# Specyfikacja wymagań: Project Raven

Wersja: 1.0.1  
Autor: Rafał Leś  
Data: 18 grudnia 2024

# Historia zmian:

|  |  |  |  |
| --- | --- | --- | --- |
| Data | Wersja | Opis zmian | Autor |
| 2024-12-04 | 1.0.0 | Stworzenie wstępnej specyfikacji | Rafał Leś |
| 2024-12-18 | 1.0.1 | Dodanie diagram UML, scalenie specyfikacji | Rafał Leś |

# Spis treści

1. Wprowadzenie  
 1.1. Cel dokumentu  
 1.2. Zakres dokumentu  
 1.3. Definicje, akronimy oraz skróty używane w dokumencie  
  
2. Opis  
 2.1. Cel systemu  
 2.2. Kluczowe cechy systemu  
 2.3. Opis technologii oraz architektury systemu  
  
3. Funkcje asystenta i działanie aplikacji  
 3.1. Główne funkcje  
 3.2. Scenariusz użycia  
 3.3. Architektura systemu i wybór technologii  
 3.4. Interfejs użytkownika  
 3.5. Zabezpieczenia przed niebezpiecznymi promptami użytkownika  
 3.6. Zabezpieczenia przed potencjalnymi atakami cybernetycznymi  
 3.7. Obsługa i pomoc użytkownikowi  
 3.8. Zapisywanie danych i dostęp do historii  
 3.9. Autoryzacja głosowa  
 3.10 Sposób zasilania i funkcjonowania systemu  
 3.11 Potencjalne rozszerzenia

4. Schematy  
 4.1 Diagram UML

## Wprowadzenie

**1.1 Cel dokumentu**

Celem tego dokumentu jest opisanie wymagań dla systemu Asystenta AI o nazwie "Raven". System ma działać na bazie Raspberry Pi 2 Zero z wbudowaną sztuczną inteligencją ChatGPT, zapewniając funkcje komunikacyjne między użytkownikiem a pojazdem w celu poprawy doświadczenia użytkowania samochodu.

**1.2 Zakres dokumentu**

Dokument obejmuje opis wymagań funkcjonalnych, architektury systemu, technologii oraz działania Asystenta AI. Uwzględnia scenariusze użycia, funkcje systemu, oraz potencjalne rozwinięcia.

**1.3 Definicje, akronimy oraz skróty używane w dokumencie**

* **Użytkownik głosowy**: Osoba znajdująca się wewnątrz pojazdu, która może komunikować się z Asystentem AI w celu uzyskania informacji o stanie pojazdu lub korzystania z jego funkcji bez ingerencji w jego rdzenne oprogramowanie.
* **Właściciel pojazdu**: Osoba z najwyższymi uprawnieniami do systemu, która ma dostęp do historii poleceń, możliwość konfiguracji i zarządzania systemem. Może dokonywać fizycznych zmian na oprogramowaniu samochodu.
* **Samochód**: Pojazd wyposażony w system "Raven", zdolny do udostępniania danych o swoich parametrach za pomocą magistrali CAN.
* **Raven**: Asystent AI utożsamiający się z pojazdem, zaprojektowany do prowadzenia interakcji głosowych. Raven nie tylko dostarcza informacji o stanie technicznym pojazdu, ale także symuluje osobowość pojazdu, umożliwiając bardziej naturalną i przyjazną komunikację.

## Opis

**2.1 Cel systemu**

Celem systemu "Raven" jest ułatwienie interakcji z pojazdem poprzez wykorzystanie technologii AI do zapewnienia użytkownikom (kierowcy i pasażerom) funkcji głosowego asystenta.

**2.2 Kluczowe cechy systemu**

1. Aktywacja głosowa za pomocą komendy "Hej Raven".
2. Integracja z magistralą CAN w celu odczytu danych o stanie pojazdu, między innymi takich jak:
   * Prędkość.
   * Obroty silnika.
   * Temperatura w kabinie i silniku.
   * Ustawienia klimatyzacji.
   * Informacje diagnostyczne.

**2.3 Opis technologii oraz architektury systemu**

* Sprzęt: Raspberry Pi 2 Zero.
* Oprogramowanie:
  + Python z biblioteką Python-CAN do komunikacji z magistralą CAN.
  + OpenAI ChatGPT jako silnik przetwarzania języka naturalnego.
  + Raspberry Pi OS Lite jako system operacyjny.
* Komunikacja:
  + Połączenie z magistralą CAN za pomocą adaptera CAN.
  + Mikrofon i głośnik jako główny interfejs użytkownika.
  + Brak wizualnych elementów interfejsu (ekranów).
* Tryb pracy:
  + System działa w trybie ciągłego nasłuchu.
  + Aktywacja po wykryciu frazy "Hej Raven".

## 3. Funkcje asystenta i działanie aplikacji

**3.1 Główne funkcje**

1. **Aktywacja głosowa**: Nasłuchiwanie komendy aktywującej i przejście w tryb interakcji.
2. **Odczyt danych z pojazdu**:
   * Prędkość, obroty, temperatura, ustawienia klimatyzacji, kody diagnostyczne.
3. **Interakcja dialogowa**:
   * Odpowiedzi na pytania dotyczące stanu pojazdu.
   * Informacje o konieczności serwisowania.

**3.2 Scenariusz użycia**

1. Użytkownik mówi: *"Hej Raven"*.
2. System uruchamia tryb rozmowy: *"Cześć! W czym mogę pomóc?"*.
3. Użytkownik pyta: *"Jaka jest temperatura w kabinie?"*.
4. System odpowiada: *"Temperatura w kabinie wynosi 21°C. Czy chcesz zmienić ustawienia klimatyzacji?"*.
5. Użytkownik wydaje kolejne polecenie lub kończy interakcję.

**3.3** **Architektura systemu i wybór technologii**

* **Sprzęt**: Raspberry Pi 2 Zero jako główny procesor obsługujący AI oraz połączenie z magistralą CAN.
* **Oprogramowanie**:
  + **Backend**: Python z bibliotekami dla magistrali CAN (np. Python-CAN) oraz integracja API OpenAI dla obsługi modelu ChatGPT.
  + **Frontend**: Prosty interfejs głosowy obsługiwany przez mikrofon i głośniki.
  + **System operacyjny**: Raspberry Pi OS Lite.
* **Interfejs komunikacyjny**: Protokół CAN do odczytu i wysyłania danych.

**3.4 Interfejs użytkownika**

Komunikacja z Asystentem AI odbywa się wyłącznie za pomocą głosu. System wykorzystuje mikrofon do nasłuchu komend i głośnik do przekazywania odpowiedzi. Nie przewiduje się interfejsu wizualnego, takiego jak ekrany czy wyświetlacze.

**3.5 Zabezpieczenia przed niebezpiecznymi promptami użytkownika**

System "Raven" posiada mechanizmy zabezpieczające przed potencjalnie niebezpiecznymi komendami, które mogłyby zaszkodzić użytkownikom lub pojazdowi, takie jak:

* Ignorowanie poleceń, które mogłyby wpływać na bezpośrednie sterowanie pojazdem, np. *"Ustaw moc wciśnięcia pedału gazu na 100%"*.
* Automatyczne wyłączanie odpowiedzi na komendy przekraczające uprawnienia użytkownika.
* Informowanie użytkownika, że próba wykonania danej komendy jest niemożliwa: *"Nie mogę tego zrobić dla bezpieczeństwa Twojego i pojazdu."*.

**3.6 Zabezpieczenia przed potencjalnymi atakami cybernetycznymi**

System "Raven" wykorzystuje szereg środków ochrony przed zagrożeniami zewnętrznymi:

* **Szyfrowanie komunikacji**: Dane przesyłane między systemem a magistralą CAN są szyfrowane, aby uniemożliwić ich przechwycenie.
* **Autoryzacja dostępu**: System wymaga autoryzacji dla wszelkich zewnętrznych prób komunikacji z systemem, blokując nieuprawnione urządzenia.
* **Monitorowanie aktywności**: System rejestruje wszelkie próby nieautoryzowanego dostępu i informuje użytkownika o podejrzanych działaniach.
* **Zabezpieczenia fizyczne**: Porty komunikacyjne są chronione przed nieautoryzowanym dostępem fizycznym.

**3.7 Obsługa i pomoc użytkownikowi**

W sytuacjach, gdy użytkownik nie wie, jak korzystać z systemu, "Raven" oferuje funkcje pomocnicze:

* **Tryb samouczka**: System może wyjaśniać swoje funkcje po aktywacji komendą *"Pomóż mi"* lub podobną.
* **Dynamiczne wskazówki**: Podpowiedzi i sugestie dostosowane do kontekstu, np. *"Możesz zapytać o prędkość pojazdu lub ustawić temperaturę w kabinie."*.
* **Wsparcie w błędach**: W razie niejasnej lub nieprawidłowej komendy system odpowiada: *"Nie rozumiem. Możesz spróbować powiedzieć: 'Hej Raven, ustaw temperaturę na 22°C'."*.

**3.8 Zapisywanie danych i dostęp do historii**

System "Raven" przechowuje historię wszystkich wydanych poleceń oraz odpowiedzi udzielonych przez asystenta w bazie danych. Dane te są dostępne wyłącznie dla użytkowników posiadających uprawnienia właściciela pojazdu.

**Funkcjonalność zapisu i dostępu:**

* **Rejestrowanie poleceń**: Wszystkie wydane komendy głosowe oraz odpowiedzi systemu są zapisywane z oznaczeniem czasu w specjalnej tabeli w bazie danych.
* **Dostęp do historii**: Na żądanie użytkownika z odpowiednimi uprawnieniami (np. właściciela), system może udostępnić logi w formie przeglądu głosowego lub tekstowego. System zapisuje komendy użyte przez użytkownika, odpowiedź asystenta, jego realne działanie, date oraz dokładną godzine w formacie HH:MM:SS wykonania.
* **Przykładowa komenda**: *"Hej Raven, pokaż historię poleceń z dzisiejszego dnia."*.

**3.9 Autoryzacja głosowa**

System "Raven" wykorzystuje zaawansowaną autoryzację głosową, aby zapewnić dostęp do funkcji zarezerwowanych dla użytkowników o odpowiednich uprawnieniach.

**Proces autoryzacji:**

1. **Rozpoznanie frazy aktywacyjnej**: System identyfikuje użytkownika na podstawie wzorca głosu oraz imienia.
2. **Hasło głosowe**: Użytkownik wypowiada wcześniej zdefiniowane hasło.
3. **Weryfikacja tożsamości**: System wybiera losowo jedno pytanie z zestawu 10 zapisanych podczas konfiguracji (np. *"Jak nazywa się Twój ulubiony film?"*).
4. **Oczekiwanie na odpowiedź**: Użytkownik musi podać poprawną odpowiedź zgodną z zapisem w bazie danych.
5. **Przyznanie dostępu**: Po poprawnym przejściu procesu, użytkownik uzyskuje dostęp do funkcji właściciela, np. przeglądania historii poleceń.

**Bezpieczeństwo autoryzacji:**

* W przypadku nieudanej próby system wyłącza dostęp po trzech błędnych odpowiedziach. Wymaga pełnego restartu.
* Informacja o próbie logowania jest zapisywana w logach systemowych.

**Przykład interakcji:**

1. Użytkownik: *"Hej Raven, uzyskaj dostęp właściciela."*
2. Raven: *"Oczywiście, proszę podaj hasło."*
3. Użytkownik: *"Raven123."*
4. Raven: *"Jak nazywa się Twoje ulubione miasto?"*
5. Użytkownik: *"Barcelona."*
6. Raven: *"Autoryzacja zakończona sukcesem. W czym mogę pomóc?"*

**3.10 Sposób zasilania i funkcjonowania systemu**

System "Raven" jest zasilany przez pojazd, poprzez połączenie Raspberry Pi z linią 12V samochodu. Gdy kierowca przekręci kluczyk na pozycję zapłonu, samochód dostaje zasilanie, co włącza Raspberry Pi. Po poprawnym uruchomieniu, system operacyjny Raspberry Pi OS Lite uruchamia automatycznie skrypt w Pythonie, który obsługuje system "Raven".

**Przebieg działania systemu:**

1. **Włączenie systemu**: Po uzyskaniu zasilania, Raspberry Pi automatycznie uruchamia skrypt odpowiedzialny za aktywację "Raven".
2. **Przywitanie użytkownika**: Po uruchomieniu, "Raven" powita użytkownika głosowo i poinformuje go o gotowości systemu: *"Witaj. Jestem gotowa do jazdy!"*
3. **Funkcjonowanie systemu**: System "Raven" pozostaje aktywny i działa w tle, umożliwiając komunikację z użytkownikiem oraz monitorowanie parametrów pojazdu.
4. **Wyłączenie systemu**: Gdy użytkownik gasi silnik pojazdu, system "Raven" pyta, czy chce zostać wyłączony: *"Czy chcesz wyłączyć system Raven przed opuszczeniem pojazdu?"*
5. **Wyłączenie zasilania**: Po potwierdzeniu wyłączenia systemu przez użytkownika, możliwe jest bezpieczne wyjęcie kluczyka i odłączenie zasilania w samochodzie, kończąc tym samym działanie systemu.

System działa w sposób automatyczny, synchronizując się z działaniem pojazdu, zapewniając wygodę użytkowania i bezpieczeństwo.

**3.11 Potencjalne rozszerzenia**

* Dodanie wsparcia dla rozpoznawania kontekstu (np. analiza historii użytkowania).
* Obsługa wielojęzyczna.
* Wsparcie dla integracji ze smartfonem lub aplikacjami mobilnymi.
* Wsparcie z systemem Android Auto / Apple Car – systemem infotainment.

## Schematy

**4.1 Diagram UML**

