



**Generalna Dyrekcja Dróg Krajowych i Autostrad
oraz
Stowarzyszenie ITS Polska**

Inteligentne Systemy Transportowe

Specyfikacja Techniczna nr 2

Obszar tematyczny:

**„Standard realizacji mediów do
łączości i transmisji danych KSZR”**

Lipiec 2012

Autorzy opracowania

Specyfikacja została opracowana pod kierownictwem:

Marek Stencel

AGH Katedra Metrologii i Elektroniki

przez zespół autorski w składzie:

Paweł Rzuciło – sekretarz

GDDKiA Oddział Kraków

Zbigniew Marszałek

AGH Katedra Metrologii i Elektroniki

Krzysztof Florian

Alcatel - Lucent Polska

Robert Król

Alcatel - Lucent Polska

Andrzej W. Mitas

APM Sp. z o.o.

Witold Konior

APM Sp. z o.o.

Bartłomiej Brzozowski

Kapsch Telematic Services

Wojciech Karp

Mark Electronics

Karol Kiryczyński

Siemens Sp. z o.o.

Sebastian Mikołajczyk

Sprint

Wojciech Apolinarski

Sprint

Łukasz Stawiarski

Trax Elektronik

Bartłomiej Krzywda

Trax Elektronik

Przedmiot i cel opracowania

Opracowanie jest efektem współpracy pomiędzy Stowarzyszeniem ITS POLSKA, a Generalną Dyрекcją Dróg Krajowych i Autostrad zawiązanej na podstawie porozumienia dotyczącego wspólnego opracowania pakietu Specyfikacji Technicznych niezbędnych do usystematyzowania i standaryzacji procesu przygotowania i realizacji projektów infrastrukturalnych z wykorzystaniem inteligentnych systemów transportowych.

Niniejsze Opracowanie stanowi jedno z ośmiu Specyfikacji dotyczących planowanego przez GDDKiA Krajowego Systemu Zarządzania Ruchem.

Specyfikacje mają charakter ogólnodostępny, dzięki czemu mogą zostać wykorzystane przez dowolny podmiot przy realizacji projektów obejmujący zastosowanie rozwiązań z obszaru inteligentnych systemów transportowych. Specyfikacja została przygotowana w sposób otwarty i transparentny, co zostało zapewnione poprzez udział w procesie tworzenia opracowania wszystkich zainteresowanych podmiotów.

ZASILANIE ELEMENTÓW SYSTEMU
ZARZĄDZANIA RUCHEM

1. Zasilanie podstawowe	5
2. Zasilanie alternatywne	6
3. Specyfikacja urządzeń zasilających	7
4. Monitoring stanu zasilania	9
5. Bezpieczeństwo	9
5.1 Instalacje odgromowe	9
5.2 Instalacje przepięciowe, określenie ilości i rodzaju zabezpieczeń	9
5.3 Bezpieczeństwo osób obsługujących, oznaczenia, zabezpieczenia	10
5.4 Normy i standardy	10
5.5 Zasady wyznaczania funkcji niezawodności	10

1. Zasilanie podstawowe

Podstawowym zasilaniem urządzeń wchodzących w skład KSZR jest jednofazowa sieć elektroenergetycznej najniższych napięć (sieć nn - 230 VAC; 50Hz) lub trójfazowa sieć elektroenergetycznej nn (3x400 VAC, 50Hz) wchodzące w skład Polskiego Systemu Energetycznego.

W przypadku zgrupowania urządzeń w pobliżu węzłów drogowych, sieć elektroenergetyczna powinna być wykonana jako podwójna sieć zasilająca (o parametrach opisanych uprzednio) – jedna sieć jako nie gwarantowana, oraz druga sieć rozprowadzająca napięcie gwarantowane.

Do sieci zasilającej nie podtrzymywanej (nie gwarantowanej) powinny być podłączane urządzenia nie wymagające podtrzymania zasilania własnego, w czasie zaniku napięcia zasilania.

Do sieci zasilającej gwarantowanej powinny być podłączane urządzenia wymagające podtrzymania zasilania własnego w czasie zaniku napięcia zasilania. Do takich urządzeń należą m.in. zespoły serwerowni, stacje meteorologiczne etc. Pełne wyspecyfikowanie rodzaju urządzeń, które wymagają zasilania awaryjnego należy do zamawiającego.

Infrastruktura dodatkowa zapewniająca działanie sieci gwarantowanej musi zostać umieszczona w budynkach wyposażonych w odpowiednie instalacje (np. wentylacji i klimatyzacji) oraz stały dozór techniczny.

Sieć gwarantowana powinna zostać wyposażona w baterie podtrzymujące (UPS) reagujące na krótkotrwałe przerwy w zasilaniu, umożliwiające podtrzymanie przez czas minimum 10min. Podtrzymanie bateryjne (UPS) powinno działać w trybie szeregowym („on-line”), niedopuszczalne są jakiekolwiek przerwy w zasilaniu w czasie zadziałania układów awaryjnego podtrzymania. Jeżeli w czasie 1 min napięcie zasilające (na przyłączy energetycznym) nie powróci do zakładanych parametrów, uruchomiony powinien zostać drugi stopień podtrzymania – generatory prądotwórcze (np. generator spalinowy, ogniwo paliwowe). Urządzenia te powinny umożliwiać nieprzerwane podtrzymywanie zasilania w sieci gwarantowanej przez okres minimum 6h bez uzupełniania paliwa (lub też inny czas określony przez zamawiającego). System powinien umożliwiać uzupełnianie paliwa w trakcie pracy.

Stosowane w sieci gwarantowanej baterie UPS powinny być odporne na zapady napięcia na przyłączy energetycznym. Poprzez zwiększenie wartości prądu wejściowego powinny utrzymywać napięcie sieci gwarantowanej w granicach $\pm 10\%$ wartości znamionowej.

Stosowane baterie UPS, po całkowitym rozładowaniu powinny umożliwiać pełne naładowanie po czasie maksimum 6h (ładowanie z generatora prądotwórczego lub prosto z przyłącza energetycznego po powrocie zasilania), lub też w innym czasie określonym przez zamawiającego.

Parametry sieci gwarantowanej (maksymalna moc podłączonych urządzeń) powinny zostać określone przez zamawiającego na etapie projektu. Projektowane parametry systemu powinny uwzględniać przyszły rozwój czyli zapewniać poprawne zasilanie nawet przy wzroście planowanego zapotrzebowania o 30% (lub inny wskaźnik wskazany przez zamawiającego).

Istnieje możliwość zasilania urządzeń wymagających podtrzymania z wykorzystaniem sieci nie gwarantowanych. W takim przypadku urządzenia muszą być wyposażone w wewnętrzne podtrzymania akumulatorowe (akumulatory bezobsługowe, ze stałym elektrolitem przystosowane do pracy w pomieszczeniach zamkniętych np. żelowe, AGM) zapewniające minimum 24h (lub też inny czas określony przez zamawiającego) podtrzymania zasilania własnego w czasie zaniku napięcia zasilającego. Urządzenia zasilające muszą gwarantować brak przerw w podtrzymaniu w czasie załączenia układów podtrzymujących. Po przywróceniu zasilania głównego, w pełni rozładowane baterie akumulatorowe muszą zostać w pełni naładowane w czasie nie dłuższym niż 24h (lub też w innym czasie określonym przez zamawiającego).

Wybór pomiędzy zasilaniem urządzeń wymagających podtrzymania zasilania z sieci gwarantowanej lub też z sieci nie gwarantowanej powinien zostać dokonany na etapie projektu poprzez wykonanie szczegółowej analizy uwzględniającej uwarunkowanie ekonomiczne, środowiskowe oraz funkcjonalne.

2. Zasilanie alternatywne

Dla urządzeń o niskim poborze mocy, występujących w lokalizacjach, w których z ekonomicznego punktu widzenia nieopłacalne jest doprowadzenie sieci elektroenergetycznej najniższych napięć (3x400 VAC, 50Hz), dozwolone jest stosowanie alternatywnych źródeł energii. Nie wprowadza się żadnych regulacji co do typów stosowanych źródeł energetycznych (np. ogniwa PV, turbiny wiatrowe itp.), oraz wykorzystywanego magazynu energii (baterie akumulatorów, baterie superkondensatorów etc.). W przypadku stosowania

akumulatorów muszą to być jednak urządzenia bezobsługowe, ze stałym elektrolitem przystosowane do pracy w pomieszczeniach zamkniętych (np. żelowe, AGM).

Wybór zastosowanych źródeł energii odnawialnej i rodzaju magazynów energii musi zostać poprzedzony staranną analizą uwzględniającą kwestie ekonomiczne, środowiskowe oraz funkcjonalne.

Wymagana jest całkowita niezależność energetyczna zaprojektowanego systemu, tzn. system zasilający powinien zostać zaprojektowany w taki sposób, aby zapewnić 100% zapotrzebowanie energetyczne dołączanego obciążenia niezależnie od warunków atmosferycznych oraz pory roku. Dodatkowo system na etapie projektu powinien zakładać przyszły rozwój czyli zapewniać poprawne zasilanie nawet przy wzroście planowanego zapotrzebowania o 30% (lub inny wskaźnik wskazany przez zamawiającego).

W przypadku stosowania stacjonarnych baterii ogniwo fotowoltaicznych, należy zapewnić orientację umożliwiającą maksymalne wykorzystanie padającego promieniowania słonecznego, dla miesięcy zimowych. Kąt instalacji baterii ogniwo musi również zapewniać łatwe zsuwanie się płatów śniegu zalegających na powierzchni paneli, w miesiącach zimowych.

3. Specyfikacja urządzeń zasilających

Wszystkie urządzenia zasilające muszą być przystosowane do pracy w warunkach przemysłowych (tzn. temperatura otoczenia $-25^{\circ}\text{C} \div +70^{\circ}\text{C}$, wilgotność względna powietrza $20\% \div 80\%$), z tego wymagania wyłączone są urządzenia pracujące w miejscach, w których dzięki systemom klimatyzacji i wentylacji zapewnione jest utrzymywanie stałych warunków środowiskowych (temperatura otoczenia powyżej 5°C , wilgotność względna powietrza $30\% \div 70\%$), niezależnie od pory roku (np. zespoły serwerowni). Używane w tym celu systemy klimatyzacji i wentylacji muszą być pod stałym nadzorem technicznym, umożliwiającym podjęcie szybkich działań naprawczych w przypadku awarii, ponieważ od poprawności ich działania zależy niezawodność układów zasilających.

W celu zapewnienia dużej niezawodności, urządzenia zasilające nie mogą posiadać wewnętrznych elementów ruchomych (wyłączone z tego mogą być urządzenia zasilające dużej mocy, umieszczone w lokalizacjach, w których obecny jest stały dozór techniczny). Urządzenia zasilające powinny cechować się wysoką sprawnością działania, umożliwiającą

stosowanie chłodzenia pasywnego (naturalna konwekcja, przewodzenie, radiacja). Stosowanie, w celu chłodzenia urządzeń zasilających, konwekcji wymuszonej, jest dopuszczalne jedynie w lokalizacjach, w których funkcjonują systemy wentylacji i klimatyzacji pod stałym nadzorem technicznym.

Jednofazowe urządzenia zasilające AC-DC muszą pracować poprawnie w zakresie $78\% \div 110\%$ znamionowej wartości napięcia zasilania (dla jednofazowej sieci nn jest to zakres: $180\text{ V (RMS)} \div 253\text{ V (RMS)}$). Wszystkie stosowane urządzenia muszą zapewniać ograniczenie wartości szczytowej prądu rozruchu (po stronie AC) do maksymalnie 3-krotnej wartości amplitudy natężenia prądu w stanie ustalonym po stronie AC. Wymaganie to może zostać spełnione poprzez zastosowanie urządzeń o odpowiedniej topologii (np. zasilacze PFC) lub poprzez zastosowanie zewnętrznych (w stosunku do urządzenia zasilającego) układów ograniczających (np. układy typu soft-start).

Zalecane jest, aby wszystkie urządzenia zasilające AC-DC, nawet jeżeli w świetle obowiązujących norm i przepisów ze względu na swoją moc znamionową są wyłączone z takich wymagań, realizowały korekcję współczynnika mocy utrzymując jego wartość na poziomie nie niższym niż 0,95 przy obciążeniu znamionowym.

Wszystkie urządzenia zasilające AC-DC muszą spełniać wymagania prawne i normatywne stawiane tego rodzaju urządzeniom pod względem poziomu generowanych harmonicznych prądu.

Wszystkie stosowane urządzenia zasilające AC-DC muszą zapewniać odporność na stałe zwarcie wyjścia (strona DC), stałe przeciążenie (do 120% mocy znamionowej), zapewniać wewnętrzną separacji galwaniczną pomiędzy stroną AC, a wyjściem DC oraz spełniać normy i wymagania prawne stawiane takim urządzeniom pod kątem kompatybilności elektromagnetycznej (emisyjność i podatność), bezpieczeństwa użytkowania, wytrzymałości elektrycznej izolacji, odporności przepięciowej.

Urządzenia, których obudowa zewnętrzna jest wykonana z metalu muszą mieć możliwość doprowadzenia przewodu PE uziemiającego obudowę i zapewniającego poprzez poprawnie zaprojektowaną oraz wykonaną instalację elektryczną bezpieczeństwo użytkowania.

Wszystkie urządzenia w których występują napięcia o poziomach wykraczających poza wartości uznawane za bezpieczne muszą być odpowiednio oznakowane.

Parametry układów zasilania awaryjnego urządzeń wchodzących w skład Systemu przydrożnej telefonii alarmowej zostały określone w innej części specyfikacji.

4. Monitoring stanu zasilania

Urządzenia zasilane z sieci nie gwarantowanej, a wymagające podtrzymania zasilania muszą monitorować stan linii zasilającej i alarmować system nadrzędny w przypadku zaników napięcia. Równocześnie monitorowany musi być stan naładowania akumulatorów stanowiących zapasowy magazyn energii, wraz z alarmowaniem o przekroczeniu 20% (lub inny poziom zaakceptowany przez zamawiającego) magazynowanej energii (w czasie działania urządzenia w trybie zasilania awaryjnego).

Urządzenia zasilane z alternatywnych źródeł energii muszą monitorować stan naładowania magazynów energii i alarmować przekroczenie progów 50, 30 i 20% (lub inne zaakceptowane przez zamawiającego) magazynowanej energii maksymalnej.

Do wszystkich urządzeń zasilających, które muszą monitorować odpowiednie napięcia zasilania powinien umożliwiony zdalny dostęp (na rozkaz).

W urządzeniach zasilanych z innych z innych przyłączy niż przyłącza zasilające sieć gwarantowaną i nie gwarantowaną należy stosować inteligentne liczniki energii umożliwiające zdalny odczyt zużytej energii.

5. Bezpieczeństwo

5.1 Instalacje odgromowe

Urządzenia infrastruktury drogowej winny posiadać wyprowadzone i prawidłowo oznaczone zaciski do podłączenia instalacji uziemiającej. Uziemienie wykonać bednarką stalową ocynkowaną Fe/Z min. 90 mm², którą należy połączyć z istniejącym uziemieniem łącz kablowych zasilających punkt. Oporność uziemienia nie większej niż 10 Ω. W przypadku uzyskania oporności uziemienia większej niż 10 Ω zainstalować należy dodatkowe uziomy pionowe w odległości 3,5 m od wcześniej instalowanych.

5.2 Instalacje przepięciowe, określenie ilości i rodzaju zabezpieczeń

Urządzenia infrastruktury drogowej winny być wyposażone w elementy zabezpieczeń przepięciowych, chroniące podzespoły elektroniczne przed skutkami zakłóceń elektrostatycznych i elektromagnetycznych, mogących wystąpić w liniach zasilających oraz na do prowadzeniach czujników pomiarowych.

5.3 Bezpieczeństwo osób obsługujących, oznaczenia, zabezpieczenia

Skrzynie i szafy zasilające należy oznakować nalepką informującą o wysokim napięciu, oraz zastosować zabezpieczenie przed niepowołanym dostępem.

Przewód ochronny zawsze oznaczony kolorem żółto-zielonym, przewód neutralny kolorem niebieskim, przewody fazowe L1-brązowy, L2-czarny, L3-szary. Dodatkowo należy zastosować etykiety informujące na przewodach zasilających.

5.4 Normy i standardy

PN-86/E 05003.01-Ochrona odgromowa obiektów budowlanych przed wyładowaniami atmosferycznymi

PN-IEC 61024:1 Ochrona odgromowa obiektów budowlanych

5.5 Zasady wyznaczania funkcji niezawodności

Określenie zasad wyznaczania funkcji niezawodności oraz zdefiniowanie warunku koniecznego dla odbioru dokumentacji techniczno-ruchowej w postaci danych katalogowych użytych elementów i podzespołów w kontekście parametrów niezawodnościowych.

Realizacja mediów do transmisji danych KSZR

1. WSTĘP	13
1.1 PRZEDMIOT I OPRACOWANIA	13
1.2 ZAKRES STOSOWANIA	13
1.3 PODSYSTEMY INTEGROWANE W SYSTEMIE ITS – WYMAGANIA TRANSMISYJNE	15
1.4 NIEZAWODNOŚĆ	19
1.5 BEZPIECZEŃSTWO SIECI	19
 2. ARCHITEKTURA SYSTEMU ITS	 22
2.1 ELEMENTY BĘDĄCE PRZEDMIOTEM OPRACOWANIA	22
2.2 INTERFEJSY DO DOŁĄCZANIA URZĄDZEŃ ITS DO SYSTEMU ŁĄCZNOŚCI	23
2.3 ZASADY DOBORU KANAŁÓW ŁĄCZNOŚCI DO POTRZEB PODSYSTEMÓW ITS	24
 3. WYMAGANIA SZCZEGÓŁOWE	 25
3.1 SIEĆ ŁĄCZNOŚCI DEDYKOWANA	25
3.1.1 Topologia sieci	25
3.1.2 Metodyka tworzenia dróg obejściowych	27
3.1.4 Kanalizacja kablowa	28
3.1.5 Światłowody	28
3.1.5 Sieci kablowe	29
3.1.6 Urządzenia aktywne	29
3.1.7 Sieci bezprzewodowe dedykowane	37
3.1.7.1 Pasma licencjonowane	37
3.1.7.1.1 Łączność trunkingowa	37
3.1.7.1.2 Radiolinie	38
3.1.7.2 Pasma nielicencjonowane	40
3.1.7.2.1 Radiolinie (punkt-punkt)	42
3.1.7.2.2 Sieci (punkt - wielopunkt)	43
3.1.7.3 Linki w falach milimetrowych i optyczne (laserowe)	44
3.2 SIECI ŁĄCZNOŚCI DZIERŻAWIONE I ZASADY KORZYSTANIA Z USŁUG W SIECIACH OPERATORSKICH	45
3.2.1 Dzierżawa kanalizacji	45
3.2.2 Dzierżawa kabli	45
3.2.3 Dzierżawa kanałów	46
3.2.4 Usługi w sieciach bezprzewodowych	46
3.3 ŁĄCZNOŚĆ DLA URZĄDZEŃ MOBILNYCH I NOMADYCZNYCH	47
3.4 ZASILANIE URZĄDZEŃ W SYSTEMACH ITS	47
3.4.1 Generalne zasady zasilania	47
3.4.2 Zasady zasilania urządzeń ITS zgrupowanych w obiektach budowlanych	48
3.4.3 Zasady zasilania urządzeń w terenie	48
3.4.3.1 Urządzenia zgrupowane w pobliżu węzłów	48
 4. TESTY , DOKUMENTACJA, SZKOLENIA	 49

4.1.DOKUMENTACJA, TESTOWANIE I SZKOLENIA	49
4.2 INSTRUKCJA UŻYTKOWANIA I KONSERWACJI	49
4.3 DOKUMENTACJA FABRYCZNYCH TESTÓW ZDAWCZO-ODBIORCZYCH (FAT)	49
4.4 DOKUMENTACJA TESTÓW ZDAWCZO-ODBIORCZYCH NA MIEJSCU (SAT)	50
4.5 SZKOLENIA	50

5. UTRZYMANIE I ZARZĄDZANIE.....51

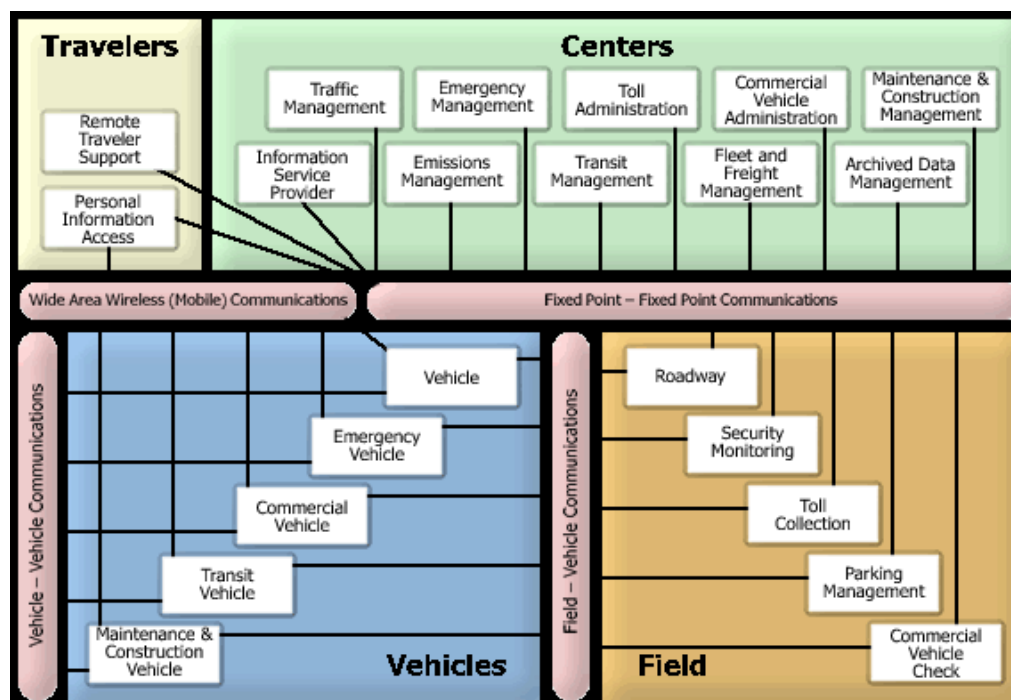
1. Wstęp

1.1 Przedmiot i opracowania

Przedmiotem opracowania są parametry techniczne mediów stosowanych w do transmisji danych w Krajowym Systemie Zarządzania Ruchem. Przez media te rozumie się fizyczne kanały transmisyjne oraz urządzenia odpowiedzialne za nadawanie i odbiór danych w ww. systemie.

1.2 Zakres stosowania

Przykładową architekturę systemu ITS zdefiniowaną przez RITA (Research and Innovative Technology Administration) przedstawiono na rys. 1.



Rys. 1 Architektura ITS wg. RITA (Research and Innovative Technology Administration - http://www.its.dot.gov/arch/arch_longdesc.htm).

Diagram przedstawia cztery klasy systemów ITS, wraz z ich podsystemami:

- * Travelers – podróżni (żółty): zdalna informacja podróżnych i dostęp do informacji personalnych
- * Centers - centra (zielony): dostawca informacji, zarządzanie ruchem, zarządzanie emisją zanieczyszczeń, zarządzanie kryzysowe, zarządzanie tranzytami, pobór opłat, zarządzanie

flotą i ładunkami, administrowanie pojazdami komercyjnymi, zarządzanie danymi archiwalnymi oraz zarządzanie i utrzymywanie infrastruktury

* Vehicles – pojazdy (niebieski): pojazdy utrzymania i serwisowe, pojazdy tranzytowe, pojazdy komercyjne, pojazdy ratunkowe oraz pojazdy

* Field – infrastruktura terenowa (pomarańczowy): drogi, monitoring bezpieczeństwa, pobór opłat, zarządzanie parkingami, monitorowanie pojazdów komercyjnych.

Wszystkie te podsystemy są połączone za pomocą kanałów przepływu informacji. Ponadto na diagramie znajdują się pola reprezentujące typy systemów łączności:

- * Wide area wireless (mobile) – łączność mobilna
- * Fixed-point to fixed-point - połączenia stacjonarne
- * Vehicle to vehicle – połączenia pomiędzy pojazdami (bezprowadowe)
- * Field – Vehicle Communication – połączenia pojazd - infrastruktura

Diagram bardzo wyraźnie pokazuje, że bez zapewnienia adekwatnej łączności i właściwego przepływu informacji w zasadzie nie ma możliwości uruchomienia, działania oraz korzystania z żadnego systemu lub podsystemu ITS. Poprawnie zaprojektowany system łączności jest szkieletem każdego systemu lub podsystemu ITS.

Każdy podsystem systemu ITS ma specyficzne wymagania na kanały łączności, które muszą być dobrane adekwatnie do potrzeb danego podsystemu, jego topologii, użytkowników, z uwzględnieniem kosztów zarówno budowy jak i eksploatacji systemu.

Przy doborze parametrów oraz technologii wykonania kanałów łączności trzeba uwzględniać też realizowane przez podsystemy zadania, oraz ich priorytet. Najwyższy priorytet powinny mieć połączenia realizowane przez systemy mające bezpośredni wpływ na bezpieczeństwo ludzi. Przy projektowaniu takich podsystemów i wyborze technologii trzeba szczególnie brać pod uwagę możliwość i niezawodność ich działania w sytuacjach kryzysowych i awaryjnych. Bardzo istotne są także połączenia mające wpływ na rozliczenia finansowe pomiędzy uczestnikami ruchu a administracją i właścicielem drogi.

Istotą działania wszystkich systemów ITS jest podejmowanie decyzji na podstawie uzyskiwanych i dostępnych informacji. Trafność podejmowanych decyzji zależy od jakości dostępnych informacji, ich dokładności i aktualności. Należy zwrócić uwagę na fakt, że wymagania na aktualność informacji, oraz skutki opóźnienia w ich przekazywaniu lub w związku z ich utratą, są różne w zależności od podsystemu. Opóźnienia w odczycie danych pogodowych w zasadzie w małym stopniu wpływają na działanie innych podsystemów. Natomiast opóźnienia w przekazywaniu informacji ratunkowych mogą skutkować utratą życia.

Generalnie oczekuje się, że systemy ITS powinny:

- zwiększyć przepustowość sieci ulic
- poprawić bezpieczeństwo ruchu drogowego
- zmniejszyć czas podróży i zużycie energii
- poprawić jakość środowiska naturalnego (redukcja emisji spalin)
- poprawić komfort podróżowania i warunków ruchu kierowców, podróżujących transportem zbiorowym oraz pieszych
- redukować koszty zarządzania taborom drogowym
- redukować koszty związane z utrzymaniem i renowacją nawierzchni

- zwiększyć korzyści ekonomiczne w regionie

Aby skutecznie realizować tego typu cele zarządzający systemem dróg powinien mieć dostęp do danych napływających automatycznie i w odpowiednim przedziale czasu. Niektóre dane muszą być dostępne w czasie rzeczywistym (np. alarmy, połączenia ratunkowe, obrazy z kamer). Inne dane mogą napływać z niewielkimi opóźnieniami. Część danych jest zbierana w urządzeniach i przekazywana dalej w określonych przedziałach czasu w postaci zagregowanej lub wstępnie przetworzonej. Dane pobierane z klasycznych czujników niosą w sobie ograniczone zasoby informacyjne. W celu podejmowania adekwatnych decyzji zarządzający powinien mieć także możliwości weryfikacji napływających danych i podglądu sytuacji. Dlatego coraz częściej wprowadza się systemy wideo. Pozwalają one na monitorowanie newralgicznych punktów na żywo oraz dokumentowanie zdarzeń i podjętych działań.

Źle zaprojektowana sieć transmisji danych może uniemożliwić realizację celów stawianych przed systemem ITS. Budowa systemu ITS nie jest jednorazowym zadaniem ale procesem w czasie którego dodawane będą kolejne zadania i podsystemy.

Ze względu na koszty, stan techniki, stan prawny itp. budowa kolejnych podsystemów będzie przesunięta w czasie, a systemy ITS będą eksploatowane przez dziesiątki lat. Powinno przewidywać się ich rozwój, a w szczególności gotowość systemów łączności do realizacji nowych zadań.

1.3 Podsystemy integrowane w systemie ITS – wymagania transmisyjne

Poniżej przedstawiona jest analiza potrzeb związanych z przepływem informacji dla kilku podstawowych podsystemów ITS które są przedmiotem opracowania. W analizie wzięto pod uwagę ilość przekazywanych danych oraz kierunki ich przepływu.

Podsystem sterowania ruchem.

W skład takiego podsystemu wchodzi lokalne czujniki ruchu (pętle indukcyjne, czujniki wizyjne) przekazujące bieżące dane pomiarowe do centrów lub lokalnie do kontrolerów sygnalizacji świetlnej. Informacje czujników i/lub sterowników świateł przekazywane są do centrów zarządzania ruchem. Natomiast z centrów zarządzania ruchem w dół sieci, do sterowników przekazywane są informacje sterujące bezpośrednio przełączeniami świateł lub korygujące ustawienia lokalne – w zależności od przyjętego rozwiązania. Oczywiście oprócz informacji zwianych bezpośrednio ze sterowaniem ruchem przekazywane są w obu kierunkach informacje utrzymaniowe. Wymagane przepływy w tego typu połączeniach to kilkanaście **kb/s** (kilobajtów na sekundę) dla każdego sterownika, w obu kierunkach.

Tablice zmiennej treści

Wymagania jak dla sterowników świateł.

Systemy wizualnej informacji dla podróżnych.

Są to systemy zainstalowane przy drogach i służą do przekazywania informacji podróżującym. W najczęstszym przypadku jest to prosta informacja tekstowa i wystarcza do jej modyfikacji przepływność rzędu pojedynczych **b/s** (bajtów na sekundę)– głównie do tablic, czyli w dół sieci. Jednak już teraz, w niektórych lokalizacjach, oczekuje się wyświetlania nie tylko informacji tekstowych, ale również wideo – reklam, materiałów

promocyjnych itp. Wtedy wymagania na przepływ w sieci rosną nawet do kilku **Mb/sek**. Przepływ danych głównie w dół sieci.

Systemy komunikacji głosowej.

Są to najczęściej dedykowane systemy połączeń alarmowych (wymagane prawem jako element wyposażenia autostrady płatnej). Umożliwiają łączność ze specjalnych stanowisk usytuowanych wzdłuż ciągów komunikacyjnych z dyspozytorami – kilkanaście **kb/s** na połączenie, połączenia dwukierunkowe. Ponadto trzeba też zapewnić łączność pomiędzy stanowiskami operatorów i służbami działającymi na drogach.

Systemy meteo, kontroli środowiska.

Przekazywanie, co określony czas lub w przypadku przekroczenia określonych progów, informacji do centrów – pojedyncze **b/s** – głównie w górę sieci.

Systemy alarmowe

Systemy alarmowe mają bardzo małe wymagania na pasmo (bez wideo). Systemy alarmowe przekazują do centrów informacje o wystąpieniu alarmu. Są to bardzo niewielkie przepływy danych, rzędu pojedynczych **b/s**

Systemy sterowania (scada).

Są to systemy związane ze sterowaniem różnymi procesami, np. nadzorowaniem energetyki. Oczekiwane przepływy to kilkanaście **kb/s**.

Systemy ważenia i preselekcji

Służą do ważenia w ruchu przejeżdżających pojazdów w celach statystycznych lub/i wykrywania pojazdów przeciążonych. Informacje z o wadze pojazdów dla celów statystycznych generują niewielkie przepływności, natomiast w przypadku wykrywania pojazdów przeciążonych system musi umożliwiać dokumentowanie przekroczeń, co jest związane z koniecznością stosowania kamer pozwalających na rejestrację pojazdów. Przesyłanie zdjęć lub krótkich sekwencji filmowych wymaga dużych przepływności rzędu kilkuset **kb/s**.

Systemy rejestracji wykroczeń

Są to systemy wykrywające i rejestrujące różnego rodzaju wykroczenia drogowe (np. przejazd na czerwonym świetle, jazda pod prąd, przekroczenie prędkości, jazda bez uprawnień lub uiszczenia opłat) i muszą umożliwiać dokumentowanie przekroczeń, co jest związane z koniecznością stosowania kamer pozwalających na rejestrację pojazdów. Przesyłanie zdjęć lub krótkich sekwencji filmowych wymaga dużych przepływności rzędu kilkuset **kb/s**.

Systemy poboru opłat

Są to systemy rejestrujące pobór opłat za przejazd. W skład takiego systemu wchodzi punkty poboru opłat oraz systemy wykrywające jazdę bez uprawnień lub uiszczenia opłat. Te drugie muszą umożliwiać dokumentowanie przekroczeń, co jest związane z koniecznością stosowania kamer pozwalających na rejestrację pojazdów. Przesyłanie zdjęć lub krótkich sekwencji filmowych wymaga dużych przepływności rzędu kilkuset **kb/s**. W punktach ręcznego poboru opłat zawsze stosuje się monitorowanie wizyjne.

Systemy monitoringu wideo

Są to systemy pozwalające na monitorowanie infrastruktury drogowej. W zależności od postawionych przed systemem wideo zadań, różne są sposoby i możliwości techniczne realizacji takiego systemu.

Parametry kamer, obiektywów, sterowania, systemów rejestracji, systemów wyświetlania obrazu muszą być dobrane do konkretnych potrzeb i zadań, jakie ma realizować monitoring:

- Śledzenie pojazdów
- Śledzenie ludzi
- Rozpoznawanie twarzy
- Klasyfikacja pojazdów
- Odczyt tablic rejestracyjnych
- Obserwacja strumienia pojazdów
- Obserwacja wejść, bram, tuneli itp.

Przepływności strumieni wideo zależą od realizowanej funkcji. Dla obserwacji strumienia pojazdów wystarczą pojedyncze klatki na minutę. Do śledzenia ludzi czy pojazdów na żywo wymagana jest jakość obrazu co najmniej jak dla telewizji. Jeżeli obraz ma być obserwowany na żywo to wymaga przesyłania większej liczby klatek na sekundę. Zbyt mała liczba klatek na sekundę powoduje szybkie męczenie się obserwatora. Jeżeli kamera ma nadążać za ruchem przemieszczających się obiektów, to powinna reagować na zdarzenia odpowiednio szybko. Wymaga to przepływności od kamery w kierunku centrum rzędu kilku **Mb/s**.

Jak widać z powyższej analizy największe wymagania na przepływność kanałów łączności związane jest ze stosowaniem technik wideo.

1.3.1 Wpływ sieci dróg na rozwiązania systemów łączności dla ITS

Sieci łączności dla systemów ITS różnią się od typowych sieci telekomunikacyjnych charakterystyką przepływu danych jak i lokalizacjami urządzeń końcowych. W typowych sieciach telekomunikacyjnych większy przepływ danych następuje od centrów do urządzeń końcowych, w sieciach ITS odwrotnie. W sieciach łączności dla systemów ITS większość urządzeń końcowych instalowana jest poza budynkami. Ponadto cechą charakterystyczną sieci ITS jest duże rozproszenie w terenie urządzeń końcowych oraz stosunkowo duże odległości pomiędzy punktami dostępu do sieci. Potrzeba jest stosowania urządzeń sieciowych o małej liczbie portów i umożliwiających realizację tanich połączeń na stosunkowo duże odległości. Wskazane jest stosowanie urządzeń nie wymagających regeneracji przysyłanych sygnałów poza lokalizacjami urządzeń końcowych.

Duże są wymagania na pasmo potrzebne do przekazywania obrazów z kamer do centrów, gdzie te obrazy są wykorzystywane, bądź archiwizowane, co stawia określone wymagania na sieć łączności. W zasadzie nie można do tego typu transmisji wykorzystywać powszechnie

stosowanych technologii agregacji strumieni danych w sieciach telekomunikacyjnych – takich jak ADSL (zbyt małe dostępne pasmo w górę sieci). Również niektóre technologie radiowe mają ograniczone zastosowania, szczególnie поблизу skupisk miejskich, terenie trudnym takim jak góry. Także topologia sieci jest inna. Większość punktów dostępowych musi być zlokalizowana w pobliżu urządzeń wchodzących w skład podsystemów ITS np. szafkach sterowników świateł, przy tablicach zmiennej treści, stacjach meteo, skrzyżowaniach itp. Przy czym często w tych samych lokalizacjach przewiduje się instalowanie kamer.

Ze względu na niezawodność komunikacji oraz dostępne pasmo preferowanym rodzajem sieci będą sieci światłowodowe, szczególnie w przypadku budowy nowych systemów. Koszty budowy nowej sieci kablowej praktycznie są podobne dla sieci kabli miedzianych i dla światłowodów. Preferowane powinny być światłowody jednodomowe ze względu duży zasięg bez konieczności aktywnej regeneracji sygnałów oraz bardzo duże dostępne pasmo. Ponadto można w razie potrzeby zwielokrotnić przepływy przez stosowanie różnych częstotliwości (barw) światła. Jest to szczególnie istotne w warunkach gęstej zabudowy co umożliwi w przyszłości rozwój bez konieczności dokładania nowych włókien.

Dodatkowo wiele urządzeń zainstalowanych w terenie (kamery bardzo często umieszczone są wysoko) narażonych jest na wyładowania atmosferyczne – światłowody stanowią naturalną izolację galwaniczną pomiędzy węzłami sieci i urządzeniami. Również cenną zaletą jest brak miedzi – nie będą tak często kradzione.

Bardzo ważnym aspektem, który powinien być brany pod uwagę jest działanie kanałów transmisji w sytuacjach kryzysowych. Np. trzeba wziąć pod uwagę, że w przypadku pewnych zdarzeń drogowych wszyscy uczestnicy sięgają po telefony komórkowe, co automatycznie może przeciążyć sieć – więc aplikacje bazujące na sieci publicznej GSM/GPRS mogą źle działać, a w tych samych warunkach sieć publiczna CDMA będzie dostępna ze względu na małą popularność tych urządzeń w kraju. Natomiast dedykowana sieć radiowa trunkingowa będzie działać niezależnie od stanu sieci publicznej.

Generalnie w zakresie zainteresowania znajdują się następujące klasy dróg publicznych:

- autostrady płatne
- autostrady
- drogi krajowe
- drogi powiatowe

W przypadku autostrad płatnych istnieje narzucony standard wyposażenia dróg w systemy techniczne, w tym w kable dla systemów łączności. Dla autostrad płatnych standardowo wymagana jest obecnie budowa światłowodów wzdłuż autostrady do wykorzystania w systemach ITS.

W przypadku budowy nowych autostrad wymagana jest budowa co najmniej kanalizacji kablowej. Samo wyposażenie w system łączności (w tym światłowody) jest często przesuwane z fazy budowy autostrady do fazy dostosowania autostrady do wymagań dla autostrad płatnych. Na drogach krajowych (na odcinkach nowo budowanych oraz modernizowanych) wymagana jest budowa kanalizacji kablowej.

Tak więc takie uwarunkowania trzeba brać pod uwagę przy projektowaniu systemów łączności dla podsystemów ITS. Dla większości dróg krajowych i powiatowych oraz na części odcinków autostrad nie ma infrastruktury pozwalającej na tworzenie dedykowanego systemu łączności. Dlatego też w takich miejscach nie ma innego wyjścia jak wykorzystywanie zasobów dzierzawionych od operatorów telekomunikacyjnych lub usług

oferowanych przez tych operatorów. Również należy brać pod uwagę uwarunkowania związane z kosztami. Tam gdzie jest duże nagromadzenie systemów ITS (np. na autostradach – wymagane są słupki z telefonami alarmowymi w odległości nie większej niż co 2 km, na obwodnicach miast, w terenie gęsto zabudowanym z dużym nasyceniem ruchu) wskazane jest budowa dedykowanego systemu łączności. Tam gdzie instalowane są pojedyncze urządzenia końcowe (np. drogi krajowe i powiatowe – pobór opłat) raczej należy korzystać z usług operatorów telekomunikacyjnych i bazować na kanałach łączności dostarczanych przez nich.

Ze względu na zmianę przepisów dotyczących budowy dróg (konieczność jednoczesnej budowy kanalizacji kablowej) należałoby wypracować model współpracy z operatorami sieci telekomunikacyjnej. Największym problemem dla operatorów telekomunikacyjnych przy budowie nowych linii kablowych jest tzw. prawo drogi, czyli uzyskanie pozwoleń na budowę kanalizacji kablowej od właścicieli gruntów. Dlatego też można w ramach porozumień udostępniać nowo budowaną kanalizację kablową za światłowody. Takie postępowanie pozwoliłoby bardzo obniżyć koszty budowy sieci łączności dla systemów ITS i zwiększyć ich funkcjonalność.

W związku z powyższymi uwarunkowaniami należy opracować wymagania docelowe dla sieci łączności, które będą stosowane jako wymagania dla autostrad. Dla pozostałych dróg, nie wyposażonych w światłowody, można jedynie opracować wskazówki jak realizować kanały łączności dla poszczególnych podsystemów z wykorzystaniem dostępnych środków i w oparciu o sieci operatorów telekomunikacyjnych. Dodatkowo należy wziąć pod uwagę specjalne odcinki dróg (poza autostradami), dla których wymagane są już obecnie dość zaawansowane systemy ITS – dotyczy to np. tuneli.

1.4 Niezawodność

Podsystem komunikacyjny musi zostać wykonany przy założeniu zapewnienia redundancji systemu. Ma to na celu podniesienie niezawodności pracy Systemu ITS w sytuacji awarii jego podsystemów lub poszczególnych elementów. Wymagane jest takie zaplanowanie połączeń, aby awaria jednego węzła łączności lub urządzenia komunikacyjnego powodowała co najwyżej przerwę w przesyłaniu danych z tego węzła, ale nie stanowiła zagrożenia dla integralności całego Systemu ITS.

Przy projektowaniu przebiegów światłowodów, w celu ograniczenia ilości niezbędnych do budowy podsystemu komunikacyjnego dla ITS włókien, należy stosować topologię budowy sieci w postaci pierścieni. W sieci szkieletowej powinny to być pierścienie (ringi) optyczne zapewniające połączenia alternatywne zarówno w przypadku pojedynczej awarii kabla (różne drogi kabli w pierścieniu), włókna jak i urządzenia aktywnego. W uzasadnionych przypadkach dopuszcza się topologię płaskiego ringu (ten sam kabel inne włókna) zapewniającą redundancję w przypadku awarii włókna i urządzeń przełączających.

Połączenia pomiędzy pierścieniami sieci dostępowej a sieci szkieletowej powinny być realizowane jako połączenia redundantne zapewniające redundancję w przypadku awarii pojedynczego urządzenia przełączającego w sieci oraz uszkodzenia pojedynczego włókna. Sieć łączności powinna posiadać możliwość łatwej rozbudowy o kolejne przyłącza i węzły sieci.

1.5 Bezpieczeństwo sieci

Sieć łączności powinna:

- umożliwiać przypisywanie i wykonywanie różnych priorytetów dla różnego rodzaju ruchu (Quality of Service),

- zapewniać separację podsystemów ITS od siebie przy jednoczesnym wspólnym wykorzystaniu zasobów sieci
- posiadać nadmiarowe włókna światłowodowe do wykorzystania w przyszłych zastosowaniach (minimum 50% włókien w przewodzie) lub do przełączenia w przypadku awarii włókna
- zapewniać szybką rekonfigurację sieci w przypadku wystąpienia awarii możliwej do usunięcia przez rekonfigurację (zalecany czas rekonfiguracji: < 100ms),

Wykorzystywane do budowy sieci rozwiązania i protokoły powinny być publicznie dostępne i otwarte.

Połączenie oparte na protokole TCP/IP w sieciach publicznych lub w sieciach, które nie są w pełni kontrolowane przez użytkownika, stwarza poważne ryzyko. Sytuacja taka ma miejsce przede wszystkim wtedy gdy partnerzy komunikacyjni są połączeni ze sobą za pośrednictwem publicznego Internetu, jak w przypadku GPRS.

Po połączeniu sieci lub systemu komputerowego z zewnętrzną siecią pojawiają się **zagrożenia** w związku z:

- możliwością niekontrolowanego korzystania z wszelkich wewnątrzsieciowych usług i zasobów przez osoby trzecie,
- możliwością niekontrolowanego korzystania przez osoby trzecie z usług, które w zasadzie powinny być udostępniane wyłącznie wybranym zewnętrznym partnerom,
- możliwością manipulowania przepływem danych między podsystemami, partnerami przez osoby trzecie
- oraz możliwością przechwytywania przez osoby trzecie poufnych danych (np. haseł itp.) wymienianych między urządzeniami wchodzącymi w skład podsystemów ITS jak i pomiędzy systemem ITS i partnerami wykorzystującymi dane udostępniane przez podsystemy ITS.

W związku z zagrożeniami wymienionymi powyżej należy podjąć **odpowiednie środki bezpieczeństwa**:

- tworzenie bezpiecznych kanałów transmisji,
- kontrola pobieranych i przekazywanych danych oraz ograniczanie dostępu tylko do wskazanych i niezbędnych danych dla partnerów,
- wzajemne uwierzytelnianie partnerów,
- zabezpieczanie integralności danych,
- zabezpieczanie poufności danych,

Ponieważ wymienione powyżej środki bezpieczeństwa muszą być stosowane nie tylko w podsystemie łączności (warstwa transportowa) ale i w warstwie aplikacji dlatego też w niniejszym dokumencie zostaną zasygnalizowane tylko pewne aspekty tego problemu mające wpływ na architekturę systemu łączności (wymagane dodatkowe urządzenia służące do zapewnienia bezpieczeństwa przepływu danych).

Przepływ danych między sieciami a systemami komputerowymi można kontrolować lub ograniczać stosując firewall na złączach pomiędzy pojedynczymi sieciami i podsieciami lub systemami komputerowymi. Programy firewall można tak skonfigurować, aby osoby trzecie nie miały dostępu do wewnątrzsieciowych usług i zasobów, a partnerzy zewnętrzni posiadali dostęp tylko i wyłącznie do przewidzianych dla nich usług.

W celu uwierzytelnienia partnerów oraz zabezpieczania integralności oraz poufności danych należy użyć zaawansowanych zabezpieczeń. W tym celu można zastosować następujące technologie:

- IPSec / Virtual Private Network (VPN)
- SecureShell (ssh)
- Secure Socket Layer (SSL) / Transport Layer Security

Wymienione technologie powinny być stosowane przy przesyłaniu danych przez sieci publiczne lub przez sieci nie będące pod kontrolą GDDKiA. Technologie te ingerują na różnych warstwach w przepływ danych w podobny sposób i mogą przy odpowiedniej konfiguracji zagwarantować wzajemne uwierzytelnienie oraz integralność i poufność danych.

IPSec / Virtual Private Network (VPN)

Zbiór protokołów IPSec umożliwia połączenie w sposób bezpieczny dwóch fizycznie nie połączonych sieci lub sieci i systemu komputerowego przy wykorzystaniu sieci publicznej i bez wpływu na działanie aplikacji pracujących w tych sieciach. Na ogół obie strony używają routerów VPN, które po wzajemnym uwierzytelnieniu kodują cały przepływ danych pomiędzy tymi dwoma sieciami. Poza tym są dostępne również zwykłe rozwiązania programowe, które są często używane przez klienta. Dotyczy to przede wszystkim łączenia pojedynczych systemów komputerowych z siecią.

Ponieważ IPSec funkcjonuje w warstwie sieciowej, przez co umożliwia przepływ danych pomiędzy połączonymi sieciami, najczęściej instaluje się program firewall w celu ograniczenia i kontroli przepływu danych pomiędzy tymi sieciami lub systemami komputerowymi.

Należy pamiętać, że środki bezpieczeństwa udostępnione przez IPSec obejmują wyłącznie przepływ danych pomiędzy dwiema połączonymi sieciami przez kanał utworzony w sieci publicznej, a przepływ danych w obrębie sieci połączonych kanałem nie podlega ochronie.

Sama konfiguracja IPSec wiąże się z dużymi nakładami i sprawia problemy przede wszystkim, gdy używane są produkty różnych producentów oraz podczas korzystania z Internetu poprzez Network Address Translation (NAT).

SecureShell (SSH)

SecureShell umożliwia bezpieczne, uwierzytelnione i zakodowane połączenie pomiędzy dwoma komputerami poprzez niepewną sieć. Podstawowy zakres zastosowania obejmuje łączenie się ze zdalnymi komputerami poprzez sieć. Za pomocą SSH można również bezpiecznie tunelować dowolne połączenia TCP/IP.

Dzięki zastosowaniu SSH można bez dodatkowych modyfikacji używać programów komunikacyjnych bazujących na TCP/IP. SSH łączy porty TCP systemów w sposób dostatecznie bezpieczny.

Podczas stosowania SecureShell należy pamiętać, że zgodnie z ustawieniami domyślnymi możliwe jest uwierzytelnienie klienta w oparciu o hasła, które należy poprzez odpowiednią konfigurację serwera wyłączyć, aby zapobiec atakom Bruteforce i Directory. Zamiast tego należy poprzez odpowiednią konfigurację wymusić uwierzytelnienie kluczem publicznym (klient-serwer).

Secure Socket Layer (SSL) / Transport Layer

SSL/TransportLayer zabezpiecza przepływ danych pomiędzy dwiema aplikacjami poprzez sieci publiczne. SSL/TransportLayer wspomaga wzajemne uwierzytelnienie oparte na certyfikatach i gwarantuje integralność oraz poufność przepływu danych w wyniku kodowania.

Zamiast normalnego pasywnego lub aktywnego zestawiania połączeń TCP stosowanego przez aplikacje przy wykorzystaniu SSL/Transport Layer realizowane jest zestawianie połączeń TCP przy zastosowaniu odpowiednich bibliotek metod wykorzystując implementację protokołu SSL/TransportLayer. Biblioteka SSL/TransportLayer jest łączona jako warstwa pośrednia pomiędzy TCP a warstwą aplikacji (np. TCPoIP) i w sposób niezależny i bezpieczny koduje bądź odkodowuje całkowity przepływ danych.

SSL/TransportLayer jest powszechnie stosowany ze względu na zastosowanie w serwerach i przeglądarkach sieciowych (https) oraz minimalną zależność od systemów sprzętowych i operacyjnych. Należy pamiętać, że implementacje protokołu SSL/TransportLayer zgodnie z ustawieniami domyślnymi wymagają uwierzytelnienia wyłącznie po stronie serwera. Z tego względu serwer wymusza uwierzytelnienie przez klienta poprzez ustawienie odpowiedniej opcji. Podczas zabezpieczania na ogół niezabezpieczonych protokołów komunikacyjnych na publicznych ścieżkach transmisji SSL/TransportLayer wyróżnia przede wszystkim łatwa konfiguracja oraz minimalne uzależnienie od sprzętu komputerowego i systemów operacyjnych.

2. Architektura Systemu ITS

2.1 Elementy będące przedmiotem opracowania

Poniższy diagram został zaczerpnięty z dokumentu „The NTCIP Guide” NTCIP 9001 version 4 z lipca 2009

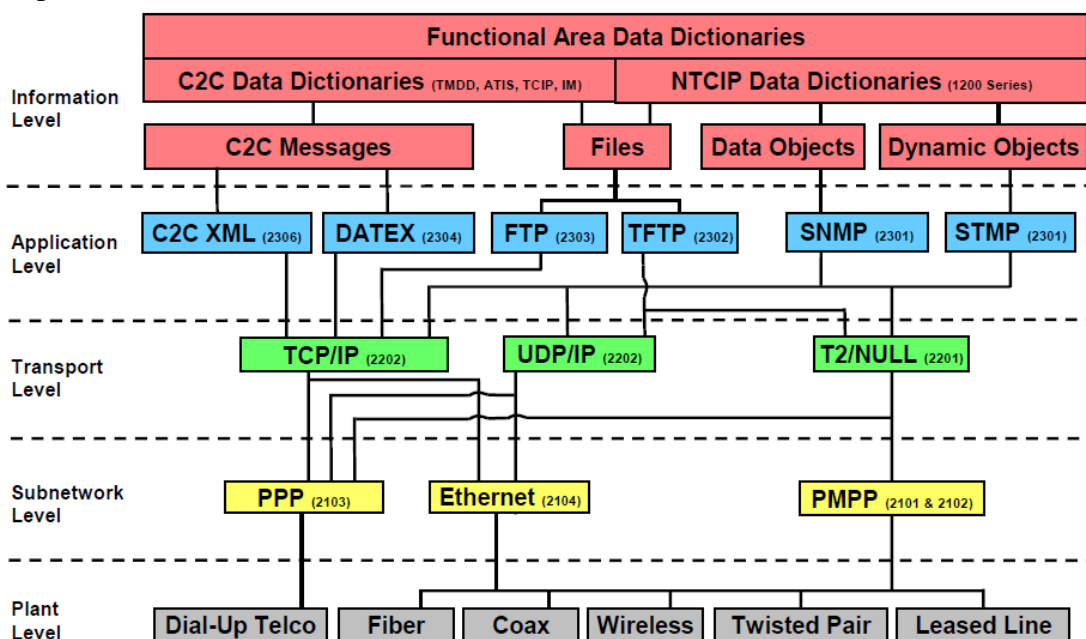
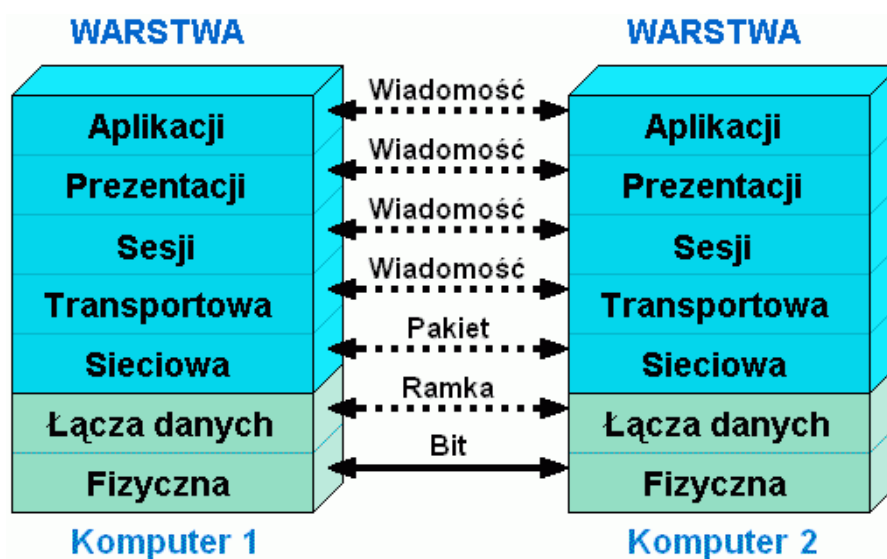


Figure 4 NTCIP Framework

Rys. 2 Przykładowy diagram przepływu informacji w systemach ITS.

Jak widać z diagramu przepływ informacji w systemach ITS został podzielony w sposób zbliżony do modelu OSI.



Rys. 3 Model OSI sieci komputerowej

Subnetworks Level (warstwa podsieci) w modelu NTCIP odpowiada warstwie fizycznej oraz warstwie łącza danych w modelu OSI. Natomiast warstwa Transport Level (warstwa transportowa) w modelu NTCIP pokrywa się z warstwami sieciową oraz transportową modelu OSI. Dlatego w wymaganiach na kanały łączności powinny znaleźć się wymagania w zakresie warstw fizycznej, łącza danych, sieciowej oraz transportowej.

Dalsza część dokumentu skupia się na warstwach związanych ściśle z siecią oraz kanałami łączności tzn. warstwie fizycznej, łącza danych, sieciowej i transportowej. Dlatego należy wszystkie urządzenia systemów ITS podzielić na dwie generalne klasy:

- urządzenia ITS
- urządzenia łączności

Należy zdefiniować interfejsy pomiędzy urządzeniami łączności (siecią łączności) a pozostałymi urządzeniami ITS. Należy wybrać takie interfejsy, które są dobrze zdefiniowane, popularne oraz tanie. Pozwoli to na stosowanie identycznych interfejsów w urządzeniach ITS, niezależnie od dostępnej sieci komunikacyjnej i stosowanych w niej urządzeń. Standaryzacja interfejsów umożliwi dołączanie dowolnych podsystemów do urządzeń sieciowych w sieciach łączności dedykowanych dla systemów ITS oraz ułatwi wybór i zmianę operatorów telekomunikacyjnych w przypadku korzystania z ich usług.

2.2 Interfejsy do dołączania urządzeń ITS do systemu łączności

Interfejsy do dołączania urządzeń ITS do sieci łączności powinny posiadać następujące cechy:

- powinny być ogólnie dostępne i popularne,
- powinny umożliwiać niezależność urządzeń ITS od zastosowanego systemu łączności tzn. zmiana kanałów łączności, dostawcy rozwiązań sieciowych, zmiana technologii sieciowej powinny wyłącznie mieć wpływ na dostępne pasmo i nie powodować istotnych zmian po stronie urządzeń ITS

- urządzenia po stronie sieciowej powinny być urządzeniami standardowymi, łatwo dostępnymi, komercyjnymi, „z półki” - co się przekłada na koszty jednostkowe i oraz dostępność wyrobów wielu producentów

Dlatego wydaje się najlepszym wybór interfejsów Ethernetowych jako podstawowych interfejsów do sieci łączności. Do przesyłania danych pomiędzy urządzeniami podsystemów ITS najbardziej preferowaną technologią obecnie jest także Ethernet.

Należy zastosować transmisję opartą na technologii Ethernet i protokołach TCP/IP oraz UDP. Zastosowanie Ethernetu pozwoli na uniwersalność interfejsów do systemu komunikacyjnego oraz zminimalizowanie liczby stosowanych typów interfejsów

Wszystkie urządzenia i aplikacje stosowane w sterowaniu ruchem mogą się komunikować poprzez sieć Ethernet wykorzystując bezpośrednio wbudowane interfejsy, bądź przez proste adaptery. Ethernet ma zdefiniowaną bardzo niewielką liczbę interfejsów elektrycznych i światłowodowych. Taki sam interfejs fizyczny jest dostępny dla różnych przepływow (10/100/1000BaseT) i różnych urządzeń końcowych. W urządzeniach dostępne są również tanie interfejsy światłowodowe 100Mb i 1Gb. Dostępne są także interfejsy 10Gb. W porównaniu do innych technologii Ethernet jest bardzo powszechny i tani. Obecnie urządzenia sieciowe na bazie Ethernetu umożliwiają zarządzanie QoS, pozwalają na zdalne zarządzanie urządzeniami, umożliwiają separację i tworzenie wirtualnych podsieci. Ethernet dostępny jest także z wykorzystaniem sieci mobilnych (komórkowych).

Dla niektórych urządzeń, tam gdzie nie będzie dostępna sieć stacjonarna można stosować inne interfejsy –np. transmisję szeregową

2.3 Zasady doboru kanałów łączności do potrzeb podsystemów ITS

Generalnie preferowaną i docelową siecią dla systemów ITS powinna być sieć TCP/IP bazująca na światłowodach lub w ograniczonym zakresie na innych dostępnych technologiach. Proponując konkretne rozwiązanie należy dążyć do wyważonego rozwiązania zapewniającego równowagę pomiędzy oczekiwaną niezawodnością a kosztami rozwiązania. Dobór zastosowanej technologii powinien wynikać również z potrzeb wynikających z konkretnego podsystemu ITS, zadań, które ma wykonywać oraz możliwości realizacyjnych i technicznych. O ile w przypadku budowy autostrad płatnych wymaga się aby w procesie ich dostosowywania wykonać sieć światłowodową, to w przypadku tworzenia punktów wyniesionych podsystemów ITS przy innych kategoriach dróg może się to okazać niemożliwe lub ekonomicznie nieuzasadnione. W takich przypadkach najlepiej wykorzystać możliwości realizacji tych kanałów za pomocą sieci i usług oferowanych przez operatorów telekomunikacyjnych. Ponieważ najczęściej będziemy mieli do czynienia z terenami o niskim nasyceniu infrastrukturą telekomunikacyjną, trzeba będzie korzystać z sieci komórkowych. Należy doprowadzić światłowody do szaf na skrzyżowaniach lub miejsc zainstalowania innych elementów podsystemów ITS, gdzie powinny być umieszczone Ethernetowe switchy przemysłowe, służące do agregacji ruchu generowanego przez różne urządzenia należące do różnych podsystemów, zainstalowanych w pobliżu.

3. Wymagania szczegółowe

3.1 Sieć łączności dedykowana

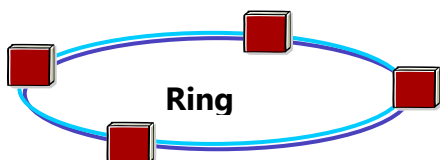
Dedykowana sieć łączności powinna zapewnić realizację m.in. następujących usług:

- komunikacja z wyposażeniem przydrożnym (sterowniki, różnego rodzaju elementy sensoryczne),
- komunikacja z infrastrukturą systemu sterowania ruchem oraz służbami wspomagającymi (bazy danych, centra kontroli, systemy monitorowania, różnego rodzaju służby),
- dostęp do informacji
- łączność głosową

Podsystem komunikacyjny musi zostać zrealizowany w sposób zapewniający niezbędną łączność o odpowiednich parametrach pomiędzy elementami systemu ITS przy założeniu, że rozmieszczenie elementów Systemu ITS ma charakter rozproszony, a infrastruktura i zasoby poszczególnych podsystemów mogą być współdzielone z innymi podsystemami. Sieć stacjonarna światłowodowa powinna być stosowana jako rozwiązanie docelowe.

3.1.1 Topologia sieci

Struktura sieci powinna uwzględniać cykliczne samo-testowanie funkcjonowania. W zależności od lokalnych możliwości i przebiegu światłowodów można wykorzystywać następujące topologie połączeń: Ring (pierścień), Flat Ring (płaski pierścień), Bus (szyna, linia) lub kombinacje tych topologii.



Rys.4 Ring (pierścień) – redundancja w przypadku uszkodzeń kabla, włókna i urządzeń



Rys. 5 Flat ring (płaski pierścień)– redundancja w przypadku uszkodzeń włókna i urządzeń

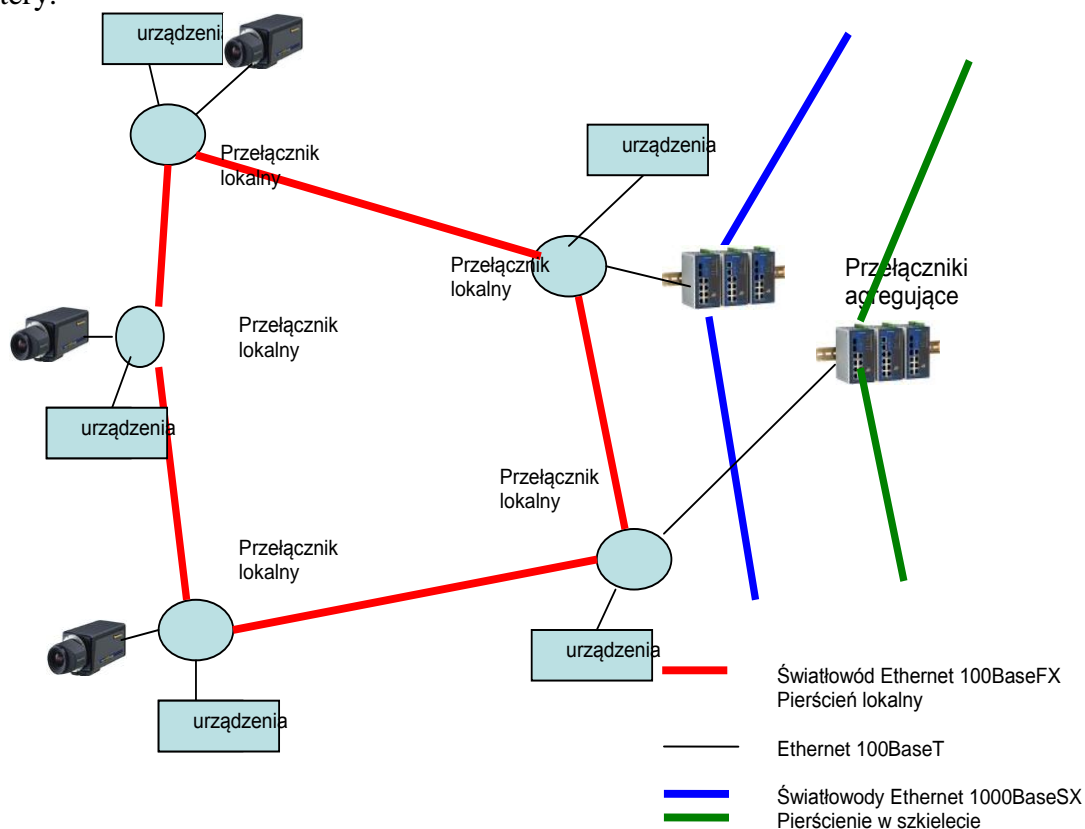


Rys. 6 Bus (szyna, linia) – brak redundancji,

Proponując konkretne rozwiązanie należy dążyć do wyważonego rozwiązania zapewniającego równowagę pomiędzy oczekiwaną niezawodnością a kosztami rozwiązania. Najwyższe wymagania niezawodnościowe stawia się szkieletowi sieci, niższe dopuszczalne są w peryferyjnych częściach sieci

Zalecana jest budowa sieci warstwowych. Pozwala to na zapewnienie odpowiedniej niezawodności sieci przy minimalnym zapotrzebowaniu na liczbę włókien światłowodowych.

W każdej warstwie sieci można wtedy stosować odpowiednio dobrane do potrzeb urządzenia – różniące się liczbą portów dostępnych w danym węźle, przepływnościami w górę sieci, obsługą protokołów (od prostszych urządzeń typu przełączniki po bardzo zaawansowane routery).



Rys. 7 Przykład sieci warstwowej.

Na rysunku 7 przedstawiony został przykład takiej sieci. Typowo mogą to być warstwy sieci umownie nazywane:

- dostępową
- agregacyjną
- szkieletową

Zakłada się, że podsystem komunikacyjny będzie budowany jako system co najmniej dwuwarstwowy:

- sieć szkieletowa
- sieć dostępową

Warstwa dostępową służy do realizacji połączeń pomiędzy obiektami leżącymi w niedalekiej odległości od siebie. Przykładem takiego segmentu sieci może być realizacja połączeń do urządzeń na autostradzie leżących w pobliżu węzła autostradowego takich jak znaki zmiennej treści, urządzenia pomiaru ruchu, kamery itp. W każdym punkcie jest zainstalowany przełącznik Ethernetowy pracujący w płaskim pierścieniu. Z pętli do warstwy wyższej sieci są wyprowadzone co najmniej dwa wyjścia z różnych przełączników lokalnych (zabezpiecza to przed odcięciem połączeń w przypadku awarii pojedynczego przełącznika – zawsze jest droga obejściowa). Warstwa agregacyjna jest zbudowana również w architekturze pierścienia łączącego ze sobą pewną liczbę węzłów na odcinku autostrady. Warstwa szkieletowa łączy ze sobą wiele pierścieni warstw niższych.

Urządzenia lokalne będą mogły łączyć się z urządzeniami centralnymi i z urządzeniami centrum zarządzania poprzez sieć WAN drogą wybraną automatycznie przez odpowiednie protokoły wyboru ścieżki. W przypadku uszkodzenia któregośkolwiek urządzenia lub interfejsu w węźle sieci WAN nastąpi przełączenie i wybór nowej ścieżki dla pakietów.

W celu ułatwienia eksploatacji, a także diagnostyki systemów należy wirtualnie separować od siebie ruch generowany poprzez urządzenia wchodzące w skład różnych podsystemów ITS. Należy stosować przełączniki pozwalające na tworzenie VLAN (wirtualnych LAN), separujących ruch pomiędzy nimi, mechanizmy uprzywilejowania pakietów, mechanizmy kontroli przepływu - co umożliwia planowanie ruchu i jego kontrolę. Podział na wirtualne sieci pozwala także, w przypadkach awarii, na ustalenie priorytetu przesyłanych danych przez drogi obejściowe (których przepływność może być mniejsza).

Jako preferowane topologie sieci należy przyjąć:

- Liniową
- Pierścień
- Drzewo

3.1.2 Metodyka tworzenia dróg obejściowych

System powinien umożliwiać realizację połączeń z określonym poziomem zabezpieczenia poprawności i pewności działania. Jedną z metod jest planowanie dróg obejściowych. W każdym przypadku powinno dążyć się do realizacji sieci redundantnej. Jednak koszty zapewnienia pełnej redundancji mogą być znaczące. Wobec czego wymagana jest analiza potrzeb i kosztów dla każdego z podsystemów ITS. Wtedy, gdy zbierane informacje mają niewielki wpływ na bieżące działanie systemu lub nie powodują zagrożenia życia można przyjąć metodę lokalnego backupowania danych i przechowywania ich do czasu przywrócenia łączności. Tam gdzie działają systemy związane z bezpieczeństwem należy dążyć do takiej konfiguracji sieci, aby była ona odporna na awarię pojedynczych połączeń, pojedynczych interfejsów lub urządzeń. Taka awaria nie powoduje odcięcia innych urządzeń lub węzłów. Dlatego też preferowana jest praca sieci łączności w topologii pierścieni.

Zapewnienie pracy w postaci pełnych pierścieni realizujących połączenia fizycznie różnymi drogami może być zbyt kosztowne do realizacji. Patrząc na mapę dróg w Polsce i topologię autostrad można przewidywać, że kolejne odcinki będą uzupełniały istniejącą infrastrukturę. Dlatego przy planowaniu połączeń backupowych należy uwzględnić przewidywany rozwój sieci.

Biorąc pod uwagę to, że typowa topologia wydzielonych sieci łączności ITS będzie pokrywała się na początku z przebiegiem autostrad to stosowana będzie praktycznie topologia pierścienia płaskiego, nie odporna na przecięcia kabla. Dlatego też można na końcach obsługiwanych przez taką sieć odcinków autostrad wykonywać dodatkowe połączenia do publicznej sieci transmisji danych czyli Internetu. Połączenia takie mogą służyć jako dodatkowa, niezależna droga przekazywania kluczowych danych w przypadku awarii. Generalnie należy w każdym przypadku przeprowadzać analizę skutków awarii i przygotować działania do minimalizowania wpływu awarii na pracę systemu. Drogi obejściowe nie muszą zapewniać pełnej przepływności identycznej jak w sprawnym systemie – powinno to wynikać z ważności przekazywanych informacji i analizy kosztów. Najbardziej pożądane są automatyczne przełączania się systemu na drogi obejściowe. To wymaga zastosowania odpowiednich urządzeń, narzędzi i protokołów.

Zastosowanie urządzeń sieciowych przygotowanych do pracy w topologii pierścienia wraz z protokołami kontroli pozwala na przełączenie się na drogę zapasową w czasie poniżej

50 lub 100 ms w zależności od zastosowanego protokołu. Powyżej tego znajdują się protokoły routingu umożliwiające znalezienie nowej drogi w sieci w ciągu kilku sekund.

Bardzo szybko działają urządzenia i protokoły MPLS (porównywalne z przełączaniem pierścieni). Pozwalają one na zaplanowanie przepływów w sieci bezpołączeniowej (transmisji danych) i kierowanie danych określonymi drogami przez określone węzły (tworzenie połączeń w sieci bezpołączeniowej). Te protokoły pozwalają, w przypadku wykrycia awarii na ścieżce połączeniowej, na przekierowanie na ścieżkę zapasową, również z uwzględnieniem priorytetów, w tym różnych dla różnych aplikacji, a także na wybór różnych dróg w zależności od priorytetu.

Zastosowanie urządzeń przełączających w warstwach wyższych modelu OSI umożliwia różnicowanie ruchu w ścieżkach zapasowych – pozwala na kierowanie na ścieżki zapasowe najbardziej potrzebnych informacji i ich uprzywilejowanie – pozostałe informacje mogą mieć niższy priorytet i mogą być przekazywane w razie możliwości.

W przypadku połączeń dzierżawionych realizacja dróg obejściowych może być przerzucona na operatora sieci – powinno się określić odpowiednie SLA (Service Level Agreement) w umowach z operatorem.

3.1.3 Kanalizacja kablowa

Ponieważ zmiany prawa wprowadziły konieczność budowy kanalizacji kablowej wzdłuż nowych i wzdłuż modernizowanych dróg bardzo ważnym stają się odpowiednie założenia do projektów dróg. Budowa kanalizacji kablowej wzdłuż dróg powinna uwzględniać przyszłe systemy ITS i przewidywaną lokalizację urządzeń. Należy wobec tego przewidywać w pobliżu skrzyżowań dróg, w pobliżu przejazdów kolejowych, mostów i dużych wiaduktów studnie telekomunikacyjne, umożliwiające wyprowadzenie światłowodów. Jeśli nawet w bliskiej perspektywie nie będą one wyprowadzone, to powinno się w tych miejscach pozostawić zapas kabla, umożliwiający łatwe wykonanie wcinki i wyprowadzenia włókien w przyszłości. Również w projektach kanalizacji kablowej powinno się uwzględnić odpowiednio rozszerzanie kanalizacji kablowej o otwory do doprowadzenia zasilania do punktów przyszłych instalacji systemów ITS z miejsc, gdzie dostępne są przyłącza energetyczne.

Budując kanalizację kablową można wykorzystać posiadane prawo drogi do zaoferowania innym podmiotom na rynku możliwości współfinansowania inwestycji za udostępnienie otworów kanalizacyjnych. To może generalnie obniżyć koszty inwestycji ponoszone przez GDDKiA. Również w ramach współpracy z operatorami telekomunikacyjnymi można zawiązać współpracę – udostępnianie drogi kablowej w zamian z utrzymanie światłowodów.

3.1.4 Światłowody

Wymogiem oferty dla sieci łączy optycznych powinna być specyfikacja wskaźników niezawodnościowych oraz sposobu wyznaczania takich współczynników dla całej struktury sieci

Ze względu na to, że typowa sieć połączeń dla systemów ITS jest siecią rozległą należy stosować światłowody jednodomowe. Światłowody wielodomowe mają niewielki zasięg i są stosowane wyłącznie do połączeń lokalnych. Co prawda można osiągnąć pewne oszczędności wykorzystując światłowody wielodomowe (tańsze interfejsy) ale w dalszej perspektywie ograniczają one przepustowość (brak możliwości zwielokrotnienia sygnałów z wykorzystaniem wielu częstotliwości światła). Również nie bagatelnym problemem jest

konieczność utrzymywania szerokiej bazy części zapasowych. Stosując tylko światłowody jednomodowe ograniczamy liczbę typów wkładek światłowodowych do urządzeń aktywnych.

Światłowody należy doprowadzić do szaf na skrzyżowaniach lub miejsc zainstalowania innych elementów podsystemów ITS, gdzie powinny być umieszczone Ethernetowe przełączniki przemysłowe, służące do agregacji ruchu generowanego przez różne urządzenia należące do różnych podsystemów, zainstalowanych w pobliżu.

3.1.5 Sieci kablowe

Wymogiem oferty dla sieci łączy kablowych powinna być specyfikacja wskaźników niezawodnościowych oraz sposobu wyznaczania takich współczynników dla całej struktury sieci

W przypadku budowy nowych systemów należy unikać budowy rozległych sieci kablowych w oparciu o kable miedziane. Koszty kładzenia kabli miedzianych i optycznych są podobne. Natomiast przepustowość kabli optycznych jest wielokrotnie wyższa. Urządzenia wykorzystujące kable miedziane mają również znacznie mniejszy zasięg. Wymaga to stosowania aktywnych regeneratorów na kablach (oraz doprowadzania do nich zasilania). Kable miedziane należy stosować tylko w ograniczonym zakresie lokalnie. Wiele urządzeń końcowych systemów ITS jest zainstalowanych na słupach, bramownicach itp. Są one narażone na wyładowania atmosferyczne. Ograniczenie kabli miedzianych tylko do dystrybucji zasilania pozwala na ograniczenie narażeń na skutki wyładowań. Dużo łatwiej jest zabezpieczyć i odseparować galwanicznie zasilanie urządzeń niż interfejsy komunikacyjne. Natomiast światłowody są naturalnym separatorem galwanicznym urządzeń. Ograniczają propagację uszkodzeń wywoływanych przez wyładowania.

W sytuacji jednak, kiedy położone są kable miedziane to ze względów ekonomicznych należy je wykorzystywać.

3.1.6 Urządzenia aktywne

Wymogiem koniecznym dla każdego rozwiązania sprzętowo-programowego powinna być jednoznaczna definicja procedury testowania serwisowego oraz cyklicznego samotestowania. Każda oferta sprzętowo-programowa powinna zawierać wiarygodną specyfikację parametrów elementów oraz sposobu wyznaczania całkowitej niezawodności obiektu złożonego.

Przełączniki bardzo małe (od kilku do kilkunastu portów)

Parametry bardzo małych urządzeń przełączających (do kilkunastu portów), pracujących w warstwie 2 modelu OSI (switching), przeznaczonych do pracy w warstwie dostępowej sieci światłowodowej:

➤ w zakresie parametrów środowiska

- poprawna praca w trudnych warunkach środowiskowych (od -40°C do 70°C), wilgotność względna 5% do 95%
- praca z pasywnym chłodzeniem (bez wentylatorów)

➤ w zakresie wspieranych interfejsów i szybkości przełączania

- matryca przełączająca umożliwiającą pracę wszystkich portów z pełną szybkością (wire-rate switching)

- porty elektryczne 10/100BaseT lub/i 10/100/1000BaseT z auto-negocjacją szybkości pracy (IEEE 802.3 dla 10BaseT, IEEE 802.3u dla 100BaseT(X), IEEE 802.3ab dla 1000BaseT(X))
- uniwersalne porty pod moduły SFP (elektryczne 10/100/1000BaseT, optyczne 100BaseX, 1000BaseX - IEEE 802.3u dla 100Base FX, IEEE 802.3ab dla 1000BaseT(X), IEEE 802.3z dla 1000BaseSX/LX/LHX/ZX/EZX)
- wsparcie dla VLAN – numeracja do 4096 – dostępnych co najmniej 96 (IEEE 802.1Q)
- wsparcie dla IP ver.6

➤ **ułatwienia w zakresie zarządzania**

- interfejs do zarządzania

- intuicyjny interfejs CLI
- łatwy do użycia, bezpieczny interfejs zarządzania urządzeniem, bazujący na technologii WEB (wsparcie dla https/SSL) – zarządzanie przez przeglądarkę (IEEE 802.1X, https, SSL)
- wsparcie dla SNMPv1/2/3
- upload plików poprzez TFTP, FTP, SFTP lub SCP

- monitorowanie i analiza (troubleshooting)

- logi lokalne lub na wskazanym serwerze: syslog i comandlog
- port-based mirroring – ułatwia debugowanie sieci, równoległe przekazywanie pakietów na wskazany port umożliwiający obserwację i rejestrację wskazanego strumienia pakietów
- monitorowanie sieci RMON – umożliwia realizację zaawansowanych pomiarów, rejestrację danych statystycznych, historycznych, alarmów i zdarzeń
- wbudowane narzędzia sieciowe IP: ping

- konfiguracja sieci

- auto negocjacje w portach 10/100/1000 – wykrywanie szybkości pracy oraz ustawień duplexu
- DHCP relay forward client request to Server (ułatwia zarządzanie urządzeniami końcowymi z centralnej lokalizacji)
- NTP – synchronizacja czasu z serwera NTP
- GARP VLAN Registration Protocol (GVRP)
- Wsparcie dla port-based VLAN (przydzielanie/zdejmowanie znaczników VLAN dla wszystkich pakietów wpływających/wychodzących ze wskazanego portu)

➤ **wysoka dostępność oraz odporność sieci**

- możliwość zasilania z redundantnych zasilaczy
- protokoły wspierające pracę w pierścieniach z czasem konwergencji poniżej 100msec
- agregacja łączy IEEE 802.3ad (możliwość wirtualnego łączenia kilku portów w jedną wiązkę w celu zwiększenia przepływności w danym kierunku)
- Spanning Tree Protocol (STP) oraz IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)
- wsparcie dla per port VLAN (IEEE802.1Q VLAN oraz GVRP) umożliwiające separację za pomocą VLANów różnych podsystemów

- port trunking – możliwość agregacji fizycznych portów, wsparcie dla protokołów IEEE802.3ad i LACP
- filtracja multicastu (IGMP Snooping oraz GMRP) – wsparcie dla multicastu ułatwia zarządzanie transmisjami wideo

➤ **bezpieczeństwo sieci i kontrola dostępu**

- SSH w celu zapewnienia bezpiecznych sesji z CLI
- Zabezpieczenie dostępu do zarządzania hasłem i loginem oraz możliwość wymuszenia szyfrowanych sesji (https,SSL)
- IEEE802.1X
- Port Access Control - funkcja ta umożliwia przypisanie do portu switcha konkretnego adresu MAC, dzięki czemu tylko urządzenie o zdefiniowanym adresie MAC będzie mogło połączyć się z siecią przez dany port lub możliwość tworzenia list kontrolnych MAC adresów (ochrona przed nieautoryzowanym dostępem)
- zarządzanie pasmem
 - IEEE802.3x flow control , back pressure flow control
 - Traffic Rate Limiting - możliwość ograniczania pasma przypadającego na port urządzenia (zapobiega możliwości zdominowania przez ruch wychodzący z pojedynczych portów)
 - Broadcast Storm Protection - mechanizm zapobiegający "burzy" pakietów broadcast, która może pojawić się w przypadku błędnego skonfigurowania sieci lub awarii urządzenia sieciowego.
- możliwość tworzenia zdalnych kopii i zdalnego zapisywania i odtwarzania konfiguracji w celu łatwego odtworzenia po wymianie urządzenia na inne
- SNMPv3 (szyfrowane wiadomości SNMP)
- wsparcie dla zewnętrznych alarmów (wejście alarmowe oraz styk sterowania przekaźnikiem) – umożliwia kontrolę innych urządzeń zainstalowanych w tym samym miejscu – może być wykorzystywane do kontroli otwarcia szaf zainstalowanych w terenie.

Przełączniki małe i średnie (od kilkunastu do kilkuset portów)

Małe i średnie urządzenia przełączające przeznaczone do budowy warstwy dostępowej i agregacyjnej sieci światłowodowej powinny charakteryzować się następującymi cechami:

➤ **w zakresie parametrów środowiska**

- poprawna praca w trudnych warunkach środowiskowych (od-40°C do 70°C) jest wymagana dla urządzeń instalowanych poza pomieszczeniami lub szafami wyposażonymi w urządzenia klimatyzacji, wilgotność względna 5% do 95%

➤ **w zakresie wspieranych interfejsów i szybkości przełączania**

- matryca przełączająca umożliwiającą pracę wszystkich portów z pełną szybkością (wire-rate switching)

- porty elektryczne 10/100BaseT lub/i 10/100/1000BaseT z auto-negocjacją szybkości pracy (IEEE 802.3 dla 10BaseT, IEEE 802.3u dla 100Base T(X), IEEE 802.3ab dla 1000BaseT(X))
- uniwersalne porty pod moduły SFC (elektryczne 10/100/1000BaseT, optyczne 100BaseX,1000BaseX - IEEE 802.3u dla 100Base FX, IEEE 802.3ab dla 1000BaseT(X), IEEE 802.3z dla 1000BaseSX/LX/LHX/ZX/EZX)
- opcjonalnie porty 10Gb (IEEE802.3ae)
- wsparcie dla VLAN – do 4096 (IEEE 802.1Q)
- wsparcie dla Jumbo Frame dla portów gigabitowych
- co najmniej per system 16000 MAC adresów
- wsparcie dla IP ver.6
-

➤ **ułatwienia w zakresie zarządzania**

- interfejs do zarządzania

- intuicyjny interfejs CLI
- łatwy do użycia, bezpieczny interfejs zarządzania urządzeniem, bazujący na technologii WEB (wsparcie dla https/SSL) – zarządzanie przez przeglądarkę (IEEE 802.1X, https, SSL)
- pełna konfiguracja oraz raportowanie via SNMPv1/2/3
- zdalny dostęp do przełącznika poprzez telnet lub SSH
- upload plików poprzez TFTP,FTP,SFTP lub SCP
- pliki konfiguracyjne tekstowe umożliwiające edycję off-line oraz rekonfigurację przez wymianę plików

- monitorowanie i analiza (troubleshooting)

- logi lokalne lub na wskazanym serwerze: syslog i comandlog
- port-based mirroring – ułatwia debugowanie sieci, równoległe przekazywanie pakietów na wskazany port umożliwiający obserwację i rejestrację wskazanego strumienia pakietów
- policy-based mirroring – ułatwia debugowanie sieci, pozwala na przekazywanie pakietów na wskazany port na bazie typu ruchu i umożliwia obserwację i rejestrację wskazanych pakietów wykorzystując QoS
- remote port mirroring – pozwala na przekazywanie obserwowanych pakietów poprzez sieć do zdalnego urządzenia
- monitorowanie sieci sFlow v.5, RMON – umożliwia realizację zaawansowanych pomiarów, rejestrację danych statystycznych, historycznych, alarmów i zdarzeń
- wbudowane narzędzia sieciowe IP: ping, trace router
- utrzymanie, działanie oraz zarządzanie wg standardu Y.1731 IEEE 802.1ag Ethernet operations, administration and maintenance (OA&M): zarządzanie błędami połączeń oraz pomiary wydajności - Fault Management and performance measurements (layer-2 ping and link trace)
- monitorowanie linków, wykrywanie zdalne błędów i kontrola pętli wg. standardu IEEE 802.3ah Ethernet in the First Mile (EFM) for link monitoring, remote fault detection, and loopback control (layer-1 ping)
- wykrywanie i wyłączenie linków światłowodowych działających tylko w jednym kierunku (drugi kierunek uszkodzony) - Unidirectional Link Detection (UDLD)
- Digital Diagnostic Monitoring (DDM): diagnostyka w czasie rzeczywistym połączeń światłowodowych w celu wczesnego wykrywania pogorszenia sygnału optycznego

- • Link Monitoring: link flap detection oraz link error counts – wykrywanie szybkich wielokrotnych zmian stanu łącza oraz liczniki błędów w celu zidentyfikowania niestabilnego łącza i zastąpienia go zapasowym
- Time Domain Reflectometry (TDR): wykrywanie i lokalizacja przerw i innych nieciągłości w kablach miedzianych

- konfiguracja sieci

- auto negocjacje w portach 10/100/1000 – wykrywanie szybkości pracy oraz ustawień duplexu
- Auto MDI/MDIX automatycznie sprawdza i ustawia w porcie Ethernetowym sygnały nadawane i odbierane bez konieczności stosowania kabli z połączeniami prostymi lub skrosowanymi
- • BOOTP/DHCP client - umożliwia auto-konfigurację przełącznika i ułatwia implementację sieci
- DHCP relay forward client request to Server (ułatwia zarządzanie urządzeniami końcowymi z centralnej lokalizacji)
- NTP – synchronizacja czasu z serwera NTP
- Multiple VLAN Registration Protocol (MVRP and GVRP) for 802.1Q/1ak-ułatwia dynamiczne kreowanie VLANów
- GARP VLAN Registration Protocol (GVRP) – ułatwia i automatyzuje konfigurację VLANów w sieci rozległej
- Wsparcie dla port-based VLAN (przydzielanie/zdejmowanie znaczników VLAN dla wszystkich pakietów wpływających/wychodzących ze wskazanego portu)
- Auto QoS dla zarządzania przełącznikiem oraz ruchem IP dla połączeń głosowych

- wysoka dostępność oraz niezawodność sieci

- możliwość zasilania z redundantnych zasilaczy przełączanych na gorąco. Ilość zasilaczy niezbędnych do pracy urządzenia w roboczej konfiguracji + 1.
- budowa modułarna, w tym możliwość konfiguracji redundantnej wg jednego z dwóch rozwiązań:
 - wirtualne chassis, zestawianie i łączenie samodzielnych modułów w stos (stack), "wymiana na gorąco" chassis, zasilaczy, transceiverów i funkcja przywracania obrazu.
 - Chassis z wymiennymi modułami w postaci kart, możliwość zainstalowania dwóch kart sterowania, „wymiana kart na gorąco”
- ITU-T G.8032 Ethernet Ring Protection - protokół umożliwiający pracę w topologii pierścienia (ring) z czasem konwergencji 50msek
- Ring Rapid Spanning Tree Protocol (RRSTP) – protokół z grupy Rapid Spanning Tree zoptymalizowany do pracy w topologii pierścienia (ring) umożliwiający konwergencję poniżej 100
- IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) obejmujący IEEE 802.1d STP oraz IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)
- agregacja łączy IEEE 802.3ad (LACP) oraz static Link Aggregation Groups (LAGs) (możliwość wirtualnego łączenia kilku portów w jedną wiązkę w celu zwiększenia przepływności w danym kierunku)
- wsparcie dla per port VLAN (IEEE802.1Q VLAN oraz GVRP) umożliwiające separację za pomocą VLANów różnych podsystemów

- port trunking – możliwość agregacji fizycznych portów, wsparcie dla protokołów IEEE802.3ad i LACP – pozwala na agregację kilku portów w jedno łącze i umożliwia zwiększanie przepływności w danym kierunku
- Virtual Router Redundancy Protocol (VRRP) w celu budowy odpornego wirtualnego środowiska routingu
- Bidirectional Forwarding Detection (BFD) w celu szybkiego wykrywania błędów i skrócenia czasu konwergencji w środowisku routującym
- Broadcast, nieznanego unicast i multicast storm control – kontrola sztormu pakietów w celu zapobiegania degradacji wydajności systemu
- Konfiguracja typu “Dual image” i dwoma przełączanymi plikami konfiguracyjnymi – pozwala na szybkie zmiany konfiguracji przez przełączenie urządzenia z jednej wersji oprogramowania na inną i z jednej konfiguracji na drugą
- filtracja multikastu (IGMP Snooping oraz GMRP) – wsparcie dla multikastu ułatwia zarządzanie transmisjami wideo
-

➤ **bezpieczeństwo sieci**

- kontrola dostępu

- SSH w celu zapewnienia bezpiecznych sesji z CLI ze wsparciem dla PKI (public key infrastructure)
- Zabezpieczenie dostępu do zarządzania hasłem i loginem oraz możliwość wymuszenia szyfrowanych sesji (https,SSL)
- Web-based authentication (captive portal): rezydujący w przełączniku portal
- TACACS+ klient pozwalający na autentykację, autoryzację we współpracy ze zdalnym serwerem TACACS+
- zcentralizowany RADIUS oraz autentykacja użytkownika Lightweight Directory Access Protocol (LDAP)
- Wbudowany system detekcji anormalnego ruchu – Embedded traffic anomaly detection (TAD) monitorujący wzorce ruchu typowe dla wirusów oraz wyłączenia portów i raportuje takie zdarzenia do systemu nadzoru
- ARP poisoning detection – służy do wykrywania prób zatrucia informacji ARP
- Wsparcie dla Microsoft® Network Access Protection (NAP)
- Bridge Protocol Data Unit (BPDU) zapobiega tworzeniu
- STP Root Guard zapobiega uznaniu urządzeń brzegowych za STP root nodes
- Port Access Control - funkcja ta umożliwia przypisanie do portu switcha konkretnego adresu MAC, dzięki czemu tylko urządzenie o zdefiniowanym adresie MAC będzie mogło połączyć się z siecią przez dany port lub możliwość tworzenia list kontrolnych MAC adresów (ochrona przed nieautoryzowanym dostępem)
- wsparcie dla zewnętrznych alarmów (wejście alarmowe oraz styk sterowania przekaźnikiem) – umożliwia kontrolę innych urządzeń zainstalowanych w tym samym miejscu – może być wykorzystywane do kontroli otwarcia szaf zainstalowanych w terenie.

- zarządzanie ruchem

- Listy kontroli dostępu ACL służące do odfiltrowania niechcianego ruchu w tym ataków typu denial of service (DoS); sprzętowe filtrowanie przepływu “flow-based filtering” (layer 1 to layer 4)
- zarządzanie pasmem

- Zarządzanie pasmem bazujące na kontroli przepływów wykorzystujące następujące techniki:
 - ingress/egress rate limiting;
 - egress rate shaping per port
 - per class of service (CoS) queue
 - IEEE802.3x flow control
 - back pressure flow control
 (zapobiega możliwości zdominowania przez ruch wychodzący z pojedynczych portów, urządzeń, aplikacji)
- Broadcast Storm Protection - mechanizm zapobiegający "burzy" pakietów broadcast, która może pojawić się w przypadku błędnego skonfigurowania sieci lub awarii urządzenia sieciowego.

- QoS

- Kolejki priorytetowe: 8 kolejek sprzętowych per port
- Zarządzanie kolejkami: konfigurowalny Scheduler
 - Algorithms:
 - Strict Priority Queuing (SPQ),
 - Weighted Round Robin (WRR), and Deficit
 - Round Robin (DRR) or combination of algorithms
- Zapobieganie natłokowi w sieci- Congestion avoidance: wsparcie przez sieć End-to-End Head-of-Line (E2E-HOL) Blocking prevention and flow control
- LLDP – polityki sieciowe - dynamiczne oznaczenie VLAN-ID i layer-2/layer-3 priorytetem dla telefonów IP – dynamic designation of VLAN-ID and layer-2/layer-3 priority for IP phones

➤ protokoły routingu

- **Layer-3 routing i multicast**
- **IPv4 routing - wymagane protokoły**
 - Routing statyczny
 - Routing Information Protocol (RIP) v1 and v2
 - Open Shortest Path First (OSPF) v2
 - Intermediate System-to-Intermediate System (IS-IS)
 - Border Gateway Protocol (BGP) v4
 - Generic Routing Encapsulation (GRE) tunneling
 - Graceful restart extensions for OSPF and BGP
 - VRRP v2
 - DHCP relay (including generic UDP relay)
 - ARP
 - IP SLA measurement

- IPv6 routing – wymagane protokoły

- routing statyczny
- Routing Information Protocol Next Generation (RIPng)
- OSPF v3
- BGP v4 (with extensions to IPv6 routing)
- Graceful restart extensions for OSPF and BGP

- VRRP v3
- Neighbor Discovery Protocol (NDP)
- IPv4/IPv6 Multicast
- Internet Group Management Protocol (IGMP) v1/v2/v3 snooping for optimized multicast traffic
- Protocol Independent Multicast - Sparse Mode (PIM-SM)/Protocol Independent Multicast - Dense Mode (PIM-DM)
- Distance Vector Multicast Routing Protocol (DVMRP)
- Multicast Listener Discovery (MLD) v1/v2 snooping for optimized multicast traffic

- **Metro Ethernet access – protokoły i usługi**

- Ethernet services support per IEEE 802.1ad Provider Bridge services (also known as Q-in-Q or VLAN stacking):
- Service VLAN (SVLAN) and Customer VLAN (CVLAN) transparent LAN services
- Ethernet network-to-network interface (NNI) and user network interface (UNI) services
- Service Access Point (SAP) profile identification
- CVLAN-to-SVLAN translation
- Ethernet OA&M compliant with ITU Y.1731 and IEEE 802.1ag version 8.1 for connectivity fault and performance management and
- IEEE 802.3ah EFM for link OA&M
- Service Assurance Agent (SAA) for SLA compliance validation
- Private VLAN feature for user traffic segregation
- MAC-Forced Forwarding support according to RFC 4562
- DHCP Option 82: Configurable relay agent information
- IP Multicast VLAN (IPMVLAN)
- Optimized Ethernet access services delivery → Network bandwidth protection against overload of video traffic
- Multicast streams isolation from multiple content providers over the same interface

Przełączniki duże (od kilkuset do kilku tysięcy portów)

Urządzenia aktywne warstwy szkieletowej sieci ITS, oprócz cech zdefiniowanych powyżej dla przełączników średnich, powinny dodatkowo wspierać:

- Usługi IP/MPLS włączając w to następujące protokoły:
 - border gateway protocol (BGP)-based MPLS VPNs,
 - VPLS,
 - VLLs
 - resource reservation protocol
 - traffic engineering (RSVP-TE),
 - label distribution protocol (LDP)
 - targeted LDP (T-LDP)

Podsystem komunikacyjny powinien zostać wyposażony w oprogramowanie monitorujące prace urządzeń, umożliwiające natychmiastowe powiadomienie operatora systemu o awarii każdego z urządzeń wchodzących w skład podsystemu.

Należy zapewnić dostęp do zasobów jedynie osobom uprawnionym poprzez stosowanie odpowiednich systemów zabezpieczeń (zapór ogniowych, sieci VPN, logowania do urządzeń

sieciowych na miejscu za pomocą portu konsolowego lub zdalnie przy użyciu protokołu SSH v2 (niezalecane jest używanie protokołu Telnet – chyba że przez szyfrowany tunel), każdy przełącznik sieciowy musi być zabezpieczony hasłem dostępu, musi także mieć zaimplementowany protokół SNMP v3.

Planowane do zainstalowania urządzenia w sieci światłowodowej podsystemu komunikacyjnego ITS w warstwie dostępowej powinny wykorzystywać dostępne pasmo na poziomie nie wyższym niż 20% w momencie uruchomienia podsystemu, co zapewni możliwość dołączania kolejnych elementów końcowych ITS bez konieczności rozbudowy warstwy dostępowej podsystemu łączności (w warstwie dostępowej mogą być stosowane małe tanie urządzenia przełączające o ograniczonych możliwościach rozbudowy).

3.1.7 Sieci bezprzewodowe dedykowane

Połączenia bezprzewodowe najczęściej realizuje się za pomocą fal radiowych, rzadziej i w ograniczonym zakresie za pomocą fal świetlnych (linki laserowe). W technologii fal radiowych można wykorzystywać różne częstotliwości. Generalnie całe pasmo radiowe zostało podzielone i poszczególne jego zakresy przeznaczone zostały dla różnych służb. Można stwierdzić, że w przypadku systemów ITS będzie można korzystać z pasma radiowego licencjonowanego lub nie licencjonowanego.

3.1.7.1 Pasma licencjonowane

Pasma licencjonowane jest przydzielane przez UKE dla realizacji określonych połączeń, o określonej przepustowości, we wskazanych lokalizacjach. Kontrolowana jest również moc urządzeń nadawczych. Za korzystanie z pasma licencjonowanego pobierane są opłaty. Pełna kontrola pasma licencjonowanego pozwala na gwarantowanie parametrów połączeń i unikanie zakłóceń przez innych użytkowników. Dlatego też urządzenia pracujące w pasmach licencjonowanych gwarantują lepsze parametry oraz większą stabilność łączy.

Do realizacji łączy bezprzewodowych dla podsystemów ITS wymagających podwyższonej niezawodności powinny być stosowane łącza wyłącznie w paśmie licencjonowanym. Można dopuszczać niewielkie odstępstwa w terenie o bardzo małym nasyceniu zabudową – np. leśnym. Tam można wykorzystywać również w ograniczonym zakresie pasma nie licencjonowane – ponieważ jest bardzo mało prawdopodobne zastosowanie w tym paśmie urządzeń przez innych użytkowników.

3.1.7.1.1 Łączność trankingowa

Tranking - komputerowo sterowany system bezprzewodowej łączności dyspozytorskiej. Polega na wykorzystaniu ograniczonej ilości kanałów radiowych przez maksymalną liczbę użytkowników. W dwukierunkowej łączności radiowej tranking jest zdefiniowany jako automatyczny i dynamiczny rozdział ograniczonej liczby kanałów pomiędzy dużą liczbą użytkowników radiotelefonów.

Systemy trankingowe służą przede wszystkim do zapewnienia dedykowanej bezprzewodowej łączności głosowej pomiędzy pojazdami oraz do lokalizacji stałych. Ponadto można wykorzystywać ją do transmisji danych, ale przepustowość takiej transmisji jest stosunkowo niska, szczególnie w przypadku systemów analogowych.

Systemy trankingowe są szczególnie przydatne tam, gdzie jest niezbędna szybka i sprawnie działająca łączność bezprzewodowa. Pozwalają na realizację połączeń w terenie,

szczególnie ze wszelkiego rodzaju służbami mobilnymi. Łączność trunkingowa jest stosowana przez służby związane z bezpieczeństwem publicznym, jak również przez służby techniczne i utrzymaniowe.. Systemy trunkingowe umożliwiają wywołanie do wielu, konferencje, połączenia alarmowe. Ponieważ łączność trunkingowa realizowana jest w wydzielonych kanałach, dzierżawionych wyłącznie dla tego celu, jest ona dostosowana do działań w warunkach kryzysowych. W wielu zastosowaniach, w normalnych warunkach, sieć trunkingowa może być zastąpiona połączeniami poprzez publiczne sieci komórkowe. Niestety publiczne sieci komórkowe, w sytuacjach kryzysowych, mogą się okazać zbyt przeciążone przez innych abonentów i korzystanie z takiej sieci przez służby ratunkowe i techniczne może być mocno utrudnione. Sieć dedykowana, a taką jest sieć rankingowa, może być zarządzana przez dysponenta i korzystanie z niej jest pod kontrolą. Stosowane są generalnie dwa podstawowe typy sieci trunkingowych –analogowe i cyfrowe

System analogowy - protokół MPT1327 (najbardziej popularny)

Zastosowanie protokołu MPT1327 pozwala użytkownikowi na swobodny wybór marki i modelu radiotelefonu. MPT 1327 umożliwia wiele rodzajów transmisji mowy i danych, a także stosowanie różnych typów modulacji. MPT 1327 dzięki swojej elastyczności umożliwia tworzenie sieci o różnym zasięgu i strukturze, począwszy od lokalnych poprzez regionalne do krajowych włącznie.

Łączność trunkingowa cyfrowa- europejski system TETRA

TETRA (ang. TErrestrial TRunked RAdio) to system naziemnej łączności radiowej. Bazuje na otwartym standardzie cyfrowej łączności dyspozytorskiej, opracowanym przez Europejski Instytut Norm Telekomunikacyjnych (ETSI). Powstał z przeznaczeniem dla służb ratownictwa i bezpieczeństwa publicznego. Standard ten ma na celu spełnienie potrzeb najbardziej wymagających profesjonalnych użytkowników mobilnej łączności radiowej. Łączy on zalety radiotelefonii konwencjonalnej i komórkowej w przesyłaniu wiadomości i danych. Umożliwia funkcjonowanie z wieloma dostawcami sprzętu i systemów. Ułatwia natychmiastowy kontakt z jednym lub nawet kilkuset członkami zespołu na dużych obszarach. Zapewnia najwyższy poziom niezawodności i możliwości połączeń, dostępny na platformie bezprzewodowej. Pozwala na zastosowanie jej do celów łączności o kluczowym znaczeniu (mission-critical).

Zalecenia

W przypadku budowy nowych systemów wskazane jest stosowanie systemów cyfrowych.

3.1.7.1.2 Radiolinie

Radiolinie służą do realizacji połączeń radiowych punkt punkt

Tab. 1 Wymagania dla sieci szkieletowej - radiolinie o dużej przepływności

Element konfiguracji	Wymagania minimalne
Pasmo	praca w licencjonowanych pasmach 13, 18, 23, 26, 32, 38 GHz
Polaryzacja	możliwość pracy w konfiguracji z obydwoma polaryzacjami: pionową (V) i poziomą (H)

Wymagana przepływność	Minimum 100Mbit/s w kanale o szerokości 28 MHz przy modulacji nie wyższej niż 32QAM. Możliwość programowej rozbudowy łącza
Alokacja pasma przez pojedynczy moduł radiowy (jeden moduł IDU + jedno ODU)	praca w organizacji kanału 7, 14, 28, 56 MHz
Automatyczna regulacja mocy nadajnika (ATPC)	Wymagany zakres min. 20 dB
Adaptacyjna modulacja	bezstratne przełączanie modulacji w trybie adaptacyjnym (brak jakichkolwiek błędów transmisyjnych (ES, SES, BBE) lub opóźnień przy przełączaniu
Zasięg systemu	budżet łącza radiowego systemu zapewniający zasięg użyteczny powyżej 5km w warunkach strefy klimatycznej H (wg. ITU-R P.837) oraz dostępności 99,99% w skali roku i antenach o średnicy maksymalnie 0,3m
Interfejsy	Zapewnienie interfejsów 10/100/1000Base-T (minimum 4 porty), SFP (2 porty) Wejścia / wyjścia dla zewnętrznych zdarzeń alarmowych.
Transparentność	zapewnienie przeźroczystości systemu w warstwie 2 transmisji typu Ethernet.
Konfiguracja systemu	Praca w konfiguracji 1+0, 2+0, 1+1
DCN	Obsługa protokołu routingu RIPv1 lub v2 oraz OSPF, możliwość zdefiniowania statycznej tablicy routingu dla ruchu NMS.
Diagnostyka	- Możliwość odczytu aktualnej mocy nadawczej oraz odbiorczej jednostki zewnętrznej ODU oraz panującej temperatury jak i podawanego napięcia. - Możliwość zachowania istniejącej konfiguracji terminala w pliku.
Funkcjonalność warstwy 2 dla Ethernet	- wbudowana funkcjonalność przełącznika Ethernet (MAC Switching, MAC Learning, MAC Ageing) - transport IEEE 802.1q VLAN, - obsługa IEEE 802.1x Flow Control - obsługa 802.3, 802.3u, 802.3ab, 802.3z, 802.3ac, 802.1p, 802.1ad, 802.3x, 802.3ad, 802.1D, 802.1w, 802.1s, RFC 1349, RFC 2474, RFC 2460 - wbudowane narzędzia do diagnostyki ruchu Ethernet: status interfejsów, aktualna przepływność (statystyki RMON reprezentacja graficzna oraz liczbowa), statystyki historyczne
Jakość usług (QOS)	Wbudowane mechanizmy priorytetyzacji ruchu na podstawie: 802.1p, Diffserv lub numeru fizycznego portu.
Zasilanie	Napięcie standardowe 48VDC

Wymagania dla radiolinii realizujących połączenia lokalne muszą być dostosowane do potrzeb konkretnych urządzeń i mogą być inne niż dla sieci szkieletowej.

3.1.7.2 Pasma nielicencjonowane

Pasma nielicencjonowane, ich przeznaczenie oraz parametry urządzeń, które można stosować bez dodatkowych zezwoleń do pracy w tych pasmach określa „Rozporządzenie Ministra Transportu z dnia 3 lipca 2007 r. w sprawie urządzeń radiowych nadawczych lub nadawczo-odbiorczych, które mogą być używane bez pozwolenia radiowego”

Są to urządzenia:

- typu PMR 446, przeznaczone do używania wyłącznie w zakresie częstotliwości 446,0-446,1 MHz w ośmiu kanałach radiowych z odstępem 12,5 kHz, gdzie najniższa częstotliwość fali nośnej wynosi 446,00625 MHz, z zastępczą mocą promieniowaną nadajnika w odniesieniu do dipola półfalowego, zwaną dalej "e.r.p.", nieprzekraczającą 500 mW, wyposażonych tylko w antenę zintegrowaną, spełniających wymagania określone w normach przenoszących normę ETSI EN 300 296;
- Cyfrowe noszone typu PMR 446, przeznaczone do używania wyłącznie w zakresie częstotliwości 446,1-446,2 MHz, w kanałach radiowych z odstępem 6,25 kHz lub 12,5 kHz, z mocą nadajnika nieprzekraczającą 500 mW e.r.p., wyposażonych tylko w antenę zintegrowaną, z wymuszonym ograniczeniem czasu nadawania do 180 s, spełniających wymagania określone w normie przenoszącej normę ETSI EN 300 113, normę ETSI EN 301 166 lub w równoważnych specyfikacjach technicznych;
- Przeznaczone do używania wyłącznie w zakresie częstotliwości 26,96-27,41 MHz:
 - typu PR27, spełniających wymagania określone w normach przenoszących normę ETSI EN 300 135,
 - b) z emisją dwuwstęgową sygnału zmodulowanego amplitudowo, zwaną dalej "DSB-AM", lub emisją jednowstęgową sygnału zmodulowanego amplitudowo, zwaną dalej "SSB-AM", spełniających wymagania określone w normach przenoszących normę ETSI EN 300 433, przy czym dopuszczalna moc wyjściowa nadajnika dla DSB-AM wynosi do 4 W, a dla SSB-AM do 12 W szczytowej mocy obwiedni;

Ponadto rozporządzenie to definiuje dodatkowe grupy urządzeń radiowych nie wymagających pozwoleń na stosowanie oraz podaje ich parametry:

- Urządzenia bliskiego zasięgu ogólnego stosowania
- Urządzenia do wykrywania ofiar lawin
- Szerokopasmowe systemy transmisji danych
- Urządzenia stosowane w transporcie kolejowym
- Urządzenia stosowane w RTTT (Road Transport and Traffic Telematics - telematyka transportu i ruchu drogowego)
- Urządzenia do wykrywania ruchu i ostrzegania o ruchu
- Urządzenia alarmowe
- Urządzenia do sterowania modelami

- Urządzenia do zastosowań indukcyjnych
- Mikrofony bezprzewodowe i urządzenia wspomagające słuch
- Urządzenia do RFID
- Urządzenia bezprzewodowe do zastosowań w ochronie zdrowia
- Bezprzewodowe urządzenia do transmisji sygnałów akustycznych
- Samochodowe radary bliskiego zasięgu przeznaczone do używania w paśmie częstotliwości 79 GHz

O ile stosowanie urządzeń z grupy „Urządzenia stosowane w RTTT ((Road Transport and Traffic Telematics - telematyka transportu i ruchu drogowego))” nie budzi wątpliwości, to jednak pasma radiowe przeznaczone dla tych urządzeń są pasmami ISM i mogą w nich działać inne urządzenia ISM – trzeba więc wziąć pod uwagę możliwości wprowadzania przez nie zakłóceń.

Do łączności głosowej mogą być wykorzystywane urządzenia PMR.446 oraz pracujące w paśmie 26,96-27,41 MHz. W tym ostatnim paśmie zwanym również CB powinno się zapewnić nasłuch na kanale ratunkowym.

W przypadku wykorzystywania rozwiązań typu WiFi jako rozwiązania komunikacyjnego pomiędzy stacjami sieci bezprzewodowej należy:

- dostęp kliencki do sieci z użyciem standardów 802.11a, 802.11b, 802.11g, a także 802.11n, , przy czym preferowany powinien być dostęp w paśmie 5,4 GHz (802.11a,n)
- bezwzględnie wymagana obsługa mechanizmów uwierzytelniania i autoryzacji, w tym przede wszystkim standardów WPA i WPA2,
- wyposażenie sieci w narzędzia administracyjne umożliwiające monitorowanie, zarządzanie, konserwację oraz kontrolę dostępu
- możliwość zrealizowania wirtualnych sieci bezprzewodowych,
- posiadanie możliwości wprowadzenia priorytetów ruchu (Quality of Service),

Przy budowie dużej sieci Wi-Fi zlecane jest stosowanie kontrolera sieci bezprzewodowej.

Parametry kontrolera sieci bezprzewodowej WiFi:

- Obsługa min. 24 sieci WLAN
- Obsługa min. 6 Access Pointów
- Wymagane funkcjonalności:
 - RADIUS Server
 - DHCP (client/server/relay)
 - Hotspot
 - 802.1D-1999 Ethernet bridging
 - 802.11-802.3 bridging
 - 802.1Q VLAN tagging, trunking
 - proxy ARP
 - IP packet steering-redirection
 - IPv6 client
- Zarządzanie:
 - Command line interface (serial, telnet, SSH)
 - secure Web-based GUI (SSL)
 - SNMP v1/v2/v3
 - SNMP trap

- Bezpieczeństwo dostępu do sieci:
 - Firewall (min. 50 000 aktywnych sesji na kontroler)
 - L2/L3/L4 ACL
 - IPSec VPN
 - Szyfracja: WEP 40/128 (RC4), KeyGuard, WPA—TKIP, WPA2-CCMP (AES), WPA2-TKIP
 - 802.11w
- Aktualizacja firmware i konfiguracji urządzeń przez TFTP, FTP i SFTP
- Możliwość klastrowania kontrolerów
- Redundancja sprzętowa (1+1) kontrolera
- Współdzielenie licencji w ramach klastra kontrolerów
- Możliwość montażu w szafie telekomunikacyjnej
- Praca w temperaturach od 0°C do +40°C
- Zasilanie: 230 VAC
- Zgodność z wymaganiami CE

Access Pointy:

- Obsługa standardów: 802.11a, 802.11b, 802.11g, 802.11n
- Technologie transmisji: DSSS, OFDM, MIMO (min. 2x3)
- Zakres temperaturowy pracy w zależności od lokalizacji (warunki biurowe, warunki zewnętrzne)
- Zgodność z wymaganiami CE

Ważne jest, aby wszystkie wykorzystywane rozwiązania i protokoły były publicznie dostępne i otwarte tak, aby uniezależnić się od jednego konkretnego dostawcy sprzętu lub innego elementu systemu. Najbardziej pożądane powinny być rozwiązania ustandaryzowane przez organizacje takie jak IEEE lub IETF. Wymaganie takie umożliwi w przyszłości dalszą rozbudowę systemu, być może z wykorzystaniem już nowszych technologicznie rozwiązań. Wybór producenta nie może doprowadzić do zmonopolizowania dostawcy sprzętu bezprzewodowego poprzez wykorzystywanie własnościowych protokołów komunikacyjnych, zarówno w warstwie dostępowej jak i dystrybucyjnej.

3.1.7.2.1 Radiolinie (punkt-punkt)

Z pasm ISM można korzystać do budowy radiolinii punkt punkt. Najczęściej wykorzystuje się standardy WiFi tj pasmo 2.4 GHz oraz 5,4GHz ponadto niezbyt często używane pasmo ISM 24GHz

Nie zaleca się budowy radiolinii wykorzystujących pasmo WiFi 2.4GHz (standard 802.11b, g lub n). To pasmo powszechnie wykorzystują wszelkiego rodzaju urządzenia komputerowe. Jest narażone na łatwe zakłócanie. Z tego punktu widzenia bardziej interesujące jest pasmo 5,4GHz. Jest to pasmo mniej narażone na zakłócanie przez innych.

Radiolinie Wi-Fi - wymagania:

- praca w paśmie częstotliwości 5,4 GHz,
- musi posiadać możliwość pracy w kanałach 5 MHz, 10 MHz lub 15 MHz
- obsługa modulacji uplink/downlink: BPSK, QPSK, 16QAM, 64QAM
- anteny dwupolaryzacyjne (polaryzacja H i V)
- technika MIMO,

- adaptacyjna modulacja OFDM,
- maksymalna przepływność zagregowana w podstawowej konfiguracji co najmniej 25 Mbit/s z możliwością programowego zwiększenia do co najmniej 50 Mbit/s oraz 100Mbit/s poprzez zakup w przyszłości odpowiedniego klucza licencyjnego,
- możliwość dynamicznej zmiany podziału pasma uplink/down link,
- dostępność wersji sprzętowej ODU z anteną zintegrowaną oraz wersji z anteną zewnętrzną,
- wbudowane zabezpieczenie ochronne przed wyładowaniami atmosferycznymi w module ODU,
- możliwość synchronizacji urządzeń nadawczo-odbiorczych sygnałem GPS,
- korekcja błędów (FEC),
- bezpieczeństwo: algorytm producentki (np. skrambling), DES lub AES
- obsługa 802.1q, 802.1p,
- wbudowany analizator widma,
- interfejs urządzenia wewnętrznego IDU 10/100BaseT z obsługą auto MDI/MDIX,
- obsługa minimum 2 poziomów priorytetów ruchu,
- zarządzania i konfiguracja poprzez wbudowany serwer WWW, SNMP (w wersji co najmniej 2c) oraz dedykowany system zarządzania NMS
- podłączenie urządzenia zewnętrznego ODU poprzez jeden kabel sieciowy kat. 5 przenoszący zasilanie (PoE) oraz transmisję danych,
- maksymalny pobór mocy nie większy niż 50 Watt,
- zasilanie modułu wewnętrznego IDU z napięcia ~230V lub =48V,
- możliwość wprowadzenia zasilania redundantnego,
- temperatura pracy urządzeń ODU (od -40° C do +55° C)
- zgodność z wymogami zasadniczymi CE

3.1.7.2.2 Sieci (punkt - wielopunkt)

Tego typu sieci buduje się z wykorzystaniem topologii punkt-wielopunkt. Pozwala ona na budowę sieci lokalnych o zasięgu w terenie otwartym do kilkunastu KM, w zależności od przyjętej technologii. Służą do obsługi wielu urządzeń końcowych z punktu dystrybucyjnego sygnału radiowego. Mogą być stosowane jako rozwiązania dla łączności stacjonarnej, nomadycznej oraz mobilnej.

➤ **Sieci bazujące na technologii Wi-Fi**

- Zasięg do 200 m w terenie otwartym
- Używane pasma 2,4 i 5 GHz

➤ **Sieci bazujące na technologii WiMAX (wymagane licencje – zasięg od kilku do kilkunastu kilometrów)**

- praca w paśmie częstotliwości 3,6 – 3,8 GHz, (pasmo dopuszczone do użytkowania w Polsce)
- możliwość stosowania anten sektorowych

- Praca dwupiętrowa z podziałem czasowym TDD (Time Division Duplex), lub z podziałem częstotliwościowym FDD (Frequency Division Duplex),
- Możliwość pracy przy braku widoczności optycznej NLOS (None Line Of Sight),
- Stosowana szerokość kanałów od 1,75 MHz, poprzez 3,5 MHz, aż do 7 MHz FDD,
- Stosowane modulacje BPSK, QPSK, 16QAM oraz 64QAM,
- Transmisja IP z QoS, z usługami VoIP

Systemy LMDS (Local Multipoint Distribution System).

Wymagane licencje – zasięg od kilku do kilkunastu kilometrów, dostępna większa przepływność niż w systemach WiMax

- Stosowane pasma częstotliwości 26 lub 28 GHz.
- Zapewnia dużą skalowalność systemu - istnieje możliwość rozbudowania sektorów aż do 4 BSSA na jeden sektor dzięki temu udaje się uzyskać przepustowość pojedynczego sektora do 134 Mbit/s.
- Anteny sektorowe 45, 90 i 180 stopniowymi, (dzięki czemu maksymalna przepustowość pojedynczej stacji bazowej może wynosić nawet 1,2 Gbit/s)
- Typowe kanały o szerokości 3,5, 7 oraz 14 MHz.
- Wysoką wydajność radiową wynoszącą 2,5 bit/s/Hz.
- pełnej QoS.
- Systemy LMDS stosuje się jako sieć dostępową lub dystrybucyjną.

3.1.7.3 Linki w falach milimetrowych i optyczne (laserowe)

Oferowane są na rynku odpowiedniki radiolinii. Element nadawczo odbiorczy takiej linii działa w zakresie fal milimetrowych lub jest to nadajnik-odbiornik optyczny. Łączy te stosuje się na stosunkowo krótkie odległości (do kilku kilometrów). Wymagana jest bezpośrednia widoczność urządzeń końcowych. Transmisja może być zakłócana w czasie intensywnych opadów deszczu lub śniegu – szczególnie na większe odległości. Nie zastępuje do budowy krótkich połączeń o dużej przepływności w warunkach bezpośredniej widoczności w miejscach o dużym nasyceniu urządzeniami radiowymi, szczególnie w miastach. Umożliwiają realizację połączeń pomiędzy budynkami bez konieczności prowadzenia prac kablowych pod ziemią. Ich stosowanie wymaga zezwoleń radiowych dla linków optycznych lub realizowane są w wysokich pasmach częstotliwościowych objętych niskimi kosztami dzierżawy.

Przykładowe wymagania techniczne na radiolinie na falach milimetrowych

- Maksymalna przepustowość min. 1000 Mbps, half-duplex
- Częstotliwość 71-76 GHz
- Szerokość kanałów 250 MHz or 500 MHz (Typowe)
- Modulacja QPSK, QAM 16 FEC Convolutional Turbo Coding (CTC)
- Adaptacyjna szerokość kanału, kodowanie i modulacja

Antena

- Średnica 26 cm
- Zysk 43 dBi

Carrier Ethernet

- Zintegrowany przełącznik warstwy 2
- Provider Bridge (802.1ad)
- QoS Quality of Service (QoS), 802.1Q
- OAM Service OAM (802.1ag / Y.1731)
- Link OAM (802.3ah)
- Ethernet Ring Protection (G.8032)
- Ethernet Linear Protection (G.8031)
- Link Aggregation (802.3ad)

Synchronizacja

- Synchronous Ethernet IEEE 1588v.2

Typ interfejsu

- Miedziany 10/100/1000BaseX
- Optyczny MMF - 1000BaseSX
- SMF - 1000BaseLX

Zarządzanie

- CLI,
- SNMP

Zasilanie

- Napięcie 48 VDC
- Pobór energii 20 W

3.2 Sieci łączności dzierżawione i zasady korzystania z usług w sieciach operatorskich

Komercyjne dzierżawienie infrastruktury telekomunikacyjnej od innych operatorów sieci może stanowić element projektów sieci łączności dla systemów ITS. Szczególnie w miejscach, gdzie jest dostępna sieć, a koszty dzierżawy są niskie. W miejscach, gdzie nasycenie infrastrukturą ITS będzie niewielkie należy wybierać rozwiązania bazujące na dzierżawie lub na wykorzystaniu standardowych usług telekomunikacyjnych oferowanych przez komercyjnych operatorów.

W trakcie budowy sieci dedykowanych dla celów systemów ITS należy również przewidywać możliwość przeznaczenia na dzierżawę podmiotom zewnętrznym nadmiarów włókien lub kanalizacji kablowej. Te elementy mogą być udostępniane operatorom telekomunikacyjnym również na zasadzie wzajemności – za udostępnienie przez nich swojej infrastruktury w innych lokalizacjach. To może stanowić istotny element obniżenia kosztów budowy i eksploatacji sieci łączności dla ITS.

3.2.1 Dzierżawa kanalizacji

Dzierżawa kanalizacji umożliwia wykorzystanie już istniejącej kanalizacji kablowej, należącej do innych podmiotów, w celu położenia własnych kabli. Dzierżawiący ponosi koszty dzierżawy.

3.2.2 Dzierżawa kabli

Dzierżawa kabli umożliwia wykorzystanie kabli lub włókien światłowodowych w kablach należących do innych podmiotów. Dzierżawiący ponosi koszty dzierżawy.

3.2.3 Dzierżawa kanałów

Dzierżawa kanałów lub pasma umożliwia wykorzystanie kanałów transmisyjnych o określonych parametrach w kablach należących do innych podmiotów. Dzierżawiający ponosi koszty dzierżawy.

3.2.4 Usługi w sieciach bezprzewodowych

Jednym z większych problemów realizacji sieci łączności w terenie jest zapewnienie komunikacji z elementami przydrożnymi, rozproszonymi w terenie, gdzie nie planuje się budowy dedykowanych systemów łączności. Najbardziej oczywistym i najtańszym rozwiązaniem jest wykorzystanie usług oferowanych przez operatorów sieci komórkowych lub satelitarnych. Wybór usługi dla każdej lokalizacji powinien być poprzedzony szczegółową analizą potrzeb, możliwości technicznych oraz ofert operatorów.

Dostępne są następujące rozwiązania:

- połączenia komutowane wykorzystujące transmisję danych za pomocą modemów w kanałach rozmownych sieci komórkowej
- przesyłanie danych przez modemy wykorzystujące technikę SMSów
- przesyłanie danych wykorzystujące transmisję pakietową

Każda z technik przesyłania danych ma wady i zalety.

W sieciach komórkowych 2 i 3 generacji dotychczasowo preferowane są połączenia głosowe. Natomiast dostęp do sieci komórkowych 4 generacji jest ograniczony terytorialnie do dużych skupisk miejskich. Dla połączeń głosowych rezerwuje się większość dostępnych kanałów (dostępnego pasma). Dla transmisji danych najczęściej rezerwowane jest minimalne pasmo, natomiast jeśli są wolne kanały przeznaczone dla transmisji głosu, to mogą być one chwilowo dodawane do pasma dla transmisji danych. Transmisja pakietowa realizowana jest na zasadzie współdzielenia. To znaczy wszyscy zalogowani do danej stacji bazowej są równouprawnieni do korzystania z kanału transmisji pakietowej. Tak więc dostępna przepływność zmienia się w zasadzie poza kontrolą użytkownika i zależy przede wszystkim od liczby współużytkowników. Transmisja pakietowa jest transmisją dwukierunkową, o innej przepływności w górę sieci i innej do abonenta końcowego.

Inaczej działa przesyłanie przez modemy pracujące w trybie SMS. Tam do przesyłania informacji wykorzystywany jest kanał sygnalizacyjny. Informacje przesyłane są w trybie pakietów SMSowych jednokierunkowo.

Wadami tych trybów pracy w przypadku dużej liczby zalogowanych do sieci urządzeń jest spadek dostępnej przepływności. Również w przypadku dużej liczby połączeń głosowych ograniczane jest, dostępne dla transmisji danych, pasmo. Typową reakcją uczestników ruchu w przypadkach wystąpienia awarii, zablokowania ruchu na drodze itp. jest korzystanie z telefonów komórkowych. Szczególnie obecnie, kiedy wiele systemów wspomaganie kierowcy korzysta z połączeń „on line”. Powoduje to zmniejszanie możliwości transmisyjnych sieci w sytuacjach krytycznych. Może to uniemożliwiać przesyłanie danych do znaków zmiennej treści, przesyłanie danych alarmowych do centrów.

Podobna prawidłowość dotyczy wykorzystywania kanałów SMSowych. Jeśli kanał sygnalizacyjny nie jest przeciążony to modemy przesyłają informacje dosyć szybko. Jeśli kanał sygnalizacyjny jest zajęty (np. przez transmisję innych SMSów to po kilku próbach przekazania SMSa jest on zapamiętywany na serwerze wiadomości i przekazywany po pewnym czasie. Tego typu technika jest zalecana do przekazywania danych niezbyt wrażliwych.

Kanały rozmówne to do niedawna główna technika przesyłania danych w sieciach pierwszej i drugiej generacji. Polega ona na zestawieniu na żądanie połączenia telefonicznego w sieci komórkowej pomiędzy dwoma modemami, które wykorzystują de facto kanał rozmowny. Po zestawieniu połączenia modemy zestawiają sesję i umożliwiają transmisję danych kanałem o przepływności nie przekraczającej 2400 bit/sek. Zaletą tej metody jest kontrola zestawionego połączenia. Jeśli już zostanie zestawione połączenie głosowe to na ogół można zestawzić sesję transmisji danych, a jego przepływność jest pod kontrolą. Wadą tego typu rozwiązania jest konieczność zestawiania połączeń (w sytuacjach kryzysowych może to być problem) oraz koszty ich realizacji wg cennika za połączenia głosowe. Do tej pory najczęściej za czas trwania, chociaż to już się zmieniło – połączenia darmowe w ramach sieci operatora mobilnego. Niestety modemy realizujące połączenia w kanale rozmownym już są bardzo trudno dostępne.

Sieci komórkowe wykorzystują różne technologie i różne pasma częstotliwości. Są to pasmo 450MHz, 900Mhz, 1800MHz i 1900 Mhz. Im mniejsza częstotliwość tym większa może być komórka sieci.

Tab. 2 Typowe parametry dla transmisji danych

Technologia	HSDPA	CDMA	UMTS	EDGE	GPRS
prędkość transmisji danych (górna granica)	7,2 Mb/s	1 Mb/s	384 kb/s	240 kb/s	56 kb/s

Analizując możliwości również trzeba brać pod uwagę takie elementy jak popularność danej usługi. W Polsce taką mało popularną w chwili obecnej usługą jest sieć CDMA oferowana przez ORANGE. Jest ona realizowana w paśmie częstotliwości 450MHz dawniej wykorzystywanej w analogowej sieci komórkowej pierwszej generacji. Ze względu na małą popularność tych urządzeń może być to stosunkowo dobry wybór (oczywiście jak na dzień dzisiejszy).

Ponadto istnieją możliwości wykorzystywania łącz satelitarnych (są wykorzystywane w systemie poboru opłat). W tym przypadku dostępne są usługi z gwarancją pasma dla danego użytkownika. Jednak takie połączenia są czułe na zakłócenia przez duże opady śniegu i deszczu.

3.3 Łączność dla urządzeń mobilnych i nomadycznych

Generalnie dla urządzeń nomadycznych i mobilnych najczęściej stosowaną techniką realizacji łączności są techniki radiowe, wykorzystujące dedykowane pasma i urządzenia, bądź bazujące na usługach oferowanych przez operatorów komercyjnych, najczęściej operatorów sieci komórkowych. W przypadku wyboru łączności komórkowej system powinien być tak konstruowany, aby umożliwiać zmianę dostawcy usługi.

3.4 Zasilanie urządzeń w systemach ITS

3.4.1 Generalne zasady zasilania

Omówione szczegółowo w osobnym dokumencie „Zasilanie Elementów Systemu Zarządzania Ruchem”.

3.4.2 Zasady zasilania urządzeń ITS zgrupowanych w obiektach budowlanych

Omówione szczegółowo w osobnym dokumencie „Zasilanie Elementów Systemu Zarządzania Ruchem”.

Proponuje się budowę jednolitego systemu zasilania obejmującego całe otoczenie podlegające infrastrukturze drogowej. Wszelkiego rodzaju wyposażenie należy podzielić na dwie grupy. Jedna grupa to wyposażenie, które nie musi być dołączane do zasilania zapasowego w momencie awarii energetycznych linii zasilających. Druga grupa to urządzenia wymagające zasilania przez określony czas po wystąpieniu awarii.

W celu obniżenia kosztów eksploatacji system zasilania awaryjnego powinien obejmować wszystkie urządzenia wymagające podtrzymania zasilania. System taki powinien być zaprojektowany w ten sposób, żeby zapewniać poprawne zasilanie nawet przy wzroście planowanego zapotrzebowania o 30% (lub inny wskaźnik wskazany przez zamawiającego). System powinien składać się z dwóch elementów – podtrzymania bateryjnego umożliwiającego pracę urządzeń przez co najmniej 10 min oraz z agregatu prądotwórczego automatycznie podejmującego pracę po awarii linii zasilających. Podtrzymanie bateryjne (UPS) powinno działać bezprzerwowo (awaria linii energetycznej nie powinna powodować zaniku napięcia gwarantowanego) i powinno zapewniać buforowe zasilanie do czasu uruchomienia agregatu i osiągnięcia przez agregat parametrów docelowych.

Zasilająca urządzenia ITS sieć energetyczna powinna być wykonana jako podwójna sieć zasilająca, trzyfazowa, o napięciach 240V dla każdej fazy - jedna sieć jako nie gwarantowana, druga rozpraszająca napięcie gwarantowane.

3.4.3 Zasady zasilania urządzeń w terenie

Omówione szczegółowo w osobnym dokumencie Zasilanie Elementów Systemu Zarządzania Ruchem

3.4.3.1 Urządzenia zgrupowane w pobliżu węzłów

W przypadku zgrupowania urządzeń w pobliżu węzłów drogowych należy dążyć do budowy jednolitego systemu zasilania, w tym wraz z zasilaniem rezerwowym. Na ogół węzły drogowe na autostradach muszą być oświetlone. Tak samo wszelkiego rodzaju Miejsca Poboru Opłat – MPO, czy Obwody Utrzymania Autostrady – OUA. W takich miejscach lub w ich bliskiej odległości montuje się najwięcej sprzętu systemów ITS.

Proponuje się budowę jednolitego systemu zasilania obejmującego całe otoczenie podlegające infrastrukturze drogowej. Wszelkiego rodzaju wyposażenie należy podzielić na dwie grupy. Jedna grupa to wyposażenie, które nie musi być dołączane do zasilania zapasowego w momencie awarii energetycznych linii zasilających. Druga grupa to urządzenia wymagające zasilania przez określony czas po wystąpieniu awarii.

W celu obniżenia kosztów eksploatacji system zasilania awaryjnego powinien obejmować wszystkie urządzenia wymagające podtrzymania zasilania. System taki powinien być zaprojektowany w ten sposób, żeby zapewniać poprawne zasilanie nawet przy wzroście planowanego zapotrzebowania o 30% (lub inny wskaźnik wskazany przez zamawiającego). System powinien składać się z dwóch elementów – podtrzymania bateryjnego umożliwiającego pracę urządzeń przez co najmniej 10 min oraz z agregatu prądotwórczego automatycznie podejmującego pracę po awarii linii zasilających. Podtrzymanie bateryjne (UPS) powinno działać bezprzerwowo (awaria linii energetycznej nie powinna powodować

zaniku napięcia gwarantowanego) i powinno zapewniać buforowe zasilanie do czasu uruchomienia agregatu i osiągnięcia przez agregat parametrów docelowych.

Sieć energetyczna, zasilająca urządzenia ITS, powinna być wykonana jako podwójna sieć zasilająca, trzyczasowa, o napięciach 240V dla każdej fazy - jedna sieć jako nie gwarantowana, druga rozprowadzająca napięcie gwarantowane. Ze względu na duże odległości (np. do znaków zmiennej treści około 2km) zasilanie gwarantowane powinno być napięciem wysokim (240V) gdyż to ograniczy średnicę przewodów zasilania.

Zastosowanie centralnego systemu zasilania gwarantowanego pozwala na długie czasy podtrzymania (z wykorzystaniem agregatów prądotwórczych) przy stosunkowo umiarkowanych kosztach eksploatacji. Pozwala też na łatwiejszą eksploatację, utrzymanie i kontrolę urządzeń zasilających.

4. Testy , dokumentacja, szkolenia

4.1.Dokumentacja, Testowanie i Szkolenia

Wykonawca powinien dostarczyć co najmniej następującą dokumentację w postaci elektronicznej:

- Instrukcja użytkowania i konserwacji
- Specyfikacja fabrycznych testów zdawczo-odbiorczych - FAT
- Specyfikacja testów zdawczo-odbiorczych na miejscu - SAT
- Dokumentacja BHP.

Dokumenty powyższe powinny być dostarczone w języku polskim.

Wszelkiego rodzaju szczegółowe dokumentacje techniczne, szczegółowe instrukcje do sprzętu mogą być dostarczone w języku angielskim.

4.2 Instrukcja Użytkowania i konserwacji

Szczegółowa zawartość tego dokumentu powinna zostanie uzgodniona z Zamawiającym po fabrycznych testach zdawczo-odbiorczych a przed testami zdawczo-odbiorczymi na miejscu. Dokument taki powinien zawierać następujące części:

- Instrukcja dla operatora
- Rysunki wszystkich nowych tras kablowych i rozmieszczenia specjalistycznych urządzeń
- Procedury konserwacji.

4.3 Dokumentacja fabrycznych testów zdawczo-odbiorczych (FAT)

Co najmniej na 4 tygodnie przed proponowanym programem fabrycznych testów zdawczo odbiorczych Wykonawca powinien przedłożyć Zamawiającemu harmonogramy testów oraz szczegółowy wykaz/harmonogram kontroli i testów zdawczo-odbiorczych do zatwierdzenia. Celem testów FAT jest zademonstrowanie zamawiającemu, że proponowane rozwiązania techniczne realizują wymagania sprecyzowane w Specyfikacji Istotnych Warunków Zamówienia (SIWS). Zatwierdzenie przez zamawiającego takiego harmonogramu nie spowoduje ograniczenia możliwości kontroli i testów tylko do tych wstępnie

zatwierdzonych; jeżeli w trakcie realizacji testów okaże się, że są one niewystarczające do wykazania, że system spełnia warunki Kontraktu to zakres testów może zostać poszerzony.

Wykonawca powinien udostępnić wszelkie wymagane instrumenty, symulatory i dodatkowe urządzenia lub przyrządy, a także personel do przeprowadzenia testów FAT. Testy FAT mogą być realizowane na sprzęcie podobnym do przewidzianego w projekcie, które będzie realizował te same funkcjonalności co sprzęt docelowy. Miejsce realizacji testów FAT powinno być wskazane przez dostawcę

Testy FAT mogą być przeprowadzane dla każdej dużej części składowej lub podsystemu w oparciu o oddzielne specyfikacje testów. Zamawiający może odstąpić od testów tych parametrów, dla których wykonawca przedstawi dokumenty badań wykonanych w laboratoriach własnych lub laboratoriach jednostek certyfikujących.

Testy powinny obejmować sprawdzenie wszystkich istotnych parametrów operacyjnych i funkcjonalnych zawartych w SIWSie w tym również parametry niezawodnościowe oraz stabilność systemu a także testy sprawdzające wymogi środowiskowe i fizyczne.

4.4 Dokumentacja testów zdawczo-odbiorczych na miejscu (SAT)

Celem testów zdawczo odbiorczych (SAT) jest sprawdzenie całych podsystemów i/lub całego systemu w zakresie realizacji funkcji i parametrów wyspecyfikowanych w SIWSie. Testy te wykonywane będą na sprzęcie zainstalowanym w ramach prowadzonego projektu

Wykonawca powinien przedstawić Zamawiającemu, przed końcowym odbiorem systemu, wyniki własnych testów przedkontrolnych oraz szczegółowy wykaz/harmonogram kontroli i testów zdawczo-odbiorczych do zatwierdzenia.

Wykonawca powinien dostarczyć wszelkie wymagane instrumenty, symulatory i dodatkowe urządzenia lub przyrządy, a także personel do przeprowadzenia testów.

Dla każdej dużej części składowej lub podsystemu powinny zostać dostarczone oddzielne specyfikacje testów.

Testy powinny obejmować sprawdzenie wszystkich istotnych parametrów operacyjnych i funkcjonalnych zawartych w SIWSie w tym również parametry niezawodnościowe oraz stabilność systemu a także testy sprawdzające wymogi środowiskowe i fizyczne.

4.5 Szkolenia

Wykonawca powinien zapewnić wszechstronne szkolenia w zakresie wszystkich części systemu, w tym dla następujących grup:

- Operatorów
- Ekip obsługi
- Operatorów stacji roboczych / terminali
- Personelu Zamawiającego.

Wykonawca powinien przedstawić program szkoleń wskazujący na grupy pracowników, których uczestnictwo jest zalecane.. Czas trwania, terminy i program szkoleń zostaną uzgodnione z Zamawiającym.

5. Utrzymanie i zarządzanie

Bardzo ważnym aspektem każdego systemu ITS jest jego poprawna praca przez wiele lat eksploatacji. Oczekuje się, że systemy ITS powinny być eksploatowane co najmniej kilkanaście lat. Systemy ITS są systemami rozległymi terytorialnie, w ich skład wchodzi wiele różnych podsystemów wykorzystujących bardzo zróżnicowane technologie

Szczegółowe omówienie zagadnień utrzymania i zarządzania zawarto w dokumencie: „Zarządzanie i utrzymanie infrastruktury sprzętowej i programowej KSZR”.

SYSTEM PRZYDROŻNEJ TELEFONII
ALARMOWEJ

1. WSTĘP	55
1.1 Przedmiot Specyfikacji Technicznej	55
1.2 Zakres robót objętych ST	55
2. WŁAŚCIWOŚCI FUNKCJONALNO-UŻYTKOWE SPTA	55
2.1 Lokalizacje	56
2.2 Kolumna alarmowa SOS	56
2.2.1 Opis ogólny	56
2.2.2 Materiały	57
2.2.3 Budowa	57
2.2.4 Funkcje użytkowe	58
2.2.5 Zasilanie	58
2.2.6 Zdalny Serwis	60
2.2.7 Instalacja	60
2.3 Medium transmisyjne i sposób łączności	60
2.4 Urządzenia centralne Systemu Przydrożnej Telefonii Alarmowej	61
2.5 Rejestrowanie zdarzeń	63
2.6 Raporty	63
3. WYMOGI FUNKCJONALNE	64
3.1 Urządzenia przydrożne	64
3.1.1 Nawiązanie i przerwanie połączenia	64
3.1.2 Odbieranie połączenia	64
3.1.3 Odbieranie i przerywanie połączeń przez operatora	64
3.1.4 Zawieszenie połączenia	65
3.1.5 Nawiązywanie połączeń	65
3.1.6 Przekierowywanie połączeń	65
3.1.7 Funkcje konserwacji	65
3.1.8 Niezawodność i dostępność systemu	66
4. PRZEPISY ZWIĄZANE	67
4.1 Normy	67
4.2 Rozporządzenia	68
4.3 Specyfikacje związane	69

1. Wstęp

1.1 Przedmiot Specyfikacji Technicznej

Przedmiotem niniejszej ST (specyfikacji technicznej) są wymagania dotyczące wykonania **Systemu Przydrożnej Telefonii Alarmowej (SPTA)** na autostradach oraz drogach ekspresowych.

System Przydrożnej Telefonii Alarmowej będzie:

- Umożliwiać operatorom odbieranie wezwań przesyłanych z kolumn alarmowych;
- Umożliwiać komunikację użytkowników autostrady z operatorami.

1.2 Zakres robót objętych ST

Ustalenia zawarte w niniejszej ST obejmują wymagania w stosunku do infrastruktury technicznej oraz konstrukcyjno-budowlanej dla elementów SPTA, zgodnie z zakresem podanym w niniejszej specyfikacji.

Wymagania dla SPTA obejmują w szczególności:

- Kolumny alarmowe usytuowane wzdłuż autostrady i/lub dróg ekspresowych na platformach przy poboczu drogi.
- System nadzoru łączności alarmowej (SPTA) zlokalizowany w pomieszczeniach Centrów Zarządzania.
- Serwer komunikacyjny pośredniczący pomiędzy kolumnami alarmowymi a Centrami Zarządzania,
- Medium transmisyjne zapewniające połączenie pomiędzy kolumnami alarmowymi a systemem nadzoru łączności alarmowej.

2. Właściwości funkcjonalno-użytkowe SPTA

SPTA obejmuje następujące elementy:

- kolumny alarmowe SOS, rozmieszczone nie rzadziej niż co 2 km na drodze po obu jej stronach.
- medium transmisyjne - zaleca się jako rozwiązanie docelowe stosowanie kabla światłowodowego jednodomowego, ułożonego wzdłuż odcinka autostrady i/lub drogi ekspresowej,

- serwer komunikacyjny umożliwiający prowadzenie rozmów pomiędzy kolumnami SOS a dyspozytorem w CZ oraz łączenie się z zewnętrznymi służbami ratowniczymi poprzez odpowiednie interfejsy komunikacyjne,
- System nadzoru przydrożnej telefonii alarmowej prezentujący graficznie rozmieszczenie kolumn SOS wzdłuż całego nadzorowanego odcinka autostrady i/lub drogi ekspresowej, jak również sygnalizujący wywołania i alarmy z poszczególnych kolumn SOS.
- Wyniesione stanowisko operatorskie

2.1 Lokalizacje

Elementy terenowe SPTA, czyli kolumny SOS zostaną zlokalizowane wzdłuż drogi na specjalnie przygotowanych platformach w odległości nie przekraczającej 2km pomiędzy sobą. Urządzenia terenowe zostaną podłączone do głównej kanalizacji kablowej biegnącej wzdłuż drogi. Podsystem Zarządzający zostanie zlokalizowany przy wybranym Systemie Zarządzającym i z nim zintegrowany w wybranym i wskazanym przez Zamawiającego Centrum Zarządzania.

2.2 Kolumna alarmowa SOS

2.2.1 Opis ogólny

Kolumna SOS jest wolno stojącym urządzeniem służącym do wzywania pomocy na autostradzie i/lub drodze ekspresowej podczas zaistniałych zdarzeń awaryjnych lub wypadków poprzez dwustronną komunikację z dyspozytorem w Centrum Zarządzania i/lub odpowiednimi służbami ratunkowymi.

Kolumna alarmowa będzie:

- Nadawała się do instalacji przydrożnej pod kątem bezpieczeństwa na wypadek jej przewrócenia w wyniku uderzenia;
- Łatwo widoczna i łatwa do znalezienia przez użytkowników autostrady (przy świetle dziennym, w ciemności i w warunkach słabej widoczności);
- Łatwo zauważalna pod względem jej lokalizacji i kierunku jazdy;
- Łatwa w obsłudze i nie wymagająca używania rąk w trakcie rozmowy (zestaw głośnomówiący);

- Wykorzystywać techniki odfiltrowania odgłosów tak, aby jakość głosu zarówno użytkownika kolumny alarmowej jak i operatora centrum kontroli spełniała odpowiedni standard umożliwiający swobodne prowadzenie rozmów w głośnych warunkach;
- Posiadać głośną i widoczną sygnalizację przychodzących połączeń;
- Posiadać instrukcje użytkownika w językach polskim i angielskim oraz uniwersalną postać graficzną.

2.2.2 Materiały

Kolumna SOS powinna być wykonana z materiałów odpornych na działanie czynników atmosferycznych, środowiskowych i spełniać jednocześnie wymogi Rozporządzenie Ministra Infrastruktury z dnia 16 stycznia 2002 r. w sprawie przepisów techniczno-budowlanych dotyczących autostrad płatnych (&-107).

Stalowe elementy konstrukcyjne kolumny (tj. np. podstawa kolumny (stopa), maszt wsporczy panelu solarnego) należy chronić warstwą ocynku o grubości min. 70 mikronów oraz zastosować powłoką malarską (malowanie proszkowe). Pozostałe elementy wewnątrz obudowy kolumny zastosować jako ocynkowane i/lub ze stali nierdzewnej jak również ze stopu aluminium lub z innych materiałów odpornych na warunki środowiskowe.

2.2.3 Budowa

Kolumna SOS powinna zawierać wyprofilowaną podstawę (stopę), która służy do przykręcenia jej na odpowiednio przygotowanym fundamencie na platformie SOS. Podstawa kolumny winna być połączona śrubami z obudową kolumny w sposób niewidoczny z zewnątrz (brak dostępu do śrub z zewnątrz).

Każda kolumna SOS winna zawierać odpowiednio zabezpieczoną przed kradzieżą komorę (poprzez zastosowanie wkładek zamkowych na klucz) na umieszczenie wyposażenia elektronicznego, baterii zasilającej oraz przyłącza światłowodowego i kablowego. Na zewnątrz obudowy oprócz wkładki zamkowej, przycisków i elementów funkcjonalnych kolumny alarmowej nie mogą być umieszczone łatwo dostępne połączenia śrubowe umożliwiające ich demontaż przez osoby niepowołane.

Kolumna alarmowa SOS, posiadać będzie odpowiednią zabezpieczoną obudowę na umieszczenie wyposażenia elektronicznego, baterii zasilających oraz przyłącza światłowodowego kablowego.

2.2.4 Funkcje użytkowe

Kolumna musi być łatwo zauważalna pod względem jej lokalizacji i kierunku jazdy. Będzie zawierać widoczne oznakowanie wskazujące na jej przeznaczenie - SOS.

Na kolumnie będzie znajdował się prosty i czytelny opis wraz z piktogramem opisującym uruchomienie wezwania pomocy.

Każda kolumna SOS będzie opisana numerem zgodnym z jej lokalizacją i w uzgodnieniu z Zamawiającym.

Kolumna SOS posiadać będzie układ rozmówny głośnomówiący oraz przycisk inicjujący połączenie z CZ w celu zawiadomienia o zdarzeniu oraz wezwania pomocy.

Układ rozmówny musi charakteryzować się dobrymi parametrami jakości prowadzonej rozmowy i nie może być zakłócony szumami i dźwiękami pochodzącymi z autostrady.

Na jakość działania układu nie mogą mieć negatywnego wpływu również warunki atmosferyczne.

Kolumna SOS winna być wyposażona w układ testujący sprawność działania odvodu rozmównego oraz stanu naładowania baterii zasilających. W przypadku niesprawności zostanie wysłany odpowiedni sygnał do SNPTA.

Układy elektroniczne w kolumnach SOS odpowiedzialne za przesyłanie głosu będą wykonane w odpowiedniej technologii pozwalające na wykorzystanie rozwiązań VOiP. Całość wyposażenia elektronicznego jak i oprogramowanie w kolumnach SOS, musi być w pełni kompatybilna z SNPTA.

2.2.5 Zasilanie

Kolumny powinny posiadać zasilanie własne – kolumny winny być w pełni autonomiczne. Para kolumn (główna –wtórna), winna być zasilana baterią lokalną doładowywaną alternatywnymi źródłami energii lub z sieci energetycznej. Nie wprowadza się żadnych regulacji co do typów stosowanych źródeł alternatywnych (np. ogniwa PV, turbiny wiatrowe

itp.), oraz wykorzystywanego magazynu energii (np. baterie akumulatorów, baterie superkondensatorów etc.). W przypadku stosowania akumulatorów muszą to być jednak urządzenia bezobsługowe, ze stałym elektrolitem przystosowane do pracy w pomieszczeniach zamkniętych (np. żelowe, AGM).

Wybór zastosowanych źródeł energii odnawialnej i rodzaju magazynów energii musi zostać poprzedzony staranną analizą uwzględniającą kwestie ekonomiczne, środowiskowe oraz funkcjonalne. Autonomia zasilania kolumn K-SOS z własnego magazynu energii (przy założeniu braku doładowywania) powinna wynosić min. 30 dni, przy założeniu prowadzenia trzech 4-ro minutowych rozmów dziennie. Okres regeneracji magazynu energii (odtworzenia zakładanej autonomii zasilania), nie powinien być większy niż 40 dni w sezonie zimowym i 4 dni w sezonie letnim. Urządzenia muszą monitorować stan naładowania magazynów energii i alarmować przekroczenie progów 50, 30 i 20% (lub inne zaakceptowane przez zamawiającego) magazynowanej energii maksymalnej i muszą umożliwiać zdalny dostęp do informacji o stanie naładowania magazynów energii (na żądanie).

W przypadku stosowania do zasilania baterii (nieładownych) należy zapewnić poprawną pracę urządzeń przy założeniu prowadzenia trzech 4-ro minutowych rozmów dziennie, przez okres 6-ciu miesięcy.

Ze względu na wymaganą energooszczędność działania system kolumn SOS przy autostradzie i/lub drodze ekspresowej powinien być wykonany w parowanym układzie - kolumna główna (master) – kolumna wtórna (slave).

Urządzenia elektroniki i układów rozmównych, winny być tak zoptymalizowane, aby pobór mocy był minimalny. Magazyn energii ładowany powinien być z nadwyżki energii produkowanej przez układ zasilania, bez konieczności jego wymiany w celu utrzymania ciągłości pracy systemu.

W celu zapewnienia wysokiej niezawodności działania SPTA docelowa pojemność znamionowa magazynu energii powinna być co najmniej o 50% większa od pojemności obliczonej dla pokrycia zakładanej autonomii zasilania, szczególnie w warunkach zimowych.

W przypadku stosowania stacjonarnych baterii ogniw fotowoltaicznych, należy zapewnić orientację umożliwiającą maksymalne wykorzystanie padającego promieniowania słonecznego, dla miesięcy zimowych. Kąt instalacji baterii ogniw musi również zapewniać łatwe zsuwanie się płatów śniegu zalegających na powierzchni paneli, w miesiącach zimowych. Nie dopuszcza się zamocowania panelu solarnego w pozycji poziomej, która

zmniejsza wydajność panelu lub całkowicie ją ogranicza w okresie zimowym i w sytuacji zalegania na nim warstwy śniegu.

2.2.6 Zdalny Serwis

Kolumna alarmowa SOS musi być wyposażona w układ testujący sprawność działania obwodu rozmównego, oraz stanu naładowania magazynów energii. W przypadku niesprawności powinien zostać wysłany odpowiedni sygnał do centrum zarządzania. Wszelkie nieprawidłowości w działaniu systemu winny być natychmiast wyraźnie sygnalizowane w CZ.

2.2.7 Instalacja

Połączenie poszczególnych par kolumn alarmowych tj. kolumna główna (master) z kolumną zależną (slave), mogą być wykonane wieloparowym kablem miedzianym ułożonym w kanalizacji kablowej pod jezdniami drogi. Pary kolumn alarmowych mogą być zasilane ze wspólnego źródła zasilania.

Wszystkie kolumny alarmowe główne (master) powinny być włączone do wydzielonych włókien kabla światłowodowego ułożonego wzdłuż autostrady i/lub drogi ekspresowej poprzez odpowiednie elementy optyczne, które nie wymagają zasilania.

2.3 Medium transmisyjne i sposób łączności

Medium transmisyjne zapewnia połączenie pomiędzy kolumnami alarmowymi SOS serwerem komunikacyjnym. Zalecany medium transmisyjnym jest kabel światłowodowy jednomodowy ułożony wzdłuż autostrady i/lub drogi ekspresowej w odpowiednio wybudowanej kanalizacji wraz z całą infrastrukturą towarzyszącą po wybranej stronie drogi.

System łączności alarmowej winien być oparty na założeniu komunikowania się kolumn alarmowych SOS z serwerem VoIP zlokalizowanym w pobliżu obsługiwanego odcinka drogi. Komunikacja pomiędzy serwerem komunikacyjnym a centrami, gdzie pracują operatorzy powinna być realizowana za pomocą sieci transmisji danych w sposób gwarantujący poprawną pracę systemu łączności alarmowej

Należy preferować budowę pasywnej sieci PON (passive optical network), wykorzystującej instalowane na magistrali światłowodowej elementy optyczne (splitery), które sumują lub rozgałęziają sygnały optyczne w sposób pasywny (nie wymagają zasilania). (Uwaga: służą one do tego, żeby dołączone urządzenia, gdy są w trybie nieaktywnym nie zakłócały transmisji do pozostałych urządzeń dołączonych do tego samego włókna światłowodowego – komunikacja punkt-wielopunkt).

Parametry splitterów powinny zostać określone na etapie projektowania wybranego odcinka systemu SPTA. Przyłącza po stronie kolumny alarmowej głównej powinno być zakończone w taki sposób, aby umożliwiało to szybkie włączenie kolumny do systemu.

2.4 Urządzenia centralne Systemu Przydrożnej Telefonii Alarmowej

Urządzenia centralne Systemu Przydrożnej Telefonii Alarmowej (SPTA) będą charakteryzowały się następującymi właściwościami technicznymi i funkcjonalno-użytkowymi:

- a) Elementem centralnym sterującym pracą systemu będzie serwer komunikacyjny wykorzystujący rozwiązanie VOIP. Serwer będzie urządzeniem w pełni integralnym z kolumnami alarmowymi SOS pod względem sygnalizacji i protokołów komunikacyjnych. Serwer będzie obsługiwał następujące urządzenia peryferyjne:
 - konsolę dyspozytorską,
 - urządzenie wizualizujące nadzorowany odcinek autostrady i/lub drogi ekspresowej w postaci graficznego rozmieszczenia kolumn alarmowych SOS,
 - rejestrator rozmów,
 - urządzenie archiwizujące kolejność wywołań i zdarzeń na magistrali SOS,
 - serwer będzie wyposażony w interfejs do współpracy poprzez telefoniczną centralę PABX lub bezpośrednie połączenia z zewnętrznymi służbami ratowniczymi.

Serwer będzie posiadał możliwości rekonfiguracji w przypadku powiększenia ilości obsługiwanych kolumn alarmowych SOS na kolejnych odcinkach autostrady i/lub drogi ekspresowej.

- b) Konsola dyspozytorska powinna być wyposażona w układ rozmówny słuchawkowy i głośnomówiący do prowadzenia rozmowy z kolumnami alarmowymi SOS oraz zewnętrznymi służbami ratowniczymi.

Konsola dyspozytorska powinna umożliwiać:

- Alarmowanie operatora (lub operatorów) o konieczności odebrania połączenia z kolumny
- alarmowej oraz będą wskazywać miejsce i kierunek ruchu użytkownika kolumny alarmowej;
- Odbieranie połączenia przez operatora;
- Zawieszanie rozmowy przez operatora i odbieranie innych połączeń lub łączenie się z innymi
- kolumnami alarmowymi;
- Nawiązywanie połączenia z kolumną alarmową;
- Przekierowywanie połączenia przez operatora na publiczną linię telefoniczną lub na linię
- wewnętrznego systemu PABX;
- Określanie błędów w systemie i zgłaszanie ich do operatora;
- Graficzną prezentację autostrady i opis statusu kolumn alarmowych przy pomocy prostych
- form graficznych i kolorów;
- Udostępniały odpowiednie urządzenia pozwalające na testowanie oraz wyszukiwanie błędów i
- naprawę systemu.

Centrum Kontroli będzie posiadać co najmniej 2 wyposażone stanowiska operatorów umożliwiające obsługę powyższych funkcji.

Konsola ma być wyposażona w przyciski lub ikony ekranowe umożliwiające nawiązanie bezpośredniego połączenia ze służbami ratowniczymi. Dyspozytor ma decydować o rozłączeniu połączeń z kolumnami alarmowymi SOS.

- c) urządzenia centralne Systemu Przydrożnej Telefonii Alarmowej (SPTA) powinny być zasilane napięciem gwarantowanym (opisanym w dokumencie dotyczącym zasilania systemu KSZR).

2.5 Rejestrowanie zdarzeń

Wszystkie zdarzenia i czynności wykonywane w ramach Systemu Łączności Alarmowej powinny być rejestrowane na nośnikach pamięci masowej. Powyższe zdarzenia i czynności obejmują m.in.:

- ☐ ☐ Wszelkie zmiany statusu urządzeń i systemu;
- ☐ ☐ Zapewnienie możliwości rejestrowania alarmów i błędów oraz eksportowania szczegółowych informacji o takich alarmach i błędach;
- ☐ ☐ Wszelkie czynności wykonywane przez operatorów
- ☐ ☐ Wszelkie zmiany w konfiguracji.

Rejestry muszą zawierać informacje o dokładnej godzinie i dacie oraz – jeśli potrzeba – szczegółowe informacje na temat operatora. Rejestry muszą być utrzymywane w sposób umożliwiający przeszukiwanie ich przy pomocy narzędzi bazy danych.

2.6 Raporty

System będzie udostępniać wszechstronne funkcje w zakresie przygotowywania raportów. Funkcje te umożliwią wcześniejsze zdefiniowanie standardowych godzinnych, dziennych, miesięcznych, rocznych itd. raportów generowanych zgodnie z życzeniem Zamawiającego. System umożliwi również definiowanie szybkich raportów w trybie off-line z wykorzystaniem wszelkich rodzajów informacji dostępnych w systemie. Funkcja ta obejmuje możliwość generowania raportów z krzyżowymi tabulacjami, raportów z filtrami, raportów dla określonych zakresów dat i czasu itp.

Należy zapewnić możliwość definiowania formatu wszystkich raportów tak, aby pozwalały one na włączenie do nich wyników w tabelach, formie graficznej lub innych formach, a także na ich eksportowanie do arkuszy kalkulacyjnych lub baz danych

Obsługa funkcji związanych z raportami w żaden sposób nie może wpływać na funkcje łączności alarmowej. I odwrotnie, na czas reakcji funkcji związanych z raportami nie może wpływać obciążenie systemu łączności alarmowej.

3. Wymogi funkcjonalne

System Łączności Alarmowej powinien być systemem autonomicznym działającym na określonym odcinku autostrady lub drogi. System musi zostać zaprojektowany i wdrożony w sposób modułarny, przy zastosowaniu nowoczesnych technik sprzętowych i technik programowania umożliwiających jego modyfikowanie bez konieczności wprowadzania zasadniczych zmian w sprzęcie i oprogramowaniu urządzeń centralnych. Musi także istnieć prosta możliwość rozbudowy systemu poprzez instalację dodatkowych urządzeń przydrożnych i modyfikacji danych konfiguracyjnych w granicach 30%.

3.1 Urządzenia przydrożne

3.1.1 Nawiązanie i przerwanie połączenia

Użytkownik kolumny alarmowej musi mieć możliwość nawiązania połączenia z centrum kontroli. Użytkownik otrzymuje informację, że kolumna alarmowa jest sprawna i że połączenie zostało nawiązane. W przypadku awarii użytkownik powinien otrzymać komunikat słowny w dwóch językach o zaistniałej sytuacji (komunikat ten powinien być odgrywany na zmianę w językach polskim i angielskim).

Użytkownik musi mieć możliwość przerywania połączenia. Jeśli użytkownik nawiązuje połączenie a następnie odchodzi, kolumna alarmowa automatycznie przerwie połączenie po wcześniej zaprogramowanym okresie braku aktywności.

3.1.2 Odbieranie połączenia

Użytkownik będzie miał możliwość odbierania połączenia w kolumnie alarmowej. W kolumnie powinna być sygnalizacja wizualna i głosowa połączenia przychodzącego.

3.1.3 Odbieranie i przerywanie połączeń przez operatora

Operator musi być mieć możliwość odbierania połączeń w dowolnej kolejności, jednakże system powinien wskazać które połączenie jest najstarsze.

Jeśli operator nie może odebrać połączenia, użytkownik powinien usłyszeć nagrany komunikat informujący go o zawieszeniu jego połączenia i że zostanie ono wkrótce odebrane

oraz o tym, że jest on połączony z centrum kontroli. Komunikat ten powinien być odgrywany na zmianę w językach polskim i angielskim. Operator musi mieć możliwość przerywania, zawieszenia i wznowienia połączenia w dowolnej chwili.

3.1.4 Zawieszenie połączenia

Operator centrum kontroli musi mieć możliwość zawieszenia połączenia. W takim przypadku użytkownikowi powinien być odgrywany komunikat informujący go o tym, że połączenie jest zawieszone i że zostanie ono wkrótce odebrane. Komunikat ten powinien być odgrywany na zmianę w językach polskim i angielskim.

3.1.5 Nawiązywanie połączeń

Operator w Centrum Kontroli musi mieć możliwość nawiązania połączenia z dowolną kolumną alarmową.

3.1.6 Przekierowywanie połączeń

Operator centrum kontroli musi mieć możliwość przekierowywania wszelkich połączeń na:

- innego operatora;
- Zewnętrzną publiczną linię telefoniczną;
- Wewnętrzną linię poprzez wewnętrzną centralę PABX.

3.1.7 Funkcje konserwacji

System powinien umożliwiać operatorowi sprawdzenie kolumny alarmowej przy pomocy prostego mechanizmu. Zalecany jest mechanizm polegający na teście pętli sprawdzającym ścieżkę dźwięku z dowolnej kolumny alarmowej i z powrotem.

System powinien być wyposażony w dodatkowe funkcje pozwalające personelowi obsługi na sporządzanie raportów o awariach, znajdowanie awarii oraz naprawę wszystkich części systemu.

3.1.8 Niezawodność i dostępność systemu

Niezawodność całego systemu łączności alarmowej jest najważniejszym wymogiem. Wykonawca powinien wykazać niezawodność projektu w następujący sposób:

- analiza elementów systemu i obliczenia mające na celu określenie dostępności systemu, średniego czasu pomiędzy awariami (MTBF – mean time between failures) oraz innych wskaźników niezawodności; także analiza rodzajów i skutków awarii obejmująca wszystkie elementy systemu do poziomu poszczególnych obwodów drukowanych lub elementów mechanicznych;
- testowanie i przedstawienie parametrów poszczególnych elementów systemu (fabryczny test zdawczo-odbiorczy (FAT) oraz test zdawczo-odbiorczy na miejscu (SAT))
- testowanie systemu po maksymalnej, określonej przez zamawiającego rozbudowie, przy pełnej przepustowości i szybkości działania; (szczegółowe parametry testów powinien dostarczyć wykonawca w celu zaakceptowania przez zamawiającego).
- testowanie w stanie poważnych awarii, w celu sprawdzenia działania zabezpieczeń i urządzeń redundantnych; testy powinny wykazać, że w takich sytuacjach parametry systemu mieszczą się w założeniach projektu (szczegółowe parametry testów powinien dostarczyć wykonawca w celu zaakceptowania przez zamawiającego).

4. Przepisy związane

4.1 Normy

1. PN-E-05125	Elektroenergetyczne i sygnalizacyjne linie kablowe. Projektowanie i budowa.
2. PN-93/E-90401	Kable elektroenergetyczne na napięcie znamionowe 0,6/1 kV
3. PN-E-05033	Wytyczne do instalacji elektrycznych
4. PN-E-79100	Kable i przewody elektryczne
5. PN-EN 61386	Systemy rur instalacyjnych do prowadzenia przewodów
6. PN-EN 61140	Ochrona przed porażeniem prądem elektrycznym. Wspólne aspekty instalacji i urządzeń
7. PN-EN 60529	Stopnie ochrony zapewnianej przez obudowy (kod IP)
8. PN-EN 1329-1	Rury kanalizacyjne z nieplastyfikowanego polichlorku winylu
9. BN-85/8984-01	Telekomunikacyjne sieci kablowe miejscowe. Studnie kablowe. Klasyfikacja i wymiary
10. BN-73/8984-05	Kanalizacja kablowa. Ogólne wymagania i badania
11. BN-74/3233-17	Słupki oznaczeniowe i oznaczeniowo-pomiarowe
12. ZN-96/TPSA-002	Linie optotelekomunikacyjne. Ogólne wymagania techniczne.
13. ZN-96/TPSA-005	Kable optotelekomunikacyjne jednomodowe dalekosiężne. Wymagania i badania.
14. ZN-96/TPSA-006	Linie optotelekomunikacyjne. Złącza spajane światłowodów jednomodowych. Wymagania i badania.
15. ZN-96/TPSA-008	Linie optotelekomunikacyjne. Osłony złączowe. Wymagania i badania.
16. ZN-96/TPSA-011	Telekomunikacyjna kanalizacja kablowa. Ogólne wymagania techniczne.
17. ZN-96/TPSA-012	Kanalizacja kablowa pierwotna. Wymagania i badania.
18. ZN-96/TPSA-013	Kanalizacja wtórna i rurociągi kablowe. Wymagania i badania.
19. ZN-96/TPSA-017	Rury kanalizacji wtórnej i rurociągu kablowego (RHDPE). Wymagania i badania.
20. ZN-96/TPSA-018	Rury polietylenowe (RHDPEp) przepustowe. Wymagania i badania.
21. ZN-96/TPSA-020	Złączki rur kanalizacji kablowej. Wymagania i badania.
22. ZN-96/TPSA-021	Uszczelki końców rur kanalizacji kablowej. Wymagania i badania.

23. ZN-96/TPSA-023	Studnie kablowe. Wymagania i badania.
24. ZN-96/TPSA-025	Taśmy ostrzegawcze i ostrzegawczo-lokalizacyjne. Wymagania i badania.
25. ZN-96/TPSA-026	Słupki oznaczeniowe i oznaczeniowo-pomiarowe. Wymagania i badania.
26. ZN-96/TPSA-041	Zabezpieczone pokrywy studni kablowych, dodatkowe (wewnętrzne). Wymagania i badania.
27. PN-EN 187000	Ogólne wymagania. Kable światłowodowe
28. PN-EN-60825-1	Bezpieczeństwo urządzeń laserowych. Klasyfikacja sprzętu, wymagania i przewodnik użytkownika
29. PN-EN 60825-2	Bezpieczeństwo urządzeń laserowych. Bezpieczeństwo światłowodowych systemów telekomunikacyjnych
30. PN-S-02205	Drogi samochodowe. Roboty ziemne. Wymagania i badania
31. PN-B-06050	Roboty ziemne budowlane. Wymagania w zakresie wykonania i badania przy odbiorze
32. PN-B-19501	Prefabrykaty z betonu. Prefabrykaty żelbetowe dla telekomunikacji
33. PN-80/B-03040	Fundamenty. Konstrukcje wsporcze pod maszty. Obliczenia i projektowanie
34. BN-68/6353-03	Folia kalandrowana techniczna z uplastycznionego polichlorku winylu
35. PN-IEC 610254	Ochrona odgromowa obiektów budowlanych. Zasady ogólne
36. PN-86/E-05003.01	Ochrona odgromowa obiektów budowlanych. Wymagania ogólne
37. EN-ISO 1461	Powlekanie stali warstwą cynku. Metoda cynkowania ogniowego
38. PN-ISO 9501-1	Ochrona przed korozją. Wzorce jakości przygotowania powierzchni stali do malowania
39. PN-EN 61000	Kompatybilność elektromagnetyczna EMC. Metody badań i pomiarów

4.2 Rozporządzenia

Rozporządzenie Ministra Infrastruktury z dnia 16 stycznia 2002r. w sprawie przepisów techniczno-budowlanych dotyczących autostrad płatnych.

4.3 Specyfikacje związane

Standardy protokołów transmisji danych dla systemu zarządzania ruchem

Architektura teletechnicznego powiązania urządzeń w systemach KSZR

Parametry techniczne urządzeń telematyki drogowej

**ZARZĄDZANIE I UTRZYMANIE
INFRASTRUKTURY SPRZĘTOWEJ I
PROGRAMOWEJ KSZR**

1. Wstęp.....	72
2. Bieżąca informacja o posiadanym i eksploatowanym sprzęcie	73
3. Zarządzanie błędami i awariami.....	75
4. Nadzór nad przebiegiem napraw	78
5. Zarządzanie utrzymaniem i eksploatacją	78
6. Kontrola uprawnień i dostępu.....	80
7. Zdalny dostęp i testowanie.....	82
8. Nadzór nad zasobami ludzkimi i planowanie pracy	83
9. Procedury postępowania i kontrola działań	83
10. Organizacja systemu składowania i zamawiania części zapasowych oraz materiałów eksploatacyjnych.....	84

1. Wstęp

Z uwagi na rosnący stopień złożoności układów i urządzeń we współczesnych systemach zarządzania ruchem drogowym oraz długi okres przewidywanej eksploatacji jest konieczne bezwarunkowe uwzględnienie problematyki niezawodności i testowania w ich projektowaniu oraz wszelkiego rodzaju ułatwienia w ich eksploatacji.

Problematyka eksploatacji i utrzymania nie dostatecznie uwzględniana na etapie projektowania i budowy systemów ITS w Polsce. Zamawiający skupia się przede wszystkim na budowie systemu i osiągnięciu zadanych parametrów. Niedostatecznie uwzględniane są potrzeby późniejszej eksploatacji systemów. Związane to jest także z przekazywaniem eksploatacji w ręce wybranych przedmiotów lub organizacji, które często są wskazywane po etapie budowy systemu. Przekazywanie eksploatacji poszczególnych podsystemów lub odcinków dróg do podmiotów zewnętrznych również skutkuje brakiem informacji lub brakiem przepływu informacji o problemach, na jakie natykają się w trakcie praktycznej eksploatacji.

Problemy utrzymania i eksploatacji możemy podzielić na kilka kategorii:

1. Bieżąca informacja o posiadanym i eksploatowanym sprzęcie
2. Zarządzanie błędami i awariami
3. Nadzór nad przebiegiem napraw
4. Zarządzanie utrzymaniem i eksploatacją
5. Kontrola uprawnień i dostępu
6. Zdalny dostęp i testowanie
7. Nadzór nad zasobami ludzkimi i planowanie pracy
8. Procedury postępowania i kontrola działań
9. Organizacja systemu składowania i zamawiania części zapasowych oraz materiałów eksploatacyjnych

Wszystkie te elementy utrzymania i eksploatacji mają bardzo duży wpływ na architekturę systemu oraz projektowanie wszystkich podsystemów ITS a także na przyjęte rozwiązania organizacyjne i wymagania przetargowe.

Systemy ITS są coraz bardziej zaawansowane i zawierają bardzo różne i mocno zaawansowane technologie, w tym elementy systemów informatycznych, elementy

systemów telekomutacyjnych, elementy systemów monitorowania wraz z analizą obrazów, systemy meteo, różnego rodzaju techniki komunikowania się, systemy radiowe itp.. Dlatego też proces eksploatacji tak wielu różnorodnych pod systemów musi być dobrze przemyślany i zorganizowany. Na dodatek nie można założyć, że zamawiający lub organizacje, do których zostanie przekazana eksploatacja, będą posiadać personel, przygotowany do obsługi i napraw wszelkiego rodzaju sprzętu zainstalowanego w ramach systemów ITS.

Wymagania dotyczące sprzętu dla ITS najczęściej określają specyfikacje parametrów niezawodnościowych na dość wysokim poziomie. Dlatego prawdopodobieństwo wystąpienia awarii będzie niskie. Co oznacza rzadkie wystąpienia awarii pojedynczych elementów w podsystemach, a więc utrzymywanie personelu dysponującego zaawansowaną wiedzą dla każdego elementu jest nierealne i ekonomicznie nie uzasadnione. W przypadkach awarii raczej należy korzystać z usług firmy zewnętrznych, wyspecjalizowanych w zakresie danego typu urządzeń i zajmujących się nimi na co dzień – najbardziej zalecana jest współpraca z serwisami producentów.

2. Bieżąca informacja o posiadanym i eksploatowanym sprzęcie

Generalnie w celu prowadzenia poprawnej eksploatacji wymagana jest bieżąca informacja o posiadanym i eksploatowanym sprzęcie. W tym celu powinna zostać stworzona baza danych, w której zostanie zinwentaryzowany cały sprzęt systemów i podsystemów ITS.

Jednocześnie należy podjąć decyzje dotyczące sposobu eksploatacji urządzeń i wskazania miejsca, gdzie będą spływać informacje o stanie urządzeń. W zależności od lokalnych uwarunkowań mogą zostać przyjęte różne rozwiązania. Na odcinkach autostrad, gdzie wybudowano i wyposażono w centra utrzymania, w tych centrach powinny być gromadzone wszelkiego rodzaju informacje obrazujące wyposażenie techniczne oraz jego stan. W przypadku dróg krajowych mogą to być odpowiednie ośrodki regionalne lub systemy ukierunkowane na określony podsystem ITS (np. system poboru opłat).

Zawsze powinno się wybierać takie lokalizacje, w których personel dyżuruje 24 godziny na dobę.

Na stanowisku dyżurnego powinien być zainstalowany terminal pozwalający na przekazywanie informacji o alarmach w podległych mu podsystemach ITS, lub na podległym mu obszarze.

Na autostradach stanowiskiem realizującym tę funkcjonalność powinno być stanowisko dyżurnego ruchu.

Baza danych inwentaryzacyjnych powinna umożliwiać rejestrację wszystkich składników majątkowych w celu śledzenia i prowadzenia ewidencji składników majątkowych oraz ich utrzymania. Przy czym nie należy przesadzać ze szczegółowością takiej bazy danych i nie wymagać rozbierania dostarczonego sprzętu na drobne podzespoły.

Baza taka powinna umożliwiać przechowywanie dokumentów, protokołów i wyników przeprowadzonych testów i kontroli w powiązaniu ze sprzętem i jego lokalizacją.

Personel eksploatacji powinien zapisywać w tej bazie aktualne zmiany stanu każdego składnika majątku. Wyniki kontroli każdego składnika, który podlega okresowym przeglądom, powinny być zapisywane w takim rejestrze.

W bazie danych powinny być umieszczone również informacje na jego temat, w tym:

- określenie położenia na drodze, autostradzie i jezdni lub określenie lokalizacji, budynku i pomieszczenia w celu łatwej zlokalizowania
- ewentualnie numery seryjne lub inne niepowtarzalne identyfikatory pozwalające na kontrolę czasu eksploatacji i śledzenie gwarancji
- dodatkowe listy, umożliwiające definiowanie dodatkowych informacji istotnych dla eksploatacji; np. jeśli składnikiem jest szafa wyposażona w sprzęt to na takiej liście można rejestrować wymianę podzespołów – takie listy powinny być otwarte i umożliwiać dopisywanie i uszczegółowianie w trakcie eksploatacji
- wiek składnika majątku oraz wynik oceny stanu danego składnika.

Pożądanym jest, aby sprzęt ITS mógłby być odpytywany zdalnie z wykorzystaniem standardowego protokołu SNMP ver.3, co umożliwiłoby automatyczną inwentaryzację oraz sprawdzanie stanu urządzeń. Takie podejście zastosowano w USA (NTCIP).

3. Zarządzanie błędami i awariami

Wszelkiego rodzaju urządzenia stosowane w systemach ITS powinny być wyposażone w moduły nadzorujące ich pracę. W przypadku wykrycia nieprawidłowości w ich pracy powinny umożliwiać automatyczne wysyłanie powiadomień o wystąpieniu błędów pod wskazany adres IP. Serwer zbierający informacje o błędach powinien prowadzić log, w którym powinny być gromadzone wszelkie komunikaty o błędach. Serwer ten powinien umożliwiać przekazywanie informacji o określonych błędach na stanowisko operatora.

Na stanowisku operatora powinna być wyświetlana informacja o istotnych błędach i awariach oraz zmiana stanu urządzenia powinna być uwidocznioma na graficznej prezentacji systemu.

Operator powinien mieć możliwość łatwej weryfikacji stanu urządzeń i w zależności od potrzeb przekazać informację do wyspecjalizowanych służb utrzymaniowych zajmujących się danym rodzajem sprzętu. Aplikacja na stanowisku operatora powinna umożliwiać wskazanie, kogo należy powiadomić w przypadku zdefiniowanych klas awarii.

Lokalny system zarządzania błędami powinien umożliwiać eksport danych do systemów nadrzędnych.

W celu kontroli podejmowanych działań na skutek awarii system powinien być wyposażony w odpowiednie narzędzia umożliwiające automatyzację procesu dokumentowania podejmowanych działań jednostkowych i kontroli czasów reakcji służb utrzymaniowych.

Podejmowane działania powinny być adekwatne do poziomu stwierdzonych awarii aby, czas reakcji służb utrzymaniowych był zgodny z wymaganiami zamawiającego.

Czasy reakcji wykonawcy lub służb utrzymaniowych na awarie i wykonanie napraw powinno być podzielone według następującej klasyfikacji:

Poziom 1 – Wykonawca przybędzie na miejsce awarii w ciągu dwóch godzin od momentu zgłoszenia awarii przez jeden z automatycznych systemów zgłaszania awarii lub w dowolny inny sposób, jak np. zgłoszenie awarii przez służby ratownicze lub przez personel Zamawiającego. Awarie zaliczane do Poziomu 1 obejmują następujące sytuacje:

- a) całkowita utrata lub poważne uszkodzenie systemu stwarzające potencjalne zagrożenie życia
- b) sytuacje potencjalnie prowadzące do sytuacji opisanej w punkcie a)
- c) całkowita utrata łączności pomiędzy jedną lub większą liczbą przydrożnych kolumn alarmowych a centrum kontroli
- d) niemożność ustawienia lub zresetowania jednego lub więcej znaków zmiennej treści lub tablic tekstowych o zmiennej treści
- e) całkowita utrata lub pogorszenie jakości obrazów generowanych przez kamery telewizji przemysłowej
- f) brak sygnału alarmowego w wyniku wykrycia zdarzenia przez urządzenia monitoringu ruchu
- g) zabezpieczenie miejsca z jakiegokolwiek powodu, jak np. w wyniku wandalizmu, kradzieży lub uszkodzenia w wyniku wypadku
- h) niemożność pobierania opłat na jednym lub więcej pasach poboru opłat w jednym kierunku lub na placu poboru opłat
- i) niemożność pobierania opłat na dowolnym pasie wyjazdowym na łącznicach
- j) niemożność wydania biletu/ żetonu na jednym lub więcej pasach wjazdowych w jednym kierunku na placu poboru opłat
- k) niemożność wydania biletu/ Źetonu na dowolnym pasie wjazdowym na łącznicy
- l) możliwość utraty ewidencji poboru opłat lub utrata opłat lub gotówki
- m) niemożność transportowania pieniędzy ze stanowisk poboru opłat lub z placów poboru opłat

Poziom 2 – W godzinach 8:30-17:00, Wykonawca przybędzie na miejsce awarii w ciągu dwóch godzin od momentu zgłoszenia awarii przez jeden z automatycznych systemów zgłaszania awarii lub w dowolny inny sposób, jak np. zgłoszenie awarii przez służby ratownicze lub przez personel Zamawiającego. W pozostałych godzinach Wykonawca przybędzie na miejsce awarii do godziny 10:30 następnego dnia. Awarie zaliczane do Poziomu 2 obejmują awarie, które pogarszają lub

wpływają na działanie systemów, z wykluczeniem sytuacji opisanych w punktach a)-m) powyżej.

Poziom 3 – Wykonawca przybędzie na miejsce awarii w następnym dniu roboczym od momentu zgłoszenia awarii przez jeden z automatycznych systemów

zgłaszania awarii lub w dowolny inny sposób, jak np. zgłoszenie awarii przez służby ratownicze lub przez personel Zamawiającego. Awarie zaliczane do Poziomu 3 obejmują awarie drobne, które nie wpływają na działanie systemu, lecz które należy usunąć.

Jeśli awaria zaistniała w wyniku szkody spowodowanej przez strony trzecie (wandalizm, kradzież, wypadek itp.), z przyczyn niezależnych od Wykonawcy, obowiązuje go czas reakcji zgodnie z wymaganiami wymienionymi powyżej.

Każdy operator systemów i podsystemów zainstalowanych w ramach projektu ITS powinien otrzymywać ze swojego systemu informacje w postaci alarmów, logów czy też informacji od personelu obsługującego o awariach i usterkach. Wszystkie zauważone awarie i usterki powinny być przez uprawnionego operatora zweryfikowane i przekazane służbom utrzymaniowym. System powinien umożliwiać zgłoszenie usterki przez każdą osobę z personelu obsługi, która stwierdziła usterkę. Powinno wskazywać podsystem, w którym nastąpiła usterka (wybór domyślnie z listy podsystemów), krótki opis usterki, link lub informacje z loga (jeśli takowe będą dostępne). Taka informacja powinna być przekazana do dyżurnego operatora lub nadzorującego w celu weryfikacji danych oraz poziomu zagrożenia.

Nadzorujący weryfikuje poprawność korelacji usterki z podsystemem oraz koreluje informacje o usterce z poziomem zagrożenia.

Po potwierdzeniu przez nadzorującego poprawności wpisu i korelacji system powinien automatycznie powiadamiać niezbędne służby o zaistniałej sytuacji oraz zaczyna odliczać czas reakcji.

Wskazany przez system i powiadomiony o awarii pracownik służb utrzymaniowych musi potwierdzić przyjęcie zgłoszenia, a po przybyciu na miejsce potwierdzić w systemie podjęcie działań naprawczych.

W przypadku braku potwierdzenia i upływie określonego dla danego zdarzenia czasu reakcji system przekazuje informacje przekroczeniu czasu do wskazanego nadzorującego i może podjąć dalsze akcje eskalacyjne wskazane w systemie.

Pracownik na miejscu awarii powinien podjąć odpowiednie czynności serwisowe. Po zakończeniu działań powinien udokumentować podjęte działania oraz ich rezultat w formie krótkiego opisu. W przypadku konieczności podjęcia dalszych działań w celu usunięcia awarii lub usterki informacja taka powinna być dołączona do opisu. Nadzorujący utrzymanie danego podsystemu powinien uzupełnić wpisy o kolejne daty kontrolne dotyczące usuwania usterki, po to żeby system automatycznie przypominał o kolejnych działaniach.

Przewiduje się również tryb automatyczny wywołania procedury działań awaryjnych i jednostkowych przez niektóre systemy, które w przypadku awarii będą mogły generować automatycznie wiadomości do modułu zarządzania utrzymaniem i moduł będzie mógł wywołać procedury naprawcze bez konieczności zatwierdzenia przez dyżurnego zarządzającego (dyżurny dostanie informacje o awarii i o automatycznym podjęciu działań).

W przypadku wymiany niesprawnych modułów i urządzeń powinny być dokonane odpowiednie wpisy do modułu rejestru stanu majątku opisanego w poprzednim akapicie.

4. Nadzór nad przebiegiem napraw

System powinien umożliwiać dokumentowanie podstawowych czynności i czasów napraw. Istotne jest dokumentowanie następujących elementów:

- Wymiana uszkodzonych elementów
- Kontrola elementów przekazywanych do naprawy
- Kontrola gwarancji w przypadku napraw
- Kontrola magazynu części zapasowych oraz ich położenia
- Prognozowanie zakupów
- Kontrola czasu i kosztów napraw
- Dokumentacja wykonywanych prac

5. Zarządzanie utrzymaniem i eksploatacją

System powinien umożliwiać zarządzanie oraz dokumentowanie czynności realizowanych w ramach utrzymania i eksploatacji.

Czynności te obejmują:

- monitorowanie dzienników i raportów usterek generowanych przez każdy system.
- codzienne kontaktowanie się z operatorami i użytkownikami każdego systemu w celu uzyskania ustnych lub pisemnych raportów na temat powstałych usterek
- wykonywanie kontroli i testów bezpieczeństwa mechanicznego i elektrycznego zgodnie z polskimi przepisami i normami
- przeprowadzanie regularnych kontroli otoczenia urządzeń oraz wykonywanie wszelkich czynności naprawczych koniecznych do utrzymania bezpiecznego dostępu do urządzeń
- wykonywanie bieżących okresowych czynności utrzymaniowych, w tym czyszczenie i sprawdzanie sprawności urządzeń.

System powinien umożliwiać nadzorowanie utrzymania i umożliwiać automatyczne dokumentowanie oraz śledzenie wszystkich czynności utrzymaniowych podlegających nadzorowi, zarówno czynności okresowych jak i czynności związanych z likwidacją błędów i awarii. System powinien kontrolować czasy reakcji oraz działanie personelu. System powinien automatycznie alarmować w przypadku przekroczenia standardowych czasów reakcji lub braków w realizacji okresowych przeglądów utrzymaniowych czy przeprowadzenia wymaganych testów.

Zadaniem modułu będzie zarejestrowanie każdego zdarzenia utrzymaniowego oraz śledzenie podjętych działań.

Pożądane jest aby system automatycznie przypominał o konieczności wykonania okresowych czynności utrzymaniowych, wysyłał przypomnienia lub zlecenia wykonania określonych zestawów czynności do wskazanych pracowników (komórek) odpowiedzialnych za utrzymanie podsystemów ITS. Każdy pracownik wykonujący okresowe czynności utrzymanie będzie musiał potwierdzić wykonanie każdej czynności. Listy czynności powinny być wprowadzone do systemu i

udostępniane pracownikom realizującym utrzymanie w celu potwierdzenia wykonania. Po uruchomieniu procedury utrzymaniowej moduł powinien automatycznie kontrolować jej wykonanie oraz zalecane ramy czasowe do ich realizacji. Do każdej grupy czynności powinien zostać określony czas wykonania. W przypadku nie potwierdzenia wykonania tych czynności w określonych przez system ramach czasowych system będzie ponownie przypominał a następnie a po przekroczeniu kolejnego eskalował do wskazanych nadzorujących.

Jeśli z czynnościami utrzymaniowymi będą związane materiały eksploatacyjne to system powinien określać, jakie materiały powinny zostać pobrane, w jakiej ilości oraz śledzić bieżące ich zapasy (np. płyn niezamarzający do kamer, papier do biletów).

Wykonanie czynności eksploatacyjnych powinno być potwierdzone przez wykonującego. Dodatkowo wykonujący będzie miał możliwość wpisania dodatkowych informacji i zaleceń.

Wpisy o wykonaniu czynności utrzymaniowych sprawdza i analizuje nadzorujący. On też na podstawie wpisanych przez wykonującego informacji i zaleceń może dokonać nowego zlecenia w trybie procedury działań awaryjnych i jednostkowych.

Brak potwierdzenia wykonania okresowych czynności utrzymaniowych w określonym czasie będzie powodował powiadomienie nadzorującego, a po upływie kolejnego odcinka czasu eskalację.

Wypełnione przez wykonawcę dokumenty będą stanowiły podstawę do wygenerowania sprawozdania. Dokumenty te będą przechowywane w systemie i będą skojarzone z elementem majątku.

6. Kontrola uprawnień i dostępu

System ITS wraz z jego podsystemem powinien być wyposażony w moduł kontroli dostępu. Wyposażenie systemu we wspólny moduł kontroli dostępu ułatwi zarządzanie podsystemami i umożliwi wykorzystywanie przypisywanie indywidualnych uprawnień pracownikom. Taki pracownik po zalogowaniu się do sieci

w różnych miejscach i z różnych stacji roboczych będzie mógł uzyskać uprawnienia, które mu zostały nadane. Moduł ten będzie odpowiedzialny za administrowanie systemem. Ten sam mechanizm można wykorzystać do kontroli zdalnego dostępu dla służb serwisowych. Ponadto będzie można ograniczać zakresy działania poszczególnych pracowników zarówno w podziale terytorialnym jak i w podziale funkcjonalnym.

W ramach tego modułu uprawniony operator będzie mógł ustawiać odpowiednie wpisy typu:

- Uprawnienia użytkowników
- Listy użytkowników
- Listy nadzorujących
- Listy eskalacyjne
- Listy wykonawców
- Listy systemów i powiązanie obiektów z systemami (informacja o tym, kto utrzymuje i reaguje na awarie danego elementu)
- Listy instrukcji
- Listy materiałów eksploatacyjnych
- Listy raportów
- Listy czynności okresowych

Każdy administrator i operator będzie miał swój indywidualny identyfikator. Wejście do systemu będzie kontrolowane przez indywidualne hasła. W logach powinna być zapisywana informacja, kto, kiedy i gdzie się zalogował. Zalogowany operator będzie miał dostęp wyłącznie do informacji koniecznych mu do działania. Wszelkie jego istotne działania będą zapisywane w logach. Natomiast zmiany wprowadzane do każdego podsystemu p zawsze powinny być skojarzone z informacją, kto zmianę wprowadził.

Każdy uprawniony pracownik powinien móc się zalogować do systemu za pomocą przeglądarki. Powinno na początku podać swój login i hasło. System po weryfikacji umożliwi mu dostęp do ograniczonych zasobów związanych z jego potrzebami.

Przewiduje się co najmniej kilka poziomów dostępu ze względu na pełnione funkcje.

Przykłady takich poziomów dostępu:

- Pracownik
- Serwisant
- Operator
- Nadzorujący
- Nadzorujący II poziomu
- Administrator
- Superuser
- Ponadto kolejnym podziałem będzie podział na podsystemy np.
- Transmisja
- Meteo
- Łączność alarmowa
- System poboru opłat
- System CCTV
- System sterowania ruchem

7. Zdalny dostęp i testowanie

Z uwagi na rosnący stopień złożoności układów i urządzeń we współczesnych systemach zarządzania ruchem drogowym oraz długi okres przewidywanej eksploatacji konieczne jest zapewnienie możliwości wsparcia specjalistów, posiadających wiedzę na temat poszczególnych urządzeń stosowanych w systemach ITS. Ze względu na rozproszenie tych urządzeń w całym kraju trudno byłoby ściągać takich specjalistów, często spoza kraju, w miejsca instalacji sprzętu. Nie ma również możliwości przygotowania do podejmowania specjalistycznych działań pracowników eksploatacji, zawsze będą mieli mniejsze doświadczenie i mniejszą wiedzę od osób zajmujących się danym sprzętem i jego naprawami na co dzień. Wysokie koszty podróży specjalistów oraz koszty czasu pracy takich osób powodują, że jedynym sensownym rozwiązaniem jest umożliwienie im zdalnego dostępu do sprzętu.

Dlatego też wszystkie urządzenia, z których budowane są systemy ITS powinny być zarządzane i umożliwiać zdalną diagnostykę, natomiast sam system ITS powinien umożliwiać kontrolowany zdalny dostęp poprzez publiczną sieć transmisji danych. Zdalny dostęp powinien być realizowany za pomocą mechanizmów IPSEC. Nie

powinno się dopuszczać do eksploatacji urządzeń, które są niezarządzalne i nie są wyposażone w moduły kontroli i alarmowania.

8. Nadzór nad zasobami ludzkimi i planowanie pracy

Istotnym elementem wpływającym na pracę systemów ITS są ludzie oraz ich wiedza. Ze względów na ciągłość pracy systemów ITS bardzo istotne jest zarządzanie zasobami ludzkimi. System ITS powinien być wyposażony w moduł do planowania pracy oraz zarządzania zasobami. Ten moduł powinien być skorelowany z modułem uprawnień oraz listami pracowników serwisów, w tym serwisów zewnętrznych. Taki moduł pozwoli operatorowi na powiadamianie niezbędnych pracowników, wyszukiwanie właściwych oraz dostępnych osób, szczególnie w sytuacjach kryzysowych. Jednym z zasadniczych celów systemów ITS jest wspomaganie pracy oraz poprawa bezpieczeństwa podróżnych. Dlatego też taki moduł powinien uwzględniać aspekty zarządzania kryzysowego.

9. Procedury postępowania i kontrola działań

System ITS powinien być uzupełniony o procedury postępowania i powinien umożliwiać kontrolę działań oraz dokumentować podjęte działania. Część procedur działań jest wywoływana automatycznie i stanowi integralną część sterowania ruchem. Jest duża grupa procedur, które są procedurami działania na poszczególnych stanowiskach, w szczególnych sytuacjach itp. Najczęściej są one wydane w postaci dokumentów i dostępne w wersjach drukowanych. W sytuacjach kryzysowych trudno je odnaleźć.

Dlatego też powinno się stworzyć bibliotekę takich dokumentów w wersji elektronicznej, dostępną w Intranecie wraz z narzędziami ułatwiającymi wyszukiwanie.

Dotyczy to również dokumentacji systemów, protokołów odbiorczych, rysunków technicznych, map itp.

10. Organizacja systemu składowania i zamawiania części zapasowych oraz materiałów eksploatacyjnych

Z każdym podsystemem skojarzone są odpowiednie części zapasowe oraz materiały eksploatacyjne. Ponieważ urządzenia są rozproszone w terenie istotne jest zarządzanie częściami zapasowymi i ich lokalizacją. To samo dotyczy materiałów eksploatacyjnych. Stworzenie narzędzi do zarządzania tymi elementami podsystemów ITS pozwoli na racjonalizację zasobów, kontrolę ich wykorzystania i rozmieszczenia oraz na planowanie zakupów.

SŁOWNIK TERMINÓW I POJĘĆ GRUPY:

**STANDARD REALIZACJI MEDIÓW DO
ŁĄCZNOŚCI I TRANSMISJI DANYCH KSZR**

KSZR – Krajowy System Zarządzania Ruchem

SAT – On Site Acceptance Test

SLA (Service Level Agreement) –

FAT – Factory Acceptance Test

SIWZ – Specyfikacja Istotnych Warunków Zamówienia

SFP – wkładka odbiornika-nadajnika światłowodowego

POE – Power Over Ethernet

port-based mirroring – dodatkowe kopiowanie wszystkich pakietów z portu obserwowanego do portu pomiarowego

policy-based mirroring – dodatkowe kopiowanie pakietów o określonych cechach do portu pomiarowego

syslog – plik z logami systemowymi

comandlog – plik z logami poleceń

FTP (File Transfer Protocol) – protokół transferu plików – protokół komunikacyjny typu klient-serwer wykorzystujący protokół TCP według modelu TCP/IP, umożliwiający dwukierunkowy transfer plików w układzie serwer FTP – klient FTP.

TFTP (Trivial File Transfer Protocol) – prosty protokół wykorzystywany do przesyłania plików, implementowany na protokole UDP, chociaż jego definicja nie wyklucza stosowania innych protokołów datagramów. Nie posiada większości funkcji protokołu FTP – np. nie może wyświetlać katalogów, ani uwierzytelniać użytkowników, a jego jedynym zadaniem jest odczytywanie plików z komputera zdalnego i transmitowanie do niego plików. Protokół TFTP wykorzystywany jest przeważnie przez aplikacje poczty elektronicznej.

SFTP (SSH File Transfer Protocol) – szyfrowany protokół komunikacyjny typu klient-serwer, który umożliwia przesyłanie plików poprzez sieć TCP/IP.

FTPS (znany także jako FTP Secure i FTP-SSL) – jest rozszerzeniem do powszechnie stosowanego protokołu File Transfer Protocol (FTP), który umożliwia wsparcie dla szyfrowanych protokołów Transport Layer Security (TLS) oraz Secure Sockets Layer (SSL).

SCP (Secure CoPy) – protokół SCP jest bardzo podobny do protokołu RCP (BSD), jednak w przeciwieństwie do niego korzysta z szyfrowanego połączenia podczas transferu, dzięki temu podsłuchiwanie transmisji jest zdecydowanie trudniejsze. Sam protokół SCP nie zapewnia uwierzytelniania, opiera się on na protokole SSH. Protokół SCP zajmuje się tylko transmisją plików, jego przewagą nad protokołem FTP jest to, że oprócz szyfrowania potrafi również przekazać razem z plikiem jego podstawowe atrybuty (np. uprawnienia).

SSH (Secure Shell) – to standard protokołów komunikacyjnych używanych w sieciach komputerowych TCP/IP, w architekturze klient-serwer. W ścisłym znaczeniu SSH to tylko następca protokołu Telnet, służącego do terminalowego łączenia się ze zdalnymi komputerami. SSH różni się od Telnetu tym, że transfer wszelkich danych jest zaszyfrowany oraz możliwe jest rozpoznawanie użytkownika na wiele różnych sposobów. W szerszym znaczeniu SSH to wspólna nazwa dla całej rodziny protokołów, nie tylko terminalowych, lecz także służących do przesyłania plików (SCP, SFTP), zdalnej kontroli zasobów, tunelowania i wielu innych zastosowań. Wspólną cechą wszystkich tych protokołów jest identyczna z SSH technika szyfrowania danych i rozpoznawania użytkownika. Obecnie protokoły z rodziny

SSH praktycznie wyparły wszystkie inne mniej bezpieczne protokoły, takie, jak np. rlogin czy RSH.

SSL (Secure Socket Layer) – to ustandaryzowany zestaw znanych algorytmów szyfrowania, technik i schematów używanych do zapewnienia bezpieczeństwa.

SNMP (Simple Network Management Protocol) – rodzina protokołów sieciowych wykorzystywanych do zarządzania urządzeniami sieciowymi, takimi jak routery, przełączniki, komputery czy centrale telefoniczne. Do transmisji wiadomości SNMP wykorzystywany jest głównie protokół UDP: standardowo port 161 wykorzystywany jest do wysyłania i odbierania żądań, natomiast port 162 wykorzystywany jest do przechwytywania sygnałów trap od urządzeń. Możliwe jest także wykorzystanie innych protokołów do przekazywania żądań, na przykład TCP.

CLI – Command Line Interface

DDM (Digital Diagnostic Monitoring) – diagnostyka w czasie rzeczywistym połączeń światłowodowych w celu wczesnego wykrywania pogorszenia sygnału optycznego.

TDR (Time Domain Reflectometry) – wykrywanie i lokalizacja przerw i innych nieciągłości w kablach miedzianych

ERT Emergency Roadside Telephone – Przydrożna kolumna alarmowa

FAT Factory Acceptance Test – Fabryczny test zdawczo-odbiorczy

MTBF Mean Time Between Failure – Średni czas pomiędzy awariami

OUA – Obwód Utrzymania Autostrady

SAT Site Acceptance Test – Test zdawczo-odbiorczy na miejscu

Tranking - komputerowo sterowany system bezprzewodowej łączności dyspozytorskiej. Polega na wykorzystaniu ograniczonej ilości kanałów radiowych przez maksymalną liczbę użytkowników. W dwukierunkowej łączności radiowej tranking jest zdefiniowany jako automatyczny i dynamiczny rozdział ograniczonej liczby kanałów pomiędzy dużą liczbą użytkowników radiotelefonów.

Specyfikacja Techniczna (ST) – zbiór wymagań technicznych dla wykonania, dostaw, instalacji i odbioru dla wybranego zakresu realizacji.

SPTA – system przydrożnej telefonii alarmowej, w skład którego wchodzi kolumny alarmowe SOS.

SNPTA – System Nadzoru Przydrożnej Telefonii Alarmowej. System informatyczny, którego zadaniem jest kompleksowa obsługa dedykowanego rodzaju urządzeń terenowych w ramach SPTA (import, przetwarzanie, wizualizacja danych pomiarowych i rezultatów ich przetwarzania, sterowanie pracą urządzeń terenowych i wizualizacja procesów sterowania) oraz współpraca z systemem zarządzającym.

Kolumna SOS – urządzenie terenowe, kolumna alarmowa SOS służąca do przekazu informacji w postaci głosowej pomiędzy zgłaszającym a odbierającym w Centrum Zarządzania.

Platforma SOS – odpowiednio przygotowane miejsce na posadowienie kolumny SOS zlokalizowane przy krawędzi drogi poprzez poszerzenie korony drogi bądź zlokalizowane MOP w niedalekiej odległości od obiektów użyteczności publicznej np. sanitariatów. Miejsce to wyposażone jest w chodniki i dojścia wykonane poprzez przygotowanie podłoża przez

zabetonowanie, asfaltowanie bądź wybrukowanie oraz odpowiednio wyposażone w wymagane przepisami elementy BRD.

Kanalizacja kablowa – zespół podziemnych rur i studni kablowych, służący do układania kabli telekomunikacyjnych.

Mufa kablowa światłowodowa – kompletny zestaw osprzętu do trwałego połączenia dwóch lub większej liczby kabli światłowodowych metodą spawania włókien.

Studnia kablowa – pomieszczenie podziemne wbudowane między ciągi kanalizacji kablowej w celu umożliwienia wciągania, montażu i konserwacji kabli.

System zarządzający – główny system informatyczny, którego zadaniem jest przetwarzanie danych, realizacja reguł decyzyjnych oraz wizualizacja procesów związanych z zarządzaniem ruchem drogowym.

Centrum Zarządzania (CZ) – zespół urządzeń i oprogramowania (sprzęt komputerowy, urządzenia zasilające, infrastruktura komunikacyjna, systemy operacyjne i bazodanowe, aplikacje zarządzające) zainstalowany w dedykowanych pomieszczeniach biurowych i umożliwiający wykwalifikowanemu personelowi realizację zadań eksploatacyjnych związanych z SPTA.

Wykonawca – podmiot realizujący Zamówienie, obejmujący wszystkie osoby fizyczne i podmioty zatrudnione do realizacji Zamówienia, w tym do projektowania i dostawy wszelkich materiałów, sprzętu, ekspertyz, konsultantów, itp.

Zamawiający (zwany też Inwestorem) – Skarb Państwa reprezentowany przez GDDKiA.

Pozostałe określenia podstawowe - są zgodne z obowiązującymi, odpowiednimi polskimi normami i zawartymi tam definicjami.

Tranking - komputerowo sterowany system bezprzewodowej łączności dyspozytorskiej. Polega na wykorzystaniu ograniczonej ilości kanałów radiowych przez maksymalną liczbę użytkowników. W dwukierunkowej łączności radiowej tranking jest zdefiniowany jako automatyczny i dynamiczny rozdział ograniczonej liczby kanałów pomiędzy dużą liczbą użytkowników radiotelefonów.