V KONFERENCJA ŁĄCZNOŚCI

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

PRACA ZBIOROWA

Sieradz 2014

V 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

23.04.2014 r.

SIERADZ 2014

Książka sfinansowana z dotacji Ministerstwa Obrony Narodowej

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

ISBN 978-83-930009-2-0

SPIS TREŚCI

WSTĘP

Postęp techniczny i rozwój nowoczesnych technologii nigdzie indziej nie jest tak dostrzegany, jak w obszarze szeroko postrzeganej łączności oraz informatyki. Współczesne możliwości przekazywania wiadomości, ich gromadzenia oraz przetwarzania stanowią odrębną sferę działalności człowieka, a powszechny dostęp do coraz nowszych źródeł różnorodnych danych stanowi fundament funkcjonowania społeczeństwa informacyjnego. Powyższe tendencje rozwoju stopniowo stają się również podstawą działalności sił zbrojnych, gdzie takie czynniki walki zbrojnej, jak ruch oraz rażenie są wynikiem dostarczenia dla wojsk wiernych, skrytych oraz terminowych informacji. Obecnie działania na poziomie taktycznym, operacyjnym i strategicznym są poprzedzone koniecznością zdobycia oraz przeanalizowania dużej liczby wiadomości o potencjalnym przeciwniku oraz zdolnościach własnych wojsk. Ma to przede wszystkim na celu ochronę wojsk własnych oraz efektywne użycie posiadanych sił i środków oraz zasobów. Jest także obszarem prowadzenia wielu analiz oraz badań naukowych, które z kolei uwzględniają potrzebę wymiany doświadczeń i wiedzy różnych specjalistów w aspekcie IT, jak również zapoznania się z najnowszymi kierunkami rozwoju myśli technicznej w zakresie teleinformatyki.

Od pięciu lat naturalnym centrum wymiany poglądów związanych z dalszym rozwojem Wojsk Łączności i Informatyki, staje się zapoczątkowana w 2009 przez Pana gen. bryg. rez. Mirosława Siedleckiego Konferencja Łączności na temat: *„Ewolucja wojskowych systemów teleinformatycznych oraz lessons learned w świetle misji pokojowych i stabilizacyjnych"*. Gospodarzem spotkań jest miasto Sieradz, drogie i bliskie sercu większości łącznościowców wraz z znajdującą się w nim 15 Sieradzką Brygadą Wsparcia Dowodzenia. Należy jednakże nadmienić, iż współorganizatorem konferencji jest także Światowy Związek Polskich Żołnierzy Łączności, Stowarzyszenie Przyjaciół 15 SBWD oraz obecnie Zakład Teleinformatyki i Bezpieczeństwa Cyberprzestrzeni Akademii Obrony Narodowej (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 dniu 23 kwietnia 2014 roku zorganizowano, pod patronatem Szefa Zarządu Planowania Systemów Dowodzenia i Łączności - P6 SG WP, kolejną Konferencję Łączności, a pięcioletni jubileusz dobitnie świadczy o dalszej potrzebie jej kontynuowania. Tegorocznym celem konferencji pozostało przedstawienie przeobrażeń mających miejsce w obrębie wojskowych systemów łączności i informatyki, a szczególne zwrócono uwagę na problemy zapewnienia bezpieczeństwa w cyberprzestrzeni. W dalszym ciągu ważnymi zagadnieniami poruszanymi były przewidywane kierunki przeobrażeń oraz oferty polskiego przemysłu zbrojeniowego w zakresie nowoczesnych rozwiązań technicznych mogące znaleźć zastosowanie w wojskach łączności, a powyższe zagadnienia znalazły swoje odbicie w poszczególnych sesjach tematycznych.

V Konferencję Łączności w Sieradzu rozpoczął dowódca 15 Sieradzkiej Brygady Wsparcia Dowodzenia płk Roman JANUSZEWSKI, który przywitał licznie przybyłych gości oraz przedstawił cel konferencji. Następnie, w wystąpieniu otwierającym konferencję głos zabrał płk Piotr BLONKA, który 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 dwie sesje tematyczne, natomiast na szczególną uwagę czytelników zasługują niżej wymienione zagadnienia:

- główne kierunki zmian w wojskowych systemach teleinformatycznych w świetle doświadczeń z misji pokojowych i stabilizacyjnych;
- wybrane aspekty inżynierii bezpieczeństwa systemów łączności;

- zarządzanie systemem łączności i informatyki w działaniach bojowych wojsk;
- wpływ nowoczesnych rozwiązań technicznych na bezpieczeństwo systemu łączności poziomu taktycznego;
- systemy C4IS jako wspomaganie procesu dowodzenia wojsk;
- zagrożenia w cyberprzestrzeni;
- zintegrowany system łączności DGT-MCS
- rozwój programowalnej radiostacji szerokopasmowej SDR R-450C w kontekście potrzeb współczesnych systemów obrony szczebla taktycznego;
.- wybrane aspekty transmisji danych w narodowych systemach C4ISR;
- model systemu łączności taktycznej w dobie zagrożeń cyberterrorystycznych;
- narodowy taktyczny system kryptograficzny;
- systemy troposferyczne w nowoczesnej komunikacji wojskowej.

Wymiana poglądów oraz liczne dyskusje podczas konferencji pozwalały na dogłębne omówienie szczegółów tematów oraz zagadnień poruszonych przez uczestników podczas ich wystąpień. Istotnym dodatkiem do prowadzonych konwersacji była możliwość zapoznania się z wybranymi rozwiązaniami technicznymi, które były zaprezentowane przez polskie firmy związane z przemysłem obronnym.

Za istotne uznano ponownie nadmienić, że wszyscy uczestnicy zgodnie podkreślili walory organizacji konferencji w gościnnym mieście Sieradzu.

ppłk dr inż. Mariusz Frączek

dr inż. HENRYK KRUSZYŃSKI, hkruszynski@teldat.com.pl
mgr inż. TOMASZ Z. KOSOWSKI, tzk@teldat.com.pl
dr inż. ŁUKASZ APIECIONEK, lapiecionek@teldat.com.pl
TELDAT

CID SERVER JAŚMIN

STRESZCZENIE

Standardy NFFI, FFI-XML-MTF, Link-16, VMF, także dane uzyskiwane z sensorów identyfikacji bojowej IFF, które mimo, że wydają się być przydatne zarówno na lądzie, jak i w powietrzu, nie dają możliwości wykorzystania informacji z wszystkich tych systemów jednocześnie. NFFI, Link-16, VMF znalazły swoje zastosowanie w NATO i używane są m.in. podczas działań koalicji w Afganistanie. Są bardzo przydatne, ale mogą być wykorzystywane tylko na niektórych obszarach i w niektórych scenariuszach. Aby to usprawnić, głównie podczas działań powietrzno-lądowych powstała NATOwska koncepcja serwera identyfikacji bojowej – (ang.) Combat Identification Server (CID Server), który gromadzi informacje z różnych źródeł CID na lądzie takich jak:

- *sensorów CID np. mogą nimi być systemy swój – obcy;*
- *systemów monitorowania położenia BFT (ang. Blue Force Tracking);*
- *systemów świadomości sytuacyjnej SA (ang. Situation Awareness).*

CID jest procesem uzyskania pewnego, precyzyjnego obrazu i charakterystyki jednostek oraz obiektów na obszarze działań, w celu zapewnienia realnego zastosowania możliwości taktycznych i użycia zasobów uzbrojenia. CID Server JAŚMIN jest implementacją koncepcji NATO w tym zakresie.

Slowa kluczowe – *(ang.)Combat Identification; (ang.), Friendly Force Information, (ang.)CID Server, System JAŚMIN, CID Server JAŚMIN.*

1. WSTĘP

Identyfikacja bojowa (ang. Combat Identification- CID [19][20][21]) jest to zdolność do efektywnej identyfikacji przynależności podmiotów w obszarze walki. Sprawność tego procesu jest kluczowym czynnikiem dla minimalizacji strat i poprawy skuteczności sił zbrojnych. Do tej pory powstało kilka rozwiązań stosowanych w tym celu w różnych sytuacjach taktycznych. Przykładami dwóch z nich są NFFI[7][8] i Link 16 [9][10]. Choć rozwiązania te mogą okazać się przydatne niezależnie na ziemi i w powietrzu, problemem jest niemożność korzystania z połączonej informacji z obu źródeł. Próba realizacji tego scenariusza spowodowała powstanie pomysłu (ang.) CID Server oraz wytworzenie przez NATO odpowiedniego dokumentu STANAG [3][4][24], dbającego o standaryzację rozwiązania. Pierwsze implementacje CID Server były stworzone przez USA (BAE Systems, [1]) oraz Niemcy (CIGAR z ESG, [2]).

Wśród definicji CID można wymienić, między innymi, poniższe opisy:

- Jest to proces pozyskania dokładnej charakterystyki podmiotów w obszarze działań i odpowiedzialności do takiego poziomu ufności, który dawałby pewność oraz możliwość bezpiecznego użycia uzbrojenia taktycznego w czasie rzeczywistym. Celem

jest maksymalizacja skuteczności walki przy jednoczesnej redukcji całkowitych strat (w wyniku wrogich działań i tzw. „ognia przyjacielskiego")[5].

- Jest to zdolność do rozróżnienia potencjalnych celów ruchomych oraz stacjonarnych na dużym obszarze oraz przy długich dystansach jako przyjacielskich, wrogich lub neutralnych, w wystarczająco krótkim czasie, z dużą pewnością oraz w wymaganym zakresie, aby wesprzeć decyzje o zaangażowaniu i alokacji broni [6].

Zdolność CID składa się z elementów:

- świadomości sytuacyjnej,
- identyfikacji celów,
- alternatyw sprzętowych.

Serwer CID poprawia proces identyfikacji przez zbieranie danych identyfikacji bojowej z różnych źródeł i dostarcza je na żądanie do odbiorców.

Z przytoczonych definicji wynika, że pojęcie CID jest bardzo ogólnym sformułowaniem, które dotyka różnych zagadnień operacyjnych i funkcjonalnych. Główną motywacją aby rozwinąć CID w działaniach połączonych jest zminimalizowanie przypadków przyjacielskiego ostrzału oraz pomoc w uniknięciu niepotrzebnych strat w walce. Jednakże CID wspomaga również inne elementy, z których między innymi wymienić można:

- efektywne wspieranie walczących sił,
- zarządzanie i kontrola obszarem walki,
- optymalne użycie sił i środków,
- wsparcie dla natychmiastowej, pozytywnej identyfikacji swój – oby oraz jednostek neutralnych na polu walki.

Koncepcja CID obejmuje zdolności zarówno operacyjne, jak i funkcjonalne. W zakresie zdolności operacyjnych jest aplikowana do następujących obszarów:

- powietrze - powietrze,
- powietrze - powierzchnia,
- powierzchnia - powierzchnia,
- powierzchnia – powietrze,

gdzie przez powierzchnię rozumie się zarówno ląd, jak i morze, czyli jednostki związane z danymi obszarami.

Aby dostarczyć zdolność CID, konieczna jest implementacja rozwiązania. Koncepcja CID może zostać zaimplementowana na bazie dwóch różnych typów rozwiązań – określanych jako materialne i niematerialne.

Wśród niematerialnych, nie będących przedmiotem zainteresowania tego artykułu, wymienić można:

- doktryny;
- taktykę, techniki oraz procedury (określane jako TTP);
- trening.

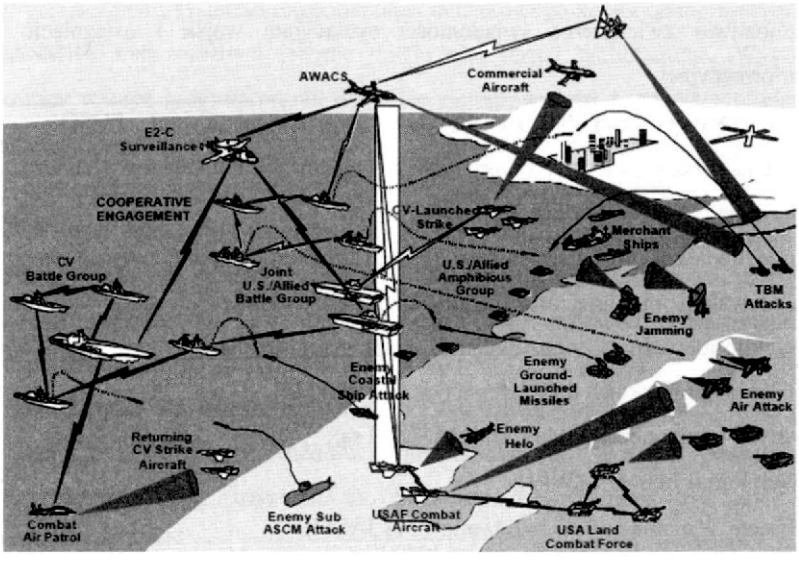
Rozwiązania niematerialne często muszą być uzupełnione przez materialne. Materialne rozwiązania mogą zostać scharakteryzowane jako:

- systemy czujników – kooperacyjne i niekooperacyjne (jak modulacja sygnału radarowego czy też elektroniczne środki wsparcia);
- systemy typu C3 (ang. command, control, and communications), w szczególności mogą to być cyfrowe połączenia danych przez radio, z których każde jest elementem składowym.

Do funkcjonalności CID zaliczamy:

- identyfikację jednostek wrogich (włączając typ platformy, klasę, narodowość, przynależność);
- identyfikację jednostek przyjacielskich;
- identyfikację jednostek neutralnych;
- interoperacyjność.

Na Rys.1 przedstawiono ogólny schemat wykorzystania CID wg. koncepcji NATO.



Rysunek 1 Wykorzystanie CID, źródło [5]

II. KONCEPCJA CID SERVER JAŚMIN

Główną ideą CID Server JAŚMIN było dostarczenie efektywnego rozwiązania, które zaspokoi wszystkie wymagania na CID Server, zarówno w środowisku narodowym, jak i międzynarodowym. Aby to uczynić możliwym, dokładnie zanalizowano problematykę CID. Przestudiowano również istniejące rozwiązania CID i ich możliwości. W trakcie implementacji użyto zaawansowanych technik programistycznych i wzorców, tak aby osiągnąć założony cel. CID JAŚMIN powstał w obrębie **Sieciocentrycznej Platformy Teleinformatycznej JAŚMIN,** która stanowi produkt firmy TELDAT (określana również jako **SPT JAŚMIN** lub **JAŚMIN**). Stanowi ona, wśród innych, **Zintegrowany System Informacyjny** wraz z dużym zbiorem specjalistycznych komponentów: systemów, podsystemów, urządzeń i oprogramowań, z których większość może być również wykorzystywana autonomicznie. Produkt ten zapewnia automatyzację procesów dowodzenia oraz wsparcie teleinformatyczne dla działania wojsk, do pojedynczego żołnierza włącznie. Cechują go także: bardzo duża kompleksowość, a jednocześnie uniwersalność i spójność – technologiczna, sprzętowa, programowa oraz komponentowa, wszechstronne i wiarygodne sprawdzenia, skalowalność, gotowość do użycia, w wielu aspektach unikalność, referencyjność także w skali międzynarodowej oraz wysokie oceny w kraju i za granicą, w tym w NATO.

Omawiana platforma teleinformatyczna (przedstawiona na Rys. 2):

- wspiera procesy dowodzenia i zarządzania działaniami wojsk na wszystkich szczeblach do pojedynczego żołnierza włącznie;
- umożliwia zwiększenie świadomości sytuacyjnej wojsk i osiągnięcie przewagi informacyjnej;
- umożliwia tworzenie Połączonego Obrazu Sytuacji Operacyjnej – POSO;
- zwiększa bezpieczeństwo komponentów wojskowych i elementów wchodzących w ich skład, w tym żołnierzy oraz pojazdów;
- umożliwia budowę w technologii IP (ang. Internet Protocol) nowoczesnej, wydajnej, skalowalnej, mobilnej oraz ekonomicznie efektywnej wielousługowej infrastruktury teleinformatycznej, umożliwiającej budowę niezależnych sieci na stanowiskach (centrach) i punktach dowodzenia (kierowania) [23].

Głównymi komponentami platformy JAŚMIN są:

- Web Portal JAŚMIN (WPJ);
- System Wspomagania Dowodzenia C3IS JAŚMIN;
- HMS JAŚMIN w wersjach: aparatowni, przenośnej i z wykorzystaniem MMSD;

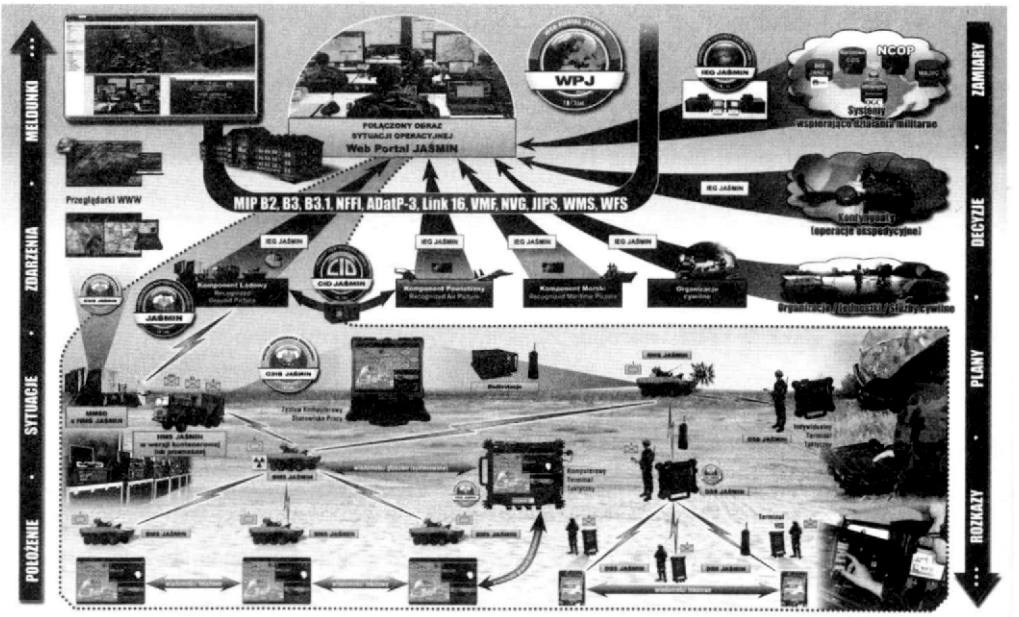
- BMS JAŚMIN;
- DSS JAŚMIN;
- CID JAŚMIN.

Sieciocentryczna Platforma Teleinformatyczna JAŚMIN jest systemem o architekturze zorientowanej usługowo, zgodnie z koncepcją SOA (ang. Service-Oriented Architecture), zawartą w założeniach NNEC. Zaleca ona tworzenie systemów informatycznych realizujących i wykorzystujących usługi zorientowane na funkcjonalności z punktu widzenia i na poziomie użytkownika. Zakłada także 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.

Zgodnie z NNEC, elementy koncepcji SPT JAŚMIN zostały zaprojektowane tak, aby być w stanie pracować na wszystkich szczeblach działań. System ten składa się ze sprzętu i oprogramowania. Urządzenia systemu JAŚMIN wraz z oprogramowaniem zostały przetestowane podczas ćwiczeń krajowych i międzynarodowych, w których przedstawiono szeroki zakres świadczonych usług. Więcej informacji na temat SPT JAŚMIN można znaleźć w [12][13][14][15][16][17].

W tak złożonym systemie implementacja dodatkowego komponentu, którym jest CID Server JAŚMIN, była możliwa jedynie dzięki elastycznej architekturze. Wykorzystując zaawansowane wzorce programowania udało się zintegrować go z istniejącymi elementami, nie naruszając spójności ani integralności SPT JAŚMIN. Wykorzystano fakt, że wszystkie elementy oprogramowania są oparte na architekturze SOA, która jest stworzona na bazie rozwiązania typu (ang.) MessageBus. W efekcie CID Server JAŚMIN pozwolił na rozszerzenie interoperacyjności istniejącego systemu. Dzięki serwerowi możliwe było połączenie komponentu lądowego z powietrznym przy tworzeniu Połączonego Obrazu Sytuacji Operacyjnej.

Poprzez takie podejście do koncepcji możliwe było również pozostawienie uniezależnienia od fizycznych mediów komunikacyjnych, które z punktu widzenia oprogramowania nie mają znaczenia. Do transmisji danych mogą być użyte zarówno radiolinie, połączenia kablowe, światłowodowe czy też radiowe – bezprzewodowe.



Rysunek 2 Umiejscowienie CID JAŚMIN w SPT JAŚMIN

III. Implementacja CID Server JAŚMIN

CID Server JAŚMIN opiera się na istniejących komponentach Systemu JAŚMIN, zarówno oprogramowaniu, jak i sprzęcie. W ramach sprzętowego komponentu CID JAŚMIN używa urządzenia Server Box V.3, który jest wydajnym i efektywnym serwerem militarnym. Dedykowane oprogramowanie CID JAŚMIN pracuje na systemie operacyjnym Microsoft Windows 2008 Server. Wszystkie elementy programowe zostały oparte na architekturze SOA i używają MessageBus do wymiany komunikatów z pozostałymi elementami Systemu JAŚMIN. (ang.) Position Location Information (PLI), będące najczęściej używanymi wiadomościami, są odbierane z użyciem protokołów NFFI IP1, IP2 (ang. NATO Friendly Force Information, Interoperability Profile 1 and 2 [8]) oraz Link 16. Wiadomości dostarczane z rozwiązania CID Server JAŚMIN są przekazywane protokołem Link 16 oraz NFFI SIP 3 (ang. Service Interoperability Profile 3 [7]) i VMF (ang. Variable Message Format). CID JAŚMIN wspiera również protokół FFI (ang. Friendly Force Identification). Możliwe jest jednak takie jego skonfigurowanie, aby każdy z wymienionych protokołów służył zarówno jako wejściowy, jak i wyjściowy. W każdej chwili możliwe jest również wykorzystanie natywnego, produkcji firmy TELDAT, protokołu BRM (ang. Battlefield Replication Mechanism [11]) do tego, aby zbierać informacje w warunkach, w których dostępne są jedynie

radiostacje o niskiej przepustowości. Z serwera CID JAŚMIN można także pobierać dane z użyciem protokołu NVG (ang. NATO Vector Graphics), który pozwala na stworzenie obrazu sytuacji operacyjnej z wykorzystaniem przeglądarki typu Web. Dzięki temu nie jest konieczne instalowanie dodatkowych aplikacji klienckich, wykorzystuje się istniejące w systemie operacyjnym komponenty aby mieć podgląd na aktualną sytuację na polu walki. W związku z tym CID Server JAŚMIN nie powinien być traktowany jedynie jako zbiór funkcjonalności - usług, ale jako rozwiązanie posiadające możliwość stworzenia tak zwanego (ang.) Common Operational Picture – Połączonego Obrazu Sytuacji Oepracyjnej na poziomie taktycznym. Architektura oraz implementacja CID Server JAŚMIN były rozwijane ze szczególnym uwzględnieniem jakości. Położono szczególny nacisk na:

- Wydajność – serwer ma możliwość przetwarzania dużych ilości danych w czasie rzeczywistym;
- Skalowalność – istnieje możliwość rozdystrybuowania CID Server JAŚMIN na kilku komputerach, co pozwala na zmniejszenie obciążenia. Możliwe jest to z użyciem MessageBus oraz architektury SOA;
- Niezawodność [18] – Server Box V.3 jest serwerem militarny, który spełnia wymagane dla sprzętu wojskowego parametry jakościowe i niezawodnościowe. Ponadto należy podkreślić, że cały proces rozwoju CID Server JAŚMIN ukierunkowany był na niezwodność.

CID Server JAŚMIN rozwijany jest z użyciem standardu STANAG 5528 [24]. Wszystkie zmiany do standardu są na bieżąco wdrażane, powodując utrzymanie pełnej kompatybilności zawsze z najnowszą jego wersją. Na poniższym rysunku (Rys.3) widać funkcjonalności CID Server JAŚMIN.

CID Server wymienia najwięcej wiadomości typu (ang.) Position Location Information (PLI), które są wymieniane z użyciem:

- NFFI IP1, IP2, SIP3 oraz FFI IP1, IP2, SIP3 – dane są wysyłane z użyciem protokołów UDP oraz TCP;
- NFFI oraz FFI SIP3 – protokół oparty na Web Services, który umożliwia pobieranie traków (wiadomości) z określonego, wskazanego w zapytaniu, obszaru;
- VMF – wdrożone, między innymi, wiadomości K11, K12, K51;
- Link 16 – wśród obługiwanych wiadomości można wymienić na przykład J3.5, J3.2. Wiadomości mogą być dostarczane na zewnątrz cyklicznie, automatycznie, lub na

żądanie, zgodnie z opisem protokołu. Wiadomości Link16 przesyłane są z użyciem protokołu JREAP C oraz SIMPLE;

- NVG – możliwe jest utworzenie połączonego obrazu sytuacji operacyjnej z uzyciem klienckiej przeglądarki Web.

Rysunek 3 Funkcjonalności CID Server JAŚMIN

Transformacja informacji pomiędzy NFFI, FFI, VMF i Link16 zachodzi na bazie tablicy transformacji ADatP-37.

CID Server JAŚMIN uczestniczył w wielu testach, między innymi sprawdzono go podczas ćwiczeń NATO CWIX 2012 oraz CWIX 2013. Przetestowano Link16, FFI, NFFI, VMF, transformację. Przeprowadzone testy zakończyły się pozytywnymi rezultatami. Testowano z nastepującymi systemami:

- **CWIX 2012**
  - 2012-DEU - CIGAR3;
  - 2012-FRA – COCCA;
  - 2012-FIN - JADEC2;
  - 2012-ITA - AF AC2IS BladeRunner;
  - 2012-DNK - C-Flex;
  - 2012-NATO - ACCS LOC1 ARS;
  - 2012-POL - PAFLINK16;
  - 2012-NATO - NC3A-IETV-NIRIS;

- 2012-NATO - TEDS JCTD/CWP;
- 2012-NATO - NLVC (FLAMES), włączając JTLS.

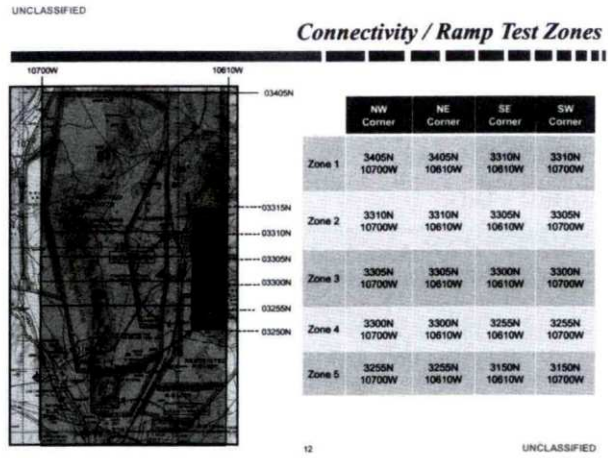
- **CWIX 2013**
  - 2013-DEU – CIGAR3;
  - 2013-DEU – DIG;
  - 2013-NATO - IFTS;
  - 2013-NATO - NC3A-IETV-NIRIS;
  - 2013-FRA – COCCA;
  - 2013-ITA - AF AC2IS BladeRunner;
  - 2013-ITA - GWLFD;
  - 2013-ITA - JMTDL;
  - 2013-SWE – ISIS NAVY C2;
  - 2013-USA – GCCS-J;

Testy obejmowały zarówno wymianę informacji, transformację, jak i wizualizację. Używano protokołu SIMPLE oraz JREAP C dla wiadomości Link16.

IV. TESTY BOLD QUEST 2014

Organizowane rokrocznie, od kilkunastu lat, amerykańskie ćwiczenie Bold Quest gromadzi zazwyczaj około 1000 jednostek koalicyjnych z kilkunastu krajów, między innymi: Australii, Belgii, Kanady, Niemiec, Danii, Finlandii, Francji, Wielkiej Brytanii, Holandii, Norwegii, Szwecji i Stanów Zjednoczonych. Od jakiegoś czasu Polska uczestniczyła w tym ćwiczeniu jako obserwator (a nie aktywny uczestnik). W 2013 roku, po raz pierwszy w historii tego ćwiczenia, strona polska została zaproszona ze swoim rozwiązaniem, opracowanym przez firmę TELDAT – CID Server JAŚMIN, do aktywnego udziału w przedsięwzięciu.
Podczas tegorocznej edycji ćwiczenia, produkt zostanie sprawdzony pod kątem możliwości generowania odpowiedzi na zapytanie otrzymane ze statku powietrznego. Po otrzymaniu zapytania o interesujący obszar, serwer musi odpowiedzieć danymi o jednostkach się w nim znajdujących. Na podstawie otrzymanych informacji statki powietrzne przeprowadzają stosowne działania. Scenariusz będzie się powtarzał w różnych wariantach w wybranych slotach czasowych wskazanych przez organizatorów (Rys.4).

Ćwiczenie odbywać się będzie od 21.04.2014 do 23.05.2014. Po ćwiczeniu dostępne będzie opracowanie podsumowujące podjęte aktywności.



Rysunek 4 Podział odpowiedzialności – ćwiczenia Bold Quest 14, źródło [22]

V. PODSUMOWANIE

W artykule przedstawiono koncepcję działania CID oraz sposoby jego wykorzystania. Zestawiono różne definicje, występujące w literaturze oraz omówiono możliwości, kryjące się za sformułowaniem. Zaprezentowano sposób podejścia do architektury oraz realizacji projektu na przykładzie implementacji CID Server JAŚMIN produkcji TELDAT. Implementacja ta jest o wiele bardziej elastyczna niż przewiduje dedykowany STANAG. Dzięki podejsciu opartemu o MessageBus oraz architekturze Service Oriented Architecture, możliwe było elastyczne rozszerzenie zakresu działania systemu JAŚMIN, nie tracąc nic z wcześniej zaimplementowanych funkcjonalności. Ponadto nadal utrzymano niezależność od środków łączności na poziomie oprogramowania, z punktu widzenia funkcjonalności usług nie ma znaczenia, który sposób komunikacji zostanie użyty. Rozwiązanie – CID Server JAŚMIN, dzięki odpowiedniemu połączeniu sprzętu (Server Box V.3) oraz zgodnemu z NNEC podejściu do tworzenia oprogramowania uzyskało cechy niezawodności, skalowalności i wydajości. Wszystkie zaimplementowane protokoły, w tym NFFI oraz FFI IP1, IP2, SIP3, VMF, Link 16, oraz NVG zostały przetestowane zarówno podczas ćwiczeń CWIX 2012, jak i CWIX 2013, potwierdzając pozytywnymi rezultatami testów zgodność ze standardami. To wszystko sprawiło, że CID Server JAŚMIN został wyróżniony zaproszeniem, jako jedyny i pierwszy w historii ćwiczenia Bold Quest polski produkt spełniający odpowiednie wymogi. Dzięki aktywnemu uczestnictwu w rozwoju standardu, CID Server JAŚMIN cały czas nadąża za aktualnie wyznaczanym sposobom implementacji.

BIBLOGRAFIA

[1] http://www.baesystems.com/capability/BAES_034933/combat-identification-iff
[2] http://www.esg.de
[3] *NATO Standard for Services to Forward Friendly Force Information to Weapon Delivery Assets*, Draft, January 2011, NATO Standardization Agency
[4] *NATO Standard for Services to Forward Friendly Force Information to Weapon Delivery Assets*, Draft, August 2011, NATO Standardization Agency
[5] *Join Warfighting Science and Technology Plan*, February 2000, Department of Defence, http://www.wslfweb.org/docs/dstp2000/jwstppdf/00-title.pdf
[6] *Join Warfighting Science and Technology Plan*, 1997, Department Of Defence, http://www.fas.org/spp/military/docops/defense/97_jwstp/jw4c.htm
[7] V. de Sortis, *NFFI Service Interoperability Profile 3 (SIP3) Technical Specifications (VERSION 1.1.5)*, NC3A, 2011
[8] *STANAG 5527 NATO Friendly Force Information Standard for Interoperability of Force Tracking Systems*, NSA
[9] *STANAG 5516, Edition 6, TACTICAL DATA EXCHANGE – LINK 16*, NSA
[10] *Interface Standard for the Joint Range Extension Application Protocol (JREAP)" MIL-STD 3011*, Departament of Defence
[11] K. Muchewicz, Ł. Sierakowski, *Means for operational data exchange in JASMINE System*, Military Communications and Information Systems Conference MCC 2009, 29-30 September 2009, Prague, Czech Republic
[12] T.Z. Kosowski, Ł. Apiecionek, *JASMINE system: network centric concept and practical solution*, Military Communications and Information Systems Conference MCC 2009, 29-30 September 2009, Prague, Czech Republic
[13] W. Zawadzki, *JASMIN wkracza do armii*, Nowa Technika Wojskowa nr 5/2007
[14] H. Kruszyński, *Sieciocentryczna Platforma Teleinformatyczna*, Bellona nr 2/2011
[15] H. Kruszynski, Ł. Apiecionek, M. Dziamski, *JAŚMIN w warsztatach Combined Endeavor 2008*, RAPORT nr 06/2008
[16] *Multilateral Interoperability Programme, The Joint C3 Information Exchange Data Model (JC3IEDM Main)*, MIP, 2007
[17] K.Muchewicz, Ł.Sierakowski, *Sposoby wymiany danych operacyjnych w systemie JAŚMIN*, XVII Konferencja Naukowa Automatyzacji Dowodzenia w Gdyni, czerwiec 2009
[18] K.Muchewicz, H.Kruszyński, M.Piotrowski, T.Z. Kosowski, M.Woźniak, *Reliable and effective management of hardware and software in battlefield environment*, Military Communications and Information Systems Conference MCC 2011, 17-18 October 2011, Amsterdam, Netherlands
[19] D.J. Bryant, D.G. Smith, *Impact of Uncertain Cues on Combat Identification Judgments* , Defence R&D Canada, Technical Report, 2009
[20] *Rethinking Combat Identification, Volume IV*, Issue 3, Joint Center For Lessons Learned. June 2002
[21] *Combat Identification Systems, Strengthened Management Efforts Needed to Ensure Required Capabilities*, United States General Accounting Office, June 2001
[22] *G2ASA Assessment Overview_Rev 1*, 27 Mar 2014 – materiały do ćwiczenia Bold Quest 2014
[23] Strona producenta: http://www.teldat.com.pl
[24] *ADatP-37 (Draft) - NATO Standard For Services To Forward Friendly Force Information To Weapon Delivery Assets, Version 2.6*, NC3B, May 2013