



**FACULTAD
DE INGENIERIA**

Universidad de Buenos Aires

Sistema de ensayos de relés ferroviarios de seguridad basado en computación en la nube

Autor:

Ing. Gaspar Santamarina

Director:

Ing. Adrián Laiuppa (CONICET-GICSAFe)

Jurados:

Nombre y Apellido (1) (pertenencia (1))

Nombre y Apellido (2) (pertenencia (2))

Nombre y Apellido (3) (pertenencia (3))

*Este trabajo fue realizado en el curso de Gestión de proyectos
entre el 22 de junio de 2020 y el 22 de Agosto de 2020.*

Índice

Registros de cambios	3
Acta de constitución del proyecto.	4
Descripción técnica-conceptual del Proyecto a realizar	5
Identificación y análisis de los interesados.	7
1. Propósito del proyecto	7
2. Alcance del proyecto	7
3. Supuestos del proyecto.	7
4. Requerimientos	7
5. Entregables principales del proyecto	9
6. Desglose del trabajo en tareas	9
7. Diagrama de Activity On Node	11
8. Diagrama de Gantt.	12
9. Matriz de uso de recursos de materiales	14
10. Presupuesto detallado del proyecto	14
11. Matriz de asignación de responsabilidades	15
12. Gestión de riesgos	15
13. Gestión de la calidad	16
14. Comunicación del proyecto	17
15. Gestión de Compras	17
16. Seguimiento y control.	17
17. Procesos de cierre	18

Registros de cambios

Revisión	Detalles de los cambios realizados	Fecha
1.0	Creación del documento: propósito, alcance, supuestos y tareas	09/07/2020
1.1	Se agrega AoN, diagrama Gantt, matriz de recursos, presupuesto y matriz de responsabilidades	30/07/2020

Acta de constitución del proyecto

Buenos Aires, 22 de junio de 2020

Por medio de la presente se acuerda con el Ing. Ing. Gaspar Santamarina que su Trabajo Final de la Carrera de Especialización en Sistemas Embebidos se titulará “Sistema de ensayos de relés ferroviarios de seguridad basado en computación en la nube”, consistirá esencialmente en el prototipo preliminar de un probador de relés ferroviarios de seguridad, basado en hardware digital, con la posibilidad de ser operado de forma remota, y tendrá un presupuesto preliminar estimado de 687 hs de trabajo, con fecha de inicio 22 de junio de 2020 y fecha de presentación pública 22 de junio de 2021.

Se adjunta a esta acta la planificación inicial.

Ariel Lutenberg
Director posgrado FIUBA

Martín Harris
Trenes Argentinos

Ing. Adrián Laiuppa
Director del Trabajo Final

Nombre y Apellido (1)
Jurado del Trabajo Final

Nombre y Apellido (2)
Jurado del Trabajo Final

Nombre y Apellido (3)
Jurado del Trabajo Final

Descripción técnica-conceptual del Proyecto a realizar

Las barreras automáticas de los pasos a nivel y los sistemas de cambios de vía del sistema ferroviario de la Argentina dependen mayormente de componentes electromecánicos. Estos componentes deben cumplir altos niveles de seguridad para alcanzar la fiabilidad necesaria. Un componente importante de estos sistemas son los relés de señalamiento, llamados también relés de seguridad (“safety relays” en inglés) o relés vitales (“vital relays” en inglés).

Un único paso a nivel automático puede emplear decenas de relés. Estos solo se consiguen por importación y cada uno tiene un valor superior a los U\$S 1,000 (mil dólares estadounidenses). Es conveniente entonces el desarrollo de una industria nacional que fabrique relés certificados; un sistema de ensayos de relés es una parte esencial para elaborar una certificación local.

El diseño del sistema de ensayos de relés se basa en la norma UNE-EN 50578. En la misma se establecen valores máximos y mínimos en las variaciones de los valores iniciales de la corriente de excitación, la corriente de caída y el factor K. El sistema de ensayos de relés debe permitir el monitoreo de estos valores eléctricos.

En la Figura 1 se puede ver la arquitectura completa del sistema, incluyendo el servidor remoto encargado de monitorear el ensayo a lo largo de todo el proceso.

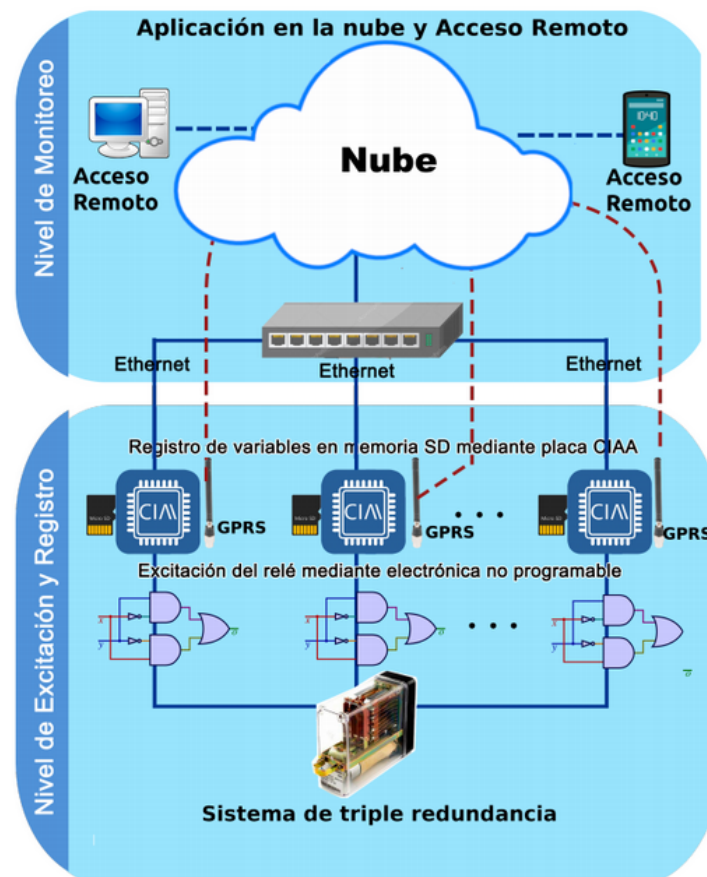


Figura 1: Diagrama en bloques del sistema

El firmware correrá sobre 3 placas CIAA-NXP en simultáneo para asegurar los niveles de disponibilidad deseados. Sobre cada una de las CIAA-NXP se monta una placa de lógica no programable. Este subsistema cuenta entre otras con las siguientes funciones:

- Generar la señal de activación del relé (incluyendo los transistores de potencia y circuitos de activación correspondientes).
- Realizar la sincronización automática de las señales de activación del relé generadas por tres placas independientes entre sí.
- Detectar cuando una de las tres placas falla y en ese caso desconectarla del relé en forma automática.
- Realizar la medición de múltiples valores de voltaje y corriente asociados al funcionamiento del relé. Estos valores son el voltaje aplicado al bobinado del relé y la corriente que circula, junto con los valores de voltaje aplicado y la corriente que circula por cada contacto. Se ensayarán relés que usualmente cuentan con hasta seis contactos normal cerrado y seis contactos normal abierto.
- Mostrar indicaciones luminosas relativas al estado del sistema mediante diodos LED.
- Establecer una comunicación MQTT sobre TCP/IP con el broker para recibir los comandos del usuario y enviar, en tiempo real, los datos recabados.

Para cumplir con los requerimientos de la norma, el sistema debe ser capaz de realizar los siguientes ensayos:

- **Sistema magnético, corriente de excitación y corriente de caída:** la corriente de excitación se define como la corriente mínima a través de la bobina que, partiendo de un valor nulo, alcanza para mover la armadura de la posición de reposo a la posición de trabajo y para aplicar la fuerza de contacto especificada por el fabricante, cerrando todos los contactos de trabajo. La corriente de caída es la corriente máxima a través de la bobina que, partiendo del valor de la corriente nominal, produce la apertura de todos los contactos de trabajo. Este ensayo permite medir el factor K. Para esto se debe generar una función de rampa que, luego de ser amplificada, se aplica al bobinado del relé.
- **Ensayo de vida útil mecánica:** este ensayo es en vacío. El usuario puede ingresar la cantidad de ciclos a ensayar siendo el valor máximo de $10 \cdot 10^6$ movimientos porque la norma se cumple cuando se llega esta cantidad de ciclos. Este ensayo registra la corriente y el voltaje del bobinado y el estado de los contactos.
- **Ensayo con carga:** este ensayo se realiza aplicando el voltaje nominal los contactos abiertos y la corriente nominal a los contactos cerrados. A la bobina del relé también se le aplica el voltaje nominal. La norma dice que en estas condiciones se debe asegurar una cantidad mínima de $2 \cdot 10^6$ movimientos durante la vida útil del relé. En este ensayo se registran los voltajes y las corrientes de la bobina y los voltajes y las corrientes de los contactos.

Identificación y análisis de los interesados

Rol	Nombre y Apellido	Organización	Puesto
Cliente	Martín Harris	Trenes Argentinos	Coordinador General de Desarrollo, de la Subgerencia de Desarrollo y Normas Técnicas
Responsable	Ing. Gaspar Santamarina	CESE 12Co2020	Alumno
Orientador	Ing. Adrián Laiuppa	CONICET-GICSAFe	Director Trabajo final
Colaboradores	Ing. Nicolás Locatelli	CONICET-GICSAFe	Integrante
	Ing. Gustavo Ramoscelli	CONICET-GICSAFe	Investigador

CONICET-GICSAFe: Grupo de Investigación en Calidad y Seguridad de las Aplicaciones Ferroviarias

1. Propósito del proyecto

El propósito de este proyecto es desarrollar el firmware para un probador de relés de seguridad ferroviarios. El mismo deberá comunicarse con un servidor remoto, desde el cuál se configurarán e iniciarán las pruebas. Además, deberá reportar en tiempo real el estado de las pruebas, junto con las mediciones que la conforman.

2. Alcance del proyecto

Se diseñará e implementará el firmware capaz de realizar, junto con el hardware, las tres pruebas mencionadas anteriormente en la descripción técnica del proyecto. En la entrega final no se incluirá el desarrollo de hardware del probador ni el software del servidor remoto.

3. Supuestos del proyecto

- Se contará con el hardware terminado al arrancar con el desarrollo de firmware.
- Se dispondrá, en una etapa avanzada del desarrollo, de un servidor de pruebas con las funcionalidades mínimas requeridas por el probador.

4. Requerimientos

1. Interfaces Externas

- 1.1. El sistema deberá ser capaz de leer el estado de 5 señales digitales.
- 1.2. El sistema deberá leer 15 señales analógicas a través de 2 integrados ADC externos.
- 1.3. El sistema deberá leer 2 señales analógicas a través de 2 ADC internos.
- 1.4. El sistema deberá leer el estado de un pin digital.
- 1.5. El sistema deberá controlar el estado de 2 pines digitales.

- 1.6. El sistema deberá comunicarse con la tarjeta MicroSD presente en el hardware.
- 1.7. El sistema deberá hacer uso de un puerto Ethernet para conectarse a Internet.
- 1.8. El sistema deberá ser capaz de generar una rampa de tensión configurable.

2. Funciones

- 2.1. El sistema debe ser capaz de enviar notificaciones de alerta al servidor remoto, generadas por el disparo de una señal de alerta del hardware.
- 2.2. El sistema debe ser capaz de enviar notificaciones de alerta al servidor remoto, generadas por sobretensión en cualquiera de las entradas analógicas.
- 2.3. El sistema debe ser capaz de interpretar los siguientes comandos enviados desde el servidor:
 - 1) Aplicar configuración de sistema.
 - 2) Definir los parámetros asociados a cada tipo de ensayo.
 - 3) Disparar ensayos.
 - 4) Parar ensayos.
- 2.4. El sistema deberá ser capaz de ejecutar los siguientes ensayos:
 - 1) **Sistema magnético, corriente de excitación y corriente de caída:** Se genera una rampa de tensión de pendiente positiva y luego otra de pendiente negativa. El valor inicial, valor final, paso de tensión y duración del paso de las señales deben ser configurables en ambos casos, además de la máxima corriente de excitación admitida. Se debe notificar al servidor entre paso y paso, indicando la tensión instantánea de la rampa y el valor de las 17 señales analógicas. La prueba finaliza al completarse la cantidad de repeticiones especificadas al inicio de la prueba.
 - 2) **Ensayo de vida útil mecánica con y sin carga:** Se debe especificar el número de ciclos. Al detectarse la secuencia de inicio se comienzan a contabilizar los ciclos, representados por el periodo entre cada secuencia de inicio. Se debe notificar al servidor cada vez que ocurre un flanco positivo de las señales CLOCK.1S o CLOCK.3S, indicando el número de ciclo y el valor de las 17 señales analógicas. La prueba finaliza al completarse la cantidad de ciclos especificados al inicio de la prueba.
- 2.5. Junto con cada paquete de datos generado a partir de una prueba, se debe anexar un ID que identifique el tipo de prueba.
- 2.6. Junto con cada paquete de datos se debe anexar una marca temporal y un ID que identifique a la placa dentro de las tres placas que conforman el sistema.
- 2.7. Cada paquete de datos debe ser almacenado en una tarjeta MicroSD a modo de copia de seguridad.
- 2.8. El sistema debe permitir realizar distintos tipos de ensayos en forma intercalada.
- 2.9. El sistema debe permitir configurar los siguientes parámetros:
 - 1) Hora del sistema.
 - 2) URL y puerto del broker MQTT.

3. Requisitos de Rendimiento

- 3.1. Para el ensayo de rampa se deben permitir hasta 25 ciclos.
- 3.2. Para el ensayo de vida útil mecánica **sin carga** se deben permitir hasta $10 \cdot 10^6$ ciclos.
- 3.3. Para el ensayo de vida útil mecánica **con carga** se deben permitir hasta $2 \cdot 10^6$ ciclos.

3.4. Para el ensayo de vida útil mecánica el periodo máximo entre ciclos es de 3 segundos.

4. Restricciones de Diseño

- 4.1. Se usará I²C como protocolo de comunicación con los ADC.
- 4.2. Se usará SPI como protocolo de comunicación con la SD.
- 4.3. Se usará MQTT sobre TCP/IP como protocolo de comunicación con el servidor remoto.
- 4.4. Se usará JSON como formato de texto para intercambio de datos con el servidor remoto.
- 4.5. La rampa de tensión debe ser capaz de alcanzar un valor máximo de hasta 10V.
- 4.6. Se usará la plataforma CIAA-NXP como placa de desarrollo.
- 4.7. Se usará un RTC para mantener la hora de forma local.
- 4.8. Se usará “Unix time” como formato de marca temporal.

5. Atributos del Sistema

- 5.1. El sistema debe ser capaz de funcionar de forma ininterrumpida durante 2 años.
- 5.2. El sistema debe hacer uso de cifrado TLS para la capa de transporte.
- 5.3. El sistema debe hacer uso de Usuario/Contraseña para autenticarse con el broker MQTT.
- 5.4. El desarrollo de software debe seguir una metodología acorde a la norma UNE-EN 50128.

6. Otros Requisitos

- 6.1. El desarrollo debe ser documentado utilizando la herramienta Doxygen.

5. Entregables principales del proyecto

- Código fuente del firmware
- Informe de avance
- Memoria del trabajo

6. Desglose del trabajo en tareas

- | | |
|---|---------|
| 1. Planificación | (55 hs) |
| 1.1. Estudio del funcionamiento básico de un probador. | (25 hs) |
| 1.2. Elaboración del documento de Planificación del proyecto. | (30 hs) |
| 2. Pruebas preliminares | (80 hs) |
| 2.1. Desarrollo del prototipo de firmware. | (25 hs) |
| 2.2. Pruebas de interacción con el hardware. | (35 hs) |
| 2.3. Pruebas de comunicación con el servidor. | (20 hs) |

3. Diseño de firmware	(100 hs)
3.1. Diseño de la arquitectura general y el flujo de datos.	(35 hs)
3.2. Diseño de las tareas del RTOS y los mecanismos de comunicación entre ellas.	(35 hs)
3.3. Configuración del entorno de desarrollo.	(15 hs)
3.4. Estudio de las herramientas de software disponibles para la plataforma de desarrollo elegida.	(15 hs)
4. Implementación de firmware	(229 hs)
4.1. Desarrollo del driver para los ADC.	(25 hs)
4.2. Desarrollo del módulo de adquisición.	(32 hs)
4.3. Desarrollo del driver ethernet.	(40 hs)
4.4. Desarrollo del módulo de comunicación.	(40 hs)
4.5. Desarrollo del módulo de almacenamiento SD.	(32 hs)
4.6. Desarrollo del módulo de detección de estados.	(20 hs)
4.7. Desarrollo del módulo de control principal.	(40 hs)
5. Verificación y Validación	(163 hs)
5.1. Pruebas individuales de los módulos de firmware.	(30 hs)
5.2. Ensayos de integración del firmware.	(20 hs)
5.3. Pruebas de integración con el hardware.	(20 hs)
5.4. Ensayos funcionales.	(40 hs)
5.5. Análisis de los efectos de los errores de software.	(20 hs)
5.6. Demostración formal.	(8 hs)
5.7. Elaboración del informe de validación.	(25 hs)
6. Documentación	(60 hs)
6.1. Elaboración de la Memoria del trabajo.	(40 hs)
6.2. Producción de la presentación final.	(20 hs)

Cantidad total de horas: (687 hs)

7. Diagrama de Activity On Node

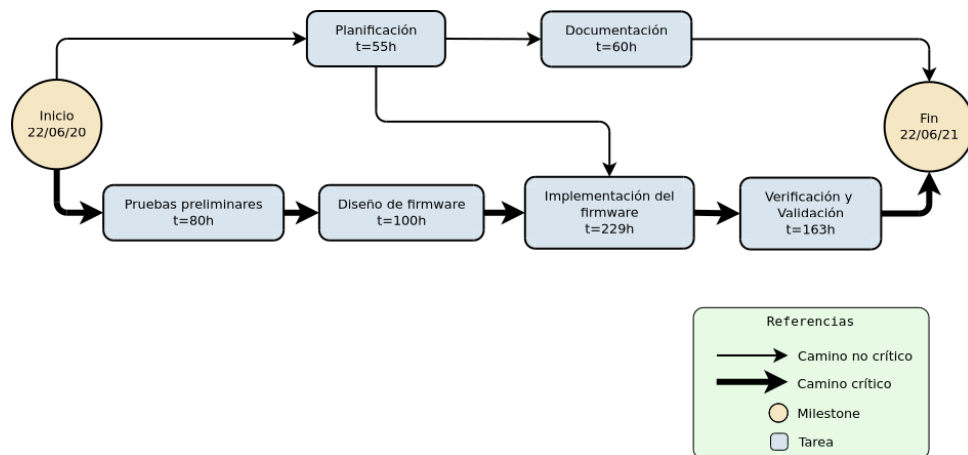


Figura 2: Diagrama en *Activity on Node*

8. Diagrama de Gantt

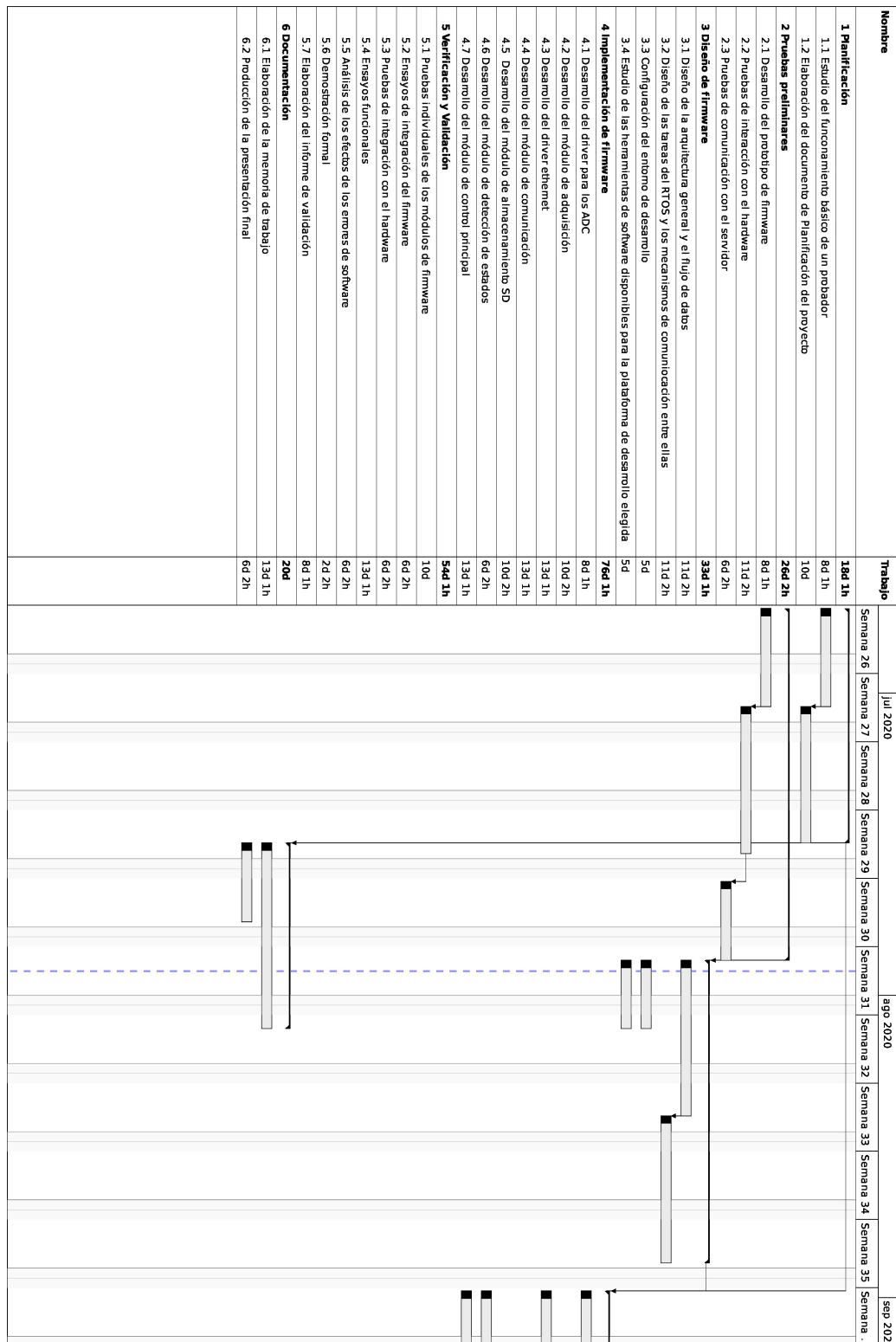


Figura 3: Diagrama de gantt

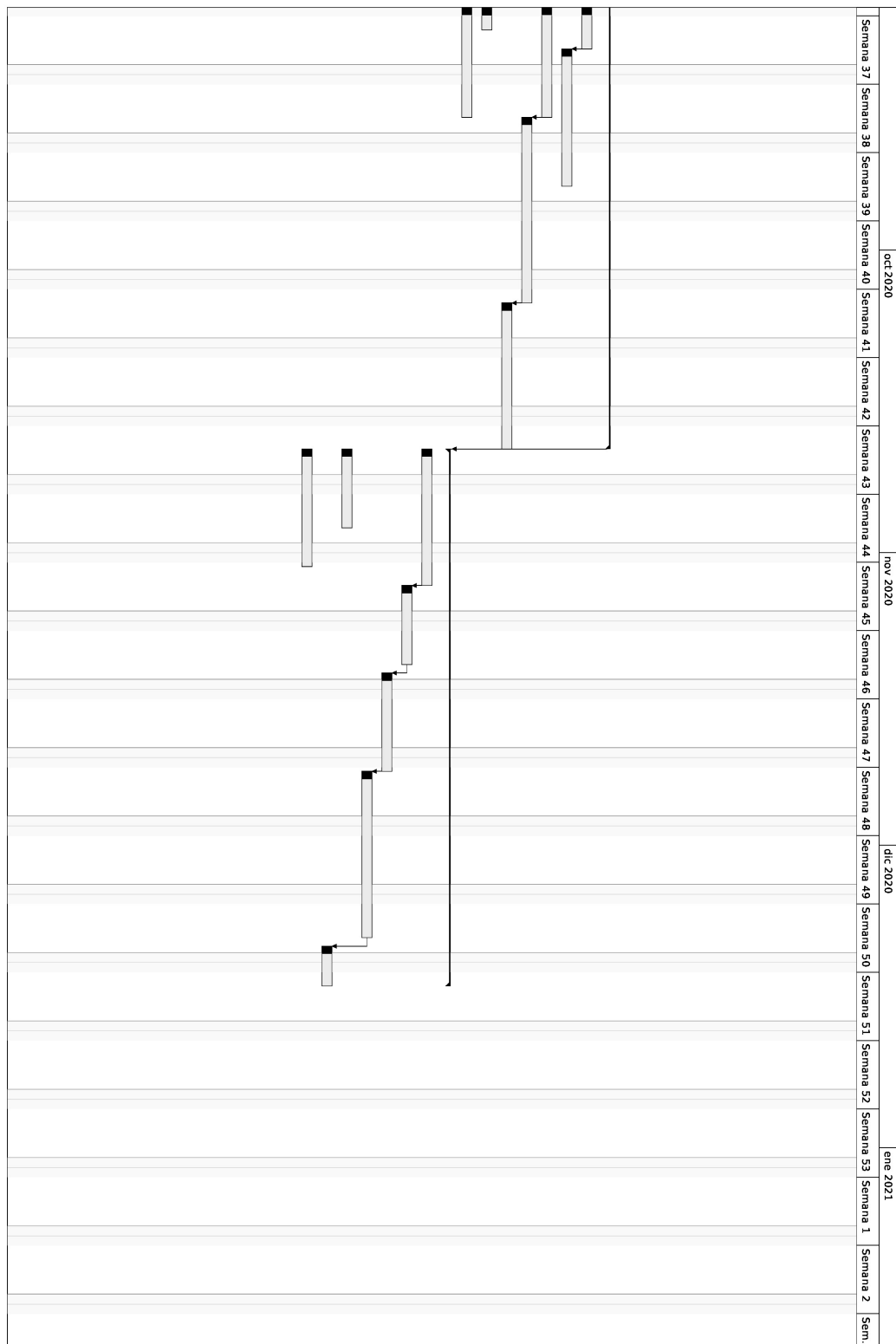


Figura 4: Diagrama de gantt (continuación)

9. Matriz de uso de recursos de materiales

WBS	Nombre de la tarea	Recursos requeridos (horas)	
		PC	Probador+CIAA
1.1	Estudio del funcionamiento básico de un probador	25	10
1.2	Elaboración del documento de planificación del proyecto	30	
2.1	Desarrollo del prototipo de firmware	25	10
2.2	Pruebas de interacción con el hardware	35	10
2.3	Pruebas de comunicación con el servidor	20	
3.1	Diseño de la arquitectura general y el flujo de datos	35	
3.2	Diseño de las tareas del RTOS y los mecanismos de comunicación entre ellas	35	
3.3	Configuración del entorno de desarrollo	15	
3.4	Estudio de las herramientas de software disponible para la plataforma de desarrollo elegida	15	
4.1	Desarrollo del driver para los ADC	25	15
4.2	Desarrollo del módulo de adquisición	32	5
4.3	Desarrollo del driver ethernet	40	5
4.4	Desarrollo del módulo de comunicación	40	
4.5	Desarrollo del módulo de almacenamiento SD	32	5
4.6	Desarrollo del módulo de detección de estados	20	5
4.7	Desarrollo del módulo de control principal	40	
5.1	Pruebas individuales de los módulos de firmware	30	10
5.2	Ensayos de integración del firmware	20	20
5.3	Pruebas de integración con el hardware	20	20
5.4	Ensayos funcionales	40	40
5.5	Análisis de los efectos de los errores de software	15	
5.6	Demostración formal	8	8
5.7	Elaboración del informe de validación	25	
6.1	Elaboración de la memoria de trabajo	40	
6.2	Producción de la presentación final	20	

10. Presupuesto detallado del proyecto

COSTOS DIRECTOS			
Descripción	Cantidad	Valor unitario	Valor total
CIAA-NXP	1	\$ 25.600	\$ 25.600
Poncho Probador de relés	1	\$ 12.693	\$ 12.693
Mano de obra	687 hs	\$ 850	\$ 583.950
SUBTOTAL			\$ 622.243
COSTOS INDIRECTOS			
Descripción	Cantidad	Valor unitario	Valor total
30 % de los costos directos	N/A	N/A	\$ 186.673
SUBTOTAL			
TOTAL			

11. Matriz de asignación de responsabilidades

Código WBS	Nombre de la tarea	Nombres y roles del proyecto				
		Responsable Ing. Gaspar Santamarina	Orientador Ing. Adrián Laiuppa	Colaborador Ing. Nicolás Locatelli	Colaborador Ing. Gustavo Ramoscelli	Cliente Martín Harris
1.1	Estudio del funcionamiento básico de un probador	P	C			
1.2	Elaboración del documento de planificación del proyecto	P	A			I
2.1	Desarrollo del prototipo de firmware	P	C			
2.2	Pruebas de interacción con el hardware	P	C			
2.3	Pruebas de comunicación con el servidor	P		C	C	
3.1	Diseño de la arquitectura general y el flujo de datos	P				
3.2	Diseño de las tareas del RTOS y los mecanismos de comunicación entre ellas	P				
3.3	Configuración del entorno de desarrollo	P				
3.4	Estudio de las herramientas de software disponible para la plataforma de desarrollo elegida	P				
4.1	Desarrollo del driver para los ADC	P	C			
4.2	Desarrollo del módulo de adquisición	P	I			
4.3	Desarrollo del driver ethernet	P				
4.4	Desarrollo del módulo de comunicación	P		I	I	
4.5	Desarrollo del módulo de almacenamiento SD	P	I			
4.6	Desarrollo del módulo de detección de estados	P	C			
4.7	Desarrollo del módulo de control principal	P	I			
5.1	Pruebas individuales de los módulos de firmware	P				
5.2	Ensayos de integración del firmware	P	I			
5.3	Pruebas de integración con el hardware	P	A			
5.4	Ensayos funcionales	P	A	A	A	A
5.5	Análisis de los efectos de los errores de software	P	C			
5.6	Demostración formal	P	A	I	I	A
5.7	Elaboración del informe de validación	P	A			
6.1	Elaboración de la memoria de trabajo	P	A			
6.2	Producción de la presentación final	P	A			

Referencias:

- P = Responsabilidad Primaria
- S = Responsabilidad Secundaria
- A = Aprobación
- I = Informado
- C = Consultado

12. Gestión de riesgos

a) Identificación de los riesgos (al menos cinco) y estimación de sus consecuencias:

Riesgo 1: detallar el riesgo (riesgo es algo que si ocurre altera los planes previstos)

- Severidad (S): mientras más severo, más alto es el número (usar números del 1 al 10). Justificar el motivo por el cual se asigna determinado número de severidad (S).
- Probabilidad de ocurrencia (O): mientras más probable, más alto es el número (usar del 1 al 10). Justificar el motivo por el cual se asigna determinado número de (O).

Riesgo 2:

- Severidad (S):
- Ocurrencia (O):

Riesgo 3:

- Severidad (S):
- Ocurrencia (O):

b) Tabla de gestión de riesgos: (El RPN se calcula como $RPN=S \times O$)

Riesgo	S	O	RPN	S*	O*	RPN*

Criterio adoptado: Se tomarán medidas de mitigación en los riesgos cuyos números de RPN sean mayores a

Nota: los valores marcados con (*) en la tabla corresponden luego de haber aplicado la mitigación.

c) Plan de mitigación de los riesgos que originalmente excedían el RPN máximo establecido:

Riesgo 1: Plan de mitigación (si por el RPN fuera necesario elaborar un plan de mitigación). Nueva asignación de S y O, con su respectiva justificación: - Severidad (S): mientras más severo, más alto es el número (usar números del 1 al 10). Justificar el motivo por el cual se asigna determinado número de severidad (S). - Probabilidad de ocurrencia (O): mientras más probable, más alto es el número (usar del 1 al 10). Justificar el motivo por el cual se asigna determinado número de (O).

Riesgo 2: Plan de mitigación (si por el RPN fuera necesario elaborar un plan de mitigación).

Riesgo 3: Plan de mitigación (si por el RPN fuera necesario elaborar un plan de mitigación)

13. Gestión de la calidad

Para cada uno de los requerimientos del proyecto indique:

- Req #1: Copiar acá el requerimiento.

Verificación y validación:

- Verificación para confirmar si se cumplió con lo requerido antes de mostrar el sistema al cliente:
Detallar

- Validación con el cliente para confirmar que está de acuerdo en que se cumplió con lo requerido:
Detallar

Tener en cuenta que en este contexto se pueden mencionar simulaciones, cálculos, revisión de hojas de datos, consulta con expertos, etc.

14. Comunicación del proyecto

El plan de comunicación del proyecto es el siguiente:

PLAN DE COMUNICACIÓN DEL PROYECTO					
¿Qué comunicar?	Audiencia	Propósito	Frecuencia	Método de comunicac.	Responsable

15. Gestión de Compras

En caso de tener que comprar elementos o contratar servicios: a) Explique con qué criterios elegiría a un proveedor. b) Redacte el Statement of Work correspondiente.

16. Seguimiento y control

Para cada tarea del proyecto establecer la frecuencia y los indicadores con los se seguirá su avance y quién será el responsable de hacer dicho seguimiento y a quién debe comunicarse la situación (en concordancia con el Plan de Comunicación del proyecto).

El indicador de avance tiene que ser algo medible, mejor incluso si se puede medir en % de avance. Por ejemplo, se pueden indicar en esta columna cosas como “cantidad de conexiones ruteadas” o “cantidad de funciones implementadas”, pero no algo genérico y ambiguo como “%”, porque el lector no sabe porcentaje de qué cosa.

SEGUIMIENTO DE AVANCE						
Tarea del WBS	Indicador de avance	Frecuencia de reporte	Resp. de seguimiento	Persona a ser informada	Método de comunic.	

17. Procesos de cierre

Establecer las pautas de trabajo para realizar una reunión final de evaluación del proyecto, tal que contemple las siguientes actividades:

- Pautas de trabajo que se seguirán para analizar si se respetó el Plan de Proyecto original:
- Indicar quién se ocupará de hacer esto y cuál será el procedimiento a aplicar.
- Identificación de las técnicas y procedimientos útiles e inútiles que se utilizaron, y los problemas que surgieron y cómo se solucionaron: - Indicar quién se ocupará de hacer esto y cuál será el procedimiento para dejar registro.
- Indicar quién organizará el acto de agradecimiento a todos los interesados, y en especial al equipo de trabajo y colaboradores: - Indicar esto y quién financiará los gastos correspondientes.