POLITECHNIKA WARSZAWSKA

Wydział Mechatroniki

Praca magisterska

Konrad Traczyk

Projekt urządzenia do lokalizacji pojazów w trybie on i offline

Opiekun pracy:
prof. dr hab. Michał Bartyś

Warszawa, 2017

Spis treści

Spis rysunków

Rozdział 1

Wstęp

1.1 Zakres pracy

Celem pracy było zaprojektowanie, wykonanie i oprogramowanie urządzenia stanowiącego dodatkowe zabezpieczenie antykradzieżowe pojazdu w postaci lokalizatora wykorzystującego system GNSS (ang. Global Navigation Satellite System) oraz GSM (ang. Global System for Mobile Communications), a także całego systemu informatycznego, który pozwoliłby na obsłużenie pozyskanych danych. W jego skład wchodzą:

- Aplikacja mobilna na telefon z systemem operacyjnym Android.
- Strona WWW, umożliwiająca zdalny podgląd danych z przypisanych do użytkownika urządzeń.
- Aplikacja serwerowa, która obsługuje zapytania użytkownika oraz zapisująca napływające dane do bazy danych SQLite.

Do dodatkowych wymagań stawianych urządzeniu należą:

- Zapewnienie bezpiecznej wymiany danych.
- Posiadanie zastępczego źródła zasilania, umożliwiającego pracę przy wyłączonym silniku pojazdu, bądź w razie odłączenia akumulatora.
- Niewielkie wymiary w celu umożliwienia łatwego ukrycia urządzenia w pojeździe.

Moduł umożliwia działanie w dwóch trybach. Pierwszy z nich polega na cyklicznym wysyłaniu na serwer pozycji samochodu w trakcie ruchu wraz z m.in. jego prędkością i przyspieszeniem. Dzięki temu możliwy jest zdalny podgląd stylu jazdy kierowcy, co ułatwia sprawowanie kontroli

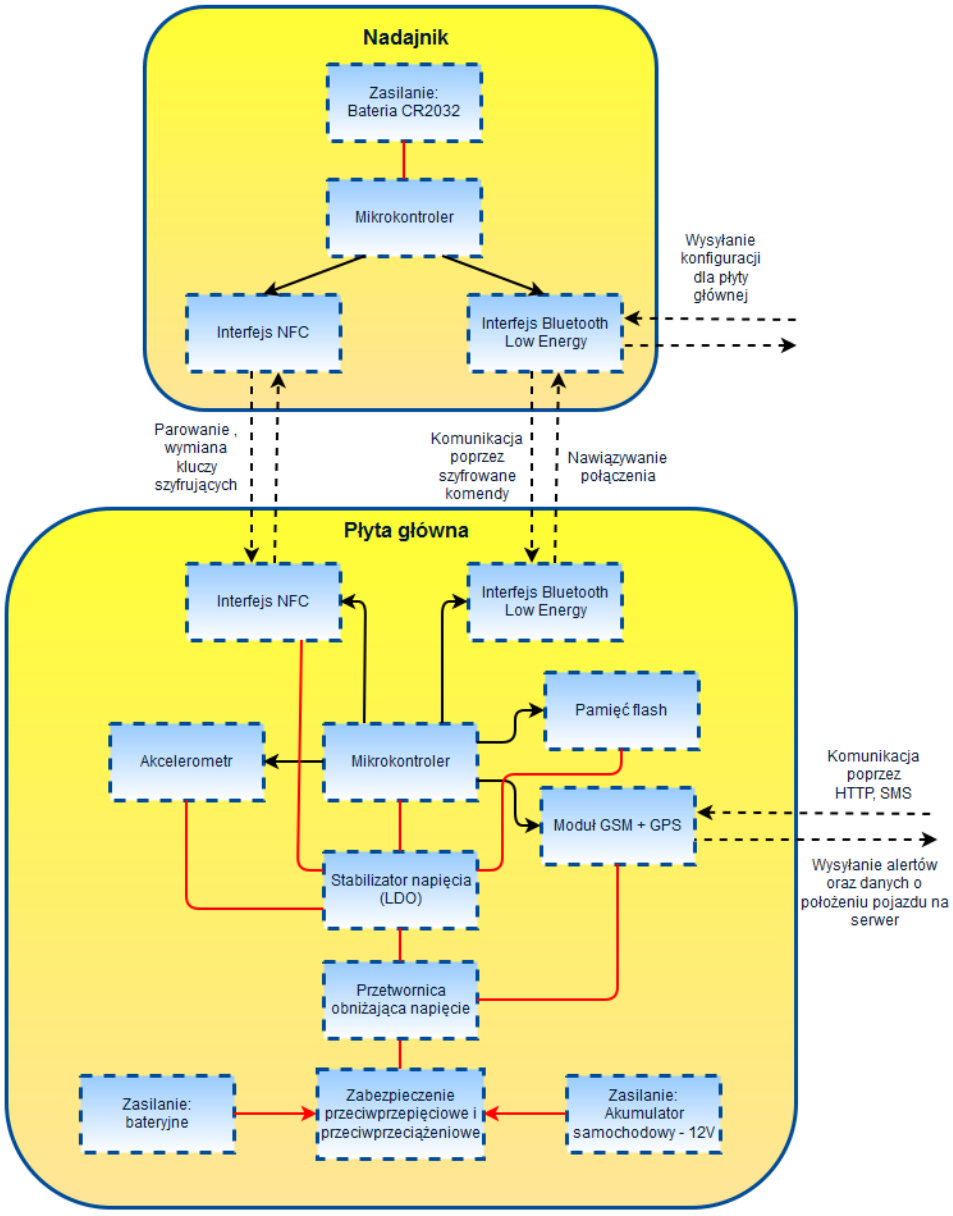
nad flotą pojazdów. Ponadto, dane te zapisywane są również w pamięci nieulotnej urządzenia, co pozwala na ograniczenie kosztów związanych z transmisją bezprzewodową i posiadaniem karty SIM od operatorów GSM.

Drugi tryb uaktywnia się w trakcie postoju i stanowi system alarmowego powiadamiania właściciela pojazdu o nieautoryzowanym jego przemieszczeniu w przypadku kradzieży.

W celu zapewnienia bezpieczeństwa, postanowiono rozbić projekt na dwa urządzenia. Jedno z nich – płytka główna stanowi rdzeń systemu, umożliwiający lokalizację pojazdu oraz wysyłanie danych na serwer. Drugi moduł stanowi układ deaktywujący, którego zadaniem jest dezaktywacja trybu alarmu po odpaleniu samochodu przez upoważnioną do tego osobę. Obie płytki komunikują się ze sobą poprzez protokół Bluetooh Low Energy, zapewniający energooszczędną wymianę danych, co pozwoli na zasilenie układu dezaktywującego z niewielkiej baterii i jego nieprzerwaną pracę nawet przez kilka lat bez konieczności wymiany źródła zasilania. Ponadto, aby umożliwić bezpieczną transmisję niezbędne jest zastosowanie szyfrowania komunikacji. W celu eliminacji ryzyka podsłuchania procesu wymiany klucza szyfrującego, oba urządzenia zostały wyposażone w moduł NFC (ang. Near Field Communication), zapewniającego bezkontaktową komunikację na odległość do 5 cm.

1.2 Schemat blokowy urządzeń

Na przedstawionym poniżej rysunku 1.1 zaprezentowano schemat blokowy urządzeń, które stanowią główną część projektu - moduł płyty głównej oraz moduł dezaktywatora.



Rysunek 1.1: Schemat blokowy urządzeń wchodzących w skład systemu.
Źródło: Twórczość własna

1.3 Istniejące rozwiązania

W ramach pracy przeprowadzono analizę rynkową pod kątem istniejących, ciekawych rozwiązań. Poniżej zaprezentowano trzy najbardziej charakterystyczne z nich.

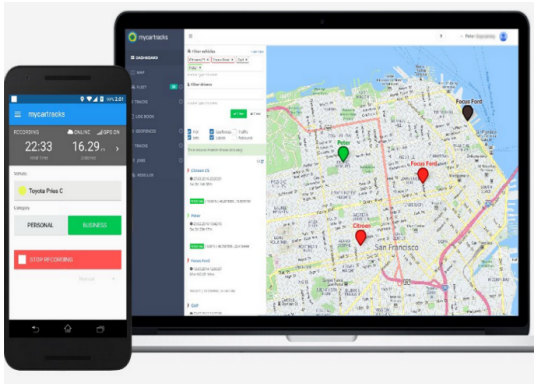
- Spark Nano 5.0 GPS Tracker

  To przenośne urządzenie do śledzenia pozycji geograficznej przy pomocy systemu GPS posiada zasilane bateryjnie. Zapewnia zdalne powiadamianie użytkownika o lokalizacji urządzenia poprzez sieć CDMA, z dokładnością do 2m. Wymiary urządzenia: 64,5 x 40 x 20,5 mm. Urządzenie pozwala na działanie przez ok. 2 tygodnie, przy założeniu pracy przez 1 godzinę dziennie. Producent udostępnia platformę online oraz aplikacje na smartphony z systemem Android oraz IOS, do przedstawiania danych użytkownikowi. Urządzenie domyślnie raportuje położenie co minutę, lecz producent umożliwia zdalne zwiększenie częstotliwości w razie chęci użytkownika. Cena urządzenia: 129,99$. Wizualizację urządzenia przedstawiono na rysunku 1.2.

Rysunek 1.2: Spark Nano 5.0 GPS Tracker. Źródło: [1]

- MyCarTracks - aplikacja mobilna

  Jest to aplikacja na smartphona, która dodaje do niego funkcjonalność trackera GPS. Stanowi rozwiązanie typowo programowe, które wykorzystuje zasoby zawarte w telefonie – moduł GPS, GSM oraz internet. Jest ono proste i tanie, lecz nie pozbawione wad. Ponieważ to aplikacja na telefon, a nie osobne urządzenie, konieczne jest umieszczenie smartphone'a w pojeździe na stałe jeśli użytkownik chciałby użytkować ją jako zabezpieczenie antykradzieżowe. Ponadto, telefony pobierają stosunkowo dużo energii co wymusza częste ich ładowanie. W rezultacie efektywne ukrycie urządzenia jest utrudnione. Do kosztów rozwiązania należy wliczyć cenę telefonu (używane urządzenie kosztuje ok. 200-300zł) oraz 7$ za każdy pojazd miesięcznie. Aplikację przedstawiono na rysunku 1.3.



Rysunek 1.3: Aplikacja MyCarTracks. Źródło: [2]

- STI GL300

  Jest to kolejne niewielkie, przenośne urządzenie wykorzystujące moduł GPS do lokalizacji. Przekazuje ono informacje o położeniu w czasie rzeczywistym (co 60, 10 lub 5 sekund w zależności od wykupionej taryfy). Producent nie przedstawił informacji o sposobie komunikacji z serwerem, lecz najprawdopodobniej również wykorzystuje sieć GSM. Urządzenie to posiada baterię pozwalającą na ciągłą pracę do 2 tygodni. Urządzenie to nie ogranicza się do lokalizacji pojazdów dzięki niewielkim wymiarom. Producent wprowadza ciekawe funkcjonalności: powiadamianie poprzez wiadomość sms o osiągnięciu przez pojazd danej pozycji geograficznej, wejście w zdefiniowany obszar czy osiągnięcie pewnej prędkości. Aktualne oraz historyczne dane są przedstawiane użytkownikowi poprzez stronę internetową na mapach od firmy Google. Wymiary urządzenia to zaledwie ok. 5 cm x 2,5 cm x 2 cm. W opcji dodatkowej można dokupić wodoodporną obudowę, pozwalającą na zamontowanie urządzenia na zewnątrz pojazdu. Cena urządzenia to 70$ oraz od 25$ do 40$ miesięcznej opłaty. Wygląd urządzenia pokazano na rysunku 1.4.

Rysunek 1.4: Urządzenie STI GL300. Źródło: [3]

Rozdział 2

Wstęp teoretyczny

2.1 System GSM

System GSM (*ang.* ***G****lobal* ***S****ystem for* ***M****obile Communication*) jest obecnie najpowszechniej wykorzystywanym systemem służącym do komunikacji bezprzewodowej dalekiego zasięgu. System ten wykorzystywany jest do przesyłania głosu oraz serwisów danych. Pomysł na stworzenie sieci umożliwiającej komunikację głosową wyłonił się we wczesnych latach 70. ubiegłego wieku z opracowywanego w siedzibie Bell Laboratories mobilnej sieci radiowej. Jednakże dopiero dwanaście lat później, w 1982 roku powstał oficjalny komitet normalizacyjny nazwany *Groupe Spécial Mobile*, którego zadaniem było utworzenie jednolitego, otwartego standardu dla telefonii komórkowej.

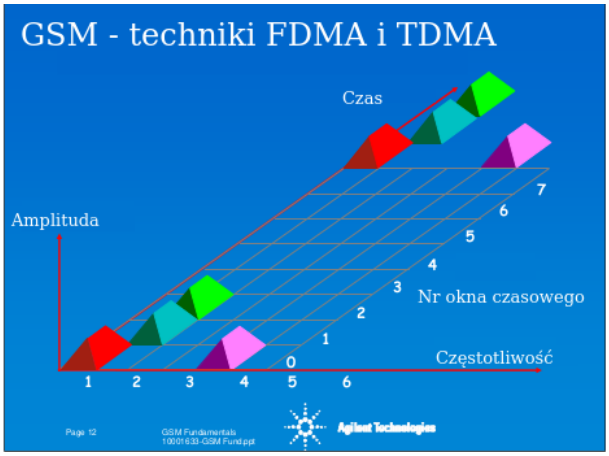
Pierwotna wersja standardu działała w paśmie 900 MHz (880 - 960 MHz) i umożliwiała jedynie transmisję głosową. Jego kolejna wersja została opublikowana w 1990r. i definiowała ona dodatkowe pasmo 1800 MHz (1710 - 1880 MHz). Ponadto, umożliwiała przesyłanie krótkich wiadomości SMS (*ang.* ***S****hort* ***M****essage* ***S****ystem*), a także faxu czy transmisję danych. Dalsze prace nad systemem wprowadziły do standardu techniki zwiększające przepustowość transmisji (maksymalna prędkość odbioru - 57.6 kb/s, maksymalna prędkość nadawania - 14.5 kb/s oraz 30 - 80 kb/s przy transmisji GPRS) oraz mechanizm przesyłania danych w pakietach (GPRS *ang.* ***G****eneral* ***P****acket* ***R****adio* ***S****ervice*).

Pomimo pojawienia się na świecie nowszych rozwiązań, takich jak sieci UMTS i LTE, ze względu na ogromną popularność, architektura sieci GSM wciąż jest rozwijana.

System GSM umożliwia skorzystanie z następujących usług:

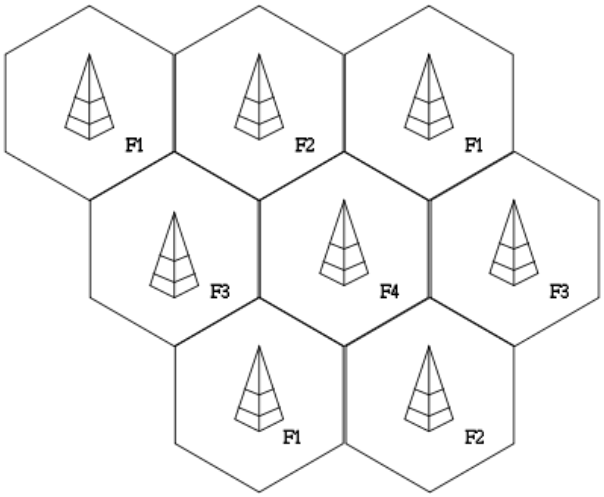
- Połączenia głosowe - Stanowią one sztandarową funkcjonalność sieci GSM. Jej standard definiuje kodek GSM, który służy do zamiany głosu (napięciowego sygnału analogowego) na postać cyfrową, która jest następnie kompresowana stratnie i transmitowana do odbiorcy. Stosowana jest kompresja na podstawie algorytmu LPC (ang. **L**inear **P**redictive **C**oding). Po stronie odbiorcy sygnał jest dekodowany, lecz ze względu na stratność LPC, słyszalny jest zniekształcony, nienaturalny głos rozmówcy.
- Transmisja danych - Umożliwia dostęp do internetu z urządzenia GSM, a także korzystanie z transmisji strumieniowej.
- Wiadomości tekstowe i multimedialne - Usługa przesyłania krótkich wiadomości tekstowych, o długości do 160 znaków, pod warunkiem korzystania jedynie z alfabetu łacińskiego. W przypadku stosowania znaków diakrytycznych maksymalny rozmiar wiadomości spada do 70 znaków. Wiadomości multimedialne (inaczej MMS), umożliwiają przesyłanie zdjęć, filmów czy dźwięków. Ich rozmiar maksymalny jest uzależniony od ograniczeń telefonu oraz operatora.

Jednym z głównych założeń systemu jest możliwość korzystania z niego przez wielu użytkowników jednocześnie. Aby rozwiązać ten problem, postanowiono zastosować technikę zmiany częstotliwości FDMA (*ang.* ***F****requency* ***D****ivision* ***M****ultiple* ***A****ccess*) oraz okien czasowych TDMA (*ang.* ***T****ime* ***D****ivision* ***M****ultiple* ***A****ccess*). Oznacza to, że pasmo częstotliwości GSM jest podzielone na wąskie kanały, o szerokości 200 kHz każdy. Czas użytkowania każdego kanału podzielony jest na 8 okien czasowych. Każde urządzenie ma zatem dostęp do sieci dostrajając się do odpowiedniego kanału w czasie trwania przydzielonego okna czasowego. Przedstawiono to na rysunku 2.1.



Rysunek 2.1: Podział pasma częstotliwości na kanały i okna czasowe. Źródło: [4]

Architektura sieci GSM powstała w oparciu o komórkowy system radiowy, skąd powszechnie stosowana nazwa - sieć komórkowa. Charakteryzuje się ona tym, że obszar terenu, na którym ma być prowadzona komunikacja radiowa dzieli się na tzw. komórki. Każdej komórce przypisana jest stacja bazowa (*ang.* ***B****ase* ***T****ranceiver* ***S****tation*), która stanowi bramę dostępową do sieci. Urządzenie mobilne GSM, takie jak na przykład telefon, znajdując się na obszarze komórki najczęściej odbiera sygnał z więcej niż jednej stacji bazowej, jednakże zawiera połączenie z tą, której sygnał jest najsilniejszy. W razie spadku mocy sygnału stacji z którą urządzenie jest połączone, możliwa jest dynamiczna zmiana połączenia do innego BTS'a.



Rysunek 2.2: Podział obszaru na komórki. Źródło: [6]

Aby móc korzystać z sieci GSM, urządzenia muszą posiadać kartę SIM (*ang.* ***S****ubscriber* ***I****dentification* ***M****odule*). Oprócz przydatnych dla użytkownika wbudowanej pamięci na wiadomości SMS i kontakty, posiada unikalny na całym świecie numer identyfikujący użytkownika w sieci. W celu zalogowania się do sieci, urządzenie GSM musi podać ten numer w trakcie nawiązywania połączenia ze stacją bazową.

Każda stacja bazowa wykorzystuje wiele kanałów GSM. Jednakże, aby nie dopuścić do wzajemnego zakłócania się, stacje bazowe z przylegających do siebie cel wykorzystują inne zbiory kanałów. Dodatkowo, w stacjach bazowych stosuje się dwa rodzaje anten - dookólne i kierunkowe o pokryciu 120°. Anteny dookólne pokrywają caly obszar komórki tym samym zbiorem kanałów, natomiast kierunkowe - dla każdego podobszaru wykorzystują ich inny zestaw. Ze względu na skończoną prędkość sygnału radiowego, istnieje również maksymalny promień pojedynczej komórki. W praktyce wynosi on około 35 km. Ze względu na konieczność umożliwienia prowadzenia komunikacji na tak duży zasięg, standard ten nie należy do najbardziej energooszczędnych. W zależności od klasy urządzenia, minimalnamoc nadawanego sygnału może wynosić od 1 do 20 mW, natomiast maksymalna nawet do 8 W. Urządzenia GSM mają możliwość do-

stosowywania mocy transmisji na podstawie mocy sygnału odebranego od stacji bazowej.

Biorąc jednak pod uwagę fakt, iż transmisja przebiega w oknach czasowych, moc średnia jest niższa. Każde okno czasowe trwa 577 μs, a w jego czasie można wysłać jedną z kilku ramek komunikacyjnych. W trakcie każdej z nich można wysłać jedynie 148 bitów danych. W przypadku ramki nadawanej w trakcie rozmowy, głos kodowany jest jedynie na 57 bitach. Każde z urządzeń w sieci otrzymuje okno czasowe co 4.615 ms, liczone od początku okna, do rozpoczęcia następnego. Stąd wynika, że w trakcie nadawania, urządzenie transmituje dane jedynie przez 12.5% czasu. Pobór prądu wówczas, w zależności od odległości do nadajnika, a więc od mocy nadawania, może wynosić nawet do 1.5 A. Przyjmując napięcie zasilania układu GSM wynoszące 4 V, maksymalna pobierana moc średnia może wynosić nawet:

$$P_{\acute{s}r} = U \cdot I \cdot \tau \tag{2.1}$$
$$P_{\acute{s}r} = 4V \cdot 1.5A \cdot 0.125 = 0.75W$$

gdzie:

$P_{\acute{s}r}$ - moc średnia

U - napięcie zasilania układu,

I - nateżęnie prądu w momencie transmisji

τ - współczynnik wypełnienia impulsu (czas trwania okna czasowego podzielony przez czas pomiędzy oknami czasowymi)

Wartość mocy średniej wynosząca 0.75 W odpowiada ciągłemu zużyciu prądu rzędu 187.5 mA przy napięciu zasilania układu rzędu 4 V.

2.2 System GPS

2.3 Protokół NMEA

2.4 Protokół Bluetooth Low Energy

2.5 Interfejs NFC

https://www.dobreprogramy.pl/Szuri21/NFC-dla-poczatkujacych,61527.html

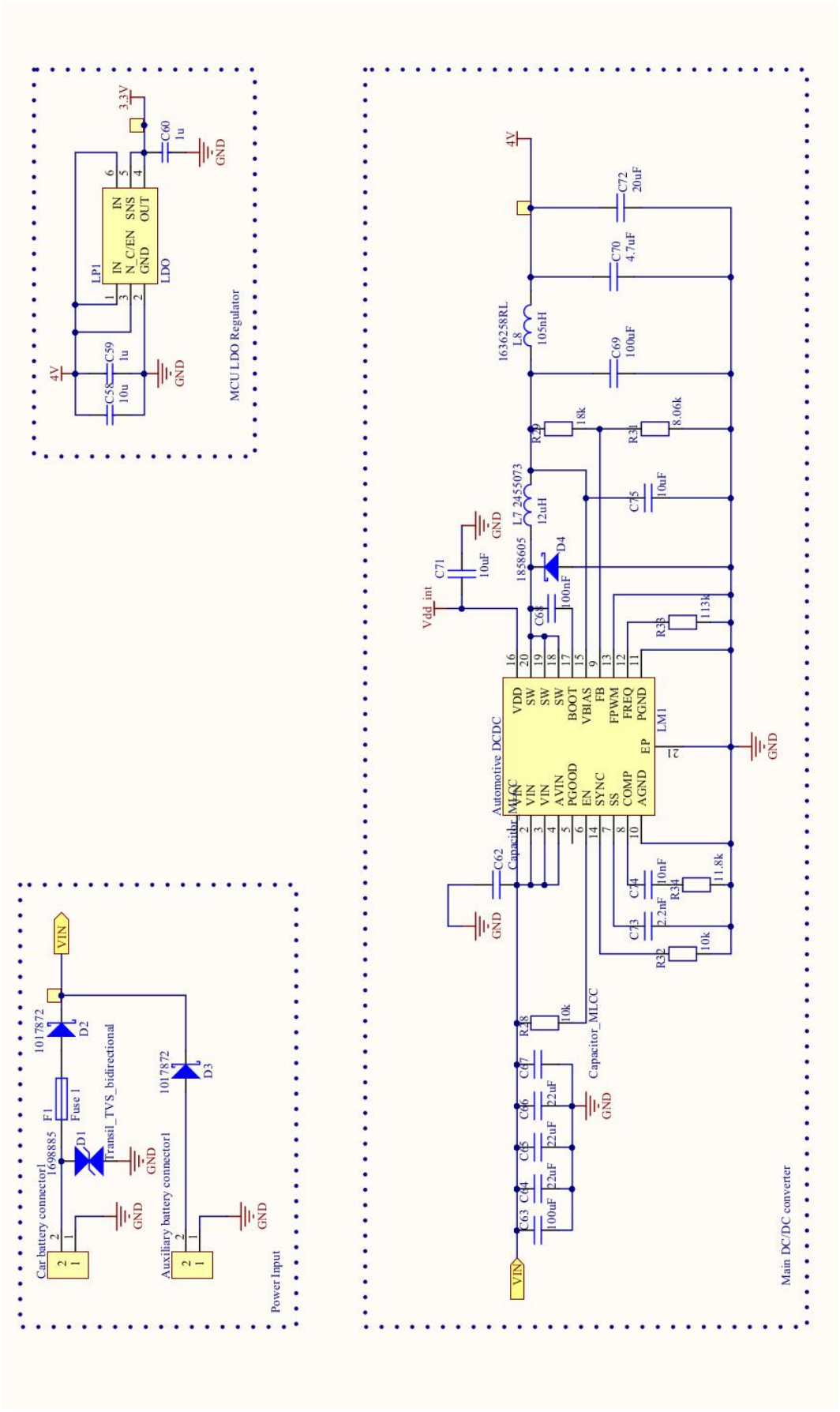
Rozdział 3

Schematy elektroniczne urządzeń

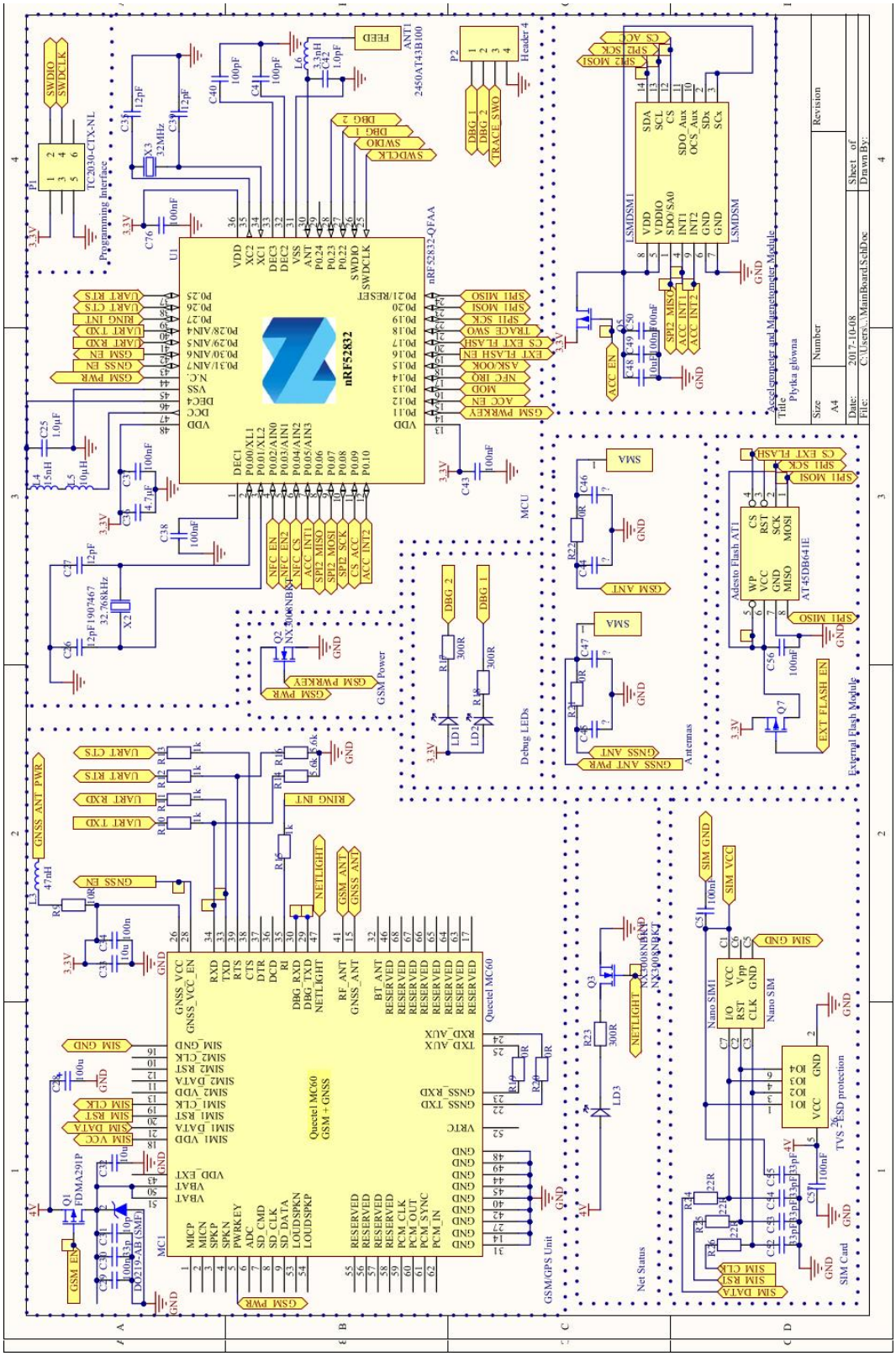
3.1 Urządzenie lokalizujące

Ze względu na poziom skomplikowania układu, schemat elektroniczny musiał zostać rozbity na podschematy. W urządzeniu lokalizującym można wyróżnić trzy znaczące moduły elektroniczne, realizujące odpowiednie funkcje. Są to:

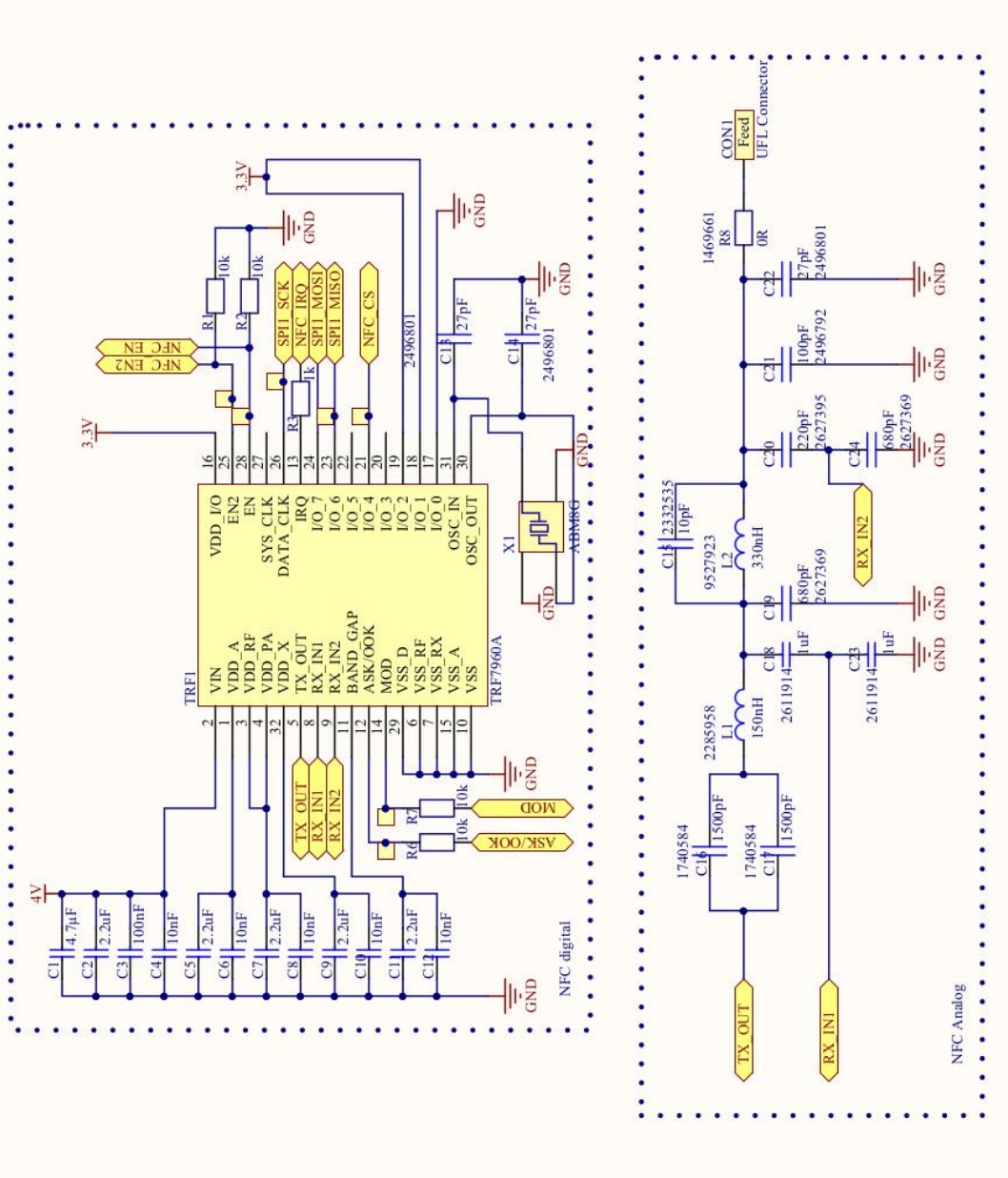
- Moduł zasilania, przedstawiony na rysunku 3.1
- Moduł funkcjonalny, przedstawiony na rysunku 3.2
- Moduł NFC, przedstawiony na rysunku 3.3



Rysunek 3.1: Schemat modułu zasilania urządzenia lokalizującego.
Źródło: Twórczość własna



Rysunek 3.2: Schemat modułu funkcjonalnego urządzenia lokalizującego. Źródło: Twórczość własna

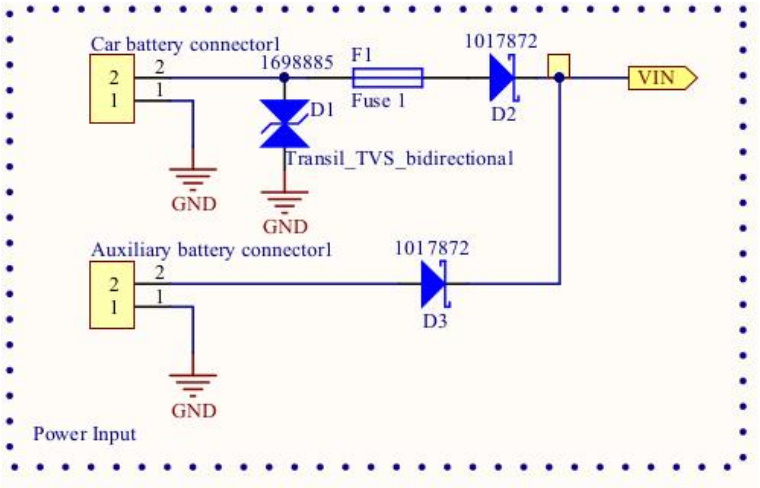


Rysunek 3.3: Schemat modułu NFC urządzenia lokalizującego.
Źródło: Twórczość własna

3.1.1 Schemat zasilania

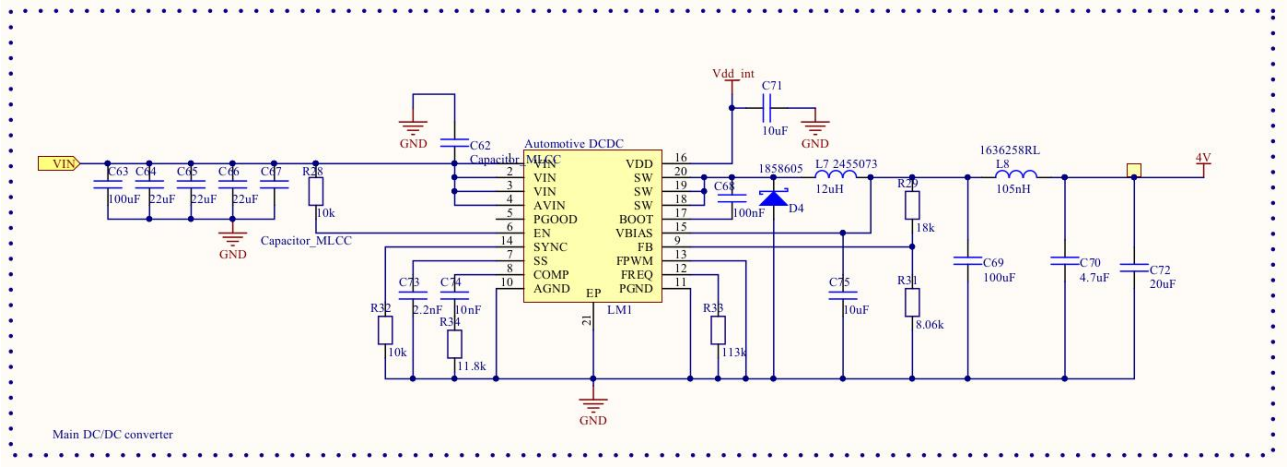
Akumulator samochodowy jest bardzo wygodnym źródłem zasilania układów elektronicznych, lecz gdy są one niewłaściwie zaprojektowane, bywa on dla nich zabójczy. Bliska odległość do alternatora i innych urządzeń indukcyjnych powoduje generowanie silnych zakłóceń na linii zasilającej. Niekiedy "szpilki" napięciowe osiągają wartość rzędu 100V. Z tego powodu należy stosować transile – diody zabezpieczające. Powodują one ograniczenie zbyt dużego napięcia do pewnej maksymalnej wartości. W przypadku zastosowanego przeze mnie komponentu wyno-

si ono 24.4V. Zabezpieczenie przeciążeniowe stanowi bezpiecznik samochodowy o wartości 4A. Ponieważ jednym z wymagań układu jest możliwość zasilania bateryjnego, konieczne jest zastosowanie dodatkowego przyłącza zasilania. Urządzenie można zasilić dowolną baterią o napięciu od 4 do 38V i wydajności prądowej co najmniej 3A w szczycie. Ze względu na prawdopodobieństwo wystąpienia różnic napięć pomiędzy dodatkowa baterią, a akumulatorem samochodu i wiążącym się z tym przepływem prądu z jednego źródła do drugiego, konieczne jest zastosowanie diód zabezpieczających przed rozładowaniem baterii przez akumulator (gdy napięcie akumulatora niższe niż napięcie baterii) lub mogącym doprowadzić baterię do zniszczenia doładowywaniem jej bezpośrednio z akumulatora (gdy napięcie baterii jest od niższe napięcia akumulatora). W trakcie projektowania, zdecydowano się na zastosowanie diód Schottky'ego ze względu na ich niski spadek napięcia (0.2 - 0.55V w zależności od natężenia prądu) oraz szybki czas przełączania ze stanu zaporowego do przewodzenia (ograniczenie krótkotrwałych zaników zasilania przy wyłączaniu samochodu). Na rysunku 3.4 przedstawiono część wejściową dla zasilania całej płytki.



Rysunek 3.4: Schemat modułu zasilania wejściowego urządzenia lokalizującego. Źródło: Twórczość własna

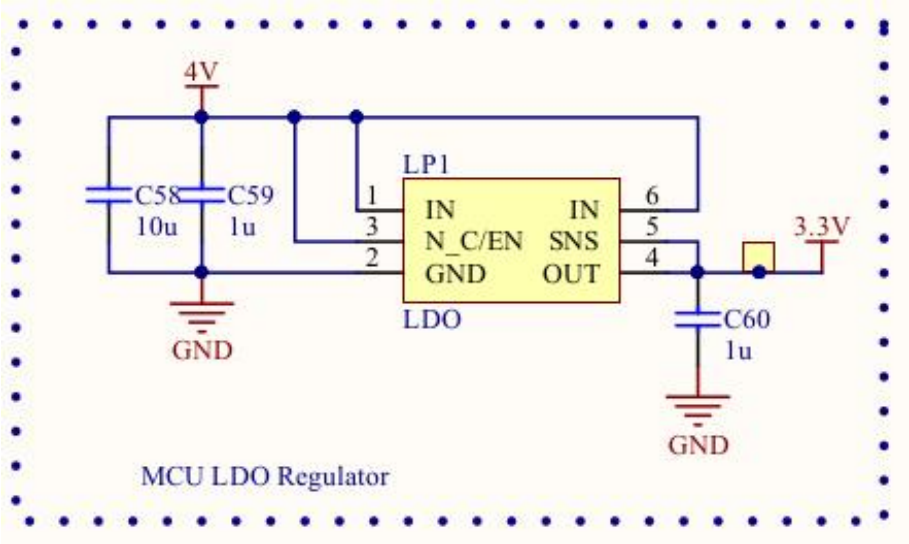
Niestety, często napięcie wejściowe, nawet po zadziałaniu zabezpieczenia w postaci transila, jest nadal zbyt duże dla zwykłych układów zasilających. Stąd konieczne jest stosowanie przetwornic impulsowych klasy automotive, które umożliwiają zasilanie napięciem wejściowym do kilkudziesięciu woltów. Schemat wykorzystanej przetwornicy przedstawiono na rysunku 3.5.



Rysunek 3.5: Schemat przetwornicy impulsowej modułu zasilania urządzenia lokalizującego. Źródło: Twórczość własna

Zastosowana w urządzeniu przetwornica umożliwia zasilanie napięciami od 4 do 38V. Wybrano ją ze względu na niewielką liczbę zewnętrznych komponentów, niezbędnych do jej działania w porównaniu do innych modułów, a także wysoką sprawność rzędu od 85% do 90% w zależności od chwilowego natężenia prądu. Wytwarza ona na wyjściu napięcie o wartości 4V, którym zasilany jest moduł GSM oraz dalszy stopień obniżania napięcia.

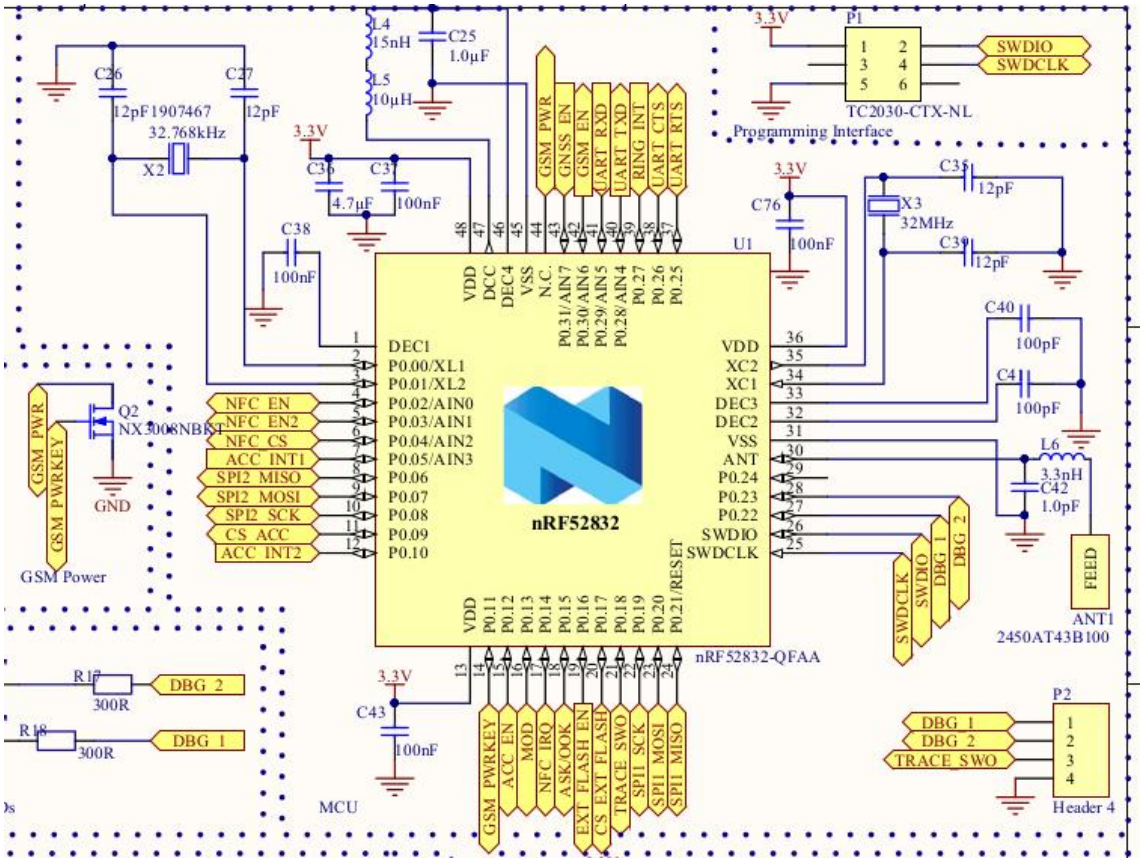
Ostatni stopień zasilania generuje z napięcia wyjściowego z przetwornicy napięcie o wartości 3.3V. Jest ono niezbędne do zasilania układów mikrokontrolera, pamięci flash, akcelerometru oraz układu GPS. Szacowany pobór prądu przez te układy wynosi ok. 200mA w szczycie, stąd dla bezpieczeństwa wykorzystano stabilizator napięcia LDO (ang. Low Dropout Stabilizer) o maksymalnym natężeniu wyjściowym 0,5A. Jego schemat przdstawiono na rysunku 3.6.



Rysunek 3.6: Schemat stabilizatora napięcia modułu zasilania urządzenia lokalizującego. Źródło: Twórczość własna

3.1.2 Moduł mikrokontrolera

Serce urządzenia stanowi mikrokontroler nRF52832 firmy Nordic Semiconductor. Układ ten posiada 32 bitowy rdzeń Cortex-M4 zaprojektowany przez firmę ARM, sprzętową jednostkę FPU oraz 512kB wewnętrznej pamięci Flash oraz 64kB pamięci RAM. Zdecydowano się na wykorzystanie tego mikrokontrolera ze względu na kilka czynników. Pierwszym z nich jest jego wyposażenie- posiada wbudowany układ radiowy działający na częstotliwości 2.4 GHz i umożliwiający komunikację w standardzie Bluetooth Low Energy, ANT lub wykorzystanie własnego protokołu. Dodatkowym atutem tego mikrokontrolera jest wyposażenie w sprzętowy interfejs NFCT, umożliwiający wykorzystanie modułu jako tag (urządzenie podrzędne) w komunikacji poprzez interfejs NFC. Ponadto ma bardzo duże możliwości obliczeniowe – wewnętrzny zegar 64 MHz umożliwia bardzo szybkie wykonywanie zaprogramowanych zadań i szybki powrót do trybu oszczędzania energii. Zużycie energii przez ten procesor jest bardzo niewielkie. W trakcie wykonywania programu pobór prądu wynosi 58 μA /MHz gdy kod wykonywany jest z pamięci flash, natomiast w trybie oszczędzania energii pobór spada do ok 1.9 μA. Ostatnim i być może najważniejszym czynnikiem decydującym na wybranie tego układu jest posiadane przez autora doświadczenie zawodowe w programowaniu układów od tego producenta, a zatem bardzo dobra znajomość jego możliwości i SDK (ang. Software Development Kit). Schemat mikrokontrolera przedstawiono na rysunku 3.7.



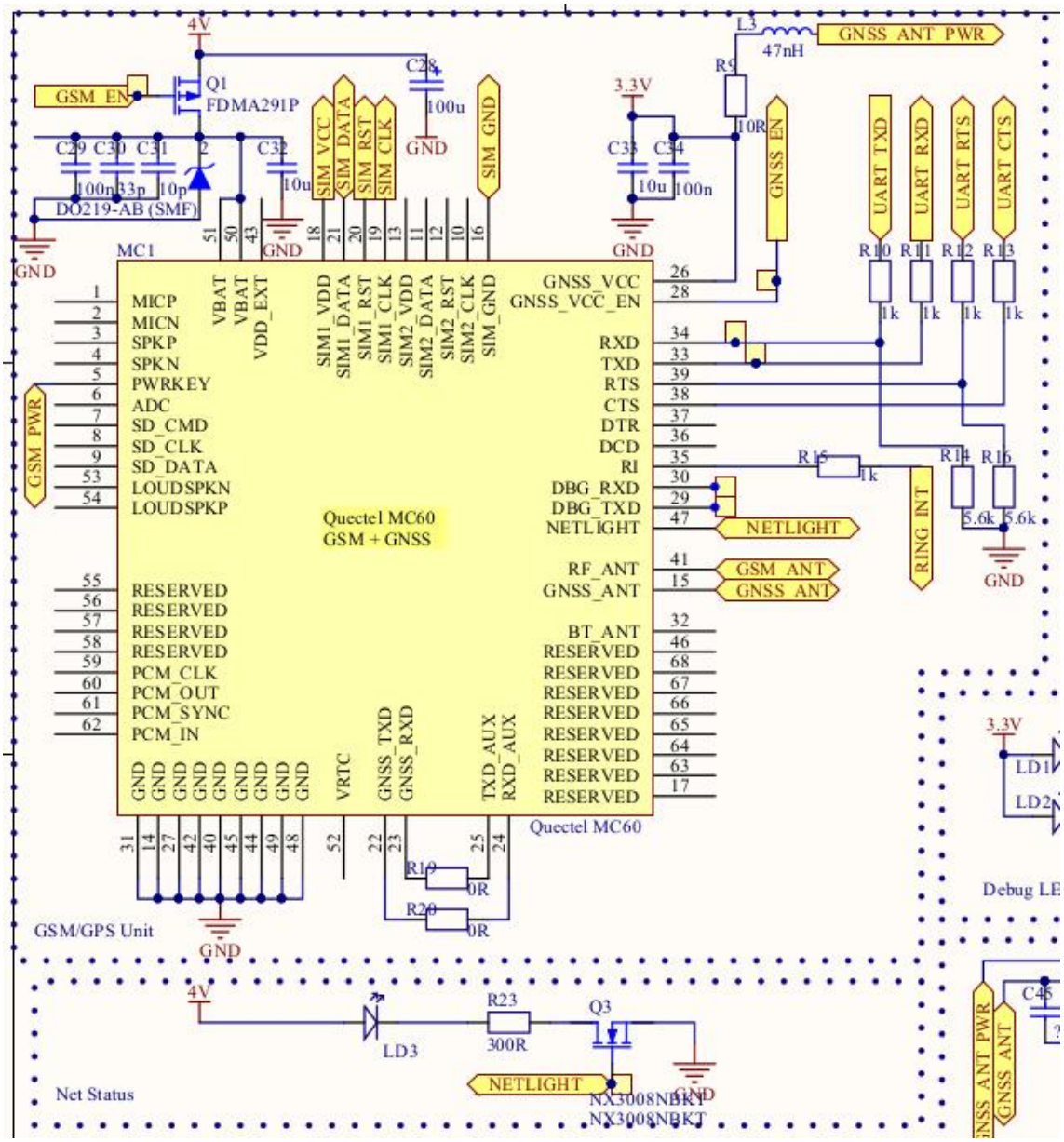
Rysunek 3.7: Schemat modułu mikrokontrolera w urządzeniu lokalizującym.
Źródło: Twórczość własna

3.1.3 Moduł GSM i GPS

Jako moduł realizujący główną funkcję urządzenia wybrano układ Quectel MC60. Stanowi on połączenie modułu GSM oraz GPS w jednym chipie. Umożliwia transmisję w wielu protokołach, takich jak: TCP/IP, UDP, FTP, PPP, HTTP czy NTP. Ponadto możliwe jest odbieranie danych w postaci krótkich wiadomości SMS. Układ posiada niewielkie wymiary: 18.7 mm x 16 mm x 2.1 mm dzięki czemu możliwe będzie zmniejszenie całego urządzenia. Zużycie energii wynosi:

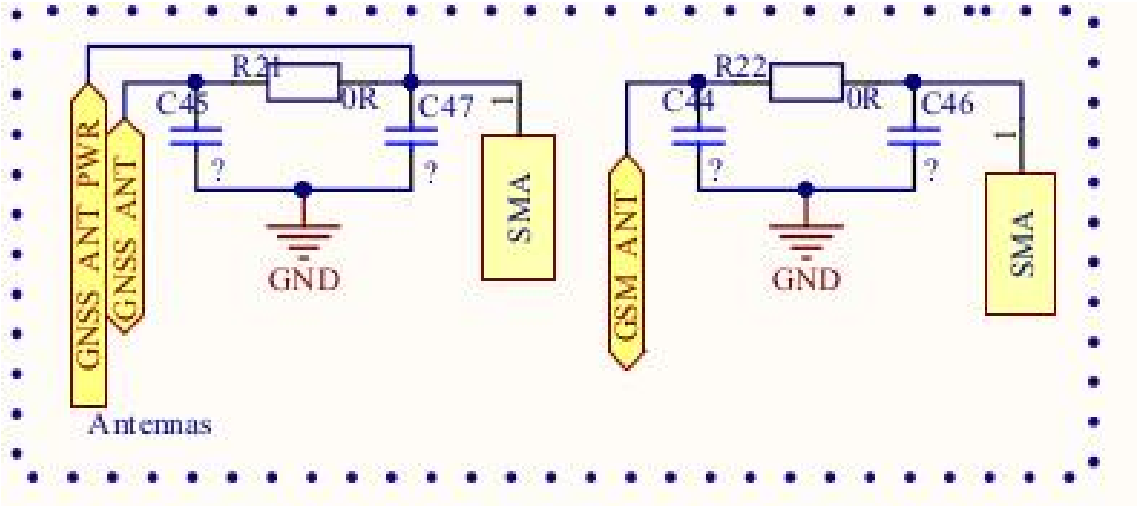
- Około 25 mA gdy działa jedynie moduł GPS
- Do 1.6 A w trakcie transmisji danych poprzez sieć GSM

Ponadto, kombinacja tych dwóch systemów umożliwia wykorzystanie funkcjonalności AGPS. Polega ona na podaniu do modułu GPS zgrubnych danych o położeniu satelitów, pobranych z sieci GSM. Dzięki temu, ustalenie własnej lokalizacji, nawet po długotrwałym wyłączeniu, trwa ok. sekundy (tzw. warm start). Schemat modułu GSM i GPS przedstawiono na rysunku 3.8.



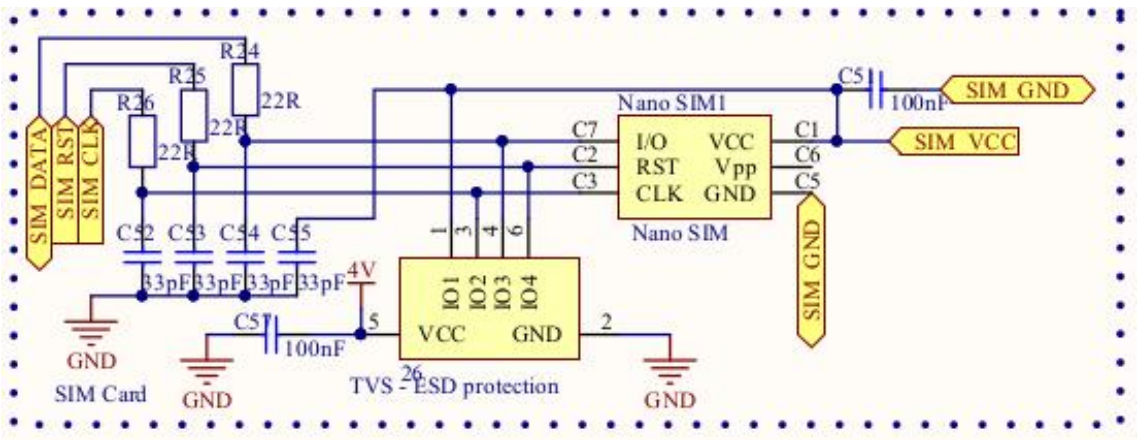
Rysunek 3.8: Schemat modułu układu GSM i GPS w urządzeniu lokalizującym. Źródło: Twórczość własna

W celu zwiększenia niezawodności działania urządzenia, zdecydowano zastosować zewnętrzne anteny GSM i GPS poprawiające jakość sygnału. Dodatkowo, w celu zwiększenia jakości sygnału, antena GPS jest anteną aktywną. Oznacza to, że dostarczane jest do niej dodatkowe zasilanie, co powoduje wzmocnienie odebranego sygnału. Schemat anten przedstawiono na rysunku 3.9. Zawarte na nim znaki zapytania, zamiast wartości kondensatorów oznaczają, że kondensatory należy dobrać po złożeniu płytki i przebadaniu jej pod kątem jak najlepszego dopasowania impedancji.



Rysunek 3.9: Schemat modułu anten dla GSM i GPS w urządzeniu lokalizującym. Źródło: Twórczość własna

Ostatnią częścią układu GSM jest połączenie modułu z kartą SIM, umożliwiającą zalogowanie do sieci. Przedstawiono je na rysunku 3.10. Widać na nim układ TVS, który jest odpowiedzialny za zabezpieczenie wrażliwej elektroniki w karcie SIM przed wyładowaniami statycznymi ESD (*ang. Electrostatic discharge*).

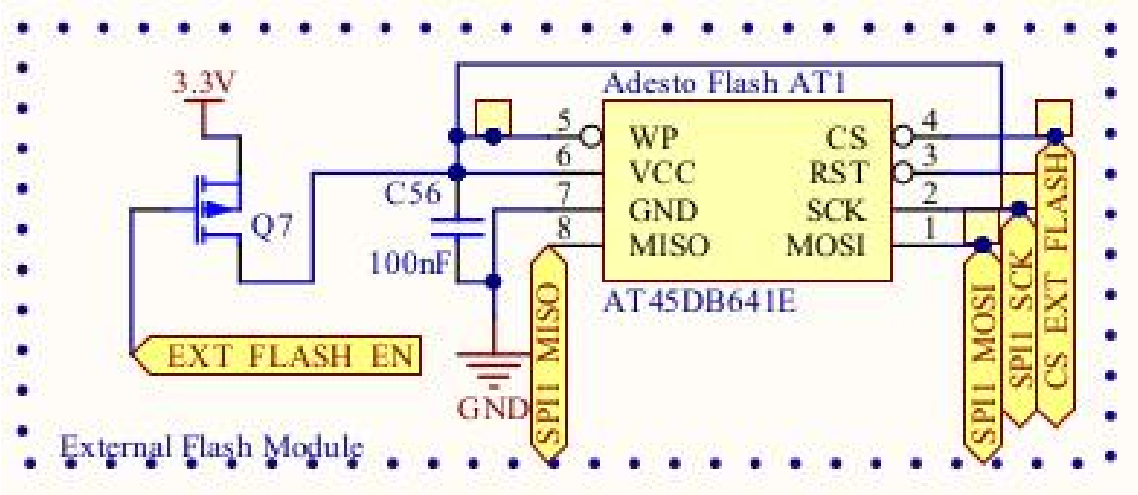


Rysunek 3.10: Schemat modułu karty SIM w urządzeniu lokalizującym. Źródło: Twórczość własna

3.1.4 Moduł pamięci flash

Wewnętrzna pamięć flash mikrokontrolera jest niewystarczająca, aby przechowywać w niej trasy wraz z parametrami jazdy. Stąd też pojawia się konieczność zastosowania zewnętrznego układu pamięci nieulotnej. Zastosowana w urządzeniu pamięć flash posiada pojemność 8 MB,

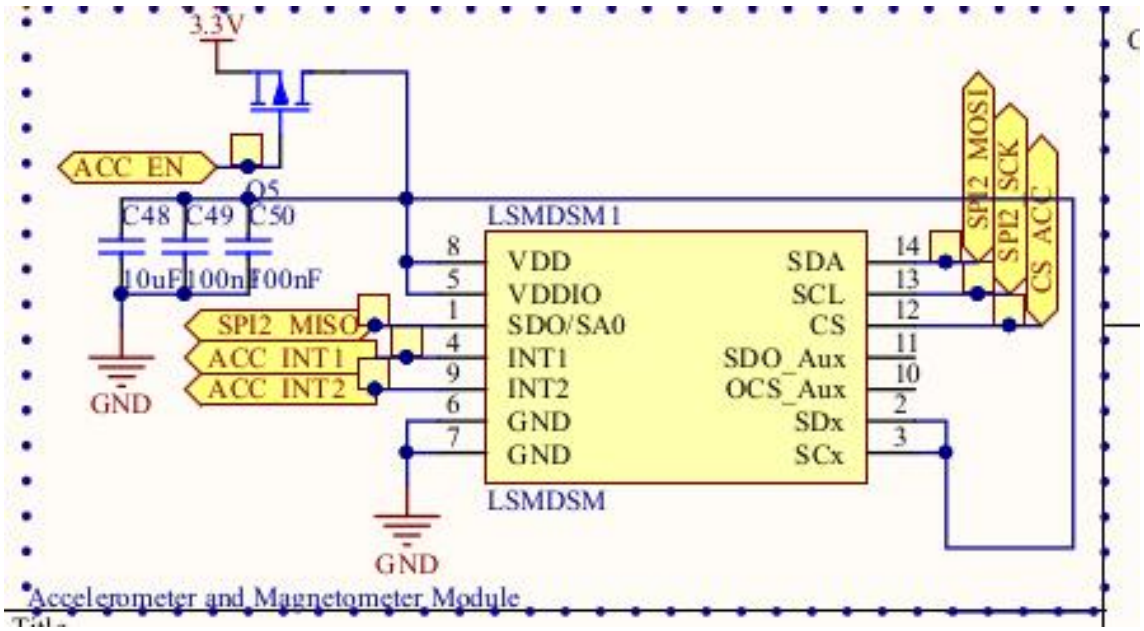
co umożliwi przechowywanie wielu długich tras oraz dokładne profilowanie statystyczne stylu jazdy kierowcy. Schemat pamięci w urządzeniu lokalizującym pokazano na rysunku 3.11.



Rysunek 3.11: Schemat modułu pamięci flash w urządzeniu lokalizującym. Źródło: Twórczość własna

3.1.5 Moduł akcelerometru

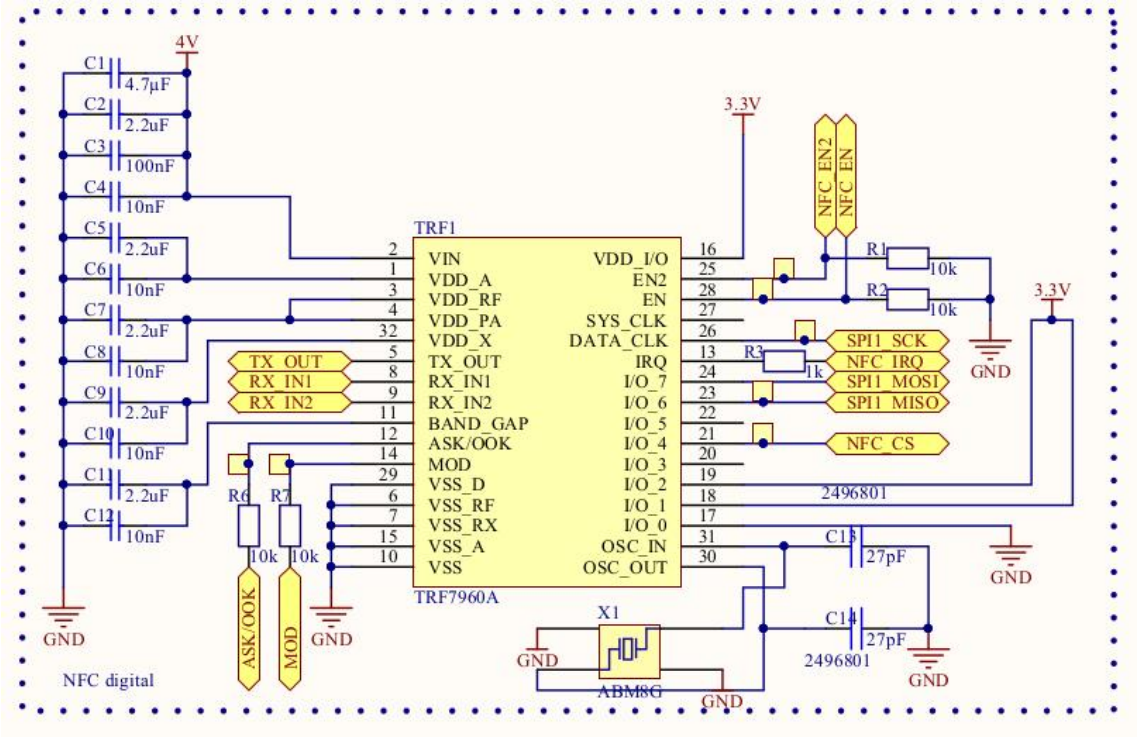
Kolejną ważną częścią urządzenia jest moduł akcelerometru. Pozwala on na wybudzenie urządzenia w momencie przemieszczenia pojazdu, a w razie braku dezaktywacji - uruchomienie procedury alarmowej. Ponadto, dzięki jego wskazaniom możliwe jest wyznaczenie przyspieszenia pojazdu pozwalające na profilowanie stylu prowadzenia pojazdu przez kierowcę. Wbudowany żyroskop pozwoli na dokładniejsze profilowanie stylu jazdy kierowcy w trakcie pokonywania zakrętów oraz zmiany pasa. Schemat modułu akcelerometra przedstawiono na rysunku 3.12.



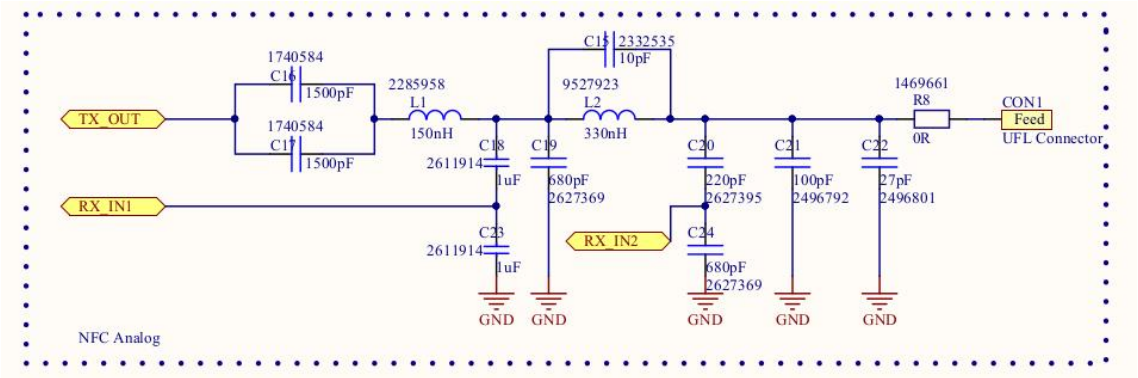
Rysunek 3.12: Schemat modułu akcelerometru w urządzeniu lokalizującym. Źródło: Twórczość własna

3.1.6 Moduł NFC

Moduł ten stanowi istotną część z punktu widzenia bezpieczeństwa komunikacji bezprzewodowej. Jest ono zapewnione poprzez zastosowanie szyfrowania wiadomości. Jeśli jednak ktoś podsłucha transmisję inicjalizacji urządzenia, w której przekazywane są klucze szyfrujące, cały koncept traci sens. Dzięki zastosowaniu modułu NFC, możliwość podsłuchania transmisji wymiany kluczy szyfrujących zostaje zniwelowana poprzez fizyczne ograniczenia zasięgu komunikacji. NFC posiada zasięg maksymalny do 5 cm. Komunikacja odbywa się pomiędzy dwoma urządzeniami. Ze względu na sposób transmisji, jedno z urządzeń inicjuje komunikację. Inicjator generuje zmienne pole magnetyczne, w który może (lecz nie musi) zawrzeć dane wysyłane do urządzenia docelowego. Urządzenie docelowe wykrywa to pole i może odpowiedzieć poprzez odpowiednie zniekształcenie go, które jest wykrywane przez inicjator. Urządzenie docelowe nie generuje żadnego pola magnetycznego. Może jedynie zniekształcać pole generowane przez inicjator. Stąd wynika, że inicjator musi mieć znacznie większe zużycie energii niż urządzenie docelowe – tag. W urządzeniu lokalizacyjnym zastosowano moduł inicjatora NFC, którego schemat przedstawiono na rysunkach 3.13 - część cyfrowa oraz 3.14 - część analogowa.



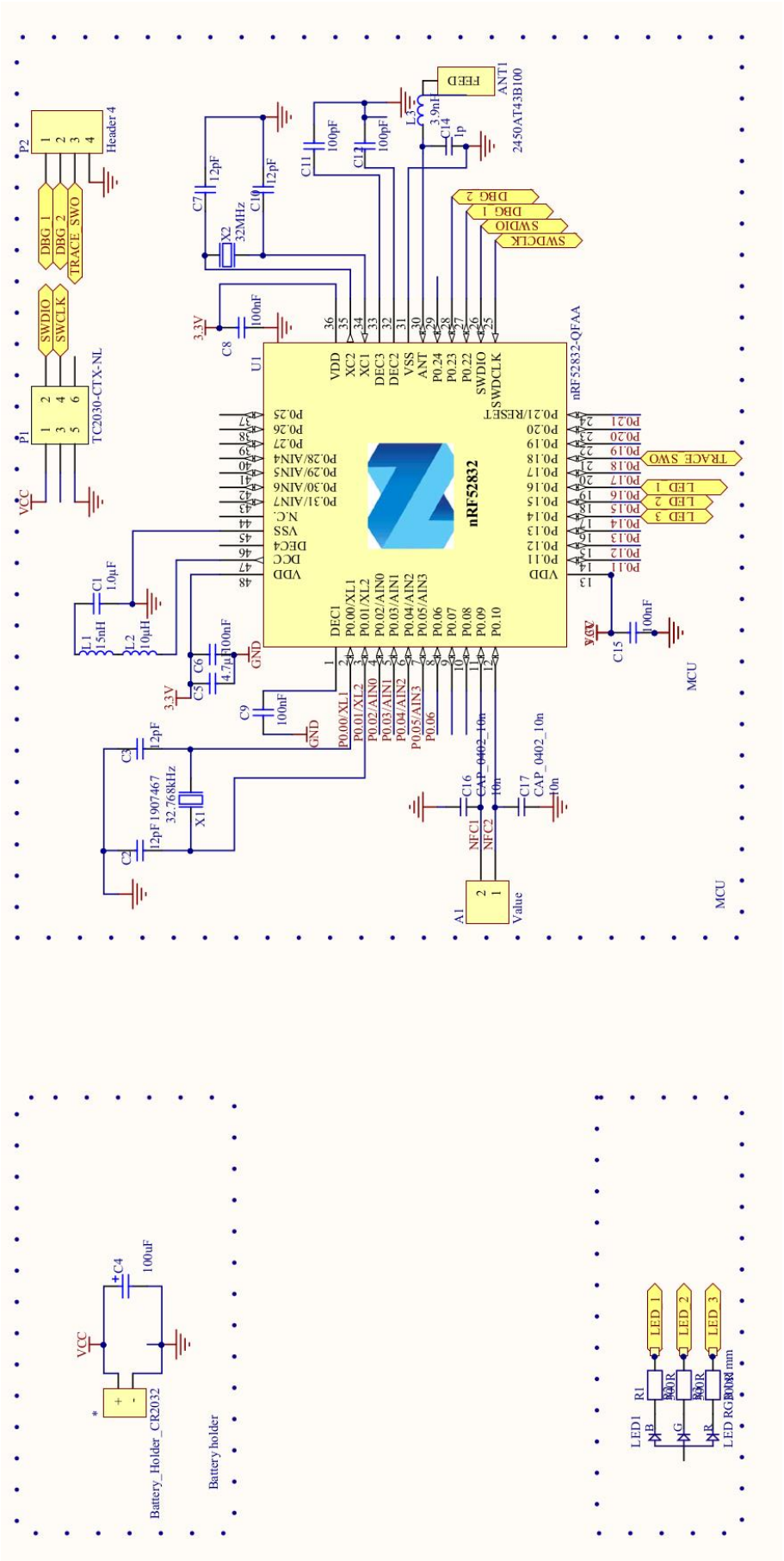
Rysunek 3.13: Schemat części cyfrowej modułu NFC w urządzeniu lokalizującym. Źródło: Twórczość własna



Rysunek 3.14: Schemat części analogowej modułu NFC w urządzeniu lokalizującym. Źródło: Twórczość własna

3.2 Urządzenie deaktywujące

Głównym zadaniem tego urządzenia jest cykliczne rozgłaszanie swej obecności. Po wykryciu przez urządzenie lokalizujące, łączy się ona z deaktywatorem oraz bezpiecznym kanałem dokonywane jest wyłączenie funkcji alarmu. Dzięki temu, że urządzenie to ma tak proste zadanie, nie pobiera ona dużo poboru energii, więc możliwe jest zasilenie go ze standardowej baterii CR2032 o promieniu 20 mm i grubości 3.2 mm. Urządzenie to, przy odpowiedniej konfiguracji parametrów transmisji może działać kilka lat bez konieczności wymiany baterii. Zastosowanie wspomnianego źródła zasilania stanowi kompromis pomiędzy czasem działania i rozmiarem urządzenia, które docelowo powinno być umieszczone przy kluczach samochodowych. Schemat deaktywatora przedstawiono na rysunku 3.3.



Rysunek 3.15: Schemat modułu zasilania urządzenia deaktywującego.
Źródło: Twórczość własna

Rozdział 4

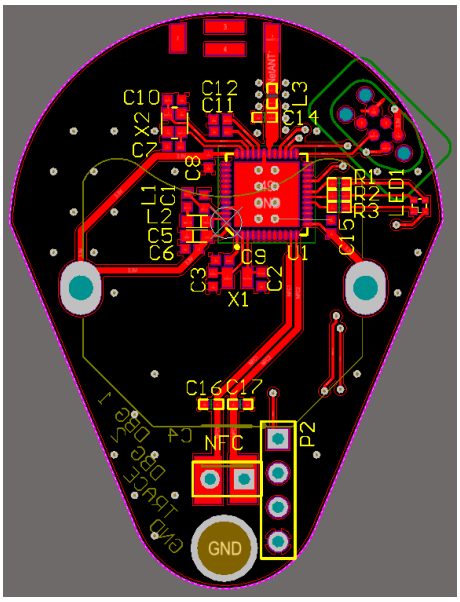
Schematy płytek drukowanych

4.1 Urządzenie deaktywujące

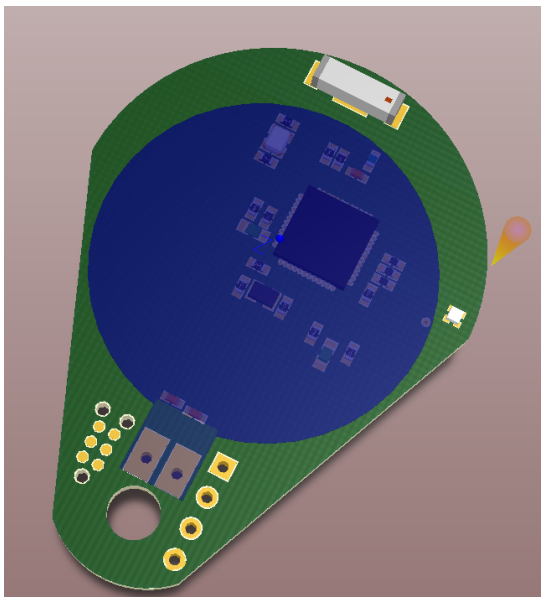
Ze względu na pełniony przez urządzenie cel, powinno ono zawsze towarzyszyć osobie upoważnionej do uruchomienia pojazdu. Biorąc pod uwagę przykład zastosowania urządzenia we flotach pojazdów, szybko można zauważyć, że zazwyczaj do pojazdu nie jest przypisana jedna osoba, lecz może być on używany przez wielu kierowców. Stąd też logicznym staje się wniosek, że urządzenie nie może być przyporządkowane do kierowcy, lecz do pojazdu. Idealnym rozwiązaniem wydaje się umieszczenie go przy kluczykach lub karcie umożliwiającej uruchomienie pojazdu bezkluczykowo, jako dodatkowy brelok. Z tego powodu kluczowe stają się wymiary samego urządzenia. nie powinno być ono zbyt grube, aby nie przeszkadzało w kieszeni, ani zbyt duże, aby nie obijało się o nogi, a tym samym nie rozpraszało kierującego w trakcie jazdy. Rozmiar płytki urządzenia dezaktywującego wynoszą odpowiednio 32 mm x 43 mm szerokości i wysokości.

Ze względu na prostotę urządzenia, składa się ono z bardzo niewielu modułów. Na górnej warstwie znajduje się serce układu - mikrokontroler nRF52832 wraz z anteną 2.4 GHz ISM do komunikacji poprzez Bluetooth Low Energy. Dodatkowo, znajdują się tam złącze do programowania, złącze debugowe oraz antena NFC, zwizualizowana jako koło w kolorze niebieskim. Górną warstwę płytki przedstawiono na rysunku 4.1.

Centralne miejsce na dolnej warstwie płytki zajmuje bateria litowa CR2032, która zapewni kilkuletnią pracę dezaktywatora. Posiada ona średnicę 20mm oraz grubość 3.2 mm co stanowi idealny kompromis pomiędzy wymiarami urządzenia, a czasem jego pracy, bowiem mniejsze baterie oferują mniejszą pojemność liczoną w miliampero godzinach. Wygląd oraz wizualizację dolnej warstwy płytki przedstawiono na rysunku 4.2.

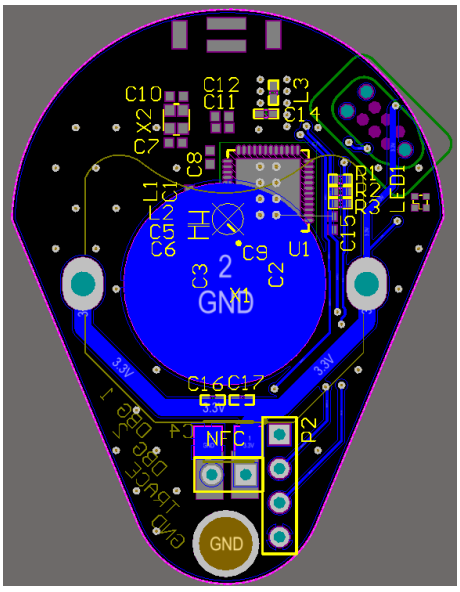


(a) Wygląd górnej warstwy płytki



(b) Wizualizacja górnej warstwy płytki

Rysunek 4.1: Wygląd górnej warstwy płytki urządzenia dezaktywującego oraz jej wizualizacja. Źródło: Twórczość własna



(a) Wygląd dolnej warstwy płytki

(b) Wizualizacja dolnej warstwy płytki

Rysunek 4.2: Wygląd dolnej warstwy płytki urządzenia dezaktywującego oraz jej wizualizacja. Źródło: Twórczość własna

4.2 Urządzenie lokalizujące

Płytka lokalizująca jest znacznie bardziej skomplikowana od urządzenia dezaktywującego. Wynika to głównie z faktu, iż stanowi podstawę funkcjonalności całego systemu, a zatem posiada wiele modułów realizujących określone zadania. Płytka ma wymiary 50 mm x 50 mm, co powinno umożliwić ukrycie jej w większości miejsc w pojeździe (na przykład pod plastikowymi zabudowami kokpitu).

Wygląd i wizualizacje urządzenia przedstawiono na rysunkach 4.4 oraz 4.5.

Ze względu na użycie kilku układów radiowych, wykorzystujących częstotliwości od 13.56 MHz (NFC), poprzez 900 MHz/ 1800 MHz (GSM) i 1575.42 MHz (GPS) aż po 2.4 GHz (Bluetooth), a także przetwornicy impulsowej o znacznym szczytowym natężeniu prądu (aż do 4 A), niezbędne jest odpowiednie rozłożenie elmentów na płytce, które zminimalizowałoby ich wzajemny wpływ. W związku z tym, postanowiono umieścić kluczowe elementy zasilające oraz radiowe w rogach płytki, aby zmaksymalizować wzajemne odległości. W ten sposób, w lewym górnym rogu płytki umieszczono złącza zasilania wejściowego, w prawym górnym - cewkę indukcyjną, stanowiącą główny element impulsowej stabilizacji napięcia. Cewka ta przy okazji stanowi główne źródło zakłóceń sygnałów. W lewym dolnym rogu znajduje się antena Bluetooth Low Energy, natomiast w prawym dolnym rogu - złącze anteny GPS.

Przewody anten GPS oraz GSM są dodatkowo ekranowane, dzięki czemu znacznie zmniejszona jest podatność tych sygnałów na zakłócenia w trakcie przepływu od anteny do płytki. Jednakże na samej płytce sygnały te nie posiadają ekranu elektromagnetycznego, przez co są podatne na szumy. Z tego względu niezbędna jest minimalizacja długości ścieżek między złączem anteny oraz wejściami układów. W dodatku, sygnał GPS stanowi najsłabszy ze wszystkich sygnałów radiowych, wykorzystywanych w urządzeniu, przez co niezbędne staje się jak największe oddalenie toru GPS od pozostałych układów. Ze względu na fakt, iż sygnał GSM jest znacznie mocniejszy, znajduje się on na środku prawego boku płytki, bliżej cewki indukcyjnej przetwornicy impulsowej.

Wszystkie sygnały radiowe użyte w urządzeniu są sygnałami analogowymi. Są one podatne na zjawisko odbicia fali elektromagnetycznej, które polega na odbiciu sygnału na końcu przewodu, bądź ścieżki elektrycznej i nałożeniu się na sygnał pierwotny. Wprowadza to dodatkowe zakłócenia w transmisji sygnału, a spowodowane jest niedopasowaniem impedancji toru transmisyjnego. Aby zminimalizować ten efekt, należy zaprojektować ścieżki po których przesyłany jest sygnał wysokiej częstotliwości tak, aby miały odpowiednią impedancję, zgodną z impedancją anteny. Robi się to poprzez wyznaczenie grubości (wynika ona z grubości warsty miedzi, zazwyczaj 35 μm) oraz szerokości (dobór pod kątem optymalności zużycia miejsca na PCB) ścieżek radiowych. Na podstawie tak wyznaczonych parametrów wylicza się ich niezbędną dłu-

gość, aby osiągnąć założoną impedancję. W przypadku sygnałów GPS, GSM oraz bluetooth wynosi ona 50 Ω. Ostateczną impedancję, uwzględniającą pojemności i indukcyjności pasożytnicze między ścieżkami, zmierzoną po złożeniu płytki można jeszcze skorygować poprzez dobór elementów w filtrach przyantenowych (filtry: C45, R21, C47 oraz C44, R22, C46). Dodatkowo, ścieżki wysokiej częstotliwości prowadzi się łagodnymi łukami, bez ostrych załamań, które mogłyby zwiększających pojemność, a tym samym mogących zmienić impedancję.

W dodatku, w trakcie projektowania urządzenia należy pamiętać o wysokim chwilowym poborze prądu (aż do około 4 - 5 A). Z tego względu, trzeba zaprojektować odpowiednio grube ścieżki zasilające. Jest to wymagane z dwóch powodów. Pierwszym z nich jest fakt oporności ścieżki.

$$R = \rho \cdot l/S \tag{4.1}$$

gdzie:

R - oporność ścieżki, ρ - oporność właściwa materiału, z którego wykonano ścieżkę,

l - długość ścieżki,

S - powierzchnia (liczona jako iloczyn grubości i szerokości) ścieżki,

Jak widać, im większa szerokość, ścieżki, tym większa jej powierzchnia a tym samym mniejsza rezystancja. Im mniejsza rezystancja, tym straty napięcia na samej ścieżce będą mniejsze, a tym samym mniejsze napięcie dostarczaqne do układów funkcjonalnych i większe straty na ciepło, generujące niepotrzebne zużycie energii.

$$U = R \cdot I \tag{4.2}$$

gdzie:

U - strata napięcie na ścieżce,

R - opór ścieżki,

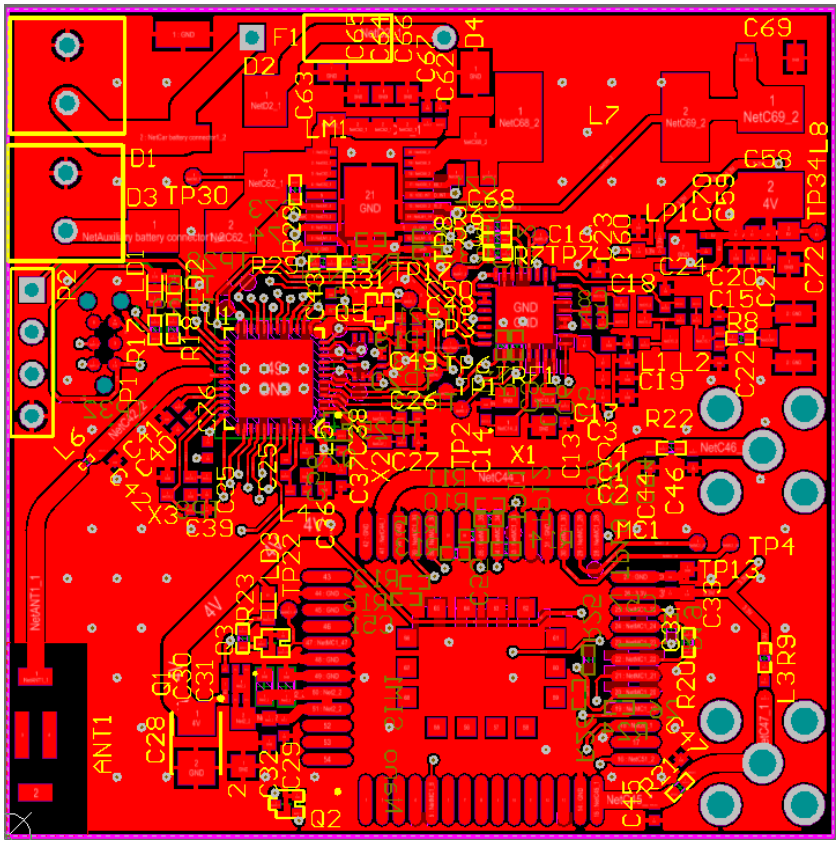
I - prąd płynący przez ścieżkę

Drugi przypadek wynika niejako z pierwszego. Gdy opór ścieżki jest zbyt duży, energia tracona na ścieżce jest tak duża, że ulega ona przepaleniu i całe urządzenie przestaje działać. Aby się przed tym ustrzec, ścieżki zasilające mają grubość 2 mm, co pozwala na przepływ około 3.5 A natężenia ciągłego prądu w temperaturze 20 stopni Celsjusza. Ze względu jednak na fakt, iż główne obciążenie urządzenia stanowi prąd chwilowy, trwający bardzo krótko, średnie natężenie prądu będzie dużo niższe od tej wartości. Tabela zestawiająca zależność między grubością ścieżek na płytce PCB od wartości maksymalnego dopuszczalnego prądu ciągłego, przepływającego przez nią, przedstawiono na rysunku 4.3.

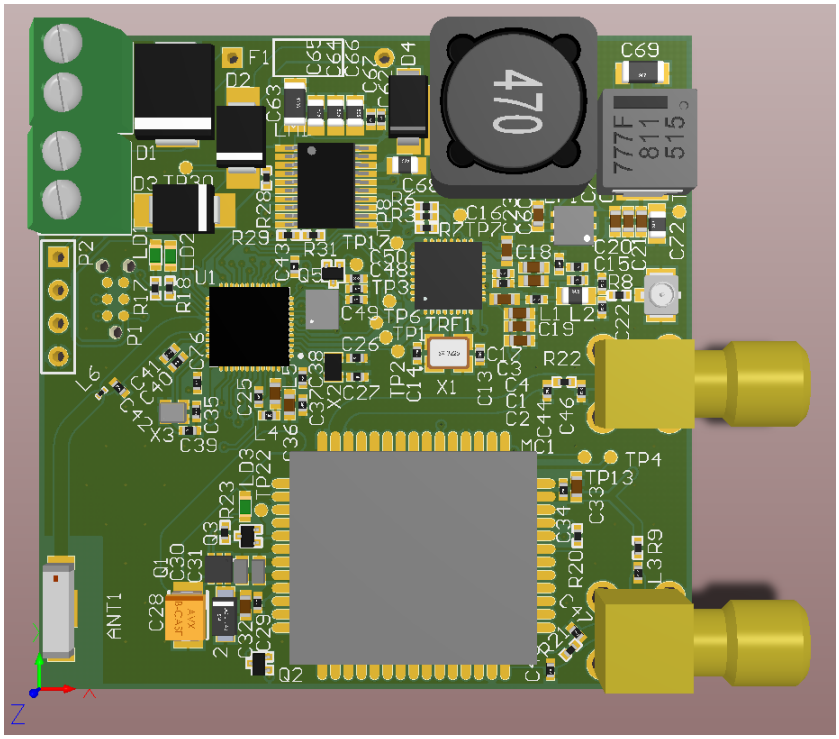
Szerokość ścieżki	Dopuszczalny prąd		
	ΔT=20°C	ΔT=80°C	prąd niszczący
0,5mm (20mil)	1,5A	3,5A	6A
1mm (40mil)	2,5A	5A	8A
2mm (80mil)	3,5A	7A	12A
3mm (120mil)	5A	10A	18A

Uwaga! dotyczy typowej płytki drukowanej o grubości miedzi 0,035…0,038mm

Rysunek 4.3: Tabela opisująca korelację między grubością ścieżek, a maksymalnym dopuszczalnym natężeniem prądu. Źródło: [9]

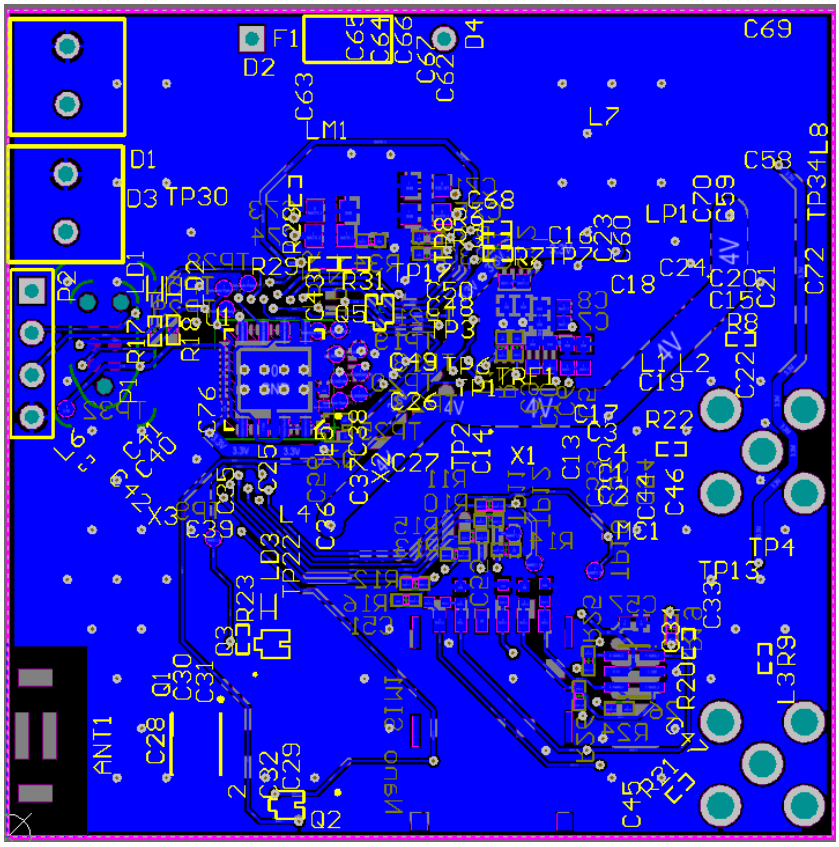


(a) Wygląd górnej warstwy płytki

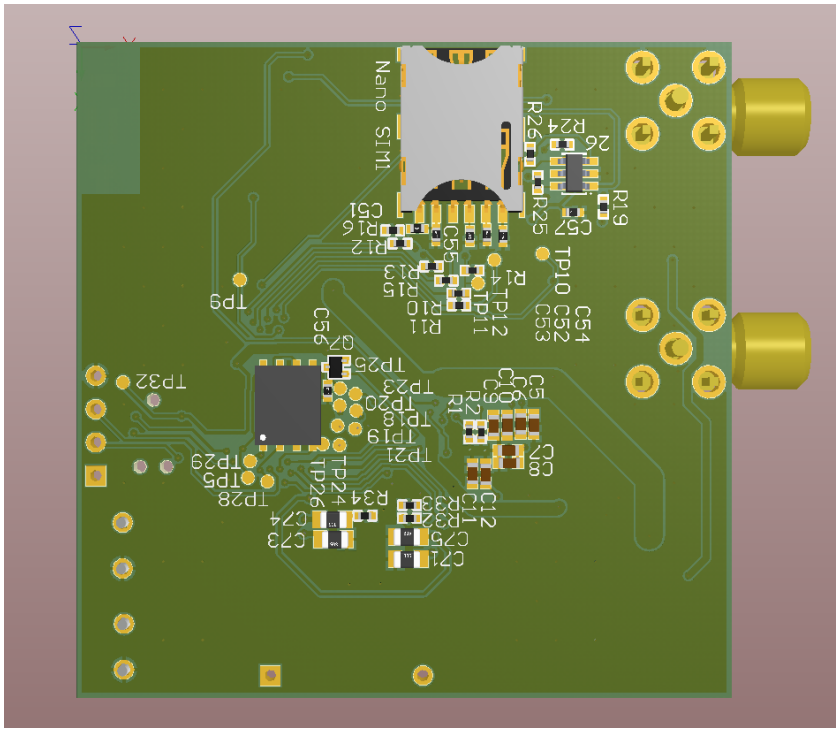


(b) Wizualizacja górnej warstwy płytki

Rysunek 4.4: Wygląd górnej warstwy płytki urządzenia lokalizującego oraz jej wizualizacja. Źródło: Twórczość własna



(a) Wygląd dolnej warstwy płytki



(b) Wizualizacja dolnej warstwy płytki

Rysunek 4.5: Wygląd dolnej warstwy płytki urządzenia lokalizującego oraz jej wizualizacja. Źródło: Twórczość własna

Rozdział 5

Bezpieczeństwo komunikacji

Jednym z podstawowych wymagań dotyczących tej pracy jest bezpieczna wymiana komunikatów poprzez Bluetooth Low Energy. Jest to tak kluczowe, ponieważ za pomocą tego protokołu, poprzez bezprzewodowe medium, przesyłane są kluczowe dane, zwłaszcza komendy dezaktywujące tryb alarmowy urządzenia. Transmisja fizycznie jest zawsze realizowana rozgłoszeniowo, co powoduje, że jej podsłuchanie nie jest trudnym zadaniem. Jest to niebezpieczne z dwóch powodów. Pierwszym z nich jest fakt wysyłania wrażliwych danych, jak na przykład dane lokalizujące pojazd. Dzięki nim, potencjalny złodziej mógłby po krótkiej analizie bezproblemowo określić miejsca, w których regularnie przebywa pojazd, a następnie wybrać dla niego najbardziej korzystne I przygotować się do kradzieży. Po drugie, co ważniejsze, będąc w pobliżu pojazdu w trakcie dezaktywacji trybu alarmowego, byłby w stanie podsłuchać komendę dezaktywującą, a następnie zapisać ją w celu późniejszego odtworzenia, umożliwiającego późniejszą bezproblemową kradzież pojazdu.

Z przytoczonych powyżej powodów komunikacja bezprzewodowa musi być szyfrowana. Jednakże operacja ta sama w sobie nie zabezpiecza tak naprawdę komendy dezaktywującej, a jedynie wrażliwe dane. Wynika to z faktu, iż w przypadku przechwycenia danych przesyłanych bezprzewodowo, dzięki szyfrowaniu są one nadal bezpieczne, ponieważ są one kompletnie niezrozumiałe. Inaczej ma się to do komendy deszyfrującej. Wynika to z faktu, że komenda ta tak naprawdę nie musi być zrozumiała dla potencjalnego złodzieja. Wystarczy, że jedynie ją odtworzy, nawet w formie zaszyfrowanej. Urządzenie wówczas ją zdeszyfruje I wykona deaktywację alarmu. Wszystko przez fakt, że komenda ta jest stała, nie zawiera elementu zmiennego w czasie. W wyniku szyfrowania stałej komendy stałym kluczem szyfrującym, uzyskamy oczywiście stały I powtarzalny pakiet zaszyfrowanych danych, które mogą być bezcenne w ręku potencjalnego złodzieja. W celu zabezpieczenia się przed tym, do komunikacji należy wprowadzić element zmienności w czasie.

5.1 AES

Jako główny algorytm szyfrowania w niniejszej pracy wykorzystano algorytm AES (ang. Advanced Encryption Standard) w wersji ze 128-bitowym kluczem szyfrującym. Wyboru tego dokonałem, ponieważ zastosowany przeze mnie mikrokontroler nRF52832 firmy Nordic Semiconductor posiada sprzetowe wsparcie szyfrowania danych wykorzystując właśnie AES128. Algorytm ten powstał w 2001 roku w Stanach Zjednoczonych w ośrodku NIST (ang. National Institude of Standards and Technology) w wyniku prac badawczych dwóch belgijskich kryptografów - Vincenta Rijmena I Joan'a Daemen, od których nazwisk powstała oryginalna nazwa algorytmu – Rijndael. Stanowi on jeden z najpopularniejszych na świecie szyfrów symetrycznych, a o jego skuteczności stanowi fakt, że w 2002r. Został przyjęty jako federalny standard szyfrowania w Stanach Zjednoczonych. Pojęcie szyfr symetryczny oznacza, że do zaszyfrowania oraz zdeszyfrowania stosuje się ten sam klucz szyfrujący (w przeciwieństwie do algorytmów asymetrycznych, gdzie stosuje się dwa klucze, jeden do szyfrowania, a drugi do deszyfracji). Z tego powodu, klucz szyfrujący stanowi ekstremalnie wrażliwą daną, której pod żadnym pozorem nie powinno się przesyłać poprzez ogólno dostępne medium komunikacyjne. Wyciek klucza szyfrującego powoduje kompromitację całej komunikacji w wyniku czego przestaje ona być uznawana za bezpieczną. Proces szyfrowania składa się z kilku kroków. Pierwszym z nich jest podzielenie danych wejściowych (zwyczajowo nazywanych tekstem jawnym) na bloki o rozmiarze 128 bitów, czyli szesnasty bajtów. Każdy blok przedstawiany jest jako macierz o wymiarach 4 bajty x 4 bajty, szeregowana kolumnami. Macierze te nazywają się macierzami stanu. Następnie, na każdej z tych macierzy (bloku danych) kolejne operacje:

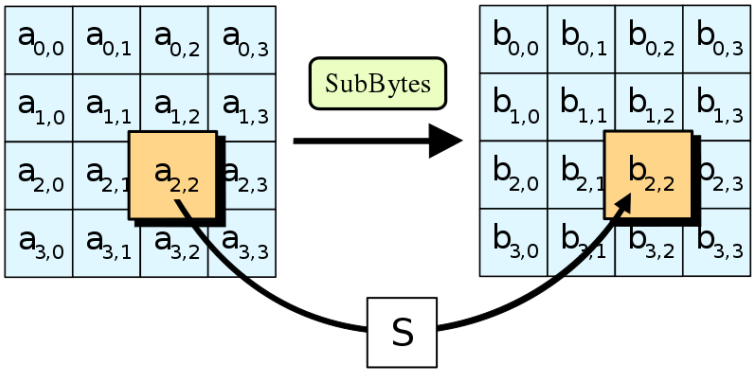
1. Utworzenie podkluczy – Etap ten polega na wygenerowaniu w sposób losowy klucza pierwotnego, a następnie na jego podstawie - po jednym podkluczu dla każdej z rund szyfrujących. Ich liczba jest uzależniona od rozmiaru klucza. Dla klucza 128-bitowego występuje 10 rund, dla klucza 192-bitowego – 12 cykli, a dla klucza 256-bitowego – 14 powtórzeń, wliczając klucz pierwotny.

2. Wykonanie rundy wstępnej (inicjującej) – Polega na wykonaniu operacji alternatywy wyłączającej – XOR (ang. Exclusive Or) dla każdego bajtu z bloku danych oraz odpowiadającego mu bajtu w kluczu pierwotnym.

3. Wykonanie rund szyfrujących – Etap ten jest wykonywany kilkukrotnie, w zależności od liczby cykli. Każda runda składa się z kilku kroków.

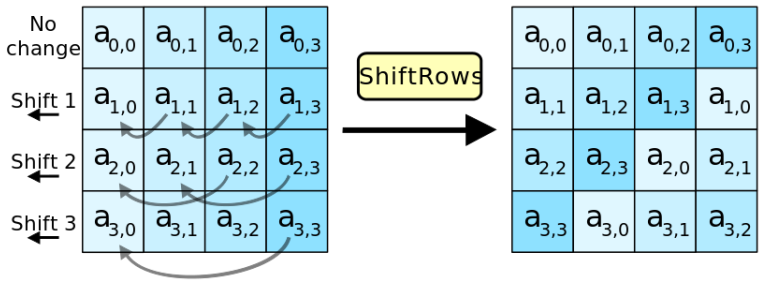
    - W pierwszym z nich, każdy bajt danych jest zastępowany innym bajtem pobranym w z góry zdefiniowanej tablicy (ang. lookup table) nazywanej S-Boxe'em Rijndael'a.

Operacja ta nazywa się w skrócie SB (ang. Substitude Bytes) i przedstawiono ją na rysunku 5.1. Zgodnie z zamysłem twórców, tablica ta gwarantuje nieliniowość przekształcenia, a w efekcie i całego szyfrowania.



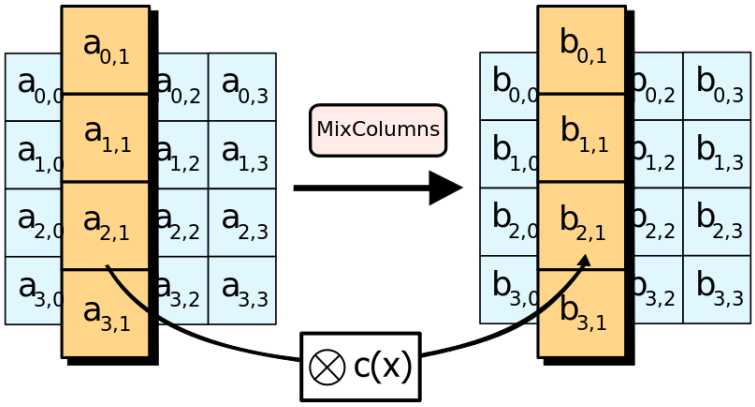
Rysunek 5.1: Wykonanie operacji Substitute Bytes. Źródło: [11]

- Kolejny krok to zamiana wierszy. Polega na przesunięciu bajtów w trzech ostatnich wierszach bloku. Pierwszy wiersz pozostaje bez zmian, w drugim wierszu bajty są przesuwane o jeden w lewo, w trzecim o dwie pozycje w lewo, a w ostatnim o 3 miejsca w tym samym kierunku. Każdy bajt, który w wyniku przesunięcia znajdzie się poza wierszem, zostaje umieszczony na jego ostatniej pozycji (wiersze w wyniku rotacji się zawijają). Operacja ta nosi miano SR (ang. Shift Rows). Przedstawiono ją na rysunku 5.2.



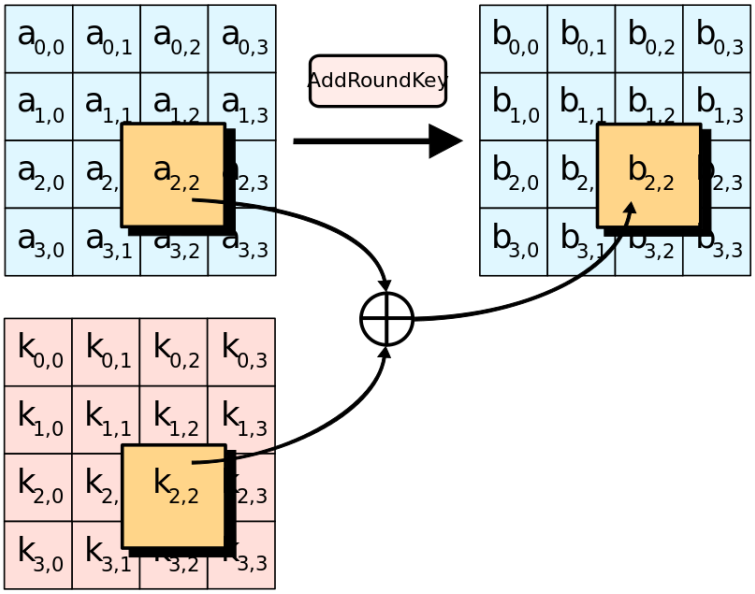
Rysunek 5.2: Wykonanie operacji Shift Rows. Źródło: [11]

- Trzecim z kolei krokiem jest operacja mieszania kolumn – MC (ang. Mix Columns). W tym etapie, każda z kolumn jest przemnażana lewostronnie przez przez stałą macierz o wymiarach 4 x 4, w wyniku czego powstaje kolumna z nowymi wartościami. Operacja ta przedstawiona jest na rysunku 5.3.



Rysunek 5.3: Wykonanie operacji Mix Columns. Źródło: [11]

- Ostatni krok nazywany jest AR (ang. Add Round Key) i polega na wykonaniu operacji XOR na każdym bajcie bloku danych i odpowiadającym mu bajcie w kluczu przypisanym do danej rundy. Wizualizację kroku przedstawiono na rysunku 5.4.



Rysunek 5.4: Wykonanie operacji Add Round Key. Źródło: [11]

4. Ostatni etap to runda kończąca – W jej trakcie wykonywane są operacje identyczne jak w rundach szyfrujących, za wyłączeniem mnożenia kolumn, która nie występuje.

Deszyfrowanie jest operacją odwrotną do szyfrowania i polega na przekształceniu danych zaszyfrowanych na tekst jawny. Tak samo jak w przypadku szyfrowania, tekst dzieli się na 16-bajtowe bloki. W jego trakcie wykonuje się analogiczne operacje co w przypadku szyfrowania.

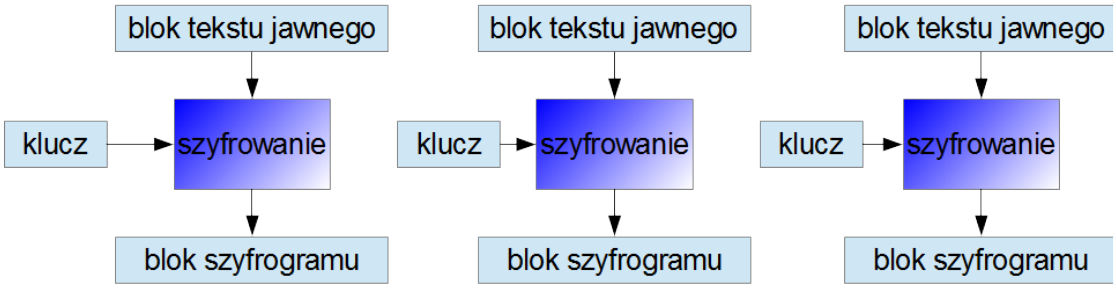
1. Odwrotne podstawianie bajtów – polega na ponownym zastosowaniu tablicy S-Box w celu podmiany bajtów.

2. Przesuwanie bajtów w wierszach w prawo. Zasada jest taka sama jak w operacji SR, zmienia się jedynie kierunek.

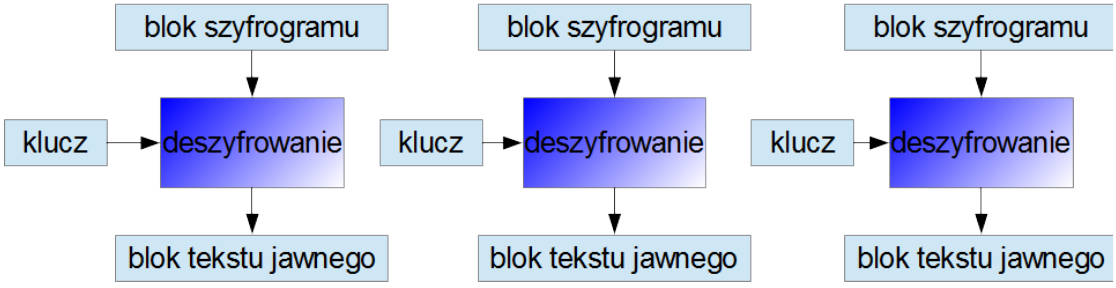
3. Wykonanie operacji XOR dla każdego bajtu bloku danych z odpowiadającym mu bajtem w podkluczu przypisanym do danej rundy deszyfrującej. Podklucze są takie same jak w trakcie szyfrowania, lecz powinny być brane w kolejności odwrotnej (zaczynając od ostatniego, a kończąc na kluczu pierwotnym).

4. Ostatnia operacja to odwrócone mnożenie kolumn.

W efekcie uzyskujemy blok danych zdeszyfrowanych. Przedstawiony tutaj wariant algorytmu szyfrowania nosi miano ECB (ang. Electronic Codebook) i stanowi najprostrzą metodę szyfrowania. Można go przedstawić na rysunkach 5.5 oraz 5.6.



Rysunek 5.5: Operacja szyfrowania metodą ECB. Źródło: [10]

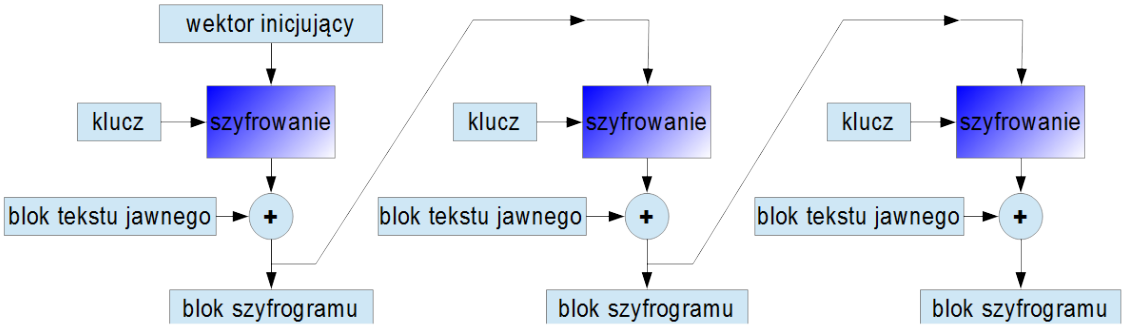


Rysunek 5.6: Operacja deszyfrowania metodą ECB. Źródło: [10]

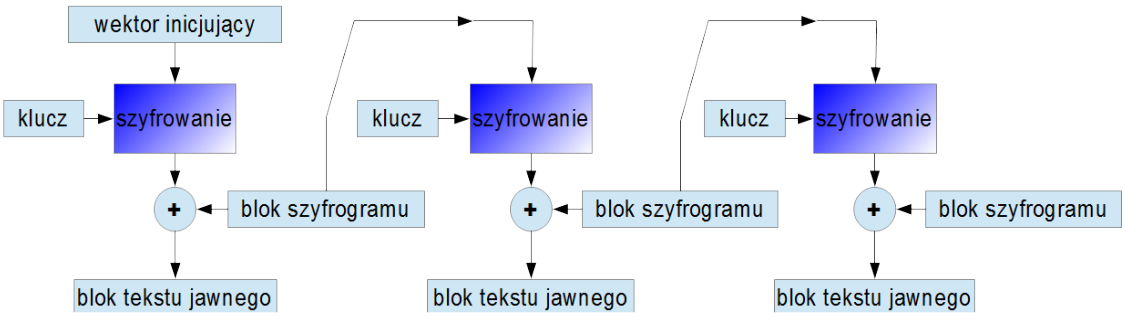
Czas trwania szyfrowania pojedynczego bloku danych o długości szesnastu bajtów na mikrokontrolerze nRF52832 wynosi około 30 μs. Deszyfrowanie trwa zaś około 60 μs.

5.2 Dodatkowe warianty szyfrowania AES

Jak zostało przedstawione wcześniej, mechanizmy szyfrowania doskonale działają w przypadku wrażliwych danych. Nie sprawdzają się natomiast w przypadku przesyłania komend, ze względu na brak zmienności pakietów w czasie i możliwości zwyczajnego odtworzenia zaszyfrowanego pakietu przez niepowołane osoby. Z tego powodu, do komunikacji należy wprowadzić element zmienności. Jednym z wariantów algorytmu AES jest tzw. CFB (ang. Cipher Feedback), przedstawiony na rysunkach 5.7 oraz 5.8. Stanowi on wysokopoziomowy algorytm, który bazuje na wariancie ECB, zmieniając jedynie logiczną strukturę informacji niezbędnych do szyfrowania. Przede wszystkim, wprowadza pojęcie wektora inicjującego (ang. initializing vector), który stanowi niezbędny dodatkowy element zmienności. Klucz główny bowiem zazwyczaj jest niezmienny na przestrzeni życia komunikujących się ze sobą urządzeń, co wynika z faktu konieczności nieupubliczniania go. Wektor inicjujący jest natomiast generowany przy każdej nowej komunikacji.



Rysunek 5.7: Operacja szyfrowania metodą CFB. Źródło: [10]



Rysunek 5.8: Operacja deszyfrowania metodą CFB. Źródło: [10]

W odróżnieniu od wariantu ECB, zamiast tekstu jawnego, szyfrowaniu ulega wektor inicjujący. Jego postać zaszyfrowana jest następnie poddawana operacji XOR z blokiem danych tekstu jawnego, a powstały w ten sposób szyfrogram stanowi nowy wektor inicjujący dla na-

stępnego bloku danych. W przypadku deszyfrowania korzysta się oczywiście z tego samego wektora inicjującego oraz klucza szyfrującego. Co ciekawe, w odróżnieniu od wariantu ECB, w metodzie CFB deszyfrowanie jest to tak naprawdę szyfrowanie. Oznacza to, że wystarczy zaimplementować jedynie mechanizm szyfrowania w algorytmie AES, aby móc zarówno szyfrować jak i deszyfrować wiadomości. Zaszyfrowany wektor inicjujący jest poddawany operacji XOR z blokiem tekstu zaszyfrowanego w efekcie czego uzyskujemy blok tekstu jawnego. Natomiast blok tekstu zaszyfrowanego stanowi wektor inicjujący dla następnych bloków szyfru.

5.3 Realizacja szyfrowania komunikacji w projekcie

W pracy zdecydowano się na wykorzystanie zarówno metod ECB oraz CFB. Pierwszym, a zarazem najbardziej podstawowym etapem jest generowanie klucza szyfrującego. Operacja ta jest realizowana przez płytę główną systemu lokalizującego. Następnie, klucz jest przekazywany p ten na żądanie użytkownika oprzez interfejs NFC (ang. Near Field Communication) do urządzenia deaktywującego, pełniącego rolę beacona (rozgłośni). Zastosowanie NFC jest powszechnie uważane za bezpieczną metodę komunikacji, ze względu na jej bardzo niską moc transmisji, a tym samym bardzo niewielki zasięg (do 5 cm). Ogranicza to zatem możliwość podsłuchania klucza szyfrującego do zera. Przy pomocy tego klucza, za każdym razem gdy płyta główna systemu połączy się z urządzeniem deaktywującym w celu uzyskania od niego komendy deaktywującej, wpierw wyśle mu zaszyfrowany, nowo wygenerowany na potrzeby danego połączenia wektor inicjalizacyjny. Umożliwi to dalszą komunikację wykorzystując wariant CFB oraz niezbędną zmienność zaszyfrowanych pakietów, praktycznie niwelującą skuteczność podsłuchiwania transmisji.

Rozdział 6

Oprogramowanie

6.1 Urządzenie dezaktywujące

6.2 Urządzenie lokalizujące

6.3 Aplikacja mobilna

6.4 Aplikacja serwerowa

6.5 Strona internetowa

Rozdział 7

Analiza stylu jazdy

Rozdział 8

Podsumowanie

Bibliografia

[1] Spark Nano. *Spark Nano 5.0 GPS Tracker*. https://ii.brickhousesecurity.com/fcgi-bin/iipsrv.fcgi?FIF=/images/brickhousesecurity//source/GPS-SN5_6.tif&wid=335&cvt=jpeg.

[2] My Car Tracks. *Aplickacja na smartphone MyCarTracks*. https://www.mycartracks.com/features;jsessionid=3D9E99856BB52CB325C6D699AA3EF5F0.mct-node-one.

[3] STI. *STI GL300 GPS Tracker*. https://images-na.ssl-images-amazon.com/images/I/81Xv5REeNxL._SL1500_.jpg.

[4] Agilent Technologies. *GSM presentation*. http://mars.merhot.dk/w/images/8/88/GSM_praesentation_noter.pdf, 2000.

[5] Tutorials Point Pvt. Ltd. *GLOBAL SYSTEM FOR MOBILE COMMUNICATIONS (GSM) TUTORIAL*. https://www.tutorialspoint.com/gsm/gsm_tutorial.pdf, 2014.

[6] *Cellular network architecture image*. https://en.wikipedia.org/wiki/Cellular_network.

[7] Nordic Semiconductor. *Dokumentacja SDK mikrokontrolerów rodziny nRF5x*. https://infocenter.nordicsemi.com/index.jsp.

[8] Monika Jaworowska. *Projektowanie płytek PCB dla linii szybkiej komunikacji*. https://elektronikab2b.pl/technika/19012-projektowanie-plytek-drukowanych-z-ukladam
.WgYv75-YUW1, 2013.

[9] Piotr Górecki. *O paskudztwach i czarodziejach, czyli zakłócenia w układach elektrycznych*. https://elportal.pl/pdf/2003/edw_2003_09_s20.pdf, 2003.

[10] Krzysztof Kowalczyk. *Advanced Encryption Standard*. http://www.crypto-it.net/pl/symetryczne/aes.html?tab=1.

[11] en.wikipedia.org. *Advanced Encryption Standard*.
`https://en.wikipedia.org/wiki/Advanced_Encryption_Standard`.

Wykaz skrótów

AES	Advanced Encryption Standard
API	Application Programming Interface
BLE	Bluetooth Low Energy
GATT	Generic Attibute
GCC	GNU Compiler Collection
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GSM	Global System for Mobile Communication
ISM	Industrial, Scientific, Medical (pasmo częstotliwości)
MAC	Media Access Control
RAM	Random Access Memory
RSSI	Radio Signal Strength Indicator
SDK	Software Development Kit
SMS	Short Message System
SIM	Subscriber Identification Module
UHF	Ultra High Frequency