**RE-SOM FOTA**

**Software Requirements Specification (SRS)**

**(Version 1.0.0)**

|  |  |  |  |
| --- | --- | --- | --- |
| S.No | Prepared By | Review By | Version No |
| 1 | Venu | Hareesha/Aparna | 1.0.0 |
| 2 | Jayanth | Hareesha/Aparna | 1.0.0 |
| 3 | Varshitha | Hareesha/Aparna | 1.0.0 |

**Table of Contents**

**1.Introduction3**

**2.System Overview3**

**3.Functional Requirements 3**

**3.1 Update Management3**

**3.2 Update Deployment4**

**3.3. Safety and Security4**

**4.Non-Functional Requirements 4**

**5.Compatibility Requirements 4**

**6.Security Requirements 5**

**7.External Interface Requirements 5**

**1. Introduction**

This document outlines the Software Requirements Specification (SRS) for the Firmware Over-The-Air (FOTA) System designed to enable seamless, secure, and efficient firmware updates for Electronic Control Units (ECUs) within automotive systems. FOTA technology allows for updates to be distributed and installed over wireless networks, eliminating the need for manual intervention or physical access to the devices. The FOTA system provides a comprehensive solution for updating the firmware of ECUs in vehicles, including the Body Control Module (BCM), Anti-lock Braking System (ABS), and Head Unit. It supports automatic updates with minimal user interaction, ensuring that devices remain up-to-date with the latest features and security enhancements.

**2. System Overview**

The FOTA system consists of the following components:

* **OTA Bundle Management**: Handles firmware/software and manifest files, digital signatures, configuration files, and validation mechanisms.
* **Firmware Update Management**: Manages the download, extraction, validation, and deployment of firmware updates.
* **UDS Flow Configuration**: Configures the Unified Diagnostic Services (UDS) protocol for pre-programming, data-block programming, post-programming, and failed programming recovery procedures.
* **OEM Backend:** This server-side component, managed by the Original Equipment Manufacturer (OEM), is responsible for managing updates, devices, and campaigns.

**3. Functional Requirements**

* 1. **Update Management:**
  + The system shall receive notifications from the OEM backend regarding available firmware updates.
  + The system shall download update packages securely over a wireless network (Wi-Fi or cellular).
  + The system shall validate the integrity and authenticity of downloaded updates using digital signatures and checksums.
  + The system shall allow manual or automatic (using MDM) initiation of the update process.

**3.2 Update Deployment:**

* + The system shall communicate with vehicle ECUs using diagnostic messages over CAN bus.
  + The system shall deploy firmware updates to specific ECUs based on the update package.
  + The system shall perform rollback to the previous firmware version in case of update failures.

**3.3 Safety and Security:**

* + The system shall ensure a safe update process, avoiding interruptions while driving.
  + The system shall encrypt update packages during transfer to prevent tampering.
  + The system shall authenticate updates to prevent unauthorized modifications.

**4.** **Non-Functional Requirements**

* **Performance:**
  + The update download time shall be minimized based on available network bandwidth.
  + The update deployment time shall be efficient to minimize downtime.
* **Reliability:**
  + The system shall be reliable and handle potential network interruptions during downloads.
  + The system shall have mechanisms to recover from update failures.
* **Usability:**
  + The system shall provide clear user instructions for manual updates.
  + The update process shall be minimally disruptive to the user experience.

**5. Compatibility Requirements**

* The system shall support updates for specific ECUs: Body Control Module (BCM), Anti-lock Braking System (ABS), and Head Unit.
* The system shall require a minimum battery level (e.g., 30%) and signal strength (e.g., 60%) before starting an update.
* The system shall not allow updates while roaming on cellular networks (configurable).

**6. Security Requirements**

* Update packages shall be encrypted during transmission.
* Authentication shall be required before applying updates.
* Downloaded update files shall be validated using checksums.
* Update events shall be logged for troubleshooting and monitoring.
* Update reports shall be sent to a designated server (configurable).

**7. External Interface Requirements**

* OEM Backend Integration: For update management, device management, and campaign management.
* Cloud Services: Utilizes cloud platforms like Firebase for real-time update notifications and update file distribution.
* Vehicle Communication Protocols: Interacts with vehicle ECUs via diagnostic CAN messages for firmware deployment.