Documento de Requerimientos de Software (SRS)

Sistema: Firmware para Sistema de Comunicación IoT Industrial

# 1. Introducción y Alcance

## 1.1 Propósito del documento

Este documento especifica los requerimientos funcionales y no funcionales del firmware diseñado para gestionar un sistema de comunicación inalámbrica en un entorno de manufactura industrial mediante tecnología IoT. Sirve como base para el desarrollo, validación y mantenimiento del sistema.

## 1.2 Alcance del sistema

El sistema se centra en:  
- Recolección de datos desde sensores remotos.  
- Transmisión segura y en tiempo real al servidor central.  
- Operación bajo condiciones industriales exigentes.  
- Prolongación de la autonomía energética de los dispositivos remotos.

# 2. Descripción General del Sistema

## 2.1 Perspectiva del sistema

Este firmware se ejecutará en microcontroladores ARM de bajo consumo instalados en nodos sensores. Se conectará con un servidor central a través de un protocolo MQTT sobre red inalámbrica, permitiendo supervisión y control de procesos industriales.

## 2.2 Funciones del sistema

- Recolección de datos desde sensores.  
- Transmisión inalámbrica mediante MQTT.  
- Corrección de errores y cifrado.  
- Operación en modo de bajo consumo.  
- Actualización remota del firmware.

## 2.3 Características del usuario

El sistema será operado por personal técnico de mantenimiento e ingenieros de planta. No requiere interacción directa del usuario final en los nodos sensores, pero sí desde la plataforma de monitoreo.

# 3. Requerimientos Funcionales

|  |  |  |
| --- | --- | --- |
| ID | Requerimiento Funcional | Descripción |
| RF1 | Transmisión de datos | El sistema debe transmitir los datos recolectados por sensores al servidor en tiempo real. |
| RF2 | Uso de MQTT | El sistema debe utilizar el protocolo MQTT para comunicación eficiente. |
| RF3 | Corrección de errores | El firmware debe detectar y corregir errores durante la transmisión. |
| RF4 | Cifrado de datos | El sistema debe cifrar los datos transmitidos con AES-128. |
| RF5 | Gestión energética | El firmware debe permitir operación en modo de bajo consumo. |
| RF6 | Operación intermitente | Los nodos deben poder despertar, transmitir datos y volver a reposo automáticamente. |
| RF7 | Almacenamiento temporal | En caso de pérdida de conexión, los datos deben almacenarse y enviarse luego. |
| RF8 | Actualización remota | El firmware debe permitir ser actualizado remotamente por el servidor. |

# 4. Requerimientos No Funcionales

|  |  |  |
| --- | --- | --- |
| ID | Requerimiento No Funcional | Descripción |
| RNF1 | Tiempo de respuesta | El sistema debe transmitir datos críticos con una latencia menor a 1 segundo. |
| RNF2 | Consumo energético | El sistema debe permitir operación por al menos 12 meses con una batería estándar. |
| RNF3 | Robustez ante interferencias | El sistema debe operar en entornos con alta interferencia electromagnética. |
| RNF4 | Seguridad | El sistema debe implementar cifrado AES-128 y protección contra ataques externos. |
| RNF5 | Memoria limitada | El firmware no debe superar los 256 KB de memoria flash. |
| RNF6 | Escalabilidad | Debe soportar hasta 100 nodos sin comprometer el rendimiento. |
| RNF7 | Conformidad | Cumplir con normativas como IEC 62443 y recomendaciones MISRA C. |

# 5. Suposiciones y Dependencias

- Se asume que la red inalámbrica está disponible en la planta.  
- Se dispone de un servidor MQTT configurado y en funcionamiento.  
- Los microcontroladores utilizados cumplen con las especificaciones mínimas de hardware.  
- Los sensores entregan datos en formatos compatibles con el firmware.  
- El sistema depende del correcto funcionamiento de las baterías.

# 6. Criterios de Aceptación y Validación

- CA1: Los datos deben llegar al servidor con una tasa de error menor al 1%.  
- CA2: La autonomía del nodo debe ser superior a 12 meses en operación típica.  
- CA3: El firmware debe funcionar correctamente en pruebas de interferencia simulada.  
- CA4: Las actualizaciones deben aplicarse remotamente sin pérdida de datos.  
- CA5: Los datos deben estar cifrados al ser capturados por herramientas de red.

Coreccion

|  |  |  |
| --- | --- | --- |
| **Observación del Stakeholder** | **Requerimiento Afectado** | **Ajuste Propuesto** |
| El protocolo de actualización remota no está definido. | RF8 | Especificar que debe usar un canal seguro como HTTPS o OTA con firma digital. |
| ¿Qué pasa si hay más de 100 nodos? | RNF6 | Indicar que la escalabilidad puede ser extendida si se optimiza la arquitectura MQTT. |
| Falta claridad sobre tipo de cifrado | RF4 / RNF4 | Añadir que se usará AES-128 en modo CBC o GCM con gestión de claves. |

**Trazabilidad:**

|  |
| --- |

|  |
| --- |
|  |

|  |  |
| --- | --- |
| **Objetivo del Caso de Estudio** | **Requerimientos Asociados** |
| Transmisión segura de datos | RF1, RF2, RF4, RNF4 |
| Operación en entornos industriales hostiles | RF3, RNF3, RNF5 |
| Ahorro energético | RF5, RF6, RNF2 |
| Actualización y mantenimiento remoto | RF8, RNF7 |
| Soporte para múltiples sensores | RNF6, RF7 |