Urządzenia IoT i CioT
Produkty Smart City - LoRaWAN & GSM

iSys – Intelligent Systems

@City

@AirQ @Bin

@Light @Metering @Trace

Table of Contents

1. Wstęp.

System @City obsługuje szereg urządzeń elektronicznych (sterowników) - zwanych jako node, mote, device. Dostępnych jest wiele rodzajów komunikacji (przewodowych i bezprzewodowych) w zależności od dostępnej infrastruktury, wymagań, warunków.

Typy urządzeń dostępne w systemie @City:

- **CIoT – Cellural Internet of Things (GSM/2G/3G/4G/NBIoT/CATM1)**
- **IoT - Internet of Things (LoRaWAN)**
- Ethernet
- WiFi

Wszystkie urządzenia są ze sobą zintegrowane poprzez chmurę @City i jest możliwość ich pracy hybrydowej w zależności od dostępności danej infrastruktury komunikacyjnej.

W przypadku lokalizacji w budynkach i dostępu do sieci lokalnych LAN lub WiFi podłączonych do internetu znacznie korzystniejsze mogą okazać się rozwiązania oparte na sieciach Ethernet/WiFi/CAN/RF/RS-485/RS-422 dostępne w systemie eHouse, które mogą przesyłać dane do chmury @City poprzez server eHouse.PRO).

Poniższy dokument opisuje urządzenia **GSM** oraz **LoRaWAN** oparte na mikrokontrolerze jednoukładowym (mikroprocesor) oraz zewnętrznym module komunikacyjnym.

Pozwala to na standaryzację systemu pomimo różnicy w sposobie komunikacji i innego modemu komunikacyjnego.

Umożliwia to uzyskanie podobnej funkcjonalności i wyposażenia sprzętowego oraz łatwą migrację do innych wariantów komunikacyjnych lub wersji.

1.1 Komunikacja @City (IoT/CIoT)

System @CITY (IoT) wykorzystuje aktualnie jeden z wybranych modułów (modemów) komunikacyjnych:

- LoRaWAN (1.0.2) + BlueTooth + BLE4.0 + NFC
- GSM (2G/NBIoT/CATM1) + GPS/GNNS
- 3G+GPS
- 4G+GPS

1.2. Zasoby sprzętowe urządzeń IoT/CIoT

Cała "Inteligencja" systemu jest uzyskana przy pomocy mikrokontrolera (mikroprocesora) i nie jest zbytnio zależna od rodzaju komunikacji. Zasoby sprzętowe urządzeń IoT/CIoT (mikroprocesor) są następujące:

- **0..4 programowalne wejścia binarne**
  - monitorowanie stanu wejść
  - powiązanie komendy wykonywanej przy zmianie stanu
  - generowanie zaawansowanych alarmów
  - podłączenie dowolnych czujek
  - zdalne raportowanie

- **0..4 wyjścia binarne**
  - Włączanie/Wyłączanie dowolnych urządzeń elektrycznych/elektronicznych (pojedyncze wyjście)
  - Otwórz/Zamknij/Zatrzymaj sterowanie napędami: rolety, bramy, markizy, elektrozawory, siłowniki, serwa (podwójne wyjścia)
  - sterowanie urządzeniami kontrolowanymi wieloma wyjściami np. silniki, wentylatory (potrójne lub poczwórne wyjścia)

- **0..4 wejścia zliczające impulsy**
  - energii elektrycznej
  - gazu
  - wody
  - ciepła
  - wystąpień zdarzeń z czujników alarmowych
  - zapis w pamięci nieulotnej

- **0..4 wyjścia ściemniaczy PWM lub 0..10V**
  - ściemnianie oświetlenia LED, zasilaczy LED
  - regulacja mocy silników
- **wejście + wyjście podczerwieni**
  - sterowanie z pilota podczerwieni lub bliska komunikacja urządzeń przez podczerwień
  - wysyłanie kodów podczerwieni
- **0..4 wejść pomiarowych (ADC)**
  - podłączenie czujników analogowych (dowolnych wartości fizycznych)
  - pomiary napięć, prądów, rezystancji, pojemności
  - pomiary i regulacje różnych wartości fizycznych
  - generowanie alarmów przy przekroczeniu zaprogramowanych progów
  - wykonywanie komend sterujących przy przekroczeniu zaprogramowanych progów
- **interfejsy szeregowe SPI/I2C/UART/CAN**
  - do instalacji dowolnych czujników i rozszerzeń, np.
  - poziomu oświetlenia
  - magnetometr (X,Y,Z)
  - żyroskop (X,Y,Z)
  - zbliżeniowy (proximeter)
  - przyśpieszenia (X,Y,Z)
  - temperatura, ciśnienie, wilgotność, ogólna jakość powietrza
  - koloru (R,G,B, IR)
  - Pomiar zanieczyszczeń powietrza cząstkami stałymi (PPM 2.5/10um)

- możliwość upgradu firmwaru OTA (Over The Air) pozwala na aktualizację algorytmów oprogramowania

oraz konfiguracji przez główny interfejs komunikacyjny

1.3. System @City GSM

Urządzenia łączą się poprzez sieć komórkową operatora telefonii GSM przez jedną lub więcej udostępnionych technologi i usług. Usługi te są rozliczane abonamentowo i zależą indywidualnie od operatorów i usług. Usługa jest autoryzowana analogicznie jak w telefonach komórkowych poprzez aktywne karty SIM (plastikowe) lub karty sim w postaci chipa (MIM).

Dostępność wybranych usług zależy od operatora komunikacyjnego i wmontowanego modemu GSM na etapie produkcji:

1) 2G (wszyscy operatorzy)

- SMS
- TCP/IP (GPRS/EDGE)
- UDP (GPRS/EDGE)

2) 2G/LTE CATM1 (Orange) - możliwe jest automatyczne przełączenie CATM1 na 2G jeśli brak usługi CATM1 lub zasięgu, kosztem dużo większego zużycia baterii.

- SMS (2G/CATM1)
- TCP/IP (GPRS/EDGE/CATM1)
- UDP (GPRS/EDGE/CATM1)

3) NBIoT (T-Mobile/Deutsche Telecom) - możliwe jest automatyczne przełączenie NB-IoT na 2G jeśli brak usługi NB-IoT lub zasięgu i usługodawca udostępnia usługę „fallback 2G”, kosztem dużo większego zużycia baterii.

- TCP/IP (NBIoT)
- UDP (NBIoT)

4) 2G/3G (wszyscy operatorzy)

- SMS
- USSD
- TCP/IP (GPRS/EDGE/3G)
- UDP (GPRS/EDGE/3G)

5) 4G/LTE (wszyscy operatorzy)

- TCP/IP (4G)
- UDP (4G)

6) Inne kombinacje usług mogą być także dostępne.

Pierwsze 3 rozwiązania pracują na tym samym modemie (NB-IoT/CATM1 + fallback 2G) i w przypadku stosowania plastikowych kart Nano SIM jest możliwość wymiany karty oraz zdalnej konfiguracji urządzenia do prawidłowej pracy w innej usłudze. W przypadku kart MIM (SIM'ów w postaci chipa (układu scalonego)), decyzja zapada na etapie produkcji urządzenia i nie jest możliwa zmiana operatora ani usługi. Operatorzy oferujący usługę NB-IoT muszą dodatkowo udostępnić usługę „falback 2G", aby była możliwość pracy urządzeń poza zasięgiem usługi NB-IoT. Dodatkowo NB-IoT jest dedykowana bardzo małej ilości przesyłanych danych (~512kB na miesiąc – należy sprawdzić aktualne ograniczenia u operatorów), co stanowi znaczną przeszkodę dla niektórych rozwiązań CIoT/IoT.

Rozwiązania 4, 5 wymagają instalacji innych modemów na etapie produkcji.

Pobór prądu urządzenia zależy od usługi i jest przedstawiony od najniższego do najwyższego:

- NB-IoT

- CATM1

- LTE

- 3G

- 2G/SMS/USSD/GPRS/EDGE

Prędkość przesyłu danych od najniższego do największego:

- NB-IoT

- CATM1

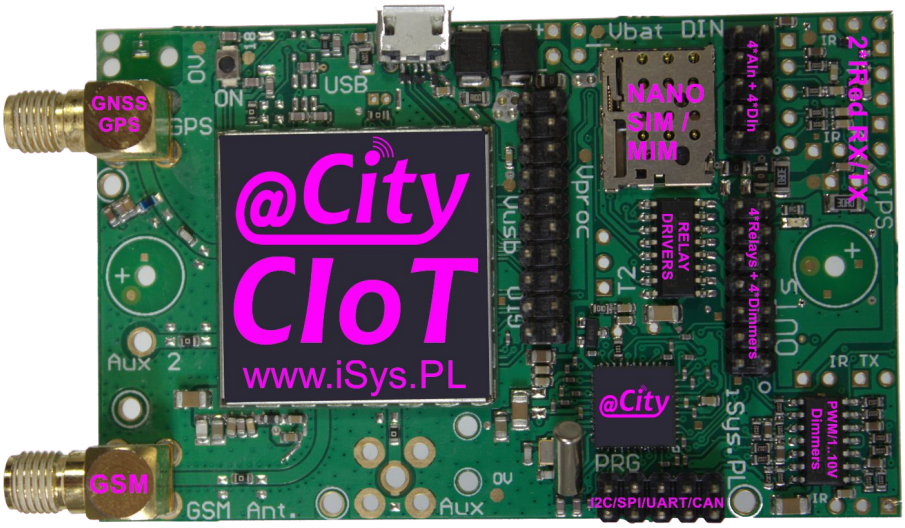
- 2G/SMS/USSD/GPRS/EDGE

- 3G

- LTE

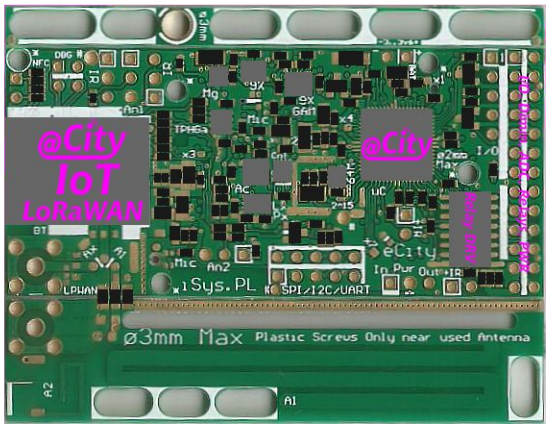
Wszystkie urządzenia @CITY GSM mogą być wyposażone w odbiornik GPS do geolokalizacji i automatycznego

pozycjonowania się na mapach. Mogą też pracować mobilnie gdy jest potrzeba pomiarów czy pracy w ruchu.



1.4. System @City LoRaWAN

LoRaWAN jest rozwiązaniem komunikacyjnym dużego zasięgu (do ok. 15km) pracujących w pasmach otwartych ISM (np. 433MHz, 863MHz, itd.). Bardzo duże zasięgi wymagają jednak znacznego ograniczenia prędkości transmisji oraz ograniczenia paczek danych (np dla najwyższego zasięgu do 250 bitów na sekundę oraz maksymalnie 51 bajtów danych). Transmisja z powtórzeniami i potwierdzeniami może trwać bardzo długo, co może eliminować LoRaWAN w niektórych rozwiązaniach. Ilość bramek LoRaWAN też ma duże znaczenie aby zapewnić dobry zasięg urządzeń co pozwala na pracę z wyższymi prędkościami, mniejszą iloscią błędów i powtórzeń.



Urządzenia LoRaWAN komunikują się z chmurą systemu @City poprzez **Bramki LoRaWAN**, które muszą być zlokalizowane tak, aby zapewnić pokrycie zasięgu na wymaganym poziomie, dla wszystkich dostępnych urządzeń LoRaWAN. Dodatkowo bramki te muszą być połączone z siecią LAN lub Internet przez dowolne łącze, aby móc przesyłać dane do serwera sieciowego/aplikacyjnego LoRaWAN.

Serwer sieciowy służy do dwukierunkowej komunikacji z bramkami LoRaWAN i przesyłania informacji do/z urządzeń LoRaWAN.

Serwer sieciowy/aplikacyjny może znajdować się w lokalnej sieci LAN lub w centrum danych usługodawcy. Dane z urządzeń są przesyłane z serwera sieciowego/aplikacyjnego przez protokoły integracyjne do chmury @City (poprzez tzw. webhook). Pozwala to na bezpośrednią integrację systemu @City LoRaWAN z bazami danych @City.

Serwer aplikacyjny może dodatkowo realizować rozszerzoną logikę dla systemu, na bieżąco przetwarzając dane i przesyłając komendy sterujące do poszczególnych urządzeń.

2. Warunki ogólne użytkowania systemu @City (LoRaWAN, GSM)

UWAGA! Niewłaściwe ustawienie głównych parametrów komunikacyjnych może spowodować zniszczenie lub permanentne zablokowanie urządzenia, do którego nie mamy fizycznego dostępu.

Ewentualna aktualizacja oprogramowania sterownika, oraz finalna konfiguracja musi zostać przeprowadzona i przetestowana (dla wszystkich urządzeń oraz co najmniej przez tydzień dla kilku urządzeń) przed ich instalacją w miejscu docelowym.

Producent nie odpowiada za niewłaściwą konfigurację/aktualizację oprogramowania wykonaną przez osoby nieuprawnione jak również wykonanie ich w miejscach instalacji poszczególnych sterowników.

Wszelkie koszty deinstalacji, usług, naprawy, wymiany, instalacji, ponosi użytkownik systemu (a nie Producent).

Do aktualizacji firmwaru i konfiguracji konieczne jest zapewnienie wystarczającego poziomu sygnału oraz dostępności wymaganych usług. Powyższe czynności mogą być NIE możliwe do wykonania w miejscach docelowej instalacji sterowników i w obudowach. Mogą być również zależne od pory roku, pogody, propagacji fal radiowych.

Wszelkie koszty usług związanych ze zmianą konfiguracji/firmwaru ponosi użytkownik (dodatkowe opłaty za transfer danych, ewentualną deinstalację, instalacje urządzeń, odblokowanie, wymianę, itd.).

Maksymalny zasięg jest czysto teoretyczny, mierzony w idealnych warunkach propagacji fal radiowych i odnosi się do pracy urządzeń (z zewnętrznymi i dopasowanymi antenami) w polu widzenia (bez przeszkód na drodze wiązki sygnału). W zależności od urbanizacji terenu, zadrzewienia, pogody, lokalizacji i sposobu instalacji urządzeń może być gorszy nawet kilkaset razy od powyższych danych.

2.1. Warunki szczególne @City GSM.

Użytkownik ponosi koszty oraz odpowiada za terminowe opłacanie abonamentu operatora GSM i hostingu @City. Brak ciągłości usług może spowodować nieodwracalne zmiany krytycznych parametrów transmisji i zablokowanie całego systemu (jak np. zmiana stałego adresu IP, utratę domeny internetowej, Utratę danych/konfiguracji na serwerze, utratę oprogramowania, kopi zapasowych, itd.).

W przypadku kiedy użytkownik reguluje ryczałtowo powyższe należności producentowi systemu @City, Producent nie odpowiada za zmiany warunków oferowanych lub zakończenie usług wykonywanych przez podmioty zewnętrzne.

Producent systemu nie ponosi odpowiedzialności za jakość usług świadczonych przez podmioty trzecie w tym operatora GSM, zewnętrzny hosting @City. Producent nie ponosi odpowiedzialności za pogorszenie się zasięgu propagacji fal radiowych (np. z powodu powstania nowych zabudowań, zmiany lokalizacji stacji nadawczych GSM (BTS), zadrzewienia, itd.).

W przypadku limitów transferu danych (szczególnie dla NBIoT) konfigurację i aktualizację oprogramowania należy przeprowadzić na początku okresu abonamentowego, przy jak najmniejszym aktualnym zużyciu danych. W przeciwnym razie istnieje możliwość zablokowania urządzenia do końca okresu rozliczeniowego ze względu na blokady związane z przekroczeniem limitu transferu.

Za jakość połączenia GSM odpowiada operator GSM a nie producent systemu @City.

Użytkownik oświadcza że przyjmuje do wiadomości poniższe informacje i wyraża na nie zgodę.

2.2. Warunki szczególne @City LoRaWAN.

Użytkownik ponosi koszty oraz odpowiada za terminowe regulowanie opłat dzierżawy i montażu bramki LoRaWAN, Serwera Komunikacyjnego/Aplikacyjnego LoRaWAN i hostingu @City. Brak ciągłości usług może spowodować nieodwracalne zmiany krytycznych parametrów transmisji i permanentne zablokowanie systemu (jak np. zmiana stałego adresu IP, utrata domeny, Utratę danych/konfiguracji na serwerze, utratę oprogramowania, kopi zapasowych, itd.).

W przypadku kiedy użytkownik reguluje ryczałtowo powyższe zobowiązania producentowi @City, producent nie ponosi odpowiedzialności za zmianę warunków czy zakończenie usług wykonywanych przez podmioty zewnętrzne.

Producent systemu nie ponosi odpowiedzialności za usługi świadczone przez podmioty zewnętrzne w tym ewentualnego operatora LoRaWAN, hosting dla serwera sieciowego/aplikacyjnego LoRaWAN, zewnętrzny hosting @City. Producent nie ponosi odpowiedzialności za pogorszenie się zasięgu propagacji fal radiowych (np. z powodu powstania nowych zabudowań, zmiany lokalizacji bramek LoRaWAN, uszkodzenia bramek LoRaWAN, zaników zasilania, zadrzewienia, zakłóceń, zaników sygnału itd.).

W przypadku limitów transferu danych konfigurację i aktualizację oprogramowania należy przeprowadzić na początku okresu abonamentowego, przy jak najmniejszym aktualnym zużyciu danych. W przeciwnym razie istnieje możliwość zablokowania urządzenia do końca okresu rozliczeniowego ze względu na blokady związane z przekroczeniem limitu transferu. Aktualizację należy przeprowadzić po jednym sterowniku od początku do końca oraz przetestowania poprawności pracy. Uruchomienie aktualizacji dla wszystkich sterowników może spowodować całkowite zablokowanie pasma radiowego na wiele dni.

LoRaWAN wykorzystuje ogólnie dostępne otwarte pasma radiowe (433 lub **868 MHz**), które mogą być zakłócane lub zajęte innymi urządzeniami pracującymi na tych samych częstotliwościach. Producent nie ponosi odpowiedzialności za jakość komunikacji w powyższym przypadku.

Użytkownik odpowiada za pokrycie obszaru odpowiednią ilością bramek LoRaWAN i ich lokalizacją aby uzyskać odpowiedni poziom sygnałów dla wszystkich urządzeń oraz całego systemu @City LoRaWAN.

W miejscach bardzo narażonych na zakłócenie sygnału można zastosować urządzenia @City GSM.

Użytkownik oświadcza że przyjmuje do wiadomości poniższe informacje oraz wyraża na nie zgodę.

3. Konfiguracja Systemu @City (LoRaWAN, GSM)

Konfigurację systemu przeprowadza się przez interfejs WWW. Konfiguracja jest bardzo krytyczna dla sterowników @City i niewłasciwe ustawienia mogą spowodować całkowite zablokowanie systemu. Zaleca się aby pełną konfigurację szablonu (domyślne ustawienia) przeprowadził i przetestował producent systemu @City.

3.1. Konfiguracja sterowników @City - Nadawanie Nazw

Adres sterownika 000000000000000 (15 zer dla GSM/16 dla LoRaWAN) jest adresem domyślnym odnoszącym

się do wszystkich sterowników z rodziny (tj. dla tego samego **Vendor Code** oraz **File Code** oraz typu sterownika **LoRaWAN/GSM**. W przypadku gdy sterownik nie posiada zdefiniowanej własnej indywidualnej konfiguracji, wgrywana jest do niego konfiguracja domyślna.

W przypadku sterowników GSM adres ten odpowiada unikalnemu numerowi IMEI (15 znaków) przyznanemu przez producenta modemu GSM.

W przypadku LoRaWAN adres ten odpowiada unikalnemu numerowi "Dev EUI" nadanemu fabrycznie przez producenta modemu LoRaWAN (16 znaków w kodzie hexadecymalnym).

Vendor Code - jest parametrem unikalnym dla klienta (użytkownika)

File Code - jest parametrem oznaczającym rodzaj firmwaru (zależny od sprzętu oraz dostępnych algorytmów)

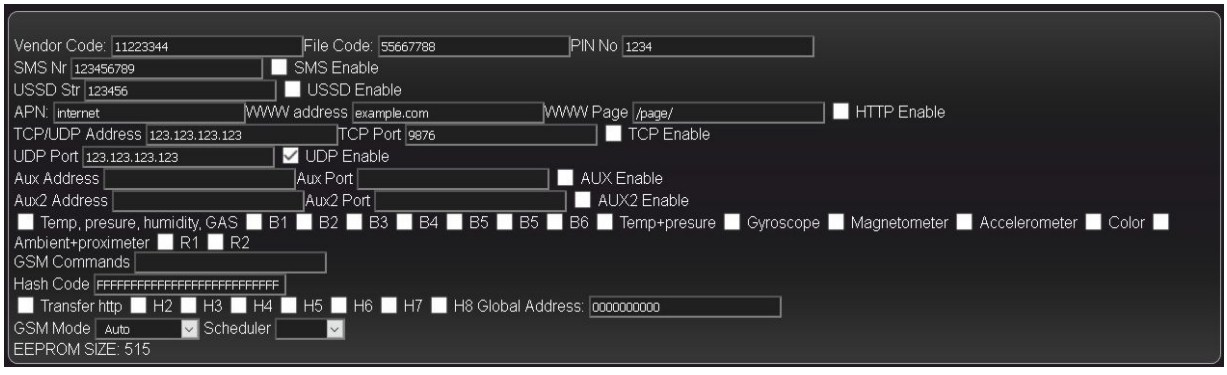
W większości przypadków wystarczające jest skonfigurowanie tego jednego urządzenia dla całego systemu lub jako szablon dla pozostałych sterowników. W przypadku tworzenia konfiguracji nowego sterownika, te ustawienia są kopiowane z szablonu.

Zarówno firmware jak i konfiguracje dla wszystkich instalacji (instancji) znajduje się na serwerach producenta systemu @City dostępnych przez WWW, do którego użytkownik może mieć dostęp. Poprawna konfiguracja jest jednak bardzo krytyczna, i nie zaleca się wprowadzania zmian bez testów na kilku urządzeniach z pełnym fizycznym dostępem. Więcej informacji znajduje się ogólnych warunkach systemu @City oraz warunkach szczegółowych dla konkretnego sposobu komunikacji.

3.2. Konfiguracja ogólna sterowników @City LoRaWAN i GSM

3.2.1 Konfiguracja ogólna sterownika @City GSM

Przed rozpoczęciem konfiguracji należy zapoznać się z informacjami znajdującymi się ogólnych warunkach systemu @City oraz warunkach szczegółowych dla systemu **@City GSM**.



Vendor Code - zawiera 8 znaków zapisanych w kodzie hexadecymalnym dedykowanym jednemu

klientowi (użytkownikowi). Jest on przyznany na etapie produkcji sterownika. Próba zmiany może spowodować permanentne uszkodzenie sterownika.

File Code - zawiera 8 znaków zapisanych w kodzie hexadecymalnym dedykowanym jednemu wariantowi firmwaru sterownika. Jest on przyznany na etapie produkcji sterownika i może być zależny od rodzaju komunikacji (GSM/LoRaWAN) i wyposażenia dodatkowego, np.: czujniki, ilość wejść/wyjść oraz indywidualnych algorytmów. Zmiana może spowodować permanentne uszkodzenie lub zablokowanie sterownika.

PIN No. - 4 cyfrowy numer pin jeśli został ustawiony dla karty SIM. Nie zaleca się ustawiania numerów PIN. W przypadku plastikowych kart SIM można usunąć je w telefonie komórkowym. Wprowadzenie niepoprawnego SIMu może spowodować permanentne zablokowanie karty w urządzeniu, do którego docelowo nie będziemy mieć fizycznego dostępu.

SMS No. - SMS numer w przypadku przesyłania statusów poprzez SMSy. Możliwość ta jest dostępna w zależności od usługi i operatora (2G/CATM1). Wymaga także włączenia flagi: **SMS Enable.**

USSD Str - Komenda USSD przy przesyłaniu statusów po USSD. Opcja ta jest dostępna tylko dla wybranych typów modemów GSM (2G/3G+GPS). Wymagane jest włączenie opcji: **USSD Enable.** Operator musi udostępnić i aktywować usługę USSD.

APN - Access Point Name. Nazwa punktu dostępowego do Internetu np. **internet** (w przypadku usług specjalnych jak LTECATM1 lub NBIoT, może on być przyznawany indywidualnie przez operatora)**.**

WWW Address - adres dostępowy komunikacji przez HTTP.

WWW Page - adres strony, na które są przesyłane statusy sterowników oraz odbierane komendy.

HTTP Enable - Włącza transmisję danych HTTP. Metoda ta generuje wielokrotnie większą ilość przesyłanych danych niż wszystkie pozostałe metody komunikacji, co może powodować wzrost kosztów, przekroczenie limitu transferu lub brak możliwości korzystania z niektórych usług jak np. NBIoT.

TCP/UDP Address - adres IP serwera @City odbierającego i przesyłającego dane między chmurą a urządzeniami. Zaleca się stosować stały adres IP a nie adres domeny internetowej.

TCP Port - Port do łączności TCP/IP

TCP Enable - Pozwala na włączenie transmisji TCP/IP. Ramki transmisyjne i potwierdzenia TCP zwiększają liczbę danych w stosunku do transmisji UDP, jednak zapewniają poprawność danych, potwierdzenia i gwarantują ich dostarczenie jeśli komunikacja jest aktywna.

UDP Port - Port do odbierania statusów poprzez UDP

UDP Enable - Włączenie transmisji UDP

Aux Address, Aux Port, Aux Enable - przyszłe zastosowania

Aux2 Address, Aux2 Port, Aux2 Enabled - przyszłe zastosowania

Włączenie obsługi czujników (muszą być one fizycznie zamontowane na module @City). W przeciwnym razie urządzenie może pracować znacznie wolniej i mniej stabilnie. Czujniki montowane są na etapie produkcji dla całych serii produkcyjnych.

Temp, presure, humidity, gas - zintegrowany czujnik temperatury, ciśnienia, wilgotności i jakości powietrza

Temp+Presure - Zintegrowany czujnik temperatury, ciśnienia

Gyroscope - Czujnik żyroskopowy w osiach (X, Y, Z)

Magnetometr - Czujnik magnetyczny w osiach (X, Y, Z)

Accelerometer - Czujnik przyśpieszenia/wibracji w osiach (X, Y, Z)

Color - Czujnik koloru (R, G, B, IR, B2)

Ambient+proximeter - zintegrowany czujnik poziomu oświetlenia oraz przybliżenia

GSM Commands - dodatkowe komendy inicjalizacyjne modem

Hash Code - Dodatkowy kod szyfrujący. Nie zmieniać.

Transfer HTTP - Dodatkowe opcje komunikacji HTTP

Global Address - Adres globalny sterownika przy sterowaniu urządzenie-urządzenie.

GSM Mode - Tryb łączności GSM (2G Only, LTE Only, CATM1, NBIoT, 2G+CAT M1, LTE 800, LTE 1800). **Niepoprawne ustawienie trybu komunikacji może skutkować permanentnym zablokowaniem komunikacji urządzenia.**

3.2.2. Konfiguracja ogólna sterownika @City LoRaWAN

Większość opcji jest taka sama jak w sterowniku GSM. W zasadzie wszystkie pola odnoszące się do komunikacji GSM są niewykorzystane podczas pracy sterownika LoRaWAN.

Po stronie urządzenia @City LoRaWAN konfiguracja jest bardzo prosta:

Application EUID - ID aplikacji dla serwera LoRaWAN (16 znaków w kodzie hex) – aplikacja zdefiniowana na serwerze Sieciowym/Aplikacyjnym LoRaWAN do którego przesyłamy dane.

Application Key - klucz autoryzacji do aplikacji dla serwera LoRaWAN (jak wyżej)

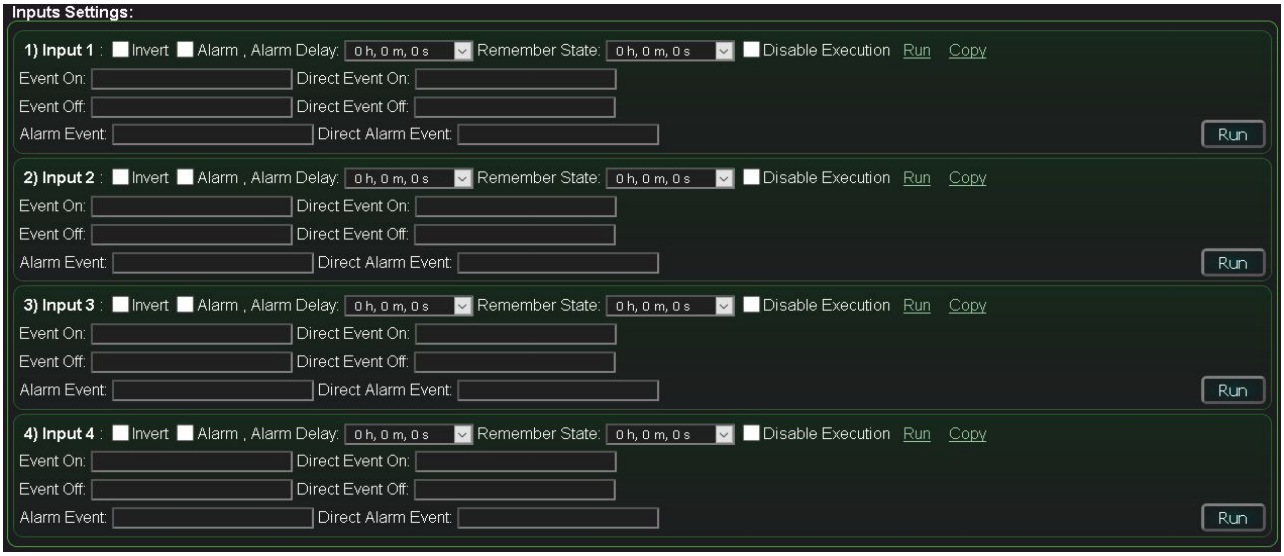
Disable Adaptive Data Rate - Zablokowanie adaptacyjnego doboru prędkości. Pozwala to na wymuszenie stałej prędkości pracy urządzenia. W niektórych sytuacjach może to spowodować duże problemy z komunikacją. Należy brać pod uwagę że wraz z polepszeniem się parametrów RSSI i SNR w trybie adaptacyjnym prędkość znacznie wzrasta. Znacznie skraca to czas przesyłu danych drogą radiową „On The Air Time" oraz znacznie częściej informacje mogą być przesyłane między urządzeniem a serwerem i vice versa.

Data Rate (DR) - wybór prędkości łącza LoRaWAN. Prędkość ta nie odnosi się do Bootloader'a. W przypadku gdy sterownik pracuje w trybie adaptacyjnego ustawienia prędkości, jest to tylko wartość startowa, gdyż sterownik po kilku/kilkunastu próbach transmisji autonomicznie wybierze sobie optymalną prędkość tak aby ograniczyć czas przesyłu wiadomości w eterze.

Update Settings – zapisuje konfigurację startową dla wszystkich ustawień

Reszta konfiguracji @City LoRaWAN znajduje się w pozostałych elementach "łańcucha" komunikacyjnego LoRaWAN w rozdziale 4.

3.3. Konfiguracja wejść binarnych



Wejścia binarne posiadają szereg funkcji i parametrów umożliwiających autonomiczną pracę sterownika:

Invert - negacja wejścia, przy podłączeniu czujników normalnie włączonych (NC).

Alarm - aktywacja funkcji alarmu.

Alarm Delay - Czas opóźnienia alarmu. W przypadku gdy stan wejścia wróci do stanu pierwotnego przed upływem tego czasu, alarm nie zostanie aktywowany.

Remember State - Czas zapamiętania zmiany stanu wejścia.

Disable Execution - Blokada uruchomienia zdarzeń powiązanych z wejściami.

Run - Uruchomienie komendy konfiguracyjnej wejście (Ad-Hoc)

Copy - Skopiowanie komendy konfigurującej wejście do schowka

Event On - Opis uruchomienia zdarzenia dla poziomu wysokiego wejścia (1)

Direct Event On - Kod zdarzenia do uruchomienia przy włączeniu wejścia (0=>1)

Event Off - Opis uruchomienia zdarzenia dla poziomu niskiego wejścia (0)

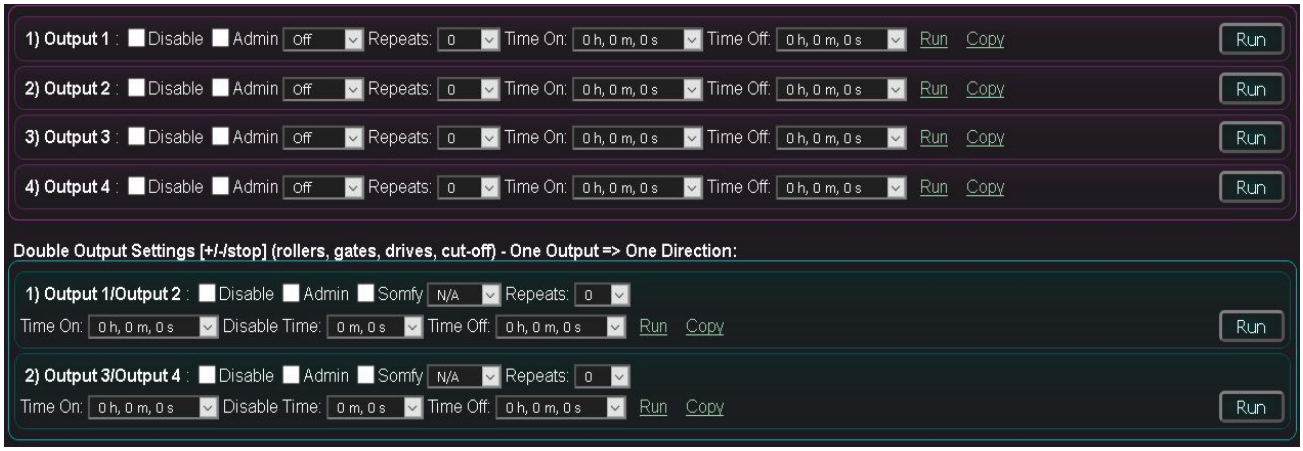
Direct Event Off - Kod zdarzenia do uruchomienia przy wyłączeniu wejścia (1=>0)

Alarm Event - Opis zdarzenia Alarmu.

Direct Alarm Event - Kod zdarzenia do uruchomienia w przypadku wystąpienia alarmu

Update Settings – zapisuje konfigurację startową dla wszystkich ustawień

3.4. Konfiguracja Wyjść Binarnych



Inteligentne wyjścia binarne mogą pracować jako pojedyncze lub podwójne. Formularz pozwala utworzyć konfigurację startową dla sterownika (jeśli ją zatwierdzimy przyciskiem **Update.**

Formularz jednocześnie służy jako kreator zdarzeń dla wyjść, które mogą być uruchamiane przyciskiem **Run** lub kopiowane do schowka w celu wykorzystania w konfiguracji sterownika np.

- terminarz
- praca autonomiczna
- powiązanie wyjść z wejściami binarnymi (reagowanie na zmianę stanu)
- powiązanie wyjść z wejściami pomiarowymi (reagowanie na zmianę progu)

Konfiguracja wyjść pojedynczych:

Disable - Blokada wyjścia w trybie pojedynczym (np. jeśli użyte jest przy sterowaniu napędami, żeby przypadkiem nie uszkodzić rolet, bram, siłowników)

Admin - Flaga administracyjna jest wymagana gdy zmieniamy krytyczne ustawienia

State - wybór stanu (przy starcie lub przy uruchomieniu zdarzenia przyciskiem **run**)

Repeats - Liczba powtórzeń (cykliczne zmiany stanu)

Time On - Czas włączenia wyjścia

Time Off - Czas wyłączenia wyjścia (ma to znaczenie przy powtarzaniu zdarzeń)

Run - Uruchomienie zdarzenia dla wyjścia

Copy - Skopiowanie zdarzenia do schowka

Update Settings – zapisuje konfigurację startową dla wszystkich ustawień

Konfiguracja wyjść podwójnych:

Disable - Blokada pary wyjść w trybie podwójnym (np. jeśli są używane jako wejścia pojedyncze)

Admin - Flaga administracyjna jest wymagana gdy zmieniamy krytyczne ustawienia jak tryb pracy napędów

Somfy - tryb pracy napędów (zaznaczone => Somfy / niezaznaczone => Direct Servo)

State - wybór stanu (przy starcie lub przy uruchomieniu zdarzenia przyciskiem **run**)

Repeats - Liczba powtórzeń (cyklicznej zmiany stanów)

Time On - Czas włączenia danego stanu

Disable Time - Czas blokady wyjść (minimalny czas przerwy między zmianami stanu wyjść) dla zabezpieczenia napędów przed uszkodzeniem.

Time Off - Czas wyłączenia wyjścia (ma to znaczenie przy powtarzaniu zdarzeń)

Run - Uruchomienie zdarzenia dla napędu

Copy - Skopiowanie zdarzenia do schowka

Update Settings – zapisuje konfigurację startową dla wszystkich ustawień

3.5. Konfiguracja Wejść Pomiarowych ADC oraz czujników dodatkowych (XIN)

Invert - odwrócona skala pomiarowa (100%-x) wejścia ADC

Alarm L - Włączenie opcji generowania alarmu w przypadku spadku wartości poniżej progu minimalnego

Alarm H - Włączenie opcji generowania alarmu w przypadku przekroczenia wartości powyżej progu maksymalnego

Alarm Delay - Czas opóźnienia alarmu. W przypadku gdy stan wejścia wróci do poziomu z zakresu „OK" przed upływem tego czasu alarm nie zostanie aktywowany.

Event Disable - Blokowanie wykonywania zdarzeń

Admin - Flaga admin umożliwiająca zmianę konfiguracji wejścia pomiarowego

Low Event - opis zdarzenia wykonanego przy przekroczeniu progu niskiego

Low Direct - kod zdarzenia do wykonania po obniżeniu wartości poniżej progu dolnego

Low Level - Poziom progu dolnego

OK Event - Opis zdarzenia z zakresu „OK"

OK Direct - kod zdarzenia do wykonania po wejściu w zakres „OK"

HIGH Event - Opis zdarzenia dla progu górnego

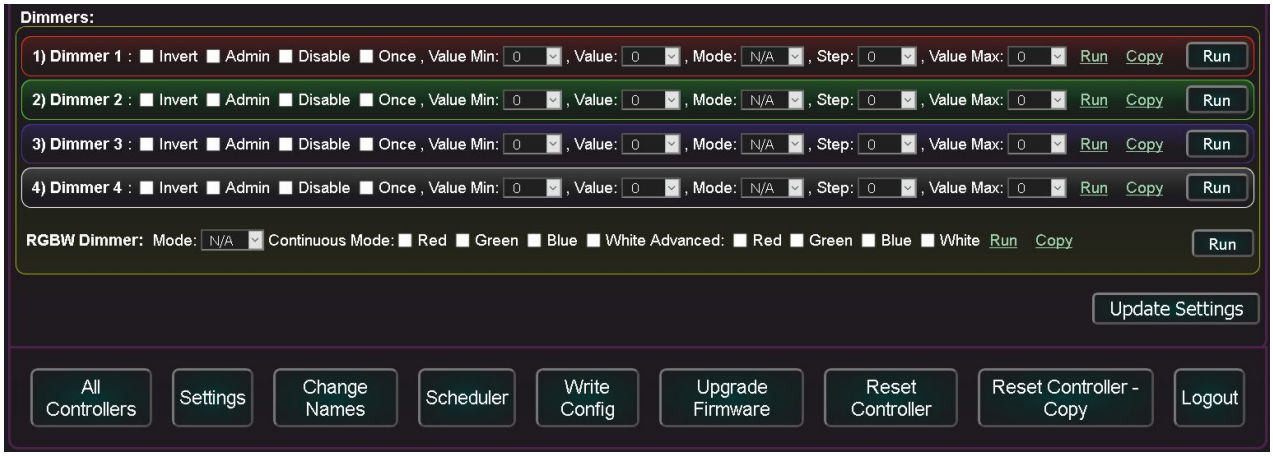
HIGH Direct - kod zdarzenia do wykonania po przekroczeniu wartości progu górnego

High Level - Poziom progu górnego

Run – uruchomienie zdarzenia konfiguracyjnego (zmiana konfiguracji ADC Ad-Hoc)

Update Settings – zapisuje konfigurację startową dla wejść ADC

3.6. Konfiguracja ściemniaczy PWM/0..10V



Invert - Odwrócenie polaryzacji ściemniaczy (100% - x)

Admin - Flaga administracyjna pozwalająca na zmianę krytycznych opcji

Disable - Blokowanie wyjścia ściemniacza

Once - Jednokrotna zmiana ustawień ściemniacza (następnie zatrzymanie ściemniacza)

Value Min - wartość minimalna ustawienia ściemniacza

Value - wartość docelowa ściemniacza

Mode - Tryb ustawienia ściemniacza (Stop/-/+/Set)

Step - Krok zmiany wartości poziomu ściemniacza

Value Max - wartość maksymalna ustawienia ściemniacza

Run - Uruchomienie zdarzenia ściemniacza

Copy - Skopiowanie zdarzenia do schowka

Ściemniacz RGBW pobiera wartości ustawień z pojedynczych kolorów.

Dodatkowo umożliwia uruchomienie trybu ciągłej zmiany kolorów korzystając z presetów ściemniaczy pojedynczych.

Update Settings – zapisuje konfigurację startową dla wszystkich ustawień

Przyciski:

Update Settings - zapisanie konfiguracji w systemie @City

All Controllers - lista wszystkich sterowników

Settings - ustawienia bieżącego sterownika

Change Names - zmiana nazw bieżącego sterownika

Scheduler - edytor terminarza bieżącego sterownika

Write Config * - wysłanie komendy do pobrania konfiguracji przez sterownik

Upgrade Firmware * - wysłanie komendy do pobrania firmwaru przez sterownik

Reset Controller * - wysłanie komendy resetu sterownika

Reset Controller - Copy - kopia zdarzenia resetu sterownika do schowka

Logout - wylogowanie użytkownika (dla bezpieczeństwa należy też zamknąć wszystkie otwarte instancje przeglądarki internetowej, które mogą przetrzymywać w pamięci podręcznej parametry logowania).

*** - wysyłanie komendy oznacza dodanie do kolejki zdarzeń. Sterownik łącząc się z systemem @City pobiera te zdarzenia.**

3.7. Konfiguracja kalendarza-terminarza

Kalendarz-terminarz pozwala na autonomiczne uruchamianie zdarzeń (komend) powtarzalnych lub zaplanowanych w czasie. Przykładem może być np. włączenie lampy ulicznej o 17 godzinie zimą i wyłączenie o 7 rano.

Del (Delete) - całkowite usunięcie pozycji terminarza.

En. (Enable) - Aktywacja pozycji terminarza (tylko te pozycje będą wykonywane które mają ustawioną flagę Enable)

Name - Nazwa zdarzenia (można opisać zdarzenie w rozpoznawalny sposób)

Event Code - kod zdarzenia w kodzie hexadecymalnym (skopiowany ze schowka przy tworzeniu komend)

Pola miesięcy (Ja, Fe, .., No, De) - miesiące Styczeń..Grudzień, w których zdarzenie będzie uruchamiane

Day - Dzień. Można wybrać dowolny dzień miesiąca lub **"*"** dla wszystkich (uruchamianie zdarzenia co dziennie).

Pola dni tygodnia (Mo, Tu, .. Su) - można wybrać dni tygodnia, w których zdarzenie będzie wykonywane.

Hour - Godzina. Można wybrać dowolną godzinę lub "*" dla wszystkich (uruchamianie zdarzenia co godzinę).

Min - Minuta. Można wybrać dowolną minutę lub "*" dla wszystkich (uruchamianie zdarzenia co minutę).

Realizowany jest algorytm **"and"** między wszystkimi polami (poza Name), więc wszystkie muszą zostać spełnione aby zdarzenie zostało uruchomione.

Np. Włączenie Lamp ulicznych (listopad, grudzień, styczeń, luty) o godzinie 17.01 poza niedzielami.

En - zaznaczone

Event code - 00002101010000000000 //uruchomienie 1'szego wyjścia binarnego

Pola Miesięcy - zaznaczone tylko **No, De, Ja, Fe**

Day - wybrana **"*"** dla każdego dnia miesiąca

Hour - wybrana godzina **17**

Min - wybrana minuta **01**

Pola dni tygodnia - wybrane wszystkie poza **Su**

4. Konfiguracja Infrastruktury Sieciowej LoRaWAN

Rozdział ten odnosi się tylko do komunikacji LoRaWAN. W przypadku systemów pracujących przy wykorzystaniu innych sposobów transmisji można go pominąć.

Zgodnie ze specyfikacją sieci LoRaWAN sterownik łączy się z chmurą @City pośrednio przez:

- Gateway LoRaWAN (np. Kerlink) z zainstalowanym pakietem Semtech Packet Forwarder (SPF) do przesyłania dwukierunkowego wszystkich pakietów LoRaWAN po protokóle UDP do Network Serwer'a LoRaWAN.
- Network Server LoRaWAN - do komunikacji między bramką LoRaWAN a serverem aplikacyjnym.
- Application server do przesyłania danych do chmury @City

4.1. Konfiguracja Bramki LoRaWAN (LoRaWAN Gateway).

Na rynku jest wiele bramek LoRaWAN, które jednocześnie mogą zawierać szereg dodatkowych opcji:

- Bramka Komunikacyjna LoRaWAN
- Pakiet SPF (Semtech Packet Forwarder)
- LoRaWAN Network Server
- LoRaWAN Application Server
- Baza danych
- Moduł Komunikacyjny LTE

4.1.1. Podstawowa konfiguracja bramki LoRaWAN

Bramka LoraWAN powinna być dostępna przynajmniej z jednej stacji konfigurującej.

W przypadku instalacji przez interfejs Ethernet/WiFi i konfiguracji tylko z lokalnej sieci LAN/WLAN bezpieczeństwo bramki nie jest zbyt krytyczne (o ile nie udostępnimy dostępu do bramki z zewnątrz tj. Internetu).

W przypadku bramki LoRaWAN podłączonej tylko poprzez GSM/LTE konieczne jest zabezpieczenie bramki przed dostępem i atakami różnego typu.

- Jeśli chcemy mieć możliwość podłączenia się zdalnego do bramki LoRaWAN, musi ona posiadać publiczny +

stały adres IP i dostępną usługę SSH. W innym przypadku konieczne będzie fizyczne podłączenie się do bramki przez interfejs Ethernet lub WiFi.

- koniecznie należy ustawić skomplikowane hasła dostępu dla wszystkich użytkowników na urządzeniu.

- wyłączyć wszystkie nieużywane usługi jak Telnet, FTP, POP, SMTP, IMAP, WWW itd mogące być celem ataków "zajmujących" bramkę innymi procesami jak np próby logowania.

- można ograniczyć możliwość logowania się tylko ze stacji z wybranymi stałymi adresami IP co stanowi dość skuteczne zabezpieczenie przed włamaniem. Dotyczy to także pozornie mało znaczących usług jak ICMP (ping), HTTP, FTP, itd.

- po pełnej konfiguracji wielotygodniowych testach systemu możemy zablokować wszystkie usługi zewnętrzne i dostęp zdalny, co jednak utrudni serwis, rewizję i możliwość sprawdzenia logów bramki.

4.1.2. Konfiguracja Semtech Packet Forwarder (SPF)

Zadaniem SPF jest przesyłanie pakietów LoRaWAN do serwera sieciowego LoRaWAN poprzez sieć IP (protokołem UDP) na wymagany adres serwera sieciowego LoRaWAN.

LoRaWAN Gateway wraz z SPF jest transparentny i przepuszcza wszystkie pakiety w obie strony (przelotka).

Nie przetwarza on ani nie autoryzuje paczek danych w żadną stronę.

Konfiguracja SPF jest bardzo prosta i polega na "skierowaniu" go na wymagany serwer sieciowy LoRaWAN.

Należy zalogować się poprzez SSH do bramki LoRaWAN przy pomocy użytkownika i hasła określonego przez producenta urządzenia.

Należy zainstalować SPF zgodnie z instrukcją producenta bramki LoRaWAN.

Katalogiem konfiguracyjnym SPF jest "**/user/spf/etc/**" jednak w zależności od producenta bramki LoRaWAN może on znajdować się w innych lokalizacjach.

Główna konfiguracja SPF znajduje się w pliku "**/user/spf/etc/global_conf.json"**, którą edytujemy dostępnym edytorem (np. vi lub nano). Zmieniamy wartość parametru: **"server_address"** wpisując stały adres IP serwera sieciowego lub nazwę domeny (Wymaga dodatkowo poprawnie skonfigurowanej usługi klienta DNS).

Domyślnymi portami komunikacyjnymi w obie strony jest **1700** (jeśli zamierzamy je zmienić, konieczne jest zrobienie tego samego na serwerze sieciowym LoRaWAN) wpisując identyczne wartości.

Logi pakietu SPF znajdują się w katalogu **/user/spf/var/logs/** w pliku **spf.log** oraz w jego kopiach archiwalnych.

Konfiguracja sieciowa linux bramki LoRaWAN znajduje się standardowo w katalogu "**/etc/**", gdzie można włączyć/wyłączyć standardowe usługi sieciowe oraz zabezpieczyć server.

Należy także zmienić hasła wszystkich użytkowników dostępnych w systemie komendą **passwd** aby zabezpieczyć przed nieautoryzowanym dostępem osób nieuprawnionych. Należy także zmienić hasło użytkownika do obsługi przez WWW.

Najlepiej także wyłączyć komunikację WiFi, gdyż intruzi mogą próbować stosować ataki przez to medium transmisji.

Po wykonaniu tej konfiguracji należy zresetować bramkę komendą **reboot**.

4.2. Konfiguracja Serwera sieciowego i aplikacyjnego LoRaWAN (Network/Application Server)

Istnieje wiele rozwiązań serwerów sieciowych i aplikacyjnych (w tym darmowych). Każdy z nich posiada własny sposób integracji z zewnętrznymi usługami i systemami (np. chmurami jak @City). Z tego względu system @City musi posiadać interfejs do integracji z zainstalowanym serwerem LoRaWAN.

W przypadku systemu produkcyjnego możemy użyć darmowej usługi "The Things Network", o ile mieścimy się w bardzo dużych ograniczeniach dziennych zdefiniowanych dla każdego urządzenia {szczególnie "On The Air Time" (30s **) oraz małą liczbę komend wysyłanych do urządzenia (10 **)}.

*** orientacyjne aktualne dzienne ograniczenia dla urządzenia, mogą się zmienić.*

W przypadku konieczności ładowania nowego firmwaru i konfiguracji konieczne jest więc stosowanie własnego serwera LoRaWAN (sieciowego+aplikacyjnego).

Daje nam to kilka możliwości:

- użycie TTN do pracy w środowisku produkcyjnym oraz dedykowanego serwera fizycznego tylko do aktualizacji konfiguracji i nowego firmwaru (*).
- użycie dedykowanego serwera fizycznego dla wszystkich powyższych czynności.
- użycie 2 dedykowanych serwerów fizycznych (jeden dla środowiska produkcyjnego a drugi do aktualizacji oprogramowania i konfiguracji) (*)

W niektórych systemach konfiguracja + firmware jest stały (dla wszystkich dostępnych sterowników w systemie) i zainicjowany na etapie wstępnej konfiguracji systemu co upraszcza wybór.

(*) - w tych przypadkach konieczne jest posiadanie drugiej bramki LoRaWAN ustawionej na drugi serwer do aktualizacji konfiguracji i firmwaru aby środowisko produkcyjne pracowało w sposób ciągły. Dla mało krytycznych aplikacji można zmienić w konfiguracji jednej bramki LoRaWAN dedykowany serwer LoRaWAN, co jednak spowoduje utratę łączności ze środowiskiem produkcyjnym i nieprawidłową pracę tych urządzeń.

Należy zdawać sobie sprawę że aktualizacja oprogramowania pojedynczego sterownika LoRaWAN trwa około godziny, przy dobrym zasięgu (DR>=4), więc warto użyć dodatkowej bramki do upgradu firmwaru i konfiguracji. Przy słabym zasięgu (DR<4) konfiguracja i aktualizacja firmwaru jest nie możliwa i wymaga usytuowania Bramki z komunikacją LTE w pobliżu aktualizowanych urządzeń.

4.2.1. Konfiguracja serwera sieciowego LoRaWAN

Na serwerze sieciowym LoRaWAN należy dodać bramkę komunikacyjną LoRaWAN (po adresie znajdującym się na jej obudowie lub w pliku "**user/spf/etc/local_conf.json**" lub wyświetlanym w logach "**/user/spf/var/log/spf.log**". Należy sprawdzić w logach serwera sieciowego czy bramka komunikacyjna łączy się z serwerem.

Kolejnymi krokami jest konfiguracja serwera aplikacyjnego (znajdującego się najczęściej na tym samym urządzeniu co serwer sieciowy).

Kolejne czynności, które należy wykonać zależą od zastosowanego rozwiązania serwera aplikacyjnego i dostępności interfejsu Back-End/Front-End. Intefejs ułatwia "pierwsze kroki" oraz konfigurację systemu.

Ogólnie należy:

- Dodać aplikację z określonym ID dla środowiska produkcyjnego
- wygenerować klucze api (API KEYS) do linkowania dla aplikacji oraz dodanie uprawnień "right-application-link" (należy skopiować klucz wygenerowany automatycznie).
- wygenerować klucze api (API KEYS) dla integracji poprzez webhook (podając nazwę aplikacji oraz webhooka) z prawami: "right-application-traffic-down-write" "right-application-traffic-read" "right-application-traffic-up-write" (należy skopiować klucz wygenerowany automatycznie). Klucz ten jest używany do komunikacji po stronie serwisu @City razem z nazwą "webhooka".
- utworzyć "webhook" integracyjny do aplikacji z serwerem @City podając:
    - ID aplikacji
    - ID webhook'a
    - adres docelowy **http://*.*.*.*/IoT/** oraz ścieżki **up.php**
- Dodanie ręczne lub skryptem wszystkich urządzeń @City LoRaWAN (z unikalnym DEV EUI) podając dodatkowo takie same wartości dla każdego pola:
    - ID dla aplikacji
    - EUID dla aplikacji

- Root Key dla aplikacji
- **Frequency plan** (regionalne ustawienia pasma LoRaWAN np **EU_863_870** dla Europy)
- DEV EUI (indywidualnego adresu każdego urządzenia nadanego przez producenta modułu). Jeśli nie znajduje się na obudowie, należy znaleźć w logach serwera aplikacyjnego adresy nieznanych urządzeń próbujących łączyć się z serwerem.
- lorawan-version=1.0.2, lorawan-phy-version=1.0.2-b
- LoRaWAN autoryzacja OTAA

5. Ogólne parametry pracy urządzenia @City GSM / LoRaWAN

Zakres temperatury pracy	- 40C .. +65C
Wilgotność	0..80% r.H. bez kondensacji (urządzenie)
Zasilanie GSM	5VDC @ 2A ±0.15 V (dla czujnika PPM oraz przy
podłączenia przekaźników)	3.5VDC..4.2VDC@2A (w pozostałych przypadkach)
Zasilanie LoRaWAN	5VDC @ 300mA ±0.15 V (dla czujnika PPM oraz przy
podłączenia przekaźników)	3VDC..3.6VDC@300mA (w pozostałych przypadkach)

Urządzenia GSM+GPS:

Wejście antenowe	50ohm
SIM	nano-SIM lub MIM
	(wybór na etapie produkcji – MIM narzuca operatora sieci)
Homologacja	Orange/T-Mobile

Pasma (Europa)	**Klasa**	**Moc wyjściowa**	**Czułość**
B3,B8,B20 (CATM1 – 800MHz) **	3	+23dB ±2	< -107.3dB
B3,B8,B20 (NB-IoT – 800MHz) **	3	+23dB ±2	< -113.5dB
GSM850,GSM900 (GPRS) *	4	+33dB ±2	< -107dB
GSM850,GSM900 (EDGE) *	E2	+27dB ±2	< -107dB
DCS1800,PCS1900 (GPRS) *	4	+30dB ±2	< -109.4dB
DCS1800,PCS1900 (EDGE) *	E2	+26dB ±2	< -109.4dB

Przy zastosowaniu zewnętrznej anteny wąsko-pasmowej dopasowanej częstotliwościowo dla danego pasma.

*** Tylko z modułem Combo:** 2G, CATM1, NB-IoT

Certyfikaty:

- RED (EU)
- GCF (AU)
- PTCRB (NA)
- FCC, IC (NA/NV)
- RoHS / REACH

GPS/GNSS:

częstotliwość pracy:	1559..1610MHz
impedancja anteny	50ohm
maksymalna czułość *	-160dB stacjonarnie, -149dB nawigacja, -145 zimny start
TTFF	1s (gorący), 21s (ciepły), 32s (zimny)
A-GPS	tak
Dynamika	2g

minimalne odświeżanie 1Hz

- - dopasowana zewnętrzna antena wąskopasmowa

Urządzenia LoRaWAN 1.0.2 (8 kanałów, Tx power: +14dBm) Europa (863-870MHz)

DR	T	modulacja	BR bit/s	Rx Czułość	Rx Testy
0	3min	SF12/125kHz	250	-136dB	-144dB
1	2min	SF11/125kHz	440	-133.5dB	
2	1min	SF10/125kHz	980	-131dB	
3	50s	SF9/125kHz	1760	-128.5dB	
4 **(*)**	50s	SF8/125kHz	3125	-125.5dB	
5 **(*)**	50s	SF7/125kHz	5470	-122.5dB	
6 **(*)**	50s	SF7/250kHz	11000	-119dB	
7		FSK 50kbs	50000	-130dB	

(*) Parametry wymagane do upgradu oprogramownia wewnątrz układowego OTA
(DR) – Data Rate
(BR) – Bit Rate
T – Minimalny okres aktualizacji danych do chmury @City

Praktyczne testy zasięgu LoRaWAN:

Warunki testowe:

- Wewnętrzny Gateway LoRaWAN Kerlink ifemtocell
- pasywna antena zewnętrzna szerokopasmowa umieszczona na zewnątrz na wysokości ~9m od poziomu gruntu Lokalizacja Wygoda gm. Karczew (~110m nad poziomem morza).
- Urządzenie LoRaWAN z wymuszonym DR0 z zewnętrzną anteną szerokopasmową umieszczoną 1.5m nad ziemią na dachu samochodu.
- Tereny wiejskie (łąki, pola o małym zadrzewieniu i rzadkiej zabudowie)

Najdalszym wynikiem był Czersk ~10.5km (~200m nad poziomem morza) przy RSSI równym -136dB (tj. przy maksymalnej czułości modemu LoRaWAN gwarantowanym przez producenta)