POLITECHNIKA GDAŃSKA
WYDZIAŁ ELEKTRONIKI, TELEKOMUNIKACJI I INFORMATYKI

Imię i nazwisko studenta: Adrianna Piekarska
Nr albumu: 165152
Studia pierwszego stopnia
Forma studiów: stacjonarne
Kierunek studiów: Informatyka
Profil: Architektura systemów komputerowych

Imię i nazwisko studenta: Grzegorz Wąs
Nr albumu: 165464
Studia pierwszego stopnia
Forma studiów: stacjonarne
Kierunek studiów: Informatyka
Profil: Inteligentne systemy interaktywne

PROJEKT DYPLOMOWY INŻYNIERSKI

Tytuł projektu w języku polskim: Bezprzewodowy system dostępu do pomieszczeń

Tytuł projektu w języku angielskim: Wireless access control system

Potwierdzenie przyjęcia projektu	
Opiekun projektu *podpis*	Kierownik Katedry/Zakładu (pozostawić właściwe) *podpis*
dr inż. Tomasz Dziubich	

Data oddania projektu do dziekanatu:

Streszczenie

Systemy wykorzystujące urządzenia elektroniczne od wielu lat stosowane są we wszystkich dziedzinach ludzkiego życia. Rozwój technologii bezprzewodowych oraz postępująca miniaturyzacja urządzeń elektronicznych sprawiają, że systemy te stają się nowocześniejsze, bezpieczniejsze i wydajniejsze. Jednym z celów, dla których stosowane są tego typu systemy jest zapewnienie bezpieczeństwa ludziom oraz mieniu. Niniejsza praca opisuje projekt i implementację bezprzewodowego systemu dostępu do pomieszczeń. Omawia architekturę rozwiązania z uwzględnieniem poszczególnych podsystemów, przedstawia ciekawe aspekty realizacji projektu oraz jego rezultaty. Ponadto, prezentuje zagadnienia związane z bezpieczeństwem oraz wydajnością energetyczną bezprzewodowych systemów opartych na mikrokontrolerach.

Słowa kluczowe: zamek elektroniczny, mikrokontroler, kontrola dostępu, WiFi, RFID, sieć bezprzewodowa, autoryzacja

Dziedzina nauki i techniki, zgodnie z wymogami OECD:

Abstract

Systemy wykorzystujące urządzenia elektroniczne od wielu lat stosowane są we wszystkich dziedzinach ludzkiego życia. Rozwój technologii bezprzewodowych oraz postępująca miniaturyzacja urządzeń elektronicznych sprawiają, że systemy te stają się nowocześniejsze, bezpieczniejsze i wydajniejsze. Jednym z celów, dla których stosowane są tego typu systemy jest zapewnienie bezpieczeństwa ludziom oraz mieniu. Niniejsza praca opisuje projekt i implementację bezprzewodowego systemu dostępu do pomieszczeń. Omawia architekturę rozwiązania z uwzględnieniem poszczególnych podsystemów, przedstawia ciekawe aspekty realizacji projektu oraz jego rezultaty. Ponadto, prezentuje zagadnienia związane z bezpieczeństwem oraz wydajnością energetyczną bezprzewodowych systemów opartych na mikrokontrolerach.

Keywords:

Spis treści

Spis rysunków

Spis kodów źródłowych

Wykaz ważniejszych oznaczeń i skrótów

Pojęcie	Wyjaśnienie
Punkt dostępu	Fizyczne zabezpieczenie chroniące przed nieuprawnionym dostępem, przykładowo: zamek, bramka
RFID	Technologia wykorzystująca fale radiowe w celu przesyłania danych (ang. Radio-frequency identification)
Karta	Karta zbliżeniowa RFID. Inne określenia: identyfikator, token
Kontroler	Komponent odpowiedzialny za zarządzanie układem zamka
Break glass device	Urządzenie awaryjne umożliwiające odcięcie zasilania w zamku

Rozdział 1

Wstep i cel pracy

Zapewnienie bezpieczeństwa przestrzeni użytkowych i osób z nich korzystających stanowi kluczowy aspekt zarządzania obiektami zarówno publicznymi, jak i prywatnymi. Dzięki zastosowaniu odpowiedniej infrstruktury, bezpieczeństwo osób przebywających na terenie obiektu rośnie, a ryzyko kradzieży lub zniszczenia mienia przez niepowołane osoby spada. Podstawową metodą kontroli dostępu do pomieszczeń są metody mechaniczne wykorzystujące jedynie fizyczne zabezpieczenia. Ze względu na postępujący rozwój technologiczny, w obecnych czasach coraz częściej stosowane są systemy oparte na uwierzytelnianiu elektronicznym.

Pod względem celu i ogólnych zasad działania, elektroniczny system kontroli dostępu do pomieszczeń nie rózni się od swojego tradycyjnego odpowiednika. Głównym celem pozostaje autoryzacja prób dostępu użytkowników na podstawie kluczy w taki sposób, aby dostęp został przyznany tylko osobie posiadającej powiązany z danym punktem dostępu klucz.

Przewagę systemów opartych na urządzeniach elektronicznych nad systemami czysto mechanicznymi stanowią cechy takie jak łatwość obsługi czy możliwość zdalnego zarządzania oraz zbierania danych i monitorowania prób dostępu w celu późniejszej analizy.

Celem niniejszej pracy jest projekt oraz implementacja sytemu dostępu do pomieszczeń z wykorzystaniem technologii takich jak WiFi oraz RFID (ang. *Radio-frequency identification*), w którym podmiotem odpowiedzialnym za autoryzację prób dostępu jest serwer, a komunikacja pomiędzy podsystemem sterowania zamkiem a podsystemem autoryzacji jest realizowana bezprzewodowo. Może on znaleźć zastosowanie jako łatwy w instalacji i obsłudze, lekki i wydajny system dla małych i średnich obiektów.

Podstawowe założenia dotyczące opisywanego systemu są następujące:

1. Logika uwierzytelniania powinna być zaimplementowana na serwerze. Urządzenie klienckie (zamek) powinno pełnić jedynie rolę pośrednika w tym procesie.

2. Komunikacja pomiędzy urządzeniami klienckimi (zamkami) a serwerem powinna odbywać się bezprzewodowo.

3. System powinien być wydajny energetycznie i umożliwiać operację zamków na zasilaniu

bateryjnym.

4. System powinien implementować niezbędne mechanizmy bezpieczeństwa.

Dzięki wykorzystaniu zdalnego serwera do przeprowadzenia procesu uwierzytelniania system zapewnia większą elastyczność i łatwość zarządzania niż alternatywne systemy wykorzystujące zamki pracujące w sposób autonomiczny. Informacje o uprawnieniach przechowywane są w centralnej bazy danych, znajdującej się na serwerze, którą można w prosty sposób zarządzać z poziomu aplikacji internetowej.

Rozwiązanie cechuje się wygodą montażu, ponieważ nie wymaga przewodów zasilających i komunikacyjnych prowadzonych w ścianach budynków. Przy wdrażaniu rozwiązania nie jest konieczna modyfikacja istniejącej infrastruktury budynku, z wyjątkiem wymiany samych zamków. System nie wymaga żadnych dodatkowych komponentów sprzętowych poza zamkami i serwerem. Do poprawnego działania systemu potrzebna jest sieć WiFi. Założono, że wykorzystana sieć nie musi być bezpieczna.

Wydajność energetyczna podsystemu sterowania zamkiem została osiągnięta przez zarządzanie zasilaniem jego peryferiów oraz kontrolę stanu zasilania mikrokontrolera w celu minimalizacji poboru mocy i maksymalizacji czasu pracy na zasilaniu bateryjnym.

Bezpieczeństwo systemu na wielu poziomach zapewnia wykorzystanie mechanizmów takich jak TLS (ang. *Transport Layer Security*) w warstwie komunikacji pomiędzy zamkiem a serwerem czy szyfrowanie pamięci Flash w warstwie operacji na danych w mikroprocesorze w układzie zamka.

1.1 Zakres pracy

Pracę nad systemem prowadziły dwie osoby. W ramach tej pracy powstały:

- Protoyp układu zamka,
- Oprogramowanie serwera uwierzytelniania,
- Aplikacja do zarządzania.

Implementacja prototypu obejmowała stworzenie pojedynczego układu zamka. Ze względu na prototypowy charakter pracy, nie przetestowano działania systemu z większą liczbą zamków. Nie ma jednak powodów by twierdzić, że system nie działałby poprawnie z większą liczbą zamków.

Tutaj podział pracy i obowiązków - TBD

1.2 Struktura pracy

Rozdział 2 pokrótce przedstawia dziedzinę problemu, przywołuje najważniejsze definicje związane z tematem oraz ogólny opis działania systemów kontroli dostępu. Dokonuje także przedstawienia oraz porównania kilku istniejących na rynku rozwiązań.

Rozdział 3 prezentuje projekt rozwiązania.

Rozdział 4 przedstawia proces implementacji systemu wraz z prezentacją najciekawszych problemów implementacyjnych oraz wykorzystanych technologii. W ramach pracy zaimplementowany został prototyp rozwiązania. Rozdział prezentuje również możliwe modyfikacje i rozszerzenia tego prototypu.

Rozdział 5 opisuje rezultaty pracy nad projektem.

Rozdział 6 dokonuje podsumowania pracy.

Rozdział 2

Dziedzina problemu

Niniejszy rozdział krótko opisuje dziedzinę problemu w oderwaniu od szczegółów technicznych przygotowanego w ramach pracy rozwiązania. Przedstawia również porównanie niektórych z obecnie dostępnych na rynku systemów kontroli dostępu.

2.1 Kontrola dostępu

Kontrola dostępu to środki mające na celu zapewnienie, że do zasobów systemu przetwarzania danych mogą mieć dostęp tylko uprawnione jednostki w uprawniony sposób [1].

British Security Industry Association wyodrębnia kilka komponentów składających się na system kontroli dostępu [2]. Poniżej przedstawiono wybrane komponenty, które mają zastosowanie lub są powiązane z opisywanem systemem.

Poświadczenie tożsamości (ang. *credentials*) to fizyczny lub materialny obiekt, element wiedzy lub cecha biometryczna umożliwiająca uzyskanie dostępu do kontrolowanej strefy. Najczęściej jako poświadczenie tożsamości stosuje się kody, np. PIN (ang. *Personal Identification Number*, osobisty numer identyfikacyjny), tokeny (karty, urządzenia mobilne itp.) oraz dane biometryczne. [2]

British Security Industry Association terminem ̈czytniki(̈ang. *readers*) nazywa urządzenia odpowiedzialne za kontrolę dostępu. Dla uproszczenia nomenklatura ta została zachowana w niniejszej sekcji. W innych częściach niniejszej pracy termin ̈czytniki̇używany jest w znaczeniu urządzenia odpowiedzialnego za odczyt danych z nośnika.

Czytniki mogą pracować samodzielnie; wyposażone są wówczas w urządzenia wejścia/wyjścia niezbędne do zarządzania zamkiem oraz pamięć i moc obliczeniową niezbędne do autonomicznego podejmowania decyzji. Zazwyczaj wyposażone są w uniwersalny kod umożliwiający uzyskanie dostępu każdemu kto wejdzie w jego posiadanie. [2]

Czytniki mogą też pracować pod kontrolą innego urządzenia. Odczytane z nośnika dane poświadczające tożsamość przekazują do nadrzędnego urządzenia zwanego kontrolerem. [2]

Istnieją również czytniki łączące funkcjonalność zarówno czytnika jak i kontrolera w jednym

urządzeniu. Posiadają one lokalną kopię bazy danych, na podstawie której podejmowana jest decyzja o przyznaniu lub odmowie dostępu. [2]

Tzw. czytniki offline (ang. *offline readers*) różnią się od zwykłych czytników łączących funkcjonalności czytnika i kontrolera tym, iż nie przechwoują kopii bazy danych. W tym przypadku to nośnik danych(karta) zawiera informacje o tym, które zamki może otworzyć. Czytnik offline analizuje te dane i na ich podstawie podejmuje stosowną decyzję o podjęciu lub odmowie dostępu. [2]

Czytniki online (ang. *online readers*) także nie przechowują kopii bazy danych. Decyzja o przyznaniu lub odmowie dostępu jest w ich przypadku podejmowana przez podłączony komputer, który przesyła odpowiednią komendę po udanej autentykacji. [2]

W rozwiązaniach sieciowych czytniki mogą być podłączone do kontrolera, który przechowuje informacje niezbędne do podjęcia decyzji o przyznaniu bądź odmowie dostępu. [2]

Urządzenia wyjściowe (ang. *egress devices*) umożliwiają użytkownikowi opusczenie strefy chronionej od wewnątrz. Jako urządzenia wyjściowe najczęściej używa się przełączników, czujników ruchu lub czytników. Według British Security Industry Association urządzenia wyjściowe można podzielić je na zwykłe oraz awaryjne (ang. *emergency egress*), przy czym, ze względu na krytyczne znaczenie w wypadku awarii, działanie tych drugich nie powinno zależeć od komponentów systemu (kontrolera systemu, oprogramowania itp.). Jako urządzenie awaryjne często stosuje się tzw. *break glass device*, którego uaktywnienie powoduje odcięcie zasilania w zamku, a tym samym wstrzymanie kontroli dostępu w danym punkcie. Dostęp uzyskany za pomocą tego urządzenia powinien wygenerować stosowne powiadomienie bądź alarm. [2]

W zależności od potrzeb, oprogramowanie w systemie może być samodzielnym programem zainstalowanym na komputerze osobistym bądź złożonym i bezpiecznym oprogramowaniem zainstalowanym na serwerze. Często opiera się na rozwiązaniach webowych lub mobilnych, umożliwiając dostęp z dowolnego urządzenia. [2]

British Security Industry Association w następujący sposób przedstawia sposób działania systemów kontroli dostępu:

W systemie on-line, w momencie gdy poświadczenie tożsamości zostaje przedstawione czytnikowi, informacja przesyłana jest do kontrolera. Kontroler porównuje otrzymane dane z listą autoryzowanych użytkowników w bazie danych. Jeżeli przedstawione dane znajdują się w bazie, kontroler wysyła sygnał otworzenia zamka. Sygnał wysyłany jest do czytnika w celu wizualnego lub dźwiękowego powiadomienia użytkownika o podjętej decyzji. [2]

W systemie off-line, w momencie gdy poświadczenie tożsamości zostaje przedstawione czytnikowi, czytnik dokonuje sprawdzenia, czy dostęp powinien zostać przyznany. Jeżeli tak, czytnik zezwala na dostęp i aktualizuje przedstawiony nośnik danych poświadczających tożsamość. W momencie zaprezentowania tego samego nośnika w czytniku wyposażonym w kontroler dane na temat dostępów zostaną zanotowane w systemie, a sam nośnik może zostać zaktualizowany o zmiany w prawach dostępu, jeśli takie nastąpiły. [2]

W większości przypadków tylko wejście podlega kontroli. Aby możliwa była również kontrola wyjścia z chronionego terenu, potrzebny jest drugi czytnik umieszczony po drugiej stronie drzwi.

Jeżeli obustronna kontrola nie jest wymagana, stosuje się zazwyczaj przycisk umożliwiający otworzenie zamka od środka. [2]

W przypadku, gdy system kontroli dostępu nie funkcjonuje odpowiednio (np. z powodu braku zasilania), stosuje się tzw. *break glass device*. [2]

2.2 Przegląd dostępnych rozwiązań

Obecnie stosowane rozwiązania różnią się od siebie pod wieloma względami. W mniej wymagających systemach często stosuje się rozwiązania oparte są na architekturze rozproszonej. W rozwiązaniach tego typu urządzenia kontrolujące zamki pracują w sposób autonomiczny. Oznacza to, iż cały proces uwierzytelniania dokonywany jest przez oprogramowanie mikroprocesora obsługującego zamek.

Na rynku dostępne są także rozwiązania sieciowe, bądź też takie, które umożliwiają konfigurację urządzeń w tryb zarówno autonomiczny, jak i sieciowy. Rozwiązania sieciowe charakteryzują się znacznym stopniem skomplikowania, zarówno pod względem architektonicznym (ilość i rodzaj potrzebnych komponentów sprzętowych) [3], jak i konfiguracyjnym (trudność instalacji, konieczność modyfikacji istniejącej infrastruktury). Mogą oferować oddzielenie funkcjonalności czytnika dostępu od kontrolera, umożliwiając obsługę do kilkunastu czytników za pomocą jednego urządzenia kontrolującego [3]. Mimo możliwości dołączenia do kontrolera zamków bezprzewodowych, działanie całego systemu wciąż pozostaje uzależnione od komunikacji przewodowej.

Ze względu na ilość komponentów sprzętowych, istniejące rozwiązania bywają drogie.

Ten podrozdział wymaga przemyślenia.

Rozdział 3

Projekt rozwiązania

Niniejszy rozdział opisuje koncept rozwiązania powstały w ramach pracy. Nakreśla wymagania funkcjonalne systemu oraz przedstawia jego schematyczną budowę. Prezentuje zakładany sposób działania w oderwaniu od aspektów implementacyjnych.

Ogólny zarys konceptu działania systemu przedstawiony jest na rysnku 3.1.

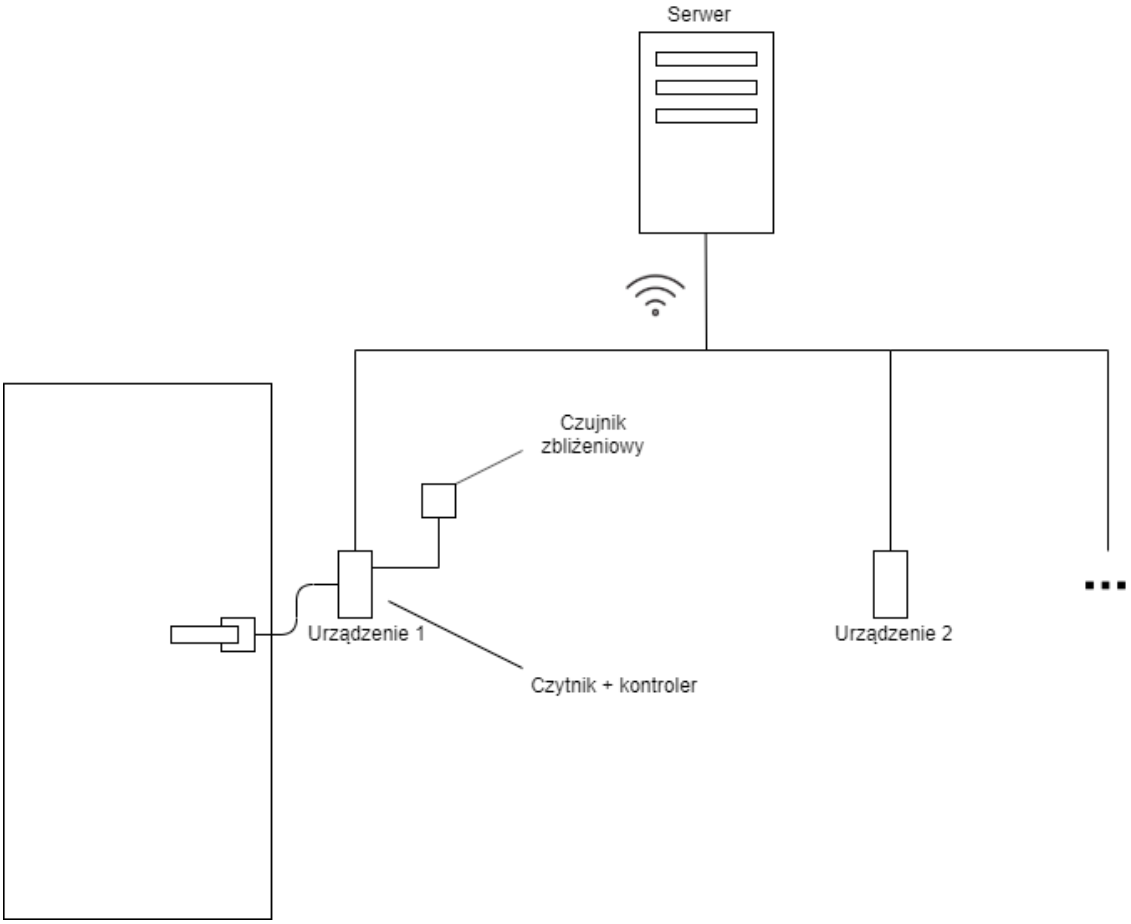
Nadrzędnym celem systemu jest umożliwienie kontroli dostępu na terenie danego obiektu. Poświadczenie tożsamości (*credentials*) stanowią karty RFID przyznawane użytkownikom systemu. Każda karta powiązana jest ze zbiorem zamków, w których zostanie z powodzeniem autoryzowana.

3.1 Działanie systemu

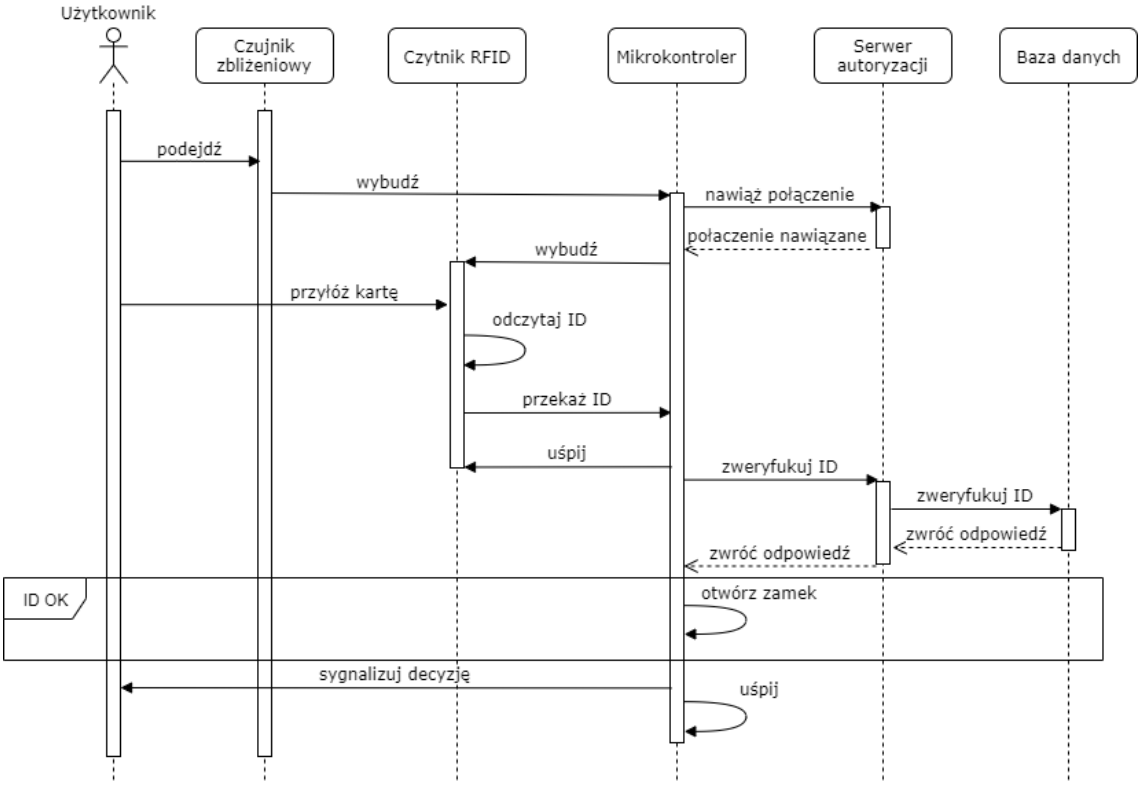
Poniżej w ogólny sposób opisano zakładany sposób działania systemu na podstawie scenariusza próby uzyskania dostępu przez użytkownika systemu.

Kontroler zamka pozostaje uśpiony do momentu wykrycia ruchu w pobliżu przez czujnik ruchu. Po wybudzeniu, kontroler nawiązuje bezpieczne połączenie z serwerem autoryzacji, jednocześnie zasilając czytnik RFID oraz oczekując na zbliżenie do niego karty. Gdy karta zostanie zbliżona, kontroler przesyła odczytany z niej numer identyfikacyjny wraz z numerem identyfikacyjnym zamka do serwera. Na podstawie tych danych, serwer podejmuje decyzję, którą jest przyznanie bądź odmowa dostępu, a następnie przesyła informację zwrotną do kontrolera. Jeżeli podjęto decyzję o przyznaniu dostępu, kontroler wysyła sygnał otwarcia zamka oraz sygnalizuje powodzenie. Jeżeli podjęto decyzję o odmowie dostępu, kontroler sygnalizuje niepowodzenie. Diagram sekwencji obrazujący opisywany scenariusz przedstawiony jest na rysunku 3.2.

Niezależnie od rezultatu, wpis o próbie dostępu zostaje zapisany w bazie danych, skąd może być pobrany przez podsystem zarządzania w celu prezentacji danych administratorowi systemu.



Rysunek 3.1: Koncept systemu kontroli dostępu



Rysunek 3.2: Diagram sekwencji ukazujący zasadę działania systemu

3.2 Architektura systemu

W ramach systemu można wyodrębnić następujące podsystemy:

1. Podsystem sterowania zamkiem,
2. Podsystem autoryzacji,
3. Podsystem zarządzania.

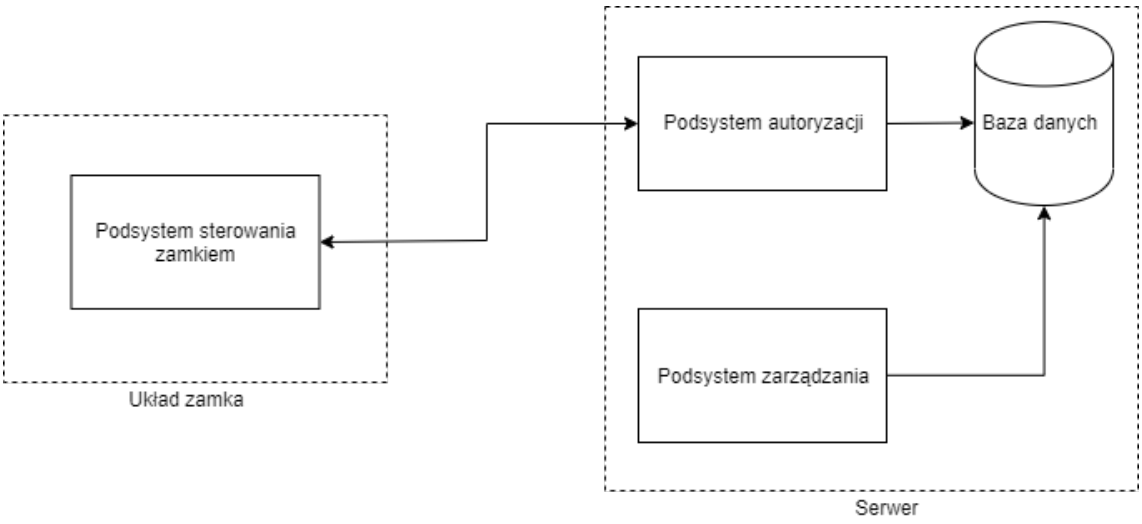
Przedstawione wyżej podsystemy współistnieją w ramach dwóch komponentów sprzętowych. Są to:

1. Komponent sterujący zamkiem (inaczej: kontroler, układ zamka),
2. Komponent serwera.

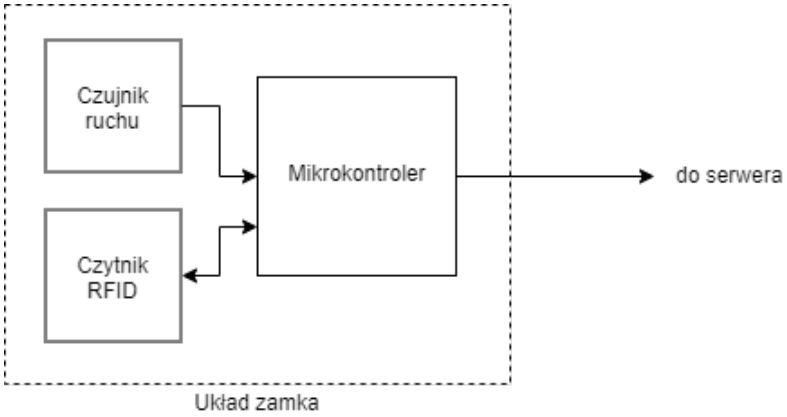
Komponenty sprzętowe zostały krótko omówione w kolejnych punktach. Ogólna sprzętowa architektura systemu z podziałem na komponenty oraz przynależne im podsystemy przedstawiona została na rysunku 3.3.

3.2.1 Komponent sterujący zamkiem

Założono realizację następujących funkcjonalności w ramach komponentu sterującego zamkiem:



Rysunek 3.3: Architektura systemu



Rysunek 3.4: Architektura układu zamka

- Komunikacja bezprzewodowa z serwerem autoryzacji,
- Komunikacja z pozostałymi komponentami podsystemu sterowania zamkiem (czujnik ruchu, czytnik RFID),
- Kontrola przepływu sterowania,
- Kontrola stanu zasilania komponentów podsystemu.

Komponent sterujący zamkiem składa się z mikrokontrolera, czujnika ruchu oraz czytnika RFID. Mikrokontroler odpowiada za sterowanie peryferiami, zarządza ich zasilaniem, inicjuje i przeprowadza bezprzewodową komunikację z serwerem i steruje samym zamkiem na podstawie otrzymanych od serwera danych. Podsystem sterowania zamkiem zlokalizowany jest w całości w tym komponencie (patrz rysunek 3.3). Architektura układu zamka została przedstawiona na rysunku 3.4.

3.2.2 Serwer

W ramach komponentu serwera działają dwa podsystemy funkcjonalne: podsystem autoryzacji, odpowiedzialny za podjęcie decyzji o przyznaniu lub odmowie dostępu na podstawie danych odebranych od podsystemu sterowania zamkiem, oraz podsystem zarządzania, odpowiedzialny za umożliwienie wygodnej konfiguracji systemu, oraz zbieranie i prezentację danych. Oba te systemy korzystają ze wspólnej bazy danych.

Podsystem autoryzacji

Zadaniem podsystemu autoryzacji jest podjęcie decyzji o przyznaniu bądź odmowie dostępu na podstawie otrzymanych danych. Podsystem komunikuje się z bazą danych w celu uzyskania informacji na temat autoryzowanych kart.

Założono realizację następujących funkcjonalności w ramach podsystemu autoryzacji:

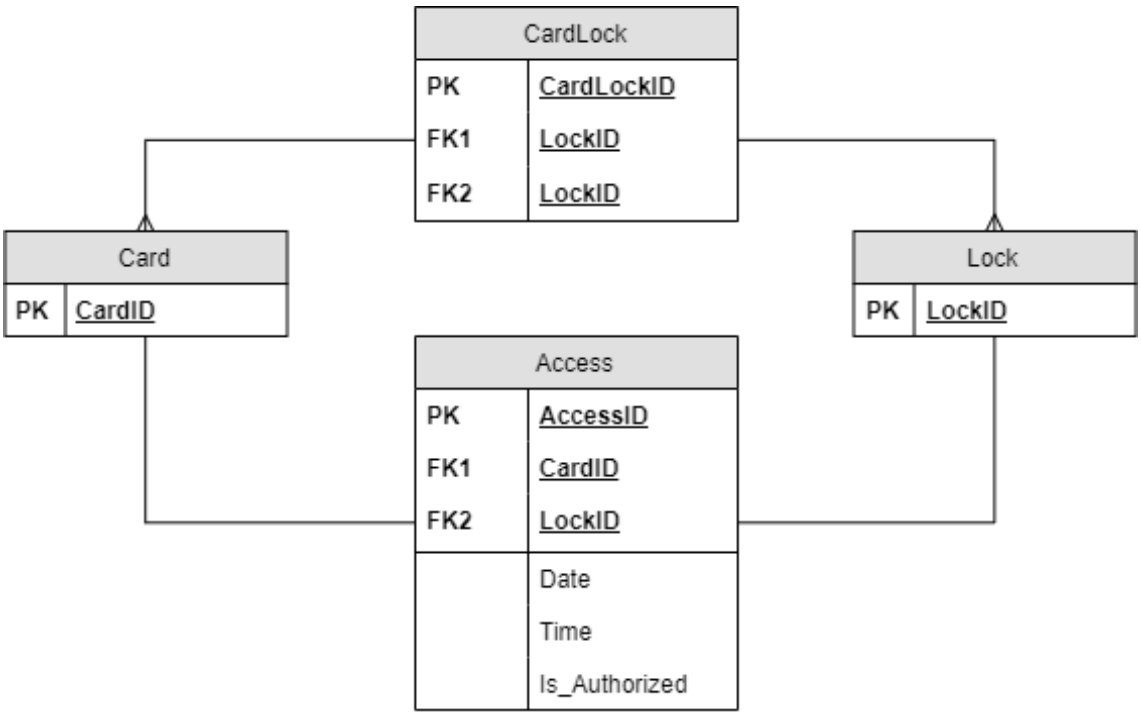
- Autoryzowanie kart w zamkach na podstawie otrzymanych od podsystemu sterowania zamkiem danych oraz zawartości bazy danych,
- Aktualizacja zawartości bazy danych o dokonane próby dostępu,
- Komunikacja z podsystemem sterowania zamkiem.

Podsystem zarządzania

Zadaniem podsystemu zarządzania jest umożliwienie użytkownikowi systemu wglądu do danych takich jak historia prób dostępu, zbiór zamków, kart oraz powiązań między nimi, oraz stan poszczególnych zamków. Dzięki niemu możliwa jest konfiguracja rozpoznawanych przez system kart, zamków oraz manualne przyznawanie dostępu poszczególnym identyfikatorom.

Podsystem zarządzania umożliwia następujące operacje:

- Dodanie zamka,
- Usunięcie zamka,
- Dodanie karty wraz z przyznaniem jej dostępu do istniejącego zamka (lub też większej ich liczby),
- Usunięcie karty,
- Zablokowanie dostępu dla karty (bez usuwania jej z systemu),
- Przegląd archiwalnych prób dostępu,
- Podgląd parametrów zamka (stan baterii). **???**



Rysunek 3.5: Schemat bazy danych

Baza danych

Częścią komponentu serwera jest baza danych. Nie jest jednak konieczne, aby pozostawała ona fizycznie na tej samej maszynie. W przypadku całkowitego rozdzielenia serwera danych od serwera autoryzacji skalowalność systemu znacząco wzrośnie.

Baza danych przechowuje dane dotyczące poszczególnych kart i zamków zarejestrowanych w systemie, autoryzacji kart w zamkach oraz dokonanych w przeszłości prób dostępu, zarówno zakończonych sukcesem jak i porażką.

Schemat bazy danych przedstawiony został na rysunku 3.5

Rozdział 4

Implementacja

Niniejszy rozdział zagłębia się w szczegóły implementacyjne projektu. Opisuje sposób konfiguracji środowiska deweloperskiego, przedstawia wybrane zagadnienia związane z implementacją oraz wykorzystane w projekcie technologie sprzętowe i programowe.

4.1 Konfiguracja środowiska

TBD

4.2 Podsystem sterowania zamkiem

Spełnienie założeń dotyczących systemu wymienionych w rozdziale 3 wymaga zastosowania mikrokontrolera integrującego układ komunikacji bezprzewodowej zgodnej ze zbiorem standardów IEEE 802.11, obsługującego interfejs szeregowej komunikacji z peryferiami (SPI) jednocześnie umożliwiając komunikację za pośrednictwem programowalnych wejść/wyjść (GPIO). Pośród wielu rozwiązań dostępnych na rynku, wybrany został mikrokontroler ESP3 ze względu na możliwość równoległego przetwarzania za pomocą dwóch fizycznych rdzeni, sprzętowe wsparcie dla algorytmów kryptograficznych oraz możliwość zaawansowanej kontroli pracy podzespołów mikrokontrolera, szczególnie w zakresie zasilania.

Kryterium wyboru czytnika kart RFID była obsługa kart o częstotliwości nośnej 13,56 MHz, dostępność oprogramowania sterującego czytnikiem dla wybranego mikrokontrolera oraz obsługa interfejsu komunikacji szeregowej SPI w celu prostej integracji czytnika z mikrokontrolerem. Do tego zadania wybrany został układ MFRC522.

Efektywne wykorzystanie energii w układzie zamka wymaga źródła impulsu wybudzającego o jak najniższym poborze mocy w stanie spoczynku. Wybranym rozwiązaniem jest czujnik PIR (ang. *Passive Infra Red*, pasywny czujnik podczerwieni), model HC-SR501.

4.2.1 Oprogramowanie

Kod podzielony jest na komponenty o zadanych funkcjonalnościach:

1. Komponent główny (*main*): odpowiedzialny za rozróżnienie rodzajów uruchomienia (pierwsze uruchomienie lub wybudzenie z uśpienia), wywołanie odpowiedniej procedury komponentu flow-controller oraz uśpienie układu po jej zakończeniu.
2. Komponent RFID: odpowiedzialny za inicjalizację czytnika MFRC522, wykrywanie i odczyt karty oraz sygnalizację zdarzeń związanych z odczytem kluczy dostępu do pomieszczeń.
3. Komponent WiFi: odpowiedzialny za realizację komumnikacji bezprzewodowej z serwerem. Obsługuje transmisje wychodzące i przychodzące wraz z opcjonalnym zestawieniem bezpiecznego kanału komunikacji z wykorzystaniem protokołu TLS.
4. Komponent sterujący (*flow-controller*): odpowiedzialny za kontrolę przepływu sterowania, aktywowanie poszczególnych komponentów **i co dalej?**.

cos o logach

4.2.2 Przeplyw sterowania

Przy pierwszym uruchomienu zamka, które następuje automatycznie po podłączeniu zasilania do układu, wykonywana jest procedura przejścia w stan głębokiego uśpienia (Deep-sleep mode) **przejście w tryb konfiguracji?**. W tym celu jako sposób wybudzenia konfigurowany jest tryb EXT0 (External Wakeup 0). Tryb ten wymusza aby po przejściu w stan uśpienia podtrzymane zostało zasilanie peryferiów RTC (ang. *Real-Time Clock*, zegar czasu rzeczywistego) [4], co z kolei pozwala na konfigurację źródła wybudzającego przerwania zewnętrznego jako wybranego wejścia RTC GPIO (ang. *General-Purpose Input/Output*, Wejście-wyjście ogólnego przeznaczenia). W projekcie w tym celu wykorzystany został pin nr 26. Ze względu na charakterystykę wykorzystanego źródła przerwania (pasywny czujnik zbliżeniowy), konieczne było zastosowanie trybu pull-down dla wspomnianego wyżej wejścia aby zapobiec występowaniu na nim stanu nieokreślonego. Po konfiguracji źródła przerwania układ zostaje wprowadzony w stan uśpienia.

Pierwsze uruchomienie

Przy pierwszym uruchomienu zamka, które następuje automatycznie po podłączeniu zasilania do układu, wykonywana jest procedura przejścia w stan głębokiego uśpienia (Deep-sleep mode) **przejście w tryb konfiguracji?**. W tym celu jako sposób wybudzenia konfigurowany jest tryb EXT0 (External Wakeup 0). Tryb ten wymusza aby po przejściu w stan uśpienia podtrzymane zostało zasilanie peryferiów RTC (ang. *Real-Time Clock*, zegar czasu rzeczywistego) [**?**], co z kolei pozwala na konfigurację źródła wybudzającego przerwania zewnętrznego jako wybranego wejścia RTC GPIO (ang. *General-Purpose Input/Output*, Wejście-wyjście ogólnego przeznaczenia).

W projekcie w tym celu wykorzystany został pin nr 26. Ze względu na charakterystykę wykorzystanego źródła przerwania (pasywny czujnik zbliżeniowy), konieczne było zastosowanie trybu pull-down dla wspomnianego wyżej wejścia aby zapobiec występowaniu na nim stanu nieokreślonego. Po konfiguracji źródła przerwania układ zostaje wprowadzony w stan uśpienia.

Wybudzenie z głębokiego uśpienia

Po wykryciu ruchu, czujnik PIR generuje stan wysoki na wejściu wybudzającym układu kontrolera co inicjalizuje procedurę wyjścia z głębokiego uśpienia. Po wybudzeniu następuje inicjalizacja systemu obsługi zdarzeń. Wszystie zdarzenia w oprogramowaniu zamka realizowane są przez grupę zdarzeń, mechanizm zapewniany przez system operacyjny czasu rzeczywistego FreeRTOS.

W celu realizacji komunikacji bezprzewodowej wykonywana jest procedura uruchomienia komponentu WiFi **konfiguracja WiFi pobierana z nvsflash**, co wiąże się z próbą połączenia z serwerem w wybranej sieci. Dane dostępu do sieci (SSID, hasło) jaki i adres serwera są osadzone w kodzie programu. W przypadku niepowodzenia kontroler zostaje uśpiony. **Tutaj dać pseudokod klienta wifi i uszczegółowić**

Listing 4.1: Pseudokod WiFi

```
def wifi_client_start():
    # WiFi Client should wait for connection to AP
    wait_event(WIFI_CONNECTED)

    while (TRUE):
        status = wifi_socket_connect()
        if (status != SUCCESS)
            break
        # Communication loop
        while (TRUE):
            # Wait for pending operation
            wait_event(WIFI_CLIENT_SEND_PENDING or WIFI_CLIENT_RECEIVE_PENDING)
            if (event_pending(WIFI_CLIENT_SEND_PENDING)):
                # Requested operation is SEND
                status = wifi_socket_send(data_to_send)
                if (status != SUCCESS):
                    # Notify transmission fail
                    notify_event(WIFI_CLIENT_TRANSMISSION_FAIL)
                    break
            else:
                # Requested operation is RECEIVE
                status, received_data = wifi_socket_receive_data()
                if (status != SUCCESS):
```

```
                # Notify transmission fail
                notify_event(WIFI_CLIENT_TRANSMISSION_FAIL)
                break
        # Notify transmission success
        notify_event(WIFI_CLIENT_TRANSMISSION_SUCCESS)
    wifi_socket_shutdown()
```

dodac tez pseudokod flow controllera Ze względu na restrykcyjne wymagania dotyczące czasu trwania procesu zestawiania połączenia z serwerem, system stosuje przetwarzanie współbieżne z wykorzystaniem dwóch głównych wątków.

4.3 Podsystem autoryzacji

4.4 Podsystem zarządzania

4.5 Wykorzystane technologie

4.5.1 ESP32

ESP32-DevKitC jest produkowaną przez firmę Espressif platformą deweloperską bazującą na module ESP32-WROOM-32D. Sercem modułu jest układ z rodziny ESP32 (ESP32-D0WD) wyposażony w CPU (ang. *Central Processing Unit*, centralna jednostka obliczeniowa) o dwóch rdzeniach, z których każdy może być kontrolowany niezależnie [5]. Moduł integruje Bluetooth, Bluetooth Low Energy oraz WiFi, a także szeroki zakres peryferiów: czujniki dotyku, czujniki pola magnetycznego, interfejs karty SD, Ethernet, SPI (ang. *Serial Peripheral Interface*), UART (ang. *Universal Asynchronous Receiver-Transmitter*), I^2S (ang. *Inter-IC Sound*) i I^2C (ang. *Inter-Integrated Circuit*) [5]. Dodatkowo umożliwia korzystanie z niskoenergetycznego koprocesora Ultra-Low-Power (ang. *ULP co-processor*), podczas gdy główne jednostki pozostają w trybie głębokiego uśpienia [6].

ESP32 oferuje efektywną i elastyczną technologię zarządzania energią. Dokument *ESP32 Series Datasheet* wymienia pięć predefiniowanychstanów energetycznych [7]:

1. Active mode: Aktywne CPU wraz z układem radiowym, możliwa bezprzewodowa transmisja.
2. Modem-sleep mode: Aktywne CPU z konfigurowalnym zegarem. Chip radiowy w tym trybie pozostaje wyłączony.
3. Light-sleep mode: Uśpione CPU. Pamięć i peryferia RTC wraz z koprocesorem ULP pozostają aktywne. Jakiekolwiek zdarzenia wybudzające (MAC, host, timer RTC i zewnętrzne przerwania) doprowadzą do wybudzenia układu.

4. Deep-sleep mode: Tylko pamięć RTC i peryferia RTC pozostają zasilone. Dane dotyczące połączeń WiFi i Bluetooth zostają przechowane w pamięci RTC. Opcjonalnie dostępny jest koprocesor ULP.

5. Hibernation mode: Wewnętrzny rezonator kwarcowy o częstotliwośći 8 MHz wraz z koprocesorem ULP zostają wyłączone. Również pamięć RTC jest wyłączona. Wybodzenie możliwe jest tylko poprzez timer RTC lub predefiniowane wejścia RTC GPIO.

4.5.2 ESP-IDF

TBD

4.5.3 Czytnik MFRC522

Do realizacji komunikacji w standardzie RFID High Frequency (13,56 MHz) wykorzystany został zintegrowany odbiornik/nadajnik MFRC522 produkowany przez firmę NXP Semiconductors, umożliwiający bezprzewodową komunikację z kartami zgodnymi ze standardem ISO/IEC 14443 A/MIFARE. Układ wspiera komunikację poprzez interfejsy SPI, UART oraz I^2C [8].

4.5.4 Czujnik zbliżeniowy

TBD

4.6 Problemy

Konfiguracja WiFi? Sygnalizacja stanu baterii? Bezpieczeństwo komunikacji zarządzanie stanami energetycznymi Enkrypcja flash mozna cos z technical reference manual

4.6.1 Zarządzanie energią

Szacunki długości życia na baterii - TBD Pomiary poboru mocy w różnych fazach działania - TBD

4.7 Możliwe rozszerzenia

W ramach niniejszej pracy stworzony został prototyp rozwiązania. Niektóre planowane funkcjonalności nie zostały zaimplementowane ze względu na ograniczenia czasowe i budżetowe. Pozostawiono jednak możliwość rozbudowy systemu. Poniżej przedstawiono kilka problemów, których system w obecnym stanie nie adresuje, wraz z możliwymi rozwiązaniami.

4.7.1 Mechanizm wyjścia

Opisywane rozwiązanie nie obejmuje implementacji mechanizmu opuszczenia strefy chronionej systemem kontroli dostępu. W zależności od potrzeb końcowego użytkownika, możliwe rozwiązanie to montaż dodatkowego czytnika po przeciwnej stronie drzwi i połączenie go z kontrolerem wejścia w przypadku gdy wymagana jest obustronna kontrola dostępu bądź zastosowanie przycisku którego naciśnięcie powoduje zwolnienie zamka w przypadku gdy wymagana jest tylko kontrola wejścia do chronionego obszaru.

4.7.2 Obsługa większej liczby zamków

W celu umożliwienia obsługi przez system liczby zamków przekraczającej 1, wystarczająca byłaby modyfikacja podsystemu autoryzacji w taki sposób, aby mógł on obsługiwać równoległe żądania od klientów.

4.7.3 Wygodna konfiguracja parametrów sieci

W obecnej implementacji dane dostępu do sieci (nazwa sieci oraz hasło) zostały zagnieżdżone w oprogramowaniu konrolera. Zmniejsza to elastyczność konfiguracji urządzenia, wymagając jego przeprogramowania za każdym razem gdy zmianie ulegnie nazwa lub klucz dostępu do sieci.

Możliwym rozwiązaniem tego problemu byłaby implementacja trybu konfiguracji. Tryb ten powodowałby przejście kontrolera w tryb Access Point przy zachowaniu dwóch warunków: (1) nastąpiło uruchomienie, a nie wybudzenie z trybu głębokiego uśpienia, oraz (2) na określonym wejściu pojawiło się napięcie. Przejście kontrolera w tryb Access Point umożliwiłoby udostępnienie prostego interfejsu webowego, za pomocą którego administrator systemu mógłby wprowadzić niezbędne do działania dane, takie jak nazwa sieci, hasło, a także adres IP i numer portu serwera autoryzacji. Aby zachować wysoki poziom bezpieczeństwa, komunikacja pomiędzy urządzeniem administratora i kontrolerem powinna odbywać się przy wykorzystaniu protokołu TLS.

4.7.4 Sygnalizacja stanu baterii

W obecnym stanie system nie implementuje mechanizmów informowania serwera o swoim stanie energetycznym. Sygnalizacja stanu baterii umożliwiłaby administratorowi systemu bieżące monitorowanie wszystkich zamków objętych systemem oraz szybką reakcję w przypadku, gdy baterie wymagałyby wymiany. Modyfikacja ta wymagałaby uzyskania dostępu do danych na temat naładowania baterii przez mikrokontroler oraz przesyłania ich okresowo do serwera, najlepiej w momentach, gdy jest on już wybudzony z powodu wykrycia ruchu w jego otoczeniu. **TBD**

4.7.5 Obsługa kont użytkowników w podsystemie zarządzania

TBD

Rozdział 5

Rezultaty

Niniejszy rozdział dokonuje podsumowania rezultatów prowadzonej pracy. Porównuje szacunki dotyczące poboru mocy z rzeczywistym poborem. Ponadto dokonuje oceny bezpieczeństwa oraz responsywności systemu.

TBD

Rozdział 6

Wnioski

Bibliografia

[1] Polski Komitet Normalizacyjny, *Technika informatyczna. Zabezpieczenia w systemach informatycznych. Terminologia*, Marzec 2002.

[2] British Security Industry Association, *A specifier's guide to access control systems*, Kwiecień 2016.

[3] Roger sp. z o.o. sp. k., *Przewodnik po systemie RACS 5.* v5.3 (dostęp 20.10.1019).

[4] Espressif Systems, *ESP32 Api Reference, Sleep Modes*, 2019. (rewizja a45e9985).

[5] Espressif Systems, *ESP32-WROOM-32D & ESP32-WROOM-32U Datasheet*, 2018. Version 1.7.

[6] Espressif Systems, *ESP32 Technical Reference Manual*, 2018. Version 4.0.

[7] Espressif Systems, *ESP32 Series Datasheet*, 2019. Version 3.2.

[8] NXP Semiconductors, *MDRC522 Product Datasheet*, 2016. Version 3.9.