

Henryk Gierszal[#], Joanna Modławska[#], Rafał Renk[#]

Wojciech Wojciechowicz^{*}

Anna Stachowicz

[#] Uniwersytet im. Adama Mickiewicza, ul. Umultowska 85, 61-614 Poznań

^{*} Instytut Informatyki, Politechnika Poznańska, ul. Piotrowo 2, 60-965 Poznań

ITTI, ul. Rubież 46, 61-612 Poznań

gierszal@amu.edu.pl

ZAPEWNIENIE INTEGRACJI ŁĄCZNOŚCI DLA SŁUŻB BEZPIECZEŃSTWA, PORZĄDKU PUBLICZNEGO I RATOWNICTWA Z WYKORZYSTANIEM BRAMY INTEROPERACYJNEJ

Streszczenie: Celem projektu HIT-GATE jest opracowanie bramy interoperacyjnej służącej zintegrowaniu komunikacji między służbami bezpieczeństwa, porządku publicznego i ratownictwa uczestniczących w akcji interwencyjnej angażującej wiele jednostek, które wykorzystują różne systemy łączności. W artykule uwypuklono zasadnicze wymagania na bramę interoperacyjną, która ma zapewnić komunikację rozmówną i transmisję danych na potrzeby obsługi krajowych i transgranicznych sytuacji kryzysowych.

1. WSTĘP

W artykule skupiono się na identyfikacji wymagań użytkowników na system telekomunikacyjny realizowany w projekcie HIT-GATE (*Heterogeneous Interoperable Transportable GATEway for First-Responders*), który jest finansowany w ramach 7. Programu ramowego prowadzonego pod auspicjami Komisji Europejskiej. Zasadniczym celem projektu HIT-GATE jest opracowanie bramy interoperacyjnej, która zapewni komunikację między europejskimi sieciami łączności użytkowników pierwszego kontaktu FR (*First Responder*) biorących udział w różnych incydentach czy zdarzeniach kryzysowych. Obecnie służby bezpieczeństwa, porządku publicznego i ratownictwa używają wiele różnych i niekompatybilnych rozwiązań łączności PSC (*Public Safety Communication*). Osłabia to skuteczność komunikacji lub ją istotnie utrudnia, a czasem nawet uniemożliwia sprawną koordynację wspólnych działań transgranicznych lub na potrzeby zarządzania kryzysowego, kiedy w incydencie uczestniczy na raz wiele służb, instytucji użyteczności publicznej [1][8][13] lub też jednostki tworzące system wczesnego ostrzegania.

Brama HIT-GATE będzie bazować na platformie systemu multimedialnego IMS (*IP Multimedia Subsystem*) obsługującej komunikację opartą na protokole transmisji RTP (*Real Time Protocol*) i sygnalizacji SIP (*Session Initiation Protocol*)/SDP (*Session Description Protocol*). Takie podejście zapewni efektywność, elastyczność i łatwość rozwoju. Platforma IMS będzie pełnić rolę węzła komutacyjnego odpowiedzialnego także za tworzenie, zestawianie i transkodowanie usług. Będzie także dostarczać operatorowi narzędzia do zarządzania jej funkcjonowaniem. Dzięki zastosowaniu bezpłatnego oprogramowania *open-source* istnieje możliwość ograniczenia kosztów budowy bramy.

Ponieważ rozwiązania powstałe w projekcie HIT-GATE będą wykorzystywane przez użytkowników pierwszego kontaktu, winny być one zgodne z wymogami zdefiniowanymi przez nich oraz powinny uzyskać ich akceptację. Jednocześnie należy brać pod uwagę rozwój, jak i ograniczenia technologiczne związane z poszczególnymi systemami łączności przewodowej lub bezprzewodowej dołączanymi do bramy HIT-GATE.

W celu zdefiniowania wymagań użytkowników na bramę HIT-GATE dokonano identyfikacji i analizy podstawowych wymagań stawianych przed systemami komunikacyjnymi dla służb bezpieczeństwa, porządku publicznego i ratownictwa. Następnie wymagania te zostały zaprezentowane i skonsultowane z użytkownikami oraz ekspertami dziedzinowymi, którzy uczestniczyli w spotkaniach typu „burza mózgów” lub wypełniali formularz kwestionariusza z otwartymi i zamkniętymi pytaniami dotyczącymi ich oczekiwań dotyczących funkcjonowania bramy interoperacyjnej.

Do opracowania listy wymagań posłużono się metodyką VOLERE [2][3], która jednak została wzbogacona o dyskusje wewnętrzne w gronie parterów oraz informacje od użytkowników. Ostateczne wymagania określono na bazie: wiedzy i doświadczenia członków konsorcjum, opinii użytkowników i ekspertów dziedzinowych, dostępnej wiedzy o systemach PSC oraz analizie zastanych danych literaturowych.

Układ publikacji jest zatem następujący. W rozdz. 2 przedstawiono projekt HIT-GATE. W rozdz. 3 zaprezentowano podstawowe cele projektu HIT-GATE, które mają znaczący wpływ na specyfikację wymagań. Z kolei metodykę wykorzystaną do zebrania wymagań opisano w rozdz. 4. Listę głównych wymagań dla systemu HIT-GATE zdefiniowano w rozdz. 6. Wnioski z tych badań i analiz stanowią treść rozdz. 7.

2. PROJEKT HIT-GATE

Projekt HIT-GATE (nr 284940) jest dwuletnim projektem badawczym realizowanym w ramach 7. Programu ramowego w tematyce bezpieczeństwa (*Security*). Konsorcjum liczy 11 członków z 8 krajów (www.hit-gate.eu). Wśród nich są duże firmy, organizacje badawcze, małe i średnie przedsiębiorstwa, a także użytkownicy służb publicznych. Potencjał i komplementarność konsorcjum pozwala opracować nowe rozwiązanie systemowe, które będzie adekwatne do dzisiejszych potrzeb i które wypełni niszę pośród dostępnych technik pozwalających na integrację różnych systemów łączności. Głównym celem projektu jest opracowanie i wdrożenie zbioru rozwiązań zapewniających interoperacyjność komunikacyjną sieci użytkowników pierwszego kontaktu. Dzięki nim zostanie zagwarantowana możliwość scalenia istniejących systemów łączności bez modyfikowania terminali ruchomych ani infrastruktury sieciowej. Organizacje bezpieczeństwa, porządku publicznego i ratownictwa na poziomie europejskim, krajowym, regionalnym, jak i lokalnym eksploatują różnorodne systemy i urządzenia oparte na różnych technikach. Zaprojektowana brama HIT-GATE ma obsłużyć te różne i niekompatybilne rozwiązania łączności począwszy od systemów PMR (*Pro-*

fessional Mobile Radio), poprzez standardy TETRA (*Terrestrial Trunked Radio*), TETRAPOL czy WiMAX (*Worldwide Interoperability for Microwave Access*), a skończywszy na systemach następnej generacji (np. LTE (*Long Term Evolution*) czy LTE-Advanced). Ponadto ze względu na to, że działania w zakresie bezpieczeństwa publicznego czy ratownictwa angażują często wielu użytkowników pierwszego kontaktu pochodzących z różnych krajów (np. podczas klęsk żywiołowych) [10][11][12], brama HIT-GATE musi skutecznie funkcjonować także w takich sytuacjach i pozwalać wówczas na koordynację działań o charakterze międzynarodowym. Zasadnicze cechy bramy HIT-GATE integrującej heterogeniczne systemy PSC obejmują:

- zapewnienie wymagań stawianych przez aplikacje wykorzystywane przez służby bezpieczeństwa, porządku publicznego i ratownictwa z punktu widzenia prowadzenia działań o kluczowym znaczeniu dla misji (*mission critical*),
- szybkie uruchomienie w nieprzewidywalnym środowisku komunikacji ruchomej o dużej dynamice zmian ruchu i w którym infrastruktura sieciowa może ulec degradacji lub zniszczeniu [4].

Działania w projekcie podzielono na 7 pakietów zadań. Dotyczą one: (1) zarządzania projektem, (2) identyfikacji potrzeb użytkowników, (3) zdefiniowania wymagań na system, (4) opracowania komponentów bramy HIT-GATE, (5) ich integracji i ocenie funkcjonowania, a także (6) demonstracji końcowego rozwiązania oraz (7) zaproponowania ścieżki standaryzacyjnej dla tego typu systemów.

3. ZASADNICZE CELE PROJEKTU

W projekcie HIT-GATE zdefiniowano poniższe cele zasadnicze, które można potraktować jako wymagania bazowe [4]. Brama HIT-GATE:

- O1 zapewni komunikację między heterogenicznymi sieciami służb pierwszego kontaktu na poziomie europejskim,
- O2 zaoferuje zestaw usług wymaganych przez służby pierwszego kontaktu korzystające z heterogenicznych rozwiązań,
- O3 zapewni usługi łącząc różne sieci w sposób „przezroczysty” (*seamless*),
- O4 będzie bezpieczna i będzie spełniać wstępnie zdefiniowane polityki bezpieczeństwa,
- O5 będzie przewoźna, zdolna do szybkiego uruchomienia i autonomiczna,
- O6 będzie spełniać wymagania dla prowadzenia działań o kluczowym znaczeniu dla misji,
- O7 będzie integrować się automatycznie z sieciami znanego typu,
- O8 wymaga minimalnych lub żadnych zmian w istniejących infrastrukturach służb bezpieczeństwa, porządku publicznego oraz ratownictwa,
- O9 będzie miała modułową architekturę pozwalającą dołączać przyszłe typy sieci,
- O10 będzie miała otwarty interfejs oraz pozwoli zaproponować przez konsorcjum standardy,
- O11 uwzględni zalecenia dla interoperacyjności biorąc pod uwagę aspekty eksploatacyjne, organizacyjne oraz prawne.

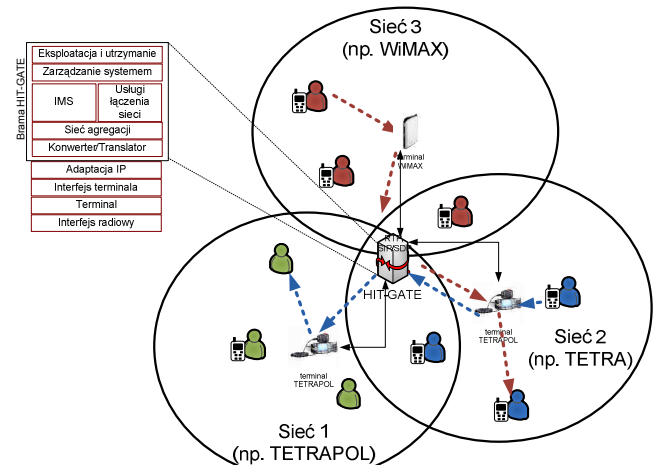
Brama HIT-GATE musi zapewnić wymianę komunikatów (informacji) między sieciami służb pierwszego kon-

taktu uczestniczących w akcji. Zatem skojarzonymi z tą potrzebą będzie [2]:

- zdolność do łączenia sieci w celu zapewnienia komunikacji,
- pewność komunikacji,
- zdolność do uruchomienia komunikacji między służbami,
- transparentność komunikacji, tzn. użytkownik nie powinien mieć świadomości, że istnieje jakieś dodatkowe urządzenie komutacyjne; użytkownicy winni komunikować się między sobą w myśl zasady: „wyślij komunikat i zapomnij jak zostanie on przesłany”.

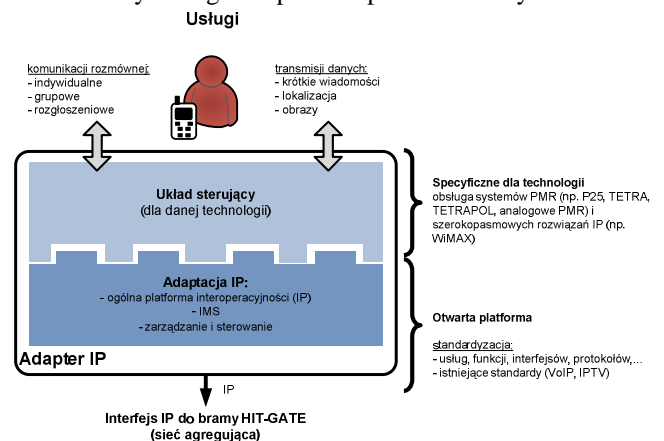
4. BRAMA HIT-GATE

Architekturę i koncepcję działania bramy HIT-GATE pokazano na rys. 1. Można w niej wyróżnić warstwę konwersji/translacji usług i protokołów przenoszonych przez daną sieć łączności. Następnie komunikat (treść) jest przekazywany za pośrednictwem agregatora sieci do platformy IMS bądź podlega przetworzeniu przez usługi łączenia różnych sieci. Z bramą zintegrowany jest także podsystem zarządzania systemem oraz podsystem eksploatacji i utrzymania. Ewentualna zamiana formatu komunikatu (np. wiadomość SDS (*Short Data Service*) w sieci standardu TETRA na wiadomość głosową dla sieci PMR) jest realizowana w warstwie konwertera/translatora.



Rys. 1. Warstwowa architektura bramy

Przyłączenie terminala danej sieci do bramy HIT-GATE jest obsługiwane przez adapter IP, który zapewnia obsługę komunikatu na poziomie elektrycznym, sygnalizacyjnym i protokołowym w taki sposób, aby dostosować go do domeny IP wykorzystywanej przez bramę. Schemat blokowy takiego adaptera IP pokazano na rys. 2.



Rys. 2. Adapter IP

5. METODYKA IDENTYFIKACJI WYMAGAŃ

W celu zebrania listy wymagań zastosowano odpowiednią metodykę działań, którą ujednolicono dla wysiłków podejmowanych przez partnerów w tym obszarze. Wykorzystano metodę VOLERE, której szablon specyfikacji wymagań zaadaptowano do szczegółów i potrzeb projektu HIT-GATE.

Każdy z członków konsorcjum realizował we własnym zakresie działania we współpracy z krajowymi użytkownikami pierwszego kontaktu w ramach procesu definiowania wymagań. Dla sformalizowania opisu wymagań zaproponowano wspólne podejście do tego zagadnienia, które jest łatwe w zastosowaniu i dostosowaniu do specyfiki projektu. Metodyka VOLERE jest prosta, gdyż nie wiąże się z koniecznością wdrożenia złożonej czy wieloetapowej analizy. Ponadto gwarantuje, że badania można przeprowadzić u wszystkich interesariuszy, którzy są zaangażowani w projektowanie i wdrożenie bramy, uwzględniając fakt, że ma ona spełniać zdefiniowane przez nich wymagania. Przyjęta i zaadaptowana metodyka pozwala zidentyfikować i formalnie przedstawić jednoznaczne wymagania oraz ocenić poprawność wymagań. Dzięki temu można uniknąć braków w ich kompletności i spójności.

Wykorzystywanie ujednoliconej metodyki zbierania, klasyfikacji i oceny wymagań jest ważne. Zarządzanie tak opracowanymi wymaganiami zapewnia wówczas mechanizmy ułatwiające identyfikowanie, definiowanie, ocenianie, opisywanie formalne i dopracowywanie zebranych wymagań jeśli jest taka potrzeba. Ponadto wymagania winny być kluczem do oceny wartości całego projektu w końcowej fazie rozwijania bramy. Zbiór dobrze zdefiniowanych i jednoznacznych wymagań jest niezbędny nie tylko jako dane wejściowe na etapie tworzenia specyfikacji i rozwijania systemu, ale także jako część działań oceniających postęp prac.

Metoda VOLERE definiuje proces zbierania i podstawy rejestrowania wymagań, sklasyfikowanych w ramach 27 kategorii podzielonych na pięć grup:

1. czynniki sprzyjające projektowi (przesłanki powiązane z aspektem biznesowym) — są to np. cele projektu, jak i interesariusze, z których każdy może mieć własne powody uczestniczenia w projekcie,
2. ograniczenia projektowe (obostrzenia w jaki sposób system ma być projektowany) — np. urządzenie musi być przenośne albo musi wykorzystywać już istniejące systemy, sprzęt, oprogramowanie lub też być oparte na dobrych praktykach biznesowych,
3. wymagania funkcjonalne, czyli fundamentalne i istotne założenia dotyczące realizowanego systemu — opisuje się co system ma robić lub jakie działania ma podejmować,
4. wymagania niefunkcjonalne, czyli właściwości którymi winny cechować się funkcje systemu — są to takie parametry jak wydajność czy użyteczność. Te wymagania są tak samo ważne jak wymagania funkcjonalne, aby wdrożenie systemu miało znamiona sukcesu,
5. zagadnienia projektowe, czyli warunki, w ramach których projekt będzie realizowany — powodem ich włączenia do zbioru wymagań jest konieczność zaprezentowania spójnego obrazu wszystkich czynników, które mają wpływ na powodzenie lub porażkę projektu, a ponadto konieczność pokazania jak kierownicy mogą

wykorzystać te wymagania jako pewne przesłanki na potrzeby zarządzania projektem.

Metodyka VOLERE jest uniwersalnym sposobem opisu wymagań. W tej publikacji skupiamy się na wymaganiach użytkowników z punktu widzenia ich potrzeb, a nie na wymaganiach systemu HIT-GATE, które zakłada się, że są pochodną tych pierwszych. Jednocześnie przyjęto, że nie jest wskazane prezentowanie jedynie punktu widzenia użytkowników, ponieważ mogą oni nie być świadomi wielu szczegółów, ograniczeń oraz innych założeń projektowych poczynionych na etapie opracowywania koncepcji bramy lub wynikających ze zróżnicowania wymagań zależnie od służby czy kraju. Dlatego zdecydowano się przedstawić kompleksowy zbiór wymagań obejmujący zarówno wymagania użytkowników, jak i wysokopoziomowe wymagania funkcjonalne i niefunkcjonalne podzielone na grupy wynikające z założeń dla bramy HIT-GATE przyjętych na etapie opracowywania koncepcji systemu i jego architektury. Dokonano zatem podziału na następujące grupy wymagań:

- komunikacja,
- transmisja danych,
- użyteczność,
- wydajność,
- eksploatacja,
- bezpieczeństwo,
- aspekty prawne.

W przyjętej metodyce VOLERE wymaganie jest opisywane przez następujące cechy:

- A. numer — każde wymaganie ma swój unikatowy numer ułatwiający śledzenie tego wymagania w czasie rozwijania systemu. Zaleca się, aby numer zawierał:
 - kolejną liczbę — zapewnia to jednoznaczność identyfikację wymagania,
 - typ wymagania — pole to może służyć za wskaźnik czego dotyczy dane wymaganie, a także pomagać porównywać wymagania tego samego typu umożliwiając wykrywanie sprzeczności i powtórzeń,
- B. numer zdarzenia lub przypadku użycia — identyfikuje zdarzenie lub przypadek użycia, którego wymaganie dotyczy. Można przypisywać do wymagania kilka zdarzeń i przypadków użycia,
- C. ocena użytkownika — jest to miara jak bardzo wymaganie jest istotne dla użytkownika. Wyraża ona poziom satysfakcji użytkownika, który zostanie osiągnięty jeśli wymaganie zostanie zrealizowane. Pozwala to dokonać priorytetyzacji wymagań, a później także funkcji systemu mając świadomość które wymagania są najważniejsze i pożądane z punktu widzenia użytkownika. Można zatem analizować wymaganie z różnej perspektywy oraz ustalić o co użytkownicy dbają najbardziej,
- D. priorytet — ważność wymagania jeśli chodzi o czas, w którym wymaganie będzie dostępne dla użytkownika,
- E. zależności — pozwala wskazać inne wymagania, które mają wpływ na dane wymaganie,
- F. konflikty — umożliwia śledzenie innych wymagań, które stoją w sprzeczności z danym wymaganiem.

W ramach przeprowadzonych badań wykorzystano uproszczony formularz wymagań zawierający elementy najbardziej odpowiadające specyfice projektu HIT-GATE. Pola w szablonie specyfikacji wymagań zawierają:

- identyfikator wymagania,
- ważność wymagania (wysoka/średnia/niska), która określa jak dane wymaganie jest istotne dla użytkow-

nika. Wysoki priorytet wskazuje, że jest to bezwzględne wymaganie dla bramy HIT-GATE; wymaganie z priorytet średnim jest pożądane; zaś niski priorytet dotyczy wymagań opcjonalnych,

- źródło wskazuje pochodzenie danego wymagania,
- wersja pozwala śledzić postęp prac nad wymaganiem,
- szybkość (normalna/pilna) informuje o czasie, w którym wymaganie winno być dostępne podczas realizacji misji,
- pewność (normalna/wysoka) wskazuje na niezawodność funkcjonowania wymagania. Wysoka pewność oznacza, że winno być dostępne potwierdzenie odebrania komunikatu,
- audyt (normalny/rozszerzony) oznacza, że winna być możliwość śledzenia realizacji wymagania podczas działania systemu,
- bezpieczeństwo (standardowe/rozszerzone) określa poziom bezpieczeństwa, który musi spełniać wymaganie,
- jakość (normalna/wysoka) wskazuje parametry jakościowe dotyczące realizacji wymagania,
- tytuł określa nazwę wymagania,
- opis wyjaśnia szczegóły wymagania.

Cały proces zbierania wymagań składał się z czterech etapów obejmujących:

- analizę informacji literaturowych w obszarze systemów ochrony publicznej i pomocy w przypadku katastrof i klęsk żywiołowych PPDR (*Public Protection and Disaster Relief*), jak i systemów PSC — bazując na różnych informacjach źródłowych dostarczonych przez partnerów lub znalezionych pośród zasobów bibliografii [1][4][5][6][7][9] zdefiniowano wstępną listę wymagań,
- opracowanie kwestionariusza wywiadu z użytkownikami i ekspertami dziedzinowymi — kwestionariusz zawierał uaktualnione na podstawie wiedzy i doświadczenia partnerów wymagania zidentyfikowane w etapie I,
- spotkania z użytkownikami, w celu wypracowania u wspólnionej wizji zapewnienia interoperacyjności z wykorzystaniem bramy — użytkownicy przeanalizowali zdefiniowane w etapie II wymagania oraz mogli określić kolejne,
- wewnętrzne dyskusje w gronie partnerów, w celu zdefiniowania końcowej listy wymagań opartej na przesłankach podanych przez użytkowników.

6. WYMAGANIA UŻYTKOWNIKÓW

Zidentyfikowane podczas badań główne wymagania funkcjonalne zebrano w tabeli poniżej (tabela 1). Zidentyfikowanymi wymaganiami niefunkcjonalnymi (m.in. jakość, efektywność itp.) powiązаныmi ze świadczonymi usługami, są:

- dla komunikacji rozmównej: klarowność komunikacji (brak szumów) oraz wysoka jakość głosu zapewniana przez kodek;
- dla transmisji danych: transmisja szerokopasmowa oraz zdolność do przenoszenia danych nawet podczas ich transferu kiedy transmitowany ruch ma dużą intensywność (*peak*).

Tabela 1. Wymagania funkcjonalne

Obszar	Wymaganie funkcjonalne
Komunikacja rozmówna	<p>Komunikacja rozmówna w ramach zdefiniowanych grup użytkowników;</p> <p>Komunikacja rozmówna z innymi służbami bezpieczeństwa, porządku publicznego i ratownictwa na poziomie lokalnym;</p> <p>Komunikacja grupowa:</p> <ul style="list-style-type: none"> • zapewnia połączenia „jeden do wielu” dla wszystkich utworzonych grup niezależnie od liczby dołączonych sieci łączności, jak i liczby użytkowników, • chroni przed nieautoryzowanym dostępem do grupy, • umożliwia automatyczną odpowiedź na wszystkie wywołania w ramach grupy, • zabezpiecza przed równoczesną komunikacją wielu użytkowników w ramach grupy, • winna informować użytkownika o przekroczeniu granic obszaru działań zdefiniowanych w systemie dla grupy, • zapewnia możliwości rozgłaszania komunikatów do wszystkich zarejestrowanych użytkowników grupy, • umożliwia prezentację identyfikatora użytkownika wszystkim użytkownikom; <p>Połączenia alarmowe na numer 112;</p> <p>Połączenia do central zakładowych PBX (<i>Private Branch eXchange</i>) użytkowników;</p> <p>Rejestracja treści połączeń (komunikatów);</p> <p>Możliwość przypisania priorytetów użytkownikom i typom połączeń;</p> <p>Zdolność do kolejowania połączeń</p>
Transmisja danych	<p>Transmisja danych w interfejsie radiowym;</p> <p>Dostęp do baz danych;</p> <p>Transmisja danych na potrzeby podejmowania decyzji;</p> <p>Możliwość wymiany danych między różnymi służbami pierwszego kontaktu;</p> <p>Transmisja zdjęć jeśli jest możliwa w danej sieci;</p> <p>Transmisja wideo jeśli jest możliwa w danej sieci;</p> <p>Transmisja metadanych na potrzeby inteligentnych systemów nadzoru</p>
Inne	<p>Możliwość realizacji usługi <i>roaming</i> na potrzeby działań transgranicznych;</p> <p>Szerokie możliwości funkcjonowania potencjalnie kompatybilnych technologii komunikacyjnych;</p> <p>Interoperacyjność kratowych sieci <i>ad-hoc</i> dla służb pierwszego kontaktu działających na tym samym obszarze wliczając w to inne funkcjonujące już sieci kratowe;</p> <p>Zdalne zarządzanie terminalem przez administratora;</p> <p>Możliwość retransmisji</p>

Innymi najważniejszymi wymaganiami zidentyfikowanymi w procesie opisanym w rozdz. 5 są m.in.:

- system dla służb bezpieczeństwa, porządku publicznego i ratownictwa musi zapewniać łączność między centrum dowodzenia (poziom taktyczny) i dowódcą akcji (poziom operacyjny) uwzględniając relacje w łańcuchu dowodzenia;

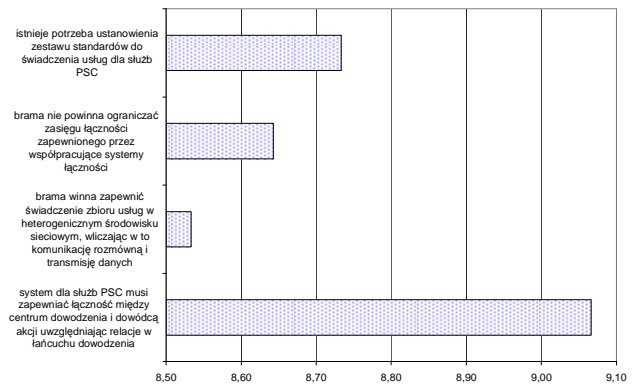
- winna być możliwość wdrożenia standardowych procedur operacyjnych;
- brama nie powinna ograniczać zasięgu łączności zapewnionego przez współpracujące systemy łączności używane podczas misji w miejscu akcji;
- brama winna obsługiwać systemy łączności zarówno odziedziczone, współczesne, jak i szerokopasmowe następnej generacji używane przez służby pierwszego kontaktu;
- użytkownicy systemów bezprzewodowych winny mieć zapewnioną mobilność na takim poziomie jakim gwarantuje system używany w miejscu akcji;
- brama winna zostać zaprojektowana w taki sposób, aby umożliwić dodawanie nowych sieci znanego typu w sposób modułarny zapewniając stały rozwój rozwiązania, które będzie stale uaktualniane;
- bazując na zaadaptowanych standardach brama powinna oferować otwarte interfejsy oraz szeroki zakres świadczonych usług przenoszonych przez wiele sieci; będą to takie standardy jak: protokół IP jako bazowy (interoperacyjność co najmniej do warstwy 3. modelu ISO/OSI), IPTV, VoIP (*Voice over IP*), RTP i SIP/SDP;
- system dla służb bezpieczeństwa, porządku publicznego i ratownictwa musi zapewniać komunikację pomiędzy różnymi służbami i między tymi służbami i centrum dowodzenia;
- brama umożliwi służbom pierwszego kontaktu komunikację w heterogenicznym środowisku sieciowym podczas działań prowadzonych przez nie z wykorzystaniem obecnie eksploatowanego sprzętu łączności oraz bez zmian w użytkowanych stacjach bazowych i infrastrukturach sieciowych poza zapewnieniem ich przyłączenia do bramy;
- brama umożliwi automatyczną integrację nowych sieci znanego typu opierając się na takich mechanizmach jak: (i) podłącz i używaj „*Plug'n'Play*” oraz (ii) dołącz w trakcie „*on-the-fly*”, które pozwolą bramie automatycznie adaptować się i pracować z nowo dołączonymi sieciami znanego typu bez potrzeby chwilowego wstrzymywania świadczenia usług;
- brama winna być zaprojektowana stosując zaadaptowaną metodykę określoną dla krytycznych systemów bezpieczeństwa; winna używać bezpiecznych technologii i wykorzystywać sprawdzone technologie zapewniające kompleksowe bezpieczeństwo dla transmisji od końca do końca przez wszystkie sieci zaangażowane w zestawione połączenie na potrzeby przesłania treści;
- system dla służb bezpieczeństwa, porządku publicznego i ratownictwa musi zapewniać komunikację wewnętrzną na potrzeby lokalnego centrum dowodzenia oraz między lokalnym centrum dowodzenia i innymi centrami dowodzenia;
- istnieje potrzeba ustanowienia zestawu standardów do świadczenia usług dla służb bezpieczeństwa, porządku publicznego i ratownictwa.

Najważniejsze wymagania z ich oceną ważności przedstawiono na rys. 3. Podano wartość średnią przy skali ocen 1-10.

7. WNIOSKI

Na rys. 4 pokazano odsetek wymagań użytkowników względem typów wymagań. Większość wymagań dotyczy

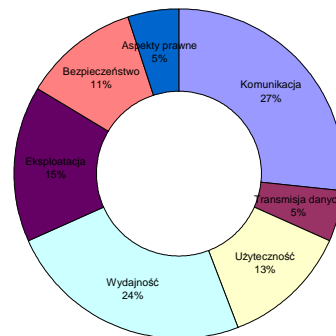
aspektów komunikacji, zaś druga najważniejsza grupa wymagań wiąże się z wydajnością projektowanego systemu.



Rys. 3. Ocena ważności zidentyfikowanych wymagań

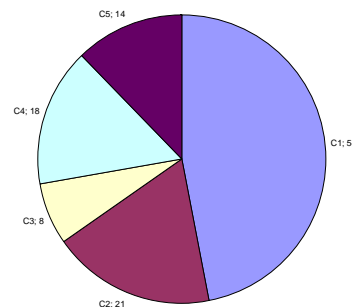
Wymagania użytkowników można podzielić na pięć kategorii:

- C1 wymagania na usługi komunikacji i wymagania wydajnościowe,
- C2 wymagania na mobilność i zestawianie połączeń,
- C3 wymagania na interoperacyjność,
- C4 bezpieczeństwo danych (poufność, dostępność, integralność itp.) i zapewnienie bezpieczeństwa pracy,
- C5 wymagania dotyczące zarządzania i monitorowania potrzeb.



Rys. 4. Odsetek wymagań użytkowników względem typów wymagań

Kategorie C1 i C2 są opisane największą liczbą zidentyfikowanych wymagań (Rys. 5).



Rys. 5. Liczba wymagań w danej kategorii

Możliwości interoperacyjne, które zaoferuje brama HIT-GATE, muszą odpowiadać potrzebom i oczekiwaniom użytkowników. Zidentyfikowane i opisane wymagania są wykorzystywane w innych pakietach zadań projektu HIT-GATE jako wskazówki projektowe dla opracowywanej bramy. Są zatem pomocne w określeniu architektury, zdefiniowaniu wymagań systemowych oraz przedstawieniu sce-

nariuszy i przypadków użycia, także na potrzeby demonstracji.



Badania opisane w tej publikacji zrealizowano w ramach projektu HIT-GATE (nr 284940).

SPIS LITERATURY

- [1] “D2.1, Case studies and scenarios report”, HIT-GATE project, 2012.
- [2] “Deliverable D2.2, Analysis of crisis management system requirements, ver. 3”, SECRI COM project, July 2009.
- [3] “Requirements specification template”, Edition 15 March 2010, James & Suzanne Robertson principals of the Atlantic Systems Guild.
- [4] “Description of work of the HIT-GATE project”, 2011.
- [5] “Report of the workshop on ‘Interoperable communications for safety and security’ ”, Workshop jointly organized by DG ENTR and DG JRC with the support of EUROPOL and FRONTEX, Gianmarco Baldini, 28-29 June 2010 – Ispra, Italy, EUR 24540 EN.
- [6] “PPDR spectrum harmonisation in Germany, Europe and globally”, WIK-Consult, Final Full Public Report, Bad Honnef, 6 December 2010.
- [7] “LTE as potential communications technology for public safety operations – a usability study taking into account the aspect ‘private vs. shared network’ ”, Baccalaurean Thesis II, Ing. Manfred BLAHA, 2011.
- [8] “Meeting the challenge: the European security research agenda”, European Security Research Advisory Board, September 2006 – <http://ec.europa.eu/enterprise/policies/security/files/esrab-re-report-en.pdf>.
- [9] S. O’Neill et al., “User requirements for mission-critical application – the SECRI COM case”, Technical Sciences, No. 15(1)/2012, 2012.
- [10] W. Wojciechowicz et al., “Seamless communication for crisis management”, Technical Sciences, No. 15(1)/2012, 2012.
- [11] W. Wojciechowicz et al., “Information and communication technology and crisis management”, Technical Sciences, No. 15(1)/2012, 2012.
- [12] ETSI TS 102 181, “Emergency communications (EMTEL): Requirements for communication between authorities/organizations during emergencies”, 2008.
- [13] Network Centric Operations Industry Consortium, “Findings and recommendations for mobile emergency communications interoperability (MECI)”, 2007.