

**POLITECHNIKA BYDGOSKA**

im. Jana i Jędrzeja Śniadeckich

**WYDZIAŁ TELEKOMUNIKACJI, INFORMATYKI  
I ELEKTROTECHNIKI**



**PRACA DYPLOMOWA INŻYNIERSKA**

**na kierunku Teleinformatyka**

**System kontroli dostępu z rejestrem zdarzeń**

Pracę wykonała:

Anna Bagniewska

Nr albumu:

114881

Kierujący pracą:

dr inż. Mirosław Miciak

Bydgoszcz, styczeń 2023



Politechnika Bydgoska  
im. Jana i Jędrzeja Śniadeckich  
Wydział Telekomunikacji, Informatyki i Elektrotechniki

Załącznik nr 1  
do Regulaminu dyplomowania 2021

## KARTA PRACY DYPLOMOWEJ

**Kierunek:** Teleinformatyka

**Forma studiów:** stacjonarne / niestacjonarne

### PRACA INŻYNIERSKA / MAGISTERSKA

NR 21/In/SP/2022/2023

**Student:** Anna Bagniewska

**Nr albumu:** 114881

**Temat pracy** (w języku polskim):

System kontroli dostępu z rejestrem zdarzeń

**Temat pracy** (w języku angielskim):

Access control system with event log

**Słowa kluczowe** (w języku polskim):

System kontroli dostępu, rejestr zdarzeń, programowanie

**Słowa kluczowe** (w języku angielskim):

Access control system, event log, programming


#### Zadania szczegółowe:

Celem pracy jest stworzenie automatycznego systemu kontroli dostępu do pomieszczenia lub schowka. System będzie zapisywał zarówno autoryzowany, jak i nieautoryzowany dostęp oraz umożliwiał podgląd tego zestawienia. Zadania: 1. Przegląd koncepcji działania systemów kontroli dostępu. 2. Określenie funkcji wykonywanych przez opracowywany system. 3. Wybór elementów realizacji sprzętowej systemu. 4. Projekt bazy danych. 5. Projekt systemu realizującego określone funkcje. 6. Implementacja systemu. 7. Testy i optymalizacja systemu. 8. Sprawdzenie możliwości wdrożenia systemu w życiu codziennym.

#### Miejsca przeprowadzenia prac:

- Zakład Podstaw Elektroniki

**Kierujący pracą:** dr inż. Mirosław Miciak

  
(Podpis)

**Podpis studenta:** Anna Bagniewska

**Recenzent/Recenzenci** (imię i nazwisko):

PRODZIEKAN  
ds. kształcenia i spraw studenckich  
dr inż. Mirosław Brutek

## Streszczenie

Niniejsza praca przedstawia opis procesu projektowania, implementacji i testowania systemu kontroli dostępu z rejestrem zdarzeń. Oprogramowanie odpowiedzialne za obsługę poszczególnych elementów systemu zostało stworzone w środowisku Thonny z wykorzystaniem języka MicroPython. Główne elementy zaprojektowanego systemu są kontrolowane przez mikrokontroler Raspberry Pi RP2040 oparty na ARM Cortex M0+. Ponadto do stworzenia części dotyczącej obsługi rejestru zdarzeń zostały wykorzystane zewnętrzne programy HiveMQ oraz IFTTT.

System został zaprojektowany tak, aby móc obsługiwać jedno pomieszczenie, jednakże jego poszczególne funkcje są przygotowane pod rozbudowę w przyszłości.

**Słowa kluczowe:** system kontroli dostępu, rejestr zdarzeń, oprogramowanie

## Summary

The present thesis contains a description of planning, implementing and testing processes of an access control system with event log. Software responsible for service of elements contained in system is created in Thonny environment with use of MicroPython programming language. Main elements of designed system are controlled by microcontroller Raspberry Pi RP2040 based on ARM Cortex M0+. Furthermore, to create a part related to a service of event log is used external programs HiveMQ and IFTTT.

The system was designed to be able to service one room, however its individual functions are prepared for extension in the future.

**Keywords:** access control system, event log, software

## Spis treści

1.	Wprowadzenie .....	7
1.1.	Wstęp.....	7
1.2.	Cel pracy .....	7
1.3.	Zakres pracy .....	7
2.	Systemy kontroli dostępu.....	9
2.1.	Charakterystyka systemów kontroli dostępu.....	9
2.2.	Wymagania stawiane systemom kontroli dostępu .....	9
3.	Projekt systemu kontroli dostępu.....	12
3.1.	Założenia projektu.....	12
3.2.	Przykładowe realizacje.....	13
3.3.	Opis tworzonego systemu .....	13
3.4.	Opis wykorzystanego oprogramowania .....	14
3.5.	Opis wybranych elementów, ich porównanie i uzasadnienie wyboru .....	15
3.5.1.	Moduł mikrokontrolera .....	15
3.5.2.	Moduł WiFi ESP8266EX .....	17
3.5.3.	Moduł RFID MFRC522.....	19
3.5.4.	Moduł zegara czasu rzeczywistego QYF-919 DS3231 .....	20
3.5.5.	Przełącznik jednokanałowy JQC-3FF-S-Z .....	21
3.5.6.	Elektrozamek .....	21
3.5.7.	Czujnik magnetyczny CMD 1423 .....	22
3.5.8.	Zasilacze .....	22
3.5.9.	Diody elektroluminescencyjne.....	23
3.5.10.	Buzzer.....	24
3.5.11.	Przyciski .....	24
3.6.	Budowa systemu kontroli dostępu .....	25

4.	Opis oprogramowania .....	28
4.1.	Algorytm .....	28
4.2.	Opis działania systemu .....	30
4.2.1.	Opis obsługi elektrozamka .....	31
4.2.2.	Opis funkcji odczytu czasu z modułu zegara czasu rzeczywistego .....	31
4.2.3.	Opis funkcji obsługi identyfikacji radiowej .....	32
4.2.4.	Opis realizacji obsługi przerwań .....	33
4.2.5.	Opis sposobu połączenia z siecią WLAN .....	34
4.2.6.	Opis realizacji rejestru zdarzeń .....	34
5.	Opis wykonanych testów działania systemu .....	40
5.1.	Test wykrycia otwarcia drzwi .....	40
5.2.	Test reakcji czytnika RFID .....	40
5.3.	Test zaniku zasilania .....	41
5.4.	Wykonanie dwóch czynności w tym samym czasie .....	42
6.	Możliwość rozbudowy systemu .....	44
7.	Wnioski i spostrzeżenia .....	45
8.	Literatura .....	47
9.	Spis rysunków .....	50
10.	Spis tabel .....	51
11.	Spis załączników .....	52

# **1. Wprowadzenie**

Pierwszy rozdział niniejszej pracy dyplomowej zawiera wprowadzenie do tematu bezpieczeństwa i ochrony. Zawiera również opis wybranego zagadnienia i wprowadzenie do sposobu jego realizacji. Scharakteryzowano także zakres działań, które powinny zostać podjęte w celu pomyślnego ukończenia projektu.

## **1.1. Wstęp**

Jedną z podstawowych potrzeb, która towarzyszy człowiekowi od zawsze jest bezpieczeństwo. Znajduje się ono na drugim miejscu w piramidzie Maslowa. Opiera się ona na hipotezie, że działania człowieka prowadzą w kierunku zapewnienia spełnienia potrzeb. Tworzą one wspomnianą już wcześniej piramidę, w której skład oprócz bezpieczeństwa wchodzi: obszary fizjologiczne, społeczne, szacunku oraz samorealizacji. W celu zaspokojenia kolejnych poziomów potrzeb, według Maslowa należy zacząć od najniższych i najszerzych warstw, aby ostatecznie móc zająć się samorealizacją [1]. W związku z powyższym, na przestrzeni lat udoskonalano sposoby zabezpieczenia osób i mienia, poczynając od ogrodzenia i wprowadzania coraz bardziej udoskonalonych zasuw i zamków do drzwi, aż po szyfrowanie i zabezpieczanie plików danych hasłem. Szczególnym przypadkiem zabezpieczeń jest ogólnie zdefiniowany system kontroli dostępu. Łączy on wiele pojedynczych funkcjonalności i od poziomu bezpieczeństwa poszczególnych z nich, zależy bezpieczeństwo całego systemu. W swoim działaniu system kontroli dostępu zapewnia administratorom zarządzanie prawami dostępu. Mogą oni zdefiniować użytkownikom pełny, ograniczony lub całkowity brak dostępu do wybranych pomieszczeń, sekcji, bądź schowków dołączonych do systemu.

## **1.2. Cel pracy**

Celem pracy jest zaprojektowanie automatycznego systemu kontroli dostępu do pomieszczenia lub schowka. System ma zapisywać zarówno autoryzowany, jak i nieautoryzowany dostęp oraz umożliwiać podgląd tego zestawienia.

## **1.3. Zakres pracy**

Praca dyplomowa polega na przejrzaniu koncepcji działania systemów kontroli dostępu. Na tej podstawie należy określić funkcjonalność opracowywanego systemu. Następnym krokiem jest wybór elementów realizacji sprzętowej systemu i projekt spełnienia założonych funkcji. W dalszej części następuje budowa prototypu oraz

przeprowadzenie testów i optymalizacja systemu. Na koniec należy sprawdzić możliwości wdrożenia systemu w życiu codziennym.



## **2. Systemy kontroli dostępu**

W rozdziale drugim została przedstawiona ogólna charakterystyka systemów kontroli dostępu. Zawiera opis podstawowych funkcjonalności, elementów oraz wymagań stawianych omawianym systemom.

### **2.1. Charakterystyka systemów kontroli dostępu**

System kontroli dostępu to zbiór powiązanych ze sobą elementów elektronicznych i mechanicznych. Mają one za zadanie blokować wybranym użytkownikom lub ich grupom dostęp do wydzielonych stref systemu. Jako strefy należy rozumieć pomieszczenia, wybrane piętra albo przestrzenie do przechowywania dokumentów. Ograniczanie dostępu może być też nałożone na określony czas lub całkowicie. Poszczególne części systemu są oddzielane różnego rodzaju zaporami. W zależności od specyfiki każdej strefy można wyróżnić: dla ruchu pojazdów szlabany i bramy, natomiast dla ruchu osób drzwi z zabezpieczeniem na przykład w formie zamka elektronicznego.

W celu identyfikacji użytkowników system musi być wyposażony w minimum jeden rodzaj urządzeń identyfikujących. Takim urządzeniem może być kamera, czytnik biometryczny, czytnik kart zbliżeniowych albo czytnik z klawiaturą. Za pomocą takiego urządzenia uzyskuje się od użytkownika pewien rodzaj klucza, który następnie zostaje odszukany w bazie danych. Na jej podstawie zostaje podjęta decyzja, czy dany użytkownik ma nadane uprawnienie do korzystania z wybranej strefy systemu.

W skład systemów kontroli dostępu mogą wchodzić także inne elementy, które zwiększają bezpieczeństwo. Są to części odpowiedzialne za detekcję ruchu oraz przerw w strukturze systemu i potencjalnych uszkodzeń. Do elementów dodatkowych należy też zaliczyć urządzenia żądania wyjścia, które umożliwiają opuszczenie chronionego pomieszczenia.

Bardziej zaawansowane systemy kontroli dostępu są wyposażone w moduły, za pomocą których można łączyć ze sobą kilka systemów, np. połączenie systemu antywłamaniowego i systemu przeciwpożarowego [9].

### **2.2. Wymagania stawiane systemom kontroli dostępu**

Od jakości systemu kontroli dostępu zależy bezpieczeństwo chronionej własności, niezależnie czy w formie materialnej, czy intelektualnej. Z tego powodu, systemom stawiane są konkretne i wymagające żądania.

Oprócz zabezpieczenia w formie elektronicznego potwierdzania tożsamości użytkowników należy zapewnić solidne wykonanie elementów pobocznych takich, jak wytrzymałe blokady przejść. Wykorzystywane zamki powinny być montowane po wewnętrznych stronach wydzielonych stref, a sposób zasilania blokad powinien być odporny na manipulacje. Montowane w systemie zamki i blokady posiadają bardzo często mechaniczne klucze, które wykorzystuje się w sytuacjach awaryjnych. Niestety obniża to trwałość całego zabezpieczenia, gdyż takie zamki są podatne na uderzenia [2]. Zagrożeniem objęte są też nośniki wykorzystywane do autoryzacji. Popularną wśród przestępców praktyką jest kopiowanie danych z używanych przez pracowników kart i późniejsze wykorzystywanie ich do podawania się za osobę uprawnioną do korzystania z zasobów chronionych przez system. W celu przeciwdziałania takiemu zagrożeniu zalecane jest składanie zamówień na nośniki z unikalnymi i losowymi numerami seryjnymi [10].

W systemach kontroli dostępu obserwuje się alarmy monitorowania wymuszonych otwarć przejść. Zgłaszają one moment otworzenia zamka bez uprzedniej identyfikacji użytkownika. Kolejnym elementem obecnym w wielu rozwiązaniach, jest funkcja informująca administratora bądź ochronę obiektu o przekroczeniu ustalonego wcześniej czasu, przez który mogą być otwarte poszczególne przejścia.

Bardzo ważnym aspektem w działaniu systemu kontroli dostępu jest też jego zachowanie w przypadku wystąpienia braku zasilania. Nie jest ważna przyczyna wystąpienia tej awarii – niezależnie, czy jest to chwilowy brak energii elektrycznej, czy długotrwały zanik spowodowany kataklizmem, system nie może przestać chronić zasobów. W związku z tym, projektując system kontroli dostępu, należy wziąć pod uwagę bezpieczne opuszczenie pomieszczeń przez personel, jednocześnie uwzględniając możliwość zamknięcia i obserwacji stref systemu.

Poza godzinami pracy zabezpieczanego obiektu można wdrażać inną politykę dostępu, na przykład można zarządzić ogłoszenie alarmu w przypadku wykrycia każdego ruchu w środku lub w pobliżu budynku.

Nie należy także zapominać o czynniku ludzkim, który również wpływa na bezpieczeństwo całego systemu. Użytkownicy, którzy mają przemieszczać się po zastrzeżonych strefach, powinni zostać przeszkoleni z dziedziny świadomości bezpieczeństwa. Powinno to zmniejszyć ryzyko występowania takich zachowań jak otwieranie drzwi do stref zamkniętych osobom nieuprawnionym przez osoby uprawnione [3]. W tym celu w trakcie przygotowywania systemu kontroli dostępu do uruchomienia

należy przygotować listy uprawnionych do korzystania z określonych stref. Zaleca się, aby kierować się zasadą najmniejszego uprzywilejowania, która wymaga, by na wybranym poziomie systemu, użytkownik miał dostęp tylko do danych i zasobów niezbędnych do realizacji przypisanych mu funkcji, czy zadań.

Uwzględniając powyższe czynniki, można dojść do wniosku, że w zależności od potencjalnych użytkowników oraz struktury zabezpieczanego budynku, wymagania stawiane konkretnym systemom kontroli dostępu będą się bardziej lub mniej różnić.

### **3. Projekt systemu kontroli dostępu**

W rozdziale trzecim zostały zawarte założenia stawiane do realizacji projektu. W tej części zostały również przedstawione przykładowe realizacje systemów wraz ich charakterystyką. W głównej części rozdziału trzeciego zostały zawarte opisy tworzonego systemu kontroli dostępu i wykorzystanego oprogramowania. Przedstawiono także potrzebne do realizacji elementy i sposób, w jaki zostaną zaimplementowane.

#### **3.1. Założenia projektu**

W celu zaprojektowania automatycznego systemu kontroli dostępu do pomieszczenia lub schowka dokonano założeń, którymi są określone poniżej funkcjonalności i cechy:

- Identyfikacja osób uprawnionych odbywa się za pomocą czytnika i kart RFID,
- Próba dostępu przez osobę uprawnioną, jak i nieuprawnioną jest zapisywana w rejestrze zdarzeń oraz sygnalizowana wskaźnikiem świetlnym,
- Nieautoryzowane otwarcie drzwi zostaje zapisane w rejestrze zdarzeń oraz aktywowany zostaje alarm dźwiękowy i świetlny,
- Czas, przez który pozostają otwarte drzwi, jest mierzony i w przypadku przekroczenia określonej jego wartości, wysyłany zostaje dźwięk przypominający o ich zamknięciu,
- Drzwi odblokowywane są za pomocą elektrozamka, który zostajeysterowany po poprawnej identyfikacji osoby lub po naciśnięciu przycisku żądania wyjścia,
- W przypadku zaniku zasilania pomieszczenie pozostaje zamknięte,
- System wyposażony jest w zegar czasu rzeczywistego, ułatwia ustalenie momentu wystąpienia zdarzenia,
- Rejestr zdarzeń dostępny dla administratora po uprzednim zalogowaniu,
- Objęte systemem jest początkowo jedno pomieszczenie,
- System jest przygotowany pod przyszłą rozbudowę.

### **3.2. Przykładowe realizacje**

Jedną z podstawowych cech systemów kontroli dostępu jest ich bezpieczeństwo i niezawodność. Dla wielu użytkowników ważną informacją jest też cena, która niejednokrotnie przeważała nad wyborem danego rozwiązania. W sektorze zabezpieczeń dostępnych jest niezliczona ilość gotowych systemów kontroli dostępu. Przykładowy system obsługujący jedno przejście oraz bez dedykowanej aplikacji umożliwiającej podgląd zdarzeń na krajowym rynku został wyceniony na 596,99 zł [11]. Nie jest to jednak kompletne zabezpieczenie. Do pełnego obrazu brakuje jeszcze zamka, kart identyfikacyjnych, czujnika magnetycznego otwarcia drzwi oraz określenia sposobu opuszczania pomieszczenia. Do wybranego systemu można dołączyć rozszerzenia, ale tylko rekomendowane przez producenta nie spowodują utraty gwarancji na urządzenie. W tym przykładzie, bez kupna zewnętrznej centrali, nie można także samodzielnie dodawać kolejnych obsługiwanych drzwi oraz funkcjonalności takich, jak automatyczne włączanie oświetlenia lub innych urządzeń.

Tworzony projekt wyróżnia się swoją prostotą budowy oraz dostępem do tylko wybranych informacji przedstawianych w rejestrze zdarzeń. W odróżnieniu od rozwiązań komercyjnych proponowane rozwiązanie jest znacznie tańsze oraz dokładniej odwzorowuje oczekiwania przyszłych użytkowników.

### **3.3. Opis tworzonego systemu**

Tworzony system kontroli dostępu ma spełnić prywatne oczekiwania względem swojego działania i poziomu bezpieczeństwa. W przypadku rozwiązań dostępnych w sklepach najczęściej wykorzystywaną częstotliwością, którą rozpoznają czytniki, jest 125 kHz. Dla tworzonego rozwiązania będzie to częstotliwość z wyższego zakresu, mianowicie 13,56 MHz. Oprócz tego, gotowe systemy umożliwiają obsługę do 4000 kart identyfikacyjnych. Ich maksymalne wykorzystanie, również w przypadku nowego projektu, może znacząco wpłynąć na szybkość reakcji systemu.

System będzie oparty o mikrokontroler, który będzie jego głównym urządzeniem. W jego instrukcjach otrzymane dane będą przetwarzane oraz przekazywane dalej, to znaczy zostaną podjęte odpowiednie reakcje ze strony elementów systemu. Wspomnianymi elementami są czytniki kart RFID. Na nich spoczywa identyfikacja użytkowników. Na podstawie rozpoznania użytkownika lub nie, zostanie podjęta przez mikrokontroler decyzja o podjęciu akcji. W przypadku pozytywnego rozpatrzenia prośby o wejście zostanie

wysterowany przekaźnik, który z kolei obsłuży otwarcie elektrozamka. Czynnością wykonywaną z tej samej przyczyny jest włączenie diody sygnalizującej zgodę na wejście. Opisane zdarzenia składają się na jedną informację umieszczoną w rejestrze zdarzeń. Moment wyjścia z pomieszczenia jest zgłaszany przez użytkownika poprzez użycie tak zwanego przycisku żądania wyjścia. Możliwość opuszczenia pomieszczenia jest sygnalizowana kolejną diodą, znajdującą tym razem po wewnętrznej stronie drzwi. W przypadku nieuzyskania przez użytkownika autoryzacji schemat działania jest następujący: włączone zostają dioda oraz buzzer, które sygnalizują odmowę dostępu. Następnie do rejestru zostaje przesłany wpis o nieautoryzowanej próbie dostępu do pomieszczenia. Kolejnym przypadkiem jest otwarcie drzwi bez uzyskania autoryzacji. To zdarzenie zostanie zgłoszone przez funkcję czujnika drzwi. Nastąpi wtedy włączenie alarmu – buzzera i diody oraz zostanie przesłana do rejestru i zewnętrznej aplikacji informacja o prawdopodobnym naruszeniu bezpieczeństwa. Ostatnia kwestia, która jest ujęta w systemie, to zanik zasilania spowodowany różnymi czynnikami. Do układu został dobrany zamek, który w momencie braku podawania napięcia jest zamknięty. Ma to na celu ograniczenie nieznanymi prób wejść do pomieszczenia. W celu poznania godziny powrotu zasilania i ponownego uruchomienia systemu, do rejestru zostaje wysłana wiadomość powitalna, która tak jak każdy wpis oznakowana jest dokładną datą wystąpienia.

Wszystkie powyższe cechy opisują gotowy projekt systemu kontroli dostępu, który przygotowany został na potrzeby pracy dyplomowej.

### **3.4. Opis wykorzystanego oprogramowania**

System kontroli dostępu, który jest głównym tematem tego opracowania, zostanie przygotowany w środowisku programistycznym Thonny. Jest ono dedykowane do pracy z modułami mikrokontrolerów tworzonych przez Fundację Raspberry Pi. Najpopularniejszym językiem programowania, który jest obsługiwany przez popularne podzespoły, jest MicroPython. W uproszczeniu jest on implementacją języka programowania kompatybilną z Pythonem 3 i zoptymalizowaną do pracy na mikrokontrolerach. W tym języku zostanie zaprogramowana cała fizyczna część projektu. W tym celu zostaną wykorzystane główne biblioteki ułatwiające pracę z mikrokontrolerem.

Pozostała realizacja utworzonych i przechowywanych danych będzie odbywać się przy użyciu następujących narzędzi programistycznych: HiveMQ oraz IFTTT. Pierwszy z nich jest platformą umożliwiającą szybkie, niezawodne i wydajne przesyłanie wiadomości

(danych) do i z podłączonych do niego urządzeń Internetu Rzeczy oraz innych systemów. Drugie z narzędzi to IFTTT, które umożliwia zautomatyzowanie przekazywania informacji pomiędzy czynnikami wyzwalającymi akcję a programem lub aplikacją realizującą wybraną czynność końcową [12].

Wybór pomocnych i posiadających dużą społeczność twórców narzędzi jest ważny. W przypadku natrafienia na problem istnieje możliwość, że w większej społeczności ktoś już miał z nim do czynienia, rozwiązał go oraz podzielił się rozwiązaniem.

### **3.5. Opis wybranych elementów, ich porównanie i uzasadnienie wyboru**

#### **3.5.1. Moduł mikrokontrolera**

Głównym elementem wykorzystanym w systemie kontroli dostępu jest mikrokontroler. Na wstępnym etapie wyboru elementów, były rozważane dwa moduły mikrokontrolerów: Arduino Uno Rev 3 oraz Raspberry Pi Pico.

Pierwszy z wymienionych modułów jest jednym z najpopularniejszych i najprostszych produktów udostępnianych przez producenta. Arduino Uno Rev 3 jest wyposażony w mikrokontroler ATmega328 i czternaście cyfrowych wejść/wyjść. Sześć spośród nich może służyć jako wyjścia PWM, a kolejne sześć jako wejścia analogowe. Drugi poddany rozważaniom, tym razem niewielkich rozmiarów, moduł jest wyposażony w mikrokontroler RP2040 oraz dwadzieścia sześć wejść/wyjść. Głównym czynnikiem ujęcia ich w rozważaniach była ich cena i dostępność. Na niekorzyść przedstawionych modułów wpływał fakt, iż nie zostały one wyposażone w układ komunikacji bezprzewodowej. W związku z tym należało także rozpatrzyć dodatkowe moduły umożliwiające takową komunikację, które byłyby zgodne z głównym modułem mikrokontrolera.

Wybór modułu mikrokontrolera został ułatwiony 30 czerwca 2022 [13, 14], gdyż fundacja Raspberry Pi oddała do użytku nowy moduł spełniający oba wymagania w jednym elemencie. Mianowicie jest to Raspberry Pi Pico W, który spełnia wszystkie funkcje swojego poprzednika oraz ma możliwość komunikacji bezprzewodowej. Moduł, pomimo swojej dodatkowej cechy, pozostał w niższym przedziale cenowym.

Szczegółowe informacje na temat omawianych modułów zostały przedstawione w tabeli 1, w której zostały ze sobą zestawione wszystkie wspomniane wcześniej moduły mikrokontrolerów.

Tab. 1. Specyfikacja techniczna modułów mikrokontrolerów Raspberry Pi Pico, Raspberry Pi Pico W i Arduino Uno Rev 3 [15, 16, 17]

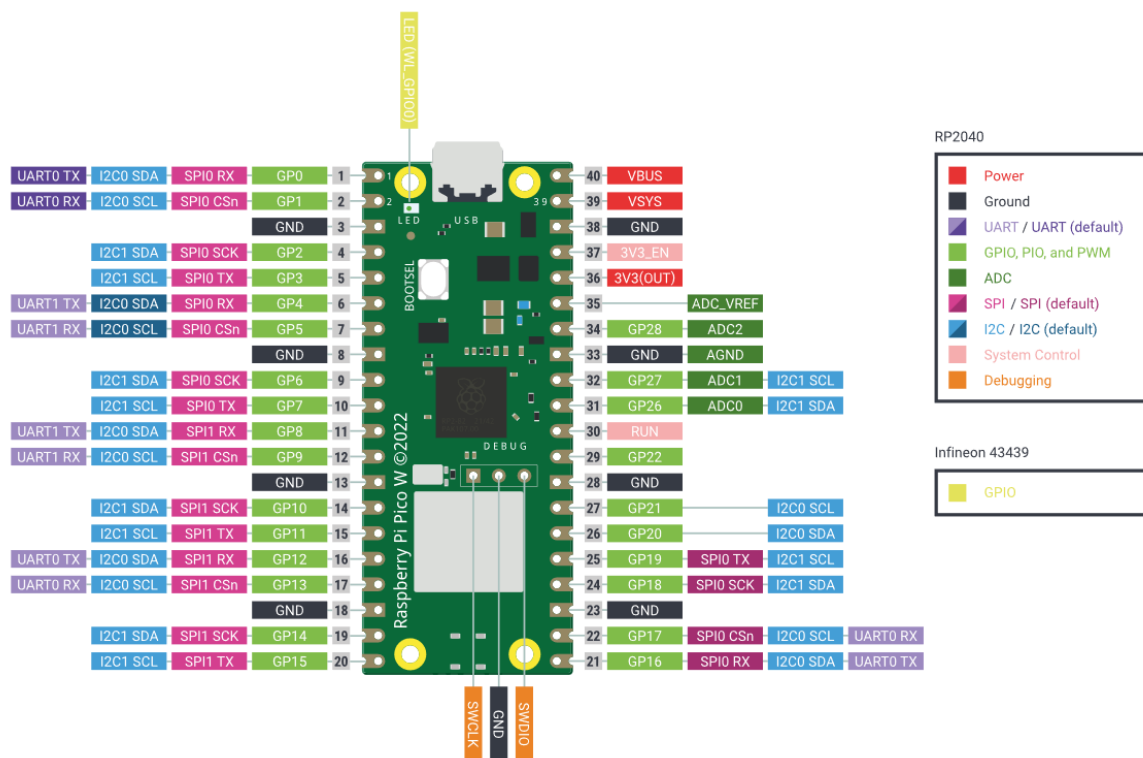
Moduł	Raspberry Pi Pico	Raspberry Pi Pico W	Arduino Uno Rev 3
Parametr	Wartość		
Pamięć Flash	2 MB	2 MB	32 kB
Pamięć SRAM	264 kB	264 kB	2 kB
Złącze	Micro USB – B	Micro USB – B	USB – B
Ilość GPIO	26	26	14
Wielofunkcyjne porty (ilość)	<ul style="list-style-type: none"> <li>• analogowe – 3</li> <li>• PWM – 16</li> </ul>	<ul style="list-style-type: none"> <li>• analogowe – 3</li> <li>• PWM – 16</li> </ul>	<ul style="list-style-type: none"> <li>• analogowe – 6</li> <li>• PWM – 6</li> </ul>
Napięcie portów GPIO	3,3 V	3,3 V	5 V
Napięcie VBUS	5 V +/- 10%	5 V +/- 10%	–
Przedział napięcia VSYS	od 1,8 V do 5,5 V	od 1,8 V do 5,5 V	–
Komunikacja	UART, I <sup>2</sup> C, SPI	UART, I <sup>2</sup> C, SPI	UART, I <sup>2</sup> C, SPI
Mikrokontroler	Raspberry RP2040	Raspberry RP2040	AVR ATmega328
Rdzenie procesora	2	2	1
Częstotliwość taktowania procesora	133 MHz	133 MHz	16 MHz
Przedział temperatury pracy	od -20 °C do 85 °C	od -20 °C do 70 °C	od -40 °C do 85 °C
Wbudowany moduł komunikacji bezprzewodowej	Nie	Tak	Nie
Zewnętrzne przerwania	Tak	Tak	Tak
Cena	26,50 zł	41,90 zł	119,00 zł

Podane w tabeli 1 wartości znacząco działają na korzyść Raspberry Pi Pico i Raspberry Pi Pico W. Jedyną ze znajdujących się w zestawieniu wartości, która miałaby zadecydować o wyborze modułu Arduino Uno Rev 3, jest ilość pinów analogowych. Nie jest jednak przewidziane ich wykorzystanie w tworzonym systemie, więc nie są decydującym parametrem. Do wszystkich wymienionych w tabeli pierwszej modułów dostępne są w ofercie rozszerzenia oraz moduły spełniające wiele funkcji potrzebnych w tworzonym systemie. Ostateczna decyzja jest poparta wygodą użytkowania modułu mikrokontrolera z wbudowaną komunikacją bezprzewodową, dzięki której nie zostaje wykorzystanych osiem dodatkowych pinów, którymi dołączony byłby moduł komunikacji bezprzewodowej.

Do zbudowania systemu wybrano moduł Raspberry Pi Pico W, który cechuje się dużą wszechstronnością, ilością portów wejść/wyjść oraz szybkością procesora. Ostatnia cecha jest ważna dla sprawnej obsługi systemów obsługujących wiele urządzeń



i dodatkowych modułów. Raspberry Pi Pico W zostało też wybrane ze względu na bezproblemową opcję podłączenia modułu zegara czasu rzeczywistego oraz modułu RFID.



Rys. 1. Wyprowadzenia Raspberry Pi Pico W [15]

Na rysunku 1 zostało przedstawione rozmieszczenie pinów modułu mikrokontrolera. W kolorowych prostokątach umieszczone są nazwy funkcji, które są dostępne na poszczególnych pinach. Taka wielozadaniowość wyprowadzeń ułatwia podłączanie urządzeń peryferyjnych do modułu mikrokontrolera, zapewniając jednocześnie przejrzystość połączeń.

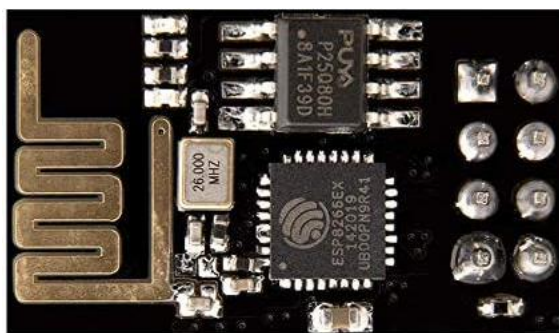
### 3.5.2. Moduł WiFi ESP8266EX

Wybrany moduł ESP8266EX pozwala na budowę urządzeń i systemów komunikujących się przez WiFi w standardach 802.11 b/g/n. Ta cecha sprawia, że nadaje się on do budowy tanich i energooszczędnych urządzeń. Moduły ESP mogą pełnić funkcje między innymi klientów lub małych serwerów WWW. Przekłada się to na szerokie zastosowanie tych elementów w projektach związanych z Internetem Rzeczy. W tabeli 2 została umieszczona najważniejsza z punktu widzenia systemu kontroli dostępu specyfikacja modułu.

Tab. 2. Specyfikacja ESP8266EX [18]

Parametr	Wartość
Standard komunikacji bezprzewodowej	IEEE 802.11 b/g/n (2,4 GHz)
Prędkość transmisji bezprzewodowej	do 72,2 Mb/s
Zabezpieczenia i szyfrowanie	WPA, WPA2, WEP, TKI, AES
Napięcie pracy	od 2,5 V do 3,6 V
Napięcie zasilania	od 4,8 V do 12 V
Antena	wbudowana lub złącze

Analizując wartość napięcia potrzebnego do zasilenia modułu, można zauważyć, że moduł jest przygotowany do pracy przy zasilaniu pochodzącym z modułu mikrokontrolera Arduino. W celu podłączenia tego modułu komunikacji bezprzewodowej do modułu Raspberry Pi Pico należałoby zadbać o odpowiednie zasilenie układu.



Rys. 2. Moduł WiFi ESP8266EX [18]

Przedstawiony na rysunku 2 element odpowiedzialny za komunikację bezprzewodową był pierwotnie rozważany, jednakże nie zostanie wykorzystany do budowy systemu kontroli dostępu, ponieważ jego funkcje realizuje wymienione wcześniej, w rozdziale 3.4.1 moduł Raspberry Pi Pico W z chipsetem CYW43439 odpowiedzialnym za komunikację bezprzewodową. W tabeli 3 znajdują się informacje uzupełniające przedstawienie modułu.

Tab. 3. Specyfikacja komunikacji bezprzewodowej modułu Raspberry Pi Pico W [19]

Parametr	Wartość
Standard komunikacji bezprzewodowej	802.11 b/g/n (2,4 GHz)
Prędkość transmisji bezprzewodowej	do 200 Mb/s
Zabezpieczenia i szyfrowanie	WPA Personal, WPA2 Personal, WPA3, WEP, AES, TKIP, CKIP
Antena	wbudowana

### 3.5.3. Moduł RFID MFRC522

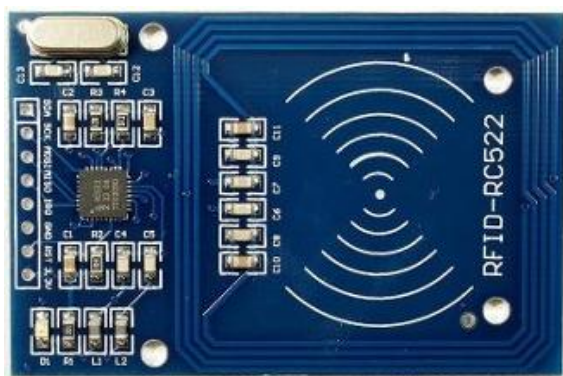
Podstawowym elementem identyfikacyjnym w systemie kontroli dostępu jest czytnik RFID. Służy on w tym przypadku do identyfikacji osoby posiadającej najczęściej kartę RFID, która jest fizyczną reprezentacją zaprogramowanego tagu. Wdrożenie takiego rozwiązania jest stosunkowo proste i nie jest ograniczone potrzebą stosowania dodatkowego zasilania dla wszystkich urządzeń w systemie – zasilania wymaga sam czytnik. Odczyt danych z nośnika następuje w momencie uruchomienia tak zwanego tagu. Energia potrzebna do tej czynności jest dostarczana przez wygenerowane przez antenę nadajnika pole. Część takich czytników jest też wyposażona w technologię NFC, jednak nie jest ona potrzebna w tworzonym systemie.

Brane pod uwagę moduły RFID, które można by wykorzystać w systemie kontroli dostępu, zostały scharakteryzowane w tabeli 4.

Tab. 4. Specyfikacja modułów RFID [20, 21, 22]

Moduł	RFID MF RC522	SparkFun SEN-15191
Parametr	Wartość	
Częstotliwość	13,56 MHz	125 kHz
Zasięg	do 10 cm	około 5 cm
Prędkość odczytu	do 10 Mb/s	do 4 kb/s
Zasilanie	3,3 V	3,3 V
Komunikacja	SPI	I <sup>2</sup> C

Z powyższego zestawienia można wyróżnić jeden parametr, który ma wpływ na działanie systemu, mianowicie prędkość odczytu danych przez czytnik. W przypadku, gdy z czytnika korzysta się sporadycznie, nie stwarza to różnicy. Na skalę masową, przy oznaczaniu produktów i ich późniejszym skanowaniu, jest to jednak znacząca wartość. W związku z tym, że z czytników zawartych w systemie kontroli dostępu pojedyncza osoba korzysta sporadycznie, na wybór jednego z przedstawionych elementów wpłynęła w tym przypadku tylko cena. W przypadku modułu RFID MF RC522 [20] jest prawie siedmiokrotnie niższa niż modułu SparkFun SEN-15191 [22]. Na rysunku 3 przedstawiono wygląd wybranego modułu identyfikacji radiowej.



Rys. 3. Moduł RFID MF RC522 [20]

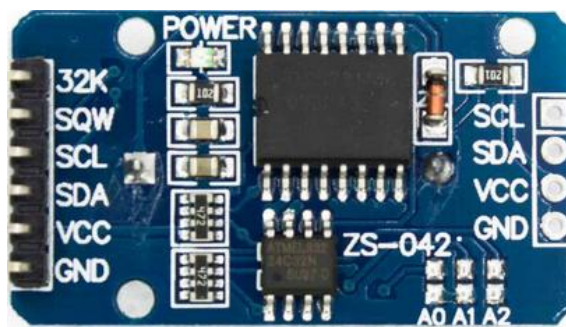
### 3.5.4. Moduł zegara czasu rzeczywistego QYF-919 DS3231

Moduł wybranego mikrokontrolera nie jest wyposażony w zegar czasu rzeczywistego. Na potrzeby zaprojektowania rejestru zdarzeń, wymagana jest możliwość pobierania aktualnej daty. Umożliwi ona chronologiczne ustalenie kolejności wydarzeń, które wystąpiły w trakcie działania systemu. Porównanie zostało wykonane na podstawie dostępnych specyfikacji technicznych dwóch modułów zegara czasu rzeczywistego.

Tab. 5. Specyfikacja wybranych modułów zegara czasu rzeczywistego [23, 24]

Moduł	DS3231	DS1302
Parametr	Wartość	
Napięcie zasilania	od 3,3 V do 5V	od 2 V do 5,5 V
Częstotliwość odświeżania	1 Hz	1 Hz
Wymagana bateria	CR2032	CR2032
Interfejs komunikacyjny	I <sup>2</sup> C	I <sup>2</sup> C

Na podstawie załączonej tabeli 5 można zauważyć, że oba moduły różnią się od siebie napięciem zasilania. W każdym z przedstawionych przypadków napięcie zasilania odpowiada wybranemu modułowi mikrokontrolera Raspberry Pi Pico W. Do stworzenia układu potrzebnego do realizacji projektu został wybrany moduł DS3231, ponieważ był już w posiadaniu autora. Opisywany moduł został przedstawiony na rysunku 4.



Rys. 4. moduł zegara czasu rzeczywistego QYF-919 DS3231 [23]

### 3.5.5. Przekaznik jednokanałowy JQC-3FF-S-Z

Sterowanie elementami nadzoru dołączonymi do systemu kontroli dostępu jest jednym z jego głównych zadań. Żeby było to możliwe, potrzebny jest przekaznik. W trakcie realizacji programu zostaje zmieniony stan wyjścia modułu mikrokontrolera, który z kolei ma za zadanie wysterować wyjście przekaznika, co przekłada się na sterowanie urządzeniem dołączonym do systemu kontroli dostępu. Jednym z dostępnych na rynku przekazników jest przekaznik jednokanałowy JQC-3FF-S-Z z cewką 5 V i stykami, które mogą obsłużyć maksymalny prąd 10 A oraz maksymalne napięcie 30 VDC/250 VAC [25].

Dołączając omawiany przekaznik do układu, należy mieć na uwadze fakt, że moduł mikrokontrolera może wystawić na porcie wyjściowym tylko napięcie o wartości 3,3 V. Aby zasilić cewkę przekaznika odpowiednią wartością napięcia, można dołączyć do obwodu tranzystor. Do tego celu wystarczający będzie tranzystor NPN BC547C [4, 5, 26, 27].

### 3.5.6. Elektrozamek

System kontroli dostępu nie może funkcjonować bez odpowiedniej blokady wejścia. Przykładem jest zamek elektromagnetyczny z cewką prądu stałego. Jego budowa opiera się na elektromagnesie działającym pod wpływem podania na jego uzwojenie napięcia o wartości 12 V. Dzięki takiemu podejściu, potencjalne pomieszczenie pozostaje zamknięte, nawet gdy nastąpi zanik zasilania. Całość jest umieszczona w metalowej obudowie z przygotowanymi do montażu otworami. Rygiel zamka jest ścięty pod kątem, co ułatwia zatraskiwanie drzwi, jednocześnie nie pozwalając na ich swobodne otwieranie w niepowołanym momencie. Wybrany elektroamek charakteryzuje też jednosekundowy czas odblokowania, prąd podtrzymania o wartości 900 mA oraz następujące wymiary obudowy:  $53 \times 38 \times 27$  mm, oraz długość rygla: 10 mm [28].

### 3.5.7. Czujnik magnetyczny CMD 1423

Gdy tematem przewodnim jest bezpieczeństwo, nie należy polegać tylko na jednym czynniku zabezpieczającym. Przewodowy czujnik zbliżeniowy załączany magnetycznie jest stosowany głównie do określania pozycji okien i drzwi. Jest to element, na podstawie którego można dowiedzieć się, czy uzyskano nieuprawniony dostęp do zamkniętych zasobów. Jednocześnie dostarcza informacji, czy przejście do danego pomieszczenia nie jest otwarte za długo, co również naraża ogólne pojęcie bezpieczeństwa obiektu.

Działanie tego czujnika magnetycznego jest następujące: obwód, w którym się znajduje, jest domyślnie rozarty. Po zbliżeniu elementów do siebie obwód zostaje zamknięty, co jest równoznaczne z tym, że zaczyna przez niego przepływać prąd. Podłączenie czujnika można zrealizować na dwa sposoby: poprzez zewnętrzny rezystor podciągający albo od strony kodowej uruchamiając wewnętrzny rezystor pull-up. Stan czujnika można sprawdzić w sposób cyfrowy przez moduł mikrokontrolera.

W poniższej tabeli 6 znajdują się szczegółowe informacje na temat opisywanego czujnika magnetycznego.

Tab. 6. Specyfikacja czujnika magnetycznego [29]

Parametr	Wartość
Napięcie pracy	do 50 V
Maksymalny prąd	0,1 A
Rezystancja wewnętrzna	200 $\Omega$
Zasięg	25 mm

### 3.5.8. Zasilacze

System kontroli dostępu w swoim działaniu polega na zasilaniu dostarczonym z zewnątrz. Aby jednak mógł działać poprawnie, należy zwrócić uwagę na maksymalne wartości prądu i napięcia, które mogą zostać do niego doprowadzone. Użyte w projekcie elementy wymagające zewnętrznego zasilania są następujące: moduł mikrokontrolera – 5 V, przekaźnik jednokanałowy – 5 V, elektrozamek – 12 V. Pozostałe elementy uzyskują wystarczające wartości zasilania prosto z modułu mikrokontrolera. W związku z tym, do zasilania tych elementów zostały wybrane następujące zasilacze:

- Stabilizowany zasilacz impulsowy sieciowy 5 V [30]:
  - Napięcie wejściowe: AC od 100 V do 240 V, od 50 Hz do 60 Hz,
  - Napięcie wyjściowe: DC 5 V,

- Prąd wyjściowy: do 2,5 A.
- Stabilizowany zasilacz impulsowy sieciowy 12 V [31]:
  - Napięcie wejściowe: AC od 200 V do 240 V, od 50 Hz do 60 Hz,
  - Napięcie wyjściowe: DC 12 V,
  - Prąd wyjściowy: do 1,25 A.

Oba opisywane zasilacze są przeznaczone do użytku wewnętrznego, co skutkuje ograniczeniem zastosowania systemu kontroli dostępu jedynie do wnętrza budynku.

### 3.5.9. Diody elektroluminescencyjne

Sygnalizowanie wybranego stanu urządzenia bardzo ułatwia jego obsługę. W związku z tym, w projekcie zostały ujęte znaczniki stanu, które będą informować użytkownika o stanie, w jakim znajduje się urządzenie. Głównym zadaniem tych diod ma być sygnalizowanie procesu weryfikacji użytkownika próbującego otworzyć drzwi. Dodatkowo mogą one informować o zdarzeniach alarmowych, czyli nieupoważnionym otwarciu drzwi lub zbyt długim czasie otwarcia drzwi.

Do projektu zostały wykorzystane dwa kolory diod oraz zostały dobrane do nich rezystory obniżające podawane na nie napięcie. Napięcie z portu modułu mikrokontrolera rozłoży się na rezystor i diodę, co obrazuje poniższy wzór:

$$U_V = U_R + U_O \quad (1)$$

gdzie:

$U_V$  - napięcie zasilania [V],

$U_R$  - napięcie odłożone na rezystorze [V],

$U_O$  - napięcie odłożone na odbiorniku [V].

Następnie należy przekształcić powyższy wzór do postaci:

$$U_R = U_V - U_O \quad (2)$$

Korzystając z danych dostarczanych przez producentów diod oraz modułu mikrokontrolera, można obliczyć już wartość potrzebnych w projekcie rezystorów. W tym celu należy skorzystać z przekształconego wzoru obrazującego prawo Ohma [32, 33]:

$$R = \frac{U_R}{I_O} \quad (3)$$

gdzie:

$R$  – rezystancja rezystora [ $\Omega$ ],

$U_R$  – napięcie odłożone na rezystorze [V],

$I_O$  – prąd przepływający przez odbiornik [A].

Dla wybranych diod wartości znamionowe napięcia i prądu przedstawiają się następująco: dioda czerwona – 2,1 V i 20 mA, dioda zielona – 2,4 V i 20 mA, dioda żółta – 2,0 V i 25 mA. Na podstawie wzorów (2) i (3) wyliczono następujące wartości rezystorów potrzebnych do obniżenia napięcia w podukładzie systemu: 60  $\Omega$ , 45  $\Omega$  oraz 52  $\Omega$ .

### 3.5.10. Buzzer

Jedną z nieobowiązkowych funkcjonalności systemu kontroli dostępu jest alarmowanie osób w otoczeniu o wystąpieniu zdarzenia, które zagraża bezpieczeństwu. Wybrany do projektu element wymaga napięcia zasilania od 3 V do 5 V oraz umożliwienia poboru prądu w wartości około 20 mA [34, 35]. Bazując na wyprowadzonych wcześniej wzorach (2) i (3), można obliczyć wartość rezystancji rezystora, który po dołączeniu do układu będzie zabezpieczał omawiany buzzer. Rezystancja potrzebna do tej części wynosi 15  $\Omega$ .

### 3.5.11. Przyciski

Ostatnim, jednak nie najmniej potrzebnym elementem systemu jest tak zwany przycisk żądania wyjścia. Ułatwia on użytkownikom przemieszczanie się na zewnątrz chronionej lub wydzielonej strefy. Jest dodatkowym elementem, który służy do zwalniania rygła zamka. Jego realizacja może zostać wykonana na kilka sposobów. Jednym z nich jest montaż przycisku, który po naciśnięciu wraca do swojego pierwotnego położenia po wewnętrznej stronie drzwi i dalsza realizacja tego podsystemu w części programowej.



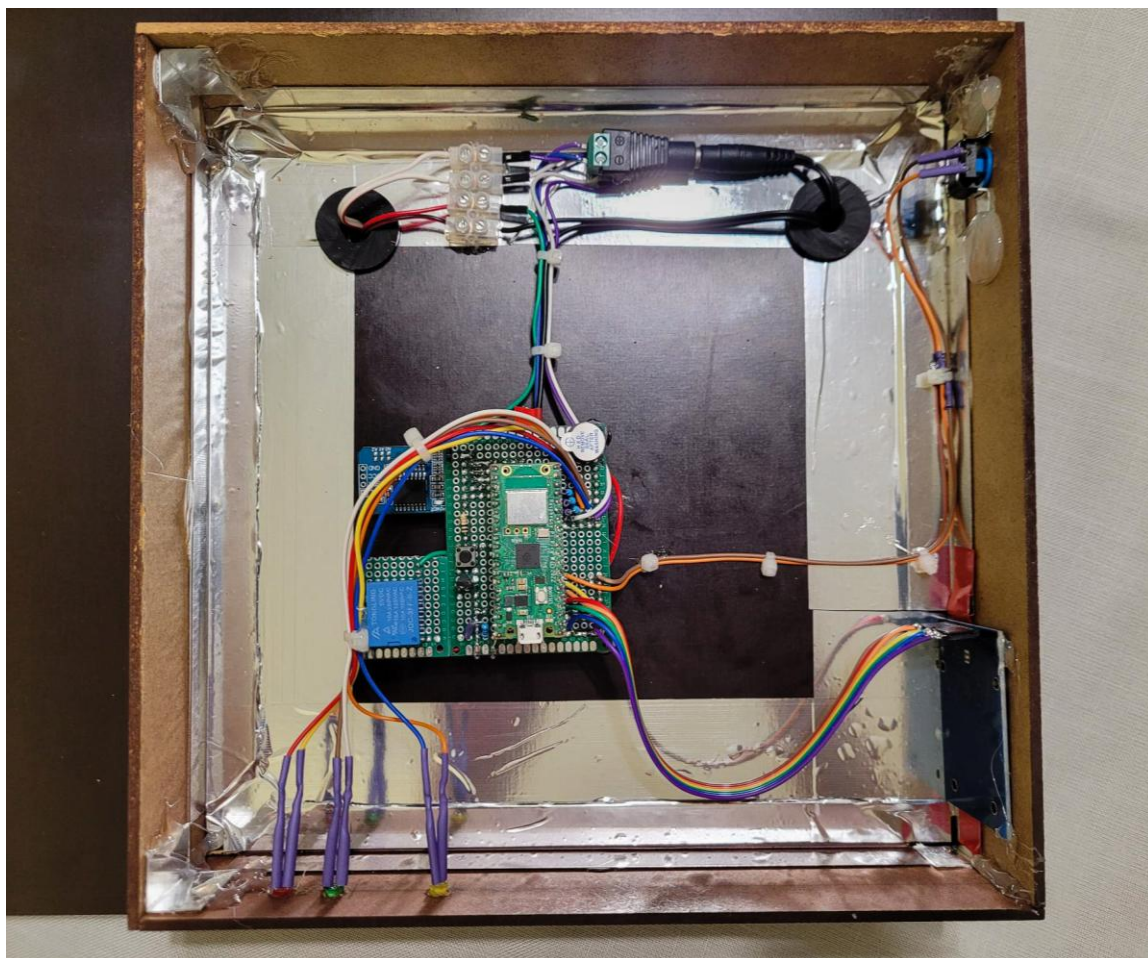
### 3.6. Budowa systemu kontroli dostępu

Makieta o wymiarach 40 cm × 50 cm ułatwiająca przedstawienie działania systemu kontroli dostępu została przygotowana i zamontowana na podstawie wykonanej ze sklejki. W celu lepszego zobrazowania poszczególnych funkcji, do makiety przymocowane są

drzwi, elementy elektroniczne, obudowa elementów elektronicznych oraz elektrozamek. Obudowa elementów elektronicznych została wykonana z płyty pilśniowej o dużej gęstości. Poszczególne części obudowy są połączone ze sobą oraz przytwierdzone do podstawy za pomocą kleju montażowego na bazie polimerów. Istnieje możliwość bezproblemowego otworzenia obudowy za pomocą uchwytu w celu demonstracji wyglądu mieszczącego się w środku układu. W obudowie znajdują się następujące, połączone ze sobą elementy: moduł mikrokontrolera Raspberry Pi Pico W, moduł zegara czasu rzeczywistego QYF-919 DS3231, moduł RFID MFRC522, przekaźnik jednokanałowy JQC-3FF-S-Z, przycisk RESET i buzzer. Moduł odpowiedzialny za identyfikację radiową jest umieszczony po wewnętrznej stronie bocznej części obudowy, ponieważ odczyt danych z kart identyfikacyjnych następuje z kilkucentymetrowej odległości, którą nieznacznie skraca obecność płyty pilśniowej. Obok czytnika przymocowany jest przycisk wyjścia, który na żądanie odblokowuje rygiel. W przygotowanych w bocznej części obudowy otworach znajdują się diody sygnalizujące stany, w których znajduje się system. Do modelu drzwi przytwierdzony został czujnik magnetyczny CMD 1423. Elektrozamek jest zamontowany w taki sposób, aby uniemożliwić otwieranie drzwi bez wystereowania sygnału zwolnienia rygla. W celu zachowania estetyki makiety, wszystkie połączenia przewodowe od elementów zewnętrznych do elementów znajdujących się w obudowie, prowadzone są pod deską i są do niej przymocowane.



Rys. 6. Wygląd przodu makiety systemu kontroli dostępu



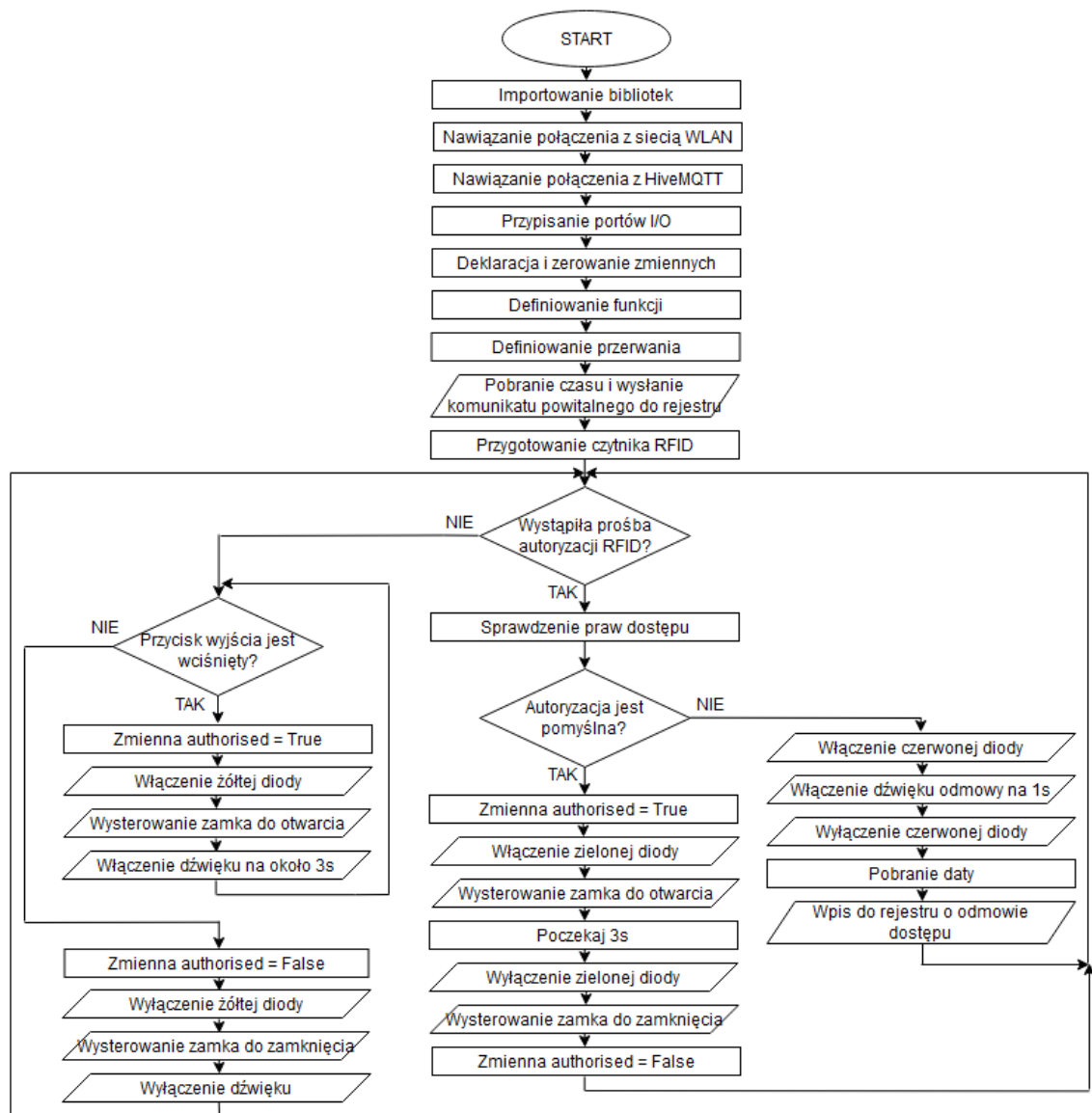
Rys. 7. Wygląd układu wewnątrz obudowy systemu kontroli dostępu

## 4. Opis oprogramowania

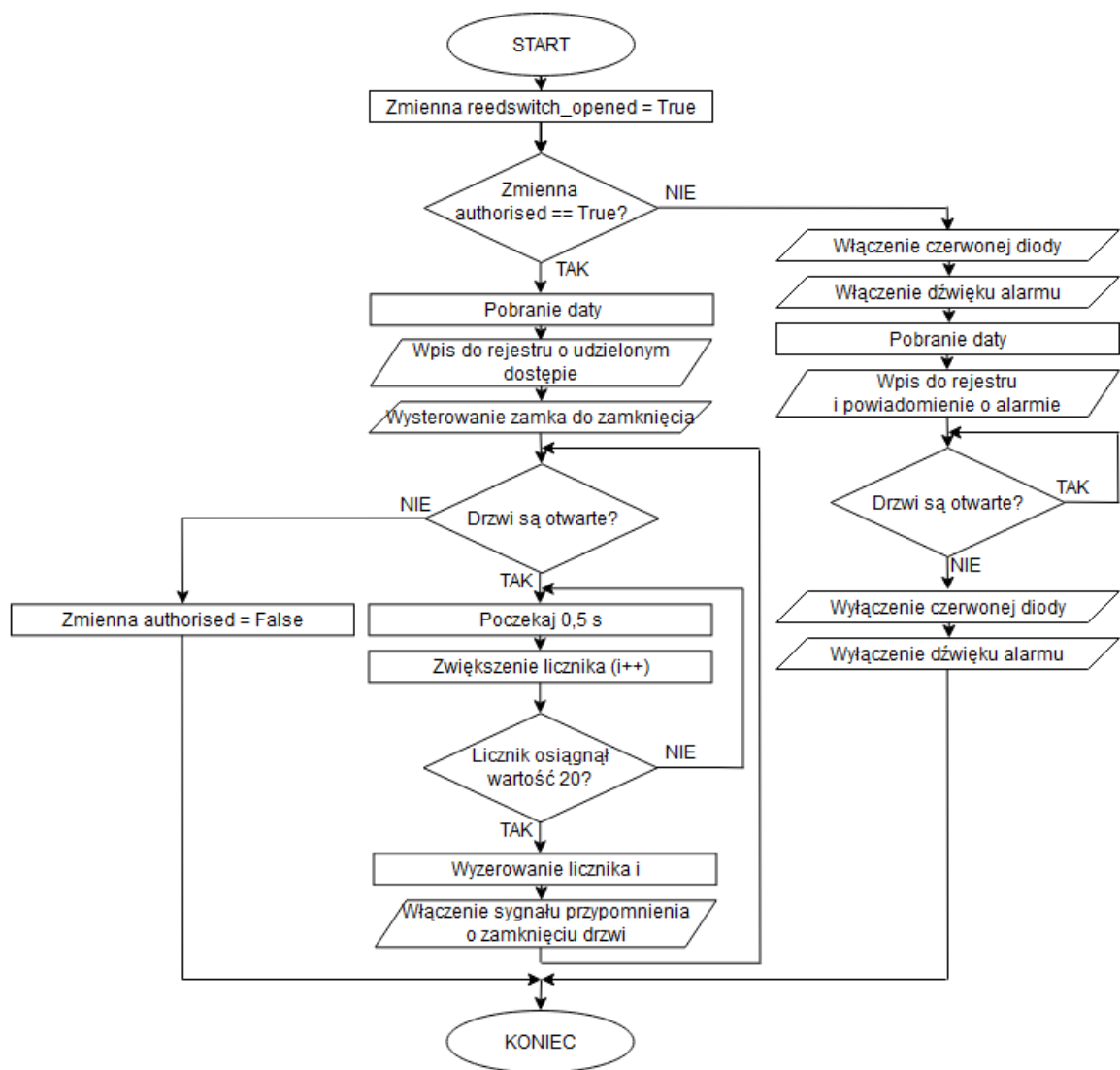
W niniejszym rozdziale został zawarty opis oprogramowania, które będzie pełniło nadrzędną funkcję w sposobie podejmowania decyzji przez system. Zostały przedstawione również ważniejsze funkcje oraz instrukcje zawarte w stworzonym kodzie.

### 4.1. Algorytm

Do obsługi systemu wykorzystane są proste instrukcje i mała ilość pętli warunkowych. Podyktowane jest to zmniejszeniem obciążenia mikrokontrolera. Zachowana została też niepisana zasada dotycząca umieszczania małej ilości instrukcji w funkcji przerwania.



Rys. 8. Algorytm blokowy głównej pętli programu



Rys. 9. Algorytm blokowy funkcji wywołanej przerwaniem zewnętrznym

Program można podzielić na fragmenty odpowiedzialne za mniejsze czynności. Na jego ogólną budowę przedstawioną na rysunku 8 składa się importowanie bibliotek, logowanie do sieci WLAN, logowanie do brokera HiveMQ, przypisanie portów wejścia/wyjścia do elementów, pobranie aktualnego czasu z wysłaniem wiadomości powitalnej systemu, definicja zmiennych wraz z ich zerowaniem, definicja funkcji, ustalenie zewnętrznego przerwania i wyłączenie wszystkich odbiorników. W skład głównej pętli programu wchodzi obsługa modułu identyfikacji radiowej, obsługa funkcji wywołanej przerwaniem oraz obsługa instrukcji przypisanych do przycisku żądania wyjścia. Kod realizuje też instrukcje odpowiedzialne za wysterowanie diod, buzzera, elektrozamka oraz przesłanie informacji o niepowołanym otwarciu drzwi do rejestru i zewnętrznej aplikacji w urządzeniu mobilnym. Na rysunku 9 przedstawiono algorytm blokowy funkcji



wywoływanej przerwaniem zewnętrznym. Owe przerwanie jest wywoływane w momencie zmiany stanu czujnika magnetycznego z logicznego 0 na logiczną 1. W treści obsługującej go funkcji znajduje się instrukcja zmieniająca wartość zmiennej `reedswitch_opened` na `True`. W następnych instrukcjach sprawdzane są warunki: czy uzyskano autoryzację oraz stan drzwi. W zależności od wartości zmiennej wywoływany jest alarm lub sygnał przypominający o zamknięciu drzwi. Po zakończeniu obsługi przerwania program powraca do pętli głównej.

#### **4.2. Opis działania systemu**

System uruchamia się po podłączeniu do zasilania. Jak każdy program, do uzyskania swojej pełnej funkcjonalności, wymaga około pięciu sekund na wykonanie instrukcji przygotowujących do pracy. Swoją gotowość sygnalizuje krótkim, około jednosekundowym dźwiękiem. System odblokowuje rygiel zamka w dwóch momentach, gdy:

- Zostanie przyłożona do czytnika RFID właściwa karta (zapewniająca autoryzację),
- Naciśnięty zostanie przycisk żądania wyjścia.

Wpis informacji (data zdarzenia, rodzaj zdarzenia) do rejestru zdarzeń ma miejsce w następujących przypadkach, gdy:

- Nastąpi nieautoryzowane otworenie drzwi,
- Nastąpi autoryzowane TAGiem otworenie drzwi,
- Nastąpi nieudana próba autoryzacji TAGu.

Przekazanie danych o zdarzeniu do zewnętrznej aplikacji mobilnej (powiadomienie) występuje w momencie zgłoszenia przez system alarmu dotyczącego nieautoryzowanego otworenia drzwi.

Użytkownik systemu rozróżnia stany autoryzacji przy pomocy buzzera oraz diod – czerwonej, żółtej i zielonej.

- Krótki sygnał dźwiękowy przy starcie systemu oznacza gotowość do pracy,
- Włączona dioda czerwona i dźwięk buzzera przez około 1 sekundę oznaczają nieuzyskanie autoryzacji,
- Włączona dioda czerwona i dźwięk buzzera przez czas, w którym są otwarte drzwi, oznacza, że zostały one otworzone bez autoryzacji,

- Krótki sygnał nadany czerwoną diodą i buzzerem co około 10 sekund oznacza przypomnienie o zamknięciu drzwi po autoryzowanym otwarciu drzwi,
- Trzysekundowy sygnał nadany diodą zieloną oznacza uzyskanie autoryzacji i zachętę do otwarcia drzwi,
- Około trzysekundowy sygnał buzzera oraz włączona w tym czasie żółta dioda oznaczają możliwość wyjścia po wciśnięciu przycisku żądania wyjścia.

#### 4.2.1. Opis obsługi elektrozamka

Obsługa elektrozamka jest realizowana w kilku krótkich poleceniach. Żeby dołączone do portu modułu mikrokontrolera urządzenie było wykrywane, w programie został przypisany numer portu [7].

```
#Przypisanie portow - przekaznik
```

```
relay = Pin(18, Pin.OUT)
```

Doysterowania portu w odpowiednim momencie, to znaczy, gdy uzyskana jest autoryzacja, używana jest metoda `value` z klasy `Pin`.

```
relay.value(0) #Rygiel zamknięty
```

```
relay.value(1) #Rygiel otwarty
```

Dzięki importowaniu odpowiednich klas na początku kodu można pominąć pisanie ich nazw w kodzie programu.

#### 4.2.2. Opis funkcji odczytu czasu z modułu zegara czasu rzeczywistego

Tak, jak każdy element dołączony do modułu mikrokontrolera, moduł zegara czasu rzeczywistego został przypisany w kodzie do właściwych mu pinów. Przesyłanie danych między modułami odbywa się za pomocą magistrali I<sup>2</sup>C.

```
#Przypisanie portow - RTC
```

```
rtc = machine.I2C(0,sda=Pin(16), scl=Pin(17))
```

Przed wprowadzeniem ostatecznego kodu obsługi modułu zegara czasu rzeczywistego, została ustawiona aktualna data i godzina w jego ustawieniach [37, 23].

```
current_time = b'\x00\x34\x14\x04\x11\x01\x23'
```

```
# sekundy\minuty\godziny\dzientygodnia\dzien\miesiac\rok
ds.set_time(current_time) #Odczyt czasu
```

Po wprowadzeniu poprawnych danych, powyższy kod został zamieniony na komentarz. Pobieranie aktualnej daty jest realizowane następująco:

```
t = ds.read_time() #Odczyt czasu
read_date = ("Data: %02x/%02x/20%x" %(t[4],t[5],t[6]))
#Przypisanie wartości do zmiennej
read_time = ("Godzina: %02x:%02x:%02x" %(t[2],t[1],t[0]))
#Przypisanie wartości do zmiennej
date_time = (read_date+' '+read_time) #Przypisanie wartości do zmiennej
```

#### 4.2.3. Opis funkcji obsługi identyfikacji radiowej

Identyfikacja radiowa jest główną częścią systemu. Dla zobrazowania obsługi kodu wybrano następujące fragmenty. Element jest podłączony i przypisany do następujących pinów modułu mikrokontrolera. Wymiana danych między modułami mikrokontrolera oraz identyfikacji radiowej odbywa się poprzez interfejs szeregowy [38].

```
#Przypisanie portow - RFID
reader = MFRC522(spi_id=0,sck=2,miso=4,mosi=3,cs=1,rst=0)
```

Kolejnym fragmentem jest ten inicjujący czytnik.

```
reader.init() #Metoda inicjowania czytnika
(stat, tag_type) = reader.request(reader.REQIDL)
#uzyskanie stanu czytnika
if stat == reader.OK: #Sprawdzenie, czy czytnik działa
    card = int.from_bytes(bytes(uid),"little",False)
#stworzenie obiektu karta, przechowuje ID
```

Sprawdzenie dopasowania kart do reguł polityki dostępu odbywa się przez zwykłe porównanie.



#### 4.2.4. Opis realizacji obsługi przerw

Przerwy to specjalne konstrukcje, które umożliwiają zatrzymanie w jednym momencie głównego programu i rozpoczęcie działania funkcji obsługującej to przerwanie. Po wykonaniu instrukcji powiązanej z przerwaniami zostaje wznowiony program główny w tym miejscu, w którym został zatrzymany. W zaprojektowanym systemie kontroli dostępu przerwanie jest wywoływane przez odczytanie stanu wysokiego z czujnika magnetycznego zamontowanego przy drzwiach. Ta instrukcja jest realizowana następująco. Zostaje określony pin wejściowy, na którym może pojawić się przerwanie oraz metoda irq. Kolejny fragment instrukcji wskazuje, jaki przypadek wywołuje przerwanie. Może to być na przykład dla sygnału odbieranego zbocze narastające, zbocze opadające, stan wysoki lub stan niski. Na potrzeby systemu kontroli dostępu została użyta opcja narastającego zbocza, jako impuls wyzwalający. Ostatnią częścią tej instrukcji jest wskazanie funkcji, która ma obsługiwać przerwanie.

*#Ustalenie przerwy w przypadku otwarcia drzwi*

*reedswitch.irq(trigger=machine.Pin.IRQ\_RISING, handler=reedswitch\_handler)*

Funkcja obsługująca przerwanie powinna być jak najkrótsza, zawierać jak najmniej instrukcji oraz nie odwoływać się do pamięci [39]. Przedstawiona funkcja zawiera jedynie nadanie wartości zmiennej globalnej. Zmiana tej wartości odsyła wykonywanie programu do wskazanego miejsca w kodzie.

*#Definicja funkcji wywoływanej przerwaniami kontaktronem*

*def reedswitch\_handler(reedswitch):*

*global reedswitch\_opened*

*if not reedswitch\_opened:*

*reedswitch\_opened = True*

Nieskomplikowane i krótkie programy można realizować z wykorzystaniem odpytywania urządzeń peryferyjnych (polling). Natomiast do realizacji większych struktur zalecane są podziały programów na funkcje i korzystanie z przerw zewnętrznych. W opisywanym programie zostało wykorzystane przerwanie ze względu na rozbudowaną strukturę instrukcji warunkowej if odpowiedzialnej za wskazany aspekt kodu.

#### 4.2.5. Opis sposobu połączenia z siecią WLAN

Przesyłanie danych między różnymi urządzeniami jest wymagane w wielu aspektach techniki. Na potrzeby zaprojektowania systemu kontroli dostępu, do przesyłania danych między jego elementami końcowymi, wykorzystano bezprzewodową sieć lokalną. Sposób podłączenia do sieci modułu mikrokontrolera Raspberry Pi Pico W jest następujący [13, 14].

```
#Logowanie do sieci

wlan = network.WLAN(network.STA_IF)

wlan.active(True)

ssid = secrets['ssid']

pw = secrets['pw']

wlan.connect(ssid,pw)
```

Ze względów bezpieczeństwa, które w tym przypadku są reprezentowane nieumieszczaniem w głównym pliku programu danych poufnych, identyfikator sieci oraz hasło zostały umieszczone w oddzielnym pliku `secrets.py`. Należy go zaimportować w tych plikach programu, w których wykorzystywane jest połączenie z siecią WLAN.

```
from secrets import secrets
```

Aby móc korzystać z takiego rozwiązania należy w dodatkowym pliku utworzyć słownik. Jest to struktura, za pomocą której wygodnie przechowuje się pary danych klucz – wartość [8].

```
secrets = {'ssid': 'nazwa_sieci',

           'pw': 'hasło'}
```

#### 4.2.6. Opis realizacji rejestru zdarzeń

Rejestr zdarzeń jest spisem wydarzeń, które wystąpiły w określonym czasie. Do realizacji tego założenia został wykorzystany HiveMQ. Jest to broker MQTT (ang. *MQ Telemetry Transport*), czyli oparty na protokole transmisji danych serwer, z którym łączą się klienci. Za jego pomocą publikowane są informacje. Jest narzędziem bardzo lekkim, przez co dobrze nadaje się do połączeń o małych przepustowościach. Jednocześnie, dzięki mniejszej prędkości transmisji zapewnia większą niezawodność. Zasada działania brokera

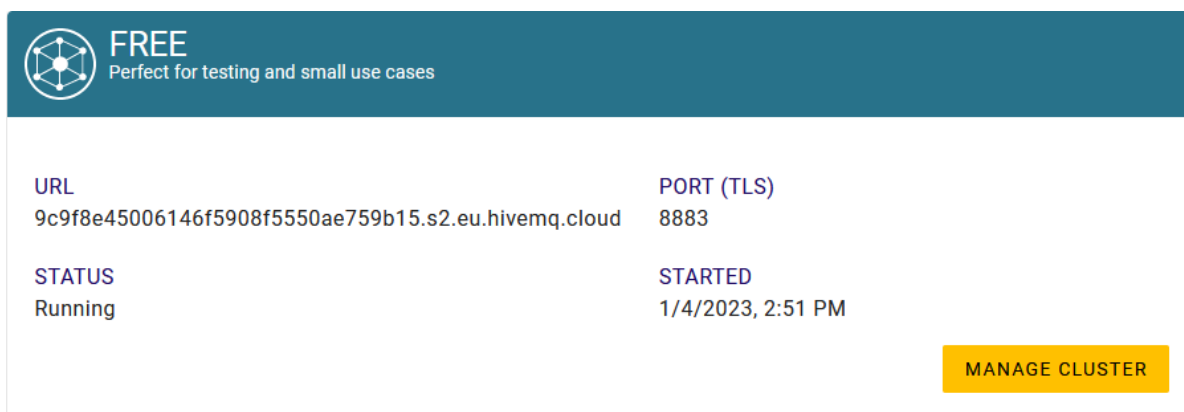
MQTT jest następująca. Klienci łączą się z brokerem i subskrybują tematy. Opublikowane w danym temacie informacje trafiają do wszystkich klientów, którzy go subskrybują.

Do realizacji przesyłania i magazynowania informacji z systemu kontroli dostępu wykorzystano polecenia z następujących linii kodu [40]. Pierwszym etapem jest uzyskanie dostępu do wydzielonej dla systemu grupy (ang. cluster).

```
from umqtt.simple import MQTTClient      #Importowanie biblioteki  
  
#Dane logowania do HiveMQ  
  
client_id = b'nazwa_klienta  
  
mqtt_server = b'nazwa_serwera'  
  
port = 0  
  
user = b'nazwa_uzytkownika'  
  
password = b'hasło'  
  
topic_pub = b'SKD2023'                  #Temat, pod którym publikowane sa informacje
```

Utworzone zostały dwie funkcje, które odpowiadają za nawiązanie połączenia ze znajdującym się w tak zwanej chmurze brokerem oraz odnowienie połączenia po ewentualnym jego zerwaniu.

```
#Funkcje - nawiązanie polaczenia i odnowienie polaczenia  
  
def mqtt_connect():  
  
    client = MQTTClient(client_id, mqtt_server, port, user, password, keepalive,  
ssl, ssl_params)  
  
    client.connect()  
  
    print('Connected to %s MQTT Broker'%(mqtt_server))  
  
    return client  
  
def reconnect():  
  
    print('Failed to connect to the MQTT Broker. Reconnecting...')  
  
    time.sleep(5)  
  
    machine.reset()
```



Rys. 10. Strona główna konsoli służącej do zarządzania grupami brokera MQTT [41]

Na rysunku 10 został przedstawiony wygląd konsoli brokera. Po nawiązaniu połączenia z brokerem można wysyłać już wiadomości. Z poziomu kodu programu jest to realizowane następującymi poleceniami.

```
#Zdefiniowanie treści przykładowej wiadomości
```

```
topic_msg = (b'Uruchomiono system -' + date_time)
```

```
#Wysłanie wiadomości
```

```
client.publish(topic_pub, topic_msg)
```

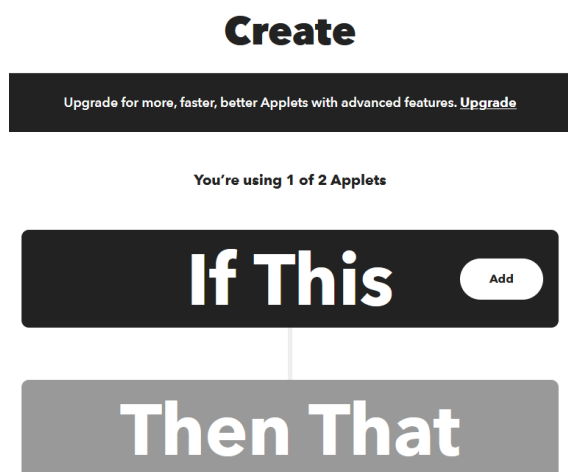
Przesyłane z modułu mikrokontrolera powiadomienia pojawiają się w rejestrze. Jest to prosta baza danych składająca się z jednej czterokolumnowej tablicy. Pierwsza kolumna to otrzymana wiadomość, druga zawiera temat, trzecia QoS, natomiast czwarta jest znacznikiem czasu. Temat może być różny dla każdej wiadomości. Każdy z nich może też zostać oznaczony innym kolorem w celu łatwiejszej identyfikacji wybranych tematów spośród wszystkich danych. Znacznik czasu prezentowany jest w mało czytelnej formie, dlatego w treści przesyłanej wiadomości zostaje umieszczona dokładna data pobrana z modułu zegara czasu rzeczywistego.

Message	Topic	QoS	Timestamp
Otworzono drzwi bez autoryzacji - Date: 18/01/2023 Time: 14:31:58	SKD2023	0	1674048724714
Otworzono drzwi z autoryzacją - Date: 18/01/2023 Time: 14:31:35	SKD2023	0	1674048698602
Uruchomiono system - Data: 18/01/2023 Godzina: 14:30:59	SKD2023	0	1674048667879

Rys. 11. Rejestr zdarzeń zaprojektowany przy użyciu HiveMQ [41]

Na rysunku 11 przedstawiono wygląd rekordów rejestru zdarzeń. W zależności od wymagań potencjalnego administratora systemu do przesyłanej wiadomości można dołączyć na przykład dane osoby, której karta identyfikacyjna została użyta do autoryzacji.

Do alarmowania wspomnianego już administratora o nieupoważnionym wejściu do pomieszczenia wprowadzono funkcję powiadomień przesyłanych do smartphona powiązanego z systemem kontroli dostępu. Smartphone musi mieć zainstalowaną aplikację IFTTT. Następnie administrator musi zalogować się na to samo konto stworzone w IFTTT, przy pomocy którego zostały utworzone powiadomienia w systemie. Na rysunkach 12, 13 i 14 przedstawiono proces tworzenia instrukcji warunkowej odnoszącej się do wywołania alarmu w przypadku nieautoryzowanego otwarcia drzwi.

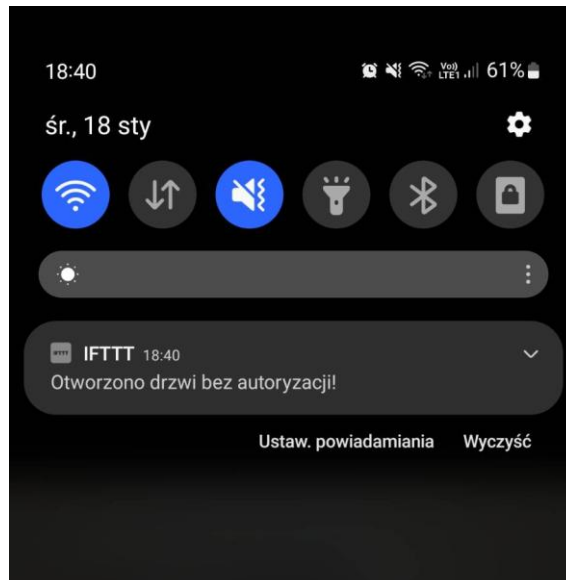


Rys. 12. Panel tworzenia instrukcji warunkowych w witrynie IFTTT [12]

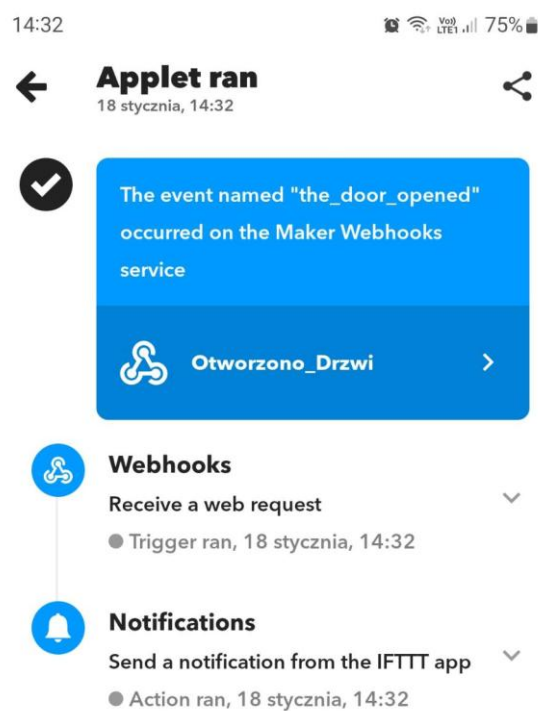
Rys. 13. Tworzenie warunku wyzwalającego akcję w witrynie IFTTT [12]

Rys. 14. Tworzenie instrukcji warunkowej w witrynie IFTTT [12]

Na rysunku 15 przedstawiony został wygląd powiadomienia wygenerowanego przez aplikację zainstalowaną w smartphonie. Po otwarciu opisywanego powiadomienia następuje przekierowanie do aplikacji IFTTT, gdzie znajduje się pełen opis zdarzenia, które miało miejsce. Opis zdarzenia wraz z dodatkowymi informacjami przedstawiony jest na rysunku 16.



Rys. 15. Wygląd powiadomienia otrzymanego z aplikacji IFTTT zainstalowanej w smartphonie [12]



Rys. 16. Opis zdarzenia w aplikacji IFTTT [12]

Po rozwinięciu powiadomienia aplikacji zostają przedstawione dodatkowe informacje dotyczące zdarzenia. Są to między innymi wskazania, co wywołało akcję, dokładna data zdarzenia oraz przesyłana wiadomość.

## **5. Opis wykonanych testów działania systemu**

W rozdziale piątym zostały opisane przeprowadzone testy, którym został poddany zaprojektowany system kontroli dostępu. Jako jedno z narzędzi do zabezpieczania dóbr materialnych, powinien cechować się niezawodnością, a jego oprogramowanie obsługiwać wszystkie możliwe przypadki działań użytkowników.

### **5.1. Test wykrycia otwarcia drzwi**

Według przedstawionych do realizacji założeń otwieranie drzwi przez użytkowników jest zgłaszane w systemie w dwóch przypadkach. Pierwszy z nich to autoryzowane wejście do pomieszczenia. Oznacza to skorzystanie z karty identyfikacji radiowej i pomyślne przejście weryfikacji uprawnień. Do rejestru zostaje w takim przypadku przesłana wiadomość oznaczona datą o treści „Otworzono drzwi z autoryzacją”. Zostaną też włączone sygnały świetlny i dźwiękowy, których źródła znajdują się przy czytniku kart RFID. Drugi przypadek to wykrycie otwarcia drzwi bez uzyskanej autoryzacji. W następstwie tej akcji zostaje przesłana do rejestru zdarzeń wiadomość o treści „Otworzono drzwi bez autoryzacji”, która również jest oznaczona datą. Dodatkowo zostaje wysłane powiadomienie wyświetlane w smartphonie administratora oraz włączony alarm dźwiękowy i świetlny przy czytniku kart.

Realizacja tych założeń wykonana została poprawnie, co zostało przedstawione na rysunkach 11 i 15.

### **5.2. Test reakcji czytnika RFID**

Czytnik RFID, w zależności od wykorzystywanej przez niego do odczytu kart częstotliwości radiowej, reprezentuje różną odległość odczytu danych z nośnika. Według danych podanych w karcie produktu „Moduł RFID MF RC522 13,56MHz” maksymalną odległością, z jakiej powinny zostać odczytane dane to 10 cm [20]. W ramach testu wykonano szereg prób mających na celu sprawdzenie maksymalnej odległości, z jakiej możliwy jest odczyt danych z karty z uwzględnieniem przeszkód fizycznych umieszczonych między czytnikiem a kartą. Wykonano poniższe próby, a otrzymane wyniki zostały umieszczone w tabeli 7.



Tab. 7. Maksymalna odległość umożliwiająca modułowi RFID MF RC522 13,56MHz odczyt danych z karty identyfikacyjnej

Przeszkoda	Grubość przeszkody	Rezultat
Powietrze (próba kontrolna)	Od 0 do 2,5 cm	Odczyt danych
Plastik 0,2 cm	Od 0,2 do 2,5 cm	Odczyt danych
Stos kartek papieru	Od 0 do 2,5 cm	Odczyt danych
Płyta pilśniowa o dużej gęstości 0,4 cm	Od 0,4 do 2,5 cm	Odczyt danych
Szkło 0,5 cm	Od 0,5 do 2,5 cm	Odczyt danych
Skóra licowa 0,2 cm	Od 0,2 do 2,5 cm	Odczyt danych
Blacha stalowa 0,1 cm	0,1 cm	Brak odczytu danych
Blacha stalowa nierdzewna perforowana 0,1 cm, średnica oczek 0,3 cm	0,1 cm	Brak odczytu danych

Przeprowadzone badanie miało na celu weryfikację danych dostarczanych przez dystrybutora elementów. Pozwoliło też określić najlepszy materiał, z którego powinna zostać wykonana obudowa modułu czytnika RFID. Do stworzenia obudowy wchodzącej w skład makiety została wykorzystana płyta pilśniowa o dużej gęstości. W ramach testu pokazano, że dane udostępniane przez sklep nie zawsze są zgodne z rzeczywistością. Potwierdzono także informację, że sąsiedztwo metalowych obiektów ogranicza rozprzestrzenianie się fali radiowych. Mając to na uwadze, w trakcie budowy makiety, elektrozamek umieszczono po jej przeciwnej stronie, w odległości około 25 cm od czytnika RFID.

### 5.3. Test zaniku zasilania

Zanik zasilania jest jednym z możliwych scenariuszy, który może wystąpić w każdym budynku. Najczęściej nie jest on zamierzony, co należy uwzględnić w trakcie projektowania różnego rodzaju systemów. Ze względu na to, że system kontroli dostępu należy do grupy systemów mających zapewnić bezpieczeństwo, jedną z kluczowych jest kwestia jego zachowania w przypadku braku zasilania. Założono, że w przypadku zaniku zasilania, pomieszczenie pozostanie zamknięte. Po przywróceniu zasilania ma natomiast zostać wygenerowany i zapisany w rejestrze specjalny komunikat. W ramach sprawdzenia tego zachowania, po wykonaniu standardowych czynności wymaganych od systemu, przeprowadzeniu autoryzowanego przejścia oraz wywołania alarmu, odłączono zasilanie. Na rysunku 17 został przedstawiony fragment rejestru zdarzeń. Najnowszy widoczny wpis został utworzony po ponownym rozruchu systemu. Nastąpił on po około 7 sekundach od

ponownego podłączenia zasilania i został zasygnalizowany krótkim dźwiękiem. W czasie, gdy system był wyłączony, sprawdzono możliwość otworzenia drzwi. Jedyne sposoby, aby tego dokonać, wymaga zniszczenia drzwi bądź innych elementów będących częścią tego przejścia.

Message	Topic	QoS	Timestamp
Uruchomiono system - Data: 18/01/2023 G odzina: 14:38:16	SKD2023	0	1674049104625
Otworzono drzwi bez autoryzacji - Date: 18/ 01/2023 Time: 14:31:58	SKD2023	0	1674048724714
Otworzono drzwi z autoryzacją - Date: 18/0 1/2023 Time: 14:31:35	SKD2023	0	1674048698602
Uruchomiono system - Data: 18/01/2023 G odzina: 14:30:59	SKD2023	0	1674048667879

Rys. 17. Fragment rejestru zdarzeń obrazujący ponowne uruchomienie systemu po zaniku zasilania [41]

#### 5.4. Wykonanie dwóch czynności w tym samym czasie

Projektując system, należy uwzględniać to, że użytkownicy nie zawsze wykonują czynności tak, jak założył to jego twórca. W tym celu testuje się prototypowe urządzenia pod wieloma czynnikami. Zaprojektowany system kontroli dostępu został przetestowany także pod względem wykonania kilku czynności jednocześnie. Sprawdzono reakcję systemu na użycie przycisku żądania wyjścia w czasie, gdy drzwi są już otwarte, próby autoryzacji kilku użytkowników jednocześnie oraz wykonywania czynności w trakcie alarmu systemu.

Do pierwszego testu została przeprowadzona autoryzacja oraz otworzone drzwi. Następnie uaktywniono przycisk żądania wyjścia. System nie wygenerował żadnej reakcji. Oznacza to, że takie działanie nie zakłóca pracy systemu i nie jest potrzebne wprowadzanie zmian w programie. W ramach jednego już aktywnego przerwania generowanego przez sygnał zgłoszenia czujnika magnetycznego nie mogą współistnieć inne przerwania. System zachował się tak, jak jest to uzgodnione w założeniach.

Kolejnym elementem, na który zwrócono uwagę, jest próba oszukania czytnika kart. W trakcie testu przykładano kilka kart identyfikacyjnych jednocześnie (jedna nad drugą). Czytnik pobierał informacje tylko z karty położonej najbliżej siebie. Ilość pozostałych kart nie wprowadzała różnicy. Oznacza to, że potencjalny włamywacz, posiadając kilka kart

identyfikacyjnych, musiałby po kolei sprawdzać wszystkie karty pod względem uzyskania autoryzacji. Ten test ujawnił możliwość wprowadzenia kolejnego zabezpieczenia systemu.

Kolejne dwa testy zostały przeprowadzone w trakcie trwania alarmu informującego o nieautoryzowanym otwarciu drzwi do zabezpieczanego pomieszczenia. W pierwszym z nich została przeprowadzona próba dokonania autoryzacji. Pomimo korzystania z właściwej karty, alarm nie przestał działać. Taki sam rezultat został uzyskany w przypadku użycia przycisku żądania wyjścia. Nie miał wpływu na działanie alarmu. Oznacza to, że autoryzacja przejścia już po otwarciu drzwi nie anuluje wywołanego alarmu.

Wykonanie nawet minimalnej ilości testów jest czynnikiem wskazującym możliwy kierunek poprawy systemu oraz wykrycie błędów, które uwidaczniają się dopiero w czasie nietypowych zdarzeń. Aby zapewnić funkcjonalność systemu, przetestowanie go jest ważnym punktem w harmonogramie prac.

## 6. Możliwość rozbudowy systemu

Możliwość rozbudowy systemu jest jedną z zalet, którymi można opisać dostępne systemy kontroli dostępu. Zaprojektowany system również ma taką możliwość.

Do potencjalnych dodatkowych funkcji należy możliwość objęcia nadzorem większej ilości pomieszczeń. Wprowadziłoby to możliwość zarządzania większą ilością przejść oraz nadawaniem uprawnień do tylko wybranych pomieszczeń.

Dodanie w pomieszczeniu czujnika ruchu PIR powodowałoby rozwój projektu w kierunku współpracujących systemów: kontroli dostępu oraz alarmu antywłamaniowego. Takie rozwiązanie podniosłoby poziom bezpieczeństwa, ale wymagałoby rozbudowy programu oraz dodania elementów składowych systemu.

Kwestią, którą należałoby przedyskutować, jest poziom bezpieczeństwa połączenia bezprzewodowego. W celu zwiększenia bezpieczeństwa połączenia można by wprowadzić łączność przewodową, która jest trudniejsza do przechwycenia. Jest jednak mniej elastyczna pod względem rozmieszczenia urządzeń i estetyki wykonania. Przykładowo w budynkach zabytkowych preferowana jest właśnie łączność bezprzewodowa.

Jeden z przeprowadzonych testów wykazał, że nie jest możliwy odczyt danych z kilku kart identyfikacyjnych jednocześnie. Otwiera to możliwość do stworzenia narzędzia bądź funkcji, które będzie zliczać ilość nieudanych autoryzacji w krótkim przedziale czasu i wskazywać podejrzanе zachowanie administratorowi systemu.

Zaprojektowany system jest gotowy do rozwoju na wielu płaszczyznach. Kierunek rozbudowy systemu zależy, zatem od preferencji użytkowników i ich ewentualnych zmian w przyszłości.

## 7. Wnioski i spostrzeżenia

W trakcie pracy nad projektem należy zwracać uwagę na wiele czynników wpływających na ogólny przebieg zadania. Jednym z ważniejszych aspektów organizacyjnych jest doliczenie dodatkowego czasu do każdego podzadania. Zapobiega to przekroczeniu terminu wykonania zadania oraz zmniejsza presję, pod którą wykonywana jest praca.

Dokładne przeanalizowanie problemu i następnie przeszukanie rynku w poszukiwaniu dostępnych rozwiązań, pomaga w jego rozwiązaniu.

Przed złożeniem zamówienia na potrzebne elementy układu warto dokładnie porównać oferowane produkty pod kątem dopasowania stosowanej przez nie komunikacji oraz napięcia zasilania. Przed przystąpieniem do montażu całego układu, dobrą praktyką jest przetestowanie każdego jego elementu w osobnym teście. Pomaga to stwierdzić wady fabryczne elementów oraz ułatwia ogólną diagnostykę błędów.

Nadmiarowa w porównaniu do wymaganej w projekcie ilość portów wejścia/wyjścia modułu mikrokontrolera Raspberry Pi Pico ułatwia projektowanie i późniejsze rozmieszczenie elementów na płytkach uniwersalnych.

Ograniczenie ilości wykorzystywanych elementów zmniejsza prawdopodobieństwo wystąpienia awarii tych elementów, a w szerszym aspekcie całego systemu.

Uzyskane w testach rezultaty wskazują kierunek możliwego rozwoju systemu. Są to przede wszystkim poprawa bezpieczeństwa komunikacji oraz rozbudowa systemu w celu dołączenia do niego większej ilości pomieszczeń. Ważnym aspektem jest też kwestia zliczania ilości nieudanych prób autoryzacji następujących po sobie.

W trakcie wykonywania zadania projektowego został dokonany przegląd koncepcji działania systemów kontroli dostępu. Następnie określono funkcje wykonywane przez zaprojektowany system. Dokonano wyboru elementów potrzebnych do realizacji sprzętowej. Stworzono także projekt systemu, który realizuje postawione wcześniej wymagania. W ramach implementacji projektu skonstruowano makietę przedstawiającą drzwi objęte systemem kontroli dostępu wraz z tym systemem. Wykonano szereg testów, których celem było sprawdzenie poprawności działania systemu oraz jego zachowanie na nieoczekiwane sytuacje. W ramach sprawdzenia możliwości wdrożenia zaprojektowanego systemu stwierdzono, że system może służyć do kontroli odwiedzania pomieszczenia.

W tym celu wymagane jest tylko zmiana obudowy wykonanej w ramach makiety na trwałą i trudną do otworzenia oraz montaż głównych elementów elektronicznych wewnątrz chronionego pomieszczenia. Oznacza to, że ustalone zadania szczegółowe zostały zrealizowane, a w konsekwencji został osiągnięty założony cel pracy.

W trakcie pracy nad projektem autorka udoskonaliła umiejętności z dziedziny programowania w języku MicroPython, elektroniki oraz zadań manualnych. Zaprojektowanie, implementacja i testowanie systemu kontroli dostępu wymagało od autorki wyszukiwania przydatnych informacji, uważnego i konsekwentnego korzystania z danych udostępnianych przez producentów elementów elektronicznych oraz pogłębienia wiedzy z zakresu infrastruktury bezpieczeństwa. Kolejną umiejętnością rozwijaną w trakcie tworzenia systemu było zarządzanie czasem i kolejnością wykonywania zadań w projekcie.

Jedną z trudności napotkanych w trakcie pisania pracy dyplomowej była potrzeba zdiagnozowania przyczyny niedziałania zaprojektowanego programu. Nie była to jednak kwestia źle napisanego kodu, a uszkodzonego w transporcie elementu.

## 8. Literatura

- [1]. A. Miler-Zawodniak, Teorie potrzeb jako współczesne teorie motywacji, OBRONNOŚĆ. Zeszyty Naukowe 4/2012, ISSN 2084-7297, Muzeum Historii Polski, 2012.
- [2]. G. Pulford, High-Security Mechanical Locks. An Encyclopedic Reference, Elsevier Academic Press, 2007
- [3]. W. D. Morse, Physical security of cut-and-cover underground facilities, United States: N. p., 1998.
- [4]. A. Chwaleba, B. Moeschke, G. Płoszajski, Elektronika, WSiP, wydanie II, 2012.
- [5]. B. Pióro, M. Pióro, Podstawy Elektroniki część 1, WSiP, wydanie XIV, 2014.
- [6]. S. Okoniewski, Technologia dla elektroników, WSiP, 1980.
- [7]. G. Halfacree, B. Everard, Get started with MicroPython on Raspberry Pi Pico, Raspberry Pi PRESS, 2021.
- [8]. M. Lassoﬀ, Programowanie dla początkujących, Helion, 2016.
- [9]. Strona Politechnika Lubelska,  
[http://www.systemy.pollub.pl/Dyd\\_MH\\_InteligentneInst07.pdf](http://www.systemy.pollub.pl/Dyd_MH_InteligentneInst07.pdf), (dostęp dnia 12.01.2023).
- [10]. Strona CloneMyKey, <https://clonemykey.com/all/smart-access-control-policies-for-residential-commercial-buildings/>, (dostęp dnia 12.01.2023).
- [11]. Strona Eltrox, <https://www.eltrox.pl/automatyka-domowa/kontrola-dostepu/kontrolery-dostepu/kontroler-dostepu-roger-pr622-g.html>, (dostęp dnia 13.01.2023).
- [12]. Strona IFTTT, [https://ifttt.com/explore/new\\_to\\_ifttt](https://ifttt.com/explore/new_to_ifttt), (dostęp dnia 16.01.2023).
- [13]. Strona Raspberry Pi, <https://www.raspberrypi.com/news/raspberry-pi-pico-w-your-6-iot-platform/>, (dostęp dnia 30.06.2022).
- [14]. Strona Mikrokontroler, <https://mikrokontroler.pl/2022/06/30/plytka-raspberry-pi-pico-w-z-komunikacja-wi-fi-i-mikrokontrolerem-rp2040/>, (dostęp dnia 30.06.2022).

- [15]. Strona Raspberry Pi, <https://datasheets.raspberrypi.com/picow/pico-w-datasheet.pdf>, (dostęp dnia 15.10.2022).
- [16]. Strona Arduino, <https://store.arduino.cc/products/arduino-uno-rev3/>, (dostęp dnia 12.01.2023).
- [17]. Strona Raspberry Pi, <https://datasheets.raspberrypi.com/pico/pico-datasheet.pdf>, (dostęp dnia 12.01.2023).
- [18]. Strona Forbot, <https://forbot.pl/blog/leksykon/esp8266>, (dostęp dnia 12.01.2023).
- [19]. Strona Infineon, [https://www.infineon.com/dgdl/Infineon-CYW43439-DataSheet-v03\\_00-EN.pdf?fileId=8ac78c8c8386267f0183c320336c029f](https://www.infineon.com/dgdl/Infineon-CYW43439-DataSheet-v03_00-EN.pdf?fileId=8ac78c8c8386267f0183c320336c029f), (dostęp dnia 12.01.2023).
- [20]. Strona Botland, <https://botland.com.pl/moduly-i-tag-rfid/6765-modul-rfid-mf-rc522-1356mhz-spi-karta-i-brelok-5904422335014.html>, (dostęp dnia 11.06.2022).
- [21]. Strona RFIDPolska, <https://www.rfidpolska.pl/standardy-rfid/>, (dostęp dnia 12.01.2023).
- [22]. Strona Botland, <https://botland.com.pl/moduly-i-tag-rfid/14072-rfid-qwiic-reader-czytnik-rfid-sparkfun-sen-15191-5904422321895.html>, (dostęp dnia 12.01.2023).
- [23]. Strona Elty, <https://elty.pl/pl/p/Modul-zegara-czasu-rzeczywistego-DS3231/3470>, (dostęp dnia 10.01.2023).
- [24]. Strona Technovade, <http://technovade.pl/zegar-czasu-rzeczywistego-rtc-modul-ds1302-bateria.html>, (dostęp dnia 13.01.2023).
- [25]. Strona Botland, [https://botland.com.pl/index.php?controller=attachment&id\\_attachment=1397](https://botland.com.pl/index.php?controller=attachment&id_attachment=1397), (dostęp dnia 15.10.2022).
- [26]. Strona Elenota, [http://www.elenota.pl/datasheet\\_download/157772/BC546B](http://www.elenota.pl/datasheet_download/157772/BC546B), (dostęp dnia 06.01.2023).
- [27]. Strona Ermicro, <http://www.ermicro.com/blog/?p=423>, (dostęp dnia 08.01.2023).
- [28]. Strona Botland, <https://botland.com.pl/zamki-elektryczne/5687-elektrozamek-elektromagnes-z-wysuwany-bolcem-12v-5903351245364.html>, (dostęp dnia 11.06.2022).



- [29]. Strona Botland, <https://botland.com.pl/czujniki-magnetyczne/3104-czujnik-magnetyczny-otwarcia-drzwi-okien-kontaktron-cmd14-srubki-5904422366247.html>, (dostęp dnia 11.06.2022).
- [30]. Strona Botland, <https://botland.com.pl/zasilacze-dogniazdkowe/1364-zasilacz-impulsowy-5v-25a-wtyk-dc-55-21mm-5907621806552.html>, (dostęp dnia 11.06.2022).
- [31]. Strona Botland, <https://botland.com.pl/zasilacze-dogniazdkowe/5044-zasilacz-impulsowy-12v125a-wtyk-dc-5525mm-5902270707502.html>, (dostęp dnia 11.06.2022).
- [32]. Strona Botland, <https://botland.com.pl/diody-led/19992-zestaw-diod-led-5mm-justpi-16szt-5904422328801.html>, (dostęp dnia 11.06.2022).
- [33]. Strona Forbot, <https://forbot.pl/blog/jak-dobrac-rezystor-do-diody-rozne-metody-zasilania-led-id14482> (dostęp dnia 10.11.2022).
- [34]. Strona Botland, <https://botland.com.pl/buzzery-generatory-dzwieku/4526-modul-z-buzzerem-aktywnym-z-generatorem-zielony-5904422300654.html>, (dostęp dnia 11.06.2022).
- [35]. Strona Botland, [https://botland.com.pl/index.php?controller=attachment&id\\_attachment=324](https://botland.com.pl/index.php?controller=attachment&id_attachment=324), (dostęp dnia 15.10.2022).
- [36]. Strona Botland, <https://botland.com.pl/tact-switch/3665-tact-switch-12x12mm-z-nasadka-grzybek-niebieski-5szt-5904422307493.html>, (dostęp dnia 11.06.2022).
- [37]. Strona AZ-Delivery, <https://www.az-delivery.de/en/blogs/azdelivery-blog-fur-arduino-und-raspberry-pi-pico-als-analoge-uhr>, (dostęp dnia 11.01.2023).
- [38]. Strona Microcontrollerslab, <https://microcontrollerslab.com/raspberry-pi-pico-rfid-rc522-micropython/>, (dostęp dnia 30.06.2022).
- [39]. Strona Electrocredible, <https://electrocredible.com/raspberry-pi-pico-external-interrupts-button-micropython/?fbclid=IwAR2JEcv5bJErSS7pFlApqISQrqb14b8mNkeZHNbWmp4bUUWilcoJhykNI>, (dostęp dnia 06.01.2023).
- [40]. Strona HiveMQ, <https://www.hivemq.com/blog/iot-reading-sensor-data-raspberry-pi-pico-w-micropython-mqtt-node-red/>, (dostęp dnia 08.01.2023).
- [41]. Strona HiveMQ, <https://console.hivemq.cloud/>, (dostęp dnia 17.01.2023).

## 9. Spis rysunków

Rys. 1. Wyprowadzenia Raspberry Pi Pico W [15] .....	17
Rys. 2. Moduł WiFi ESP8266EX [18] .....	18
Rys. 3. Moduł RFID MF RC522 [20] .....	20
Rys. 4. moduł zegara czasu rzeczywistego QYF-919 DS3231 [23] .....	21
Rys. 5. Schemat połączeń układu systemu kontroli dostępu .....	25
Rys. 6. Wygląd przodu makiety systemu kontroli dostępu .....	26
Rys. 7. Wygląd układu wewnątrz obudowy systemu kontroli dostępu .....	27
Rys. 8. Algorytm blokowy głównej pętli programu .....	28
Rys. 9. Algorytm blokowy funkcji wywołanej przerwaniem zewnętrznym .....	29
Rys. 10. Strona główna konsoli służącej do zarządzania grupami brokera MQTT [41] .....	36
Rys. 11. Rejestr zdarzeń zaprojektowany przy użyciu HiveMQ [41] .....	37
Rys. 12. Panel tworzenia instrukcji warunkowych w witrynie IFTTT [12] .....	37
Rys. 13. Tworzenie warunku wyzwalającego akcję w witrynie IFTTT [12] .....	38
Rys. 14. Tworzenie instrukcji warunkowej w witrynie IFTTT [12] .....	38
Rys. 15. Wygląd powiadomienia otrzymanego z aplikacji IFTTT zainstalowanej w smartphonie [12] .....	39
Rys. 16. Opis zdarzenia w aplikacji IFTTT [12] .....	39
Rys. 17. Fragment rejestru zdarzeń obrazujący ponowne uruchomienie systemu po zaniku zasilania [41] .....	42

## 10. Spis tabel

Tab. 1. Specyfikacja techniczna modułów mikrokontrolerów Raspberry Pi Pico, Raspberry Pi Pico W i Arduino Uno Rev 3 [15, 16, 17] .....	16
Tab. 2. Specyfikacja ESP8266EX [18] .....	18
Tab. 3. Specyfikacja komunikacji bezprzewodowej modułu Raspberry Pi Pico W [19] .....	18
Tab. 4. Specyfikacja modułów RFID [20, 21, 22] .....	19
Tab. 5. Specyfikacja wybranych modułów zegara czasu rzeczywistego [23, 24] .....	20
Tab. 6. Specyfikacja czujnika magnetycznego [29] .....	22
Tab. 7. Maksymalna odległość umożliwiająca modułowi RFID MF RC522 13,56MHz odczyt danych z karty identyfikacyjnej .....	41

## **11.Spis załączników**

Załącznik 1: Karta pracy dyplomowej.

Załącznik 2: Biblioteki i program wymagane do uruchomienia systemu.