

**UNIVERSIDAD TECNOLÓGICA NACIONAL**



**FACULTAD REGIONAL CÓRDOBA**  
**Ingeniería Electrónica - Proyecto Final**

**RED MULTINODAL PARA DETECTAR  
INHIBICIONES EN SISTEMAS DE  
SEGURIDAD VEHICULAR**

**Coronel, Martín  
Fantin, Stefano  
Giletta, Julian**

*Agradecemos profundamente a nuestra familia  
que siempre nos apoyó en este largo camino  
y a la Universidad Tecnológica Nacional,  
particularmente a la carrera de ingeniería electrónica, la cual siempre se  
caracterizó por la buena organización y la búsqueda del bienestar estudiantil.*

# Resumen

En este documento se plasma el proceso de investigación y desarrollo de un sistema multinodal pensado para detectar inhibiciones en los sistemas de seguridad vehicular que funcionen en la frecuencia de 433,92MHz.

El dispositivo planteado cuenta con tres unidades de recepción, las cuales denominamos nodos y una central de procesamiento encargada de comunicarse y gestionar la información por estos recolectada.

Para la comunicación entre los nodos y la central se utiliza el protocolo RS485 y para comunicar la central con un servidor web, teniendo así los datos a disposición remotamente, se hace uso de un módulo GPRS.

# Índice general

Resumen . . . . .	II
<b>1. Introducción</b>	<b>1</b>
1.1. Marco teórico . . . . .	2
1.1.1. Codificación en sistemas de seguridad vehicular . . . . .	2
1.1.2. Estructura de transmisión . . . . .	3
1.1.3. Tipos de inhibiciones . . . . .	5
1.1.4. Estrategias de inhibición . . . . .	8
1.1.5. Detección de inhibiciones . . . . .	12
<b>2. Características generales del diseño</b>	<b>16</b>
2.1. Objetivos globales del sistema . . . . .	16
2.2. Esquema de funcionamiento . . . . .	17
2.3. Subsistemas que lo componen . . . . .	18
<b>3. Selección de componentes</b>	<b>19</b>
3.1. Etapa receptora de RF . . . . .	19
3.1.1. CC1101 . . . . .	21
3.2. Comunicación . . . . .	23
3.2.1. Comunicación local . . . . .	24
3.2.2. MAX485 . . . . .	25
3.2.3. Comunicación con Servidor Web . . . . .	26
3.2.4. SIM800L . . . . .	26
3.3. Procesamiento . . . . .	28
3.3.1. Blue Pill STM32 . . . . .	29
<b>4. Central de procesamiento</b>	<b>32</b>
4.1. Descripción general . . . . .	32
4.1.1. Funcionamiento . . . . .	32



4.2.	Prototipo . . . . .	33
4.2.1.	Diseño . . . . .	33
4.2.2.	Problemas surgidos . . . . .	33
4.3.	Diseño final . . . . .	34
4.3.1.	Software . . . . .	34
4.3.2.	Hardware . . . . .	37
4.4.	Gabinete . . . . .	41
<b>5.</b>	<b>Nodos de recepción</b>	<b>45</b>
5.1.	Descripción general . . . . .	45
5.2.	Prototipo . . . . .	45
5.3.	Diseño final . . . . .	48
5.3.1.	Software . . . . .	48
5.3.2.	Hardware . . . . .	51
5.3.3.	Gabinete . . . . .	53
<b>6.</b>	<b>Ensayos</b>	<b>55</b>
6.1.	Análisis de llaves e inhibidores . . . . .	55
6.2.	Pruebas y configuración del CC1101 . . . . .	56
6.3.	Ensayos de las estrategias de detección . . . . .	56
6.4.	Servidor Web y conexión a internet . . . . .	57
6.5.	Desarrollo de la comunicación serial del sistema . . . . .	57
6.6.	Ensayos Finales . . . . .	58
<b>7.</b>	<b>Desarrollo de servidor web</b>	<b>59</b>
7.1.	Objetivos . . . . .	59
7.2.	Página web . . . . .	60
7.2.1.	Pestañas . . . . .	62
7.3.	Base de datos . . . . .	65
7.3.1.	Carga de datos . . . . .	66
<b>8.</b>	<b>Conclusiones y trabajo futuro</b>	<b>67</b>
8.1.	Conclusiones . . . . .	67
8.2.	Trabajo futuro . . . . .	68

# Índice de figuras

1.1.	Software Defined Radio utilizado para tomar las primeras mediciones . . . . .	4
1.2.	Demodulación ASK de señales de controles remotos en 433,92 MHz . . . . .	5
1.3.	Espectro de señal random bits modulada ASK en 433,92 MHz	6
1.4.	Presencia de inhibidor en ancho de banda de recepción . . . . .	7
1.5.	Compresión de la ganancia . . . . .	9
1.6.	Donde a) es el canal a inhibir, b) inhibición por ruido de banda ancha, c) inhibición por ruido de banda parcial continuo, d) inhibición por ruido de banda parcial discontinuo, e) inhibición por ruido de banda angosta, f) inhibición por tono . . . . .	11
1.7.	Diagrama en bloques de sistema de comunicación ASK inhibido	12
1.8.	Bit Error Rate para comunicación ASK inhibida. . . . .	13
1.9.	Curva de ganancia de MAX1470 . . . . .	14
2.1.	Diagrama en bloques sobre el funcionamiento del sistema global	18
3.1.	Etapa receptora - primer opción . . . . .	20
3.2.	Etapa receptora - opción elegida . . . . .	21
3.3.	Transceptor CC1101 . . . . .	21
3.4.	Esquemático CC1101 . . . . .	23
3.5.	Módulo CC1101 . . . . .	24
3.6.	Max 485 . . . . .	26
3.7.	Módulo SIM800L . . . . .	27
3.8.	Esquemático de Blue Pill . . . . .	31
4.1.	Prototipo de placa de la central de procesamiento. . . . .	34
4.2.	Estados de la central en comunicación con nodos. . . . .	36



4.3.	Cristal para el MCU . . . . .	38
4.4.	Regulador de 5V a 3.3V para MCU. . . . .	38
4.5.	Reset de microcontrolador. . . . .	38
4.6.	MCU, modulo GSM/GPRS y leds indicadores de nodos. . . .	39
4.7.	Sección de comunicación RS485. . . . .	40
4.8.	Pines de alimentación, regulación para SIM800 y pines libres para conexiones adicionales. . . . .	40
4.9.	Diseño final de placa de la central de procesamiento. . . . .	41
4.10.	Vista en 3D de la placa final de la central de procesamiento. .	41
4.11.	Placa de la central terminada. . . . .	42
4.12.	Gabinete de central armado. . . . .	43
4.13.	Partes para el armado del gabinete de central. . . . .	43
4.14.	Gabinete de central terminado. . . . .	44
5.1.	Primer placa del nodo armada . . . . .	46
5.2.	Asignación de pines para comunicación . . . . .	47
5.3.	Estrategia de detección por corrupción de datos . . . . .	50
5.4.	Estrategia de detección por saturación de etapa receptora . .	50
5.5.	Estados de comunicación en nodo . . . . .	51
5.6.	Esquemático del nodo receptor . . . . .	51
5.7.	Diseño 3D del nodo receptor. . . . .	52
5.8.	Placa final del nodo receptor. . . . .	53
5.9.	Diseño 3D del nodo receptor terminado. . . . .	54
5.10.	Gabinete del nodo receptor terminado. . . . .	54
7.1.	Página de inicio . . . . .	62
7.2.	Presentación de grupo de trabajo . . . . .	63
7.3.	Gráficos de estadísticas . . . . .	63
7.4.	Pestaña de triangulación . . . . .	65
7.5.	Formulario de contacto . . . . .	65

# Capítulo 1

## Introducción

Hoy en día en muchos países, y particularmente en la Argentina, se presenta una recurrente modalidad de delincuencia que trata de inhibir los sistemas de seguridad vehicular, no permitiendo que estos se cierren y pudiendo tener completo acceso a su interior. Es una metodología muy usada debido a que no se hace uso de la fuerza bruta para ingresar al vehículo y apela a la distracción del usuario.

Siendo conscientes de esta problemática nos hemos empeñado en desarrollar un sistema de detección de los dispositivos utilizados con este fin. Como se verá más adelante se ha hecho un relevamiento de los dispositivos incautados por la policía a través de notas periodísticas y con vínculos internos a departamentos policiales que pusieron a disposición la información presente sobre estos.

Los inhibidores pueden operar corrompiendo la trama de datos emitida por el llavero, no dejando así, que el receptor del vehículo pueda identificar el intento de comunicación. También lo pueden hacer saturando el receptor. Creemos importante que el dispositivo a diseñar abarque estas dos posibilidades.

Otra característica importante a la hora de encarar el proyecto es determinar la frecuencia de operación. Los controles remotos poseen transmisores de radio de corto alcance que operan en dos bandas posibles: 433,92 MHz para vehículos de origen europeo y asiático, y 315 MHz para vehículos de origen norteamericano. En la Argentina la mayor cantidad de sistemas de seguridad operan en 433,92 MHz por lo que nos pareció adecuado diseñar el detector para esta frecuencia.

Una vez definidos los requerimientos básicos del desarrollo es importante



establecer el lugar en el que creemos adecuado que opere. Es así que surge la idea de tener al menos tres nodos receptores capaces de identificar si hay o no un inhibidor en las inmediaciones de este y que la información que recolecte sea enviada a una unidad de procesamiento, que denominamos "central", la cual se encargaría de comunicarse con los nodos, recopilar la información y subirla a una base de datos, permitiendo la visualización remota de lo que está sucediendo en tiempo real y, de ser posible, triangular la posición estimada del dispositivo inhibidor dentro del arreglo de receptores.

Esto sería emplazado en un estacionamiento utilizando una estrategia de disposición que se analizará más adelante

## 1.1. Marco teórico

Es importante realizar un estudio profundo sobre el tema que vamos a abordar, ya que es necesario definir un método novedoso que satisfaga la necesidad de distinguir señales legítimas generadas por un control remoto de interferencias.

### 1.1.1. Codificación en sistemas de seguridad vehicular

Desde los inicios de los sistemas remotos de apertura y control vehicular hasta ahora se ha transitado un largo camino. El primer sistema de identificación por radiofrecuencia fue ingresado en el mercado por Renault en el modelo Fuego en el año 1995. Todo este tiempo, desde su puesta en uso hasta la fecha, ha servido para definir y universalizar las metodologías usadas para comunicarse, intentando dar una mejora en cuanto a la seguridad y efectividad del sistema.

#### Sistemas de código fijo

Esta es la forma más difundida de codificación para los controles remotos vehiculares en nuestro país. Se trata de un código de comunicación fijo, que precisa estar preestablecido en el circuito integrado del dispositivo, el cual se mantiene constante para la acción a realizar. De esto podemos notar que para los controles remotos comunes que poseen opción de cierre y apertura del automóvil se tienen solo dos códigos fijos que realizan cada una de estas acciones y que, eventualmente, podrían ser copiados y replicados para generar la acción codificada.



### Sistemas de código variable

Esta metodología no está muy difundida en nuestra región. Se trata de un sistema de seguridad que no repite el mismo patrón para ejecutar la acción de cierre o apertura del vehículo para evitar que se pueda leer y replicar el código. Usualmente se hace uso de un generador de números pseudoaleatorios que se encuentra en el emisor y receptor, un contador de pulsaciones en el emisor y un contador de recepciones en el vehículo. Cuando el control remoto envía la señal para realizar una acción en el vehículo este manda su contador, el cual será comparado con el interno del receptor y, de estar dentro de la ventana de aceptación definida en el sistema de seguridad, el automóvil autentica el mensaje recibido y actualiza el contador interno, ya que este puede diferir al de la llave. Hay diversos tipos de encriptación de la comunicación; aquí solo mencionaremos los más difundidos: Hitag 1, Hitag 2, Hitag AES, DST-40, Keeloq

### Sistemas por desafío

El sistema por desafío es actualmente el más utilizado en autos de alta gama. En este caso el control remoto intenta comunicarse y el vehículo envía una pregunta desafío que tiene que ser respondida correctamente para validar la comunicación.

En esta variante se puede observar que es necesario que el control remoto y el vehículo tengan la capacidad de emitir y recibir datos, generando una comunicación bidireccional. Hay diversas opciones de desafíos de requerimiento realizados por el vehículo, pero la más utilizada es la de validación de contraseña, donde el desafío es pedir la contraseña y esta será o no validada. Esto en definitiva no impide que sea replicado el patrón de comienzo de comunicación y la autenticación, por lo que hay modalidades más avanzadas como tener una tabla de códigos pseudoaleatorios definida en ambos dispositivos y asociada a un identificador, de modo que el vehículo requiera el código por medio de este no dando lugar a que un escucha externo pueda saber a qué valor está asociado.

#### 1.1.2. Estructura de transmisión

Tener noción previa de lo que esperamos recibir cuando hacemos un análisis de una señal es de gran importancia, por lo que en esta sección analiza-



remos la estructura de transmisión de un control remoto de autos.

Como antes fue mencionado no hay solo una frecuencia de operación, pero sí hay una que es ampliamente difundida en nuestro país y en esa nos centraremos (433,92 MHz), la modulación utilizada en la mayor cantidad de estos dispositivos es ASK, por su fácil implementación. Con esta información ya seríamos capaces de demodular la señal y analizar la estructura.

Para la demodulación de la señal hemos utilizado un SDR (Software Defined Radio) como el que se puede observar en la figura 1.1, el cual fue facilitado por el centro de investigación G.In.T.E.A (Grupo de Investigación y Transferencia en Electrónica Avanzada) de la Universidad Tecnológica Nacional, facultad regional Córdoba.



Figura 1.1: Software Defined Radio utilizado para tomar las primeras mediciones

En la figura 1.2 podemos observar las primeras mediciones tomadas. Aquí distinguimos la estrategia de transmisión que se utiliza. En un comienzo la señal posee un preámbulo, el cual es utilizado por el receptor para sincronizar el reloj del receptor para decodificar correctamente los paquetes del transmisor. Después del preámbulo hay una palabra de sincronización que se utiliza para evitar choques con otros dispositivos que operan en esa banda y por último se encuentra la señal de código real.

Al presionar el botón del control remoto el preámbulo es enviado una única vez y luego se envía la palabra de sincronización y el comando de acción repetidamente hasta que se deje de accionar. El espectro de la señal transmitida se puede observar en la figura 1.3, la cual es una simulación en el software AWR de una transmisión de datos random modulados ASK.

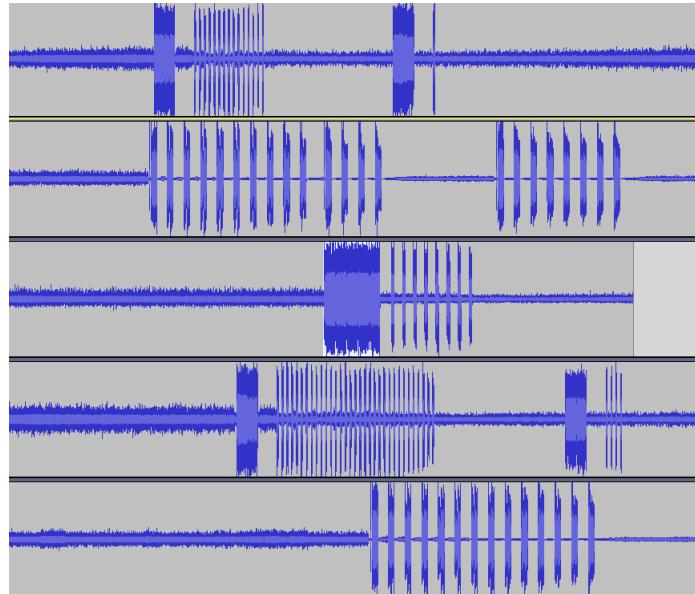


Figura 1.2: Demodulación ASK de señales de controles remotos en 433,92 MHz

### 1.1.3. Tipos de inhibiciones

Un inhibidor, o en inglés jammer, es un dispositivo desarrollado con el objetivo de deteriorar la comunicación en un enlace de radiofrecuencia. Esto puede ser logrado mediante dos estrategias:

- Inhibición por corrupción de datos
- Inhibición por saturación de etapa receptora

#### Inhibición por corrupción de datos

El ataque más evidente que se presenta para inhibir una comunicación es el de inyectar en el canal que se desea perjudicar una señal con datos aleatorios que perjudique la relación señal ruido (SNR) y dificulte la recepción para el sistema.

En el caso particular de los vehículos, los receptores de radiofrecuencia que se utilizan y sobre los que basamos nuestro análisis son de 433,92 MHz con un filtro de ancho de banda de entrada de 300 KHz -como se analiza en [3].

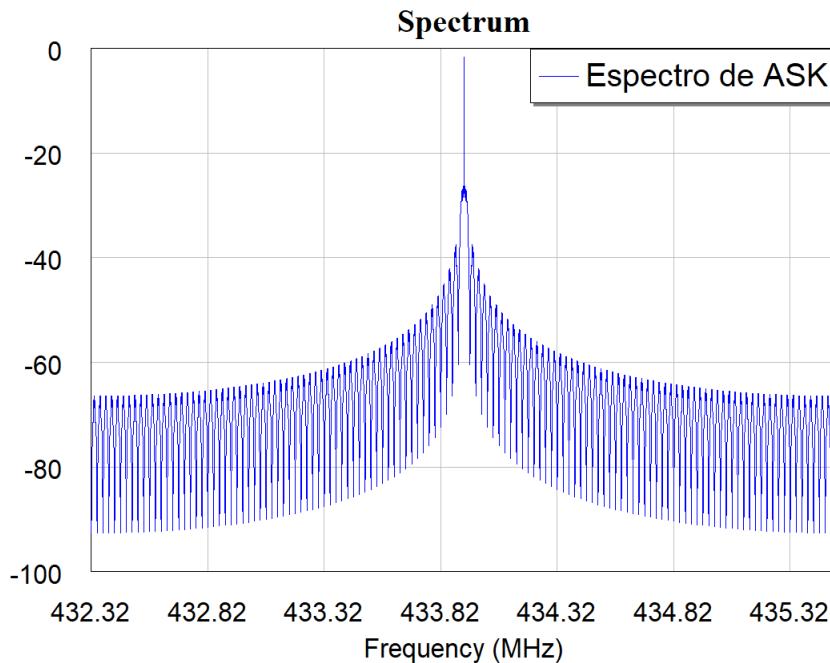


Figura 1.3: Espectro de señal random bits modulada ASK en 433,92 MHz

El ancho de banda de recepción da lugar a sumar ruido en el canal, alterando así los datos recibidos por el demodulador. Una figura ilustrativa se puede observa en la imagen 1.4 de [4].

Existen diversas alternativas para efectivizar este tipo de interferencias. En la figura 1.4 se observa que se ha inyectado una interferencia de ancho de banda angosto, pero también podría sumarse un tono, multitonos o sumar una señal de gran ancho de banda que tape completamente el canal.

Las alternativas antes mencionadas hacen referencia a inhibidores no inteligentes, los cuales están metiendo ruido constantemente. Hay otras alternativas de inhibiciones que de manera continua están escuchando el canal y cuando detectan una señal que desean interferir comienzan a emitir el ruido. Estos casos serán detallados más adelante.

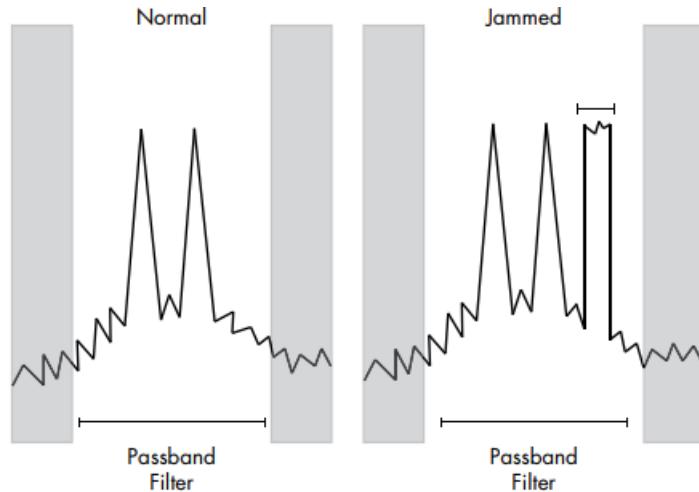


Figura 1.4: Presencia de inhibidor en ancho de banda de recepción

### Inhibición por saturación de etapa receptora

Los receptores de radiofrecuencia usualmente están diseñados asumiendo que se recibirá una pequeña señal de entrada, por lo que la primer etapa presente es un amplificador de bajo ruido. Este es clave para que el ruido del mezclador no afecte la relación señal ruido de las etapas siguientes. Entre las especificaciones importantes de dichos amplificadores de RF se incluyen la figura de ruido, la ganancia y la intercepción de intermodulación de tercer orden.

La influencia de grandes señales de interferencia se manifiesta de varias formas. Una de estas es en la intermodulación de tercer orden en la que dos señales, una pequeña (de interés) y la interferente (de gran amplitud), se superponen. La interferente podría saturar el receptor de modo que la señal de interés presente una pequeña ganancia como hace referencia [8] y [9]. Este efecto es causado por la no linealidad de tercer orden del sistema.

La saturación de un sistema suele tener un comportamiento de compresión de la ganancia, decrementando la misma a medida de que la entrada aumenta. Este efecto puede ser cualificado como el punto de 1 dB de compresión el cual está definido como el punto en el que la amplitud de la señal de entrada genera que la ganancia caiga 1 dB. Esto antes mencionado está claramente ilustrado en la figura 1.1.



$$y(t) \approx a_1x(t) + a_2x^2(t) + a_3x^3(t) \quad (1.1)$$

Donde  $y$  es la salida del sistema y  $a_1, a_2, a_3$  son coeficientes. Ahora supongamos que la entrada, como es de esperar con lo antes descripto, resulta:

$$x(t) = V_1\cos(\omega_1 t) + V_2\cos(\omega_2 t) \quad (1.2)$$

$V_1$  representando a la señal de interés y  $V_2$  a la interferente.

Reemplazando en la ecuación 1.2 en 1.1 y asumiendo que la interferencia es mucho más grande que la señal, la salida del sistema en la frecuencia de interés  $\omega_1$  resulta ser 1.3.

$$y(t) \approx \left( a_1x(t) + \frac{3}{2}a_3V_2^2 \right) V_1\cos(\omega_1 t) \quad (1.3)$$

Para que el sistema comprima la ganancia, como es evidente que sucede, el producto  $a_1a_3 < 0$ . De aquí se puede observar entonces que la salida del sistema en la frecuencia deseada es función de  $V_2^2$ , que la ganancia decae saturando el sistema y por ende se decremente la SNR. Esto es fácilmente observable en la figura 1.5.

#### 1.1.4. Estrategias de inhibición

Antes hemos presentado los principios de inhibición que se pueden utilizar, en este apartado se tratará de una manera generalizada las diversas estrategias existentes para inhibir sistemas de comunicación. Cada una de estas tienen ventajas y desventajas, por lo que es necesario hacer un análisis del ámbito de aplicación para elegir la más adecuada.

##### Inhibición por ruido de banda ancha

La característica principal de este tipo de estrategia es que introduce energía dentro de todo el ancho del espectro donde opera la comunicación. Es aplicable a cualquier tipo de señal y es ideal para inhibir comunicaciones que tienen destinada una gran parte del espectro de frecuencias.

Este método tiene una fuerte desventaja y es que la potencia de interferencia aportada en el canal deseado tiene una muy baja densidad debido a que es aplicada a un gran ancho de banda.

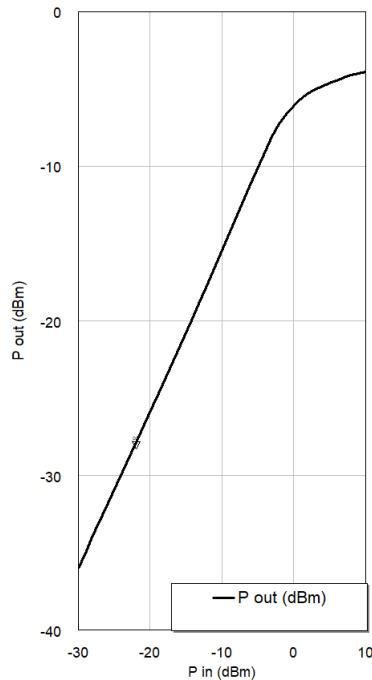


Figura 1.5: Compresión de la ganancia

### Inhibición por ruido de banda parcial

Este método opera inyectando ruido en bandas específicas del espectro, de modo que se efectúa la inhibición en zonas de interés. Estas pueden ser continuas o discontinuas, por lo que se destina más inteligentemente la potencia consumida. El ejemplo más trivial aplicado a nuestro campo sería el de un inhibidor que funcione en 433,92 y en 315 MHz, siendo aplicable a todos los canales de comunicación de controles remotos.

### Inhibición por ruido de banda angosta

Este caso es el más utilizado en el campo de inhibición sobre el que nos centramos ya que permite puntualizar la potencia en una pequeña banda aumentando la densidad de potencia espectral. Para su aplicación es necesario conocer precisamente el canal a atacar debido a que las comunicaciones inalámbricas de banda angosta poseen un angosto filtrado.



### Inhibición por tono

Se utiliza una señal constante que se modula con la portadora resultando una señal de muy angosto ancho de banda. En sistemas de comunicación avanzados posee una alta eficiencia de interferencia ya que perjudica la recuperación de la sintonización a causa de que el receptor detecta la señal como una segunda portadora y de que más potencia por Hertz (densidad de potencia espectral) gracias a que está más concentrado en el canal, como profundamente se analiza en [10].

### Inhibición por pulsos

En esta estrategia nos enfocamos en el tiempo que se genera la interferencia. Se hace uso de uno de los métodos anteriores de inhibición y se desata la misma de manera inteligente. De aquí surge el concepto de aplicar la estrategia a casos específicos, permitiendo, por ejemplo: romper tramas específicas de datos conocidas cuando se detecta un CLT/RTS, interferir el dato de direccionamiento MAC o romper exclusivamente la trama de datos.

### Inhibición por barrido y seguimiento

Esta es una aplicación del ruido de banda parcial. Se realiza una variación rápida del posicionamiento espectral de la interferencia para inhibir un gran ancho de banda teniendo un mejor aprovechamiento de la potencia disponible.

De esta alternativa se desprende la capacidad de seguimiento de la señal inhibidora, permitiendo contrarestar estrategias de comunicación que hacen uso de saltos de canales para ser efectivas.

### Simulación de inhibición por ruido de banda parcial

En este apartado se ha elegido la metodología de inyección de ruido de banda parcial para ser simulado y mostrar como decae la calidad de comunicación y, por ende, la capacidad de recepción de la información. La simulación fue realizada con el software AWR de Cadence.

El diagrama en bloques se puede observar en la figura 1.7, este cuenta de 4 secciones principales:

- Inhibidor de potencia variable: este bloque inyecta ruido blanco al sistema en la frecuencia definida como portadora, que en nuestro caso es

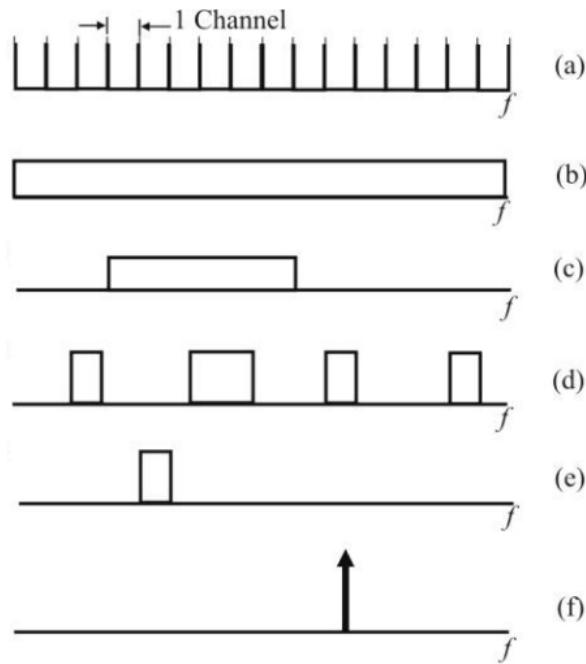


Figura 1.6: Donde a) es el canal a inhibir, b) inhibición por ruido de banda ancha, c) inhibición por ruido de banda parcial continuo, d) inhibición por ruido de banda parcial discontinuo, e) inhibición por ruido de banda angosta, f) inhibición por tono

433,92 MHz. La potencia de ruido va a variar entre 0 y -30 dBW, lo que sería igual a decir entre -30 y -60 dBm.

- Emisor de señal: el emisor de señal es un modulador de ASK que modula una generación aleatoria de bits a 2500 baudios con la portadora.
- Medio de enlace: en este caso está representado con un combinador de señal RF, el cual va a servir para sumar la potencia de las dos señales anteriores.
- Demodulador: en esta instancia se produce la demodulación de la señal ASK más el ruido blanco agregado. Al final posee un bloque que se encarga de controlar el BER (Bit Error Rate), chequeando cuántos datos de los enviados efectivamente fueron recibidos.

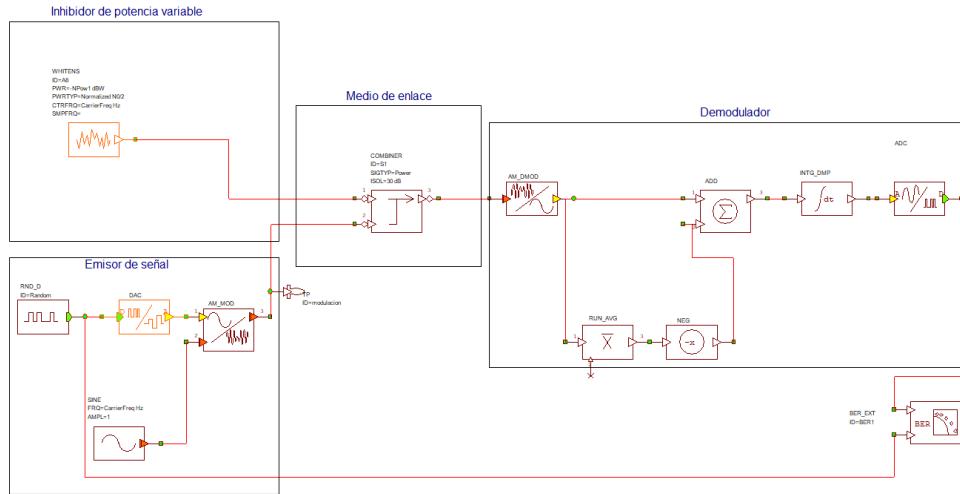


Figura 1.7: Diagrama en bloques de sistema de comunicación ASK inhibido

Como antes se menciona, y como se puede observar en la figura 1.8, el error de recepción alcanza su valor máximo cuando el ruido inyectado es de 0 dBW (-30 dBm). En la figura se puede leer un valor de  $BER = 0.4866$ , el cual es lógico debido a que la modulación ASK solo posee dos símbolos, por lo que la probabilidad de que coincida el dato generado por el ruido y el esperado es del 50 %. Por otro lado el valor mínimo de error en la simulación propuesta sucede cuando la potencia del inhibidor es de -30 dBW (-60 dBm) teniendo un error de cuatro bits por cada diez mil recibidos.

### 1.1.5. Detección de inhibiciones

En esta sección trataremos los métodos que pueden utilizarse para detectar interferencias en enlaces de radiofrecuencia. Es importante que sea robusta la detección, en principal que el funcionamiento del sistema que se pretende asegurar no pueda desatar una falsa alarma. En el caso puntual de aplicación de este proyecto, el sistema debería poder identificar una inhibición y no identificar como tal a las señales de controles remotos que van a estar funcionando en el área circundante. Hay algunas características las cuales son naturales pensar como sensibles de analizar para detectar inhibiciones, y estas son:

- Potencia de la señal recibida

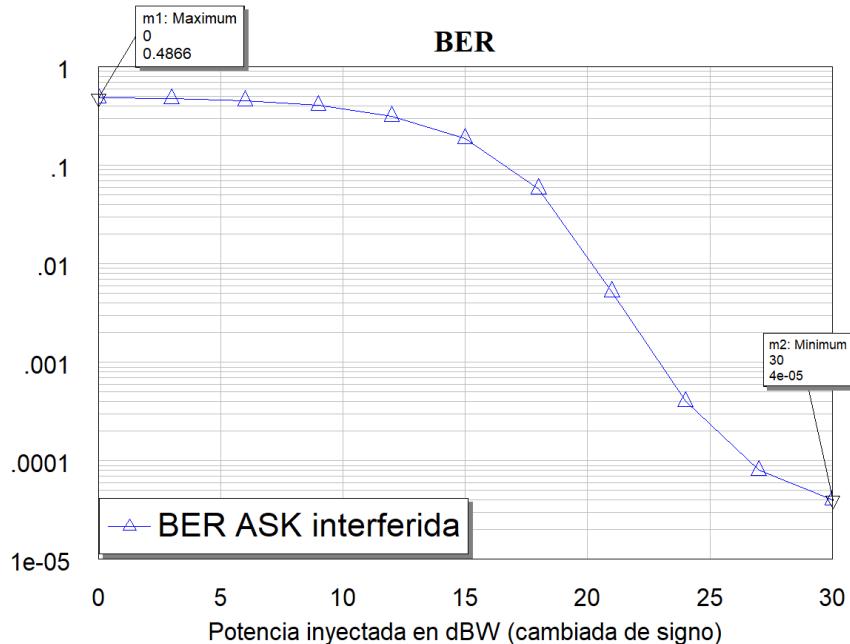


Figura 1.8: Bit Error Rate para comunicación ASK inhibida.

- Sensado temporal de portadora
- Ocupación del canal

### Potencia de la señal recibida

Como antes se ha definido, el receptor sufre compresión de ganancia en su primera etapa amplificadora cuando la potencia recibida es alta comparado a la potencia de señal que se espera recibir y para el que fue diseñado. Es por esto que resulta natural analizar los niveles de potencia recibidos, estableciendo un valor a partir del cual se señale como alarmante para la correcta recepción de la información. En el caso particular de los dispositivos de control remoto en los sistemas de seguridad vehicular resulta más sencillo el análisis debido a que los dispositivos emisores que se utilizan son de baja potencia comparado a la necesaria para saturar un receptor típico.

En [9] se realiza el análisis del receptor MAX1473 [3], muy difundido en sistemas de control remoto tanto en el ámbito automotriz como también en sistemas de portones de apertura inalámbrica, sistemas de seguridad, sensores



inalámbricos y mucho más. Este integrado es un receptor de ASK superheterodíneo de bajo costo que posee un mezclador de rechazo de imagen que mezcla la señal a una frecuencia intermedia de 10,7 MHz. En la figura 1.9 se puede observar que la ganancia del sistema de recepción se aplana aproximadamente con una entrada de -35 dBm.

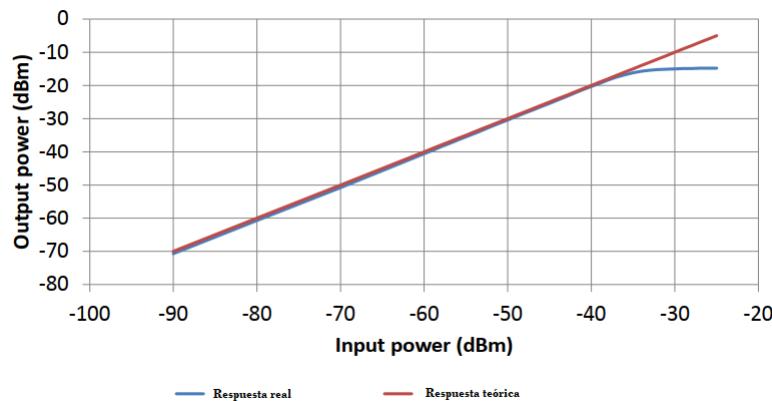


Figura 1.9: Curva de ganancia de MAX1470

### Sensado temporal de portadora

Esta es una estrategia muy utilizada en sistemas de comunicación en que se realiza un envío efectivo de paquetes cuando se detecta que el canal de transmisión está desocupado. Esta característica hace sensible al sistema de ser engañado dejando presente una señal portadora de información que engañe a los dispositivos emisores de la red.

En nuestro caso no nos detendremos a hacer un análisis profundo de esta metodología ya que es ajena a nuestro potencial mecanismo de detección debido a que, como se menciona en 3.1.2, el control remoto emite señal cuando es accionado un botón que este posee, haciéndolo de manera continua hasta que deje de ser apretado. Es fácil ver que esta característica de la comunicación hace inútil aplicar esta estrategia de detección.

### Ocupación del canal

El sistema de comunicación que nos basamos para desarrollar este trabajo tiene la particularidad de que la comunicación unilateral que sucede



entre los dispositivos de emisión (controles remotos) y recepción (vehículos) tienen una muy baja tasa de ocupación de canal. Esto se debe a la trama de datos empleada. La misma, como antes fue explicado, posee un período de sincronización que es una rápida variación de estados, para que el receptor pueda engancharse en fase a la recepción, y luego envío de paquetes de datos separados por espacios vacíos de información. Esta característica nos da una relación de bits en alto recibidos respecto a los medidos de un valor porcentual muy bajo. Es por esto que esta medición en el canal, usandola estratégicamente, nos puede dar mucha información de lo que está sucediendo.

## Capítulo 2

# Características generales del diseño

### 2.1. Objetivos globales del sistema

En base a la información recolectada establecemos los requerimientos base del que se parte para el diseño del producto final. Creemos adecuado realizar la separación de requerimientos en primarios y secundarios, ya que el sistema a desarrollar está enmarcado en el proyecto final de la carrera de grado de ingeniería electrónica donde, en conjunto con la cátedra, se intenta que los proyectos puedan culminarse en un plazo de tiempo lógico para la obtención del título, dando la posibilidad de seguir explayándose en el mismo a posterior.

De este modo, como objetivos primarios se establecen:

- Identificar la presencia de señales con una potencia suficiente para inhibir la comunicación: como en el marco teórico se ha estudiado en profundidad, la etapa amplificadora receptora sufre una compresión de la ganancia cuando en su entrada hay presente una señal de alto nivel de potencia. Es por esto que se establece como requerimiento del sistema poder identificar una señal que cumpla con estas características.
- Medir la ocupación del canal: Ha quedado claro que la trama de comunicación de las llaves remotas con los receptores de los automóviles poseen características de espaciado entre paquetes de datos transmitidos, es por esto que el sensado de la ocupación del canal se vuelve una



medida crucial para determinar si hay o no presencia de interferencias.

- Activar alarmas sonoras y visuales en caso de estar en presencia de una inhibición: el sistema debe tener la capacidad de determinar si hay presente una inhibición en su área de operación y, de ser así, debe disponer de métodos para dar alerta local de lo que está sucediendo.
- Disponer de comunicación a sistemas externos complementarios: un requisito del sistema es que posea la capacidad de enviar la información recolectada a un lugar remoto. Se prefiere la utilización de una metodología de comunicación inalámbrica y ampliamente distribuida.
- Cargar los datos en una base de datos: es importante que la información de las inhibiciones detectadas sea subida a una base de datos que permita visualizar de manera remota y en tiempo real lo que está sucediendo con los sistemas de seguridad activos, brindando la posibilidad de generar estadísticas y observar qué tipos de inhibidores están operando en la zona.
- Orientar el diseño del proyecto a la optimización de costos y recursos: es muy importante para el curso del trabajo que el diseño se realice haciendo uso racional de los recursos disponibles, apuntando a la posibilidad de producir muchas unidades del sistema de seguridad y obtener ganancias.

Como objetivo secundario se define:

- Estimar la procedencia de la interferencia: el único objetivo secundario del sistema es que tenga la capacidad, mediante el método más conveniente, de determinar la posición estimada de la fuente de interferencia activa. Esto está planteado de esta manera debido a que se desconoce la factibilidad de su realización en el marco del proyecto de fin de grado de ingeniería electrónica.

## 2.2. Esquema de funcionamiento

En la figura 2.1 se puede observar el sistema planteado para solucionar el desafío de detectar inhibiciones en los sistemas de seguridad vehicular. El mismo contará con nodos detectores que operarán en 433,92 MHz, un canal



de comunicación hacia la central, haciendo uso de un protocolo que más adelante se detallará y una central de operación donde se decidirá si hay o no inhibición en su área de operación desatando las alarmas pertinentes y subiendo la información al servidor.

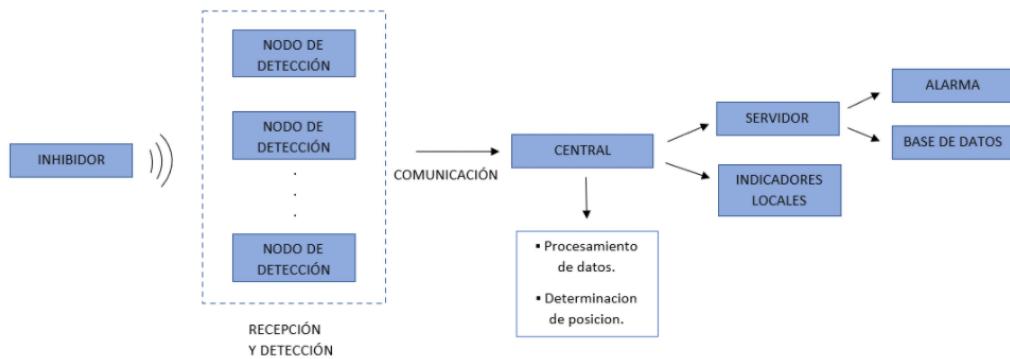


Figura 2.1: Diagrama en bloques sobre el funcionamiento del sistema global

### 2.3. Subsistemas que lo componen

En esta sección únicamente se hará mención de los subsistemas que componen al producto final, más adelante se detallará en capítulos el funcionamiento particular de cada uno de estos bloques.

- Nodo receptor
  - Microcontrolador STM32F103C8T6.
  - Receptor de RF.
  - Integrado para comunicación RS-485.
- Central de procesamiento
  - Microcontrolador STM32F103C8T6.
  - Integrado para comunicación GSM/GPRS.
  - Integrado para comunicación RS-485.

# Capítulo 3

## Selección de componentes

En este capítulo se procede a exponer las características mas importantes de los componentes del sistema, así como las consideraciones y posibilidades que tuvimos en cuenta en el proceso de selección de los mismos.

En el momento de comenzar este proyecto, rápidamente nos vimos ante la necesidad de seleccionar los componentes de nuestro sistema. En este proceso tuvimos en cuenta los objetivos y el diagrama de funcionamiento general que se trató en el capítulo de características que precede, además de otras consideraciones como el costo, los conocimientos previos del equipo sobre el componente, disponibilidad, etc. Para poder explicar como fue este proceso, dividimos el sistema en tres etapas: Recepción, procesamiento, y comunicación.

### 3.1. Etapa receptora de RF

De acuerdo al planteamiento del sistema, una parte crucial en el funcionamiento del mismo es la recepción de la señal de interés. Vale recordar que la etapa de recepción se encuentra presente en todos los nodos del sistema, por lo que las diferencias de costos en este apartado se ven multiplicadas.

La recepción debe cumplir con las siguientes características:

- Antena para 433MHz. Es el primer componente a tener en cuenta cuando hablamos de comunicaciones inalámbricas. En este caso, este transductor nos servirá para obtener la energía eléctrica que podemos entender y analizar, a partir de las ondas electromagnéticas emitidas por la llave de automóvil y por los inhibidores. Planteamos la posibilidad



de utilizar dos tipos de antenas, del tipo omnidireccional o una con la capacidad de generar un barrido, característica importante si se quiere obtener la posición del inhibidor.

- Demodulación de señales ASK en 433MHz. Es el principal requerimiento de la recepción debido a las características de las comunicaciones presentes en los sistemas de seguridad de vehículos.
- Medición de RSSI. La medición del nivel de potencia de la señal recibida es crucial para poder identificar adecuadamente a los inhibidores. También cumple un rol indispensable en uno de los objetivos secundarios mas desafiantes del sistema como lo es la obtención de la posición del elemento inhibidor mediante triangulación.
- Comunicación con microcontrolador. Es importante tener en cuenta las posibilidades que nos ofrece esta etapa a la hora de comunicarse con la siguiente. Los datos obtenidos de la recepción de la señal serán procesados por un microcontrolador.

Luego de estudiar las mejores opciones llegamos a una que consiste en utilizar un esquema como el que vemos en la figura 3.1. En primer lugar elegimos utilizar una antena omnidireccional, es la opción que nos permite reducir los precios y simplificar el proyecto al evitar sistemas de matrices antenas o antenas con rotación. El inconveniente de esta elección, es que la antena omnidireccional no nos entrega información referida al ángulo en que recibe la señal, por lo que complica la obtención de la posición. Sin embargo, todavía es posible comparando la lectura del nivel de RSSI de cada nodo. Luego encontramos un divisor de potencia de RF que se encarga de entregar la señal al demodulador ASK, y al medidor de potencia.

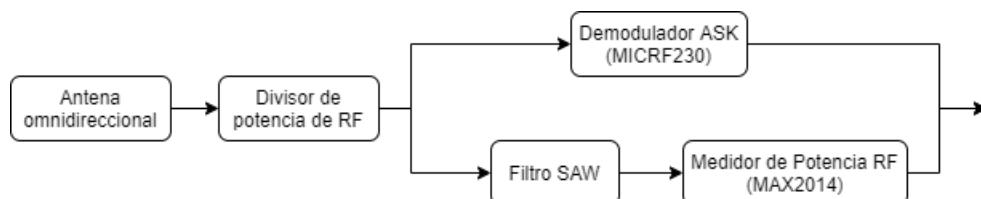


Figura 3.1: Etapa receptora - primer opción

Vemos que este diagrama cumple con las características anteriormente expuestas. Sin embargo, al final nos decantamos por otra opción, que consiste



en utilizar el circuito integrado CC1101 (transceptor de RF hasta 1GHz). La incorporación de este nos permite reducir mucho los costos y simplificar el sistema sin sacrificar características importantes.

En la figura 3.2 vemos como resulta el nuevo diagrama de la etapa receptora.

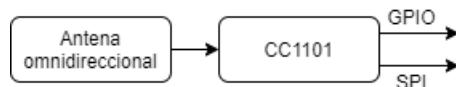


Figura 3.2: Etapa receptora - opción elegida

A simple vista podemos apreciar que se reducen la cantidad de componentes. Esto se debe a que el módulo CC1101 es capaz de demodular la señal y entregar la secuencia de bits mediante un pin de GPIO, así como también medir la potencia de la señal y comunicar el valor mediante comunicación SPI. La única desventaja de esta opción es que posee peor rango de RSSI que un componente medidor de potencia específico para ese fin, esto provoca que señales de gran potencia saturen nuestro receptor y nos imposibilite triangular de manera correcta, sin embargo la determinación de la posición es un objetivo secundario.

En la sección [1] se exponen en detalle las características del módulo.

### 3.1.1. CC1101

#### Transceptor



Figura 3.3: Transceptor CC1101



**Descripción del componente** El integrado CC1101 es un transceptor de frecuencias inferiores a 1GHz de bajo costo para aplicaciones inalámbricas de baja potencia. Está destinado principalmente a aplicaciones ISM (industrial, científico y médico) y bandas de frecuencia SRD (Dispositivo de corto alcance) a 315, 433, 868 y 915Mhz, pero puede ser programado para funcionar en otras bandas. El transceptor RF está integrado con un módem de banda base configurable que admite varios formatos de modulación.

Proporciona un amplio soporte de hardware para manejo de paquetes, almacenamiento en búffer de datos, transmisiones de ráfagas, evaluación de canal, indicación de calidad de enlace y wake-on-radio.

En un típico sistema, el CC1101 se utiliza junto con un microcontrolador y algunos componentes pasivos adicionales.

**Características generales** En este apartado mostramos algunas características importantes del CC1101 sin extendernos demasiado. Si se quiere mas información sobre este integrado ver [1].

- Alimentación de 3.3V
- Sensibilidad:
  - 116 dBm a 0.6kBaud en 433MHz
  - 112 dBm a 1.2kBaud en 868 MHz
- Velocidad de datos: Hasta 250kbaud en ASK.
- Bajo consumo de corriente: 14.7mA en RX.
- Admite 2-FSK, 4-FSK, GFSK y MSK, así como OOK y ASK.
- Medición de RSSI entre -110dBm a -20dBm.
- Interfaz SPI, a través de la cual se puede configurar todos los registros.
- Filtro digital de banda ancha programable. 58-812kHz.



## Módulo

El modulo aporta simplicidad al sistema, ya que contiene los componentes pasivos necesarios para el funcionamiento del CC1101. También permite mejor acceso a los pines del integrado y tiene conexión SMA para antena. En nuestro caso particular, este módulo fue necesario debido a que simplifica la soldadura manual y porque tiene una gran disponibilidad en el mercado.

En la figura 3.4 podemos ver el esquemático del módulo y en la figura 3.5 podemos ver su aspecto físico.

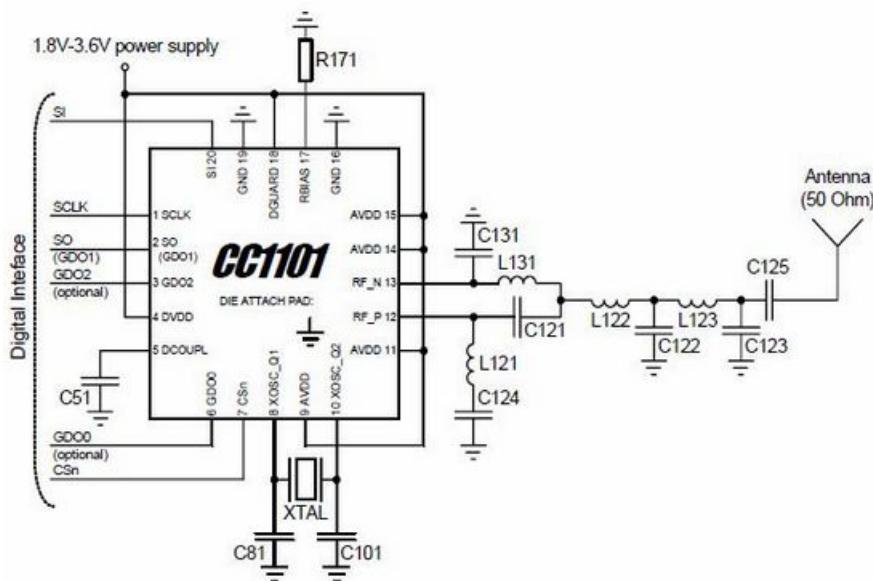


Figura 3.4: Esquemático CC1101

Se puede observar en el esquemático, que el módulo es muy simple en cuanto a los componentes que posee. Pero aún así es muy útil para nuestra aplicación.

## 3.2. Comunicación

La comunicación se puede dividir en dos partes, la primera referida a la comunicación entre los nodos y la central y la otra, referida a la comunicación de la central con un servidor web.



Figura 3.5: Módulo CC1101

### 3.2.1. Comunicación local

Según nuestros objetivos, la comunicación debe reunir las siguientes características:

- Resistencia a ataques de inhibidores. Es importante que la comunicación local no sea vulnerable a los mismos ataques que intentamos identificar, ya que si fallara la comunicación entre los nodos y la central el sistema no puede dar aviso de la presencia de una señal interferente.
- Comunicación bidireccional. Para establecer una red multinodal adecuada necesitamos un sistema de comunicación half-duplex o full-duplex, ya que la central comandará a los nodos, los cuales le responden con la información que la central les requiere.
- Distancia mayor a 1000m. Es probable que el sistema sea instalado en lugares abiertos como estacionamientos, por lo que necesitamos un protocolo de comunicación capaz de funcionar a largas distancias.
- Buena velocidad de comunicación. No requerimos de velocidades muy altas, sin embargo es una característica a tener en cuenta.
- Cableado de bajo costo. Como ya mencionamos, es probable que la distancia entre nodos sea grande, por lo que el precio del cableado debe ajustarse a nuestros objetivos.



Teniendo en cuenta las necesidades y analizando las opciones, determinamos que la mejor opción para nuestra aplicación es usar el estándar de comunicación RS485. Este está definido como un sistema de bus diferencial multipunto, ideal para transmitir a altas velocidades sobre largas distancias y a través de canales ruidosos. El medio físico de transmisión es un par trenzado con una longitud máxima de 1200 metros operando entre 300 y 19200 bit/s y la comunicación semiduplex.

Las especificaciones de este estándar son:

- Interfaz diferencial
- Conexión multipunto
- Alimentación de 5V
- Hasta 32 estaciones
- Velocidad Máxima de 10Mbit/s (a 12 metros)
- Longitud máxima de alcance de 1200 metro (a 100kbit/s)
- Rango de bus de -7V a +12V

Para nuestra aplicación usaremos el RS485 en combinación de la UART de nuestro microcontrolador, por lo que necesitaremos utilizar un transceptor MAX485 (ver sección 3.2.2). Se dispone uno en cada nodo y en la central. El MAX485 tiene la capacidad de transformar los datos de la UART al estándar RS485 y viceversa.

### 3.2.2. MAX485

MAX 485 es un transceptor de baja potencia para comunicación RS-485 y RS-422. Cada integrado contiene un controlador y un receptor.

La velocidad de respuesta del controlador del MAX485 no está limitada, lo que les permite transmitir hasta 2,5 Mbps. Estos transceptores consumen entre 120  $\mu$ A y 500  $\mu$ A de corriente de suministro cuando están descargados o completamente cargados con controladores desactivados. Todas las piezas funcionan con un solo suministro de 5V.

Los controladores tienen limitación de corriente de cortocircuito y están protegidos contra una disipación de energía excesiva mediante un circuito



Figura 3.6: Max 485

de apagado térmico que coloca las salidas del controlador en un estado de alta impedancia. La entrada del receptor tiene una característica a prueba de fallas que garantiza una salida lógica alta si la entrada está en circuito abierto. El MAX485 está diseñado para aplicaciones semidúplex.

### 3.2.3. Comunicación con Servidor Web

Una de las características mas importantes del proyecto, es la capacidad de subir la información a un Servidor Web, por lo que es indispensable que la central disponga de conexión a internet.

Debido a que no podemos asegurar que en el lugar donde se instale el sistema cuente con conexión a internet cableada o WiFi, decidimos utilizar conexión GPRS/2G.

En el mercado podemos encontrar varios módulos para este tipo de conexiones. En la tabla 3.1 podemos ver algunas opciones.

Nosotros elegimos el módulo sim800l por dos razones, la primera es el bajo precio comparado con el sim900 y la segunda por la experiencia previa que disponíamos con este módulo. En la sección 3.2.4 se detallan las características de este componente.

### 3.2.4. SIM800L

#### Descripción del componente

Utilizamos el SIM800L a través de un módulo del mismo nombre, como se suele utilizar normalmente. El módulo nos permite acceder a los pines mas importantes del SIM800L para manejarlo desde un microcontrolador.



Módulo	SIM800L	SIM900	A6
Velocidad de transmisión	1200 bp - 115200 bp.	1200bp - 115200bp.	1200bp - 115200bp.
Tensión de operación	3.4V - 4.4V	9V - 20V	3.3V - 4.2V
Corriente	Hasta 2A	Hasta 2A	Hasta 2A
Comunicación	Comunicación serial	Comunicación UART	Comunicación serial
Precio	13,39 usd	48,70 usd	18,26 usd

Cuadro 3.1: Módulos GSM/GPRS disponibles en el mercado

Consiste en un circuito integrado cuatribanda que permite agregar funcionalidades avanzadas de comunicación a través de la red celular, como mandar mensajes de texto, datos o realizar llamadas en un tamaño sumamente compacto.



Figura 3.7: Módulo SIM800L

### Características Generales

A continuación se listan algunas características importantes de este módulo. Sin embargo, si se quiere ver en mayor profundidad ver [2].

- Tensión de operación: 3.4V - 4.4V
- Nivel lógico de 3-5V



- Consumo de corriente:
  - Máximo: 500mA con picos de 2A
  - En reposo: 0,7mA
- Interfaz serial UART
- Quad-Band 850/900/1800/1900MHz. Conexión a cualquier red mundial por 2G.
- Controlado por comandos AT
- Velocidades de transmisión serial desde 1200bps hasta 115 200 bps
- Tamaño de la SIM: Micro SIM

### 3.3. Procesamiento

Tanto en los nodos como en la central, es indispensable el uso de un microcontrolador. En el caso del nodo, se encarga de comunicarse con la etapa receptora, procesar la información y decidir si la señal recibida proviene de un inhibidor, luego debe ser capaz de comunicarse con el MAX485 para establecer la comunicación RS485 con el resto del sistema. En la central, el microcontrolador es el encargado de recibir la información de nodos a través del MAX485 y, en caso de la presencia de una inhibición, activar las alarmas correspondientes y actualizar la información en el servidor web mediante el módulo sim800l.

El microcontrolador que utilizamos, tanto para los nodos como en la central, es el STM32F103C8T6. La decisión de utilizar este se tomó debido a sus características, el bajo precio y sobre todo porque ya contábamos con experiencia en su uso. En este caso, decidimos utilizar un módulo de desarrollo llamado "Blue Pill". Las características de esta placa la podemos ver en la sección 3.3.1.

En la tabla 3.2 podemos ver una comparación entre nuestro microcontrolador y otras opciones similares de otros marcas.

Es importante añadir que podemos programar la Blue Pill mediante un programador STLINK v2, que tiene un precio bajo comparado a otros programadores, y utilizar el programa STM32CubeIDE del fabricante para debuggear el sistema, característica que fue muy importante en el desarrollo del proyecto.



	Blue Pill	Arduino Nano	PIC18F4520
Procesador	ARM 32 bits	AVG 8bits	PIC 8bits
Frecuencia de Funcionamiento	72MHz	20MHz	8MHz
Memoria FLASH	64 o 128kb	32kb	32kb
SRAM	20Kb	2Kb	2Kb
comunicación	USB. SPI. I2C. USARTs	USB. SPI. I2C. USARTs	EUSART. SPP. USB. SPI. I2C
Precio	6,20 usd	6,67 usd	13,39 usd

Cuadro 3.2: Comparación de microcontroladores

En la sección 3.3.1 ahondamos mas sobre este módulo y el microcontrolador en cuestión.

### 3.3.1. Blue Pill STM32

#### STM32F103C8T6

Es un microcontrolador perteneciente a la linea de rendimiento medio de la familia STM. Incorpora el núcleo RISC ARM Cortex de 32 bits de alto rendimiento, posee memorias integradas de alta velocidad y una amplia gama de entradas y salidas. Este dispositivo ofrece dos ADC de 12bits, tres temporizadores de 16bits de uso general mas un temporizador PWM, así como diversas interfaces de comunicación.

Es apto para gran variedad de aplicaciones, como unidades de motor, control de aplicaciones, equipos médicos y portátiles, periféricos de PC y juegos, plataformas GPS, aplicaciones industriales, PLC, inversores, impresoras, escáneres , sistemas de alarma, videoporteros y HVAC.

A continuación se listan algunas de las características que nos parecen mas importantes:

- Tensión de operación: 2 a 3,6V
- Frecuencia de 72MHz
- Memorias integradas de alta velocidad



Memoria Flash de 128Kbytes

Memoria SRAM de hasta 20Kbytes

- Interfaces de comunicación: Dos I2C y SPI, tres USART y un USB.
- 37 GPIOs
- Dos ADC de 10 canales.

### Módulo Blue Pill

En nuestro sistema utilizamos la placa de desarrollo llamada Blue Pill. Esta placa incorpora al STM32F103C8T6 y aporta los componentes pasivos adecuados para su uso, además de dos cristales, entrada microUSB, leds indicadores, botón de reset e integrado para regulación de tensión.

Incorporar esta placa simplifica el diseño de nuestros PCB, ya que nos facilita el acceso a los pines del microcontrolador y posibilita la conexión con el programador, además nos permite desarrollar un proyecto donde soldemos de forma manual los componentes, reduciendo costos.

En la figura 3.8 vemos el esquemático de esta placa.

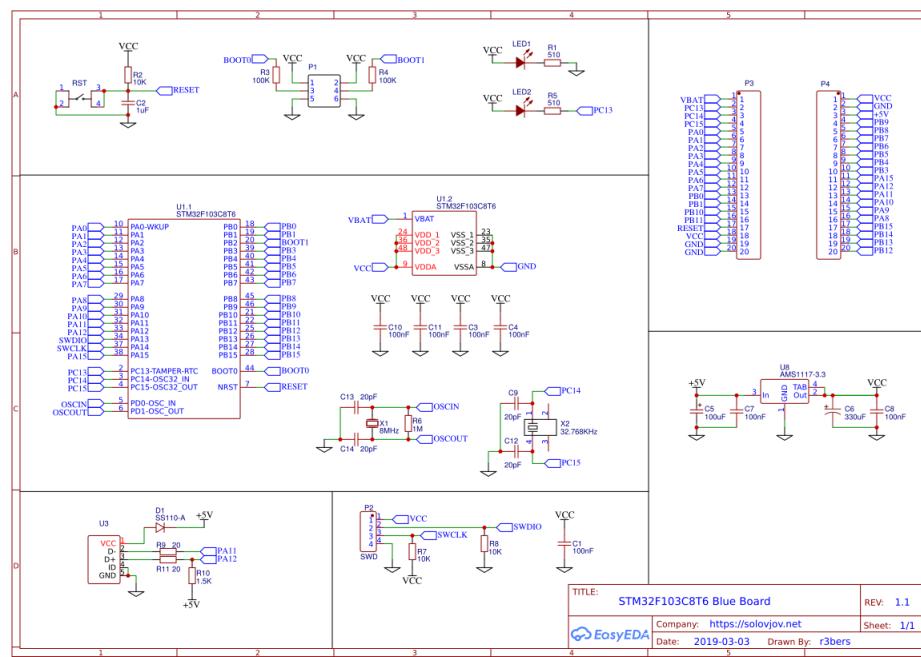


Figura 3.8: Esquemático de Blue Pill

# **Capítulo 4**

## **Central de procesamiento**

### **4.1. Descripción general**

El diseño general del sistema se pensó como tres nodos de escucha que son comandados por medio de una central de procesamiento. Los requerimientos de la misma se establecen para lograr una comunicación estable y segura con cada uno de los nodos, donde en caso de detectar una inhibición por parte de cualquiera de ellos, requiera el estado de los otros dos para así activar las alarmas correspondientes, comunicarse al servidor web y volver a iniciar el sistema de cero una vez que se haya terminado el proceso correctamente, dando también un reporte del estado de salud de cada nodo en particular.

En este capítulo se presentará la forma en que se llevó a cabo el desarrollo de la misma, indicando su funcionamiento, primer prototipo, diseño final y la implementación de un gabinete.

#### **4.1.1. Funcionamiento**

El funcionamiento de la central se podría dividir en tres partes interconectadas que se detallan a continuación.

##### **Comunicación con nodos**

Como ya se detalló en el apartado 3.2.2, la comunicación optada para la conexión de los 4 dispositivos es RS485 por su forma de transmisión diferencial y largo alcance.



Al inicio del sistema la central (funcionando como el maestro en la comunicación) requiere el estado de cada nodo, del cual si alguno detecta una inhibición comenzaría el proceso para ver el estado de los demás nodos y comenzar a activar alarmas.

### **Alarmas locales**

Una vez detectada la inhibición y procesado el estado del sistema en general se dan las alarmas visuales y sonoras en la central misma para dar aviso al personal de seguridad que se encuentra en el lugar.

### **Comunicación remota al servidor web**

Como ya vimos en el apartado 3.2.4, la comunicación con el servidor web se hace de manera remota mediante GPRS una vez que se encuentra el sistema en un estado de alarma, cargando en el mismo la ubicación, ID de nodos, entre otros que se detallarán en las siguientes secciones.

## **4.2. Prototipo**

### **4.2.1. Diseño**

#### **PCB**

En la figura 4.1 podemos ver una vista superior (izquierda) e inferior (derecha) de la placa prototipo para llevar a cabo la implementación de esta.

### **4.2.2. Problemas surgidos**

Los principales problemas de esta primer aproximación al diseño final fueron en base a la alimentación requerida por el integrado de comunicación GPRS.

En primer lugar, era necesario un capacitor en la alimentación del SIM800 para suavizar el arranque del mismo, ya que al conectarse a una red GSM/GPRS requiere un pico de corriente de 2A.

Por otra parte, al tener que rediseñar la placa, notamos que la fuente conmutada implementada (encerrada en líneas cortadas en la figura 4.1) requería

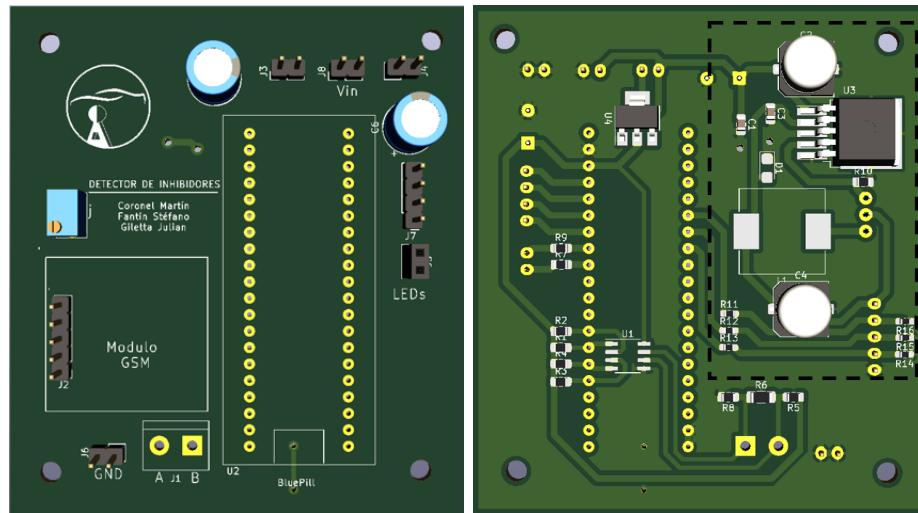


Figura 4.1: Prototipo de placa de la central de procesamiento.

gran cantidad de componentes, aumentando así el costo, principalmente con el integrado e inductor necesarios. Por ello, se optó como solución un regulador lineal que con tan solo dos capacitores y dos resistencias se obtienen los requerimientos necesarios.

### 4.3. Diseño final

#### 4.3.1. Software

Para no volver redundante la explicación respecto del prototipo, se optó que el funcionamiento del sistema embebido se detalle en esta sección ya que en cuanto a este no fueron grandes los cambios realizados.

En este apartado se nombraran como se llevaron a cabo los siguientes items:

- Comunicación con nodos
- Salud de nodos
- Alarma sonora y visual
- Subida de datos al servidor web



## Comunicación con nodos

Comenzamos nombrando esta etapa ya que es la tarea mas importante que ocurre en el dispositivo, un buen esquema de comunicación determina el buen funcionamiento del sistema en fin, ya que si bien los nodos son los encargados de detectar las inhibiciones, la central es el maestro que activa o no las alarmas y avisos.

Como ya se nombró en la sección 3.2.2, la comunicación RS485 es half-duplex y debe existir un dispositivo maestro (en nuestro caso es el que se está desarrollando), el cual es el encargado de generar requerimientos a cada dispositivo de la red y, si es necesario, esperar una respuesta de estos.

Para entender el funcionamiento podemos ver la imagen 4.2 en donde se observan 3 columnas correspondientes cada una a un estado de funcionamiento.

En el estado 0, la comunicación es continua y rige un ciclo de un requerimiento de nodo por vez. La palabra es de 2 bytes, donde el primero corresponde al ID del nodo requerido y el segundo indica el estado que ocurre, esperando una respuesta por parte del nodo de una trama de 3 bytes designada de la forma que el primer byte corresponde nuevamente al ID del nodo, el segundo byte en este caso es 0 y en el tercero el nodo reporta su estado de inhibición (0 para decir que no detecto inhibición, 1 y 2 para alertar a la central que hay una inhibición ocurriendo). En caso de que el tercer byte de respuesta sea distinto de 0, pasaremos al estado siguiente.

En el estado 1, los requerimientos nuevamente es de un nodo a la vez y solo se volverá a ejecutar en el momento que un nodo no responda y deba chequear que solo fue una desincronización o que este se encuentre fallando. Aquí la palabra que envía la central es de 2 bytes indicando en el primero el ID del nodo y en el segundo un 1, correspondiente al estado que se encuentra, esperando recibir una respuesta de cada nodo con 3 bytes (ID de nodo, valor de RSSI medido y estado de inhibición). Al tener la respuesta o no de cada uno se actualizan las banderas de presencia de inhibición, salud de los nodos, comienza la activación de alarmas y carga de datos al servidor web.

Posterior al comienzo de carga de datos al servidor, se pasa al estado 2 el cual envía repetidas veces en poco tiempo la palabra de 2 bytes ^2correspondiente al reset del sistema para volver a ponerse en modo de escucha y comenzar el ciclo nuevamente.



ESTADO 0	ESTADO 1	ESTADO 2
Requerimientos a nodos por turnos  ID_Nodo   0	Requerimientos a nodos por turnos  ID_Nodo   1	Envío orden de reseteo a nodos  A   2
Recepción de trama  ID_Nodo   0   Estado de Inhibición	Recepción de trama  ID_Nodo   Valor RSSI   Estado de Inhibición  Actualización de banderas y activación de alarmas	Limpieza de vectores y banderas de recepción
Si Estado de Inhibición ≠ 0 Paso a Estado 1		

Figura 4.2: Estados de la central en comunicación con nodos.

### Salud de nodos

La salud de los nodos es un dato muy importante para saber que el sistema no falle, por ello la central tiene 3 leds en la parte frontal que indican si alguno no esta contestando los requerimientos pedidos, los cuales actualizan su estado en cada ciclo, permitiendo así una visualización en tiempo real de la misma.

### Alarma sonora y visual

Localmente, al haberse activado las alertas de inhibición presente se activa un indicador lumínico en la central y un pitido de 1 segundo para avisar al personal de seguridad o a la persona a cargo el hecho que ocurre.

### Subida de datos al servidor web

El enfoque que se le quiso dar a este sistema en general es la posibilidad de generar una base de datos de acceso remoto, no solo para poder triangular la posición en caso de ser posible, sino también pensando en que se pueda disponer este tipo de dispositivos en diferentes zonas y así generar estadísticas



que tenga acceso cualquier persona y alertar sobre este tipo de episodios.

El desenlace de carga de datos remotamente vía GPRS se da al fin del ciclo de detección. En este caso pasa algo particular, donde el integrado utilizado requiere que se le envíen una serie de comandos para ser ejecutados con cada acción y a su vez cada uno de ellos se puede enviar cada cierto tiempo. Por ello, para que el sistema no se congele cargando datos y dejando de escuchar los canales de 433.92MHz, esta se realiza en una interrupción del sistema, con los comandos a enviar cargados por DMA (direct memory access) y los retardos necesarios son generados por la cuenta de ticks (pulsos que se dan en el sistema cada 1ms) que no interrumpen la ejecución del código, permitiendo que mientras se cargan los datos, también se reinicie el sistema y se siga escuchando el canal por una nueva presencia de inhibición.

La carga se realiza mediante un proceso de HTTP POST, que consiste de un formulario HTML, donde se le pasan los atributos necesarios para establecer el formato a cargar, en este caso se configura como “application/x-www-form-urlencoded”, que indica que los datos se pasan en forma de tuplas llave-valor separadas por ‘&’ y un ‘=’ entre la llave y el valor. Un ejemplo de como se vería la carga es:

```
POST / HTTP/1.1
Host: www.jammer-detector.ml
Content-Type: application/x-www-form-urlencoded
Content-Length: 19
```

RSSI=45&mode\_inhi=1

#### 4.3.2. Hardware

En este apartado se mostrará una descripción de la placa que contiene el MCU, los esquemáticos finales, el pcb obtenido y su modelo en 3D.

##### Esquemático

Como en el apartado de selección de componentes se ha expliado, como microcontrolador se hace uso del STM32F106C8T6. Este cuenta con un cristal de 8 MHz, el cual mediante un PLL interno es llevado a la frecuencia de operación de 72 MHz. En la figura 4.3 se puede observar lo antes mencionado.

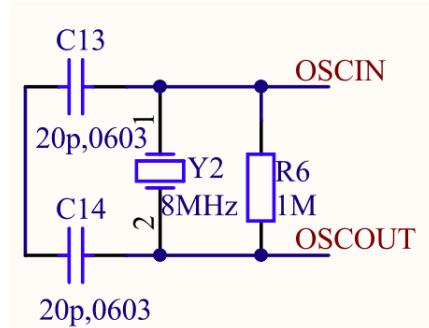


Figura 4.3: Cristal para el MCU

También cuenta con un regulador de 5V a 3.3V (figura 4.4) para la alimentación a los pines que manejan estos niveles de lógica y es utilizado también para el debugger. Por último como se observa en la figura 4.5, la placa tiene un botón de reset el cual es activo por bajo.

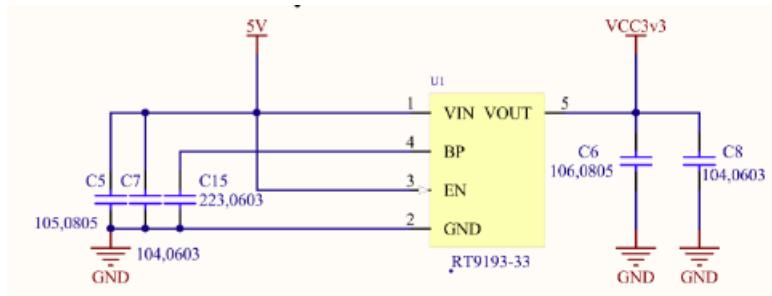


Figura 4.4: Regulador de 5V a 3.3V para MCU.

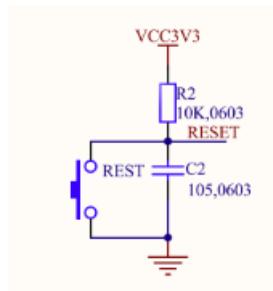


Figura 4.5: Reset de microcontrolador.



El esquemático en general se separó en varias partes para que se puedan observar de una manera mas ordenada en el presente informe. Estas 3 partes nombradas se pueden ver en las figuras 4.6, 4.7 y 4.8 con su descripción de la correspondencia de cada una de ellas.

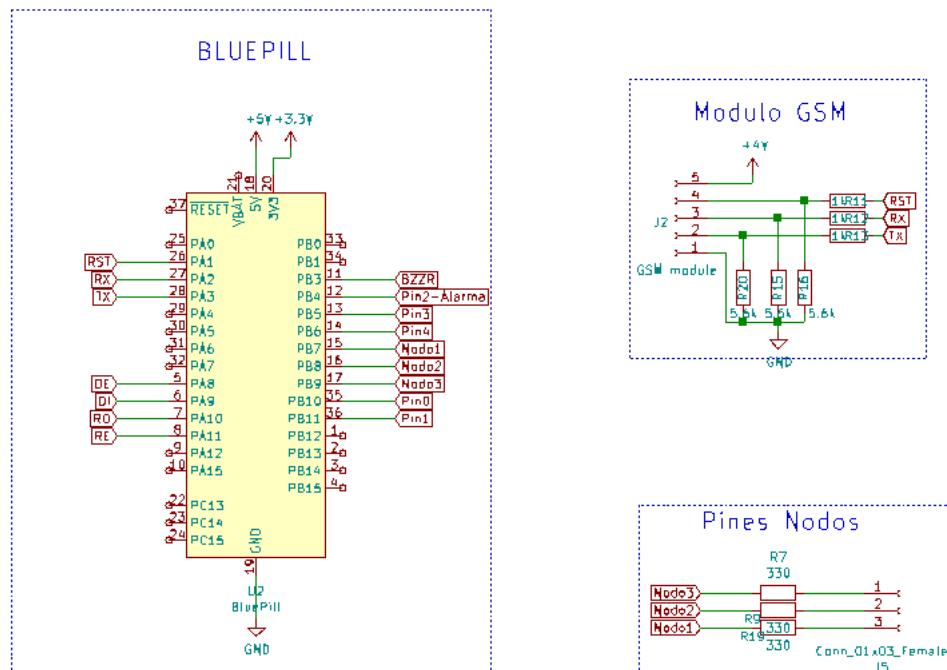


Figura 4.6: MCU, modulo GSM/GPRS y leds indicadores de nodos.

## PCB

En la figura 4.9 vemos el diseño final de la placa de la central, el cual se diferencia al prototipo (figura 4.1) en la fuente comutada, que fue reemplazada por una lineal y en la adición de los leds indicadores de estado de cada nodo.

## Modelo 3D

El modelo 3D de la placa la podemos observar en la figura 4.10 y el resultado finalizado en la imagen 4.11.

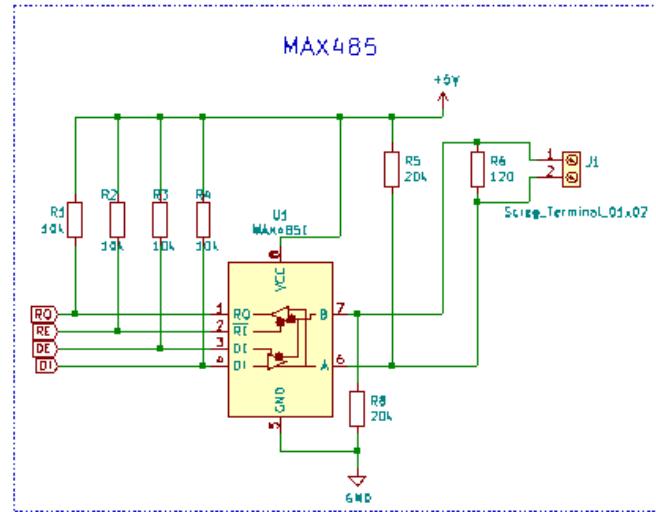


Figura 4.7: Sección de comunicación RS485.

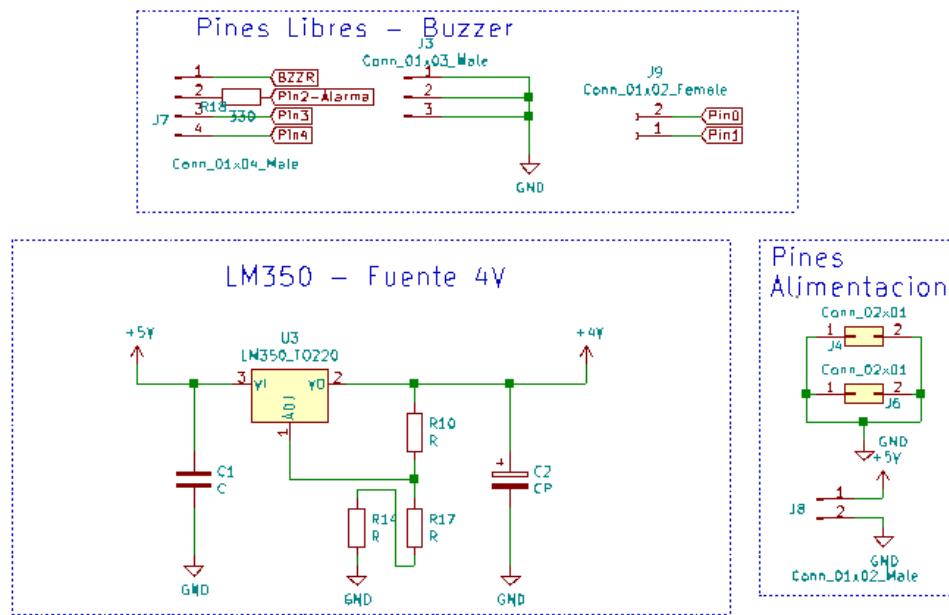


Figura 4.8: Pines de alimentación, regulación para SIM800 y pines libres para conexiones adicionales.

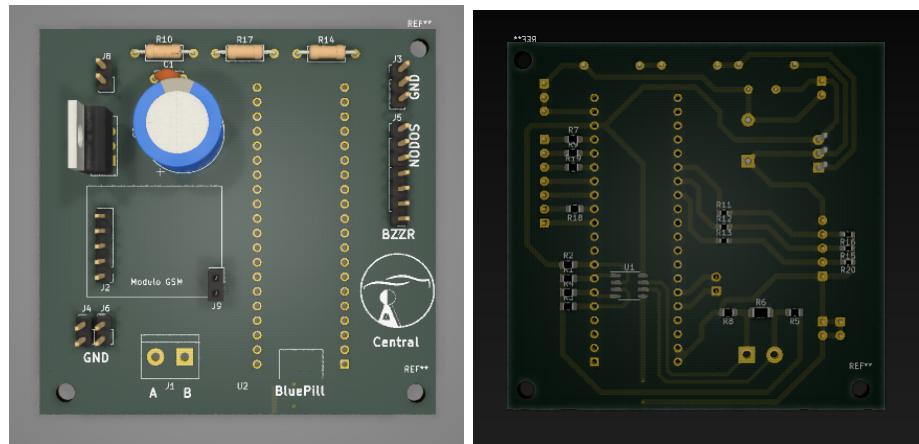


Figura 4.9: Diseño final de placa de la central de procesamiento.

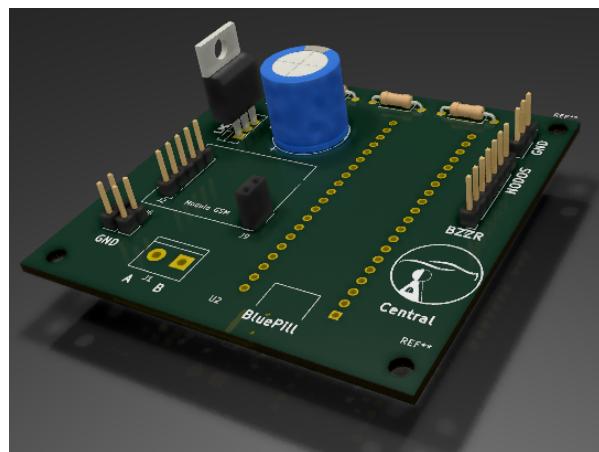


Figura 4.10: Vista en 3D de la placa final de la central de procesamiento.

#### 4.4. Gabinete

El diseño del gabinete (figura 4.12) de la central se buscó que fuera de una forma vertical, en donde por delante se observen cinco indicadores lumínicos que informar sobre el estado de inhibición del sistema (agregado de un buzzer también), el estado de salud de cada nodo y si está en funcionamiento o no.

Por la parte trasera encontramos un interruptor para alimentar a todos los nodos, conector para 12V y un conector GX5 para la comunicación RS485



Figura 4.11: Placa de la central terminada.

y llevar la alimentación a cada nodo bajo el concepto de power over ethernet.

El mismo se llevó a la realidad por medio de impresión 3D en plástico PLA negro. Para comodidad en el armado e impresión, vemos en la figura 4.13 que el modelo se dividió en 2 partes, donde una llamada ”base.” es la encargada de soportar la placa principal de la central y a la derecha de la imagen vemos lo que denominamos ”tapa”, donde encontramos los indicadores y demás conectores.

En las figuras 4.14 se puede apreciar el resultado final de la central en sus dos secciones de impresión y con el gabinete ya finalizado y ensamblado.

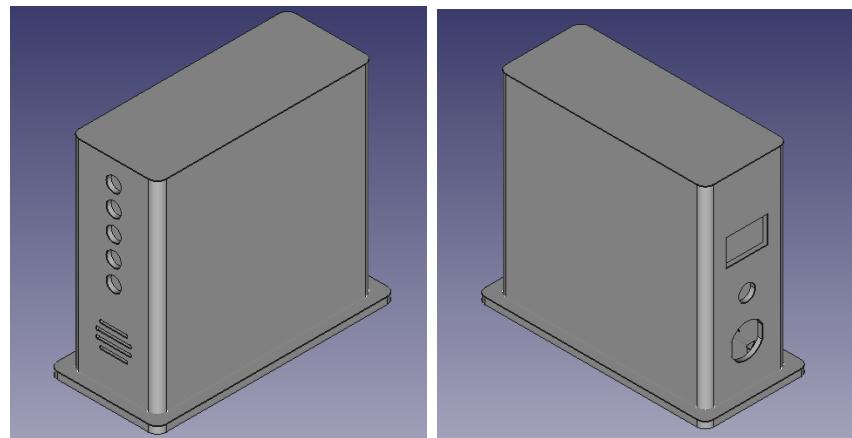


Figura 4.12: Gabinete de central armado.



Figura 4.13: Partes para el armado del gabinete de central.



Figura 4.14: Gabinete de central terminado.

# **Capítulo 5**

## **Nodos de recepción**

### **5.1. Descripción general**

En este capítulo haremos un análisis profundo sobre el funcionamiento de los nodos en el sistema de detección de inhibidores de alarma de autos. Para comenzar con el mismo es importante preguntarse: ¿qué funciones debe cumplir un nodo en el sistema? La respuesta a esto es evidente, en el nodo se producirá la recepción de la señal de RF mediante el módulo CC1101 de Texas Instruments, luego de esto la demodulación ASK efectuada por el receptor será procesada en el microcontrolador seleccionado para determinar si hay o no inhibición según estrategias más adelante detalladas y este se encargará de realizar la comunicación mediante el protocolo RS485 con la central de procesamientos. Integrado en el nodo se utilizan tres protocolos de comunicación: en primer lugar tenemos la comunicación SPI que se encarga de la interacción entre el microcontrolador y el receptor seleccionado; esta comunicación se utiliza para configurar los registros del CC1101 para establecer el modo de trabajo deseado. En segunda instancia tenemos comunicación serial asíncrona con un pin de salida del receptor por el cual se mandan los datos RAW de demodulación en el canal seleccionado y en último lugar tenemos el protocolo RS485 para la comunicación de la red armada.

### **5.2. Prototipo**

El proceso de obtener un sistema sólido y que responda a las necesidades planteadas llevó consigo la necesidad de elaborar dos modelos distintos



Figura 5.1: Primer placa del nodo armada

de nodo. En un comienzo se buscó que el mismo tenga una realimentación visual de las mediciones tomadas, por lo que, además de procesar las señales mediante las estrategias de detección establecidas, se asignaron salidas en seis leds que se encargaban de indicar la potencia de RF medida con el RSSI como se puede observar en la figura 5.1.

El prototipo es bastante rudimentario, las placas fueron fabricadas de manera casera y sin tener grandes cuidados en los detalles. De igual modo este diseño bastó para pulir las imperfecciones que poseía en camino al desarrollo final.

Para el diseño del esquemático nos hemos basado en las prestaciones que nos brinda el microcontrolador STM32F106C8T6. El mismo cuenta con comunicación SPI y serial integradas, por lo que haciendo uso del entorno de programación propio del fabricante (STM32 Cube IDE) hemos asignado los pines respectivos a cada comunicación, como muestra la figura 5.2.

Trabajar con este entorno es muy beneficioso ya que facilita en algunos aspectos la configuración del microcontrolador seleccionado, teniendo la capacidad de, mediante una interfaz gráfica, activar comunicaciones, configurar los relojes, activar o desactivar interrupciones de timers y comunicaciones, entre otras.

Las interrupciones en nuestro diseño juegan un papel clave debido a que en la comunicación se ha optado en algunos casos particulares realizar el envío de los datos mediante interrupciones para que el procesador pueda continuar operando y no aboque todos sus recursos y tiempo de ejecución en enviar una palabra. De modo similar las interrupciones de timers nos han servido para realizar acciones con alta prioridad y que deben ejecutarse en un tiempo específico, como por ejemplo la lectura asíncrona de datos RAW

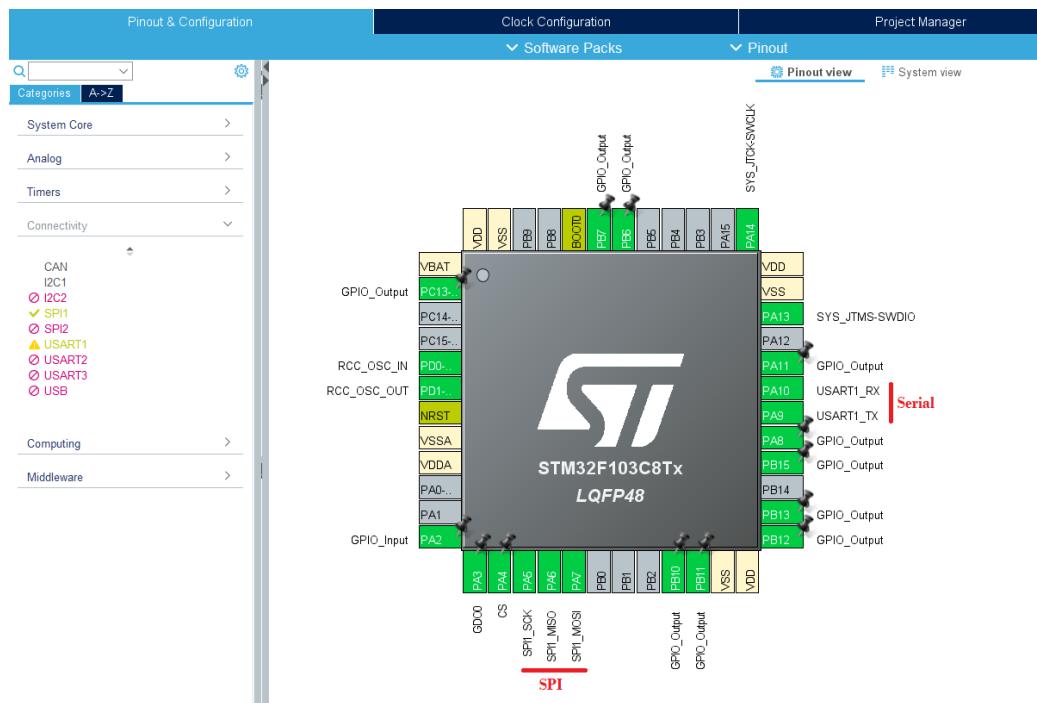


Figura 5.2: Asignación de pines para comunicación



enviados por un pin del CC1101. La configuración para las mismas se realiza de manera muy sencilla teniendo en cuenta el contador de ticks del sistema, la frecuencia del clock utilizada y un preescalador a determinar para lograr el tiempo deseado.

### 5.3. Diseño final

El diseño el nodo ha surgido ciertas variaciones en el transcurso de la búsqueda del producto final. Entre estas se encuentra la optimización del PCB reduciendo el tamaño del mismo, retirar los indicadores led y dotar la placa con el integrado destinado a la comunicación (SN75176). Para hacer un análisis particular del funcionamiento del nodo hemos decidido analizar independientemente el software del hardware.

#### 5.3.1. Software

El nodo al ser el encargado de recibir la señal de RF, demodularla y determinar si hay o no inhibición posee una alta carga de software desarrollado sobre él. De este modo señalaremos particularmente el desarrollo en cada uno de los siguientes aspectos.

- Recepción de RF.
- Estrategia de detección de inhibiciones.
- Comunicación con la central.

#### Recepción RF

El desarrollo de software en este aspecto satisface la necesidad que presenta el integrado receptor que utilizamos de ser configurado cada vez que este comienza a operar. Como previamente es analizado debemos establecer al dispositivo, que por características es un transceptor, en modo de recepción. Además se debe configurar la frecuencia de operación, el modo de demodulación, el tipo de salida de datos, entre otras muchas cosas que son cargadas en un total de 46 registros.

La carga de registros y los requerimientos de valor de RSSI que se le producen al CC1101 para tener noción de la potencia de RF en dBm que está



llegando al receptor se realizan mediante comunicación SPI. Estos requerimientos son periódicos y han sido establecidos con un tiempo prudencial para que la comunicación resulte efectiva y los datos permanezcan actualizados.

### **Estrategia de detección de inhibiciones**

La estrategia de detección de inhibiciones ha sido uno de los mayores desafíos a la hora de encarar el proyecto a causa de que el sistema debe ser confiable y robusto para poder instalarlo en una zona de operación y que no tenga fallos. Principalmente los errores de funcionamiento que son inadmisibles son:

- Falsas detecciones: que el sistema desate las alarmas cuando no hay presente un inhibidor o cuando en el canal se está comunicando un dispositivo que sí es apto para hacerlo, como por ejemplo una llave de auto.
- Falsos negativos: que el sistema sea incapaz de reconocer una señal que sea perjudicial para el sistema de seguridad de un automóvil.

Antes se ha profundizado en las estrategias de inhibición y se ha llegado a la conclusión de que existen dos métodos posibles para inhibir una comunicación, un método es saturación de la etapa receptora y el otro es por corrupción de la trama de datos. Para ambos métodos se ha debido realizar una estrategia de detección diferente, las cuales funcionan en simultáneo en el nodo para desatar las alertas correspondientes si detectaran positivo. A continuación en las figuras 5.4 y 5.3 se demuestra en bloques el funcionamiento de la estrategia de detección.

### **Comunicación con la central**

Para el corriente funcionamiento del sistema se precisa que los nodos se mantengan comunicados a la central, dando información de lo que cada uno está recibiendo y esta encargándose de manejar las alertas y los requerimientos a cada uno de los receptores.

Para que la comunicación sea lo más efectiva posible se decidió que respete siempre una estructura de comunicación constante en la que únicamente se cambiarán los parámetros a enviar. La comunicación se base en un maestro -la central- que genera peticiones por turnos a cada uno de los esclavos -los nodos-.

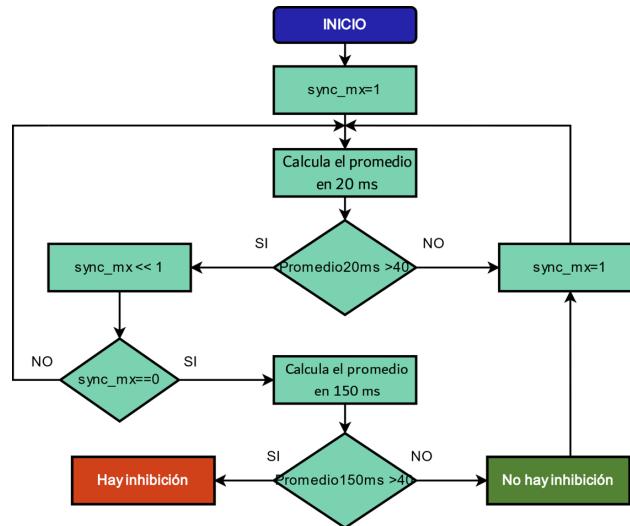


Figura 5.3: Estrategia de detección por corrupción de datos

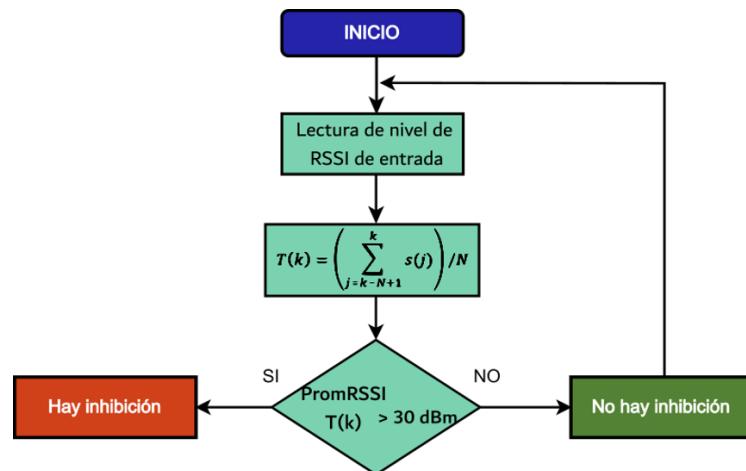


Figura 5.4: Estrategia de detección por saturación de etapa receptora



ID_Nodo	Valor RSSI	Estado
---------	------------	--------

Figura 5.5: Estados de comunicación en nodo

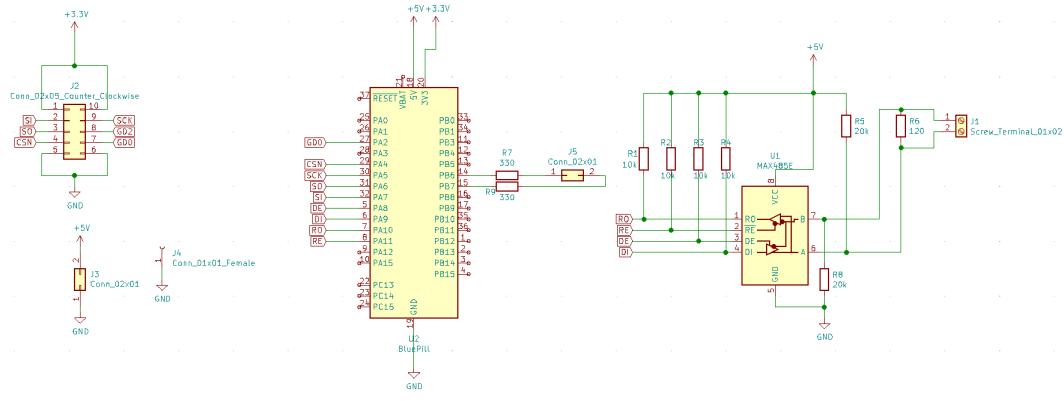


Figura 5.6: Esquemático del nodo receptor

Como antes se mencionó la trama de comunicación es única y puede observarse en la figura 5.5, donde ID Nodo hace referencia al identificador propio del nodo en la red, Valor RSSI al valor de intensidad de señal recibido por cada nodo y Estado hace referencia al estado de inhibición detectado, siendo 0 para no inhibición, 1 para inhibición por corrupción de datos y 2 para inhibición por saturación.

### 5.3.2. Hardware

En el nodo de recepción se hace uso del mismo MCU que en la central, de modo que las características de hardware antes mencionadas tienen completa validez aquí también. Comunicado por SPI y comunicación serial se encuentra el módulo CC1101, luego mediante comunicación serial asíncrona tenemos el SN75176. En la figura 5.6 podemos observar los tres bloques principales que lo componen.

Tenemos de izquierda a derecha en el esquemático los pines de conexión del CC1101, el cual está unido al MCU por seis pines, los cuales pueden ser seguidos por las etiquetas que este y el microcontrolador poseen y por último



tenemos el esquemático para la comunicación RS485.

El diseño 3D de la placa terminada se puede ver en la figura 5.7 y en la imagen 5.8 podemos apreciar el diseño final de la placa impresa. En las perforaciones que se observan van instalados los módulos utilizados que en el apartado de selección de componentes se mencionan.

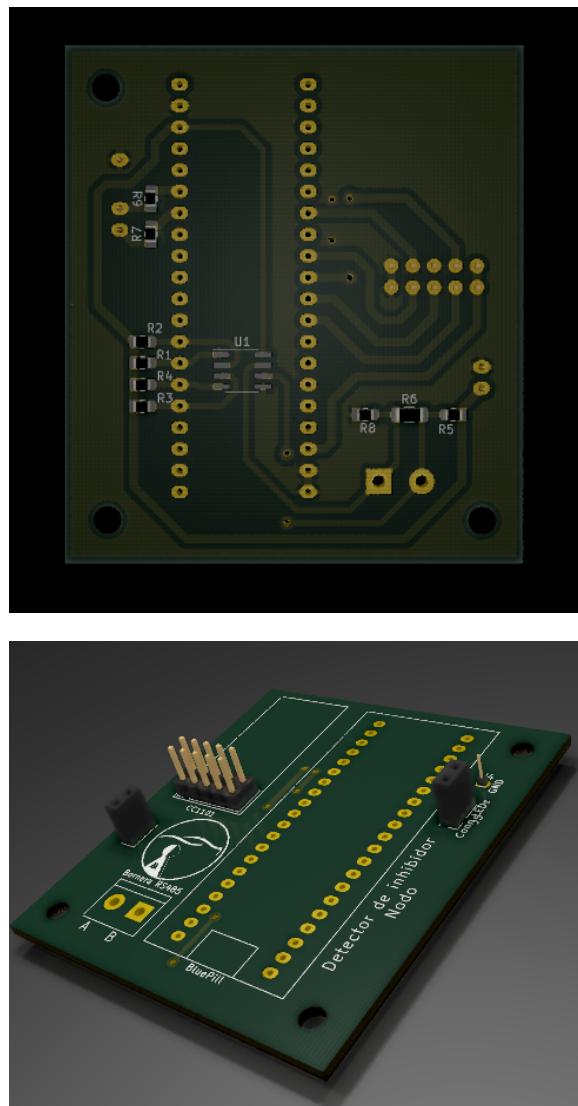


Figura 5.7: Diseño 3D del nodo receptor.



Figura 5.8: Placa final del nodo receptor.

### 5.3.3. Gabinete

El diseño del gabinete del nodo fue realizado con un diseño minimalista y con características cúbicas, separado en tres secciones que facilitan la impresión y el armado. El diseño terminado se muestra en la imagen 5.10.

El gabinete no posee realimentación visual del estado de funcionamiento, a simple vista es un cubo flotante con la antena de 433,92MHz asomando por uno de sus lados al que se ha buscado que no sea visible de qué manera ingresan los cables y la ficha GXS al sistema, para mayor estética. Está impreso en PLA negro, al igual que la central de procesamientos y tiene orificios para cuatro tornillos de modo que pueda ser instalado en una superficie plana.

En las figuras ?? se puede apreciar el resultado final del nodo en sus tres secciones de impresión y con el gabinete ya finalizado y ensamblado.

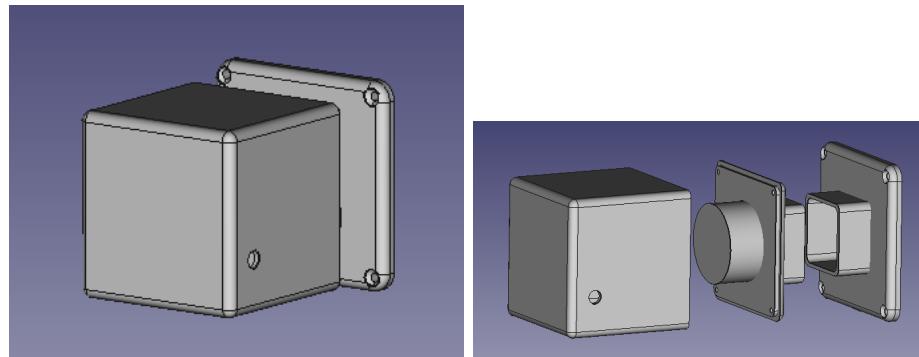


Figura 5.9: Diseño 3D del nodo receptor terminado.

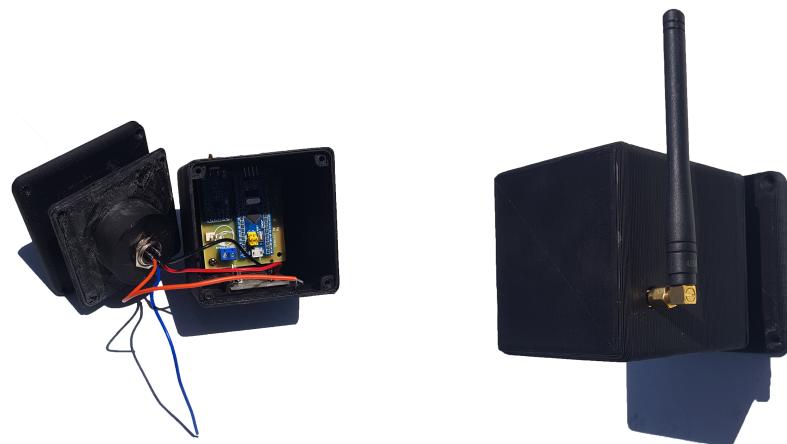


Figura 5.10: Gabinete del nodo receptor terminado.

# **Capítulo 6**

## **Ensayos**

En este capítulo hablaremos sobre los ensayos que se han realizado a lo largo del desarrollo del proyecto. Se llevaron a cabo diversas pruebas sobre las diferentes partes que componen el sistema, en cada sección de este capítulo se exponen los ensayos realizados a cada una de esas partes o subsistemas.

### **6.1. Análisis de llaves e inhibidores**

El primer conjunto de ensayos que realizamos fueron enfocados a conocer la naturaleza de las comunicaciones de los sistemas de seguridad vehicular y de los inhibidores. En esta instancia fue muy importante el uso de un SDR (Radio definida por software) para analizar el espectro de las señales y llevar a cabo la demodulación, como ya explicamos en la sección 1.1.2.

Las primeras mediciones las realizamos a distintas llaves, como podemos observar en la figura 1.2. Los datos obtenidos mediante el SDR fueron de gran importancia para conocer en profundidad la estructura de la comunicación de las llaves, información indispensable para establecer métodos de inhibición adecuados. Como ya lo mencionamos en 1.1.3, hay dos tipos de inhibiciones, por lo cual fue necesario obtener al menos dos inhibidores que ataquen al sistema de seguridad de esas maneras.

El primer inhibidor que usamos consiste sencillamente en un handie (o transceptor de radio portátil) que es capaz de emitir en la misma frecuencia que las llaves de los autos y debido a la potencia que posee logra saturar la etapa receptora de los automóviles. Por otro lado, para lograr inhibir por corrupción de datos fabricamos nuestro propio inhibidor, el cual emite un



tono de baja potencia dentro del ancho de banda del receptor, logrando corromper la trama de comunicación.

Los ensayos realizados con los inhibidores consistieron en conocer la vulnerabilidad de los sistemas de seguridad de los vehículos así como las distancias y potencias que se requerían para inhibir. En el caso del handie, es capaz de lograr interferir en la comunicación de la llave y el auto a distancias grandes debido a su alta potencia, mientras que en el caso del inhibidor por corrupción de datos necesita situarse a distancias cortas del vehículo. Esta información es muy importante para plantear un sistema realista y desarrollar una adecuada estrategia de detección.

## 6.2. Pruebas y configuración del CC1101

Una vez analizadas las características de las señales de interés con ayuda de un SDR estábamos listos para probar el integrado elegido para la recepción. En este ensayo utilizamos la Blue Pill para configurar los registros del CC1101 mediante comunicación SPI. La primer prueba consistió simplemente en constatar que la comunicación SPI funcionaba, esto se hizo configurando los registros con valores predeterminados y posteriormente requiriendo el valor de alguno de ellos desde la Blue Pill.

Con la comunicación funcionando procedimos a encontrar los valores adecuados para los registros de configuración del CC1101. Lo que se buscaba en este punto era configurar el integrado para que nos entregue la demodulación y el valor de RSSI de la señal que recibía, así como también dar con los valores adecuados de sensibilidad y ancho de banda. Para calcular los valores de los registros nos ayudamos del datasheet del CC1101 y del software SmartRF Studio, que recomienda el fabricante.

## 6.3. Ensayos de las estrategias de detección

En esta instancia ya éramos capaces de extraer los datos relevantes de la señal recibida y acceder a ellos mediante la Blue Pill, por lo que se procedió a desarrollar un algoritmo que, mediante estos datos, pueda decidir si la señal recibida se trata de una interferencia emitida por un inhibidor.

En primer lugar se creó un mecanismo simple y, gracias a ensayos utilizando llaves y nuestros propios inhibidores, fuimos mejorando nuestras es-



trategias de detección hasta volver al sistema confiable. La lógica de funcionamiento la podemos ver en las figuras 5.3 y 5.4

Hasta ahora, la Blue Pill la utilizamos conectada a una computadora para poder debuggear los programas que ensayábamos y así encontrar fallos de forma rápida. Sin embargo, en un producto final, debía ser capaz de actuar independiente, es por esto que en este punto desarrollamos el primer prototipo de nodo, que ya mostramos en la figura 5.1). Sobre este primer prototipo se realizaron diversos ensayos para terminar de afinar la detección.

## 6.4. Servidor Web y conexión a internet

Paralelo al desarrollo del nodo trabajamos en contruir un sitio web propio capaz de recibir información y plasmarla en tablas y gráficos. En una primera instancia se ensayó el servidor web subiendo datos de forma manual, lo que nos permitía ver como organizaba y mostraba los datos.

Una vez funcionando bien el sitio web procedimos a realizar pruebas sobre el SIM800L. Recordemos que este módulo es el responsable de dar a la central conexión a internet mediante 2G. El SIM800L se comunica mediante comandos AT, por lo que lo usamos en conjunto con la Blue Pill para relizar los ensayos. En primer lugar solamente buscábamos que el SIM800L logre conectarse a la red gracias a una SIM que le insertamos. Puede parecer un paso simple, pero debido a que este módulo posee requerimientos particulares en cuanto a la alimentación fue importante realizar pruebas para desarrollar una fuente adecuada para el mismo. Cuando logramos que el SIM800L se conecte con la red ensayamos la capacidad que tenía de subir datos al servior mediante las órdenes recibidas desde la Blue Pill a través de los comandos AT.

## 6.5. Desarrollo de la comunicación serial del sistema

En este punto ya logramos tener un nodo capaz de recibir señales y de detectar inhibiciones y un servidor web funcional al cual podemos subir datos mediante el SIM800L y una Blue Pill. El siguiente paso, era desarrollar una comunicación robusta entre nodos y la central. Fue en este momento que decidimos usar el MAX485 para comunicar el sistema mediante RS485.



Al añadir el MAX485 al conjunto de SIM800L y Blue Pill, queda conformado el primer prototipo en protoboard de nuestra central.

Los primeros ensayos consistieron simplemente en comunicar dos Blue Pill aisladas, esto era necesario para conocer el estandar de comunicación en cuestión y familiarizarnos con el manejo de la UART del nuestro microcontrolador. El siguiente paso fue añadir el prototipo del nodo con el agregado de un max485 y nuestro prototipo de central. En este punto todavía no estábamos enviando datos de recepción a través de la comunicación, solamente envíabamos datos sin importancia para entender como conformar un red de rs485. Estos ensayos nos permitieron desarrollar una estrategia de comunicación confiable.

Fue en este momento cuando desarrollamos nuestra trama de comunicación y, luego de varios ensayos, definimos por completo como se iban a comunicar los nodos y la central. En este punto se realizaron numerosos ensayos del sistema funcionando en conjunto, desde la detección de la inhibición y la comunicación de los nodos a la central, hasta encender alarmas y subir los datos a la web. Cabe aclarar que todas las pruebas de comunicación realizadas hasta el momento se hicieron a cortas distancias con un par trenzado telefónico.

## 6.6. Ensayos Finales

Al quedar ya conformado el formato de nuestro sistema, diseñamos nuestras placas definitivas y las mandamos a fabricar. Con nuestros nodos y la central llevamos a cabo los últimos ensayos, esta vez utilizando un cable de mayor longitud y situándonos en un espacio de gran tamaño. Gracias a estas pruebas realizamos los últimos ajustes para lograr un sistema robusto y funcional.

Por último se puso a pruebas el sistema en un estacionamiento real, obteniendo excelentes resultados.

# Capítulo 7

## Desarrollo de servidor web

En este capítulo se describirán los objetivos, el diseño, las prestaciones y la forma en que se llevó a cabo el montaje del servidor web.

### 7.1. Objetivos

Los objetivos de tener un servidor web que disponga de una base de datos y una interfaz visual, como lo es la pagina web, son:

- Recabar la información brindada por cada lugar en donde se instale el sistema.
- Organizar todos los datos obtenidos en un solo lugar para que cada usuario tenga en forma remota y de fácil acceso las zonas donde se presentan este tipo de hechos.
- Mostrar en forma de tabla cada una de las inhibiciones detectadas.
- En base a esta tabla, generar diferentes gráficos que muestren de una forma mas amigable el texto plano.
- Tener un lugar de soporte/sugerencias.
- Procesamiento matemático para la triangulación y muestra gráfica de la última detección de un lugar de interés.



## 7.2. Página web

El dominio es <http://www.jammer-detector.ml> y la programación de la misma fue realizada en:

- HTML, siglas en inglés de HyperText Markup Language, hace referencia al lenguaje de marcado para la elaboración de páginas web. Es un estándar que sirve de referencia del software que conecta con la elaboración de páginas web en sus diferentes versiones, define una estructura básica y un código para la definición de contenido de una página web, como texto, imágenes, videos, scripts, entre otros. Es el estándar que se ha impuesto en la visualización de páginas web y es el que todos los navegadores actuales han adoptado.

El lenguaje HTML basa su filosofía de desarrollo en la diferenciación. Para añadir un elemento externo a la página (imagen, vídeo, script, entre otros.), este no se incrusta directamente en el código de la página, sino que se hace una referencia a la ubicación de dicho elemento mediante texto. De este modo, la página web contiene solamente texto mientras que recae en el navegador web (interpretador del código) la tarea de unir todos los elementos y visualizar la página final. Al ser un estándar, busca ser un lenguaje que permita que cualquier página web escrita en una determinada versión, pueda ser interpretada de la misma forma (estándar) por cualquier navegador web actualizado.

Es un lenguaje de marcado que nos permite indicar la estructura de nuestro documento mediante etiquetas. Este lenguaje nos ofrece una gran adaptabilidad, una estructuración lógica y es fácil de interpretar tanto por humanos como por máquinas.

- CSS (siglas en inglés de Cascading Style Sheets), en español "Hojas de estilo en cascada", es un lenguaje de diseño gráfico para definir y crear la presentación de un documento estructurado escrito en un lenguaje de marcado. Es muy usado para establecer el diseño visual de los documentos web, e interfaces de usuario escritas en HTML o XHTML. Junto con HTML y JavaScript, CSS es una tecnología usada por muchos sitios web para crear páginas visualmente atractivas, interfaces de usuario para aplicaciones web y GUIs para muchas aplicaciones móviles.



CSS está diseñado principalmente para marcar la separación del contenido del documento y la forma de presentación de este, características tales como las capas o layouts, los colores y las fuentes. Esta separación busca mejorar la accesibilidad del documento, proveer más flexibilidad y control en la especificación de características presentacionales, permitir que varios documentos HTML compartan un mismo estilo usando una sola hoja de estilos separada en un archivo .css, y reducir la complejidad y la repetición de código en la estructura del documento.

- PHP es un lenguaje de programación de uso general que se adapta especialmente al desarrollo de aplicaciones web dinámicas con acceso a información almacenada en una base de datos. El código fuente escrito en PHP es invisible al navegador web y al cliente, ya que es el servidor el que se encarga de ejecutar el código y enviar su resultado HTML al navegador.

Es libre, por lo que se presenta como una alternativa de fácil acceso para todos y además posee una amplia documentación en su sitio web oficial, entre la cual se destaca que todas las funciones del sistema están explicadas y ejemplificadas en un único archivo de ayuda.

- JavaScript (abreviado comúnmente JS) es un lenguaje de programación interpretado. Se define como orientado a objetos, basado en prototipos, imperativo, débilmente tipado y dinámico.

Se utiliza principalmente del lado del cliente, implementado como parte de un navegador web permitiendo mejoras en la interfaz de usuario y páginas web dinámicas.

JavaScript se diseñó con una sintaxis similar a C, aunque adopta nombres y convenciones del lenguaje de programación Java.

Puntualmente la aplicación que se le dio en este proyecto es realizar operaciones matemáticas para la triangulación y únicamente en el marco de la aplicación cliente, sin acceso a funciones del servidor generar gráficas a partir de base de datos, previamente obtenidas mediante el lenguaje PHP.



### 7.2.1. Pestañas

#### Inicio

Apenas ingresamos a la página podemos observar en la parte superior el logo y nombre del proyecto y sobre la misma barra en la parte derecha vemos el menú.

En esta pestaña de inicio se colocó la tabla donde muestra la información recabada de todos los lugares donde está instalado el sistema y se encontró una inhibición. La información que posee la misma es: ubicación, ID de cada nodo, fecha y hora y el nivel de RSSI y tipo de inhibición detectada por cada uno de los nodos. En la figura 7.1 podemos ver la misma.

UBICACIÓN	ID1	ID2	ID3	FECHA	RSSI-1 [dBm]	RSSI-2 [dBm]	RSSI-3 [dBm]	MODO DE INHIBICIÓN-1	MODO DE INHIBICIÓN-2	MODO DE INHIBICIÓN-3
Disco	A	B	C	2020-11-04 09:09:32	-45	-87	-90	1	1	0
Disco	A	B	C	2020-11-10 17:25:42	-59	-40	-23	2	1	2
SuperMami	A	B	C	2020-11-20 13:25:42	-45	-54	-32	2	0	1
SuperMami	A	B	C	2020-11-20 13:27:05	-45	-54	-32	2	0	1
Disco	A	B	C	2020-11-20 15:25:42	-27	-30	-29	2	2	0

Figura 7.1: Página de inicio

#### Nosotros

Esta pestaña está realizada para mostrar la tarjeta de cada uno de los integrantes del grupo de trabajo, dando así también un medio de contacto.

En la figura 7.1 podemos ver la pestaña.



The screenshot displays the 'Equipo de trabajo' (Team) section of the website. It features three team members in a grid:

- Julián Giletta**: Estudiante Ing. Electrónica, UTN FRC. Córdoba, Argentina. juligiletta97@gmail.com
- Martín Coronel**: Estudiante Ing. Electrónica, UTN FRC. Córdoba, Argentina. martin97Coronel@gmail.com
- Stefano Fantin**: Estudiante Ing. Electrónica, UTN FRC. Córdoba, Argentina. fantinstefano96@gmail.com

At the bottom left is the text "UTN - FRC" and "Córdoba, Argentina - 2020". At the bottom right is the text "Powered by 000webhost".

Figura 7.2: Presentación de grupo de trabajo

## Estadísticas

La sección de estadísticas, quizás la mas importante para los usuarios del sistema, es en donde, de una forma gráfica y amigable, se visualizan todos los datos representados por los gráficos que mas describan la situación.

En la figura 7.3, a la izquierda podemos ver un gráfico de torta con las formas de inhibiciones detectadas y a la derecha vemos un gráfico de barras que indica la cantidad de inhibiciones por cada lugar.

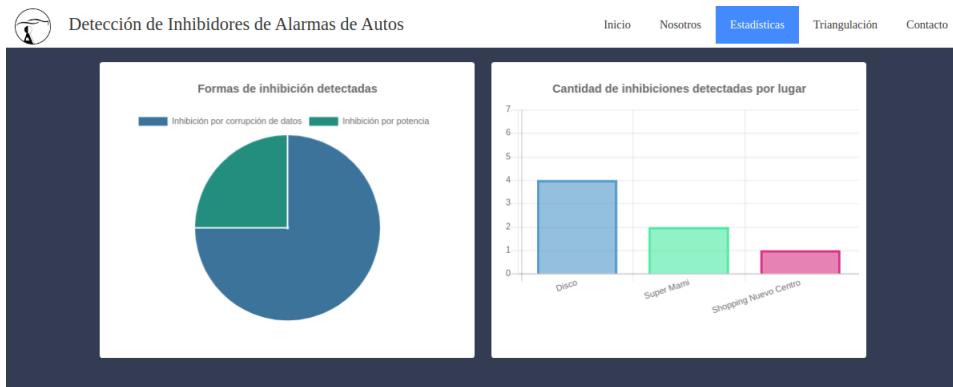


Figura 7.3: Gráficos de estadísticas



## Triangulación

Esta sección está dedicada al procesamiento matemático y muestra de la triangulación de inhibiciones detectadas por corrupción de datos con baja potencia. En la figura 7.4 un circulo de un radio de 7 metros el cual nos indica la posición de la inhibición detectada.

El proceso matemático para el calculo de este punto se basa en la relación de potencia recibida y transmitida de una onda en el espacio libre, considerado así para la simplificación de cálculos, ecuación 7.1.

$$\frac{P_R}{P_T} = \left[ \frac{4 * \pi * d_1}{\lambda} \right]^2 \quad (7.1)$$

Operando con la ecuación 7.1 para una misma señal recibida por dos nodos a la vez y haciendo la relación entre ellas obtenemos:

$$\left( \frac{d_1}{d_2} \right)^2 = 10^{\frac{P_{dBm2} - P_{dBm1}}{10}} \quad (7.2)$$

$$\frac{d_1}{d_2} = 10^{\frac{P_{dBm2} - P_{dBm1}}{20}} \quad (7.3)$$

Esta relación de distancias nos establece un punto en la recta que une cada nodo entre si (estos se encuentran en los vértices del triangulo azul como se ve en la figura 7.4), del cual trazando una linea perpendicular a ella, tenemos la linea de acción del inhibidor.

Haciendo esta relación entre todos los nodos tenemos 3 lineas que conforman un triángulo por la intersección entre ellas, donde luego obtiene la intersección de dos de las mediatrices de estas rectas que nos determinan el centro de la circunferencia que une los 3 puntos encontrados. El punto central, con un radio de 8 metros es el área donde se encuentra la inhibición detectada.

## Contacto

Finalmente la última pestaña es la de contacto, la cual tiene el fin de que cualquier persona que entre a la página y tenga alguna duda o sugerencia pueda tener un contacto rápido con cada uno de nosotros (figura 7.5).



Figura 7.4: Pestaña de triangulación

The figure shows a contact form with fields for "Nombre y apellido:" (Name and last name), "Email:" (Email), and "Consulta:" (Query). There is also a "ENVIAR" (Send) button. The page includes a header with the logo and navigation links, and a footer with copyright information.

Figura 7.5: Formulario de contacto

### 7.3. Base de datos

La base de datos esta realizada y gestionada en phpMySQL y cuenta con una tabla con el mismo contenido que la que podemos ver en la figura 7.1.

Es el lugar en el cual se almacena cada inhibición detectada y luego, mediante un enlace con la página web, todo su contenido es visualizado en esta la misma.



### 7.3.1. Carga de datos

El enlace desde el servidor web con la central instalada en cada lugar se realiza mediante el acceso a una pestaña oculta de la web, en la cual se interactúa con la central mediante un algoritmo de http-POST-request para cargar cada uno de los datos de los nodos correspondientes a cada lugar, para luego procesarlos y obtener los gráficos ya mencionados, la triangulación en caso de ser posible y otras utilidades que se le puedan dar.

# **Capítulo 8**

## **Conclusiones y trabajo futuro**

De acuerdo al trabajo previamente expuesto, en este capítulo haremos mención de las conclusiones que pudimos extraer al finalizarlo y se evaluarán posibilidades de desarrollos futuros.

### **8.1. Conclusiones**

En primera instancia nos parece importante dar nuestra perspectiva respecto a la viabilidad del proyecto. El mismo fue enfocado con carácter de costos minimizados buscando que el uso de los recursos monetarios disponibles sea el más eficiente posible. De esta manera nos encontramos con un producto finalizado que luce muy adecuado para la fabricación en cantidad aunque se reconoce que la utilización de módulos prefabricados -como previamente se analiza- es muy beneficiosa para la producción de los prototipos y primeros sistemas, pero en la posibilidad de producir en serie debería hacerse una adaptación de esto a un sistema que integre todo los bloques en fabricación propia. En las primeras instancias de fabricación se observa que muchos de los componentes utilizados precisan ser importados y, debido a la situación actual del país y a la alta carga impositiva que esto implica, resulta no ser conveniente la compra de un pequeño número de dispositivos en el exterior, quedando así avalado el uso de algunos bloques componentes.

Desde el punto de vista económico el sistema planteado cuenta con un punto débil el cual está definido en los requerimientos del mismo. Se busca que el sistema de seguridad no pueda ser inhibido por un agente externo por lo que los nodos y la central se comunican entre sí de manera cableada.



Resulta ser que el cableado debe ser de calidad que asegure la comunicación RS485 y en el mismo la alimentación para los nodos. Es por esto que en la aplicación del sistema planteado la mayor cantidad de gastos reside en las tiradas de cable necesarias paraemplazar el sistema en el lugar de operación. Esto podría solucionarse con una metodología de comunicación inalámbrica pero daría lugar a altas vulnerabilidades.

La seguridad en la detección de inhibiciones en sistemas de seguridad de alarma de auto fue el eje central del desarrollo, por lo que siempre se buscó eliminar las vulnerabilidades que pudieran ocurrir. Es por esto que al momento de presentar el sistema podemos decir que posee un sistema de detección robusto. Las pruebas de campo han sido muy variadas y han buscado eliminar cualquier falla en el funcionamiento, ahora restaría el realizar un análisis en largo plazo de operación con una realimentación del cliente que fuera a utilizarlo.

Como cierre, podemos decir que se ha conseguido un sistema que es capaz de detectar en fracciones de segundos señales que alteren el funcionamiento de seguridad inalámbricos en la frecuencia de 433,92 MHz. El área de operación segura para que las señales de baja potencia puedan ser trianguladas se estima que es de 50m a la redonda desde el punto central de una disposición en forma triangular de los tres nodos, de igual modo esto podría ser ampliado con la penalización de que no todos los nodos en simultáneo alcancen a medir un valor de intensidad de señal en una inhibición por corrupción de datos.

## 8.2. Trabajo futuro

Después de terminar el trabajo enmarcado en el proyecto final de grado de ingeniería electrónica hemos podido divisar algunos puntos sobre los cuales nos parece importante realizar mejoras en un futuro:

- Frecuencia de operación: nuestro sistema fue diseñado para una única frecuencia de operación; como previamente fue expuesto existen dos principales en las que funcionan los receptores vehiculares, por lo que a futuro creemos importante que el sistema tenga la capacidad de detectar en ambas las inhibiciones presentes.
- Las inhibiciones y las estrategias de inhibición son diferentes para cada sistema de comunicación, por lo que creemos interesante evaluar la posibilidad de detectar inhibiciones en diversos sistemas, aplicando e



invetigando sobre métodos para determinar las inhibiciones particularmente para cada comunicación.

- El sistema de detección fue elaborado con tres nodos distribuidos espacialmente para tener la capacidad de predecir la procedencia de la señal. En nuestros planes cabe la posibilidad de desarrollar un sistema único portable que detecte inhibiciones a su alrededor, dando lugar a la venta de un producto para particulares. Este debería disponer de alarmas locales y un sistema de memoria de datos recolectados que puedan ser descargados por el usuario.
- Como antes fue mencionado es importante que en un futuro el diseño del sistema sea completamente integrado a una placa única, esto nos daría la posibilidad de reducir los tamaños y tener un sistema más redituable para ventas en cantidad.

# Bibliografía

- [1] Texas Instruments, *CC1101. Low power Sub-1 GHz RF Transceiver - Datasheet.*
- [2] SIMCom, *SIM800L - Datasheet.*
- [3] Maxim Integrated, *MAX1473 - Datasheet.*
- [4] C. Smith, “The car hacker’s handbook: a guide for the penetration tester,” 2016.
- [5] Wenyuan Xu, Wade Trappe, Yanyong Zhang and Timothy Wood, “The feasibility of launching and detecting jamming attacks in wireless networks.” Rutgers University.
- [6] Konstantinos Pelechrinis, Marios Iliofotou and Srikanth V. Krishnamurthy, “Denial of service attacks in wireless networks: The case of jammers,” *IEEE communications surveys and tutorials*, 2011.
- [7] Wenyuan Xu, Ke Ma, Wade Trappe and Yanyong Zhang, “Jamming sensor networks: Attack and defense strategies.” Rutgers University.
- [8] Robert G. Meyer and Alvin K. Wong, “Blocking and desensitization in rf amplifiers,” *IEEE JOURNAL OF SOLID-STATE CIRCUITS, VOL. 30*, 1995.
- [9] Stefan van de Beek, Robert Vogt-Ardatjew and Frank Leferink, “Intentional electromagnetic interference through saturation of the rf front end,” *APEMC*, 2015.
- [10] Matthias Wilhelm, Ivan Martinovic, Jens B. Schmitt and Vincent Lenders, “Reactive jamming in wireless networks — how realistic is the threat?.” Disco Labs.