Paweł KLIMEK
INTEGRATOR Sp. z o.o.

GEBLOCK – KOMPLEKSOWY SYSTEM ZABEZPIECZENIA INFRASTRUKTURY TELEKOMUNIKACYJNEJ

Streszczenie. Artykuł przedstawia opis działania i elementy składowe systemu zabezpieczającego infrastrukturę telekomunikacyjną. Celem przeprowadzonych prac badawczych było opracowanie kompleksowego zautomatyzowanego systemu umożliwiającego monitoring i nadzór nad infrastrukturą teletechniczną. Szczególny nacisk położono na automatyzacje funkcji określonych w przewidywanych scenariuszach typu kradzież, prace serwisowe, działania patroli interwencyjnych. Specyfika opracowanych algorytmów w głównej mierze skupia się na minimalizacji „czynnika ludzkiego" i automatyzacji procesów. W przypadku zdarzenia niepożądanego jakim jest kradzież, priorytetem stało się skrócenie czasu reakcji służb interwencyjnych i precyzyjne określenie miejsca zdarzenie celem udaremnienia kradzieży bądź też zabezpieczenia miejsca zdarzenia.

GEBLOCK - A COMPREHENSIVE TELECOMMUNICATION INFRASTRUCTURE SYSTEM FOR SECURITY

Summary. The article presents a description of the operation and components of the system securing telecommunications infrastructure. The aim of the research work was to develop a comprehensive automated system enabling monitoring and supervision of teletechnical infrastructure. Particular emphasis was placed on the automation of functions defined in the anticipated theft scenarios, service works, intervention patrols. The specificity of developed algorithms focuses mainly on the minimalization of the "human factor" and the automation of processes. In the case of an adverse event that is stealing it became a priority to shorten the response time of emergency services and the precise determination of the place to thwart the event of theft or security scene.

1. Wstęp

Kanalizacja kablowa (inaczej telekomunikacyjna lub teletechniczna) stanowi infrastrukturę złożoną z systemu rur w budynkach i na zewnątrz potrzebnych do instalacji i przeciągania kabli sieci telekomunikacyjnych. W skład kanalizacji kablowej wchodzą: studnie kablowe (rewizyjne, zasobnikowe), ciągi rur prowadzonych na zewnątrz oraz wprowadzenia do budynków. Zarówno studnie

kanalizacyjne jak i plastikowe rury zawierają w sobie kable: miedziane bądź rzadziej światłowodowe [1]. W 2015 roku łączna wartość rynku telekomunikacyjnego wyniosła 39,5 mld zł. Choć w niektórych segmentach przychody były niższe niż w roku poprzednim, to jednak w ogólności nastąpił wzrost przychodów całego sektora. Spadek w niektórych segmentach wynikał z migracji do nowszych usług opartych o transmisję danych, bardziej charakterystycznych dla nowoczesnego e-społeczeństwa. Przykładowo zmalały przychody z usług telefonii stacjonarnej, wzrosły zaś te z komórkowej [2]. Ewolucja świadczonych przez Operatorów usług powoduje zwiększenie nakładów na budowę sieci opartych na światłowodach wypierając kable miedziane. W 2015 roku odnotowano ogółem 30% przyrost sieci światłowodowych. Na koniec roku długość sieci optycznej w Polsce wyniosła prawie 420 000 km. Liczba węzłów światłowodowych na koniec 2015 roku była aż o 21% wyższa w porównaniu z deklarowaną w poprzedniej inwentaryzacji [2]. Jednocześnie nastąpiły zmiany strukturalne w obrębie samego dostarczania Internetu. Wartość światłowodowych usług dostępu do Internetu wzrosła w roku 2015 aż o 58% w stosunku do roku 2014. Powyższe dane potwierdzają jak ważnym dla społeczeństwa staje się dostęp do transmisji danych, można stwierdzić, że Internet staje się medium krytycznym. Zjawiskiem, z którym z którym borykają się operatorzy telekomunikacyjni są kradzieże i dewastacji infrastruktury teletechnicznej. Kradzieże kabli ze studni telekomunikacyjnych powodują nie tylko utratę samego materiału, ale również generują koszty odtworzenia infrastruktury. Kradzieże dodatkowo generują trudne do oszacowania straty, wynikające z przerw w dostarczaniu usług do klientów. Ponadto bezpośrednim następstwem zdarzeń kradzieżowych są ponoszone przez firmy telekomunikacyjne koszty utrzymywanych systemów zabezpieczeń. Na świecie rozwija się różnego typu rozwiązania [3, 4] mające zabezpieczyć urządzenia telekomunikacyjne.

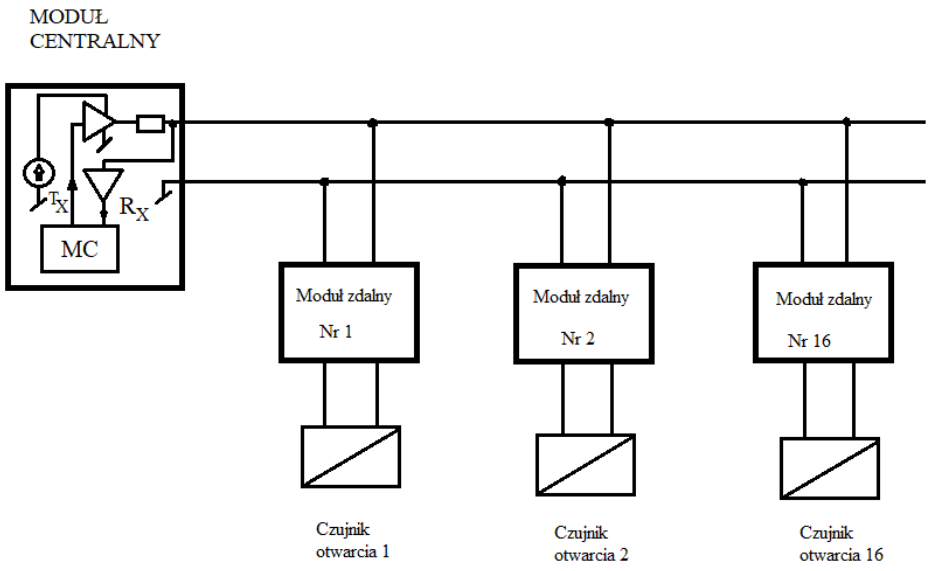
2. Koncepcja systemu zabezpieczenia studzienek telekomunikacyjnych

Badanie prowadzone w ramach niniejszego projektu zatytułowane „Innowacyjny system zabezpieczenia i minimalizacji strat infrastruktury technicznej dla branży telekomunikacyjnej” miało na celu opracowanie założeń do zbudowania systemu urządzeń, które umożliwią natychmiastowe wykrycie otwarcia obiektów telekomunikacyjnej infrastruktury kanalizacyjnej („real time monitoring”). Jednym z kluczowych założeń było uzyskanie informacji o potencjalnym otwarciu studzienki kanalizacyjnej w momencie zajścia, z uwzględnieniem dokładnej lokalizacji danej studzienki. Na bazie pełnych danych o miejscu zdarzenia w czasie jego wystąpienia opracowano system skutecznej, bardzo szybkiej interwencji służb interwencyjnych w celu zapobieganiu kradzieżom, potencjalnym uszkodzeniom i jakimkolwiek innym aktom niedozwolonym w obszarze funkcjonowania podziemnej infrastruktury telekomunikacyjnej. Intencją było stworzenie systemu, który będzie działał w trybie reaktywnym, czyli uruchomi mechanizm oraz procedurę podejmowania akcji interwencyjnych natychmiast po zajściu zdarzenia mogącego skutkować uszkodzeniami infrastruktury kanalizacyjnej.

Realizacja wyżej wymienionych założeń wymaga także opracowania i przetestowania rozwiązania pozwalającego na monitoring studni kablowych na duże odległości, przy niskim poborze energii.

Założenia systemu monitorującego infrastrukturę techniczną branży telekomunikacyjnej przewidują pełną identyfikację miejsc zdarzeń wraz z wizualizacją. Najbardziej skutecznym, a także bardzo prostym rozwiązaniem jest użycie lokalizacji poszczególnych czujek poprzez użycie adresowalnych elementów systemu. Adresowalność modułów lub czujników jest warunkiem koniecznych do skutecznej pracy badanego systemu. Nie ma możliwości wykorzystania rozwiązań radiowych lub GPS, ponieważ propagacja fal radiowych pod ziemią jest zawodna. Znacznie skuteczniejsze jest użycie adresowalnych elementów systemu, którym szczegółowa lokalizacja jest przypisana systemowo. Rozwiązanie jest specyficzne dla badanego systemu, ponieważ elementy są statyczne, nie przemieszczają się. Stąd też przypisanie lokalizacji dla adresowalnych elementów systemu monitorującego jest rozwiązaniem skutecznym i wybranym do badanego systemu.

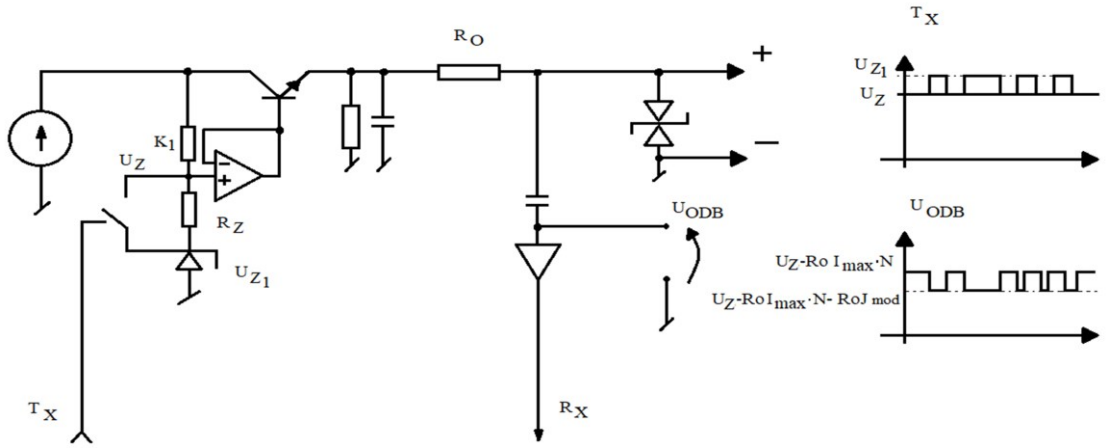
Bardzo ważnym założeniem podczas prac nad opracowaniem systemu było uproszczenie linii danych. Ograniczenie ilości przewodów do dwóch jest optymalnym rozwiązaniem. Ułatwia bowiem zarówno ułożenie kabli, zwłaszcza na terenach miejskich, gdzie zagęszczenie zabudowań miejskich jest ogromne oraz liczba studzienek telekomunikacyjnych znacząca, oraz w sytuacji linii podmiejskich, gdzie odległości pomiędzy studniami i punktem dystrybucyjnym są znaczne.



Rys 1. Moduł centralny, uproszczony schemat sieci

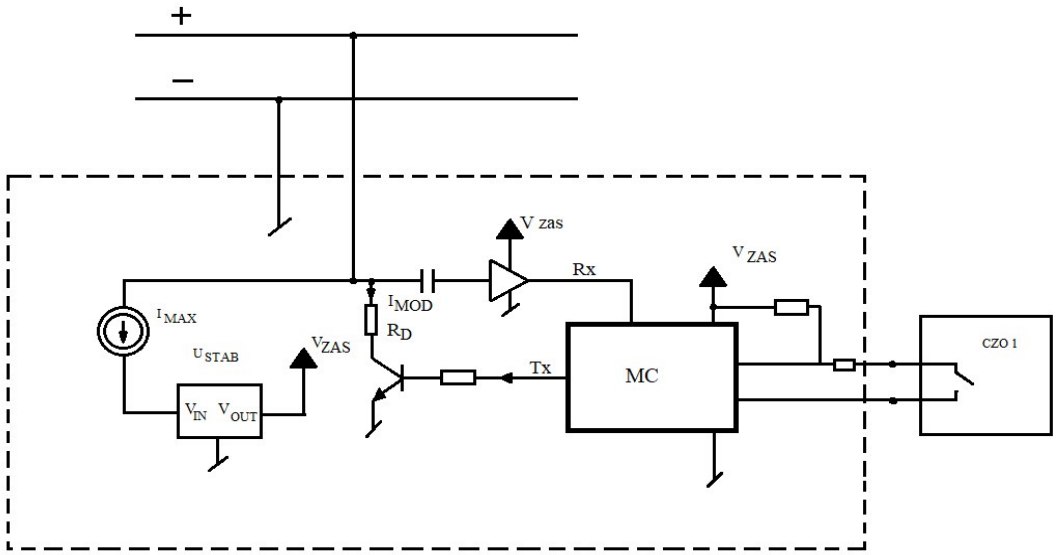
W wyborze elementów badanego rozwiązania istotnym ograniczeniem jest dostęp do zasilania w energię elektryczną. Standardowo studzienki branży telekomunikacyjnej nie mają dostępnego zasilania prądowego. Zasilanie do monitorowanych studni należy doprowadzić z punktu dystrybucyjnego, w niektórych przypadkach znajdującego się w odległości kilku kilometrów. Ze względu na ograniczenia dotyczące średnicy kabla i związane z tym spadki napięcia, elementy systemu moni-

torującego, które znajdują się w studzienkach, muszą pobierać poniżej 1 mA prądu. Moduły zdalne instalowane są jako elementy czujnika – DETEKTORA. System zbierania danych z modułów zdalnych wykonano w oparciu o dwuprzewodową linię zasilającą będącą zarazem linią transmisji danych.



Rys. 2. Schemat modułu centralnego – koncepcja bloku zasilania i transmisji

W celu zminimalizowania wpływu pracy modułu zdalnego na transmisję danych zasilacz stabilizujący napięcie zasilania modułu zdalnego jest poprzedzony źródłem prądowym o maksymalnej wydajności potrzebnej do zasilania modułu. Prąd maksymalny źródła nie może powodować dużego obciążenia, dlatego przejmuje się, że będzie zachowana nierówność Imax << Imod. Przyjęto, że prąd modulujący Imod = 20 mA. Ustalono, że napięcie zasilania Uz = 24 V. Jednocześnie w celu znacznego obniżenia poboru mocy układ elektroniczny (mikroprocesorowy) modułu zdalnego został wyposażony w mikrokontroler (µpower) o maksymalnym poborze prądu I ~ 1..4 µA. Dodatkowo postanowiono zastosować kwarc taktujący Fmax ~ 500 kHz.



Rys. 3. Moduł zdalny, zasilanie i transmisja danych w systemie monitorowania czujników.

3. Metoda transmisji danych w systemie GEBLOCK

3.1. Nadawanie danych przez modułu centralny

Nadawanie danych z modułu centralnego **MC** odbywa się za pomocą modulacji napięcia zasilającego pomiędzy **Uz** i **Uz1**. Rozwiązano to za pomocą klucza sterowanego sygnałem **Tx** i zmieniającego napięcie zasilacza stabilizowanego. Na wyjściu układu zastosowano opornik pomiarowy **Ro** służący do:
- pomiaru spadku napięcia w celu kontroli obciążenia układu zasilającego i wykrywania awarii na linii,
- odbioru danych.

W układzie zastosowano kodowanie typu Manchester z uwagi na możliwość prostej synchronizacji nadajnik - odbiornik i odtworzenia taktu zegara.

3.2. Odbiór danych przez moduł zdalny

Odbiór danych odbywa się poprzez odczyt zmiany napięcia na linii zasilającej. Do tego celu służy kondensator **Csep** wraz z wzmacniaczem sygnału. Następnie sygnał kierowany jest do układu wejściowego mikroprocesora.

3.3. Nadawanie danych przez moduł zdalny

Nadawanie sygnału przez moduł zdalny odbywa się za pomocą klucza tranzystorowego sterowanego bezpośrednio z układu mikroprocesorowego. Maksymalny prąd kluczowania wynosi 20mA.

3.4. Odbiór danych przez moduł centralny

Odbiór danych przez moduł centralny odbywa się za pomocą pomiar spadku napięcia na rezystorze **Ro**. Kondensator separacyjny oddziela stałą składową modulowanego zasilacza i następnie sygnał zostaje wzmocniony w wzmacniaczu sygnałowym. Po wzmocnieniu sygnał skierowany jest do układu mikroprocesora modułu centralnego.
Właściwości transmisji danych w systemie:

- Nadawanie sygnału przez moduł centralny odbywa się za pomocą wyższego poziomu napięcia niż napięcie zasilające, prosta możliwość odróżnienia komunikatów modułu centralnego od komunikatów modułu zdalnego.
- Nadawanie sygnału przez moduł zdalny odbywa się za pomocą zwiększenia poboru prądu przez moduł a co za tym idzie modulacji napięcia na linii zasilającej.
- Niska wrażliwość na zmianę częstotliwości nadawania ze względu na zastosowane kodowanie Manchester.

4. Główne elementy struktury systemu GEBLOCK

Projekt zakłada utworzenie ogólnopolskiego centrum monitorowania w celu wdrożenia kompleksowego systemu nadzoru na siecią studni telekomunikacyjnych, zarządzania mobilnymi patrolami interwencyjnymi oraz dysponowania służbami technicznymi i serwisowymi. Głównymi elementami struktury systemu są:

- **DETEKTORY** – czujniki systemu są adresowalnymi urządzeniami mikro-procesorowymi umieszczone wewnątrz studzienki monitorują otwarcie włazu oraz stan zabezpieczonej infrastruktury. Kontrolę nadrzędna nad siecią inteligentnych czujników sprawuje moduł centralny **MC** podłączony do **KONCENTRATORA**

(kontroler przemysłowy), który obsługuje maksymalnie 32 MC oraz odpowiada za transmisję danych pomiędzy siecią a bazą danych (złącze Ethernet).

- **OPROGRAMOWANIE** systemu z następującymi modułami:

  1/ **Baza danych GEBLOCK** służy do gromadzenia wszystkich danych systemu monitoringu oraz wykrytych alarmów i stanów awaryjnych. Baza danych bezpośrednio korzysta z danych przesyłanych z koncentratorów oraz programu Operator GEBLOCK zainstalowanego na stacji operatorskiej.

  2/ **Moduł OPERATOR GEBLOCK** – którego głównym celem jest wizualizacja i obsługa zdarzeń alarmowych systemu monitoringu, zarządzanie i administracja system monitoringu.

  Oprogramowanie GEBLOCK posiada następujące funkcje:

  - wizualizacja stanu monitorowanych studzienek telekomunikacyjnych na mapie,
  - obsługa i zarządzanie systemem w zakresie bieżących zdarzeń alarmowych,
  - wizualizacja, położenie i przekierowywanie patroli interwencyjnych (możliwość ręcznego lub automatycznego przekierowania alarmu do patrolu lub kilku patroli z potwierdzeniem przyjęcia zgłoszenia i podjęcia interwencji),
  - wizualizacja, położenie i przekierowywanie służb technicznych, rejestracja prac planowych serwisantów, autoryzacja dostępu serwisowego oraz monitorowanie czasu serwisowego (czas pomiędzy deaktywacją i aktywacją detektora),
  - prowadzenie ewidencji magazynowej detektorów,
  - archiwizowanie historii zdarzeń,
  - obsługa systemu w trybie prac serwisowych,
  - tworzenie terminowych raportów i zestawień w celach rozliczeniowych.

  3/ **Aplikacja mobilna – Instalator GEBLOCK** przeznaczona jest dla serwisantów i służb technicznych.

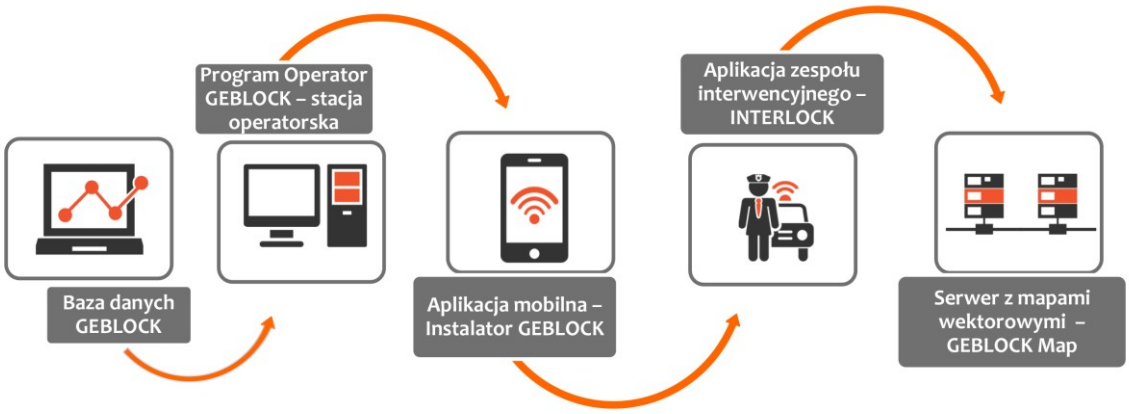
  Zainstalowana na tablecie z modułem GPS oferuje następujące funkcje:

  - sprawdzanie stanu sieci i urządzeń monitorujących.
  - dodawanie i odejmowanie urządzeń.
  - przeprowadzanie testów i kontrola sprawności urządzeń.
  - raportowanie wykonanych przeglądów

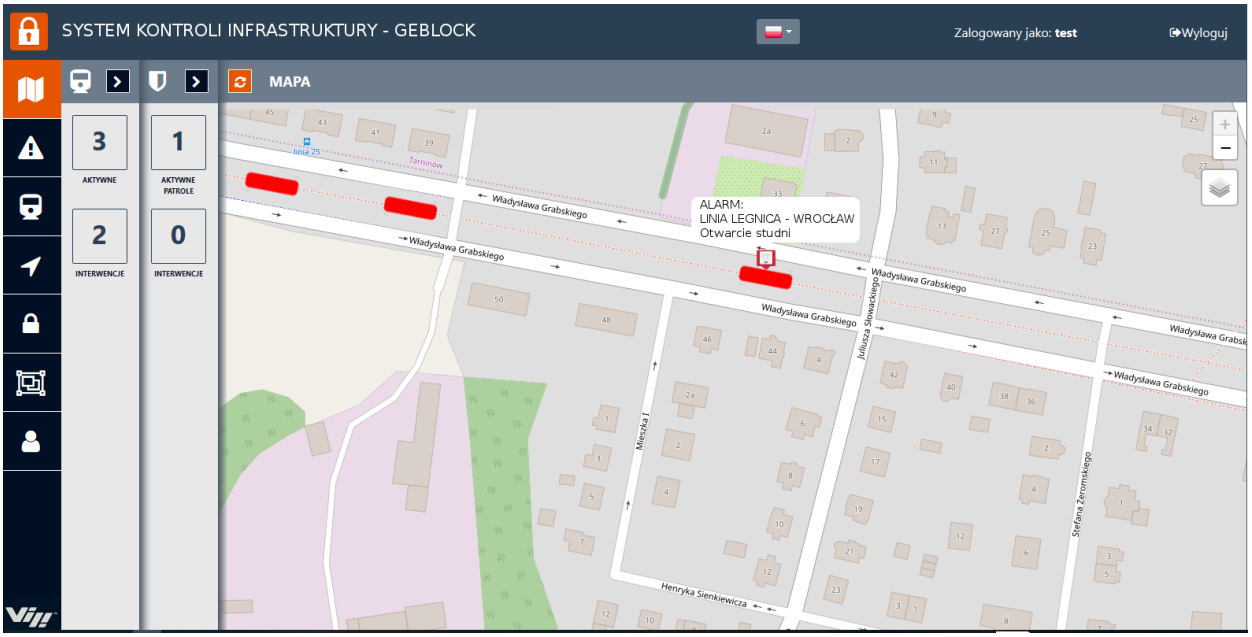
  4/ **Aplikacja mobilna – INTERLOCK** przeznaczona jest służb interwencyjnych. Zainstalowana na tablecie z modułem GPS oferuje następujące funkcje.

  - Potwierdzenie interwencji w zakresie otrzymanego zdarzenia alarmowego.
  - Lokalizacja na mapie zdarzenia alarmowego.
  - Wyznaczenie najszybszej drogi dojazdu do punktu docelowego.
  - Raportowanie wykonanych wyjazdów interwencyjnych.

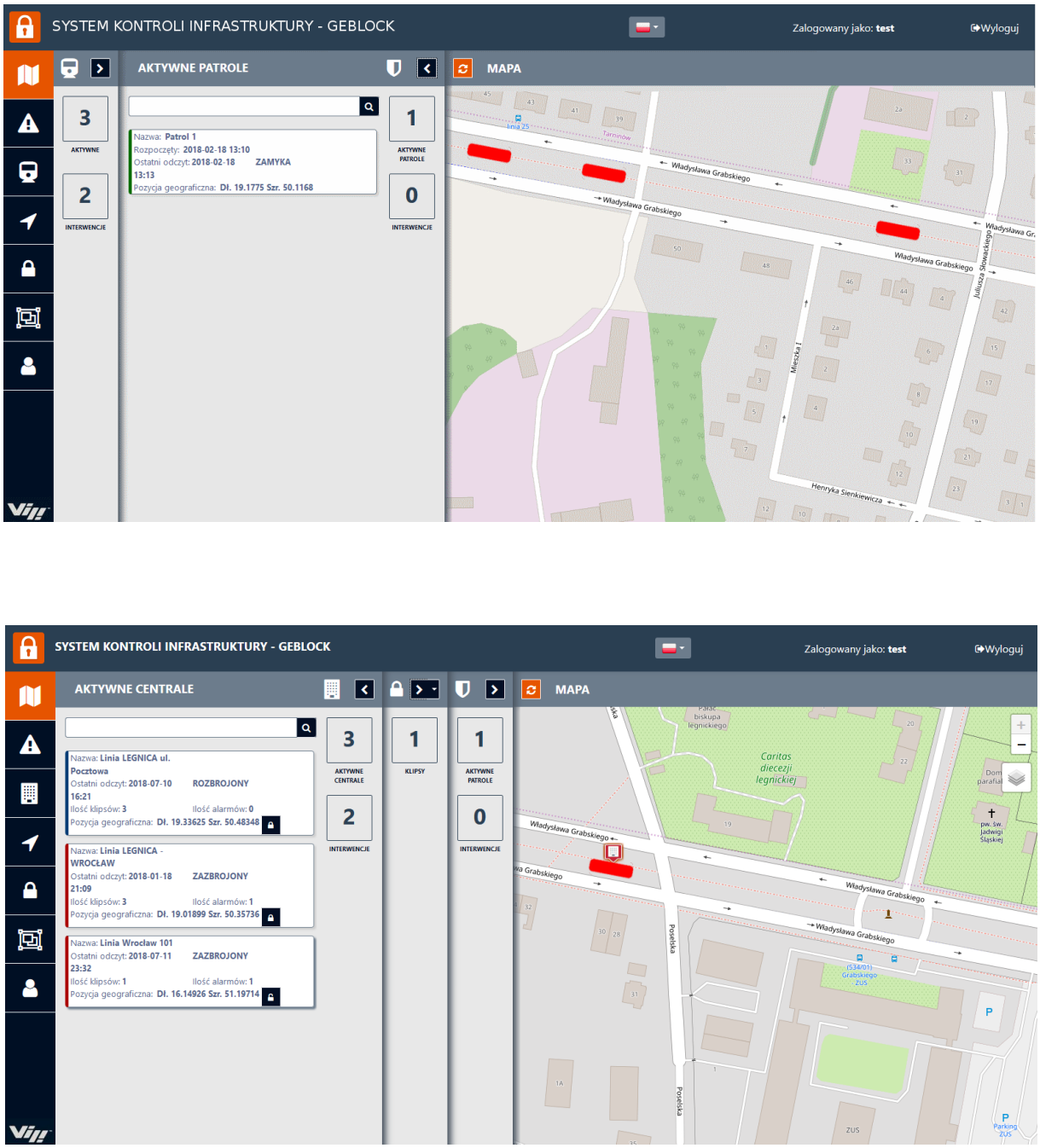
  5/ Serwer z mapami – **GEBLOCK Map**



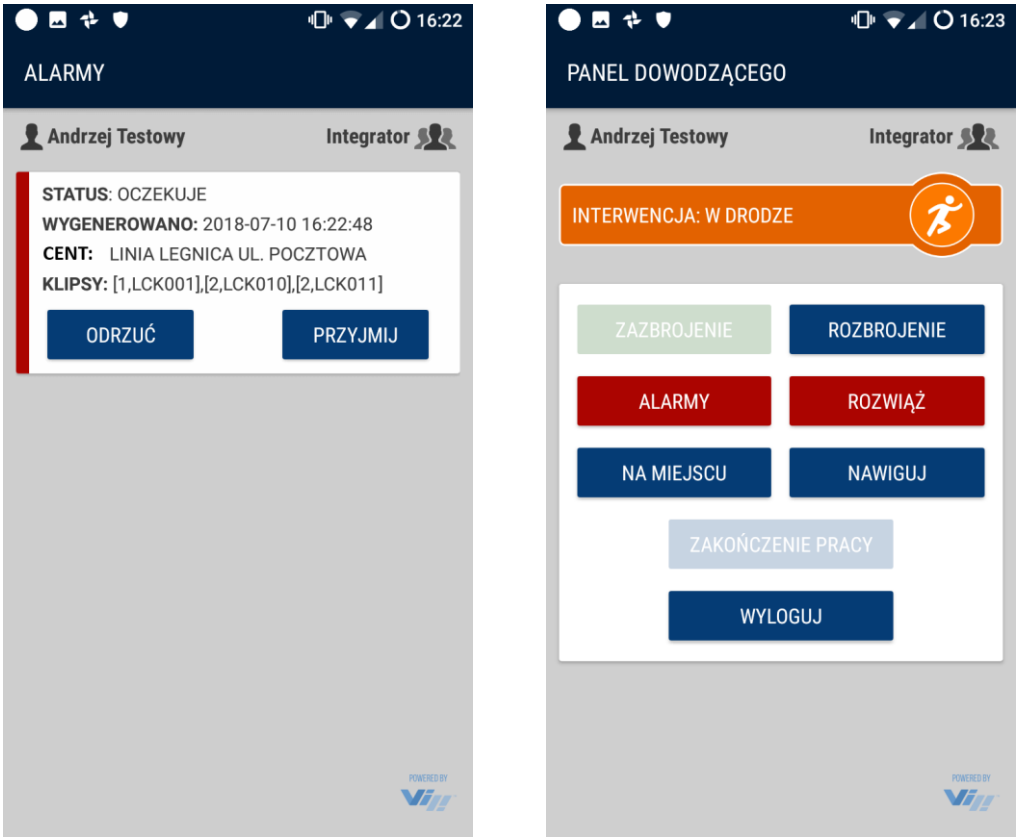
Rys. 4. Moduły oprogramowania systemu GEBLOCK



Rys. 5. Wizualizacja alarmu na ekranie operatora w systemie GEBLOCK



Rys. 6. Wizualizacja zakończenia interwencji na ekranie operatora w systemie GEBLOCK



Rys. 7. Okno dialogowe w aplikacji mobilnej INTERLOCK

Rys. 8. Widok panelu grupy interwencyjnej w aplikacji mobilnej INTERLOCK w systemie GEBLOCK

5. Badania

W celu stworzenia systemu w pełni reaktywnego do zakresu badań włączono założenia i testy urządzeń oraz oprogramowania umożliwiającego skuteczną komunikację z centrum obsługi firmy telekomunikacyjnej jak i również z zewnętrznymi jednostkami interwencyjnymi, takimi jak prywatne firmy ochroniarskie, straż miejska lub policja. Jak wcześniej podkreślano, najkrótszy z możliwych czas interwencji odpowiednich służb po otrzymaniu sygnału zdarzenia w określonej lokalizacji jest kluczowy dla zapewnienia skuteczności ochrony lub minimalizacji strat infrastruktury telekomunikacyjnej. Dla prowadzonego badania założono, że skuteczna ochrona infrastruktury podziemnej wymaga czasu reakcji ok. 5-10 minut od momentu otrzymania sygnału z systemu monitorującego studzienki. Na podstawie dostępnych ogólnie informacji wynika, że interwencja w czasie nieprzekraczającym 10 minut od włamania do studzienki pozwala zapobiec kradzieży bądź istotnym uszkodzeniom okablowania oraz innych urządzeń znajdujących się w miejscu, gdzie dokonano włamania. Szybkość reakcji po zajściu zdarzenia oraz znajomość dokładnej lokalizacji miejsca zdarzenia według założeń powziętych do prowadzonego badania umożliwia także natychmiastowe podjęcie akcji przez służby serwisowe firmy działającej w branży komunikacyjnej w celu ewentualnej naprawy uszkodzonych elementów infrastruktury.

Rozpatrując powyższe zagadnienia dotyczące niezawodności transmisji danych wykonano model sieci na którym przeprowadzono próby niezawodności transmisji. Projektując model sieci kierowano się następującymi wytycznymi:

- urządzenie (czujnik) o małym poborze mocy,
- linia zasilająca i linia transmisji danych w systemie dwuprzewodowym,
- indywidualna transmisja danych z niestandardowym protokołem danych i kodowaniem w obszarze chronionym,
- zastosowanie zabezpieczeń zarówno w warstwie elektrycznej i warstwie protokołu.

6. Podsumowanie

W wyniku prac badawczych powstał nowoczesny system ochrony infrastruktury telekomunikacyjnej montowanej w przestrzeni publicznej. Proponowany system posiada unikatowe cechy odróżniające go od podobnych systemów obecnych na rynku, opracowane urządzenia i metody pozwalają między innymi na:

- niestandardowe kodowanie sygnału (poziomy elektryczne) nie mające odpowiedników wśród dostępnych urządzeń, co w znacznym stopniu utrudnia dokonania poprawnego odczytu danych przez nieuprawnione osoby,
- zastosowane kodowanie i szyfrowanie sygnału uniemożliwiają interpretację ewentualnie podsłuchanych ramek danych,
- zakłócenia linii, dodanie dodatkowego urządzenia, zwarcia i inne anomalie są natychmiast odczytywane przez moduł nadrzędny w formie alarmu (awaria lub intruz),

- wybór urządzeń zdalnych – DETEKTORÓW o małym poborze mocy, minimalizuje powstanie awarii

W trakcie realizacji projektu dokonała się istotna zmiana technologiczna, dotycząca głównie dostępu do usług szerokopasmowego Internetu. Firmy chcąc nadążyć za zmieniającym się rynkiem rezygnują z przewodów miedzianych na rzecz światłowodów – co w dużym stopniu może mieć wpływ na zmniejszenie liczby kradzieży. Jednak w ocenie autorów systemu GEBLOCK założenia przyjęte przy budowie systemu w dalszym ciągu pozostają aktualne:

- **zmniejszenie strat materialnych i odszkodowań** wynikających z kradzieży i dewastacji infrastruktury telekomunikacyjnej, skrócenie przerw w ciągłości świadczonych usług,
- dokładna **geolokalizacja i ewidencja czujników**,
- **inwentaryzacja** chronionej infrastruktury, studzienek telekomunikacyjnych,
- **precyzyjna lokalizacja** występujących zdarzeń,
- znaczące **skrócenie czasu reakcji** służb interwencyjnych,
- **optymalizacja drogi** do miejsca zdarzenia,
- **zmniejszenie nieprawidłowości** w rozliczaniu służb serwisowych,
- **zmniejszenie fraudów wewnętrznych** związanych ze służbami serwisowymi,
- **możliwa integracja** z już działającymi systemami monitoringu,
- **rozbudowa** funkcji o dodatkowe moduły (serwisowy, magazynowy), umożliwiające **zarządzanie i nadzór** nad służbami technicznymi.

Zrealizowany w trakcie prac badawczych projekt, z uwagi na swoją modułowość, nie zamyka się tylko na zastosowanie do monitoringu infrastruktury telekomunikacyjnej. System może obsługiwać inne branże posiadające infrastrukturę teletechniczną jak kolej, energetyka, gazownictwo. Będzie to wymagało jedynie zmian o obrębie funkcjonalności i konstrukcji samego czujnika – DETEKTORA, które zostaną określone przez zainteresowane podmioty branżowe.

Praca finansowana z Regionalnego Programu Operacyjnego Województwa Dolnośląskiego 2014-2020, w ramach projektu ***„Innowacyjny system zabezpieczenia i minimalizacji strat infrastruktury technicznej dla branży telekomunikacyjnej”,*** *współfinansowanego ze środków Unii Europejskiej w ramach Poddziałania 1.2.1 „Innowacyjne przedsiębiorstwa – konkurs horyzontalny”, Schemat nr 1.2 A „Wsparcie dla przedsiębiorstw chcących rozpocząć lub rozwinąć działalność B + R” Numer umowy dofinansowania:* ***RPDS.01.02.01-02-0039/15-00***

LITERATURA

1. Norma Zakładowa ZN-96 TPSA-011: Telekomunikacyjna kanalizacja kablowa. Ogólne wymagania techniczne; Telekomunikacja Polska S.A.
2. Raport o stanie rynku telekomunikacyjnego w Polsce w 2015 roku, Urząd komunikacji Elektronicznej, Warszawa 2016

3. Marshall B. Cummings, Christopher R. Young, Network security system for detecting removal of electronic equipment, US Patent US5406260A.
4. Źródło internetowe: Strona internetowa firmy CNIguard – https://www.cniguard.com/