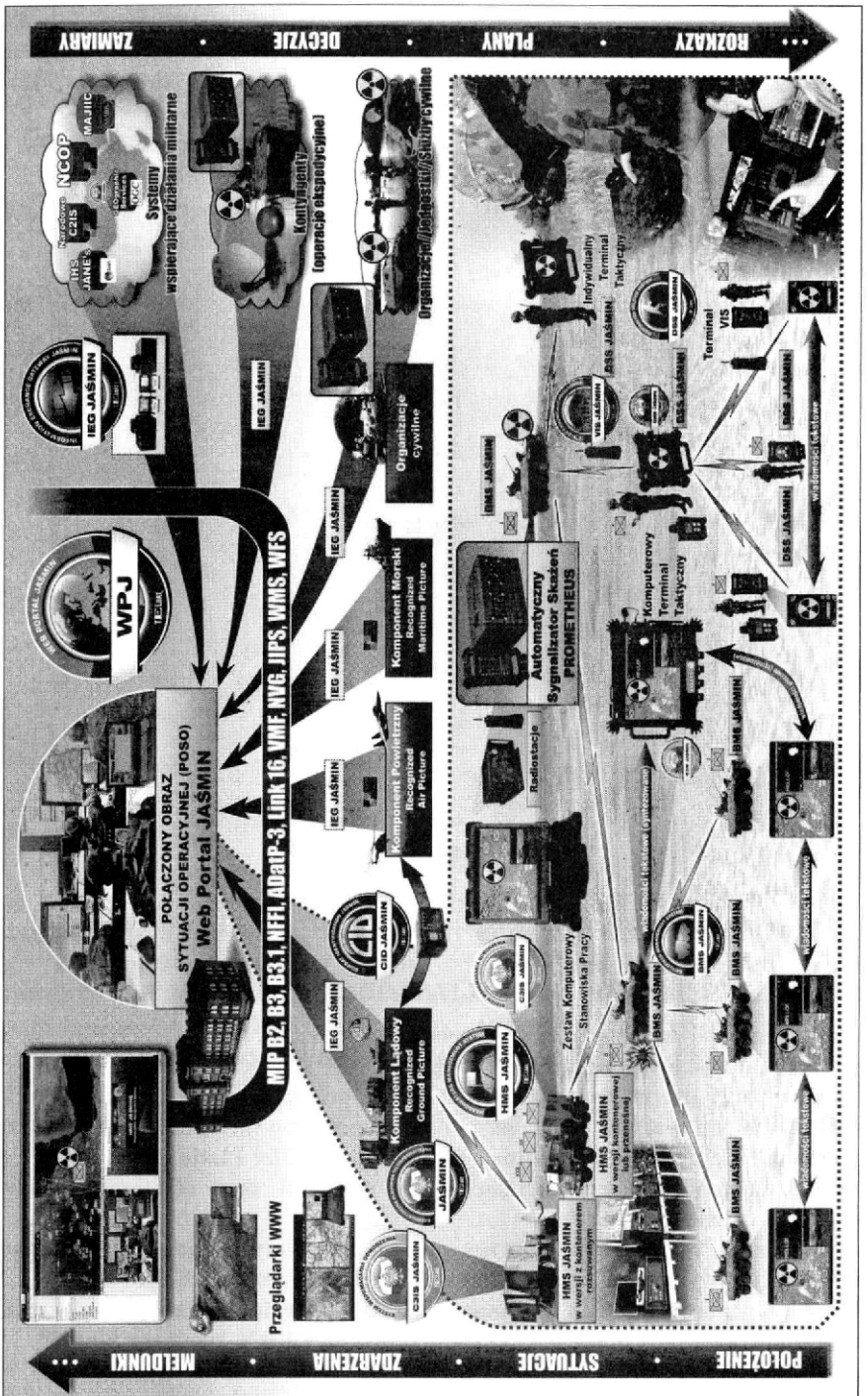
BMS JAŚMIN jest jednym z podstawowych elementów SPT JAŚMIN i **od lat jedynym narodowym, tak dojrzałym, sprawdzonym i rzeczywiście w pełni działającym systemem tej klasy**. Rozwiązanie to jest przystosowane do zastosowania w mobilnych systemach dowodzenia na poziomie taktycznym z uwzględnieniem radiowych środków łączności. Służy ono do budowy kompleksowych pokładowych systemów wsparcia dowodzenia i łączności, dedykowanych dla wszelkich pojazdów, jednostek pływających, a także obiektów latających w siłach zbrojnych. **Interfejs tego rozwiązania jest w pełni dostosowany do obsługi na wozach bojowych i/lub dowódczych**. Omawiany BMS, podobnie jak inne komponenty platformy JAŚMIN, może być również wykorzystany jako rozwiązanie autonomiczne.

Główne zalety i zastosowanie BMS JAŚMIN:

- współdziałanie z systemami rozpoznania i wykorzystanie m.in. informacji pozyskiwanych z wszystkich dostępnych sensorów pola walki
- tworzenie świadomości sytuacyjnej wojsk na poziomie taktycznym;
- obsługa komunikatów w standardzie ADatP-3;
- integracja i monitoring środków łączności wewnętrznej pojazdu;
- integracja i monitoring stanu wyposażenia wozu bojowego i/lub dowódczego.

System znacząco wpływa również na zwiększenie bezpieczeństwa wojsk, zwłaszcza poprzez:

a) dostarczenie bieżących informacji dowództwom, sztabom i wojskom bez opóźnień w ich przekazywaniu;
b) zautomatyzowane i ciągłe monitorowanie położenia, poprzez śledzenie wojsk własnych – BLUE FORCE TRACKING z zastosowaniem standardów NATO Friendly Force Information, komponentów i elementów bojowych na poziomie taktycznym, głównie żołnierzy i pojazdów;
c) zapewnienie bezpieczeństwa teleinformatycznego dla sieci, transmisji danych, głosu i obrazu;
d) wykorzystanie czujników monitorujących skażenie CBRN na polu bitwy.



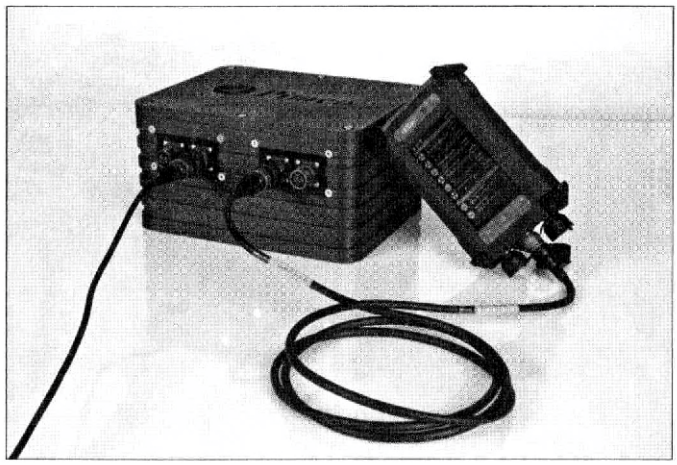
Rys.1. Przykład globalnego zastosowania integracji platformy JAŚMIN z Automatycznym Sygnalizatorem Skażeń PROMETHEUS

Automatyczny Sygnalizator Skażeń PROMETHEUS to innowacyjny i unikalny system wykorzystujący technologię IMS (*Spektroskopia Ruchliwości Jonów*). Umożliwia on:

- wykrycie oraz identyfikację substancji z grupy Bojowych Środków Trujących (*BST*) oraz Toksycznych Substancji Przemysłowych (*TIM*);
- monitoring stężenia substancji niebezpiecznych wewnątrz pojazdu (*m.in.: CO i NO*).

Urządzenie posiada również unikatowe rozwiązania techniczne zapewniające:

- wysoką czułość w zakresie krótkiego czasu wykrycia substancji TIM na poziomie pojedynczych sekund;
- bardzo niską podatność na zakłócenia oraz fałszywe alarmy;
- wysoką odporność na działanie czynników atmosferycznych, co umożliwia montaż czujników na zewnątrz pojazdu;
- wyświetlanie informacji na terminalu o: skażeniach chemicznych w postaci skali wielopoziomowej oraz podając przybliżoną wartość skażenia w jednostkach mg/m^3.



Rys. 2. Automatyczny Sygnalizator Skażeń PROMETHEUS z Terminalem VIS

III. INTEGRACJA SPT JAŚMIN I SYGNALIZATORA PROMETHEUS

Implementacja Automatycznego Sygnalizatora Skażeń **PROMETHEUS w BMS JAŚMIN i tym samym integracja tego rozwiązania z SPT JAŚMIN stanowi nową jakość w dziedzinie obrony przed bronią CBRN**, także w pokładowych systemach dowodzenia i łączności. Jest to innowacyjne, unikalne i w pełni zintegrowane rozwiązanie [11]. Nadto **potwierdza ona kolejny raz duże zdolności integracyjne całej Platformy JAŚMIN**, także w zakresie podłączania do niej szerokiej gamy sensorów oraz efektorów. Omawiane **rozwiązanie umożliwia głównie**:

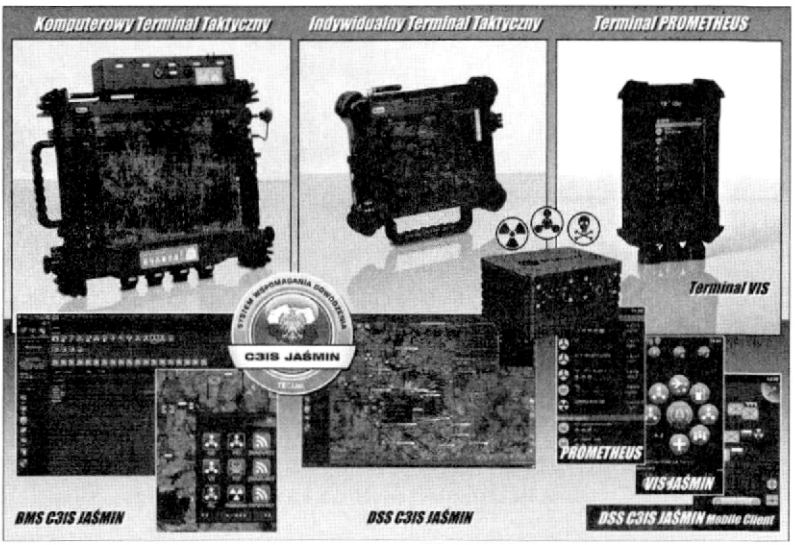
a) **wyświetlanie, rozgłaszanie i obrazowanie na dowolnych podkładach mapowych informacji o wykrytych i zidentyfikowanych zagrożeniach CBNR i TIM;**

b) **szybkie generowanie i automatyczne przesyłanie w rozległym systemie ustandaryzowanych przez NATO raportów typu CBRN**, zgodnie z STANAG 2103 (*ang. NATO Friendly Force Information Standard for Interoperability of Force Tracking Sysnems*);

c) **współpracę ze wszystkimi systemami funkcjonalnymi platformy JAŚMIN** (*głównie: HMS, BMS i DSS*) **oraz automatyczną wymianę danych o zaistniałych zagrożeniach na wszystkich szczeblach** dowodzenia i/lub zarządzania kryzysowego;

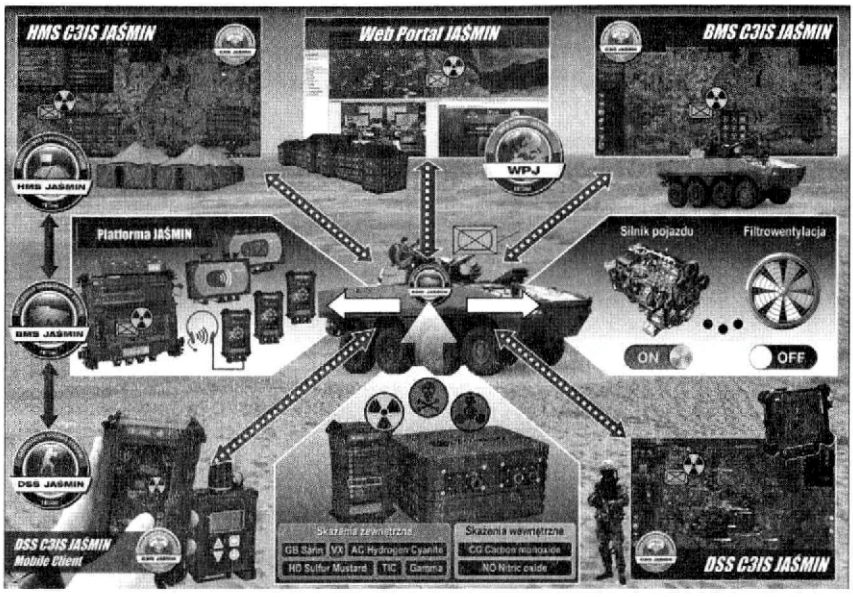
d) **zwiększenie poziomu bezpieczeństwa żołnierzy i obiektów wojskowych** poprzez natychmiastową i skuteczną dystrybucję informacji o zagrożeniach w Systemie Wspomagania Dowodzenia C3IS JAŚMIN (*kolejnym ważnym komponencie programowym JAŚMINA*);

e) **uruchamianie odpowiednich dla wykrytych zagrożeń efektorów** (*np. filtrowentylacji*) **i/lub pożądane zatrzymanie silników pojazdów bojowych itp.**

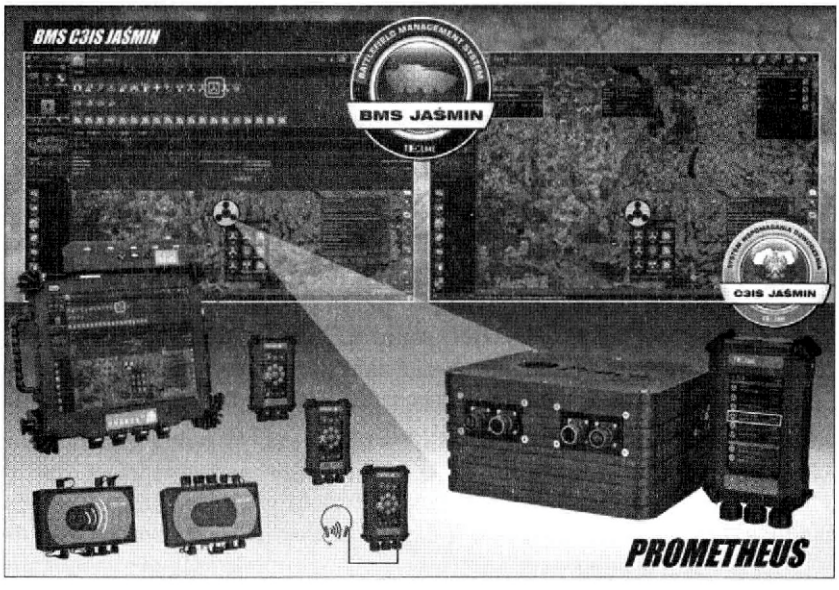


Rys. 3. Przykład sygnalizowania zagrożeń w różnych aplikacjach przedmiotowego rozwiązania

Połączenie opisywanych systemów pozwala na przesłanie w dowolnie wybrane miejsca i następnie zobrazowanie na mapach informacji o wystąpieniu skażenia, natychmiast po jego wykryciu. Nie byłoby by to możliwe bez wykorzystania szerokiej gamy innowacyjnych i w wielu przypadkach unikalnych rozwiązań zaimplementowanych w SPT JAŚMIN, które umożliwiają także uruchomienie m.in. wspomnianej już filtrowentylacji i/lub niezbędne zatrzymanie pracy innych efektorów. Dzieje się tak poprzez zastosowanie spójnych mechanizmów kontroli i sterowania urządzeń, zaimplementowanych np. w BMS JAŚMIN.



Rys. 4. Przykład także integracji oraz właściwego wykorzystania sensorów i efektorów



Rys. 5. Przykładowe zobrazowanie wykrytych skażeń w platformie JAŚMIN w pojeździe wojskowym i zarządzaniu kryzysowym

Rys. 6. Przykładowe zobrazowanie wykrytych skażeń w platformie JAŚMIN na wyższych szczeblach wojskowych i zarządzania kryzysowego

Rys. 7. Przykładowe zobrazowanie wykrytych skażeń w platformie JAŚMIN na poziomie indywidualnego żołnierza / ratownika

IV. PODSUMOWANIE I WNIOSKI

Integracja systemów JAŚMIN i PROMETHEUS (*także na poziomie pojazdów wojskowych*) **znacznie zwiększa m.in. poziom i skalę bezpieczeństwa żołnierzy oraz obiektów wojskowych**, także mobilnych. **Jest to rozwiązanie gotowe, unikalne, posiadające rozległy zasięg działania i** jednocześnie już **dostępne na rynku. Jego wartość,**

znaczenie i wspomniana szeroka skala m.in. szybkiego pozyskiwania i dystrybuowania informacji o tak istotnych zagrożeniach były możliwe do osiągnięcia dzięki modułowej budowie innowacyjnej platformy JAŚMIN – unikalnego tego typu Systemu Systemów, **w tym jego opisywanego BMS**.

W kontekście powyższego ważnym jest, że omawiana integracja obu opisywanych rozwiązań (*jedna z wielu możliwych do wykonania*) nie wymagała realizacji złożonej i długotrwałej pracy badawczo-rozwojowej, a jedynie implementacji modułu integrującego sygnalizację skażeń w BMS JAŚMIN. Zapewniło to jednocześnie pełną kompatybilność tego rozwiązania z innymi komponentami SPT JAŚMIN, np. HMS JAŚMIN i DSS JAŚMIN, co umożliwia przekazywanie informacji o skażeniach w sposób automatyczny na dużą skalę, m.in. na wszystkie szczeble dowodzenia/zarządzania.

Powyższe także ponownie potwierdza zasadność zastosowania modułowej budowy w SPT JAŚMIN (*w tym w zakresie systemów funkcjonalnych*) **i łatwość osiągania poprzez to wysokiej interoperacyjności tego systemu. Stanowi również potwierdzenie jego integracyjnych zdolności** wielu innych sensorów, także stacjonarno-mobilnych sygnalizatorów skażeń, możliwych do wykorzystania np. na poziomie/szczeblu obsługiwanym przez systemy HMS i DSS JAŚMIN. To także **kolejny raz udowadnia innowacyjność wymienionej platformy teleinformatycznej** m.in. w niniejszym zakresie.

LITERATURA:

[1] AEP-45(C) WARNING AND REPORTING AND HAZARD PREDICTION OF CHEMICAL, BIOLOGICAL, RADIOLOGICAL AND NUCLEAR INCIDENTS (REFERENCE MANUAL), December 2010.

[2] ATP-45(D) WARNING AND REPORTING AND HAZARD PREDICTION OF CHEMICAL, BIOLOGICAL, RADIOLOGICAL AND NUCLEAR INCIDENTS (OPERATORS MANUAL), May 2010.

[3] Strona producenta: http://www.teldat.com.pl, dostęp online 2015.03.24.

[4] H. Kruszyński, T.Z. Kosowski, Ł. Apiecionek, *CID Server JAŚMIN*, Ewolucja Wojskowych Systemów Teleinformatycznych oraz Lessons Learned w Świetle Misji Pokojowych i Stabilizacyjnych, V Konferencja Łączności, Sieradz 2014, str. 179-189.

[5] T.Z. Kosowski, Ł. Apiecionek, *JASMINE system: network centric koncept and practical solution*, Military Communications and Information Systems Conference MCC 2009, 29-30 September 2009, Prague, Czech Republic.

[6] W. Zawadzki, *JAŚMIN wkracza do armii*, Nowa Technika Wojskowa nr 5/2007.

[7] H. Kruszyński, *Sieciocentryczna Platforma Teleinformatyczna*, Bellona nr 2/2011.

[8] H. Kruszyński, Ł. Apiecionek, M. Dziamski, *JAŚMIN w warsztatach Combined Endeavor 2008*, RAPORT nr 06/2008.

[9] *Multilateral Interoperability Programme, The Joint C3 Information Exchange Data Model (JC3IEDM Main)*, MIP, 2007.

[10] K. Muchewicz, Ł. Sierakowski, *Sposoby wymiany danych operacyjnych w systemie JAŚMIN*, XVII Konferencja Naukowa Automatyzacji Dowodzenia w Gdyni, czerwiec 2009

[11] Strona producenta: http://www.pimco.pl, dostęp online 2015.03.24.