INSTYTUT ŁĄCZNOŚCI
PAŃSTWOWY INSTYTUT BADAWCZY

Zakład Radiokomunikacji Morskiej w Gdańsku (Z-8)

Opracowanie podstaw do wdrożenia cyfrowych systemów trankingowych dla potrzeb systemów bezpieczeństwa publicznego

Praca nr 08300038

Gdańsk, grudzień 2008

Opracowanie podstaw do wdrożenia cyfrowych systemów trankingowych dla potrzeb systemów bezpieczeństwa publicznego

Praca nr 08300038

Słowa kluczowe:

Kierownik pracy: dr inż. Rafał Niski

Wykonawcy pracy: mgr inż. Krzysztof Bronk
dr inż. Rafał Niski
mgr inż. Mirosław Radziwanowski
dr inż. Jacek Stefański
dr inż. Jerzy Żurek

Kierownik Zakładu: dr inż. Rafał Niski

Spis treści

1. Wprowadzenie 4

2. Planowanie sieci radiowej dla potrzeb bezpieczeństwa publicznego 5

2.1. Specyficzne potrzeby służb związanych z bezpieczeństwem publicznym 5

2.2. Dostępność 5

2.3. Obszar pokrycia 6

2.4. Niezawodność sieci 7

2.5. Bezpieczeństwo 7

2.6. Współdziałanie (Interoperacyjność) 9

2.7. Podsumowanie 10

3. Projekt radiowy systemu TETRA dla Trójmiasta 11

4. Podsumowanie 12

5. Bibliografia 14

1. Wprowadzenie

Celem niniejszej pracy była analiza i zaplanowanie infrastruktury zintegrowanego systemu łączności bezprzewodowej dla potrzeb bezpieczeństwa publicznego w oparciu o cyfrowy system trankingowy TETRA na przykładzie Trójmiasta. Zadaniem tego systemu będzie integracja różnych służb (policji, straży miejskiej, straży pożarnej, pogotowia, straży granicznej itp.) mająca na celu zapewnienie wysokiego poziomu bezpieczeństwa publicznego.
W pierwszej kolejności została przedstawiona metodologia projektowania sieci radiokomunikacyjnych dla potrzeb systemów bezpieczeństwa oraz sformułowano wytyczne, którymi powinni kierować się projektanci systemu. W dalszej kolejności zrealizowano projekt zintegrowanego systemu trankingowego TETRA dla potrzeb Aglomeracji Trójmiejskiej. Zrealizowany projekt oparty został o praktyczne dane pozyskane podczas analizy zurbanizowania Trójmiasta. Na tej podstawie zostały wytypowane potencjalne lokalizacje stacji bazowych, a następnie wykonano projekt części radiowej systemu z wykorzystaniem cyfrowych map terenu.
Opracowany projekt systemu TETRA stanowi cenny materiał w dyskusji nad sposobem realizacji zintegrowanego systemu łączności w niebezpieczeństwie na terenie Trójmiasta, jak również może stanowić podstawę do realizacji szczegółowego projektu radiowego takiego systemu w kontekście zbliżającego się EURO 2012.

2. Planowanie sieci radiowej dla potrzeb bezpieczeństwa publicznego

2.1. Specyficzne potrzeby służb związanych z bezpieczeństwem publicznym

Użytkownicy służb związanych z bezpieczeństwem publicznym, w przeważającej mierze korzystają z łączności fonicznej typu dyspozytorskiego. Podczas gdy jedna osoba mówi, grupa osób wysłuchuje wiadomości w tym samym czasie (typowy rozmiar takiej grupy wynosi 10-20 osób, choć czasami może być dużo większy). Systemy dedykowane poprawiają nie tylko skuteczność poszczególnych ratowników, ale również całego procesu ratowania. Uzyskuje się to dzięki temu, że możliwości szybkich połączeń grupowych typu „jeden do wielu" pozwala pracownikom uzyskać wiedzę o tym, co każdy z nich ma robić.

Jedną z podstawowych zalet radiowych systemów dla potrzeb bezpieczeństwa publicznego jest to, że użytkownicy mogą projektować systemy dostosowane do swoich rzeczywistych potrzeb. Użytkownicy związani z bezpieczeństwem publicznym mają szeroki zakres specjalnych wymagań, których wprowadzenie, w przypadku systemów komercyjnych, jest często nieuzasadnione ekonomicznie. Możliwości systemów obejmują takie właściwości, jak priorytet dla połączeń związanych z akcją ratowniczą, połączenia w trybie bezpośrednim (*Direct Mode*), dynamiczna rekonfiguracja systemu, sterowanie alarmami, wiadomości statusowe, śledzenie i monitorowanie stanu każdego terminala radiowego, monitorowanie i rejestrowanie ruchu. Systemy takie umożliwiają również wprowadzanie w razie potrzeby szerokiego zakresu usług mobilnej transmisji danych, począwszy od serwisów pozycjonowania satelitarnego po zarządzanie zasobami, dostęp do tajnych baz danych itp.

Terminale stosowane w sieciach specjalnych często również muszą spełniać specyficzne wymagania. Powinny być dostosowane do pracy w ekstremalnych warunkach klimatycznych oraz środowiskach o dużym poziomie zakłóceń. Muszą również charakteryzować się wysokim stopniem niezawodności i wytrzymałości mechanicznej oraz możliwością pracy w środowiskach zagrażających wybuchem.

Służby związane z bezpieczeństwem publicznym muszą mieć pełny dostęp do swoich środków komunikacji i możliwość sprawowania kontroli nad nimi. Centrum dowodzenia lub scentralizowane stanowisko dyspozytorskie musi kontrolować dostęp do systemu poszczególnych zespołów lub pojedynczych użytkowników oraz możliwości ich kontaktowania się z innymi zespołami (użytkownikami), zestawiać połączenia grupowe oraz określać priorytety poszczególnych użytkowników. Taka scentralizowana kontrola jest bardzo istotna w przypadku działań związanych z bezpieczeństwem publicznym.

Przedstawione wyżej wymagania funkcjonalne powodują, że większość organizacji i ministerstw odpowiedzialnych za bezpieczeństwo publiczne doszła do wniosku, że najlepszą drogą do zapewnienia niezawodnej komunikacji ruchomej jest wykorzystanie dedykowanej sieci radiowej, opartej na technologii PMR, np. według standardu TETRA.

2.2. Dostępność

W przeciwieństwie do sieci operatorów komercyjnych, przeznaczonych do powszechnego użytku, sieci specjalne tworzone są pod kątem specyficznych działań związanych z bezpieczeństwem publicznym. Muszą zapewniać „ciągłą dostępność" łącza alarmowego przez całą dobę.

W wielu sytuacjach kryzysowych usługi komercyjne zawodzą; w przypadku wystąpienia klęski żywiołowej telefony komórkowe zawodzą w wyniku przeciążenia sieci, która często zostaje kompletnie zablokowana. Użytkownicy należący do organizacji zajmujących się bezpieczeństwem publicznym nie mogą pozwolić sobie na pozostawanie bez łączności, szczególnie podczas sytuacji kryzysowych.

Współczynnik dostępności, w przypadku kluczowych składowych sieci specjalnych, powinien wynosić 99,999%. Sieci takie powinny kontynuować lokalną pracę swojej stacji bazowej, nawet w przypadku utraty przez nią połączenia z centrum komutacyjnym. Sieci komercyjne nie mają takich możliwości. Zasadniczo różne jest również podejście do problemu zasilania. W sieciach komercyjnych podtrzymanie zasilania w przypadkach awaryjnych (backup) nie występuje wcale lub realizowane jest w bardzo ograniczonym przedziale czasu (1-2 godzin). Dedykowane sieci specjalne mogą zapewniać podtrzymywanie zasilania za pomocą akumulatorów lub agregatów prądotwórczych przez okres nawet do kilku dni.

Bardzo ważną cechą sieci specjalnych jest realizacja połączeń priorytetowych oraz możliwość rozłączania w razie potrzeby innych użytkowników. Zarządzający łącznością związaną z bezpieczeństwem publicznym muszą mieć również narzędzia do dynamicznego przydzielania priorytetów poszczególnym użytkownikom w celu umożliwienia realizacji różnych scenariuszy akcji ratowniczych.
Ponieważ, w przypadku systemów komercyjnych, następuje szybkie przeciążenie i kanały telekomunikacyjne stają się niedostępne podczas sytuacji krytycznych, użytkownicy biorący udział w akcji ratowniczej polegają na systemach łączności specjalnej, zapewniających szybki dostęp niezbędny dla realizacji ich zadań. Przykładowo, w dzisiejszych systemach, użytkownicy uzyskują dostęp i zestawiają połączenia w czasie około 1/3 sekundy i wynik ten może być uzyskiwany dla dużej grupy użytkowników.

W komercyjnym systemie komórkowym, nawet podczas normalnego obciążenia, czas dostępu do kanału i zestawienia połączenia wynosi co najmniej dziesięć sekund. Podczas szczytu obciążenia, w szczególności podczas sytuacji kryzysowej, czas dostępu często rozciąga się do minut lub dostęp w ogóle nie jest możliwy ze względu na szybkie przeciążenie systemu.

Zarówno sieci specjalne, jak i komercyjne są projektowane dla poziomu obciążenia w godzinie największego ruchu i zakładają pewien margines na dodatkową pojemność. W systemach specjalnych należy jednak uwzględnić dodatkową pojemność na czas sytuacji kryzysowych, podczas których zapewnienie łączności jest sprawą szczególnie ważną.

Liczba członków zamkniętej grupy użytkowników może podczas sytuacji krytycznych znacząco wzrastać, np. do 100 użytkowników.

2.3. Obszar pokrycia

Model biznesowy przyjmowany dla komercyjnej infrastruktury bezprzewodowej różni się zasadniczo od modelu wymaganego dla organizacji związanych z bezpieczeństwem publicznym. Dochody komercyjnych operatorów pochodzą od indywidualnych użytkowników, co powoduję, że muszą oni rozbudowywać swoją infrastrukturę na obszarach gdzie występuje największe zapotrzebowanie na ich usługi. Systemy łączności dla potrzeb

bezpieczeństwa publicznego muszą być projektowane z myślą o potencjalnych zagrożeniach, które mogą wystąpić na dowolnym obszarze. Systemy specjalne muszą zapewniać pokrycie również pod ziemią oraz w niedostępnych miejscach budynków, czego nie można wymagać od systemów komercyjnych. Inne, specjalne wymagania dotyczą komunikacji pomiędzy wyposażeniem lotniczym i morskim a systemem naziemnym. Wymagania na systemy łączności specjalnej obejmują również pracę w trybie bezpośrednim (bez udziału stacji bazowych) a także stosowanie przewoźnych stacji wzmacniających sygnał radiowy (*repeterów*) dla zwiększenia zasięgu.

Utrzymanie lokalnego pokrycia sygnałem radiowym wokół stacji, nawet w przypadku awarii sieci transmisyjnej jest czasami możliwe, ale jedynie sieci specjalne mogą działać również w przypadku wyłączenia stacji bazowej.

2.4. Niezawodność sieci

Sieci specjalne wymagają bardzo wysokiego stopnia niezawodności opartego na:

- zachodzeniu na siebie pokrycia od różnych komórek na tym samym obszarze,
- nadmiarowości wyposażenia w ramach komórki (np. nadajniki-odbiorniki, sterowniki, anteny itp.),
- nadmiarowości zasilania, włączając w to akumulatory i agregaty prądotwórcze,
- przyjęciu strategii awaryjnej (*fallback*) w celu umożliwienia samodzielnego działania stacji, nawet w przypadku odcięcia jej od elementów komutacyjnych sieci,
- przyłączeniu nadmiarowych łączy transmisyjnych do stacji przy użyciu różnych topologii sieciowych typu gwiazdowego i pierścieniowego,
- przyjęciu takiej konfiguracji sieci, aby sąsiadujące ze sobą stacje podłączone były do różnych centrów komutacyjnych,
- w przypadku całkowitego odcięcia stacji od sieci, pozostają jeszcze terminale, które mogą komunikować się pomiędzy sobą bez udziału sieci. (W standardzie TETRA tryb ten określany jest skrótem DMO – *Direct Mode Operation*).

Sieci komercyjne nie są projektowane pod kątem spełnienia powyższych wymagań. Funkcje, które poprawiają niezawodność w sieciach wykorzystywanych dla potrzeb bezpieczeństwa publicznego, takie jak zachodzenie na siebie pokrycia mogą powodować zmniejszenie pojemności sieci, co nie leży w interesie operatora. W sieciach komercyjnych, które wymagają scentralizowanego sterowania połączeniami i tworzenia rekordów taryfikacyjnych umożliwiających wystawianie abonentom rachunków, nie ma możliwości pracy w trybie bezpośrednim.

2.5. Bezpieczeństwo

Na świecie wykorzystywanych jest szereg technologii radiokomunikacyjnych, zarówno znormalizowanych, jak i zastrzeżonych. Zalety każdej z nich uwydatniają się w różnych konkretnych zastosowaniach. Każda technologia wykorzystuje mechanizmy bezpieczeństwa łączności, których poziom dostosowany jest do potrzeb określonych grup użytkowników. Inne technologie zwykle nie dorównują jednak standardowi TETRA ze względu na zakres aplikacji i nie charakteryzują się równie wysokim poziomem bezpieczeństwa.

TETRA, z jednej strony, jest najbardziej bezpieczną znormalizowaną technologią na świecie, z drugiej zaś strony, jest wytwarzana przez wielu dostawców i łatwo dostępna w handlu. Oferuje więcej warstw zabezpieczeń i wyższy poziom bezpieczeństwa niż wszystkie inne technologie komunikacyjne przeznaczone do masowego wykorzystania komercyjnego.

Środki bezpieczeństwa

TETRA dostarcza określonych środków do potwierdzania autentyczności użytkowników i sieci oraz zabezpieczania poufności komunikacji o różnych poziomach. Wprowadza również zabezpieczenia przeciwko analizie ruchu i innym różnym formom ataków na użytkowników i sieci. Jednakże główną siłą tej technologii są możliwości zarządzania bezpieczeństwem umożliwiające sterowanie szyfrowaniem, wymianą kluczy szyfrowych itp.

Uwierzytelnianie

TETRA wykorzystuje zaawansowane procedury uwierzytelniania terminali podczas próby ich dostępu do systemu. Może stosować również uwierzytelnianie wzajemne umożliwiające równoczesną weryfikację sieci przez terminal. Wiele starszych publicznych systemów komórkowych nie ma nawet wbudowanego systemu uwierzytelniania, co uznano za słabość niektórych systemów CDMA. Nawet system GSM nie został wyposażony w uwierzytelnianie wzajemne. Brak uwierzytelniania wzajemnego może nie być poważnym problemem w publicznych systemach komórkowych, w których ataki polegające na podszywaniu się pod infrastrukturę przydarzają się bardzo rzadko, może jednak być poważnym uchybieniem w systemach związanych z bezpieczeństwem publicznym, w których podszywanie się pod stację bazową może całkowicie zdezorganizować łączność.

Szyfrowanie w interfejsie radiowym

TETRA wykorzystuje system zbiorczego szyfrowania, który zabezpiecza wszystkie przekazywane informacje (sygnalizacja, mowa i dane), zapewniając w ten sposób zarówno poufność informacji jak i zabezpieczenie przeciwko atakowi polegającemu na analizie ruchu.

Niektóre systemy komórkowe nie stosują szyfrowania w interfejsie radiowym. Jeżeli jest stosowane, często zabezpiecza jedynie zawartość informacyjną, pozostawiając sieć nieodporną na ataki polegające na analizie ruchu. Zabezpieczenie danych identyfikacyjnych i sygnalizacyjnych jest możliwe w nowszych sieciach UMTS, ale nie występuje w starszych sieciach GSM. Wydaje się, że większość sieci CDMA polega wyłącznie na zabezpieczeniu wynikającym z samej natury transmisji bez dodatkowych środków kryptograficznych. Brak silnego zabezpieczenia kryptograficznego przeciwko analizie ruchu powinien wzbudzać poważne obawy wśród użytkowników specjalnych.

Szyfrowanie informacji w interfejsie radiowym w systemie TETRA jest przeznaczone w szczególności dla pracy w zamkniętych grupach użytkowników. Istnieje możliwość stosowania różnych klas kluczy szyfrujących, od kluczy statycznych (SCK) poprzez często zmieniane klucze wspólne (CCK) do kluczy grupowych (GCK), które umożliwiają kryptograficzne rozdzielenie informacji przekazywanych w różnych grupach. Publiczne technologie komórkowe z reguły nie obsługują połączeń grupowych. Jedynym wyjątkiem jest wyspecjalizowane odgałęzienie technologii GSM, przeznaczone dla aplikacji związanych z transportem kolejowym – GSM-R, posiadające pewne ograniczone możliwości połączeń grupowych. Systemy GSM-R nie stosują jednak szyfrowania swoich połączeń grupowych.

Zarządzanie kluczami szyfrującymi

Mechanizm zarządzania kluczami szyfrującymi jest integralną częścią standardu TETRA. Wszystkie klucze szyfrujące mogą być zmieniane poprzez interfejs radiowy, za wyjątkiem tajnego klucza uwierzytelniania, przypisanego do określonego terminala. Klucze mogą być również przydzielane drogą radiową, co oznacza, że terminal może otrzymywać instrukcje, jaki konkretnie klucz ma być stosowany w określonej grupie użytkowników.

Zarządzanie terminalami

W standardzie TETRA przewidziane zostały różne możliwości zdalnego blokowania i odblokowywania terminali. Może zostać wydane polecenie zablokowania terminala, który traci w takim przypadku możliwości oddziaływania na sieć lub, w przypadku połączeń bezpośrednich, na innych użytkowników. Nie ma potrzeby stosowania takiej procedury w systemach komórkowych, które mogą po prostu nie zezwolić na dostęp terminala do sieci i akceptują niewielkie dodatkowe obciążenie spowodowane próbami dostępu. W łączności kryzysowej może to powodować jednak szereg problemów, jeżeli ukradziony terminal trybie bezpośrednim może być wykorzystywany do podsłuchu lub zakłócania pracy innych terminali.

2.6. Współdziałanie (Interoperacyjność)

Pojęcie „współdziałanie" może obejmować szereg zagadnień, najważniejszym jednak jest współdziałanie w zakresie bezpieczeństwa łączności, to jest dostarczenie prawidłowej wiadomości do właściwej osoby w odpowiednim czasie.
Istnieją trzy kategorie współdziałania:

- Współdziałanie organizacyjne – czyli zdolność organizacji do posiadania skoordynowanych planów operacyjnych i procedur, wspólnie przećwiczonych.
- Współdziałanie transgraniczne – czyli zdolność organizacji do współpracy ze swoimi sąsiadami. Jest to szczególnie istotne w przypadku Europy, w której dzięki porozumieniu z Schengen, zarówno ludzie jak i towary mogą przemieszczać się swobodnie pomiędzy stowarzyszonymi krajami.
- Współdziałanie techniczne – czyli możliwość kupowania przez organizacje współdziałających ze sobą urządzeń od różnych dostawców.

Współdziałanie transgraniczne jest możliwe wówczas, kiedy sieci działają w oparciu o ten sam standard technologiczny i pracują w tym samym paśmie częstotliwości. W ciągu ostatnich 5 lat, wszystkie rządy w Europie, które zdecydowały się budować nowe sieci dla łączności kryzysowej, wybrały standard TETRA. Ostatnie uczyniły to takie kraje jak Niemcy, Litwa, Portugalia i Norwegia. Stowarzyszenie TETRA (TETRA MoU) rozwija procesy certyfikacji współdziałania w celu zapewnienia użytkownikom i dostawcom sprzętu korzyści wynikających z w pełni otwartego rynku wielu wytwórców systemów i urządzeń.

Taki zdrowy, konkurencyjny, otwarty rynek wielu dostawców przynosi określone korzyści dla użytkowników, dzięki możliwości wyboru urządzeń, wyboru dostawców oraz ciągłemu rozwojowi nowych produktów o większej funkcjonalności i atrakcyjnych cenach. Producenci korzystają w wyniku rosnącego rynku, eliminacji różnic i braku kompatybilności ze standardem TETRA

Użytkownicy mogą być przekonani, że produkty, którym przyznano certyfikat współdziałania TETRA, były rygorystycznie testowane i że funkcje wyszczególnione w certyfikacie są w pełni zgodne ze standardem TETRA. Pozwala to użytkownikom wybierającym sprzęt z pośród kilku dostawców na zredukowanie kosztów integracji systemu i testowania.

2.7. Podsumowanie

Podczas planowania sieci dla potrzeb bezpieczeństwa publicznego należy uwzględnić jej specyficzne potrzeby, takie jak

- funkcjonalność (functionality),
- dostępność (availability),
- obszar pokrycia (coverage),
- niezawodność (resilience),
- bezpieczeństwo (security) i
- zdolność współdziałania (interoperability).

Zastosowanie technologii komunikacyjnej wykorzystywanej w sytuacjach kryzysowych wymaga zaprojektowania jej od początku do pracy w takich właśnie sytuacjach. W szczególności dotyczy to problematyki bezpieczeństwa, która musi być odpowiednio uwzględniona w projekcie. System TETRA został zaprojektowany pod kątem w pracy w szczególnie trudnych sytuacjach kryzysowych, dostarczając niezbędnych funkcji, takich jak połączenia grupowe i działanie w trybie bezpośrednim oraz specyficznych funkcji związanych z bezpieczeństwem łączności.

Nawet, jeżeli sieć komercyjna była projektowana pod kątem wypełnienia potrzeb użytkowników PSS - funkcjonalnych, operacyjnych, niezawodnościowych, QoS, itp., większość Administracji cały czas chciałaby zapewnić, żeby własność operatora była pod ich kontrolą. Dodatkowo, mogą oni wymagać gwarancji, że dany operator utrzyma się na rynku i prawa do kontrolowania, w razie potrzeby, kierownictwa firmy operatora. Konflikty interesów pomiędzy bezpieczeństwem publicznym i powszechnym wykorzystywaniem sieci nie powinny mieć miejsca. Większość istniejących, wyspecjalizowanych operatorów ma prawne ograniczenia tego typu. Wiele Administracji odczuwa dodatkowo potrzebę zachowania kontroli nad pasmem częstotliwości radiowych. Administracje będą również wymagały awaryjnego zasilania i utrzymania, co jest możliwe wyłącznie przy zastosowaniu dedykowanej technologii, dostarczanej przez wielu dostawców.

Systemy publiczne znakomicie sprawdzają się w ramach łączności powszechnej. TETRA jest ukierunkowanym rozwiązaniem o dużej pojemności i stanowi narzędzie dla łączności radiowej służb ratowniczych. Podczas katastrof lub innych sytuacji kryzysowych służby ratownicze wymagają od wykorzystywanego systemu najlepszych parametrów i maksymalnej niezawodności. Jest to dokładnie taka sytuacja, w której sieci komercyjne uwydatniają swoje ograniczenia.

3. Projekt radiowy systemu TETRA dla Trójmiasta

Ze względu na charakter pracy, ten rozdział nie może być udostępniony.

4. Podsumowanie

W ślad za spotkaniami odbywającymi się w Instytucie Łączności w Warszawie w ramach Forum TETRA Polska, w ramach niniejszej pracy, w dniu 24 czerwca 2008r. Zakład Z-8 zorganizował w Gdańsku jednodniową konferencję pt. „System TETRA dla Trójmiasta". Konferencja ta spotkała się z ogromnym zainteresowaniem zarówno ze strony urzędów i służb bezpieczeństwa publicznego jak i producentów sprzętu dla systemu TETRA. Konferencja odbyła się w nowym gmachu Wydziału Elektroniki, Telekomunikacji i Informatyki Politechniki Gdańskiej. Było to możliwe dzięki uprzejmości Dziekana Wydziału a zarazem Rektora Elekta i stanowi dowód dobrej współpracy pomiędzy WETI PG oraz Zakładem Z-8. W trakcie spotkania została zorganizowana prezentacja urządzeń i funkcjonalności systemu TETRA w oparciu o sprzęt rzeczywisty. Zostały zaprezentowane produkty firm: AKSEL Sp. z o.o., ICOM Polska Sp. z o.o. oraz Motorola Polska Sp. z o.o. Szczególne słowa uznania należą się firmie Motorola, która uruchomiła i zaprezentowała kompletną instalację wraz z kontrolerem, stacją bazową, serwerami etc., co umożliwiło zaprezentowanie użytkownikom bardzo wielu funkcjonalności systemu „na żywo". Wielu uczestników przyznało po spotkaniu, że dopiero teraz uświadomili sobie możliwości systemu TETRA.

Jak już wspomniano spotkanie cieszyło się dużym zainteresowaniem ze strony wielu instytucji, urzędów i służb bezpieczeństwa publicznego. Uczestniczyli w nim przedstawiciele m.in.:

- Urząd Miasta Gdańsk
- Urząd Miasta Gdańsk Biuro ds. EURO – Główny Specjalista do Spraw Bezpieczeństwa
- Urząd Miasta Gdańsk Wydział Zarządzania Kryzysowego i Ochrony Ludności
- Straż Miejska Gdańsk
- Komenda Miejska Państwowej Straży Pożarnej w Gdańsku
- Komenda Wojewódzka Policji Gdańsk
- Morska Służba Poszukiwania i Ratownictwa SAR
- Centrum Koordynacji Ratownictwa WOPR w Sopocie
- Jednostka terenowa WOPR woj. pomorskie
- Pomorska Grupa Operacyjna WOPR
- Morski Oddział Straży Granicznej
- Straż Miejska Sopot
- Urząd Miasta Sopot
- Urząd Morski w Gdyni
- DGT sp. z o.o.

Obradom towarzyszyła bardzo żywa i konstruktywna dyskusja. Zebrani wymienili wiele uwag merytorycznych oraz wyrazili uznanie dla organizatorów za zorganizowanie tak potrzebnego spotkania.

W konkluzji wszyscy zebrani podkreślali absolutną konieczność budowy systemu TETRA na potrzeby służb w Trójmieście w związku z organizacją EURO2012. Obecni przedstawiciele urzędów i instytucji zadeklarowali konieczność i wolę dalszej współpracy w tej materii.

Niniejsza praca stanowi przemyślany element w dalszych pracach nad możliwością budowy systemu TETRA w Trójmieście. W pracy dokonano rzetelnej analizy możliwości systemowych oraz odpowiedniego wyboru potencjalnych lokalizacji stacji bazowych dla przyszłego systemu łączności na potrzeby bezpieczeństwa publicznego. W oparciu o wybrane lokalizacje, wykorzystując posiadane oprogramowanie, dokonano obliczeń zasięgowych. W wyniku przeprowadzonych obliczeń dokonano selekcji lokalizacji oraz odpowiedniego

doboru parametrów stacji bazowych, tak aby zapewnić jak najkorzystniejsze pokrycie zasięgowe systemu minimalizując jego komplikację i tym samym przyszłe koszty budowy.
Uzyskane i zaprezentowane w pracy wyniki stanowią nominalny planning radiowy systemu TETRA w Trójmieście oraz bardzo dobry materiał do realizacji szczegółowego projektu technicznego systemu i określenia rzeczywistych kosztów budowy takiego systemu w Trójmieście. Zaprezentowana w pracy koncepcja budowy systemu jest rzeczywista i nadaje się do wdrożenia.
Zdobyte w trakcie realizacji pracy doświadczenie i rozwinięte narzędzia stanowią bardzo dobrą podstawę do zaprojektowania sieci systemu TETRA dla innych miast i obszarów Polski.

5. Bibliografia

[1] TETRA Association, *Wireless Public Safety Communications Network – planning consideration*, UK, 2008

[2] M. Kowalewski, B. Kowalczyk, *Ogólnokrajowy system radiokomunikacyjny zgodny ze standardem TETRA*, Telekomunikacja i Technik Informacyjne 3-4/2004, Instytut Łączności, Warszawa.

[3] M. Kowalewski, *Modele ogólnokrajowego systemu radiokomunikacyjnego zgodnego ze standardem TETRA*, KKRRiT 2003, Wrocław.

[4] K. Biernat, M. Grzybkowski, *Skutki użycia różnych metod propagacyjnych do wymiarowania ogólnopolskiej sieci radiokomunikacyjnej systemu TETRA*, KKRRiT 2003, Wrocław.

[5] Dunlop J., Grima D., Irvne J.: *Digital mobile Communications and the TETRA System;* John Wiley & Sons Ltd, 2000.

[6] *Bezpieczeństwo łączności w systemie radiokomunikacji ruchomej TETRA*, praca statutowa nr 08300054, Instytut Łączności 2004

[7] Niski R., Radziwanowski M., *Zagadnienia bezpieczeństwa informacyjnego w standardzie TETRA V+D,* Telekomunikacja i Techniki Informacyjne, Instytut Łączności, Warszawa 2005

[8] Niski R., Radziwanowski M., *Bezpieczeństwo informacyjne w systemie TETRA,* Zeszyty Naukowe Wydziału ETI Politechniki Gdańskiej, Seria: Technologie Informacyjne, Gdańsk 2005

[9] Niski R., Radziwanowski M., *Uwarunkowania ochrony informacji w systemie TETRA,* Akademia Marynarki Wojennej, Gdynia 2005

[10] Chater-Lea D.: *Design considerations for secure TETRA systems*, TETRA Forum Norge, 2002, www.tetramou.com.

[11] Dunlop J., Grima D., Irvne J.: *Digital mobile Communications and the TETRA System;* John Wiley & Sons Ltd, 2000.

[12] EN 300 392-2: *Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 2: Air Interface (AI)*, ETSI, 2003.

[13] ETS 300 396-1: *Terrestrial Trunked Radio (TETRA); Technical requirements for Direct Mode Operation (DMO); Part 1: General network design*, ETSI, 1998.

[14] Dokumentacja techniczna produktów firmy *Motorola*

[15] Dokumentacja techniczna produktów firmy *EADS*

[16] Dokumentacja techniczna produktów firmy *Nokia*

[17] Dokumentacja techniczna produktów firmy *Radmor*

[18] Dokumentacja techniczna produktów firmy *ICOM*

[19] Dokumentacja techniczna produktów firmy *Sepura*

[20] Katalog Kathrein *27 – 512 MHz Base Station Antennas for Mobile Communications,* 2008

[21] Materiały i prezentacje *Forum TETRA Polska*