Table of Contents

# INTERFACES CTC-ITCS - PROTOCOLO FFFIS

## APP La Dorada-Chiriguaná - Comunicación entre Sistemas

**Estado:** 🔄 **EN DESARROLLO - FASE 1 CRÍTICA**  
**Fecha:** 27 de Enero, 2025  
**Responsable:** Ing. Integración - EPC  
**Especialista:** Especialista Senior en Control de Trenes  
**Estándar Base:** CENELEC EN 50159, UIC 438, Protocolo FFFIS

## 🎯 **PROPÓSITO Y ALCANCE**

### **1.1 PROPÓSITO**

Este documento define las **interfaces de comunicación entre CTC e ITCS** usando el **protocolo FFFIS (Form Fit Function Interface Specification)** para garantizar interoperabilidad segura y confiable entre sistemas de control ferroviario.

### **1.2 ALCANCE**

Las interfaces CTC-ITCS cubrirán: - **Comunicación bidireccional** entre Centro de Control y Radio Block Center - **Intercambio de información** de autorizaciones de movimiento - **Coordinación operacional** en tiempo real - **Gestión de alarmas** y eventos críticos - **Integración segura** según estándares CENELEC

### **1.3 REFERENCIAS NORMATIVAS**

* **CENELEC EN 50159:** Comunicación segura en sistemas ferroviarios
* **UIC 438:** Especificaciones técnicas ETCS Level 2
* **IEC 62280:** Seguridad en comunicaciones ferroviarias
* **EN 50128:** Software para sistemas de control ferroviario

## 📡 **ARQUITECTURA DE COMUNICACIÓN**

### **2.1 ARQUITECTURA GENERAL**

#### **2.1.1 DIAGRAMA DE INTERFACES**

ARQUITECTURA CTC-ITCS INTERFACES  
┌─────────────────────────────────────────────────────────────────┐  
│ CENTRO DE CONTROL CTC │  
│ │  
│ ┌─────────────────────────────────────────────────────────┐ │  
│ │ CTC APPLICATION LAYER │ │  
│ │ │ │  
│ │ ┌─────────┐ ┌─────────┐ ┌─────────┐ ┌─────────┐ │ │  
│ │ │ Traffic │ │ Signal │ │ Safety │ │ Monitor │ │ │  
│ │ │ Control │ │ Control │ │ Control │ │ System │ │ │  
│ │ └─────────┘ └─────────┘ └─────────┘ └─────────┘ │ │  
│ └─────────────────────────────────────────────────────────┘ │  
│ │ │  
│ ┌─────────────────────────────────────────────────────────┐ │  
│ │ CTC COMMUNICATION LAYER │ │  
│ │ │ │  
│ │ ┌─────────┐ ┌─────────┐ ┌─────────┐ ┌─────────┐ │ │  
│ │ │ Protocol│ │Security │ │Message │ │Network │ │ │  
│ │ │ Handler │ │Manager │ │Queue │ │Manager │ │ │  
│ │ └─────────┘ └─────────┘ └─────────┘ └─────────┘ │ │  
│ └─────────────────────────────────────────────────────────┘ │  
└─────────────────────────────────────────────────────────────────┘  
 │  
 │ FFFIS Protocol  
 │  
┌─────────────────────────────────────────────────────────────────┐  
│ RADIO BLOCK CENTER RBC │  
│ │  
│ ┌─────────────────────────────────────────────────────────┐ │  
│ │ RBC COMMUNICATION LAYER │ │  
│ │ │ │  
│ │ ┌─────────┐ ┌─────────┐ ┌─────────┐ ┌─────────┐ │ │  
│ │ │Network │ │Message │ │Security │ │Protocol │ │ │  
│ │ │Manager │ │Queue │ │Manager │ │Handler │ │ │  
│ │ └─────────┘ └─────────┘ └─────────┘ └─────────┘ │ │  
│ └─────────────────────────────────────────────────────────┘ │  
│ │ │  
│ ┌─────────────────────────────────────────────────────────┐ │  
│ │ RBC APPLICATION LAYER │ │  
│ │ │ │  
│ │ ┌─────────┐ ┌─────────┐ ┌─────────┐ ┌─────────┐ │ │  
│ │ │Movement │ │Train │ │Safety │ │System │ │ │  
│ │ │Auth. │ │Superv. │ │Monitor │ │Monitor │ │ │  
│ │ └─────────┘ └─────────┘ └─────────┘ └─────────┘ │ │  
│ └─────────────────────────────────────────────────────────┘ │  
└─────────────────────────────────────────────────────────────────┘

#### **2.1.2 COMPONENTES PRINCIPALES**

COMPONENTES DE INTERFACE:  
  
1. CTC SIDE:  
 - Protocol Handler: Gestión de protocolo FFFIS  
 - Security Manager: Autenticación y cifrado  
 - Message Queue: Cola de mensajes  
 - Network Manager: Gestión de red  
  
2. RBC SIDE:  
 - Network Manager: Gestión de red  
 - Message Queue: Cola de mensajes  
 - Security Manager: Autenticación y cifrado  
 - Protocol Handler: Gestión de protocolo FFFIS  
  
3. COMMUNICATION CHANNEL:  
 - Red Ethernet redundante  
 - Protocolo TCP/IP  
 - Cifrado AES-256  
 - Autenticación mutua

### **2.2 GATEWAY INTEROPERABILIDAD CTC-FENOCO** ⭐ **NUEVO (DT-INTERFACES-001)**

#### **2.2.1 PROTOCOLO UIC 918-4**

El Gateway de interoperabilidad con FENOCO implementa el protocolo UIC 918-4, estándar europeo para intercambio de información operativa entre sistemas ferroviarios.

**Características técnicas:** - **Estándar:** UIC 918-4 (Interface for Operational Information) - **Tipo de Gateway:** Industrial con capacidad multi-protocolo - **Medio físico:** Ethernet redundante sobre fibra óptica - **Seguridad:** IEC 62443 Security Level SL-3 - **Redundancia:** N+1 (Gateway activo + Gateway standby)

#### **2.2.2 FUNCIONES DEL GATEWAY**

1. **Conversión de Protocolos:**
   * CTC nativo (interno) ↔ UIC 918-4 (externo FENOCO)
   * Mapeo de mensajes operativos
   * Normalización de datos de estado de vía
2. **Intercambio de Información Operativa:**
   * Estado de ocupación de vías compartidas
   * Programación de trenes en puntos de interoperabilidad
   * Avisos operativos y restricciones
   * Sincronización de horarios
3. **Gestión de Interfaz:**
   * Autenticación mutua CTC-FENOCO
   * Cifrado de comunicaciones operativas
   * Monitoreo de salud del enlace
   * Log de todas las transacciones

#### **2.2.3 ARQUITECTURA DEL GATEWAY**

CTC APP LA DORADA-CHIRIGUANÁ FENOCO (Red existente)  
┌──────────────────────────┐ ┌──────────────────────┐  
│ │ │ │  
│ CTC Virtual │ │ CTC FENOCO │  
│ (Protocolo propietario) │ │ (Protocolo UIC) │  
│ │ │ │  
└────────────┬─────────────┘ └────────┬─────────────┘  
 │ │  
 │ │  
 ┌────▼───────────────────────────────▼────┐  
 │ │  
 │ GATEWAY UIC 918-4 (Ítem 1.1.106) │  
 │ Bloque Lógico de Integración │  
 │ │  
 │ ┌─────────────────────────────────┐ │  
 │ │ Middleware Interoperabilidad │ │  
 │ │ - Conversión protocolos │ │  
 │ │ - Mapeo de mensajes │ │  
 │ │ - Normalización datos │ │  
 │ └─────────────────────────────────┘ │  
 │ │  
 │ ┌─────────────────────────────────┐ │  
 │ │ Firewall IEC 62443 (SL-3) │ │  
 │ │ - Inspección paquetes │ │  
 │ │ - Control acceso │ │  
 │ └─────────────────────────────────┘ │  
 │ │  
 └─────────────────────────────────────────┘  
 │  
 Fibra Óptica N+1

#### **2.2.4 MENSAJES UIC 918-4 SOPORTADOS**

| Tipo Mensaje | Dirección | Descripción |
| --- | --- | --- |
| **OPR-001** | CTC → FENOCO | Solicitud de autorización operativa |
| **OPR-002** | FENOCO → CTC | Confirmación/rechazo autorización |
| **STA-001** | CTC ↔ FENOCO | Estado de ocupación de vía compartida |
| **TRN-001** | CTC → FENOCO | Programación de tren en punto interoperabilidad |
| **ALR-001** | CTC ↔ FENOCO | Alertas operativas y restricciones |
| **HRT-001** | CTC ↔ FENOCO | Heartbeat / Keep-alive |

#### **2.2.5 REQUISITOS DE RENDIMIENTO**

* **Latencia máxima:** <200ms end-to-end
* **Disponibilidad:** 99.9% (con redundancia N+1)
* **Throughput:** Mínimo 100 mensajes/minuto
* **Failover automático:** <2 segundos
* **Retención de logs:** 180 días (requisito regulatorio)

**Presupuesto:** Incluido en ítem 1.1.106 - $150.000.000 COP  
**Decisión Técnica:** DT-INTERFACES-001-2025-10-09

## 🔧 **PROTOCOLO FFFIS**

### **3.1 ESPECIFICACIÓN DEL PROTOCOLO**

#### **3.1.1 ESTRUCTURA DE MENSAJES**

ESTRUCTURA MENSAJE FFFIS:  
  
┌─────────────────────────────────────────────────────────┐  
│ HEADER (16 bytes) │  
│ │  
│ ┌─────────┐ ┌─────────┐ ┌─────────┐ ┌─────────┐ │  
│ │Version │ │Type │ │Length │ │Sequence │ │  
│ │(2 bytes)│ │(2 bytes)│ │(4 bytes)│ │(4 bytes)│ │  
│ └─────────┘ └─────────┘ └─────────┘ └─────────┘ │  
│ │  
│ ┌─────────┐ ┌─────────┐ ┌─────────┐ ┌─────────┐ │  
│ │Source │ │Dest │ │Flags │ │Reserved │ │  
│ │(2 bytes)│ │(2 bytes)│ │(2 bytes)│ │(2 bytes)│ │  
│ └─────────┘ └─────────┘ └─────────┘ └─────────┘ │  
└─────────────────────────────────────────────────────────┘  
 │  
┌─────────────────────────────────────────────────────────┐  
│ PAYLOAD (Variable) │  
│ │  
│ ┌─────────────────────────────────────────────────────┐│  
│ │ APPLICATION DATA ││  
│ │ ││  
│ │ - Movement Authority Data ││  
│ │ - Train Status Information ││  
│ │ - Safety Alerts ││  
│ │ - System Status ││  
│ └─────────────────────────────────────────────────────┘│  
└─────────────────────────────────────────────────────────┘  
 │  
┌─────────────────────────────────────────────────────────┐  
│ TRAILER (8 bytes) │  
│ │  
│ ┌─────────┐ ┌─────────┐ ┌─────────┐ ┌─────────┐ │  
│ │Checksum │ │CRC32 │ │Timestamp│ │Reserved │ │  
│ │(2 bytes)│ │(4 bytes)│ │(2 bytes)│ │(2 bytes)│ │  
│ └─────────┘ └─────────┘ └─────────┘ └─────────┘ │  
└─────────────────────────────────────────────────────────┘

#### **3.1.2 TIPOS DE MENSAJES**

TIPOS DE MENSAJES FFFIS:  
  
1. MOVEMENT AUTHORITY (MA):  
 - Tipo: 0x0001  
 - Dirección: CTC → RBC  
 - Contenido: Autorización de movimiento  
 - Frecuencia: Por cada autorización  
 - Prioridad: Alta  
  
2. TRAIN STATUS (TS):  
 - Tipo: 0x0002  
 - Dirección: RBC → CTC  
 - Contenido: Estado del tren  
 - Frecuencia: Cada 10 segundos  
 - Prioridad: Media  
  
3. SAFETY ALERT (SA):  
 - Tipo: 0x0003  
 - Dirección: Bidireccional  
 - Contenido: Alerta de seguridad  
 - Frecuencia: Por evento  
 - Prioridad: Crítica  
  
4. SYSTEM STATUS (SS):  
 - Tipo: 0x0004  
 - Dirección: Bidireccional  
 - Contenido: Estado del sistema  
 - Frecuencia: Cada 30 segundos  
 - Prioridad: Baja  
  
5. EMERGENCY STOP (ES):  
 - Tipo: 0x0005  
 - Dirección: CTC → RBC  
 - Contenido: Comando de parada  
 - Frecuencia: Por evento  
 - Prioridad: Crítica  
  
6. CONFIGURATION (CF):  
 - Tipo: 0x0006  
 - Dirección: CTC → RBC  
 - Contenido: Configuración  
 - Frecuencia: Por cambio  
 - Prioridad: Media

### **3.2 PROCESAMIENTO DE MENSAJES**

#### **3.2.1 FLUJO DE COMUNICACIÓN**

FLUJO DE COMUNICACIÓN CTC-ITCS:  
  
1. ENVÍO DE MENSAJE (CTC → RBC):  
 - Aplicación CTC genera mensaje  
 - Protocol Handler encapsula en FFFIS  
 - Security Manager cifra y autentica  
 - Network Manager envía por TCP/IP  
 - RBC recibe y valida mensaje  
  
2. PROCESAMIENTO EN RBC:  
 - Network Manager recibe mensaje  
 - Security Manager valida y descifra  
 - Protocol Handler extrae datos  
 - Aplicación RBC procesa información  
 - RBC genera respuesta si es necesaria  
  
3. RESPUESTA (RBC → CTC):  
 - Aplicación RBC genera respuesta  
 - Protocol Handler encapsula en FFFIS  
 - Security Manager cifra y autentica  
 - Network Manager envía por TCP/IP  
 - CTC recibe y procesa respuesta

#### **3.2.2 GESTIÓN DE ERRORES**

GESTIÓN DE ERRORES:  
  
1. ERRORES DE COMUNICACIÓN:  
 - Timeout: 5 segundos  
 - Reintentos: 3 intentos  
 - Escalación: Alerta al operador  
 - Recuperación: Reconexión automática  
  
2. ERRORES DE PROTOCOLO:  
 - Mensaje corrupto: Descarte y solicitud de retransmisión  
 - Secuencia incorrecta: Reordenamiento de mensajes  
 - Checksum inválido: Validación y retransmisión  
 - CRC32 inválido: Descarte y alerta  
  
3. ERRORES DE SEGURIDAD:  
 - Autenticación fallida: Bloqueo temporal  
 - Cifrado inválido: Descarte de mensaje  
 - Timestamp incorrecto: Validación de tiempo  
 - Certificado expirado: Renovación automática

## 🔒 **SEGURIDAD DE COMUNICACIÓN**

### **4.1 AUTENTICACIÓN Y AUTORIZACIÓN**

#### **4.1.1 AUTENTICACIÓN MUTUA**

AUTENTICACIÓN MUTUA:  
  
1. INTERCAMBIO DE CERTIFICADOS:  
 - CTC envía certificado digital  
 - RBC valida certificado CTC  
 - RBC envía certificado digital  
 - CTC valida certificado RBC  
 - Establecimiento de sesión segura  
  
2. ALGORITMO DE AUTENTICACIÓN:  
 - Algoritmo: RSA-2048  
 - Hash: SHA-256  
 - Firma digital: PKCS#1 v1.5  
 - Validez: 1 año  
 - Renovación: Automática  
  
3. GESTIÓN DE CERTIFICADOS:  
 - Autoridad certificadora: ICA (Internal CA)  
 - Almacenamiento: HSM (Hardware Security Module)  
 - Backup: Redundante en 3 ubicaciones  
 - Revocación: Lista de certificados revocados

#### **4.1.2 AUTORIZACIÓN DE ACCESO**

AUTORIZACIÓN DE ACCESO:  
  
1. ROLES Y PERMISOS:  
 - CTC Operator: Lectura/escritura completa  
 - RBC Operator: Lectura/escritura limitada  
 - Maintenance: Solo lectura  
 - Administrator: Acceso completo  
  
2. CONTROL DE ACCESO:  
 - Lista de control de acceso (ACL)  
 - Validación de permisos por mensaje  
 - Logging de accesos  
 - Auditoría de cambios  
  
3. GESTIÓN DE SESIONES:  
 - Timeout: 30 minutos de inactividad  
 - Renovación: Automática cada 15 minutos  
 - Cierre: Automático al finalizar  
 - Monitoreo: Continuo de sesiones activas

### **4.2 CIFRADO Y INTEGRIDAD**

#### **4.2.1 CIFRADO DE DATOS**

CIFRADO DE DATOS:  
  
1. ALGORITMO DE CIFRADO:  
 - Algoritmo: AES-256-GCM  
 - Modo: Galois/Counter Mode (GCM)  
 - Longitud de clave: 256 bits  
 - Vector de inicialización: 96 bits  
 - Tag de autenticación: 128 bits  
  
2. GESTIÓN DE CLAVES:  
 - Generación: HSM (Hardware Security Module)  
 - Distribución: Protocolo seguro  
 - Rotación: Cada 24 horas  
 - Almacenamiento: HSM cifrado  
 - Backup: Redundante y cifrado  
  
3. IMPLEMENTACIÓN:  
 - Hardware: Aceleración por CPU  
 - Software: OpenSSL 3.0  
 - Validación: FIPS 140-2 Level 3  
 - Rendimiento: < 1ms por mensaje

#### **4.2.2 INTEGRIDAD DE DATOS**

INTEGRIDAD DE DATOS:  
  
1. ALGORITMO DE INTEGRIDAD:  
 - Hash: SHA-256  
 - HMAC: HMAC-SHA256  
 - Checksum: CRC32  
 - Firma: RSA-2048  
  
2. VALIDACIÓN DE INTEGRIDAD:  
 - Checksum: Validación rápida  
 - CRC32: Detección de errores  
 - HMAC: Autenticación de mensaje  
 - Firma digital: No repudio  
  
3. PROTECCIÓN CONTRA ATAQUES:  
 - Replay attacks: Timestamp y nonce  
 - Man-in-the-middle: Certificados mutuos  
 - Tampering: Múltiples validaciones  
 - Denial of service: Rate limiting

## 📊 **ESPECIFICACIONES TÉCNICAS**

### **5.1 ESPECIFICACIONES DE RED**

#### **5.1.1 CONFIGURACIÓN DE RED**

CONFIGURACIÓN DE RED:  
  
1. TOPOLOGÍA:  
 - Tipo: Red Ethernet redundante  
 - Protocolo: TCP/IP  
 - Velocidad: 1 Gbps  
 - Latencia: < 10 ms  
 - Jitter: < 1 ms  
  
2. DIRECCIONAMIENTO:  
 - CTC: 192.168.100.10/24  
 - RBC: 192.168.100.20/24  
 - Gateway: 192.168.100.1/24  
 - DNS: 192.168.100.2/24  
  
3. REDUNDANCIA:  
 - Enlaces: 2 enlaces redundantes  
 - Switches: 2 switches en stack  
 - Conmutación: Automática < 1 segundo  
 - Monitoreo: Continuo de enlaces

#### **5.1.2 PROTOCOLO TCP/IP**

CONFIGURACIÓN TCP/IP:  
  
1. PARÁMETROS TCP:  
 - Puerto: 50000 (configurable)  
 - Buffer size: 64 KB  
 - Keep-alive: 60 segundos  
 - Timeout: 30 segundos  
 - Retransmisión: 3 intentos  
  
2. PARÁMETROS IP:  
 - TTL: 64  
 - TOS: 0x10 (precedencia)  
 - Fragmentación: Deshabilitada  
 - ICMP: Habilitado para diagnóstico  
  
3. OPTIMIZACIÓN:  
 - TCP\_NODELAY: Habilitado  
 - SO\_KEEPALIVE: Habilitado  
 - SO\_REUSEADDR: Habilitado  
 - Buffer tuning: Optimizado

### **5.2 ESPECIFICACIONES DE RENDIMIENTO**

#### **5.2.1 MÉTRICAS DE RENDIMIENTO**

MÉTRICAS DE RENDIMIENTO:  
  
1. LATENCIA:  
 - Objetivo: < 100 ms  
 - Medición: Tiempo de ida y vuelta  
 - Frecuencia: Cada mensaje  
 - Alerta: > 200 ms  
  
2. THROUGHPUT:  
 - Objetivo: > 1000 mensajes/segundo  
 - Medición: Mensajes por segundo  
 - Frecuencia: Cada minuto  
 - Alerta: < 500 mensajes/segundo  
  
3. DISPONIBILIDAD:  
 - Objetivo: > 99.9%  
 - Medición: Uptime/tiempo total  
 - Frecuencia: Diaria  
 - Alerta: < 99.5%  
  
4. ERROR RATE:  
 - Objetivo: < 0.1%  
 - Medición: Errores/mensajes totales  
 - Frecuencia: Cada hora  
 - Alerta: > 0.5%

#### **5.2.2 OPTIMIZACIÓN DE RENDIMIENTO**

OPTIMIZACIÓN DE RENDIMIENTO:  
  
1. BUFFER MANAGEMENT:  
 - Buffer size: 64 KB  
 - Pool de buffers: 100 buffers  
 - Reutilización: Automática  
 - Limpieza: Periódica  
  
2. THREADING:  
 - Threads de red: 4 threads  
 - Threads de procesamiento: 8 threads  
 - Thread pool: Dinámico  
 - Prioridad: SCHED\_FIFO  
  
3. MEMORY MANAGEMENT:  
 - Memory pool: Pre-allocated  
 - Garbage collection: Manual  
 - Memory mapping: mmap()  
 - Cache: LRU algorithm

## 🔧 **PLAN DE IMPLEMENTACIÓN**

### **6.1 FASES DE DESARROLLO**

#### **6.1.1 FASE 1: ESPECIFICACIÓN (2 semanas)**

TAREA RESPONSABLE PLAZO  
Especificación protocolo Ing. Integración 1 semana  
Especificación seguridad Ing. Seguridad 1 semana  
Especificación red Ing. Redes 1 semana

#### **6.1.2 FASE 2: DISEÑO (3 semanas)**

TAREA RESPONSABLE PLAZO  
Diseño software Ing. Software 2 semanas  
Diseño hardware Ing. Hardware 1 semana  
Diseño de pruebas Ing. Calidad 1 semana

#### **6.1.3 FASE 3: IMPLEMENTACIÓN (6 semanas)**

TAREA RESPONSABLE PLAZO  
Desarrollo software Proveedor SW 4 semanas  
Integración hardware Proveedor HW 2 semanas  
Integración sistemas Ing. Integración 2 semanas

### **6.2 CRONOGRAMA CRÍTICO**

SEMANA 1-2: Especificación detallada  
SEMANA 3-5: Diseño arquitectural  
SEMANA 6-11: Implementación  
SEMANA 12-14: Pruebas FAT  
SEMANA 15-17: Pruebas SAT  
SEMANA 18-19: Puesta en servicio

## 📊 **MÉTRICAS Y MONITOREO**

### **7.1 MÉTRICAS DE COMUNICACIÓN**

| Métrica | Objetivo | Medición | Frecuencia |
| --- | --- | --- | --- |
| **Latencia** | ≤ 100ms | Tiempo ida y vuelta | Por mensaje |
| **Throughput** | ≥ 1000 msg/s | Mensajes por segundo | Cada minuto |
| **Disponibilidad** | ≥ 99.9% | Uptime/Tiempo total | Diaria |
| **Error rate** | ≤ 0.1% | Errores/Mensajes totales | Cada hora |

### **7.2 MÉTRICAS DE SEGURIDAD**

| Métrica | Objetivo | Medición | Frecuencia |
| --- | --- | --- | --- |
| **Autenticación** | 100% | Intentos exitosos | Cada hora |
| **Cifrado** | 100% | Mensajes cifrados | Cada hora |
| **Integridad** | 100% | Validaciones exitosas | Cada hora |
| **Certificados** | 100% | Certificados válidos | Diaria |

### **7.3 SISTEMA DE MONITOREO**

#### **7.3.1 HERRAMIENTAS DE MONITOREO**

HERRAMIENTAS IMPLEMENTADAS:  
  
1. PROMETHEUS + GRAFANA:  
 - Métricas de rendimiento  
 - Dashboards personalizados  
 - Alertas automáticas  
 - Análisis de tendencias  
  
2. ELK STACK:  
 - Logging centralizado  
 - Análisis de logs  
 - Búsqueda avanzada  
 - Correlación de eventos  
  
3. ZABBIX:  
 - Monitoreo de infraestructura  
 - Alertas de hardware  
 - Monitoreo de red  
 - Disponibilidad de servicios

#### **7.3.2 ALERTAS CRÍTICAS**

CONFIGURACIÓN DE ALERTAS:  
  
CRÍTICAS (INMEDIATAS):  
- Pérdida de comunicación  
- Fallo de autenticación  
- Error de cifrado  
- Pérdida de integridad  
  
ALTAS (5 MINUTOS):  
- Latencia > 200ms  
- Throughput < 500 msg/s  
- Error rate > 0.5%  
- Disponibilidad < 99.5%  
  
MEDIAS (15 MINUTOS):  
- Uso CPU > 80%  
- Uso memoria > 85%  
- Conexiones > 90%  
- Buffer usage > 90%

## 📋 **CONTROL DE VERSIONES**

| Versión | Fecha | Responsable | Descripción |
| --- | --- | --- | --- |
| **v1.1** | 27/01/2025 | Ing. Integración EPC | **Interfaces CTC-ITCS FFFIS** - Fase 1 crítica en desarrollo |
| **v1.0** | 27/01/2025 | Ing. Integración EPC | **Interfaces CTC-ITCS inicial** - Protocolo FFFIS especificado |
| **v0.1** | 27/01/2025 | Admin. Contractual EPC | **Especificaciones provisionales** - Desarrollo inicial |

## ✅ **CONCLUSIONES Y PRÓXIMOS PASOS**

### **🎯 ESTADO ACTUAL**

* ✅ **Interfaces CTC-ITCS especificadas** con protocolo FFFIS
* ✅ **Protocolo de comunicación detallado** con seguridad completa
* ✅ **Especificaciones técnicas** de red y rendimiento
* ✅ **Plan de implementación** con cronograma de 19 semanas

### **🔄 PRÓXIMOS PASOS INMEDIATOS**

1. **Validación técnica** de las interfaces con especialistas
2. **Desarrollo de especificaciones detalladas** de software
3. **Plan de pruebas** para validar comunicación
4. **Implementación de seguridad** y cifrado

### **📞 CONTACTOS**

* **Responsable Técnico:** Ing. Integración EPC
* **Especialista Senior:** Control de Trenes
* **Revisión:** Cada 2 semanas durante desarrollo

**Documento desarrollado según estándares CENELEC EN 50159 y UIC 438**  
**Fecha:** 27 de Enero, 2025  
**Estado:** 🔄 **EN DESARROLLO - FASE 1 CRÍTICA**  
**Próxima actualización:** 3 de Febrero, 2025