

---

# ESTUDIO, DISEÑO Y SIMULACIÓN DE UN SISTEMA DE RFID BASADO EN EPC

José María Ciudad Herrera  
Eduard Samà Casanovas

# ÍNDICE

1. INTRODUCCIÓN	4
2. CARACTERIZACIÓN DE UN SISTEMA RFID	7
2.1 ¿Qué es un sistema RFID?	8
2.2 Evolución de los sistemas RFID	11
2.3 Elementos de un sistema RFID	14
2.4 Principios básicos de funcionamiento de un sistema RFID.	19
2.4.1 Acoplamiento inductivo	20
2.4.2 Acoplamiento backscatter	24
2.4.3 Close coupling	26
2.5 Rangos de frecuencia	28
2.6 Diferentes sistemas de identificación	30
2.7 Criterios diferenciales de los sistemas RFID	34
2.8 Clasificación de los sistemas RFID	37
2.9 Aplicaciones de los sistemas RFID	43
2.10 Principales sistemas de RFID según su frecuencia	47
2.10.1 Sistemas a 13,56 MHz	47
2.10.2 Sistemas en la banda UHF: 400 a 1000 MHz	51
2.10.3 Sistemas a 2,45 GHz	55
2.11 Principios físicos de los sistemas RFID	58
2.11.1 Campo Magnético	58
2.11.2 Ondas Electromagnéticas	69
2.12 Códigos y Modulaciones	76
2.12.1 Codificación en banda base	76
2.12.2 Modulaciones digitales	79
2.12.3 ASK	79
2.12.4 2-FSK	79
2.12.5 2-PSK	80
2.12.6 Modulaciones que usan subportadora	80
2.13 Seguridad: encriptación de datos	82
2.13.1 Criptografía de clave secreta o simétrica	82
2.13.2 Algoritmo DES	84
2.13.3 IDEA	88
2.13.4 Criptografía de clave pública o asimétrica	89
2.14 Control de errores	93
2.14.1 Control de paridad	93
2.14.2 Método LRC	94
2.14.3 Método CRC	94
2.15 Multiacceso: anticolisión	97
2.15.1 SDMA	99
2.15.2 FDMA	100
2.15.3 TDMA	101
2.15.4 Ejemplos de métodos anticolisión	103
2.16 Regulación y estandarización	116

2.16.1	Regulación	116
2.16.2	EPC	118
2.16.3	EN 302 208	123
2.17	Privacidad	124
<b>3.</b>	<b>MEMORIA</b>	<b>126</b>
3.1	Introducción	127
3.2	Parámetros de diseño del sistema	128
3.3	Las etiquetas: EPC Clase 1	131
3.3.1	Estructura y contenido de los datos de una EPC Clase 1	131
3.3.2	Comunicación lógica entre el lector y la etiqueta EPC	132
3.4	CHIPCON CC1000	141
3.5	CC1000 PLUG & PLAY MODULE	150
3.6	El puerto paralelo	154
3.7	Diseño a alto nivel del software	159
3.8	Simulación del entorno wireless	163
3.8.1	Simulación de la señal FSK	164
3.8.2	Simulación de la onda continua (CW)	178
<b>4.</b>	<b>GLOSARIO</b>	<b>182</b>
<b>5.</b>	<b>BIBLIOGRAFÍA</b>	<b>185</b>
	<b>ANEXO I</b>	<b>188</b>
	<b>ANEXO II</b>	<b>210</b>

# **1. INTRODUCCIÓN**

El objeto de realización de este proyecto es el conocimiento de la tecnología RFID (Radio Frequency IDentification), así como el diseño de un prototipo de sistema de identificación y la simulación del canal inalámbrico en el que se realiza la comunicación entre los elementos del sistema.

La tecnología RFID no está muy asentada en la sociedad actual, pero poco a poco ha ido ganando terreno entre los sistemas de identificación automáticos. Pensado en un origen como sustituto del código de barras, ahora mismo se aplica en numerosos campos y sectores de la industria. Además hay multitud de investigaciones orientadas al uso de esta tecnología en un futuro no muy lejano. Por estos motivos nos hemos interesado en los sistemas de RFID y hemos seleccionado esta tecnología para su estudio en profundidad en este proyecto.

La tecnología RFID no tiene ni una historia ni un descubridor claro, ha surgido por la aportación de numerosos investigadores y gracias a la aplicación de avances en otros campos tecnológicos. Los sistemas de RFID se han ido transformando, en pocas decenas de años, de simples apariciones en artículos de revistas científicas a toda una realidad.

En el proyecto hemos realizado una caracterización inicial de la tecnología, la idea es dar una primera aproximación de los elementos que suelen formar un sistema de RFID, la historia de la tecnología, y los principios básicos de operación en los que se basan estos sistemas.

Debido a la gran libertad que hay en el diseño de estos sistemas, son muchos los parámetros que podemos fijar, necesitamos unos criterios para diferenciar estos sistemas, parámetros como la frecuencia, el rango de alcance, la alimentación, etc. clasifican los sistemas RFID.

También se hace referencia, en modo de comparación, a los diferentes tipos de sistemas de identificación, haciendo hincapié en la “batalla” por el mercado entre los códigos de barras y los sistemas de RFID.

Como ya hemos comentado las aplicaciones para los sistemas RFID son cada vez más numerosas y se adentran en campos más distintos. Veremos ejemplos de como se han introducido en la vigilancia de automóviles, logística, etc.

Haremos un estudio de los principios físicos más importantes que afectan a los sistemas de RFID, centrándonos en los dos principales tipos de comunicación, los sistemas de acoplamiento inductivo y los sistemas de acoplamiento backscatter basado en la tecnología de los radares.

Para caracterizar un sistema RFID hace falta también tratar los temas de codificación y modulación de datos, el control de errores, y los problemas de colisión ocasionados por varias etiquetas cercanas.

Como todas las tecnologías, tienen unos organismos de regulación y estandarización que también veremos.

La tecnología RFID ha creado polémica en el sentido de que puede ocasionar una invasión de la intimidad. Es un tema complicado que en algún caso ha impedido el desarrollo de alguna aplicación novedosa de la tecnología.

Hemos realizado un diseño completo, listo para implementar, de un sistema de RFID que trabaja a una frecuencia UHF en el rango de 868 MHz y de alimentación pasiva, es decir las etiquetas no poseen alimentación. El sistema está pensado para que el usuario identifique una etiqueta concreta, o que lea todas las etiquetas en un su rango de alcance.

El diseño del lector de este sistema parte del chip CC1000 de CHIPCON y del kit del mismo fabricante CC1000PP, como emisor y receptor de RF. Usamos los valores de los componentes adecuados para esta frecuencia de operación, así como los demás parámetros de potencia, etc. según el sistema que diseñamos.

Las etiquetas usadas en el sistema serían etiquetas EPC pasivas clase 1. Estas etiquetas contendrían información referente a su código EPC, un password programable y el CRC correspondiente a su código EPC.

Realizamos un desarrollo de la programación a alto nivel de cómo sería el software que controlaría los procesos de transmisión y recepción de datos, así como la comunicación con el usuario mediante un PC.

Por último hemos simulado a partir de las especificaciones de las etiquetas EPC clase 1 las tramas a enviar e introduciéndolas en el simulador WinIQSim de Rhode&Schwarz. Hemos configurado la modulación usada (FSK u onda continua) viendo los efectos que pueden provocar la propagación multicamino o la existencia de una señal de ruido dentro del área de interrogación.

Como resumen comentar que con este proyecto hemos querido dar una visión global de tecnología RFID, un diseño completo de un sistema RFID listo para implementar, aunque difícil ya que muchos componentes son difíciles de conseguir en España, y la simulación de los problemas que pueden surgir en la comunicación de un sistema inalámbrico como el diseñado.

## **2. CARACTERIZACIÓN DE UN SISTEMA RFID**

## 2.1. ¿Qué es un sistema RFID?

Un sistema de RFID (Radio Frequency IDentification) es la tecnología inalámbrica que nos permite, básicamente, la comunicación entre un lector y una etiqueta. Estos sistemas permiten almacenar información en sus etiquetas mediante comunicaciones de radiofrecuencia. Esta información puede ir desde un Bit hasta KBytes, dependiendo principalmente del sistema de almacenamiento que posea el transponder.

Los sistemas de RFID no son del todo nuevos, aparecen en los años 80 en sistemas de identificación, pero sí es cierto que actualmente están recibiendo una especial atención en muchos campos de la industria, lo que permite grandes avances en esta tecnología. Por ese motivo aparecen continuos estándares, aplicaciones e innovaciones.

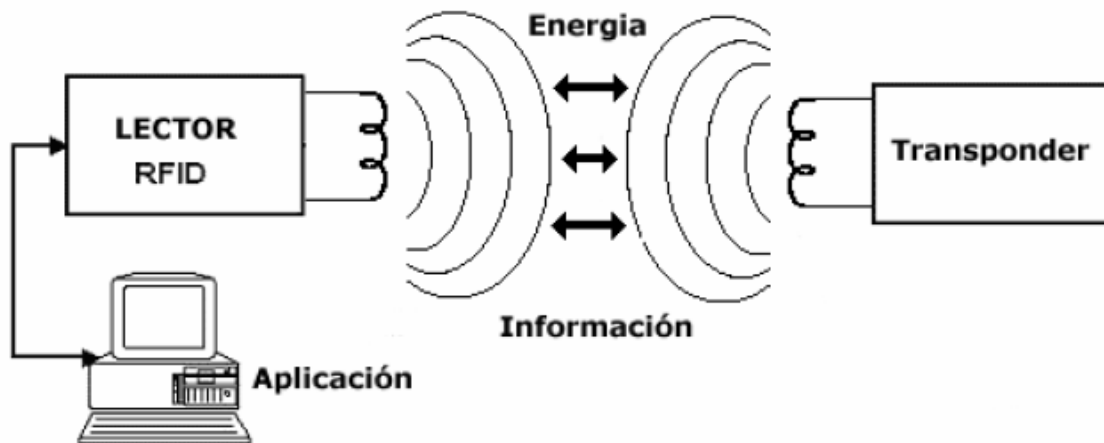


Figura 2.1 Esquema de un sistema RFID

Un tag, transponder o etiqueta electrónica contiene un microchip y una antena, que puede adherirse a cualquier producto. Incluso se están desarrollando tags que son de un tamaño tan pequeño que pasarían inadvertidas en algunos objetos. El microchip almacena un número de identificación -una especie de matrícula única de dicho producto-. Hay varios tipos de esquemas propuestos para estos números, como por ejemplo el Electronic Product Code (EPC), diseñado por Auto-ID Center. Podemos decir, que cada objeto tendrá un código único que lo diferenciará e identificará no sólo de otros tipos de productos, sino de productos iguales.

El funcionamiento del sistema, es a priori, bastante sencillo, como podemos observar en la Figura 2.1, el lector envía una serie de ondas de radiofrecuencia al tag, que son captadas por la microantena de éste. Dichas ondas activan el microchip, el cual, a través de la microantena y mediante ondas de radiofrecuencia, transmite al lector la información que tengan en su memoria. Finalmente, el lector recibe la información que tiene el tag y lo envía a una base de datos en la que previamente se han registrado las características del producto o puede procesarlo según convenga a cada aplicación.

La comunicación entre el lector y la etiqueta se realiza mediante señales de radiofrecuencia a una determinada frecuencia que generan las antenas de lector y



etiqueta, estas frecuencias pueden ser iguales o pueden ser armónicos. La comunicación entre ellas tiene unas determinadas características de alcance, velocidad y seguridad según el rango de frecuencia, el tipo de antenas utilizadas, el tipo de etiquetas y demás parámetros que se pueden configurar para una aplicación u otra.

En equipos RFID nos podemos encontrar con sistemas anticolidión que permiten leer varias tarjetas al mismo tiempo. En caso de que varias tarjetas estén en el rango de alcance del interrogador y dos o más quieran transmitir al mismo tiempo, se produce una colisión. El interrogador detecta la colisión y manda parar la transmisión de las tarjetas durante un tiempo. Después irán respondiendo cada una por separado por medio de un algoritmo bastante complejo. Obviamente a mayor capacidad de la etiqueta y el lector, más efectivos serán estos algoritmos.

El funcionamiento de los dispositivos de RFID se realiza entre los 50 KHz y 2.5 GHz. Las unidades que funcionan a bajas frecuencias (50 KHz-14 MHz) son de bajo coste, corto alcance, y resistentes al "ruido" entre otras características. No se requiere de licencia para operar en este rango de frecuencia. Las unidades que operan a frecuencias más altas (14 MHz-2.5 GHz), son sistemas de mayor coste y tecnología más compleja. La carga electromagnética de una antena lectora de RFID es menos de una quinta parte de la que produce un teléfono móvil, lo que significa que cinco antenas activas situadas cerca de una persona generan menos carga que un teléfono móvil; en la práctica, es muy improbable que una persona se sitúe cerca de una o más antenas activas a la vez, por lo que las emisiones electromagnéticas no son perjudiciales para la salud.

La etiqueta contiene información que puede ser sólo leída o puede permitir la escritura, dependiendo del tipo de memoria que posea el transponder. La mayor parte de los sistemas tienen memoria EEPROM (Electrically Erasable Programmable Read-Only Memory). En algunos casos llevan datos grabados de fábrica y en otros se puede grabar por parte del usuario. El usuario habitualmente recibe esta información en un lector portátil con un display alfanumérico o puede pasar directamente a un ordenador que procese los datos obtenidos.

Para la creación de un sistema RFID hay que tener en cuenta diversos factores de diseño como el rango de alcance donde se puede mantener la comunicación, la cantidad de información que puede almacenar el transponder, la velocidad de flujo de datos que podemos obtener entre lector y etiqueta, el tamaño físico de la etiqueta, la habilidad del lector para mantener la comunicación con varias etiquetas a la vez o la robustez que ofrece la comunicación a posibles interferencias de materiales entre lector y etiqueta. Se debe tener en cuenta también el nivel de emisión para no sobrepasar las regulaciones impuestas en cada país, si existe una batería suplementaria para realizar la comunicación entre etiqueta y lector o la frecuencia portadora RF usada en la comunicación entre lector y transponder.

Los sistemas RFID tienen la ventaja de su total funcionamiento sin visibilidad directa entre lector y etiqueta. En este aspecto es donde claramente supera al código de barras y a otros sistemas ópticos. Pero debido a su coste, que aunque ha ido reduciéndose progresivamente siempre será superior al del código de barras, no se ha implementado en aplicaciones sencillas donde el código de barras sigue dominando el mercado. Pero es en las aplicaciones donde el código de barras y la tecnología óptica es

más limitada y no resultan efectivos, donde el crecimiento de la tecnología RFID es más notorio.

Los sistemas de RFID tienen multitud de aplicaciones. Pueden utilizarse como tarjetas identificadas sin contacto, un uso de este tipo se puede ver por ejemplo en el sistema de pago utilizado en peajes llamado viaT, que permite que el vehículo no tenga que detenerse o en los accesos a edificios oficiales o a empresas privadas. Otra aplicación muy usada son los inmovilizadores de vehículos, que consisten en un sistema interrogador situado en el vehículo a proteger y en un identificador en la llave. Se pueden usar para identificar envío de cartas o paquetes en agencias de transporte, identificadores de animales, identificadores de equipajes aéreos, gestión de supermercados, inventario automático, distribución automática, localización de documentos, gestión de bibliotecas, etc. Incluso se está hablando de usar la tecnología RFID para la identificación de personas con libertad vigilada, gente con deficiencias mentales o que se puedan considerar peligrosas para la sociedad. También se están realizando proyectos para incluir chips con el historial médico en personas y en billetes de curso legal para evitar posibles robos y localizar en todo momento el dinero.

Está claro que estas aplicaciones pueden aportar muchas ventajas. Por ejemplo, poder conocer el historial médico de una persona inconsciente al instante con un lector que lleve el equipo médico, puede reducir el tiempo de acción y salvarle la vida. No obstante no son pocas las personas e instituciones que se oponen a estas implementaciones en pro a una violación de la intimidad. El uso de un identificador RFID en los billetes de curso legal, provoca que alguien con un lector capaz de detectar estos transponders puede saber al instante el dinero que lleva encima una persona o en una casa.

Se intenta aplicar los sistemas en todos los procesos industriales, teniendo eso sí, un mayor peso en procesos logísticos, creándose así el concepto de trazabilidad. De esta forma podemos conocer como usuario, en el punto final de venta o en cualquier otro intermedio, toda la historia anterior del producto, así como todos los procesos de manufacturación por los que ha pasado. Marcas como Codorniu han experimentado de manera satisfactoria desde el año 2004 el uso de esta tecnología en toda su cadena de fabricación y distribución. Esto resulta, sin duda, un avance para este sector, que ninguna otra tecnología había aportado hasta este momento.

## 2.2 *Evolución de los sistemas RFID*

Los sistemas de RFID han revolucionado la identificación a distancia a principios del siglo XXI. Pero el estudio de estos sistemas se remonta a mediados del siglo XX.

Muy lejos están las primeras suposiciones de la existencia de un campo magnético en el estudio de imanes naturales, por parte de la cultura china en el primer siglo a.C. Fue a principio del siglo XIX cuando se comenzó a entender verdaderamente el concepto de electromagnetismo. Personajes como Maxwell, Hertz, Marconi, etc. contribuyeron con sus inventos y descubrimientos a ello. Posteriormente a principios del siglo XX la generación y la transmisión de ondas de radio y la aparición del radar, basado en ondas de radio que rebotan sobre un objeto localizándolo, son el fundamento sobre el que se constituyen el concepto de sistemas de identificación por radio-frecuencia ó RFID.

La tecnología RFID ha tenido un pasado confuso. No hay un descubridor destacado, se ha ido desarrollando con la suma de numerosas aportaciones y colaboraciones. Al comienzo uno de los investigadores más destacados, que no el primero, Harry Stockman, dictaminó que las dificultades para la comunicación usando ondas de radio reflejadas en objetos estaban superadas, con todas las aplicaciones que esto podía permitir. No pudo ser hasta treinta años después cuando el trabajo de Stockman fue de nuevo estudiado. Faltaban aún por desarrollar transistores, microprocesadores y eran necesarios adelantos en redes de comunicación, incluso un cambio en la visión de hacer negocio, para que los sistemas RFID fueran factibles.

Fue en la década de los 50 cuando la tecnología de RFID siguió un proceso de desarrollo similar al que experimentaron la radio y el radar en las décadas anteriores. Diferentes sectores de la tecnología RFID se vieron impulsados, entre ellos los sistemas con transponders de largo alcance, especialmente los conocidos como “identification, friend or foe” (IFF) usado en la industria aeronáutica. Trabajos como los creados por F.L Vernon “Application of microwave homodyne” y por D.B. Harris “Radio transmisión systems with modulatable passive responder” fueron determinantes para que la tecnología RFID dejase de ser una idea y se convirtiese en una solución.

La década de los 60 se pueden considerar como el preludeo de la explosión que se producirá en la siguiente década. Se realizaron numerosos artículos, y la actividad comercial en este campo comenzó a existir. El primer sistema que fue usado era el EAS (Electronic Article Surveillance) para detectar robos en grandes almacenes. El sistema era sencillo con un único bit de información, para detectar la etiqueta o no, dentro del radio de acción del lector y hacer sonar una alarma acústica en caso de que una etiqueta no desactivada pasase por el alcance del lector. Típicamente son dos lectores ubicados de tal forma que el cliente tenía que pasar entre ellos para salir el establecimiento. A pesar de sus limitaciones, era económico y efectivo. Su uso se comenzó a extender de manera rápida.

En los 70 se produjeron notables avances como los aportados por instituciones como Los Alamos Scientific Laboratory, Northwestern University y el Microwave Institute Foundation sueco. Al principio de esta década se probaron varias aplicaciones para logística y transporte, como las usadas por el puerto de New York y New Jersey,

aplicaciones para el rastreo de automóviles. Pero las aplicaciones en el sector logístico todavía no estaban listas para una inserción completa en el mercado. En esta década hubo un gran desarrollo técnico de los sistemas, sobretodo enfocado a aplicaciones de seguimiento de ganado, vehículos y automatización industrial. Basados en microondas en los EEUU y sistemas inductivos en Europa. La creación de nuevas empresas dedicadas a la tecnología RFID aumentaba continuamente, era un signo positivo del potencial que tenían los sistemas RFID.

Llegó la década de los 80, y con ella la implementación de tantos estudios y desarrollos logrados en años anteriores. En EEUU se interesaron por aplicaciones en el transporte, accesos y en menor grado en los animales. En países europeos como Francia, España, Portugal e Italia se centraron más en aplicaciones industriales y sistemas de corto alcance para controlar animales.

En los primeros años de los 90 se inició el uso en EEUU del peaje con control electrónico, autopistas de Houston y Oklahoma incorporaban un sistema que gestionaba el paso de los vehículos por los pasos de control. En Europa también se investigó este campo y se usaron sistemas de microondas e inductivos para controles de accesos y billetes electrónicos. Un nuevo avance en el mundo del automóvil vino con la tecnología RFID de la mano de Texas Instruments (TI), un sistema de control de encendido del automóvil. Apareció también un sistema de Philips que permitía la gestión del encendido, control del combustible, y control de acceso al vehículo entre otras acciones. Aplicaciones para autopistas y billetes electrónicos se fueron extendiendo por Asia, África, Suramérica y Australia. A partir de aquí el éxito de la tecnología RFID en estos campos hizo que se aplicaran a otros segmentos económicos. Fue en Dallas por primera vez cuando con un solo tag era utilizado para el acceso a una autopista, al campus universitario, a diferentes garajes de la ciudad, incluido el del aeropuerto. El avance de la tecnología durante esta década fue rápido debido a los desarrollos tecnológicos en otros campos que permitían fabricar cada vez equipos más pequeños, con más memoria, con más alcance y abaratando su coste de fabricación apareciendo así nuevos usos hasta esa fecha descartados.

El futuro de RFID parece ser esperanzador, en un mundo basado en el poder de la información y donde cada vez se desecha más el cable, el radio de acción de esta tecnología parece ser bastante grande. El interés por el comercio virtual parece que tiene su principal valedor en estos sistemas en los que basar una correcta gestión de todo el proceso. Por ese motivo la FCC (Federal Communications Commission) escogió el espectro entorno de los 5,9 GHz para nuevos sistemas inteligentes de transporte y para las nuevas aplicaciones que necesiten. Pero para estas nuevas aplicaciones se necesita un gran desarrollo de la tecnología. El futuro de RFID parece alentador, pero como todas las tecnologías necesita de los otros campos tecnológicos para avanzar.

Podemos resumir el avance que ha experimentado la tecnología RFID por décadas en la Tabla 2.1:

Década	Avances Tecnológicos
1940-1950	Se rediseña el radar para uso militar tomando gran relevancia en la IIª Guerra Mundial. RFID aparece en 1948.
1950-1960	Primeras experimentos con RFID en laboratorios.
1960-1970	Desarrollo de la tecnología RFID, primeros ensayos en algunos campos de la tecnología.
1970-1980	Explosión de la tecnología. Se realizan más tests. Primeras aplicaciones.
1980-1990	Aparecen más aplicaciones para la tecnología.
1990-2000	RFID toma relevancia en el mundo cotidiano. Aparecen los estándares.

Tabla 2.1 Resumen de la evolución de la tecnología RFID.

## 2.3 Elementos de un sistema RFID

Un sistema RFID se compone básicamente de dos elementos: un lector (reader) y una etiqueta (transponder).

### 2.3.1 Transponder

La palabra transponder deriva de TRANSmitter/resPONDER, lo cual explica su funcionamiento. Los componentes básicos de un transponder los podemos distinguir en la figura 2.2 y son:

- Una memoria no volátil donde se almacenan datos.
- Una memoria ROM donde se almacenan instrucciones básicas para el funcionamiento, como son temporizadores, controladores de flujo de datos, etc.
- También puede incorporar memoria RAM para almacenar datos durante la comunicación con el lector.
- La antena por la cual detecta el campo creado por el interrogador, y del que extrae energía para su comunicación con él.
- Restos de componentes electrónicos que procesan la señal de la antena y para el proceso de datos, como buffers, filtros, etc.

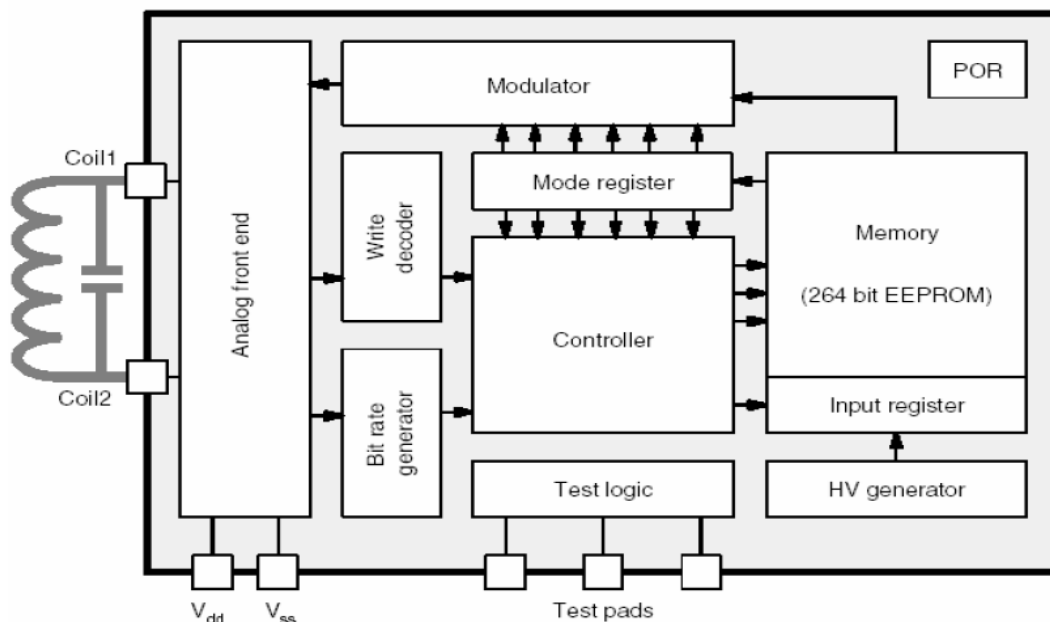


Figura 2.2 Esquema de un transponder de RFID

## Alimentación

Los transponders necesitan poca alimentación, del orden de los mW. Podemos diferenciar dos tipos de etiquetas dependiendo de la energía que utilizan para la comunicación:

- *Etiquetas activas*: son transponders que necesitan el apoyo de baterías adicionales, ya que no tienen suficiente energía con la que proporciona el lector. Este tipo de etiqueta tiene la ventaja de poseer un alcance mayor de comunicación e incluso no necesitan que el lector sea quién inicie la comunicación. Además permiten habitualmente procesos de lectura y reescritura enviando previamente instrucciones al lector y la utilización de memorias más grandes (existen etiquetas con 1Mb de memoria). Por el contrario ofrecen una vida útil limitada (menos de diez años), dependiendo del tipo de batería y de las temperaturas a las que opera. También hay que destacar que su coste es bastante elevado, su precio suele ser 5 veces más alto. De esta forma aparecen nuevas aplicaciones para sistema RFID gracias a este tipo de etiquetas alimentadas por baterías.
- *Etiquetas pasivas*: son transponders que no necesitan baterías adicionales, ya que únicamente se alimentan de la energía del campo generado por el lector. Para las etiquetas pasivas, la energía que necesitan para transmitir la información que contienen, proviene en su totalidad de la señal generada por el lector. Estas etiquetas aprovechan la energía subministrada por un lector para generar su propia señal que recibe nuevamente el lector.

	Memory (Bytes)	Write/read distance	Power consumption	Frequency	Application
ASIC#1	6	15 cm	10 $\mu$ A	120 kHz	Animal ID
ASIC#2	32	13 cm	600 $\mu$ A	120 kHz	Goods flow, access check
ASIC#3	256	2 cm	6 $\mu$ A	128 kHz	Public transport
ASIC#4	256	0.5 cm	<1 mA	4 MHz*	Goods flow, public transport
ASIC#5	256	<2 cm	~1 mA	4/13.56 MHz	Goods flow
ASIC#6	256	100 cm	500 $\mu$ A	125 kHz	Access check
ASIC#7	2048	0.3 cm	<10 mA	4.91 MHz*	Contactless chip cards
ASIC#8	1024	10 cm	~1 mA	13.56 MHz	Public transport
ASIC#9	8	100 cm	<1 mA	125 kHz	Goods flow
ASIC#10	128	100 cm	<1 mA	125 kHz	Access check

\*Close coupling system.

Tabla. 2.2 Gráfico del consumo de potencia varios sistemas RFID (Amtel 1996) la mínima es 1.8V y máx. 10V.

## Frecuencia y velocidad de transmisión

Las etiquetas también las podemos clasificar según el rango de frecuencias en el que opera, es decir, en que frecuencias se comunicará con el lector:

- LF (Low Frequency) en el rango de 120 KHz-134 KHz.

- HF (High Frequency) en el rango de 13.56 MHz.
- UHF (Ultra High Frequency) en el rango de 868-956 MHz.
- Microondas (Microwave) en el rango de 2,45 GHz, conocida como banda ISM (Industrial Scientific and Medical).

Una mayor frecuencia suele significar una mayor velocidad en la transmisión de datos, aunque también encarece el precio del sistema. Elegir el rango de frecuencia es uno de los parámetros de diseño más importante a la hora de crear un sistema RFID, y se deberá adecuar a la aplicación diseñada.

### Opciones de programación

Dependiendo del tipo de memoria de la que disponga el transponder. Puede permitir la sólo la lectura, programable una sola vez y de múltiples lecturas, o de lectura/escritura. Los tags que sólo permiten lecturas suelen venir programados en su fabricación, generalmente con número de identificación. Ambos tipos pueden ser programados por el usuario.

### Forma y dimensiones

Los transponders tienen diversas formas y tamaños, todo dependiendo de la aplicación a la cual están destinados. Actualmente se están fabricando de tamaño muy reducido, incluso la firma Hitachi, anunció que tenían la tecnología suficiente para incorporar a los billetes de curso legal un transponder que pasaría totalmente desapercibido. Claro está que para otras aplicaciones industriales donde no se busca que pase desapercibido se están usando etiquetas de un tamaño de 120x100x50 mm, como por ejemplo palets o contenedores. Los transponders que se utilizan para el control y localización de ganado tienen un tamaño inferior a 10 mm. Fabricantes diversos también afirmaron que se podría incluir en productos unos transponders que no podrían ser localizados fácilmente por el comprador, noticia que causó mucha polémica por la clara oposición realizada por las asociaciones de consumidores.

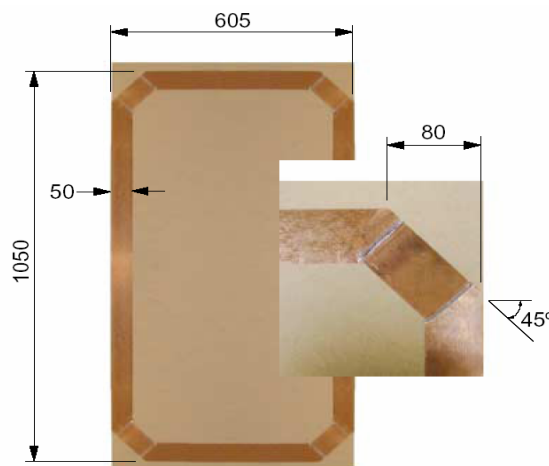


Figura 2.3 Detalle de un tag típico de aplicaciones logísticas, con las unidades expresadas en mm.



## Coste

El coste de los transponder ha ido disminuyendo conforme avanzaba la tecnología. Esta claro que cuanto mayor capacidad de memoria y más complicación tenga su circuitería, mayor será su coste. Hay que tener en cuenta también que el encapsulado del transponder puede encarecer el precio de éste, ya que pueden trabajar en zonas como minas, metalúrgicas, donde reciben unas condiciones extremas de humedad y de temperatura. Por tanto deben ser unos encapsulados muy resistentes, lo que suele conllevar un alto precio.

Los tags activos suelen ser más caros que los pasivos, así como los transponders que operan a una frecuencia más elevada son también más caros.

### 2.3.2 Lectores

El otro elemento principal de un sistema RFID es el lector o interrogador.

Los lectores (readers) son los encargados de enviar una señal de RF para detectar las posibles etiquetas en un determinado rango de acción. En su fabricación se suelen separar en dos tipos:

- Sistemas con bobina simple, la misma bobina sirve para transmitir la energía y los datos. Son más simples y más baratos, pero tienen menos alcance.
- Sistemas interrogadores con dos bobinas, una para transmitir energía y otra para transmitir datos. Son más caros, pero consiguen mayores prestaciones.

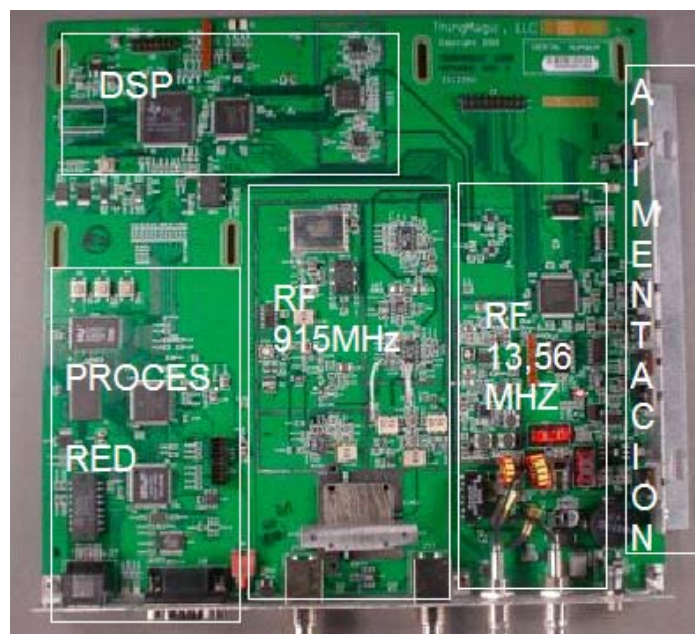


Figura 2.4 Diseño interno de un lector que puede trabajar con dos frecuencias.

Los lectores son más complejos dependiendo del transponder, si son sofisticados, los componentes del interrogador tienen que ser capaces de acondicionar la señal, detectar y corregir errores. Además pueden trabajar a más de una frecuencia.

Una vez que se ha recibido toda la información por parte del lector, se pueden emplear algoritmos para no confundir la transmisión actual con una nueva, indicándole al tag que deje de transmitir. Se suele usar para validar diversos tags en un espacio corto de tiempo. Otro algoritmo usado por el lector, es ir llamando a los transponders por su número de identificación, indicándole de esta forma el tiempo en el que deben transmitir. Son mecanismos para impedir la colisión de información.

En las figuras 2.5 y 2.6 podemos observar dos tipos de lectores de RFID:



Figura 2.5 Lector de mano de corto alcance que trabaja a la frecuencia de 900MHz



Figura 2.6 Lector del fabricante SAMSys UHF de largo alcance.

## 2.4 Principios básicos de funcionamiento de un sistema RFID

Un sistema de comunicación RFID se basa en la comunicación bidireccional entre un lector (interrogador) y una etiqueta (transponder), por medio de ondas de radiofrecuencia.

El sistema de transmisión de información varía según la frecuencia en la que trabaja. Así se puede clasificar un sistema de RFID en sistemas basados en el acoplamiento electromagnético o inductivo, y basados en la propagación de ondas electromagnéticas. Podemos apreciar esta diferenciación en la Figura 2.7.

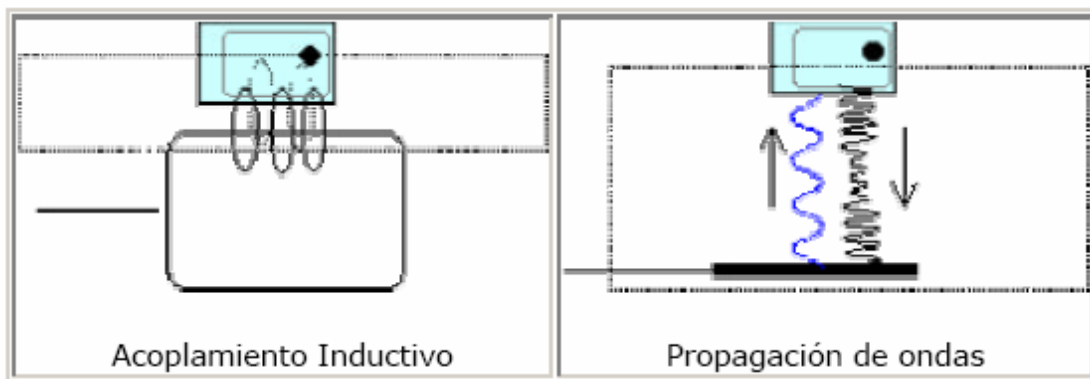


Figura 2.7 Métodos de propagación de la información en la tecnología RFID

Hay que tener en cuenta que la comunicación se puede realizar en zonas industriales con metales, lo que unido a las características de ruido, interferencia y distorsión de estas comunicaciones vía radio complica la correcta recepción de bits. Además de que esta comunicación es del tipo asíncrona, lo que repercute en una mayor atención en parámetros como la forma en que se comunican los datos, la organización de flujo de bits. Todo esto conlleva el estudio de la denominada codificación de canal, con el fin de mejorar la recepción de información.

Como en toda comunicación vía radio se necesita entre los dos componentes de la comunicación un campo sinusoidal variable u onda portadora. La comunicación se consigue aplicando una variación a ese campo, ya sea en amplitud, fase o frecuencia, en función de los datos a transmitir. Este proceso se conoce como modulación. En RFID suelen ser aplicadas las modulaciones ASK (Amplitude shift keying), FSK (Frequency shift keying) y PSK (Phase shift keying).

Los diferentes métodos de propagación de la información son usados en diferentes frecuencias. De este modo el acoplamiento inductivo funciona a frecuencias más bajas y el sistema de propagación de ondas a frecuencias más elevadas. Existe también otro tipo de propagación usado en distancias menores a 1cm, que puede trabajar teóricamente en frecuencias bajas hasta 30MHz, son los sistemas “close coupling”.

Estos sistemas usan a la vez campos eléctricos y magnéticos para la comunicación. La comunicación entre el lector y el transponder no ocasiona un gasto

excesivo de energía, por lo que en estos sistemas se pueden usar microchips que tengan un consumo de energía elevado. Son sistemas usados generalmente en aplicaciones con un rango de alcance mínimo pero con estrictas medidas de seguridad. Se usa en aplicaciones como cerraduras de puertas electrónicas o sistemas de contactless smart card. Estos sistemas tienen cada vez menos importancia en el mercado de la tecnología RFID.

Por otro lado existen los sistemas de “remote coupling” basados en el acoplamiento inductivo (magnético) entre el lector y el transponder. Por eso, estos sistemas también son conocidos como “inductive radio systems”. Los sistemas basados con acoplamiento capacitivo (eléctrico) no son casi usados por la industria; en cambio los inductivos se puede decir que abarcan el 80% de los sistemas de RFID. Este sistema de comunicación entre el lector y el transponder trabaja en el rango de frecuencia comprendido entre los 135 KHz y los 13,56 MHz. Aunque en algunas aplicaciones pueda trabajar a una frecuencia ligeramente más elevada. Su rango de alcance suele comprenderse alrededor de 1 m. Estos sistemas siempre usan transponders pasivos.

#### 2.4.1 Acoplamiento inductivo

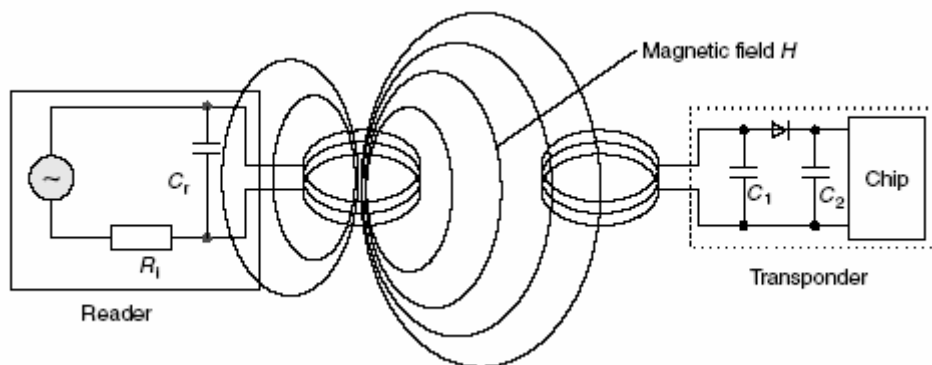


Figura 2.8 Esquema del acoplamiento inductivo entre lector y transponder.

El acoplamiento inductivo se basa en el mismo funcionamiento de los transformadores. En la Figura 2.8 podemos observar un esquema del acoplamiento inductivo. En estas frecuencias el campo creado por la antena del interrogador es la energía que aprovecha el transponder para su comunicación. Este campo está cerca de la antena del interrogador, lo que permite alcanzar unas distancias cercanas al diámetro de la antena. A distancias mayores la potencia necesaria es muy elevada. La bobina del lector genera un fuerte campo electromagnético, que penetra en la sección de la antena del transponder y en su zona cercana.

Las antenas de estos sistemas son bobinas, tanto del lector como del transponder, de gran tamaño, debido a la circunstancia de que la longitud de onda ( $\lambda$ ) (como inverso de la frecuencia) es elevada. Estamos hablando de 2400m para frecuencias menores de 135KHz, y de 22,4m a una frecuencia de 13,56 MHz. Como esta longitud de onda es sensiblemente mayor que la distancia entre el lector y el transponder, el campo electromagnético puede ser tratado como un simple campo magnético alternante con respecto a la distancia entre transponder e interrogador.

Una parte pequeña del campo emitido penetra en la bobina del transponder. Se genera una tensión en la antena (bobina) por inducción. Este voltaje es rectificado y sirve como alimentación para el microchip del transponder encargado de almacenar la información. Como podemos observar en la Figura 2.8, un condensador es conectado en paralelo con la antena del lector, el valor de este condensador es seleccionado según la inductancia de la antena que forma un circuito paralelo de resonancia con una frecuencia de resonancia que tiene que coincidir con la frecuencia de transmisión del lector. En la antena del lector se generan grandes corrientes debido a la resonancia del circuito paralelo, lo que permite crear campos intensos necesarios para la comunicación entre lector y transponder.

La antena (bobina) del transponder y el capacitador en paralelo forman el circuito resonante a la misma frecuencia que emite el lector. El voltaje generado en el transponder es máximo debido a la resonancia producida por el circuito del transponder.

La eficiencia de la energía transmitida entre las antenas del lector y del transponder es proporcional a la frecuencia de operación, la relación entre el número de espiras que tienen las bobinas (en los transformadores conocido por el factor  $n$ ), el área encapsulada por la antena del transponder, el ángulo que forman las bobinas una en relación a la otra y la distancia entre las dos bobinas. Cuando la frecuencia se incrementa, la inductancia requerida en el transponder y el número de espiras decrece. Como ejemplo, podemos decir que a una frecuencia de 135 KHz, el valor del factor  $n$  oscila entre 100 y 1000, y para una frecuencia de 13,56 MHz el valor del factor  $n=3-10$ .

Esto es debido a que el voltaje inducido en el transponder es todavía proporcional a la frecuencia de resonancia, en cambio el número de espiras de la bobina apenas afecta a la eficiencia de la energía transmitida a altas frecuencias.

### **Transferencia de datos entre transponder y lector**

En este apartado para trabajar con sistemas de acoplamiento inductivo se suelen usar tres tipos:

- Load modulation
- Load modulation con subportadora
- Subarmónicos

#### *Load modulation*

Se fundamenta en el funcionamiento de un transformador, siendo la bobina primaria la del lector y la secundaria la del transponder. Esto es cierto si la distancia entre las bobinas no es mayor de  $0,16\lambda$ , por lo que el transponder y el lector deben estar próximos. Si un transponder en resonancia se encuentra dentro del campo magnético de un lector, coge energía de ese campo magnético.

El resultado del “feedback” del transponder en la antena del lector puede ser representado como una impedancia ( $Z_T$ ). Conectando y desconectando la resistencia de carga presente en la antena del transponder se consigue variar el valor de  $Z_T$ , con lo que el voltaje que existe en la antena del lector también varía. Esto tiene un efecto en la modulación de amplitud del voltaje del lector por culpa del transponder remoto. El tiempo en el que se desconecta y se conecta la resistencia de carga es controlado por los datos, es lo que se usa para enviar los datos del transponder al lector.

### *Load modulation con subportadora*

Debido al acoplamiento débil que se realiza entre lector y transponder, las fluctuaciones que se producen en la tensión en la antena del lector (la información) es varios órdenes de magnitud inferior a la tensión de salida del propio lector. En la práctica para un sistema de 13,56 MHz, se entrega a la antena un voltaje de 100V en resonancia, la señal recibida del transponder es del orden de 10mV.

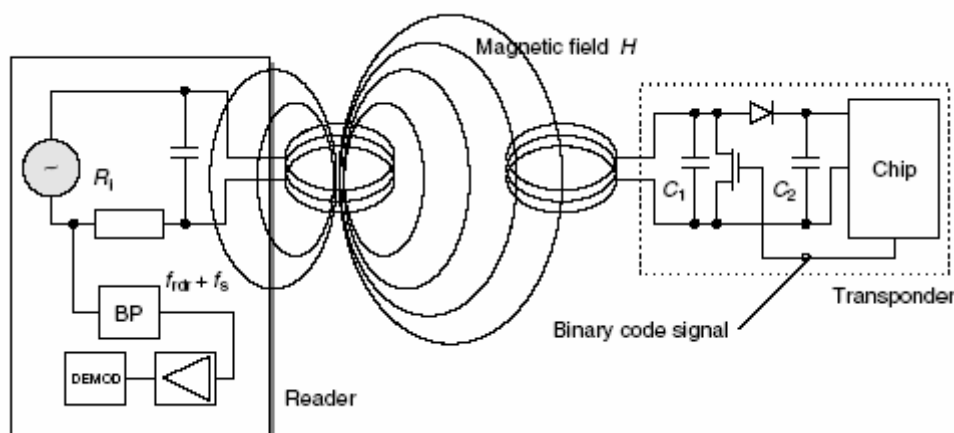


Figura 2.9 Generación de load modulation conectando y desconectando la resistencia del drain-source del FET del chip. El lector tiene un circuito capaz de detectar la subportadora.

Detectar esta fluctuación requiere una circuitería complicada, como solución se usan las bandas contiguas a la modulación creada. Para ello se incorpora una nueva resistencia de carga en el transponder que se conecta y desconecta a una frecuencia elevada  $f_s$ , entonces dos líneas espectrales son creadas a una distancia  $f_s$  de la frecuencia de resonancia entre lector y transponder. Uno de los métodos posibles es utilizar un transistor FET e el transponder, como vemos en la Figura 2.9.

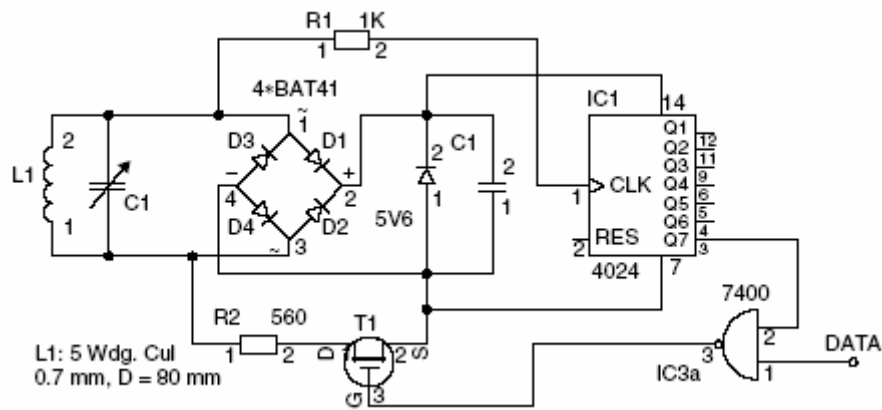


Figura 2.10 Ejemplo más detallado de un generador de modulación de carga con subportadora en sistema de acoplamiento inductivo.

En esas frecuencias conocidas como subportadoras, es más fácil detectar las variaciones de tensión. La información se puede modular en ASK, FSK o PSK con el flujo de datos. Esto significa una modulación de amplitud en la subportadora. Por último solo se requiere un filtro de paso banda para aislar una de las dos subportadoras. Debido a la amplia banda de guarda que requieren estos filtros, este procedimiento sólo es usado en la banda ISM en las frecuencias 6,78 MHz, 13,56 MHz y 27,125 MHz.

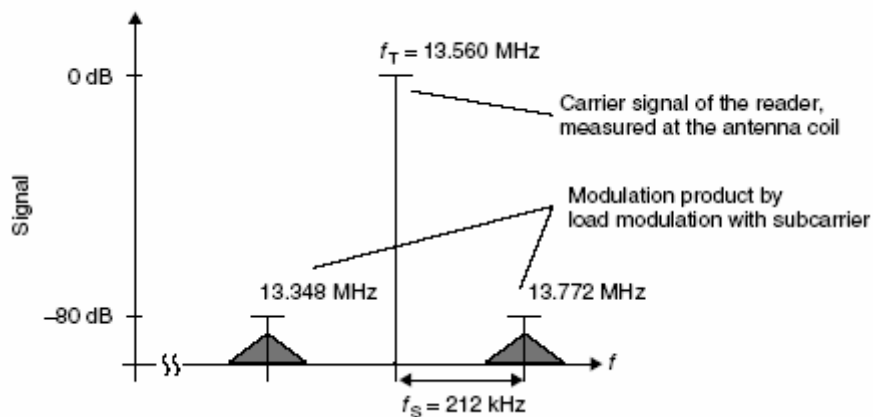


Figura 2.11 La load modulation crea dos subportadoras a una frecuencia  $f_S$  de la frecuencia de transmisión del lector. La información se encuentra en las bandas laterales de las dos subportadoras.

### Subarmónicos

Basado como su propio nombre indica en la utilización de subarmónicos de una frecuencia  $f_A$ , es decir,  $f_1=f_A/2$ ,  $f_2=f_A/3$ , etc. Se suele utilizar el primer subarmónico, es decir la mitad de la frecuencia en la que transmite el lector. La señal después del divisor es modulada por el flujo de datos y enviada para el transponder. Esta será la frecuencia a la que responda el transponder. El transponder necesitará un divisor binario de frecuencia para realizar dicha operación. La frecuencia de operación más popular para los sistemas subarmónicos es de 128 kHz. Por lo que la frecuencia de respuesta del transponder es de 64 kHz.

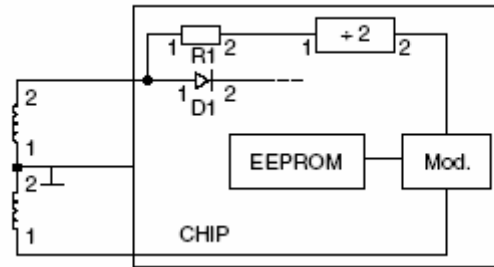


Figura 2.12 Diseño de un transponder que usa subarmónicos,

### 2.4.2 Acoplamiento backscatter

Otro sistema de transferencia de información son los sistemas “long-range”, que como su propio nombre indica son de largo alcance, mayores a 1 m. Estos sistemas se basan en el uso de ondas electromagnéticas en el rango de UHF o microondas. La mayoría de estos sistemas son conocidos como sistemas “backscatters” debido a su principio de operación. Existen otros sistemas de largo alcance que utilizan ondas acústicas de superficie en el rango de microondas.

Todos estos sistemas “long-range” operan en los rangos de UHF, 868 MHz (Europa) y 915 MHz (USA) y en rango de microondas en 2,5 GHz y 5,8 GHz. La principal ventaja de trabajar a estas frecuencias es tener una longitud de onda corta, lo que permite la construcción de antenas de un tamaño muy pequeño y de gran eficiencia. Los sistemas que usan el principio backscatter tienen unos alcances típicos de 3 m en transponders pasivos (sin baterías) y de unos 15 m en transponders activos. La batería de los transponders activos no proporcionan la energía necesaria para la comunicación entre lector y transponder, únicamente alimentan el microchip en su proceso de almacenamiento y consulta de memoria. La energía para la transmisión entre el transponder y el lector, por tanto, es únicamente la extraída del campo electromagnético generado por el interrogador al realizar la comunicación con el transponder.

Básicamente el transponder modula la información recibida desde el lector variando la impedancia de la antena, esto se realiza variando el valor de la resistencia de carga  $R_L$ . Podemos ver en la Figura 2.13 al igual que en el ejemplo de acoplamiento inductivo, la impedancia del transponder es modulada por el transistor FET del chip.

El lector tiene un acoplador direccional para separar la señal transmitida de la señal recibida mucho más débil. El interrogador detecta los datos transmitidos por la tarjeta como una perturbación del propio nivel de la señal. La señal recibida por el interrogador desde la tarjeta está a un nivel de unos -60db por debajo de la portadora de transmisión del propio sensor.



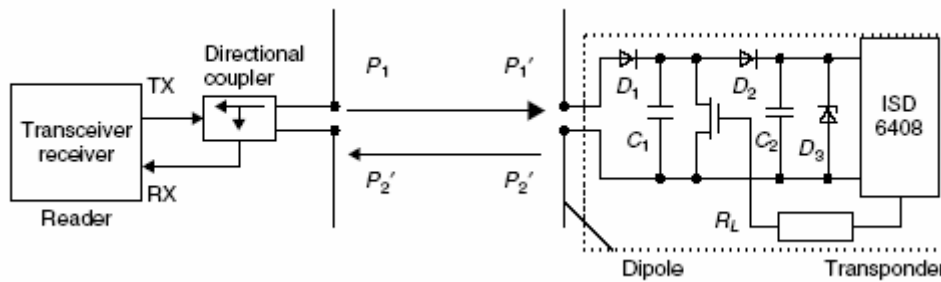


Figura 2. 13 Esquema del funcionamiento de los sistemas backscatter.

En referencia a la energía necesaria para la transmisión de información a estas frecuencias, se debe realizar con anterioridad un cálculo de las pérdidas por espacio libre en relación a la distancia  $r$  entre transponder y lector, podemos ver la ecuación (1.1). En este caso tendremos como variables las ganancias de las dos antenas y la frecuencia a la que opera el sistema. Por lo que respecta a las unidades, la frecuencia está expresada en Hz y la distancia en m.

$$a_F = -147.6 + 20 \log(r) + 20 \log(f) - 10 \log(G_T) - 10 \log(G_R) \quad (2.1)$$

Las pérdidas en espacio libre son la relación entre la potencia emitida por el lector y la potencia recibida en el transponder, todo esto a una determinada frecuencia.

Usando la tecnología de semiconductores de baja corriente los chips de los transponders pueden operar con un consumo no mayor de  $5\mu W$ . Existen sistemas que incorporan al transponder unas baterías adicionales, lo que implicaría un aumento en el rango de alcance, estos sistemas permiten incluso optimizar el consumo de estas baterías, cuando el transponder no esta en el rango de alcance del lector, las baterías permanecen en un estado de desconexión hasta que nuevamente se encuentran bajo la acción del interrogador. En este estado de “stand-by” el consumo es de pocos  $\mu A$ . El chip no es reactivado hasta que recibe una señal lo suficientemente fuerte en el rango de alcance del lector para volver al estado normal.

En la Tabla 2.3 podemos observar las perdidas en espacio libre a diferencias frecuencias, vemos como se esperaba que a más frecuencia y más distancia, más pérdidas.

Distance $r$	868 MHz	915 MHz	2.45 GHz
0.3 m	18.6 dB	19.0 dB	27.6 dB
1 m	29.0 dB	29.5 dB	38.0 dB
3 m	38.6 dB	39.0 dB	47.6 dB
10 m	49.0 dB	49.5 dB	58.0 dB

Tabla 2.3 Perdidas en espacio libre considerando la ganancia del transponder como 1.64 (dipolo), y la ganancia de la antena del lector como 1 (emisor isotrópico)

La principal diferencia con los sistemas inductivos es de donde proviene la energía que aprovecha el transponder para realizar la comunicación, mientras los sistemas a una frecuencia más elevada utilizan las ondas electromagnéticas, consiguiendo así un rango de alcance mayor, los sistemas inductivos utilizan la energía que una antena crea a su alrededor.

### Transferencia de datos entre transmisor y transponder

Por la tecnología de radares sabemos que las ondas electromagnéticas se reflejan en objetos con dimensiones mayores a la mitad de la longitud de onda. La eficiencia con la que estos objetos reflejan las ondas se describe por el término conocido como “reflection cross-section”. Una pequeña parte de la potencia emitida por la antena del lector es absorbida por la antena del transponder, pasa por la antena del transponder como un voltaje de HF y después es rectificado por diodos. El voltaje debe ser suficiente para servir como alimentación para rangos pequeños. Una proporción de la potencia absorbida es reflejada por la antena y retornada.

Las características de esta reflexión pueden ser influenciadas por las alteraciones en la carga de la antena. Para transmitir del transponder al lector, la resistencia de carga presente en el transponder conectada e paralelo con la antena, se conecta y desconecta según el flujo de datos. La amplitud de esa onda reflejada desde el transponder es lo que se modula, de ahí el nombre de modulación backscatter. Esta potencia reflejada es radiada en el espacio libre, una pequeña parte de esa potencia es recogida por la antena del lector. Esa potencia, el lector la recoge por medio de un acoplador direccional, depreciando así la potencia que emite él mismo la cual es sustancialmente mayor.

#### 2.4.3 Close coupling

Los sistemas close coupling están diseñados para rangos de alcance entre 0.1 cm y un máximo de 1 cm. El transponder cuando se realiza la comunicación suele estar en el centro de un aro que es la bobina del lector, o bien, en el centro de una bobina en forma de “u”. El funcionamiento de las bobinas del transponder y del lector es el mismo que el de un transformador. El lector representa las espiras primarias y el transponder las secundarias del transformador. Podemos verlo en la Figura 2.14.

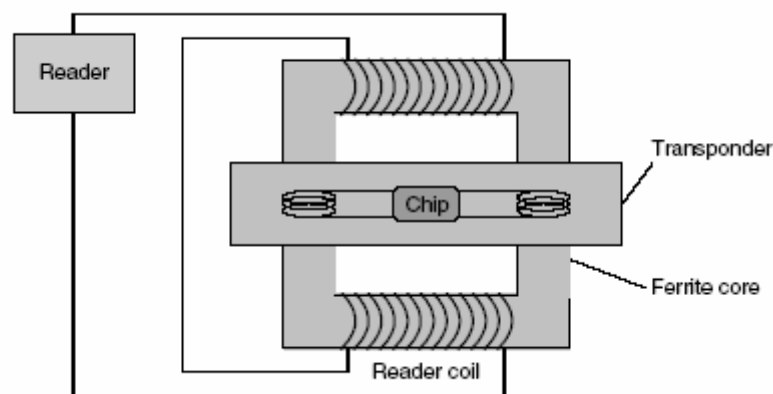


Figura 2.14 En los sistemas Close Coupling el transponder debe insertarse en el reader para producirse el acoplamiento magnético entre bobinas.

Una corriente alterna de alta frecuencia en las espiras primarias genera un campo magnético de alta frecuencia que se transmite por la bobina del transponder. Esta energía es rectificadora y proporciona la alimentación al chip del transponder. Debido a que la tensión inducida es proporcional a la frecuencia de la corriente entrante, la frecuencia seleccionada debe ser lo más elevada posible. En la práctica son usados rangos entre 1 – 10 MHz. Para mantener las pérdidas en el núcleo del “transformador” estas bobinas son elaboradas con ferrita, un material que optimiza las pérdidas a estas frecuencias.

A diferencia con los sistemas de acoplamiento inductivo y microwave, la eficiencia de la energía transmitida del lector al transponder es excelente, por eso suelen ser usados en sistemas que necesitan del uso de chips potentes, que consuman mucha energía, como por ejemplo microprocesadores.

## 2.5 Rangos de frecuencia

El hecho de que los sistemas de RFID generen y radien ondas electromagnéticas implica que éstos sean clasificados como sistemas de radio.

El funcionamiento de otros sistemas de radio no debe verse interrumpido o perjudicado, bajo ninguna circunstancia, por las ondas emitidas por un sistema de identificación por radiofrecuencia.

Es particularmente importante asegurarse de que los sistemas RFID no interfieren con la televisión y la radio, los servicios de radio móviles (policía, seguridad, industria), las comunicaciones marinas y aeronáuticas y los teléfonos móviles. La necesidad de acomodar otros servicios de radio disminuye significativamente la variedad de frecuencias disponibles en las que podemos trabajar a la hora de implementar un sistema de RFID. Por este motivo, normalmente sólo es posible usar rangos de frecuencia que han sido reservados específicamente para aplicaciones industriales, científicas o médicas. Estas son las frecuencias clasificadas mundialmente como rangos ISM (Industrial-Scientific-Medical) o SRD y pueden también ser usadas para aplicaciones de identificación por radiofrecuencia.

En la siguiente tabla 2.4 vemos algunos rangos de frecuencia usados en sistemas de RFID y sus principales características:

<b>Rangos de frecuencia para sistemas de RFID</b>		
Rango de frecuencia	Observaciones	Intensidad de campo / Potencia de TX.
< 135 kHz	Baja potencia. Acoplamiento inductivo.	72 dB $\mu$ A/m
6.765 ... 6.795 MHz	Media frecuencia (ISM), acoplamiento inductivo.	42 dB $\mu$ A/m
7.400 ... 8.800 MHz	Media frecuencia, usado sólo para EAS (electronic article surveillance).	9 dB $\mu$ A/m
13.553 ... 13.567 MHz	Media frecuencia (13.56 MHz, ISM), acoplamiento inductivo, ISO 14443, MIFARE, LEGIC..., smart labels (ISO 15693, Tag-It, I-Code,...) y control de artículos (ISO 18000-3).	42 dB $\mu$ A/m
26.957 ... 27.283 MHz	Media frecuencia (ISM), acoplamiento inductivo, sólo aplicaciones especiales.	42 dB $\mu$ A/m
433 MHz	UHF (ISM), acoplamiento por backscatter, raramente usado para RFID.	10 ... 100 mW
868 ... 870 MHz	UHF (SRD), acoplamiento por backscatter, nueva frecuencia, sistemas bajo desarrollo.	500 mW, sólo Europa
902 ... 928 MHz	UHF (SRD), acoplamiento por backscatter, varios sistemas.	4 W – espectro ensanchado, sólo USA/Canadá.
2.400 ... 2.483 GHz	SHF (ISM), acoplamiento por backscatter, varios sistemas, (identificación de vehículos: 2.446 .. 2.454 GHz)	4 W – espectro ensanchado, sólo USA/Canadá, 500 mW. Europe
5.725 ... 5.875 GHz	SHF (ISM), acoplamiento por backscatter, raramente usado para RFID.	4 W USA/Canadá, 500 mW Europa

Tabla 2.4 Rangos de frecuencia para RFID.

Como podemos ver en el Figura 2.15 la banda ISM recoge un amplio grupo de frecuencias que se pueden usar en los sistemas de RFID:

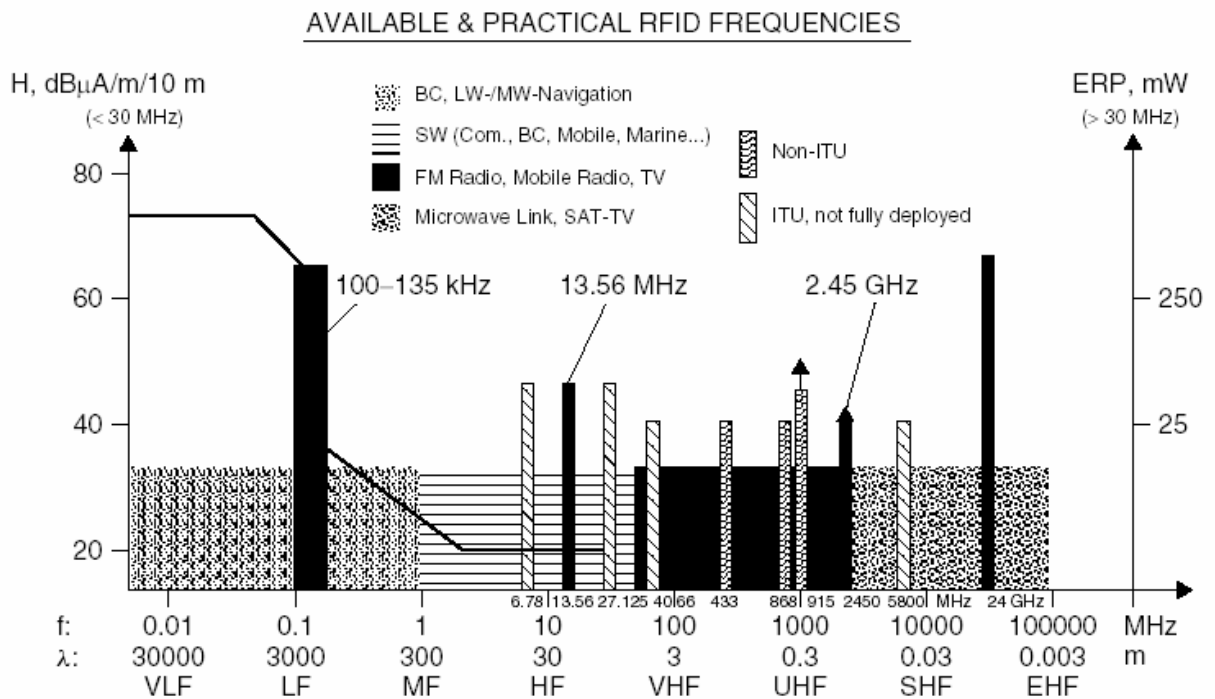


Figura 2.15 Representación de la banda de frecuencia ISM.

## 2.6 Diferentes sistemas de identificación

Existen diversos sistemas de identificación automática. Dentro de esta familia se encuentran sistemas como el código de barras, tarjetas inteligentes, RFID o en otro ámbito los sistemas reconocedores de voz o de huellas dactilares. Se puede observar el esquema de los diferentes sistemas en la Figura 2.16.

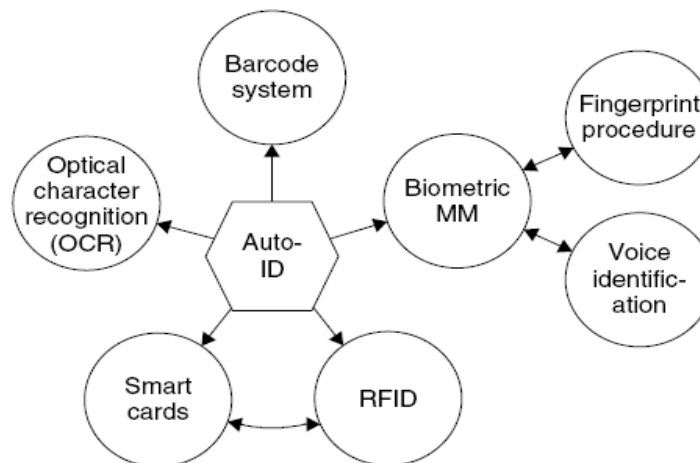


Figura 2.16 Esquemas de los sistemas más importantes de auto-identificación.

### Códigos de barras

Es el sistema de identificación más utilizado. El código de barras es un código binario comprendido por una serie de barras y espacios configurados paralelamente. El diseño de estos campos representa unos datos relacionados con un elemento. La secuencia puede ser interpretada de forma numérica o alfanumérica. Esta secuencia es leída por un scanner óptico láser, que se basa en la diferente reflexión que sufre la luz del láser en las barras negras o en los espacios en blanco. Podemos ver un clásico código de barras en la Figura 2.17.



Figura 2.17 Código de barras con el ISBN de un producto.

El más popular de todos estos sistemas de código de barras es el código EAN (European Article Number), el cual se diseñó especialmente para el sector de la alimentación. Este código es una evolución del UPC (Universal Product Code) estadounidense, el cual fue introducido en EEUU antes de 1973. Actualmente los dos códigos son totalmente compatibles. El código EAN está formado por 13 dígitos: el identificador del país, el identificador de la empresa, el número de manufactura y el denominado “check digit”. Aparte del EAN, existen diversos sistemas de código de barras en otros campos industriales como el código Codabar, en el sector médico, el código 2/5 utilizado en la industria del automóvil, contenedores de barcos, industria

pesada en general o el código 39, usado en procesos industriales, logísticos o librerías. Podemos ver la estructura de un código de barras con código EAN en la Figura 2.18

Country identifier		Company identifier					Manufacturer's item number					CD
4	0	1	2	3	4	5	0	8	1	5	0	9
FRG		Company Name 1 Road Name 80001 Munich					Chocolate Rabbit 100 g					

Figura 2.18 Ejemplo de una estructura del código de barras en código EAN.

Existe también otro tipo de sistema óptico denominado OCR (Optical Character Recognition) que fue usado por primera vez en la década de los 60. Estos sistemas tienen como ventaja la gran densidad de información. Actualmente se usan en producción, campos de servicios y administrativos, y en algunos bancos para el registro de cheques. Los inconvenientes de estos sistemas residen en su alto precio, y la complejidad de los lectores en comparación con otros sistemas de identificación.

Actualmente se rebate la posibilidad de los sistemas RFID como sustitutos de los códigos de barras, por ello se puede realizar una comparación entre estas dos tecnologías:

El código de barras se inventó hace más de 25 años y, durante este tiempo, ha sido la tecnología más utilizada por los comercios para identificar los productos en venta. Sin embargo, el código de barras tiene una serie de limitaciones:

- Necesita visibilidad para funcionar. Es decir, el código de barras debe ser visible ante el lector para que el producto pueda ser identificado (es lo que en inglés se denomina *line of sight*).
- El código de barras tradicionalmente identifica un tipo de producto, no una unidad de dicho producto. El código de barras X puede identificar botellas de agua, pero no puede identificar una botella en concreto. Esta no es una limitación inherente de la tecnología, pero normalmente los sistemas de código de barras no se utilizan como identificadores únicos.
- Un código de barras se daña o se rompe fácilmente, porque normalmente se adhiere a la superficie del producto y no forma parte de él (como sí puede formar parte un tag), y si se rompe no puede ser leído.

La tecnología RFID supera estas limitaciones. Se trata de una tecnología radial (es decir, no es necesario que el tag y el lector estén cara a cara, pues funcionan en un radio de acción determinado), puede identificar productos en concreto y no sólo tipo de productos y, finalmente, los dispositivos son muy resistentes y normalmente forman parte del producto o se colocan debajo de una superficie protectora.

También cabe mencionar que por muy reducido que sean los costes de fabricación de un tag pasivo y todo el sistema, nunca será inferior al precio de un sistema de código de barras, pero en un plazo más largo puede resultar más económica

la instalación de un sistema RFID que un sistema óptico dado las ventajas que aportan al comprador.

### **Procedimientos biométricos**

Son sistemas que identifican personas por comparación de unas características individuales y comparándola con una característica física que es individual y que no admite equivocación. Podemos hablar de sistemas identificadores por huella dactilar, identificación por voz y en menor número identificador por retina.

### **Tarjetas inteligentes (Smart Cards)**

Una smart card, es un sistema de almacenamiento electrónico de datos, con una adicional capacidad para procesar dichos datos (microprocessor card). Por conveniencia está instalado dentro de una tarjeta de plástico del tamaño de una tarjeta de crédito. Las primeras smart cards se lanzaron en 1984 como tarjetas telefónicas. El contacto con el lector proporciona la alimentación y un pulso de reloj. La transferencia de datos entre el lector y la tarjeta suele usar una interfaz serie bidireccional (puerto E/S). Una de las principales ventajas de las tarjetas inteligentes es la facilidad de almacenaje de información, así como la protección que posee de posibles accesos indeseados. Son seguras y baratas.

Su desventaja es la vulnerabilidad a contactos con ropa, corrosión y suciedad. Los lectores que son usados frecuentemente son muy caros de mantener debido a su malfuncionamiento.

Es posible diferenciar dos tipos de smart card según su funcionamiento interno: “memory card” y “microprocessor card”. En las memory card, usualmente una EEPROM se accede usando una secuencia lógica, máquina de estados. Tiene unos sencillos algoritmos de seguridad y una funcionalidad específica para cada aplicación. Estas tarjetas son muy limitadas en lo que a funcionalidad se refiere, pero lo suplen con un coste mínimo.

Las tarjetas con microprocesadores, tienen éstos conectados a segmentos de memoria (ROM, RAM y EEPROM). Los que tienen ROM incorporan un sistema operativo para el microprocesador insertado durante su fabricación. No puede ser modificado posteriormente. La RAM, zona donde el microprocesador trabaja con la memoria temporalmente, los datos almacenados son borrados cuando se desconecta la alimentación. La EEPROM contiene datos de la aplicación y de los programas que gestionan la aplicación. Se modifican mientras se opera con ella. Son tarjetas muy flexibles, que pueden realizar más de una aplicación.



System parameters	Barcode	OCR	Voice recog.	Biometry	Smart card	RFID systems
Typical data quantity (bytes)	1–100	1–100	—	—	16–64 k	16–64 k
Data density	Low	Low	High	High	Very high	Very high
Machine readability	Good	Good	Expensive	Expensive	Good	Good
Readability by people	Limited	Simple	Simple	Difficult	Impossible	Impossible
Influence of dirt/damp	Very high	Very high	—	—	Possible (contacts)	No influence
Influence of (opt.) covering	Total failure	Total failure	—	Possible	—	No influence
Influence of direction and position	Low	Low	—	—	Unidirectional	No influence
Degradation/wear	Limited	Limited	—	—	Contacts	No influence
Purchase cost/reading electronics	Very low	Medium	Very high	Very high	Low	Medium
Operating costs (e.g. printer)	Low	Low	None	None	Medium (contacts)	None
Unauthorised copying/modification	Slight	Slight	Possible* (audio tape)	Impossible	Impossible	Impossible
Reading speed (including handling of data carrier)	Low ~4 s	Low ~3 s	Very low >5 s	Very low >5–10 s	Low ~4 s	Very fast ~0.5 s
Maximum distance between data carrier and reader	0–50 cm	<1 cm Scanner	0–50 cm	Direct contact**	Direct contact	0–5-m, microwave

Tabla 2.5 Comparación de los diferentes sistemas RFID con sus principales ventajas y desventajas.

## **2.7 Criterios diferenciales en sistemas RFID**

Actualmente el volumen de uso de los sistemas de RFID es muy grande, y ha tenido una evolución importante en estos últimos años. Están plenamente integrados en aplicaciones de identificación, y cada vez aparecen más aplicaciones para esta tecnología. Desarrolladores de sistemas RFID han conseguido que la tecnología necesaria para optimizar estos sistemas a campos como el procesamiento de tickets, la identificación animal, automatización industrial o el control de acceso estén disponibles en el mercado. Uno de las principales complicaciones es la inexistencia de unos estándares para estos sistemas RFID.

A la hora de seleccionar un sistema de RFID es indispensable adecuar unos parámetros de diseño a la aplicación en la que se está trabajando. Hay unos criterios principales a la hora de seleccionar un sistema de RFID u otro, como por ejemplo la frecuencia a la que trabaja el sistema, el rango de alcance, los requerimientos de seguridad y la capacidad de memoria.

### **Frecuencia de operación**

Los sistemas RFID que operan a frecuencias entre 100 KHz y 30 MHz que usan acoplamiento inductivo, y los sistemas de microondas en el rango de 2.45-5.8 GHz que usan campos electromagnéticos para el acoplamiento. Hay que tener en cuenta la absorción que realiza el agua o sustancias no conductivas es 100000 veces menor a 100 KHz que a 1 GHz. Por esta razón sistemas HF fueron los primeros en ser usados por su gran penetración en los objetos.

Un claro ejemplo son los sistemas que operan en el ganado que puede ser leído con un lector operando a una frecuencia menor de 135 KHz. Los sistemas de microondas pueden trabajar a un rango mayor, entre los 2-15 metros. Pero estos sistemas suelen requerir el uso de una batería adicional para alimentar el transponder, que no tiene suficiente con la energía que le proporciona el interrogador.

Otro factor importante es la sensibilidad a la interferencia con campos electromagnéticos, como son los que producen por ejemplo motores eléctricos. Los sistemas con acoplamiento inductivo tienen un peor comportamiento delante de estas interferencias. Por este motivo sistemas de microondas son usados líneas de producción como pueden ser los sistemas de pintado dentro de la industria del automóvil. Otros factores que se deben tener en cuenta para una elección de un sistema RFID de una frecuencia u otra, son la mayor capacidad de memoria que tienen los sistemas de microondas (<32 Kbyte) y la mayor resistencia que tienen a las altas temperaturas.

Por estas ventajas e inconvenientes la elección de un sistema a una frecuencia u otra determinará la eficiencia de este sistema para la aplicación.

### **Rango de alcance**

El rango de alcance necesario para una aplicación determinada viene dado por tres factores:

- La posible posición del transponder.
- La distancia mínima entre muchos transponders en la zona de operación.
- La velocidad del transponder en la zona de interrogación del lector.

La Figura 2.19 muestra cuál es el rango de alcance de los diferentes sistemas de acoplamiento.

Por ejemplo en aplicaciones de pago, como los tickets en el transporte público, la velocidad del transponder es pequeña cuando pasa el viajero por el lector, la distancia mínima corresponde a la distancia entre dos pasajeros, por eso no se puede poner un rango muy elevado y que detecte varios billetes de diversos pasajeros.

Otro ejemplo puede ser la industria del automóvil, en una línea de montaje puede haber mucha variación en la distancia entre un transponder y el lector, por eso hay que preparar el sistema para que alcance la mayor distancia prevista. En esa distancia sólo puede haber un transponder. Para este problema los sistemas de microondas, los cuales tienen un campo mucho más direccional ofrecen claras ventajas sobre los campos no direccionales que crean los sistemas con acoplamiento inductivos.

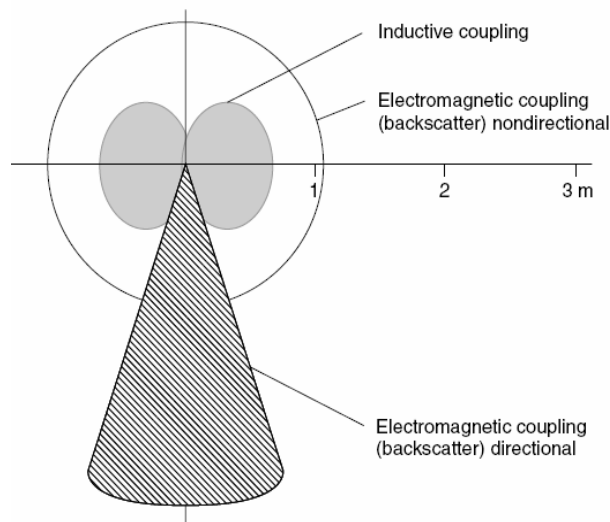


Figura 2.19 Comparación entre las zonas de interrogación de los lectores de diferentes sistemas.

La velocidad de los transponders con respecto al lector, junto con la máxima distancia de lectura/escritura, determina la duración del tiempo que tiene que estar en la zona de interrogación del lector para poder transmitir toda su información.

### Requisitos de seguridad

Como requisitos de seguridad en sistemas de RFID, tenemos por ejemplo la encriptación y autenticación. Debido a que estos sistemas pueden estar trabajando con objetos de valor, o incluso con dinero, estos sistemas deben estar probados en la planificación inicial para no encontrarse con ninguna sorpresa a la hora de

implementarlo. Podemos clasificar las aplicaciones según su necesidad de seguridad en dos grupos:

- Aplicaciones industriales o privadas.
- Aplicaciones públicas con dinero y bienes.

Esta clasificación se puede entender mejor con dos ejemplos:

Las líneas de producción en la industria del automóvil son aplicaciones del primer grupo, industriales o privadas. Suelen sufrir menos ataques, ya que un ataque por parte de una persona, alterando o falsificando datos, no supondrían un beneficio personal, pero sí provocaría un malfuncionamiento de toda la cadena.

En el segundo grupo están los sistemas de ticket para transporte público, donde el peligro de un ataque es mucho más elevado. Si se realizase un ataque y diera resultado, podría reportar un daño económico muy elevado a la compañía y su imagen quedaría afectada. Para este tipo de aplicaciones procesos de autenticación y encriptación son indispensables. Para aplicaciones con unos requisitos de seguridad máxima como aplicaciones de banca y tarjetas monedero, sólo transponders con microprocesadores pueden ser usados.

### **Capacidad de memoria**

La cantidad de información que puede albergar el chip del transponder y el precio, es otra variable que se debe manejar a la hora de diseñar un sistema de RFID para una aplicación determinada. Se necesita saber cuanta cantidad de información usa el sistema, que datos maneja.

Principalmente los transponders con sistemas de memoria de solo lectura se usan para aplicaciones de bajo coste con necesidades de información baja. Si lo que se necesita es que la información se pueda escribir, no sólo leer del transponder, son necesarios transponders con memoria EEPROM o RAM. La memoria EEPROM se usa principalmente en los sistemas de acoplamiento inductivo, dispone de capacidades de memoria entre los 16 bytes a los 8 Kbytes. Las memorias SRAM disponen de baterías, son usadas en sistemas de microondas, con una memoria que oscila alrededor de los 256 bytes y 64 Kbytes.

## 2.8 Clasificación de los sistemas RFID

Los sistemas RFID se pueden clasificar siguiendo varios criterios, como pueden ser la frecuencia a la que trabajan los sistemas (LF, HF, UHF o microondas), la alimentación de los transponders (activos o pasivos) o según el principio de funcionamiento en el que se basan (acoplamiento inductivo, backscatter o microwave).

Como ya se ha hecho hincapié en estas diferencias, es conveniente centrarse en otras características que diferencian entre sí los sistemas de RFID. Estas clasificaciones tienen por criterio diferencial el sistema de memoria que incorpora el transponder, el rango de información y la capacidad de procesamiento que tiene el transponder o el procedimiento de comunicación que se realiza entre transponder y lector.

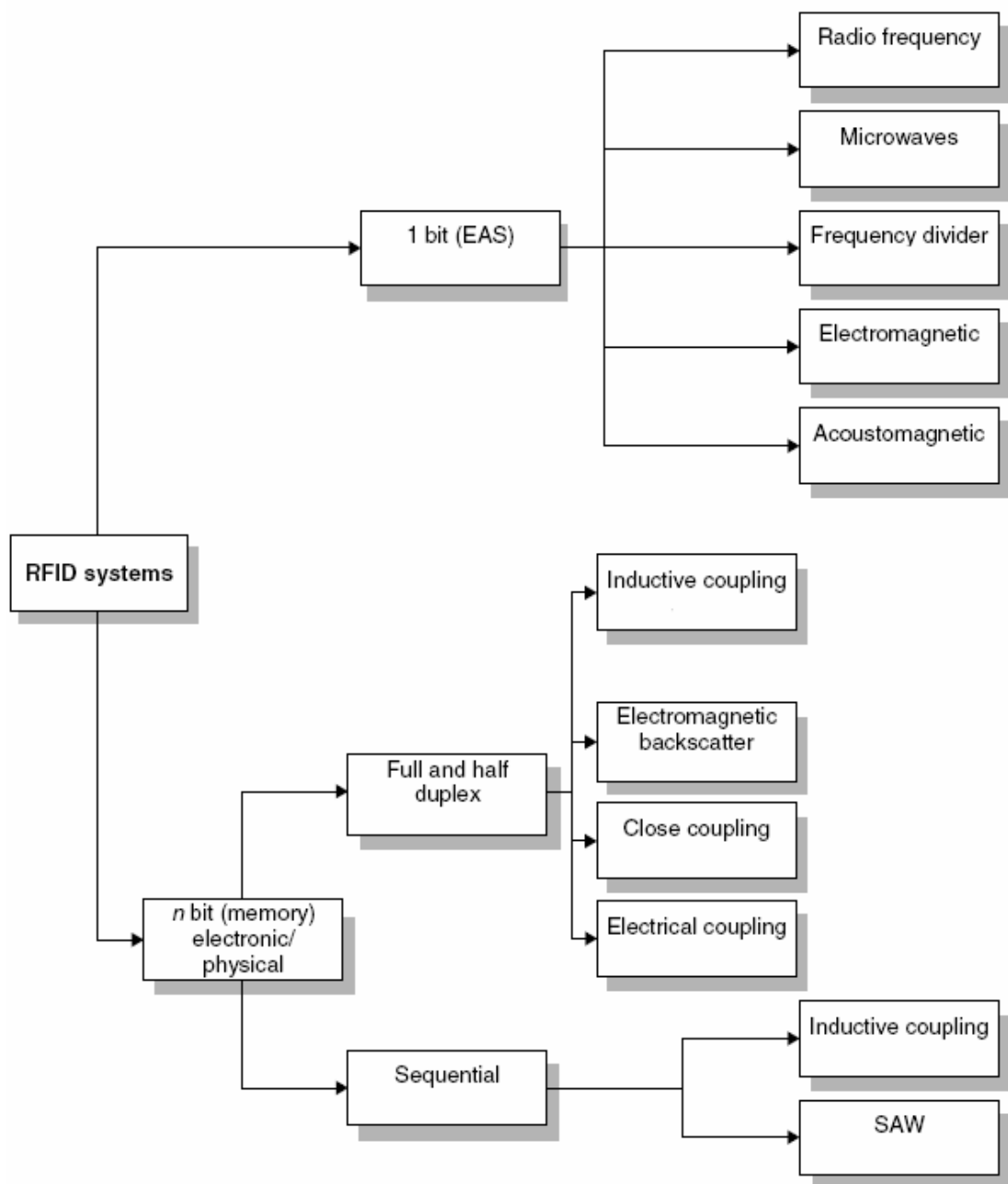


Figura 2.20 Esquema de los diferentes principios de operación de los sistemas RFID.

Uno de estos criterios es según el rango de información y la capacidad de proceso de datos que ofrece el transponder, así como el tamaño de su memoria de datos. Realizando esta clasificación obtenemos un amplio espectro de variantes que se dividen en sistemas Low-end, Mid-range y High-end.

- **Sistemas Low-end:** los sistemas EAS (Electronic Article Surveillance) componen principalmente este grupo, son sistemas que reconocen la presencia de un artículo en la zona de alcance del lector. Transponders de sólo lectura también son sistemas Low-end, estos transponders tienen grabados permanentemente los datos que pueden consistir en un único número de serie. Si una de estas etiquetas entra en el radio de acción de un lector inicia una comunicación broadcast con su número de serie. Existe el problema de que haya la presencia de más de un transponder en el radio de acción del lector, en este caso puede haber una colisión de datos enviados por los transponders y el lector no podrá detectar ninguno de ellos.

Estos sistemas son adecuados para diversas aplicaciones que necesitan cantidades de información pequeñas. Por ejemplo sustituyendo a los códigos de barras, ya que la simplicidad de sus funciones permite que el área de chip sea reducida, así como su consumo y su coste de producción. Estos sistemas son capaces de trabajar en todo el rango de frecuencias que opera RFID.

- **Sistemas Mid-range:** estos sistemas permiten la escritura en la memoria. El tamaño de la memoria va desde los pocos bytes hasta el orden de 100Kbyte EEPROM (transponders pasivos) o SRAM (transponders activos).

Estos transponders son capaces de procesar comandos simples de lectura para la selectiva lectura/escritura de la memoria en una máquina de estados permanentemente codificados. Estos transponders son capaces de soportar procesos de anticollisión, por lo que varios transponders en el radio de acción de un lector no se interfieren y el lector es capaz de diferenciarlas. En estos sistemas se utilizan procedimientos de encriptación de datos y autenticación entre lector y transponder. Estos sistemas son capaces de trabajar en todo el rango de frecuencias que opera RFID.

- **Sistemas High-end:** estos sistemas poseen microprocesadores y un sistema de funcionamiento de tarjeta inteligente. El uso de los microprocesadores facilita el uso de algoritmos de autenticación y encriptación más complejos. Estos sistemas operan en una frecuencia de 13.56 MHz.

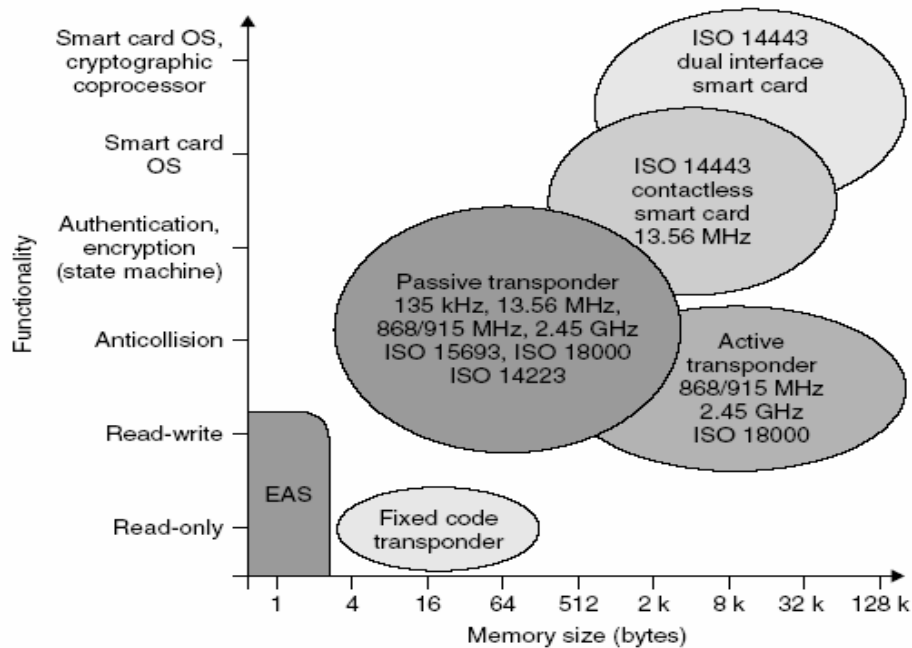


Figura 2.21 Esquema de los diferentes sistemas en función del tamaño de memoria y su funcionalidad.

Podemos clasificar los sistemas de RFID según la cantidad de información que contiene los transponders.

Aunque los sistemas RFID suelen tener una capacidad de información que va desde los pocos bytes a centenares de KBytes. Pero existen numerosos sistemas que únicamente poseen un bit de información, los justos para tener controlados dos estados por el lector: la presencia del transponder en el campo creado por el lector o la ausencia del transponder. A pesar de su simpleza, son sistemas especialmente adecuados para aplicaciones como monitorizaciones o funciones de señalización. Debido a que los “1-bit transponder” como son conocidos, no precisan un chip electrónico, su coste es ínfimo.

Una de sus principales aplicaciones es el EAS (Electronical Article Surveillance) para la protección de objetos en tiendas y negocios. Cuando alguien intenta sustraer un artículo, sin haber sido desactivado el transponder, debe pasar por un lector situado en la salida de la tienda, si el lector detecta la presencia de un transponder inicia la reacción apropiada.

Estos sistemas pueden clasificarse según también su principio de funcionamiento: procedimiento RF basado en unos circuitos LC resonantes ajustados a una determinada frecuencia de resonancia; sistemas EAS en el rango de microondas que generan armónicos con componentes con características no lineales como los diodos; divisores de frecuencia que operan en el rango de 100-135,5 KHz donde la frecuencia de resonancia proporcionada por el lector es dividida en el transponder y enviada hacia el lector nuevamente, generalmente dividida entre 2.

Los denominados “Electromagnetic types” que usan campos magnéticos muy fuertes en el rango NF (10Hz-20KHz), los elementos de seguridad contienen una línea

metálica que sufren una saturación magnética ya que esta sometida a un campo magnético muy fuerte y alternante, esto crea unos armónicos a la frecuencia básica del lector.

También es posible superponer frecuencias más elevadas a la señal básica; como son elementos no lineales crean frecuencias suma y diferencia con las frecuencias añadidas. El lector no reacciona a los armónicos de la frecuencia básica pero si que lo hace a la frecuencia suma o diferencia de las señales creadas.

Por último tenemos a los sistemas acústico magnético basados en pequeñas cajas de plástico que contienen dos líneas metálicas, una de ellas no esta conectada a la caja y produce una pequeña vibración al pasar por un campo magnético. La amplitud de esta vibración es especialmente alta si la frecuencia del campo magnético alterno producido por el lector, corresponde con la frecuencia de resonancia de la línea metálica.

Para contrastar con los transponders de un solo bit, el cual normalmente explota los efectos físicos (procesos oscilación estimulada, estimulación de armónicos por diodos no lineales en la curva de histéresis de metales), existen transponders que usan un microchip electrónico como sistemas portador de datos. Tienen una capacidad de almacenamiento de información mayor a pocos Kbytes. Para leer o escribir en estos sistemas de almacenamiento se realiza una transferencia de datos entre lector y transponder, esta transferencia puede seguir tres procesos: half duplex, full duplex y secuencial.

Podemos ver un esquema de la transmisión downlink y uplink de los tres procesos en la figura 2.22.

Dentro de la clasificación que podemos hacer por la cantidad de información transmitida, cuando hablamos de memorias con más de un bit podemos realizar otra clasificación a tenor del procedimiento que sigue la comunicación entre lector y etiqueta.

**Sistemas half/full duplex:** El lector inicia la comunicación con el transponder. El transponder responde en broadcast cuando detecta el campo RF. Debido a que la señal generada por el transponder que recibe el lector es mucho más débil que la propia señal generada por el lector, éste debe tener sistemas capaces de diferenciar ambas señales. En la práctica la transferencia de datos se realiza por modulaciones con portadora o subportadoras, pero también con armónicos de la frecuencia de transmisión del lector.

La diferencia radica en que en los sistemas half duplex la transferencia de datos entre lector y transponder, se alterna con la comunicación entre transponder y lector. Estos sistemas suelen usar las modulaciones de carga con o sin subportadora, y armónicos.

Por lo que se refiere a los sistemas full duplex, la comunicación entre el transponder y el lector se realiza al mismo tiempo que la comunicación entre lector y transponder. Incluye procedimientos en la que la transferencia de datos se realiza mediante en una fracción de frecuencia del lector, en subarmónicos o en frecuencias completamente distintas, no armónicos.



Estos sistemas utilizan como principios de funcionamiento para la transmisión y recepción de datos, el acoplamiento inductivo, backscatter, close coupling y electrical coupling.

**Sistemas secuenciales:** Emplean el sistema en el cual el campo generado por el lector se enciende y se apaga en intervalos regulares. Lo que significa que el transponder es alimentado de forma intermitente (pulso). La transferencia entre transponder y lector se produce en esos intervalos en los que el lector no se comunica con el transponder. La desventaja de estos sistemas es la pérdida de energía en el transponder en los intervalos que se corta la comunicación, este problema puede ser solucionado con una alimentación externa.

Estos sistemas utilizan como principios de funcionamiento para la transmisión y recepción de datos, el acoplamiento inductivo y SAW (Surface Acoustic Wave); basado este último en el efecto piezoeléctrico y una dispersión en la superficie de las ondas acústicas a pequeña velocidad.

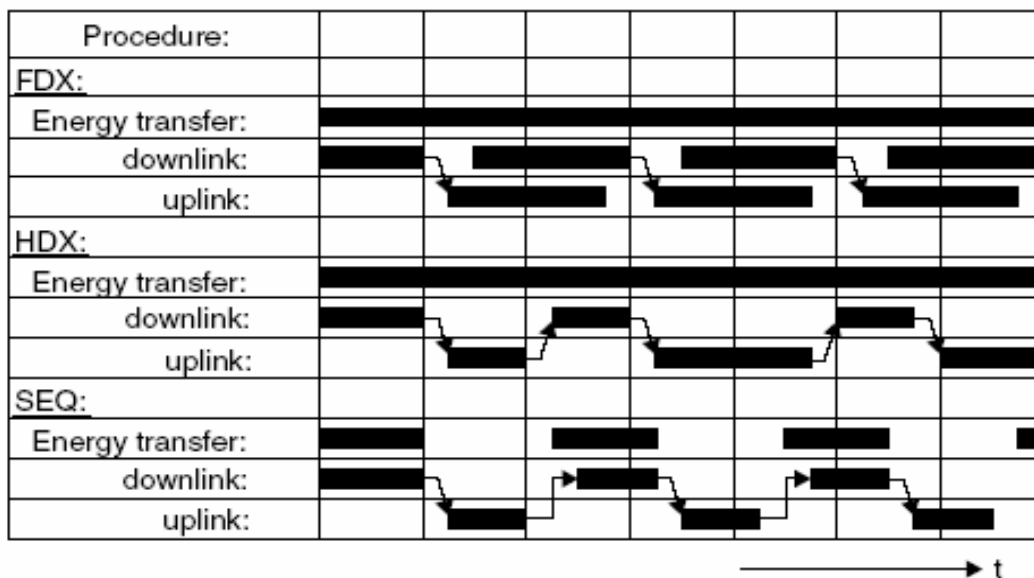


Figura 2.22 Esquema de los diferentes procedimientos, Full-duplex, Half-duplex y Secuencial.

Se puede clasificar los sistemas RFID según el tipo de memoria del transponder, EEPROMs, FRAMs o SRAMs. Existen numerosos transponders que tienen únicamente con información de un número de serie que se incorpora cuando se fabrica y no puede ser alterado después. En otro tipo de transponders sí es posible el escribir en la memoria.

- **EEPROMs (Electrically Erasable Programmable Read-Only memory):** la memoria más utilizada en acoplamiento inductivo. Como desventaja tiene el alto consumo de energía durante la operación de escritura y el número limitado de ciclos de escritura (100.000 y 1.000.000).
- **FRAMs (Ferromagnetic Random Access Memory):** tiene un consumo del orden de 100 veces menor que los EEPROMs y el tiempo de escritura 1000 veces menor.

- **SRAMs (Static Random Access Memory):** más utilizado en los sistemas de microondas. Facilita rápidamente el acceso a los ciclos de escritura. Por el contrario necesita un suministro de energía ininterrumpido de una batería auxiliable.

En sistemas programables la lectura, escritura y la autorización se realizan mediante lógica interna. Mediante máquinas de estado generalmente, se pueden realizar secuencias complejas, pero no posibilita cambios en el programa sin realizar cambios en el layout. El uso de microprocesadores mejora este problema, incluyendo software para cada aplicación.

Podemos clasificar también los sistemas RFID según los diferentes procedimientos para enviar datos desde el transponder al lector.

- **Reflexión o backscatter:** La frecuencia de la transmisión es la misma que la usada por el lector para comunicarse con el transponder (1:1).
- **Load modulation:** El campo del lector es influenciado por la frecuencia del transponder (1:1).
- **Subarmónicos:** Uso de subarmónicos ( $1/n$ ) y la generación de ondas armónicas de frecuencia múltiplos de  $n$  en el transponder.

## 2.9 Aplicaciones de los sistemas RFID

La tecnología RFID se ha ido haciendo un hueco en el mercado, con un progreso espectacular en los últimos años. Muchos son los sectores que se han visto beneficiados con la incursión de nuevos sistemas de identificación basados en la tecnología RFID, como los transportes, las tarjetas inteligentes, expedición de tickets, control de acceso, identificación de animales, identificación de contenedores, medicina o la industria del automóvil.

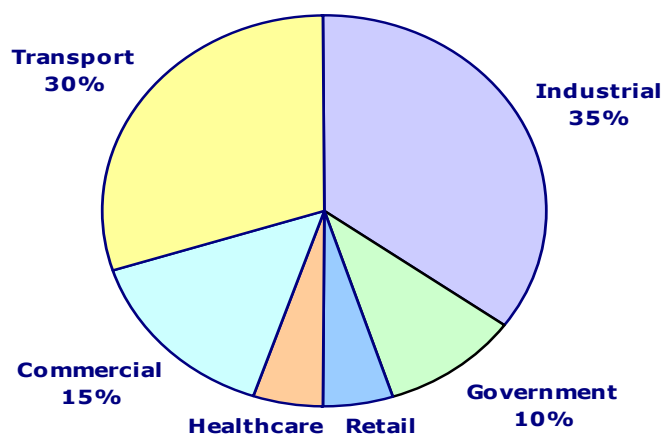


Figura 2.23 Estadística sobre la situación de la demanda de sistemas de RFID en 2002. Fuente: Palmer Brian & Company Inc. 2003.

### Control de accesos

Las aplicaciones en este campo han sido uno de los puntos fuertes de los sistemas RFID. No son unos sistemas nuevos, ya que llevan varios años usándose en empresas o recintos, para controlar el acceso a sus instalaciones. También se suelen usar para el acceso a parkings. Estas tarjetas son cada vez más funcionales, pudiendo permitir no sólo el acceso a distintas zonas, sino también a máquinas expendedoras o para pagos pequeños, por ejemplo en una cafetería de la empresa.

### Identificación de equipajes en el transporte aéreo

Es un claro ejemplo de una aplicación que puede reducir costes y tiempo a las compañías aéreas y a los aeropuertos. Se puede sustituir personal si el equipaje es direccionado mediante sensores, por toda la cadena, que detectan el transponder con la información del avión en el cual tiene que ser cargado. Aparte de esta ventaja, también es más cómodo a la hora de identificación del equipaje sobre posibles pérdidas. Además no supone un gasto excesivo para la rentabilidad que el sistema puede ofrecer. No ocurre ningún problema al ponerlo sobre las etiquetas ya usadas en los aeropuertos ni importa que los equipajes estén orientados de cualquier forma o apilados de cualquier manera.

Un sistema RFID es mucho más eficaz en esta aplicación que los usados códigos de barras. Las principales ventajas por las que las compañías del sector están incorporando estos sistemas son:

- La posibilidad de convivir con los sistemas de códigos de barras ya existentes y sus scanners. Así como encajar perfectamente en los sistemas de control de aeropuertos y sus sistemas de seguridad especialmente.
- Incorporar más información en el dispositivo sin aumentar el tamaño.
- La información va incorporada en la propia etiqueta, por lo que se ahorra la comunicación continua con una base de datos.

La mayoría de estos sistemas trabajan a una frecuencia de 13,56 MHz, como es el sistema instalado por los aeropuertos de Manchester y Munich en 1999, en acuerdo con la compañía aérea British Airways. Podemos ver un ejemplo de estas etiquetas en la Figura 2.24.



Figura 2.24 Etiqueta identificadora de RFID en el aeropuerto de Munich.

### **Industria del automóvil**

A principios de los 90 aparecieron sistemas RFID con transponders de sólo lectura destinados a la inmovilización de automóviles como un adelanto importante en la seguridad de los vehículos ante posibles robos. Los transponders de estos sistemas eran muy pequeños (cabían en la llave), no necesitaban baterías y eran de solo lectura. Cada uno de estos transponders disponía de un único y fijo código de seguridad. Su funcionamiento era sencillo, cuando el propietario giraba la llave producía unas señales electromagnéticas que eran las que verificaban la llave y permitían el arranque del motor.

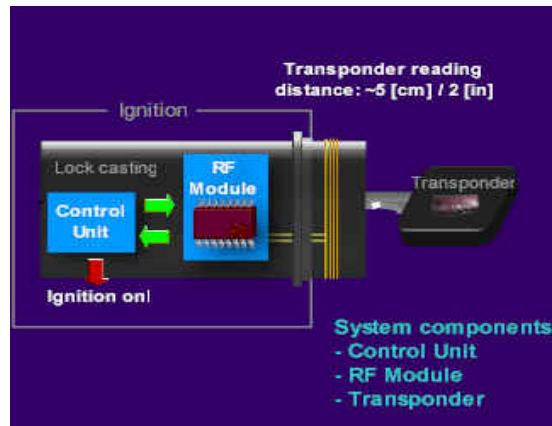


Figura 2.25 Esquema de funcionamiento del sistema de seguridad de automóvil.

En el sector de la seguridad en el automóvil, también se diseñó un sistema que inmoviliza el vehículo, de modo que cuando el usuario cerraba la puerta con su mando, generaba un código que recibía el coche y que volvía a enviar al transponder del mando a modo de confirmación. Podemos ver el funcionamiento en Figura 2.25.

Otra aplicación en los automóviles que cada vez incorporan más, es la tarjeta identificadora que permite que el vehículo se abra sin necesidad de introducir ninguna llave. Sólo necesita que el propietario se acerque lo suficiente al vehículo con su tarjeta para que detecte un transponder, lo confirme y proceda a desbloquear las puertas. Es un sistema más útil que el tradicional “mando a distancia”; en el que había que presionar un botón para abrir el vehículo.

### Comercio a distancia

Los sistemas RFID son los suficientemente seguros como para permitir pagos con ellos. Por ejemplo pagar combustible o usarlo en una máquina expendedora de comida o bebida. El cliente paga con su teléfono móvil o con una llave especial. Además proporciona información a las empresas sobre los gustos del cliente, pudiendo ofrecerle un servicio con más calidad.

El transponder posee una información única programada que al pasar cerca del lector es identificada, se verifica la autenticidad del transporte, y se pide permiso para la transacción.

Por lo que hace al sistema de pago en gasolineras, es muy cómodo tanto para el cliente como para la estación de servicio. Aumenta el número de coches que pueden repostar por hora, así como ofrece al usuario un tiempo menor de espera. Existen dos métodos:

- *Método Token:* Es muy similar al pago en dispensadores de bebida, cada transponder tienen un único código ya programado, que además está relacionado con una tarjeta de crédito. Se inicia la comunicación con el lector situado en el surtidor, nunca se envía el número de la tarjeta de crédito que no está ni siquiera

almacenado en el transponder. Se pide autorización a través de la estación de servicio, y se le permite repostar.

- *Método “Manos Libres”*: Es un sistema que difiere del anterior en que el transponder va adherido al cristal trasero del coche. Se realizan las mismas operaciones que en el caso anterior pero con más velocidad; con lo que la comunicación se realiza incluso antes que el cliente baje del coche.

## ***2.10 Principales sistemas RFID según su frecuencia***

Como ya hemos visto los sistemas de RFID tienen como uno de sus criterios diferenciales más importantes la frecuencia a la que operan. Por este motivo, es útil hacer una nueva comparación entre los sistemas RFID según su frecuencia, en ella nos centramos en los sistemas más usuales como son los que operan a 13,56 MHz, los que operan en el rango de 400 MHz a 1000 MHz y en el rango de los 2.45 GHz.

La inmensa mayoría de productos que se encuentran actualmente en el mercado usando la tecnología RFID y un gran número de los nuevos proyectos operan en estos tres rangos de frecuencia.

### ***2.10.1 Sistemas RFID a 13.56MHz.***

#### **Principios de Operación**

Hoy en día, la mayoría de los sistemas RFID que funcionan a 13.56MHz son pasivos, lo cual implica la no necesidad del uso de baterías. Esto tiene ventajas en cuanto al coste, tiempo de vida de las etiquetas y entorno en que se pueden emplear estos sistemas. El principio básico de operación es la transmisión de energía y datos usando acoplamiento inductivo. Este es el mismo principio que usan los transformadores.

A diferencia de otros sistemas de RFID que trabajan a frecuencias más altas (por ejemplo dentro de la banda UHF o microondas), los sistemas a 13.56MHz (e incluso los que trabajan a <135KHz) tienen la zona de operación en el campo creado junto a la antena del lector, lo que permite alcanzar unas distancias del orden del diámetro de la antena. Hay que tener en cuenta que esto es así siempre que estemos trabajando con sistemas con una sola antena.

Para distancias mayores al equivalente al diámetro de la antena, la intensidad del campo decrece con la tercera potencia de la distancia, lo cual significa que la potencia de transmisión requerida se incrementa con la sexta potencia de la distancia.

La Figura 2.26 muestra la dependencia de la intensidad del campo, normalizada, en función de la distancia para antena con un diámetro de 0.8m.

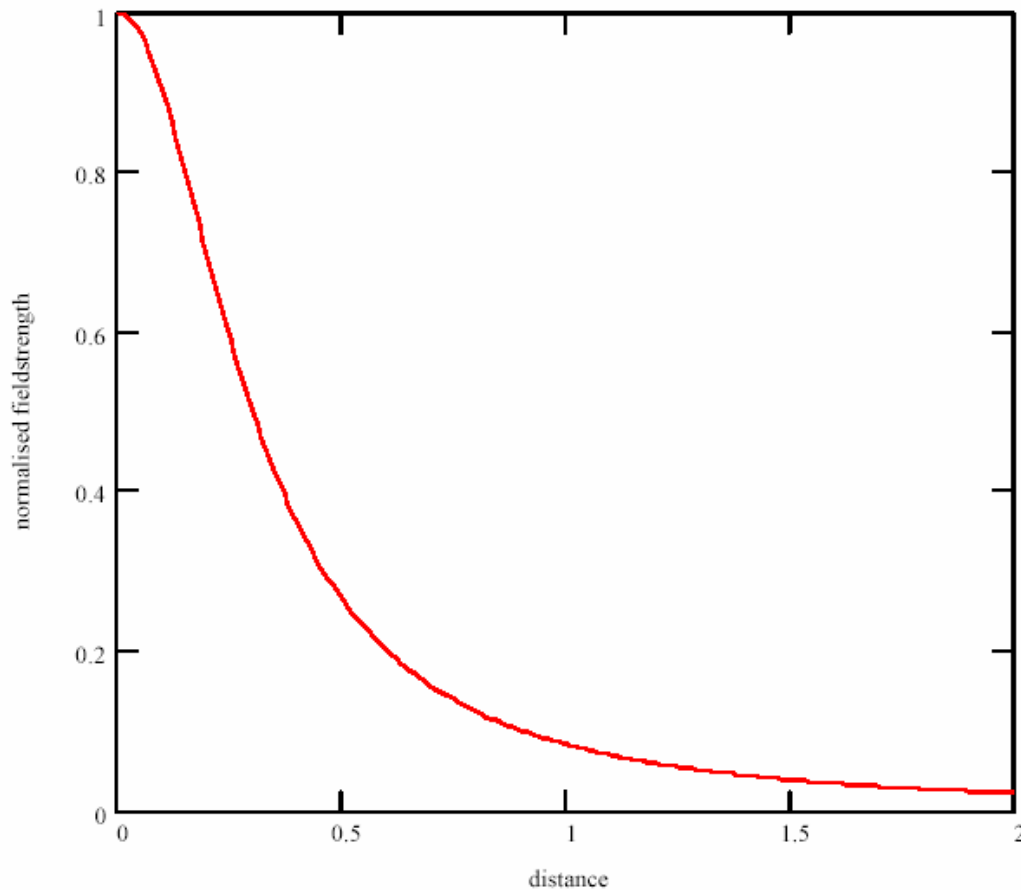


Figura 2.26. Comportamiento de la intensidad de campo en función de la distancia.

A diferencia que en los sistemas de RFID que usan frecuencias dentro del rango de UHF o microondas, la radiación emitida a 13.56MHz no es absorbida por el agua ni la piel humana, lo que permite que las ondas se propaguen con mayor facilidad puesto que la influencia del agua o las personas en su comportamiento es insignificante.

Debido a los efectos de blindaje o reflexión, los sistemas de RFID son sensibles a los metales dentro del campo de operación. Esto afecta a todos los sistemas de identificación por radiofrecuencia, aunque los motivos físicos son diferentes para cada caso concreto.

El hecho del que el campo magnético sea un campo vectorial implica que la orientación del tag tiene influencia dentro del mismo. Esta influencia de la orientación puede resolverse mediante el uso de antenas de transmisión más complejas (por ejemplo, mediante el uso de campos rotantes). Así es posible trabajar con las etiquetas independientemente de su orientación dentro de la zona de operación.

Debido también a que los sistemas RFID inductivos operan a distancias cortas, la influencia de sistemas adyacentes o ruidos externos es mucho menos que en sistemas que trabajan en la zona UHF o microondas (debido a que la potencia decrece con el cuadrado de la distancia, cuando a 13.56MHz decrece con la sexta potencia de la distancia).



## Etiquetas típicas

Hoy en día las etiquetas a 13.56MHz están disponibles en muchas formas y con diferentes funcionalidades. Por supuesto esto ha sido muy influenciado por las aplicaciones y sus requerimientos. El hecho de que unas pocas vueltas de la antena de la etiqueta (habitualmente menos de 10) sean suficientes para lograr una etiqueta con un buen funcionamiento es uno de los beneficios reconocidos para permitir la producción de tags a bajo coste basados en diferentes tecnologías de antena.

## Formas

Hay tres tipos principales de tags a 13.56MHz:

- Tarjetas ISO:
  - o ISO 14443: son “Tarjetas de identificación- Proximity integrated circuit cards”. Con un rango entre 7-15 cm, usadas principalmente en el campo de la expedición de tickets.
  - o ISO15693: son “Tarjetas de identificación- contactless integrated circuit cards”. Con un rango superior a 1 m, usadas principalmente en los sistemas de control de acceso.
- Tags rígidos industriales para logística
- Etiquetas inteligentes, delgadas y flexibles.

## Funcionalidad

- Tamaño de la memoria: típicamente desde 64 bits (en dispositivos simples de identificación) hasta varios kilobytes (empleados en tarjetas inteligentes).
- Tipo de memoria: programadas de fábrica, de sólo lectura (típicamente en identificación y pequeña memoria), sólo programables una vez (OTP) y de lectura/escritura (permitiendo la modificación de datos).
- Seguridad: básicamente todos los niveles de seguridad se pueden alcanzar. En el caso, por ejemplo, de aplicaciones en las que haya una transferencia de dinero se requieren los niveles más altos de seguridad.
- Capacidades multitag: resueltas y soportadas por la mayoría de los nuevos productos.

## Tipos de lector

Sin lugar a dudas la etiqueta tiene una gran importancia dentro de un sistema RFID, sin embargo el lector tiene la misma importancia dentro de un sistema RFID de índole profesional. La parte principal del interrogador es un módulo de radiofrecuencia encargado de la comunicación entre él y el tag. Hay diferentes dispositivos según la

potencia de salida y según la sensibilidad del mismo. Podemos encontrar tres tipos principales:

- Módulo RF para aplicaciones de “proximidad” (hasta 100mm). Se emplean en dispositivos portátiles, impresoras y terminales. Esta funcionalidad se puede integrar en un circuito impreso, permitiendo módulos de reducido tamaño y reducción de costes.
- Módulo de RF para aplicaciones de “vecindad” (amplio rango, en el caso de 13.56MHz hasta 1.5m). Son más complejos que los módulos de “proximidad”, tienen un mayor consumo de potencia y una circuitería más compleja.
- También se puede encontrar en ocasiones una tercera clase, de “medio rango” para distancias de hasta 400mm.

Los interrogadores fijos suelen colocarse a lo largo de las líneas de producción para identificar y hacer el seguimiento de los objetos. En algunas aplicaciones es necesario blindar los interrogadores para protegerlos de perturbaciones externas. Los lectores con forma de puerta se emplean en almacenes, establecimientos y bibliotecas para EAS (Electronic Article Surveillance).

También existen interrogadores que emplean múltiples antenas que permiten extender el rango de cobertura y leer los tags en cualquier orientación. Existe la posibilidad de emplear protocolos anticolidión que permiten la lectura de múltiples tags simultáneamente dentro del campo de la antena. Dependiendo del protocolo y la configuración empleada pueden leerse hasta 30 tags por segundo, lo que equivale a leer los tags colocados uno detrás de otro separados una distancia de 0.1m y desplazándose a 3m/s.

### ***Funcionamiento***

Que el sistema funcione es una de las principales cuestiones dentro de los requerimientos de las aplicaciones. Así la meta es cumplir con el propósito de tener un sistema con un funcionamiento bueno dentro de una probabilidad elevada. Mientras que las cuestiones funcionales como el tamaño de la memoria o nivel de seguridad pueden ser seleccionadas teniendo en cuenta los requerimientos de las aplicaciones, algunos otros parámetros clave (rango, fiabilidad y velocidad de la comunicación) están sujetos a leyes físicas y, por lo tanto, muestran cierta independencia. Típicamente las distancias más pequeñas permiten velocidades mayores (los sistemas de “proximidad” operan aproximadamente a 100kBaud o más), mientras que distancias mayores sólo se pueden lograr con velocidades más lentas (entre 25 y 70kBaud).

Esto tiene un impacto en la integración y la optimización del sistema. Sin embargo, existe la evidencia de que los sistemas RFID a 13.56MHz pueden alcanzar aproximadamente 1.5m sin problemas en aplicaciones “puerta” o cubrir una “ventana” de 1x1m en un “lector túnel” y solucionan los requisitos clave de las aplicaciones en términos de tamaño de datos y movilidad de objetos. Estas ideas están basadas en tags del tamaño de una tarjeta de crédito.

El funcionamiento no está tan sólo fijado por las regulaciones y por la velocidad de transmisión sino que también depende de la sensibilidad o robustez que tiene al ruido. Debido a que la señal del transponder puede ser transmitida por una subportadora que opera fuera de la (ruidosa) banda ISM, el funcionamiento del sistema puede ser muy estable comparado, por ejemplo, con los sistemas a  $<135\text{kHz}$ . La robustez al ruido puede ser realizada por receptores selectivos y por el hecho de que ambas subportadoras pueden ser procesadas independientemente en sistemas de alto rendimiento.

Esto da una idea de la “ventana de funcionamiento” de los sistemas que trabajan a  $13.56\text{MHz}$ . Evidentemente, el funcionamiento final depende de muchos factores que deben ser optimizados para cada aplicación concreta.

### 2.10.2 Sistemas RFID en la banda UHF: de 400 a 1000MHz.

#### Principios de Operación

Los sistemas de RFID que operan en el rango de frecuencias de UHF emplean la propagación convencional de una onda electromagnética para la comunicación y alimentación de tags no alimentados por batería. Este funcionamiento difiere del de los sistemas a bajas frecuencias que usan la inducción electromagnética, más similar a los transformadores.

El lector emite una onda electromagnética que se propaga con un frente de onda esférico. Las etiquetas colocadas dentro del campo recogen parte de la energía de la onda emitida. La cantidad de energía disponible en un punto está relacionada con la distancia que hay desde el punto emisor y decrece con la segunda potencia de la misma (es decir, que  $E$  es proporcional a  $1/d^2$ ).

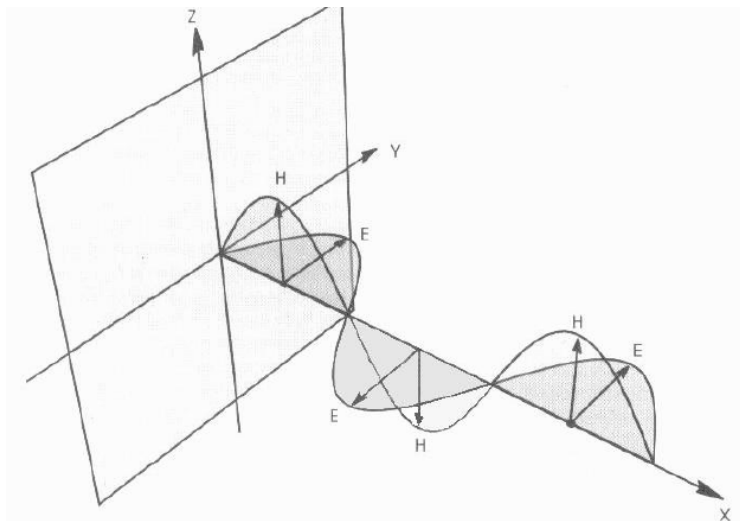


Figura 2.27- Propagación de una onda electromagnética. E y H son perpendiculares y están en fase la una con la otra.

La densidad de potencia que reciben los tags no depende directamente de la frecuencia, sino que depende del tamaño de la antena. De todos modos, el tamaño de la antena sí que depende de la frecuencia, por lo que podemos afirmar que,

indirectamente, la densidad de potencia recibida por las etiquetas, sí que depende de la frecuencia.

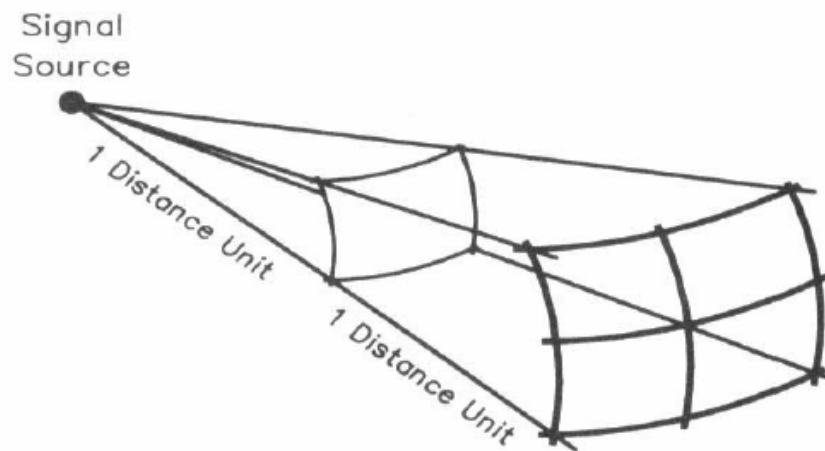


Figura 2.28 Reducción de la potencia por unidad de área recibida en función de la distancia.

La cantidad de energía recibida es función de la apertura de la antena receptora, lo que en términos simples es lo mismo que decir que depende de la longitud de onda de la señal recibida. Consideremos, por ejemplo, una antena de media de longitud de onda para 300MHz (0.5 m) y de 0.25m a 600MHz. El área activa alrededor de la antena tiene la forma de una elipse.

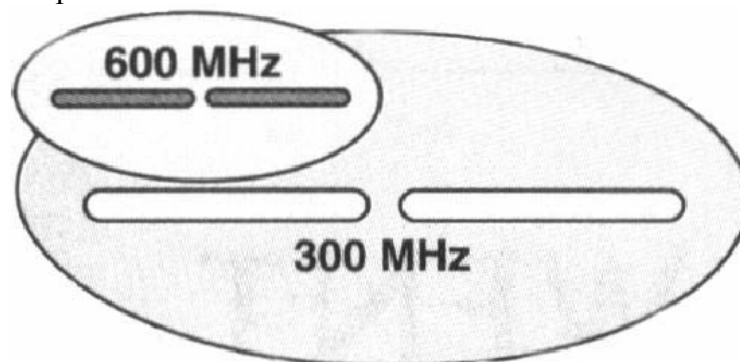


Figura 2.29 Área activa para antenas de 300 y 600MHz.

Como se observa en la Figura2.29, el área de la elipse de la antena a 300MHz es cuatro veces la de la antena a 600MHz. De esta forma el área de captación de energía a 300MHz es cuatro veces la de 600MHz.

La antena receptora puede ser físicamente más pequeña y, aún así, tener la misma apertura ya que existen compensaciones para reducir el tamaño de la antena como reducir el ancho de banda o un ajuste más fino. En la práctica, el rango de trabajo depende de la energía que radia el lector, de la frecuencia de trabajo y del tamaño de la antena de la etiqueta.

Para que la tecnología RFID pasiva sea correctamente explotada el lector debe producir un adecuado campo magnético para alimentar las etiquetas a una distancia

que sea útil. Atendiendo a las regulaciones actuales, que son más restrictivas en Europa, la potencia radiada está limitada a 500mW, lo que se traduce en un rango de lectura de unos 0.7m a 870MHz. En EEUU y Canadá se permite una potencia radiada de 4W, lo que se traduce en un rango del orden de 2m. Existen licencias especiales en Estados Unidos que permiten una potencia que supera los 5m.

## Funcionamiento

Cuando se realiza una transmisión en RF, hay diversos factores que pueden influir en el correcto funcionamiento de la comunicación entre emisor y receptor.

## Absorción, Reflexión, refracción y difracción

Una onda electromagnética puede verse afectada por alguno de estos cuatro factores, esto puede provocar que la comunicación no se realiza correctamente. Por tanto el estudio de estos factores y de cómo afectan cada uno a las características de las ondas electromagnéticas es estudiado en cada caso.

Por ejemplo, la absorción depende de las características del material a través del cual la onda se propaga. La absorción de energía se produce debido a que parte de esta energía se disipa en el material que opone una resistencia al paso de la onda.

Las ondas electromagnéticas son afectadas también por el fenómeno de refracción y difracción, cuando estas ondas pasan por diferentes medios o cuando inciden en el borde de un objeto. Las transmisiones a frecuencias más elevadas son más propensas a este tipo de fenómenos.

Las ondas electromagnéticas se pueden reflejar en una superficie conductora como un metal, agua, hormigón, etc. La reflexión puede provocar que la transmisión se anule completamente, pero también puede beneficiarla. Todo dependerá de cómo se encuentran la onda reflejada y la onda directa, en fase o contratase. Podemos apreciarlo en la Figura 2.30

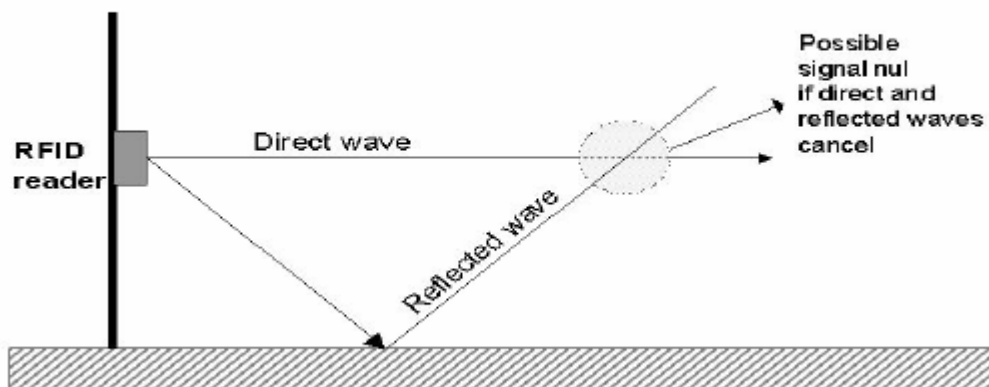


Figura 2.30 Esquema de la propagación de una onda electromagnética y su onda reflejada.

## **Penetración en líquidos**

Las ondas de radio penetran en diferentes líquidos dependiendo de la conductividad eléctrica del líquido en el cual penetran. Por ejemplo, el agua tiene una alta conductividad eléctrica y, por tanto, tiende a reflejar y absorber energía electromagnética mientras que el aceite o el petróleo tienen una baja conductividad permitiendo el paso a través de ellos con unos niveles relativamente bajos de atenuación.

## **Rango de lectura**

El rango de lectura depende de la potencia de transmisión y, en el caso de los tags pasivos, también los requerimientos de energía de los mismos. El rango efectivo de lectura depende también del factor de absorción del material al cual va unido el tag.

El tamaño del tag también juega un papel importante en el rango de lectura. Cuanto menor es el tag, menor es el área de captura de energía, por lo que menor es el rango de lectura. Un diseño adecuado del sistema, la optimización de la potencia del lector, la orientación de la antena y una colocación óptima del tag ayudan a superar estas limitaciones.

## **Interferencias**

El ruido eléctrico procedente de motores, luces fluorescentes, etc., es mínimo en UHF. De mayor consideración es el efecto de otros sistemas RFID, teléfonos móviles, aparatos que trabajen en la banda ISM, etc. Aunque la mayoría de estas fuentes de señal emiten en una banda muy estrecha.

FHSS (Frequency hopping spread spectrum) es una de las formas más efectivas de reducir los efectos de las interferencias y de reducir las interferencias sobre otros dispositivos que comparten el espectro. De este modo la energía transmitida se distribuye a lo largo de la banda de frecuencias, reduciendo las posibles interferencias creadas a otros sistemas y, así, como la frecuencia del receptor está continuamente cambiando, evita los efectos de otros usuarios bloqueando el receptor.

## **Capacidad de lectura direccional**

La naturaleza de las ondas de UHF permite el uso de pequeñas antenas direccionales. Esto permite dirigir el rayo del interrogador hacia un área en particular y poder leer selectivamente un grupo de tags y evitar la lectura de otros. Esta capacidad de direccionalidad tiene otra ventaja, que es la de permitir que el interrogador evite zonas con posibilidad de interferencias.

## **Orientación de la etiqueta**

La orientación de la antena de la etiqueta con respecto a la antena del interrogador influye en el rango de lectura. Cuando la onda electromagnética está polarizada linealmente, la antena del tag debe estar orientada en la misma dirección que

la del interrogador para permitir la máxima recepción de energía. La situación de peor caso se da cuando la orientación entre ambas antenas forma un ángulo recto. Si la onda electromagnética no está polarizada linealmente no importa la orientación que tenga la antena de la etiqueta. Por ejemplo, si empleamos una onda electromagnética polarizada circularmente podemos emplear cualquier orientación para el tag.

### ***2.10.3 Sistemas RFID a 2450 MHz.***

#### **Principios de operación**

Los sistemas RFID en el rango de las microondas se vienen usando desde hace más de 10 años en aplicaciones de transporte (seguimiento de vehículos por vías o raíles, peajes y otro tipo de control de acceso a vehículos). Los sistemas que operan en la banda UHF y en la región de microondas se dividen en “activamente alimentados” y “pasivamente alimentados”. El rango de operación y la funcionalidad son superiores en los tags activos (con una batería en el tag) mientras que un bajo coste y un mayor tiempo de uso son las ventajas de los tags pasivos.

En el pasado las etiquetas para microondas eran bastante complejas y caras debido al desafío de procesar señales de microondas con circuitos integrados CMOS. Actualmente, la mayoría de estos dispositivos para seguimiento de artículos usan un único circuito integrado y alimentación pasiva. Esto conlleva ventajas en cuando a coste y tiempo de vida.

El principio básico de operación a 2450MHz consiste en la transmisión de datos y energía usando la propagación de señales de radio. Una antena en el interrogador genera una onda electromagnética que es recibida en la antena del tag. En un tag pasivo se convierte esta señal recibida en un voltaje DC para alimentarse. La transmisión de datos desde el lector hacia un tag se lleva a cabo cambiando algún parámetro de la onda transmitida (amplitud, fase o frecuencia).

La transmisión de retorno desde el tag hacia el interrogador se lleva a cabo cambiando la carga de la antena del tag (amplitud y/o fase). En este contexto, los sistemas que trabajan por debajo de 135KHz, a 13.56MHz y en microondas usan el mismo principio. Para los sistemas RFID de microondas este método se llama “modulated backscatter”. De forma alternativa, se puede generar otra señal de diferente frecuencia y modularla para transmitirla al interrogador. Los sistemas que usan este último método emplean tags transmisores RF activos.

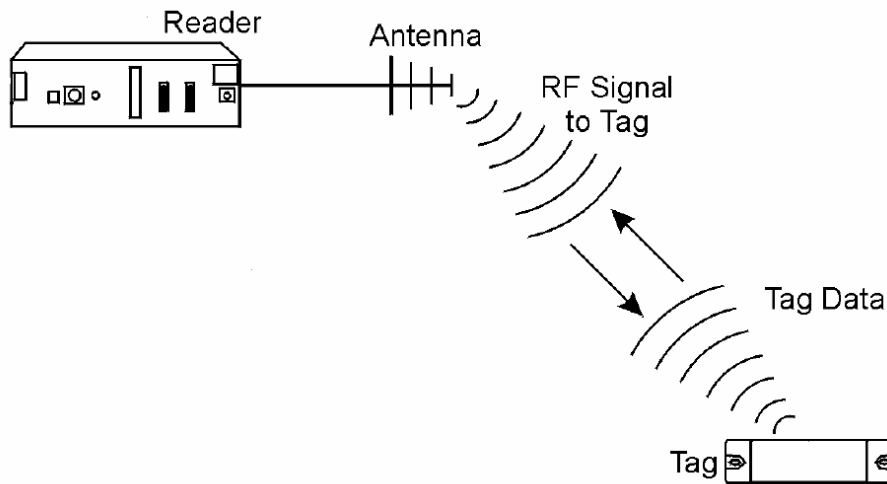


Figura 2.31 Principio básico de los sistemas RFID que trabajan con microondas.

A diferencia de los sistemas RFID inductivos (13.56MHz y <135KHz), los sistemas de UHF y microondas operan en el “campo lejano” de la antena de transmisión del interrogador. Las distancias alcanzables para tags pasivos están entre los 0.5 y los 12m y más allá de los 30m para los tags activos, dependiendo de la frecuencia de microondas, las regulaciones del país o región donde trabaja y las características de la antena. Como los tags operan en el “campo lejano” de la antena del interrogador, la intensidad de este campo decrece con la primera potencia de la distancia (es decir, E es proporcional a  $1/d$ ).

Las ondas en UHF y microondas se atenúan y reflejan en materiales que contienen agua o tejidos humanos y se reflejan en objetos metálicos. Al contrario que en los sistemas RFID inductivos, es posible diseñar tags que trabajen unidos a objetos metálicos. También atraviesan fácilmente madera, papel, ropa, pintura, suciedad, etc. Adicionalmente, debido a la corta longitud de onda de las señales de radio empleadas y a las propiedades de reflexión de los objetos metálicos, los sistemas lectores se pueden diseñar para tener una alta capacidad de lectura en zonas con gran contenido en objetos metálicos. Como el campo eléctrico es un campo vectorial, existe una relación entre la orientación del tag y la distancia de lectura. El impacto de esta dependencia de la orientación se puede solucionar mediante el empleo de antenas más complejas sin que influya así la orientación de la etiqueta.

### Etiquetas típicas

En la actualidad los tags de 2450MHz están disponibles en muy diferentes formatos en cuanto a forma y funcionalidad. A diferencia de los sistemas RFID inductivos, los cuales requieren bastante área o bastantes vueltas de cable o incluso un núcleo magnético para recoger el campo magnético, los tags de UHF y los de microondas pueden ser muy pequeños requiriendo sólo una determinada longitud en una sola dimensión. Por eso los tags son más fáciles de encapsular. Tamaños típicos son de 2 a 10 cm.



## **Forma**

Hay dos clases de tags para los 2450MHz:

- Tags industriales rígidos para usos logísticos.
- Etiquetas finas y flexibles.

Las expectativas son que en el futuro se empleen muchos más tipos diferentes de etiquetas. Esta es una ventaja de los tags de 2450MHz, que se pueden conseguir una gran variedad de formas y tamaños.

## **Funcionalidad**

El tamaño de la memoria (como en todas las frecuencias) está limitado sólo por el coste. Es posible conseguir una gran oblea con una capacidad del orden de Kb, pero el coste se incrementa de acuerdo con ello. Las memorias típicas suelen estar entre los 64 bits (aplicaciones simples para identificación) y algunos Kb (empleadas en aplicaciones logísticas con gran cantidad de datos).

En cuanto a la seguridad, se pueden conseguir todos los niveles de seguridad deseados (desde niveles bajos para una simple tarea de control hasta los más elevados para tareas de transferencias económicas, por ejemplo).

## **Funcionamiento**

Hay que tener en cuenta que si hablamos de sistemas activos, las velocidades de transmisión no dependen en gran medida de si empleamos UHF o microondas, mientras que para tags pasivos, los bajos requisitos de consumo para el mismo exigen unas velocidades de transmisión bajas. Los sistemas de amplio rango de lectura (distancias mayores a 15m) operan a velocidades de hasta 1Mbit/s. Los tags pasivos de UHF y microondas operan típicamente a velocidades entre 10 y 50Kbits/s.

## 2.11 Principios físicos de los sistemas RFID

La inmensa mayoría de los sistemas RFID operan de acuerdo con el principio de acoplamiento inductivo, por tanto comprender los procedimientos de transferencia de datos y alimentación requiere un conocimiento detallado de los principios físicos del magnetismo. Los campos electromagnéticos son usados por los sistemas que operan a frecuencias por encima de los 30 MHz. Para ayudar a entender estos sistemas hay que estudiar la propagación de las ondas en campos lejanos y los principios de la tecnología de los radares.

Los campos eléctricos tienen un rol secundario y sólo son explotados para la transmisión de datos en los sistemas “close coupling”.

### 2.11.1 Campo magnético

#### El campo magnético $\vec{H}$

Cada movimiento de carga se asocia con un campo magnético. La presencia de los campos magnéticos se demuestra, por ejemplo, en la creación de una corriente eléctrica secundaria. El campo magnético depende de las cargas que lo crean, del punto donde se estudia, y del medio donde se crea el campo. Pero experimentalmente se descubrió que existe una magnitud que no depende del medio donde se cree, esta magnitud del campo magnético se define como intensidad del campo magnético  $H$ . Se puede ver en (2.2) y (2.3) la relación con el campo magnético  $\vec{B}$ , como es la relación entre el campo magnético y la corriente que circula, por ejemplo, por un conductor.

$$\vec{H} = \frac{\vec{B}}{\mu} \quad (2.2)$$

$$\sum I = \oint \vec{H} \cdot d\vec{s} \quad (2.3)$$

Podemos usar (2.2) para calcular el campo magnético para diferentes tipos de conductores, como los de la Figura 2.32.

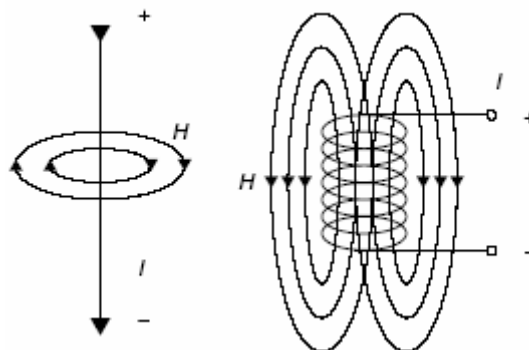


Figura 2.32 Líneas de flujo magnético alrededor de un hilo conductor y de una bobina.

En las tablas 2.6 y 2.7 podemos ver las constantes usadas en los cálculos de campos magnéticos, las unidades y abreviaturas.

Constant	Symbol	Value and unit
Electric field constant	$\epsilon_0$	$8.85 \times 10^{-12}$ As/Vm
Magnetic field constant	$\mu_0$	$1.257 \times 10^{-6}$ Vs/Am
Speed of light	$c$	299 792 km/s
Boltzmann constant	$k$	$1.380 662 \times 10^{-23}$ J/K

Tabla 2.6 Constantes

Variable	Symbol	Unit	Abbreviation
Magnetic field strength	$H$	Ampere per meter	A/m
Magnetic flux ( $n$ = number of windings)	$\Phi$	Volt seconds	Vs
Magnetic inductance	$\Psi = n\Phi$ $B$	Volt seconds per meter squared	Vs/m <sup>2</sup>
Inductance	$L$	Henry	H
Mutual inductance	$M$	Henry	H
Electric field strength	$E$	Volts per metre	V/m
Electric current	$I$	Ampere	A
Electric voltage	$U$	Volt	V
Capacitance	$C$	Farad	F
Frequency	$f$	Hertz	Hz
Angular frequency	$\omega = 2\pi f$	1/seconds	1/s
Length	$l$	Metre	m
Area	$A$	Metre squared	m <sup>2</sup>
Speed	$v$	Metres per second	m/s
Impedance	$Z$	Ohm	$\Omega$
Wavelength	$\lambda$	Metre	m
Power	$P$	Watt	W
Power density	$S$	Watts per metre squared	W/m <sup>2</sup>

Tabla 2.7 Unidades y abreviaturas

El campo magnético se representa mediante líneas de fuerza, trazadas de modo que en cada uno de sus puntos el vector  $\vec{B}$  es tangente.

### Campo magnético H en espiras

Un aspecto importante para los diseños en la trayectoria que forma campo magnético (H) creado por una corriente que atraviesa unas espiras (conductor loop), también llamadas “short cylindrical coils”. Estas espiras son usadas como antenas generadoras de un campo magnético en diseños de sistemas RFID con acoplamiento inductivo. Podemos ver en la Figura 2.33 las líneas de campo magnético en conductores cilíndricos.

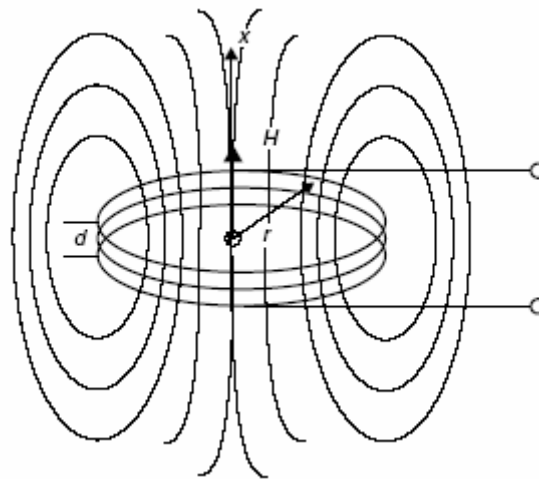


Figura 2.33 Las líneas de flujo magnético que alrededor de los conductores en espira son similares a las empleadas en las antenas transmisoras de los sistemas RFID de acoplamiento inductivo.

El campo magnético H decrece con la distancia en el eje x. También se sabe que el campo H en relación con el radio de la espira r, permanece constante a una cierta distancia, y comienza a decrecer rápidamente. La Figura 2.34 permite visualizar gráficamente estas relaciones.

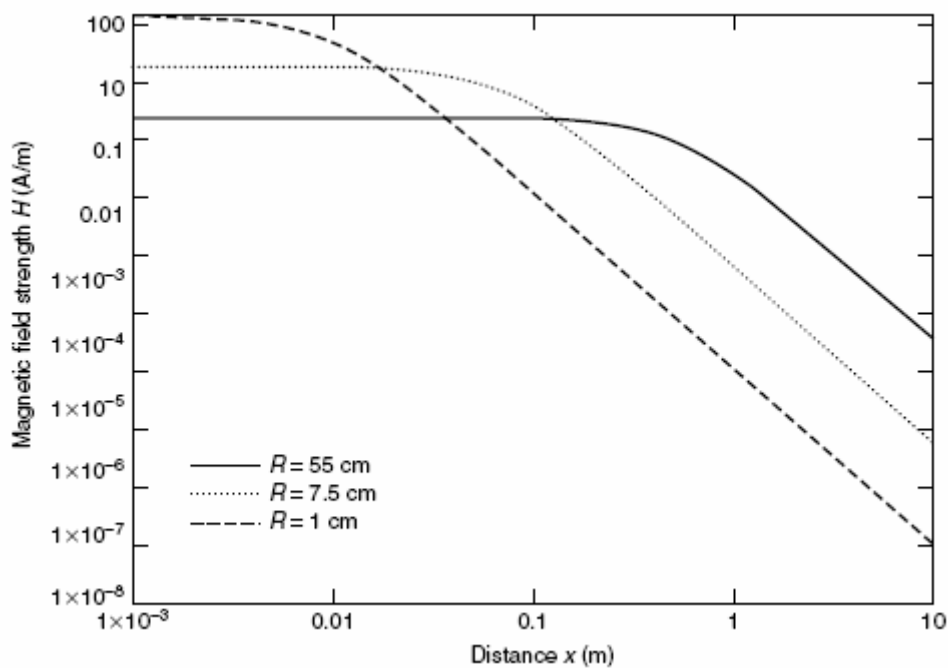


Figura 2.34 Intensidad del campo magnético H en relación con la distancia del centro de las espiras (eje x) y el radio de las espiras.

Para calcular el valor de H en el eje x usamos (2.4).

$$H = \frac{I \cdot N \cdot R^2}{2\sqrt{(R^2 + x^2)^3}} \tag{2.4}$$

Donde  $N$  es el número de espiras,  $R$  es el radio de la espira y  $x$  la distancia desde el centro de la espira, en la dirección del eje  $x$ . Para estas ecuaciones se toman como aproximaciones  $d \ll R$  y  $x \ll \lambda/2\pi$ .

Por otro lado tenemos que en centro de la espira, es decir, con  $x=0$ :

$$H = \frac{I \cdot N}{2R} \quad (2.5)$$

En general, para lo que nos afecta al diseño de antenas transmisoras de RFID, hemos de saber cuanto más grande es el radio de la espira que forman la antena, en los sistemas con acoplamiento inductivo, más fuerte es el campo magnético en distancias mayores que el radio, y en cambio cuando el radio es pequeño más fuerte es el campo en distancias menores al radio.

Por estos motivos, a la hora de diseñar un sistema RFID debemos elegir un diámetro de antena óptimo. Si elegimos un radio demasiado grande, si es cierto que tendremos un mayor alcance, pero el campo magnético cerca del centro de la espira ( $x=0$ ) será muy débil, y por el contrario si elegimos un radio demasiado pequeño, nos encontraremos con un campo magnético que decrece en proporción de  $x^3$ .

Por tanto el radio óptimo de la antena de transmisión debe ser el doble del máximo alcance de lectura deseado.

En la práctica, aplicando estas teorías a los sistemas RFID, para conocer el alcance máximo de un lector, hay que saber también las características del campo magnético mínimo a recibir del transponder a leer. Si la antena seleccionada tiene un radio muy grande, entonces se corre el peligro que el campo magnético  $H$  pueda ser insuficiente para alimentar a los transponders que se encuentren más cerca de la antena del lector.

### Flujo magnético y densidad del flujo magnético

El número total de líneas de campo magnético que pasan a través de una espira circular se conoce como flujo magnético  $\Phi$ , definido en un área  $A$  y con una densidad de flujo magnético  $B$  como podemos ver en la Figura 2.35. La fórmula (2.6) representa esta relación.

$$\Phi = B \cdot A \quad (2.6)$$

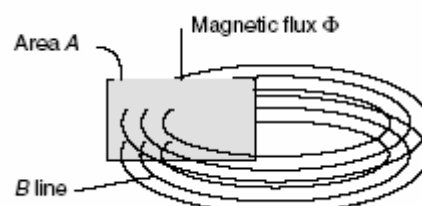


Figura 2.35 Relación entre el flujo magnético  $\Phi$  y la densidad de flujo  $B$ .

La relación entre el campo magnético  $\vec{B}$  y el campo magnético  $H$  se expresa según (2.7)

$$B = \mu_0 \mu_r H = \mu H \quad (2.7)$$

Donde la constante  $\mu_0$  describe la conductividad magnética o permeabilidad en el vacío. La variable  $\mu_r$  es la permeabilidad relativa e indica cuanto de grande o cuanto de pequeña es que  $\mu_0$  dependiendo del material.

### Inductancia L

Cualquier circuito es atravesado por un flujo creado por el mismo y que debe ser proporcional a la intensidad que lo recorre como vemos en (2.8). El flujo es particularmente elevado si el conductor tiene forma de espira. Normalmente hay más de una espira,  $N$  espiras en la misma área  $A$ , a través de las cuales circula la misma corriente. Cada espira contribuye con la misma proporción  $\Phi$  al flujo total  $\Psi$ , podemos ver la relación en (2.8).

$$\Psi = \sum_N \Phi_N = N \cdot \Phi = N \cdot \mu \cdot H \cdot A \quad (2.8)$$

Definimos como inductancia  $L$ , la relación entre el flujo total y la corriente que atraviesa el conductor.

$$L = \frac{\Psi}{I} = \frac{N \cdot \Phi}{I} = \frac{N \cdot \mu \cdot H \cdot A}{I} \quad (2.9)$$

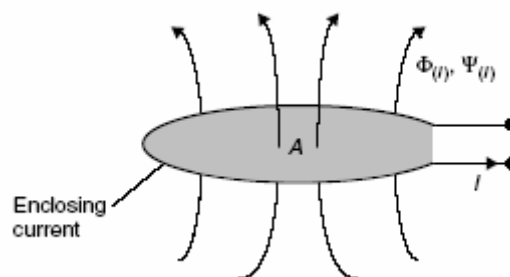


Figura 2.36 Definición de Inductancia L

La inductancia es una de las características variables de este tipo de conductores. La inductancia de los conductores en espira depende totalmente de las propiedades del material (permeabilidad) que la atraviesa el flujo del campo magnético y de la geometría del layout.

Si suponemos que el diámetro  $d$  del conductor usado es muy pequeño comparado con el diámetro  $D$  de la espira del conductor ( $d/D < 0.0001$ ), podemos realizar la aproximación (2.10):

$$L = N^2 \mu_0 R \cdot \ln \left( \frac{2R}{d} \right) \quad (2.10)$$

Dónde  $R$  es el radio de la espira del conductor y  $d$  el diámetro del conductor usado.

## Inductancia Mutua M

La inductancia mutua se produce por la proximidad de dos conductores en forma de espira. La corriente que atraviesa una de las espiras induce un flujo magnético en el otro y al inverso. La magnitud del flujo inducido depende de las dimensiones geométricas de ambos conductores, la posición de un conductor respecto al otro y las propiedades magnéticas del medio. Para dos conductores de áreas  $A_1$  y  $A_2$ , e  $I_1$  la corriente que circula por la primera espira vemos:

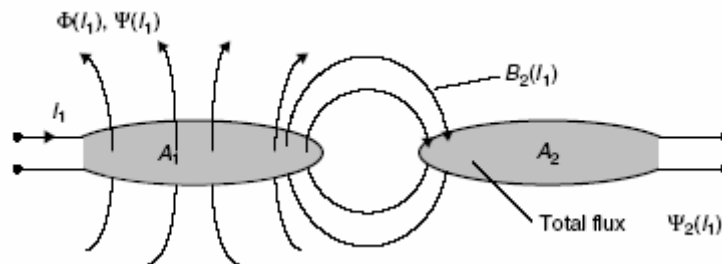
$$M_{21} = \frac{\Psi_{21}(I_1)}{I_1} = \oint_{A_2} \frac{B_2(I_1)}{I_1} \cdot dA_2 \quad (2.11)$$

Por definición tenemos que la inductancia mutua es igual:

$$M = M_{12} = M_{21} \quad (2.12)$$

La inductancia mutua siempre esta presente entre dos circuitos electrónicos, en este principio físico es en el que se basa el acoplamiento inductivo de los sistemas RFID.

En la Figura 2.37 podemos ver la definición de inductancia mutua por dos espiras.



En la Figura 2.37 podemos ver la definición de inductancia mutua por dos espiras.

Si aplicamos (2.13) a dos espiras:

$$M_{12} = \frac{\mu_0 \cdot N_1 \cdot R_1^2 \cdot N_2 \cdot R_2^2 \cdot \pi}{2\sqrt{(R_1^2 + x^2)^3}} \quad M_{12} = \frac{B_2(I_1) \cdot N_2 \cdot A_2}{I_1} = \frac{\mu_0 \cdot H(I_1) \cdot N_2 \cdot A_2}{I_1} \quad (2.13)$$

## Coefficiente de acoplamiento k

Si la inductancia mutua describía cualitativamente el flujo creado por la corriente que circula por otra espira, el coeficiente de acoplamiento realiza una predicción cualitativa de la inducción creada entre dos espiras independientemente de las dimensiones geométricas de los conductores.

$$k = \frac{M}{\sqrt{L_1 \cdot L_2}} \quad (2.14)$$

Tenemos que  $0 \leq k \leq 1$ , por lo que en los casos extremos:

$k=0$ : No hay acoplamiento debido a la gran distancia no hay acción del campo magnético.

$k=1$ : Acoplamiento total. Las dos espiras están sometidas al mismo  $\Phi$ . El transformador es la aplicación técnica con total acoplamiento.

### Ley de Faraday

Los circuitos en los que se inducen las corrientes tienen una determinada resistencia. Para que en un circuito resistivo circule una corriente eléctrica es necesario que exista en él una fuerza electromotriz. Si un circuito está sometido a variaciones de flujo magnético, existe en él una fuerza electromotriz que estará relacionada con la variación de flujo magnético.

El efecto del campo eléctrico generado depende de las propiedades del material donde se provoca.

La ley de Faraday en general se escribe a (2.15)

$$u_i = \oint E_1 \cdot ds = - \frac{d\Psi(t)}{dt} \quad (2.15)$$

Para comprender el acoplamiento inductivo en los sistemas RFID debemos considerar el efecto de la inductancia en el acoplamiento magnético en bobinas.

Una corriente variante en el tiempo  $i_1(t)$  en una espira  $L_1$ , genera un flujo magnético variante en el tiempo  $\frac{d\phi(t)}{dt}$ . Por tanto, un voltaje es inducido en las espiras  $L_1$  y  $L_2$ . Como ya hemos comentado anteriormente, podemos diferenciar entre que el voltaje inducido sea en el mismo conductor del circuito, o que el voltaje inducido sea en el conductor adyacente.

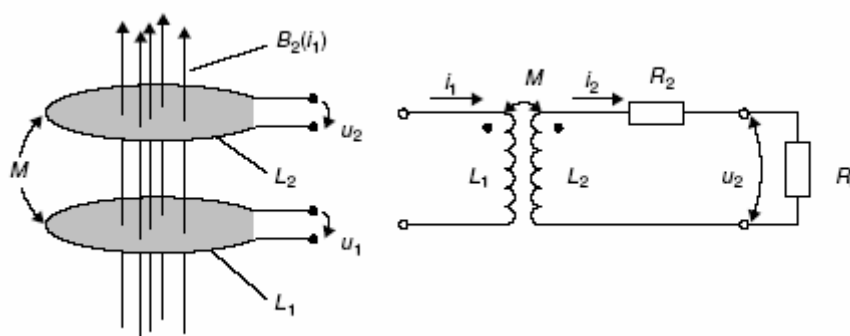


Figura 2.38 Representación y circuito equivalente del acoplamiento magnético inductivo.

En un sistema RFID con acoplamiento inductivo  $L_1$  representaría la antena del lector y  $L_2$  la antena del transponder. La corriente consumida es representada por el resistor de carga  $R_L$ . Un flujo variante en el tiempo produce un voltaje  $u_{21}$  en el conductor  $L_2$  debido a la inductancia mutua  $M$ . La corriente que circula crea un voltaje



adicional, este voltaje se puede medir en los terminales de  $R_L$ . La corriente que atraviesa  $L_2$  genera un flujo magnético  $\Psi_1$  ( $i_1$ ). Podemos ver el voltaje en (2.16).

$$u_2 = + \frac{d\Psi_2}{dt} = M \frac{di_1}{dt} - L_2 \frac{di_2}{dt} - i_2 R_2 \quad (2.16)$$

## Resonancia

El voltaje inducido  $u_2$  en la antena del transponder es usado como alimentación necesaria para el chip en su proceso de almacenamiento de datos en memoria. Para mejorar la eficiencia un capacitador  $C_2$  se conecta en paralelo con la bobina del transponder  $L_2$ , como vemos en la Figura 2.39, de manera que forma un circuito paralelo resonante con una frecuencia resonante que es la frecuencia de operación del sistema de RFID. La frecuencia resonante se puede calcular en (2.17).

$$f = \frac{1}{2\pi\sqrt{L_2 \cdot C_2}} \quad (2.17)$$

En la práctica existe un capacitador parásito en paralelo  $C_p$  por lo que el valor del capacitador sería  $C'_2$ , como vemos en (2.18).

$$C'_2 = \frac{1}{(2\pi f)^2 L_2} - C_p \quad (2.18)$$

En la Figura 2.39 podemos ver el circuito equivalente de un transponder real, donde  $R_2$  es la resistencia natural de la bobina del transponder  $L_2$  y el consumo de corriente del chip viene dado por la resistencia de carga  $R_L$ .

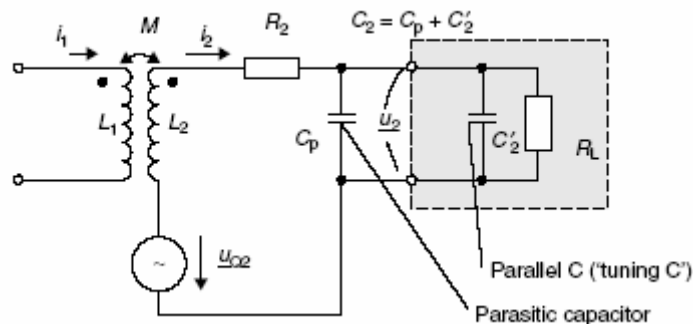


Figura 2.39 Diagrama del circuito equivalente para el acoplamiento magnético de dos bobinas. La bobina  $L_2$  y el condensador en paralelo  $C_2$  forman el circuito resonante.

Cuando la frecuencia de operación es igual a la frecuencia de resonancia del circuito tenemos el mayor voltaje en la resistencia  $R_L$ .

Se introduce el factor  $Q$  para comprobar como influyen los componentes del circuito  $R_L$ ,  $R_2$  y  $L_2$  en el voltaje  $u_2$ . El factor  $Q$  es sencillo de calcular, (2.19), en este caso  $\omega$  es la frecuencia angular, y es igual a  $2\pi f$  en el circuito resonante.

$$Q = \frac{1}{R_2 \cdot \sqrt{\frac{C_2}{L_2}} + \frac{1}{R_L} \cdot \sqrt{\frac{L_2}{C_2}}} = \frac{1}{\frac{R_2}{\omega L_2} + \frac{\omega L_2}{R_L}} \quad (2.19)$$

El voltaje  $u_2$  es proporcional a la calidad del circuito resonante, lo que quiere decir que depende de  $R_2$  y  $R_L$ . Por tanto a la hora de diseñar el transponder tendremos en cuenta estos parámetros y escogerlos para optimizar el rango de alcance del sistema.

### Funcionamiento práctico de los transponders

Ya hemos tratado el tema de la alimentación en los transponders, por lo que teníamos transponders activos que incorporaban su propia batería que era la encargada de alimentar el chip en su proceso de lectura/escritura; mientras que los transponder pasivos eran únicamente alimentados con el voltaje  $u_2$ , comentado anteriormente.

El voltaje inducido  $u_2$  en la antena del transponder alcanza rápidamente valores elevados. Este voltaje hay que regularlo, para ello, independientemente de los valores del coeficiente de acoplamiento  $k$  o de otros parámetros, se utiliza el resistor  $R_S$  conectado en paralelo con la resistencia de carga  $R_L$ . Podemos ver el circuito equivalente en la Figura 2.40.

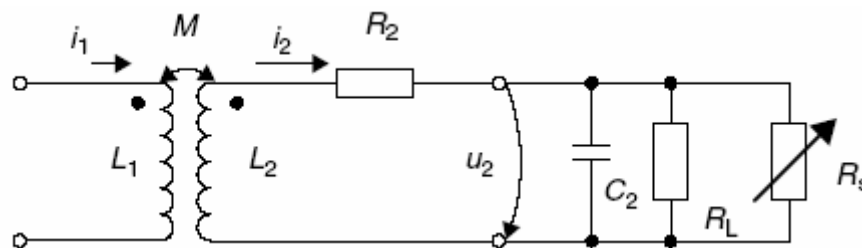


Figura 2.40 Regulador del voltaje en el transponder.

La tensión incrementa en medida que el valor de  $R_S$  disminuye.

En el proceso de funcionamiento del transponder tenemos el valor del campo de interrogación del transponder,  $H_{\min}$ . Es la mínima intensidad de campo (a la máxima distancia entre transponder y reader) a la cual el voltaje inducido  $u_2$  es justo el suficiente para realizar las operaciones del chip.

Para el cálculo de  $H_{\min}$  tenemos (2.20), donde  $N$  es el número de espiras de la bobina  $L_2$ , y  $A$  es la sección de la bobina.

$$H_{\min} = \frac{u_2 \cdot \sqrt{\left(\frac{\omega L_2}{R_L} + \omega R_2 C_2\right)^2 + \left(1 - \omega^2 L_2 C_2 + \frac{R_2}{R_L}\right)^2}}{\omega \cdot \mu_0 \cdot A \cdot N} \quad (2.20)$$

En (2.20) vemos que el campo de interrogación depende de la frecuencia por medio del factor  $\omega=2\pi f$  y del área  $A$  de la antena, del número de espiras  $N$  de la bobina, del mínimo voltaje  $u_2$  y de la resistencia de entrada  $R_2$ . Por eso cuando la frecuencia de transmisión del lector corresponde con la frecuencia de resonancia del transponder, el campo de interrogación mínimo  $H_{\min}$  tiene su valor mínimo.

Para optimizar la sensibilidad de un sistema RFID con acoplamiento inductivo, la frecuencia de resonancia del transponder debe ser precisamente la frecuencia de resonancia del lector. Desafortunadamente esto no es siempre posible en la práctica. Primero en la fabricación del transponder puede haber tolerancias, las cuales pueden provocar una desviación en la frecuencia de resonancia. Segundo, por razones técnicas a la hora de configurar la frecuencia de resonancia del transponder hay procedimientos que pueden diferenciarla de la frecuencia de transmisión del lector (por ejemplo en sistemas que usan procedimientos de anticollisión para que dos transponders no se estorben a la hora de comunicar datos).

En la ecuación (2.21) la frecuencia de resonancia es calculada como el producto de  $L_2C_2$ .

$$L_2C_2 = \frac{1}{(2\pi f_0)^2} = \frac{1}{\omega_0^2} \quad (2.21)$$

Si lo sustituimos en (2.22) encontramos la dependencia de  $H_{\min}$  con la frecuencia del lector ( $\omega$ ) y la frecuencia de resonancia del transponder ( $\omega_0$ ). Se basa en el supuesto que la variación en la frecuencia de resonancia del transponder esta causada por la variación de  $C_2$ .

$$H_{\min} = \frac{u_2 \cdot \sqrt{\omega^2 \left( \frac{L_2}{R_L} + \frac{R_2}{\omega_0^2 L_2} \right)^2 + \left( \frac{\omega_0^2 - \omega^2}{\omega_0^2} + \frac{R_2}{R_L} \right)^2}}{\omega \mu_0 \cdot A \cdot N} \quad (2.22)$$

Si se conoce  $H_{\min}$ , entonces se puede conocer el rango de energía asociado a ese rango de alcance del lector. El rango de energía del transponder es la distancia desde la antena del lector a la cual la energía para que opere el transponder es justo la suficiente (definido como  $u_2$  en  $R_L$ ), lo vemos en (2.23). El resultado de la pregunta de si el rango de energía es el igual al máximo alcance funcional que tiene el sistema depende de si la transmisión de datos desde el transponder puede ser detectado por el lector a esa distancia en cuestión.

$$x = \sqrt{\sqrt[3]{\left( \frac{I \cdot N_1 \cdot R^2}{2 \cdot H_{\min}} \right)^2} - R^2} \quad (2.23)$$

En (2.23) tenemos  $I$  como la corriente que circula por la antena,  $R$  el radio de las espiras y el número de espiras de la antena transmisora como  $N$ .

Se puede decir que cuando incrementa el consumo de corriente, una  $R_L$  más pequeña, la sensibilidad del lector se incrementa, por lo que el rango de energía decrece.

Durante todas las explicaciones hemos considerado un campo  $H$  homogéneo paralelo al eje de la bobina  $x$ . Por ejemplo la tensión inducida por un campo magnético en un ángulo  $\theta$  viene dada (2.24).

$$u_{0\theta} = u_0 \cdot \cos(\theta) \quad (2.24)$$

Donde  $u_0$  es el voltaje inducido cuando la espira es perpendicular al campo magnético, mientras que cuando el ángulo formado es de  $90^\circ$  no hay voltaje inducido en la espira. Podemos ver un ejemplo en la Figura 2.41 de las diferentes zonas alrededor de los lectores. Por eso, los transponders orientados en el eje  $x$  de la bobina obtienen un rango de lectura óptimo.

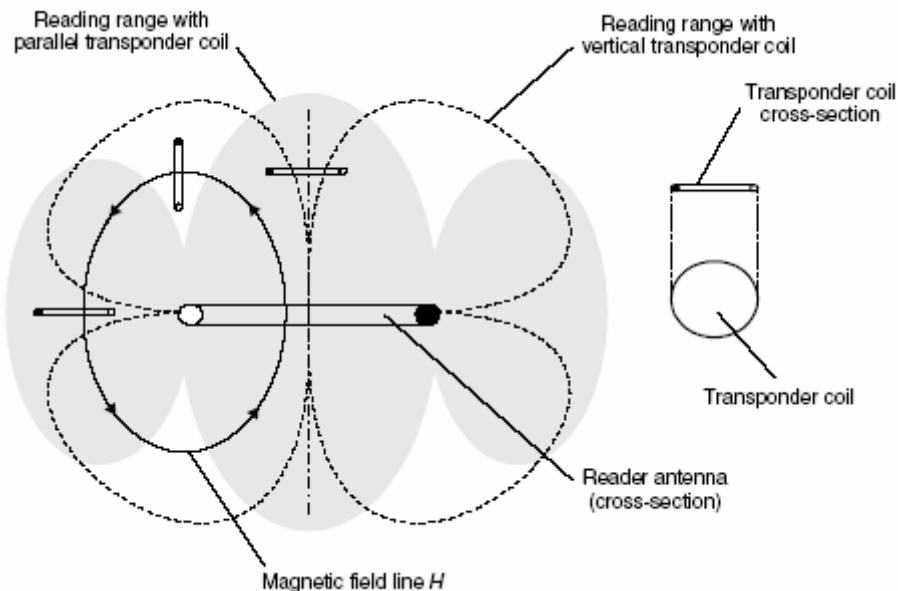


Figura 2.41 Zonas de interrogación del lector para diferentes alineamientos del transponder.

### Sistema transponder-reader

En este punto consideraremos las características de los sistemas con acoplamiento inductivo desde el punto de vista del transponder.

En la Figura 2.42 podemos ver el diagrama del circuito de un lector. La bobina necesaria para generar el campo magnético  $L_1$ . El resistor en serie  $R_1$  corresponde con las pérdidas resistivas de las espiras de la bobina. Para obtener la máxima corriente en la bobina a la frecuencia de operación del reader  $f_{TX}$ , se crea el circuito resonante en serie con la frecuencia de resonancia  $f_{RES} = f_{TX}$ , con la conexión en serie del capacitor  $C_1$ . Se calcula con (2.25).

$$f_{TX} = f_{RES} = \frac{1}{2\pi\sqrt{L_1 \cdot C_1}} \quad (2.25)$$

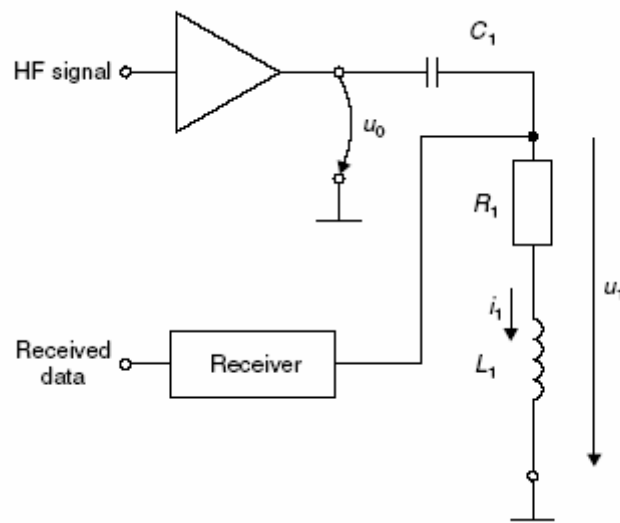


Figura 2.42 Diagrama del circuito equivalente de un lector RFID.

### 2.11.2 ONDAS ELECTROMAGNÉTICAS

Como ya hemos visto una variación del campo magnético induce un campo eléctrico con líneas de campo cerradas.

Como el campo magnético propaga un campo eléctrico, éste originalmente puramente magnético se va transformando en un campo electromagnético. Además a la distancia de  $\lambda/2\pi$  el campo electromagnético comienza a separarse de la antena y comienza a desplazarse por el espacio en forma de onda electromagnética, podemos ver como se crea una onda electromagnética en la Figura 2.43.

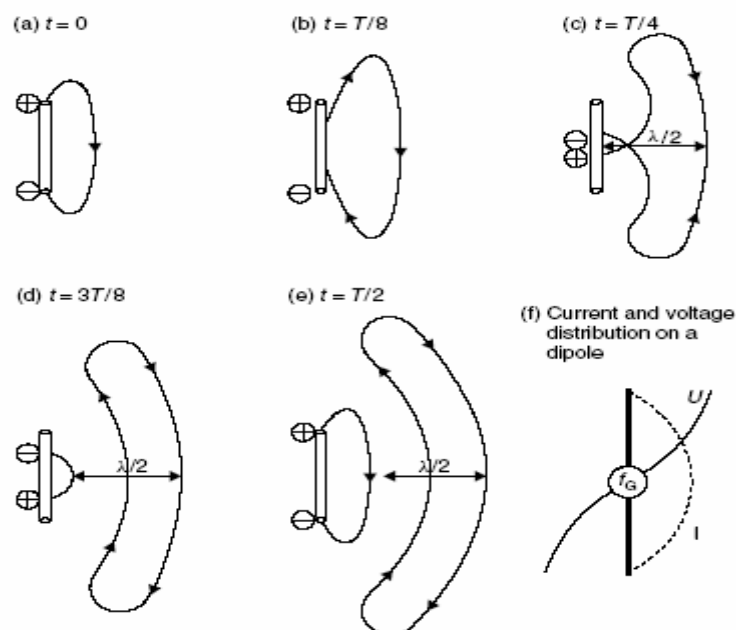


Figura 2.43 Creación de una onda electromagnética en un dipolo. El campo magnético forma un anillo alrededor de la antena.

El área desde la antena hasta el punto donde se forma la antena se conoce como “near field” de la antena, y el área a partir del punto donde se forma completamente la onda electromagnética se conoce como “far field”.

Esto permite que el alcance de los sistemas por ondas electromagnéticas sea mayor que el producido por acoplamiento inductivo o capacitivo, que suelen representar su rango límite al principio del “far field”.

En la Figura 2.44 podemos observar como en el “near field” el campo magnético decrece en función de  $1/d^3$  mientras que en el “far field” sólo decrece en función de  $1/d$ .

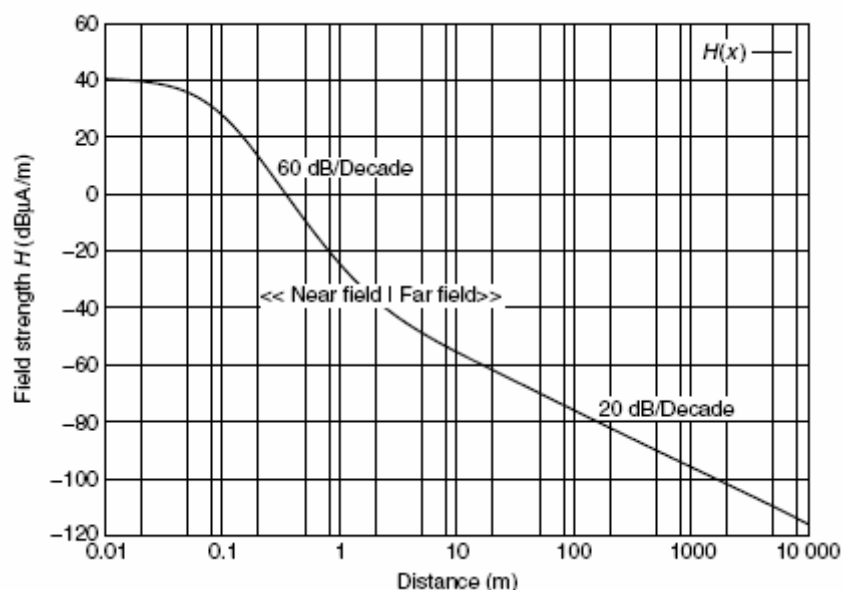


Figura 2.44 Gráfico de la intensidad de campo magnético en la transición de near y far field a la frecuencia de 13,56 MHz.

## Densidad de Radiación

Una onda electromagnética se desplaza en el espacio esféricamente desde su punto de creación. Al mismo tiempo, las ondas electromagnéticas transportan energía. A medida que nos alejamos de la fuente de radiación, la energía es dividida en el área de la superficie esférica que forma que se va incrementando. Aquí se introduce el término de densidad de radiación  $S$ .

En un emisor esférico, llamado isotrópico, la energía es radiada uniformemente en todas las direcciones. A la distancia  $r$  la densidad de radiación  $S$  puede calcularse fácilmente en (2.26) como el cociente de la energía emitida  $P_{\text{EIRP}}$  (transmisor isotrópico) por el emisor y el área de la superficie de la esfera.

$$S = \frac{P_{\text{EIRP}}}{4\pi r^2} \quad (2.26)$$

La energía transportada por las ondas electromagnéticas se almacena en los campos eléctrico y magnético de la onda. La relación entre los campos  $E$  y  $H$  y la densidad de radiación lo vemos en (2.27).

$$S = E \times H \quad (2.27)$$

En el vacío podemos aproximar la relación entre E y H como vemos en (2.28).

$$E = H \cdot \sqrt{\mu_0 \epsilon_0} = H \cdot Z_F \quad (2.28)$$

Donde  $Z_f$  es la impedancia característica de la onda e igual a  $120\pi \Omega$ .

$$E = \sqrt{S \cdot Z_F} \quad (2.29)$$

En la Figura 2.45 vemos el vector S como producto de E y H.

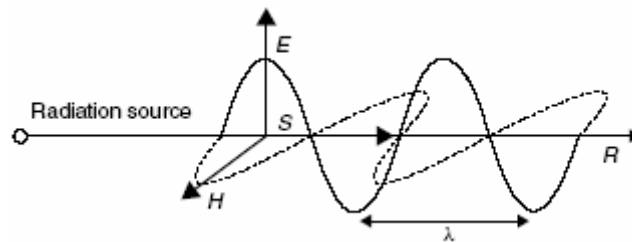


Figura 2.45 Vector S

## Polarización

La polarización de una onda electromagnética se determina por la dirección del campo eléctrico de la onda. En la Figura 2.46 podemos diferenciar entre los diferentes tipos de polarizaciones.

Diferenciamos primero entre polarización lineal, donde también se diferencia entre polarización vertical y horizontal. Las líneas de campo eléctrico se desplazan en paralelo o perpendicular a la superficie terrestre. La transmisión de energía entre dos antenas linealmente polarizadas es máximo cuando las dos antenas están polarizadas en la misma dirección, y mínima cuando forman un ángulo de  $90^\circ$  o  $270^\circ$ .

En los sistemas RFID no se puede conocer cual será la orientación entre la antena del transponder y la del lector. El problema es solucionado por el uso de la polarización circular del lector de la antena. El principio de generación de polarización circular se ve en la Figura 2.46, dos dipolos son unidos en forma de cruz. De esta forma el campo electromagnético generado rota  $360^\circ$  cada vez que se mueve el frente de onda una longitud de onda. Se diferencia por el sentido de giro del frente de onda izquierdas o derecha.

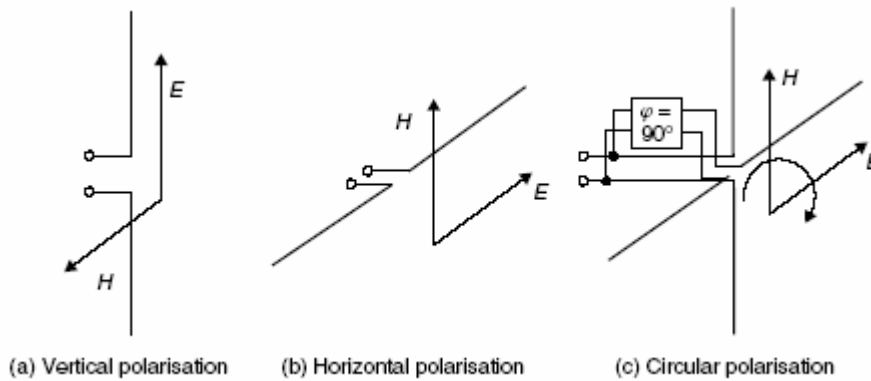


Figura 2.46 Definición de la polarización de ondas electromagnéticas.

### Reflexión en ondas electromagnéticas

Una pequeña parte de la energía reflejada en objetos es devuelta a la antena transmisora. Es la tecnología en que se basa el radar para calcular la distancia y posición del objeto. En los sistemas de RFID la reflexión de las ondas electromagnéticas (sistema backscatter) es usada para la transmisión del transponder al lector. Las propiedades de la reflexión se hacen más notorias cuando se incrementa la frecuencia. La potencia de la onda reflejada decrece en proporción a  $r^2$ .

Los sistemas backscatters emplean antenas con diferentes áreas de reflexión, llamado cross-section, que depende de varios factores como son el tamaño del objeto, el material, la estructura de la superficie, la longitud de onda ( $\lambda$ ) y la polarización.

### Antenas

La elección de la antena es uno de los principales parámetros de diseño de un sistema RFID.

Definimos  $P_{\text{EIRP}}$  como la potencia emitida por un emisor isotrópico, y la podemos obtener en (2.30).

$$P_{\text{EIRP}} = \int_{A_{\text{sphere}}} S \cdot dA \quad (2.30)$$

Aunque una antena real difiere de una isotrópica en que no radia uniformemente en todas las direcciones. Incluimos el término de ganancia ( $G_i$ ) para una antena como la dirección de máxima radiación, indicando el factor por el cual la densidad de radiación es mayor que la de un emisor isotrópico con la misma potencia de transmisión. Si  $P_1$  es la potencia emitida por la antena. Así definimos también en (2.31)  $P_{\text{EIRP}}$ . Vemos estos factores en la Figura 2.47.

$$P_{\text{EIRP}} = P_1 \cdot G_i \quad (2.31)$$



Un emisor isotrópico tiene una ganancia igual a 1.

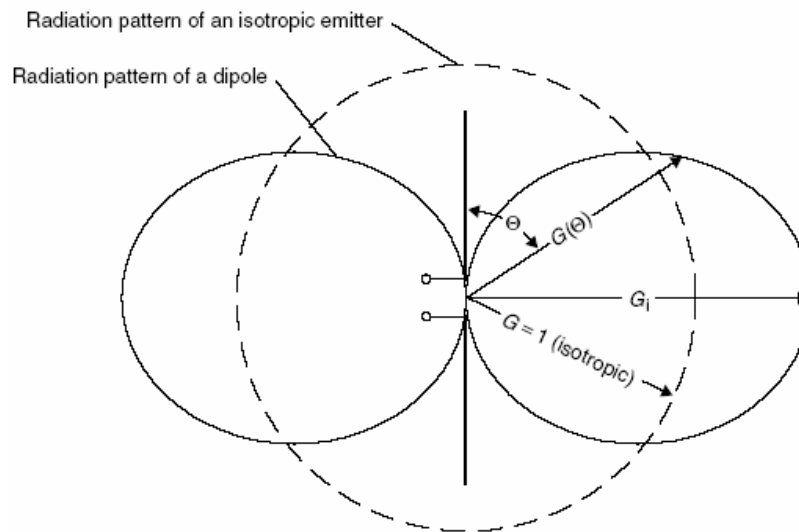


Figura 2.47 Comparación entre la radiación de un dipolo y un emisor isotrópico.

Podemos diferenciar entre EIRP o ERP, mientras EIRP como comentábamos es la potencia emitida por una antena isotrópica, EIR es la emitida por un antena dipolo. Y están relacionadas por (2.32).

$$P_{EIRP} = P_{ERP} \cdot 1.64 \tag{2.32}$$

Si nos centramos en el tipo de antenas de dipolos, las utilizadas en nuestro diseño, vemos que consiste en una sola línea de cobre. La antena más utilizada el dipolo  $\lambda/2$ , consiste en una línea de longitud  $l = \lambda/2$ , la cual está cortada a mitad, que es por donde se alimenta. Vemos en la tabla 2.8 las principales características de los dipolos  $\lambda/2$ .

Parameter	Gain $G$	Effective aperture	Effective length	Apex angle
$\lambda/2$ dipole	1.64	$0.13 \lambda^2$	$0.32 \lambda$	$78^\circ$
$\lambda/2$ 2-wire folded dipole	1.64	$0.13 \lambda^2$	$0.64 \lambda$	$78^\circ$

Tabla 2.8 Propiedades eléctricas del dipolo y el doble dipolo  $\lambda/2$ .

### Funcionamiento práctico de los transponders de microondas

Nos centramos en el funcionamiento del transponder cuando se encuentra en el rango de alcance del lector. La Figura 2.48 muestra el modelo simplificado de un sistema backscatter. El lector emite una onda electromagnética con una potencia efectiva de  $P_1 \cdot G_1$  y el transponder recibe una potencia proporcional  $P_2$  al campo  $E$  y a la distancia  $r$ . La potencia  $P_s$  es la reflejada por la antena del transponder y la potencia  $P_3$  es recibida por el lector a una distancia  $r$ .

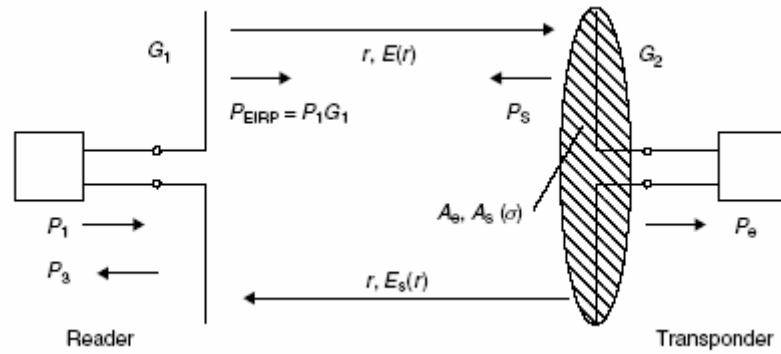


Figura 2.48 Modelo de sistema RFID por microondas cuando el transponder está en la zona de interrogación del lector.

### Sensibilidad del transponder

A pesar del tipo de alimentación que tenga el transponder, activa o pasiva, un mínimo campo eléctrico es necesario para activar el transponder o alimentar con suficiente energía para que opere el circuito. La mínima intensidad de campo  $E_{\min}$  se calcula fácilmente (2.33).

$$E_{\min} = \sqrt{\frac{4\pi \cdot Z_F \cdot P_{e-\min}}{\lambda_0^2 \cdot G}} \quad (2.33)$$

En esta ecuación tenemos a  $Z_F$  como impedancia de entrada y la  $P_{e-\min}$  como la potencia mínima requerida. Esto está basado en el requisito que las direcciones de polarización de las antenas del lector y del transponder correspondan. De otro modo el  $E_{\min}$  incrementaría.

### Rango de lectura

Para la comunicación entre el lector y el transponder se deben cumplir dos condiciones. Primero el transponder debe estar suficientemente alimentado para su activación y la señal reflejada por el transponder debe ser lo suficientemente potente para que cuando la reciba el lector la pueda detectar sin errores.

En los lectores backscatter la permanente transmisión, la cual es requerida para activar el transponder, introduce un ruido significativo, que reduce la sensibilidad del receptor del lector. Se puede asumir en la práctica que para que el transponder sea detectado, la señal del transponder no debe ser inferior a 100 dB por debajo del nivel de transmisión del lector.

Para la transmisión de datos reflejados por el transponder se usan modulaciones. La potencia  $P_s$  reflejada se modula en una señal portadora y dos bandas laterales. La señal portadora no contiene información, pero es necesaria. En una modulación pura ASK las dos bandas laterales contienen el 25% del total de la potencia reflejada  $P_s$ . Podemos ver una representación de los niveles de estas bandas laterales en la Figura 2.49.

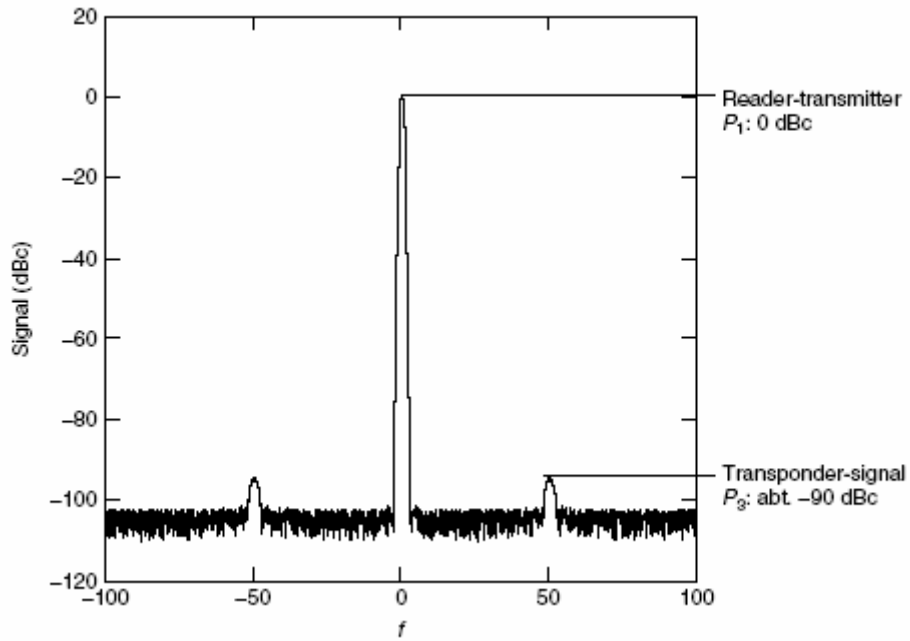


Figura 2.49 Niveles en el lector, podemos ver la señal propia del lector y las bandas laterales que provienen del transponder.

Podemos obtener la potencia de la onda que transmite el transponder al lector. (2.34).

$$P_3 = \frac{P_1 \cdot G_{\text{Reader}}^2 \cdot \lambda_0^4 \cdot G_{\text{T}}^2}{(4\pi r)^4} \quad (2.34)$$

El valor de la  $P_3$  representa la potencia total reflejada por el transponder.

## 2.12 Códigos y modulaciones

En el diagrama de bloques de la Figura 2.50 vemos descrito un sistema de comunicación digital. Similarmente, la transferencia de datos entre el lector y la etiqueta en un sistema RFID requiere 3 bloques básicos de funcionamiento.

Desde el lector hacia el tag (dirección de la transferencia de datos) son:

- En el lector (Transmitter): codificación de señal (signal processing) y el modulador (carrier circuit).
- El medio de transmisión (channel).
- En la etiqueta (Receiver): el demodulador (carrier circuit) y el decodificador de canal (signal processing).

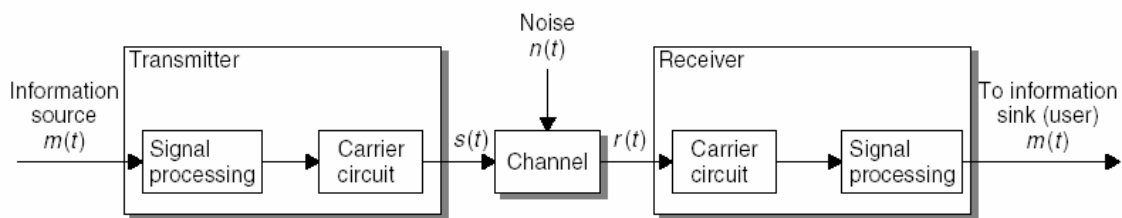


Figura 2.50 Bloques de funcionamiento de un sistema RFID.

Un sistema codificador de señal toma el mensaje a transmitir y su representación en forma de señal y la adecua óptimamente a las características del canal de transmisión. Este proceso implica proveer al mensaje con un grado de protección contra interferencias o colisiones y contra modificaciones intencionadas de ciertas características de la señal.

### 2.12.1 Codificación en Banda Base.

Los signos binarios “1” y “0” pueden ser representados por varios códigos lineales. Los sistemas de RFID suelen usar una de las siguientes codificaciones: NRZ, Manchester, Unipolar RZ, DBP (“diferential bi-phase”), Miller o Codificación Pulso-Pausa (PPC).

#### Código NRZ (No Return to Zero):

Un ‘1’ binario es representado por una señal ‘alta’ y un ‘0’ binario es representado por una señal ‘baja’. La codificación NRZ se usa, al menos, exclusivamente con una modulación FSK o PSK.

#### Código Manchester:

Un ‘1’ binario es representado por una transición negativa en la mitad del periodo de bit y un ‘0’ binario es representado por una transición positiva. El código Manchester es, por lo tanto, también conocido como codificación de ‘parte-fase’ (split-phase coding).

El código Manchester es frecuentemente usado para la transmisión de datos desde el transponder al lector basados en una modulación con sub-portadora.

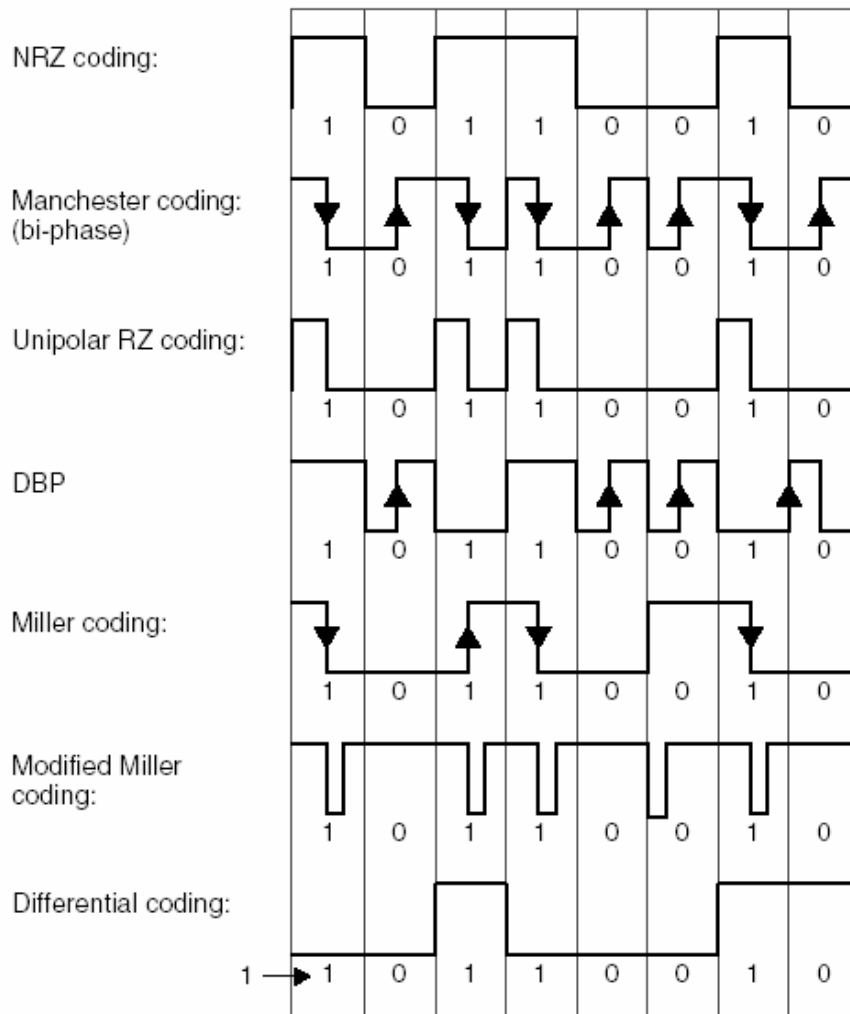


Figura 2.51 Representación gráfica de las principales codificaciones.

### Código Unipolar RZ:

Un '1' binario es representado por una señal 'alta' durante la primera mitad del periodo de bit, mientras que un '0' binario es representado por una señal 'baja' que dura todo el periodo de bit.

### Código DBP:

Un '0' binario es codificado por una transición, de cualquier tipo, en mitad del periodo de bit. Un '1' es codificado con una ausencia de transición. Además, el nivel de señal es invertido a inicio de cada periodo de bit, de modo que el pulso pueda ser más sencillamente reconstruido en el receptor si es necesario.

### Código Miller:

Un '1' es representado por una transición de cualquier tipo en la mitad del periodo de bit, mientras que el '0' binario es representado con la continuidad del nivel de la señal hasta el próximo periodo de bit. Una secuencia de ceros crea una transición al principio de cada periodo de bit, de modo que el pulso pueda ser más sencillamente reconstruido en el receptor si es necesario.

### Código Miller Modificado:

En esta variante del código Miller, cada transición es reemplazada por un pulso 'negativo'. El código Miller Modificado es altamente recomendable para transmitir del lector al tag en sistemas RFID que usan acoplamiento inductivo.

Debido a la tan corta duración del pulso ( $t_{\text{pulso}} \ll T_{\text{bit}}$ ) es posible asegurar una continua alimentación del transponder debido al campo magnético del lector mientras dura la transferencia de información.

### Codificación Diferencial:

En la codificación Diferencial cada '1' binario que se tiene que transmitir causa un cambio en el nivel de la señal, así como para un '0' el nivel permanece invariante. El código diferencial puede ser generado muy simplemente a partir de una señal NRZ usando una puerta XOR y un biestable D. En la siguiente figura vemos el circuito que logra este cambio en la señal.

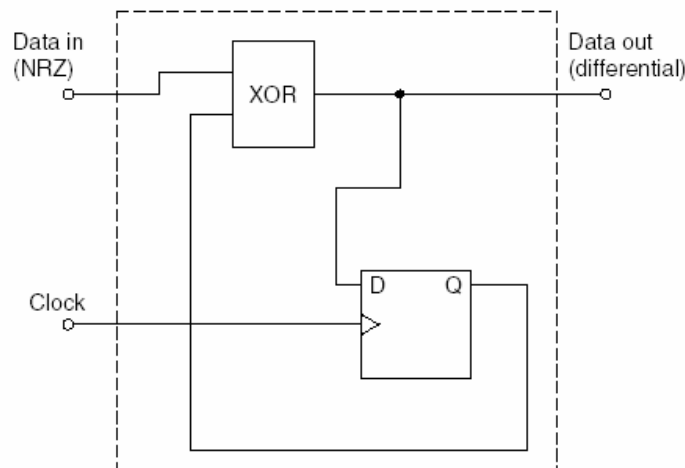


Figura 2.52 Generamos un código Diferencial a partir de uno NRZ.

### Codificación Pulso-Pausa:

En la codificación Pulso-Pausa (PPC – Pulse Pause Coding) un '1' binario es representado por una pausa de duración  $t$  antes del próximo pulso; un '0' binario es representado por una pausa de duración  $2t$  antes del próximo pulso. Este método de codificación es popular para la transmisión de datos del lector a la etiqueta en los sistemas de RFID que usan acoplamiento inductivo.

Debido a la tan corta duración del pulso ( $t_{\text{pulso}} \ll T_{\text{bit}}$ ) es posible asegurar una continua alimentación del transponder debido al campo magnético del lector mientras dura la transferencia de información.

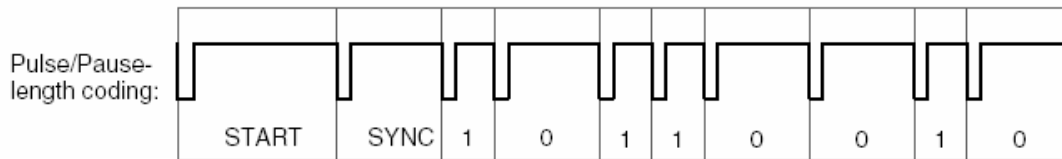


Figura 2.53 Posible transmisión de una señal usando PPC.

Debe tenerse en cuenta varias importantes consideraciones cuando se selecciona un posible sistema de codificación para un sistema RFID.

La consideración más importante es el espectro de la señal después de la modulación y lo susceptible que pueda ser a los posibles errores. Además, en el caso de tags pasivos (la alimentación de las etiquetas viene dada por el campo magnético que genera el lector), la fuente de alimentación (es decir, la señal que emite el lector) no debe ser interrumpida por una combinación inapropiada los métodos de codificación de señal y modulación.

### 2.12.2 Modulaciones Digitales usadas.

La tecnología clásica de radiofrecuencia está fuertemente implicada con los métodos analógicos de modulación. Podemos diferenciar entre modulación de amplitud (AM), modulación de frecuencia (FM) y modulación de fase (PM), siendo éstas las tres principales variables de una onda electromagnética. Todos los demás métodos de modulación son derivados de cualquiera de uno de estos tres tipos.

Las modulaciones usadas en RFID son ASK (amplitude shift keying), FSK (frequency shift keying) y PSK (phase shift keying).

#### 2.12.3. - ASK (Amplitude shift keying)

En Amplitude shift keying la amplitud de la oscilación de una portadora es variada entre dos estados  $u_0$  y  $u_1$  (keying) por un código de señal binario.  $U_1$  puede tomar dos valores entre  $u_0$  y 0. El intervalo entre  $u_0$  y  $u_1$  es conocido como el factor de trabajo (duty factor)  $m$ .

#### 2.12.4 2 FSK (Frequency shift keying)

En la modulación llamada '2 frequency shift keying' la frecuencia de la señal portadora se varía entre dos frecuencias  $f_1$  y  $f_2$ .

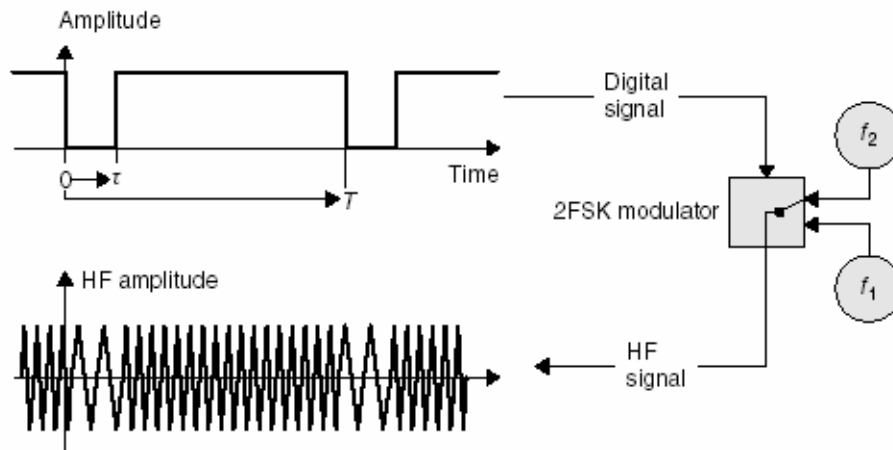


Figura 2.54 Generación de una 2FSK variando entre dos frecuencias  $f_1$  y  $f_2$  en tiempo, con una señal binaria.

La frecuencia portadora es la media aritmética de las dos frecuencias características  $f_1$  y  $f_2$ . La diferencia entre la frecuencia de la portadora y las frecuencias características es conocida como la desviación de frecuencia  $\Delta f_{CR}$ :

$$f_{CR} = \frac{f_1 + f_2}{2} \quad \Delta f_{CR} = \frac{|f_1 - f_2|}{2} \quad (2.35)$$

### 2.12.5. - 2 PSK (Phase shift keying)

En la modulación PSK los estados binarios '0' y '1' de una señal código se convierten en los respectivos "estados de fase" de la portadora, en relación a una fase de referencia. En el caso que nos ocupa, la 2 PSK, la fase de la señal varía entre los estados de fase de  $0^\circ$  y  $180^\circ$ .

### 2.12.6 Modulaciones que usan subportadora

En los sistemas de RFID, las modulaciones que usan subportadora son básicamente usadas cuando se trabaja con acoplamiento inductivo, normalmente en las frecuencias 6.78MHz, 13.56MHz o 27.125MHz en transferencias de información desde la etiqueta al lector.

Para modular la subportadora se puede elegir entre ASK, FSK o PSK.

Una vez tenemos esta primera señal modulada (subportadora modulada), entonces se procede a una segunda modulación de la subportadora con la señal portadora (la que nos dará la frecuencia final a la que transmitiremos nuestra señal).

El resultado de este proceso es una señal modulada con subportadora que transporta la información a una frecuencia 'menor', aunque la señal que lleva a la señal que contiene la información si que va a una frecuencia mayor.



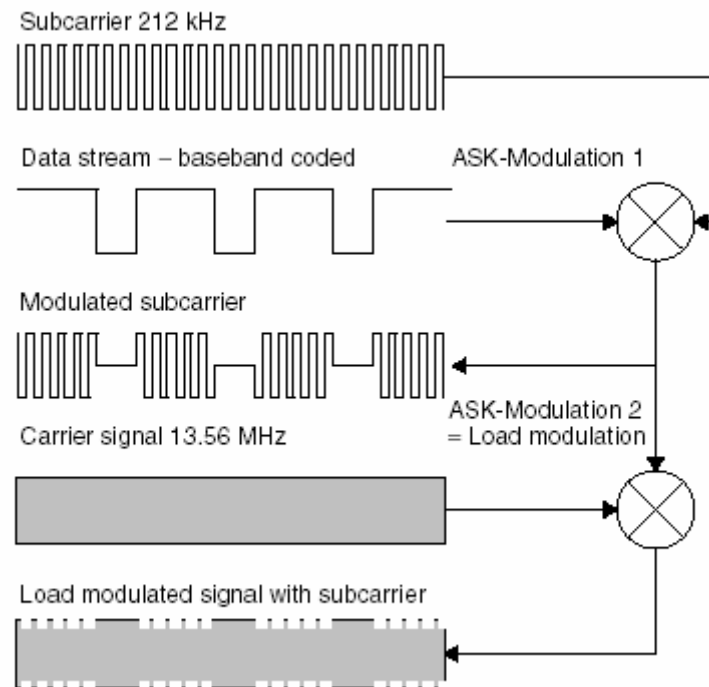


Figura 2.55 Proceso detallado de una modulación múltiple, con una subportadora modulada en ASK.

La auténtica ventaja de usar una modulación con subportadora sólo se aclara cuando consideramos el espectro de la señal generada. Esta modulación inicialmente genera dos líneas espectrales a una distancia de  $\pm$  la frecuencia de la subportadora  $f_H$  alrededor de la frecuencia central. La información se transmite, así, en las bandas laterales de las dos líneas subportadoras, dependiendo de la modulación de la subportadora generada a partir del código en banda base. Si la modulación usada es en banda base, las bandas laterales caerán justamente al lado de la señal portadora en la frecuencia central.

En las etiquetas que usan acoplamiento y que tienen unas pérdidas muy elevadas, la diferencia entre la señal portadora del lector  $f_T$  y las bandas laterales recibidas de la modulación varían en un rango de entre 80 y 90 dB.

Una de los dos productos de la modulación con subportadora puede ser filtrado y remodulado usando la frecuencia de la modulación de las bandas laterales del flujo de datos. Aquí es irrelevante si se usa la banda ‘alta’  $f_T + f_H$  o si se usa la banda ‘baja’  $f_T - f_H$  ya que la información está contenida en ambas.

### **2.13 Seguridad: encriptación de datos.**

Los sistemas de RFID se están usando cada vez más en aplicaciones de alta seguridad como son los sistemas de acceso o para realizar pagos y tickets de caja. Por eso mismo el uso de los sistemas de identificación por radiofrecuencia necesita del uso de sistemas de seguridad para protegerlos de ataques.

Los métodos de autenticación modernos funcionan como en la antigüedad: comprueban el conocimiento de un secreto para poder permitir una autenticación segura (por ejemplo conocer una clave criptográfica).

De todos modos se deben implementar algoritmos para prevenir que la clave secreta sea descubierta. Los sistemas de seguridad de los sistemas de RFID deben tener un modo de defensa contra los siguientes ataques individuales:

- La lectura no autorizada de la portadora de la información para poder conseguir una réplica y/o modificar los datos que lleva.
- Colocar una portadora de información extraña en la zona de influencia del interrogador con la intención de obtener un acceso no autorizado a un edificio o a una serie de servicios sin tener que pagarlos.
- Escuchar, sin ser advertido, en las comunicaciones radio y recolocar los datos imitando una portadora original ('respuesta y fraude').

Cuando se selecciona un sistema de RFID para su posterior implementación, debe tenerse en cuenta las medidas de seguridad que necesitan adoptarse dependiendo de su posterior funcionalidad. Así pues, un sistema que pretende una finalidad de automatización industrial o de reconocimiento de herramientas quizás no necesite añadir un coste adicional por medidas de seguridad que sí necesitarán sistemas de alta seguridad como pueden ser los sistemas de pago o de control de acceso a edificios. En el caso de los sistemas que necesitan seguridad, omitir un gasto en un proceso de criptología puede suponer un gasto posterior mucho más elevado si un intruso consigue acceso ilegal a servicios restringidos.

#### **2.13.1 Criptografía de clave secreta o simétrica**

Los criptosistemas de clave secreta se caracterizan porque la clave de cifrado y la de descifrado es la misma, por tanto la robustez del algoritmo recae en mantener el secreto de la misma.

Sus principales características son:

- Rápidos y fáciles de implementar
- Clave de cifrado y descifrado son la misma
- Cada par de usuarios tiene que tener una clave secreta compartida
- Una comunicación en la que intervengan múltiples usuarios requiere muchas claves secretas distintas

El cifrado de Verman verifica las condiciones de secreto perfecto definidas por Shannon, sin embargo presenta el inconveniente de que requiere un bit de clave por cada bit de texto claro. El hacer llegar tal cantidad de clave al emisor y receptor por un canal seguro desbordaría la propia capacidad del canal. Además requiere una clave aleatoria, y un ordenador genera claves pseudo aleatorias. La solución por tanto es la creación de claves de tamaño fijo y reducido.

Actualmente existen dos métodos de cifrado para criptografía de clave secreta, el *cifrado de flujo* y el *cifrado en bloques*.

### Cifrado de flujo

El emisor A, con una clave secreta y un algoritmo determinístico (RKG), genera una secuencia binaria ( $s$ ) cuyos elementos se suman módulo 2 con los correspondientes bits de texto claro  $m$ , dando lugar a los bits de texto cifrado  $c$ . Esta secuencia ( $c$ ) es la que se envía a través del canal. En recepción, B, con la misma clave y el mismo algoritmo determinístico, genera la misma secuencia cifrante ( $s$ ), que se suma modulo 2 con la secuencia cifrada ( $c$ ), dando lugar a los bits de texto claro  $m$ .

Los tamaños de las claves oscilan entre 120 y 250 bits:

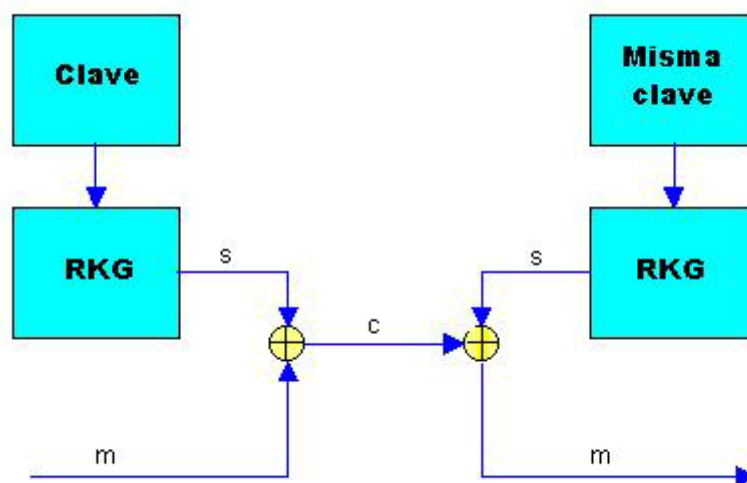


Figura 2.56 Ejemplo del diagrama de bloques del cifrado de flujo.

### Cifrado en bloque

Los cifrados en bloque se componen de cuatro elementos:

- Transformación inicial por permutación.

- Una función criptográfica débil (no compleja) iterada  $r$  veces.
- Transformación final para que las operaciones de encriptación y desencriptación sean simétricas.
- Uso de un algoritmo de expansión de claves que tiene como objeto convertir la clave de usuario, normalmente de longitud limitada entre 32 y 256 bits, en un conjunto de subclaves que puedan estar constituidas por varios cientos de bits en total.

### **Cifrado de Feistel**

Se denominan así los criptosistemas en los que el bloque de datos se divide en dos mitades y en cada vuelta de encriptación se trabaja, alternativamente, con una de las mitades. Pertenecen a este tipo los criptosistemas LUCIFER, DES, LOKI y FEAL.

#### **2.13.2 Algoritmo DES**

El algoritmo DES surge como consecuencia de un concurso organizado por NBS (National Bureau of Standards, USA) el cual solicitaba un “algoritmo de encriptación para la protección de datos de ordenador durante su transmisión y almacenaje”. Este concurso lo ganó IBM con su algoritmo DES (modificado del LUCIFER).

DES es un algoritmo de cifrado en bloque; la longitud de bloque es de 64 bits (8 símbolos ASCII); la longitud de la clave es de 56 bits, lo que equivale a que existan:

$$2^{56} = 7,2 \cdot 10^{16} \text{ claves diferentes}$$

La norma del DES es FIPS (Federal Information Processing Standards). La norma exige que el DES se implemente mediante un circuito integrado electrónico. El chip de DES es un producto estratégico USA. No está permitida su exportación sin un permiso especial, y no se permite comercializar en USA chips fabricados en el exterior.

El ANSI (American National Standards Institute, USA) adopta el DES con el nombre de DEA (Data Encryption Algorithm) el cual no exige la implementación del algoritmo en un chip, pudiendo ser programado mediante software. Las librerías de implementación de DES y DEA son openssl.

### **Estructura del DES**

El DES trabaja alternativamente sobre las dos mitades del bloque a cifrar. En primer lugar se hace una permutación. Después se divide el bloque en dos mitades, a continuación se realiza una operación modular que se repite 16 veces; esta operación consiste en sumar módulo 2 la parte izquierda con la función  $F(K_i)$  de la derecha, gobernada por una subclave  $K_i$ .

Después se intercambian las partes derecha e izquierda. En la vuelta 16 se remata el algoritmo con una permutación final que es la inversa de la inicial.

Para descifrar el DES basta con repetir la operación modular, es decir, su aplicación repetida dos veces conduce a los datos originales.

### Función F(K<sub>i</sub>)

Las operaciones realizadas por la función F son:

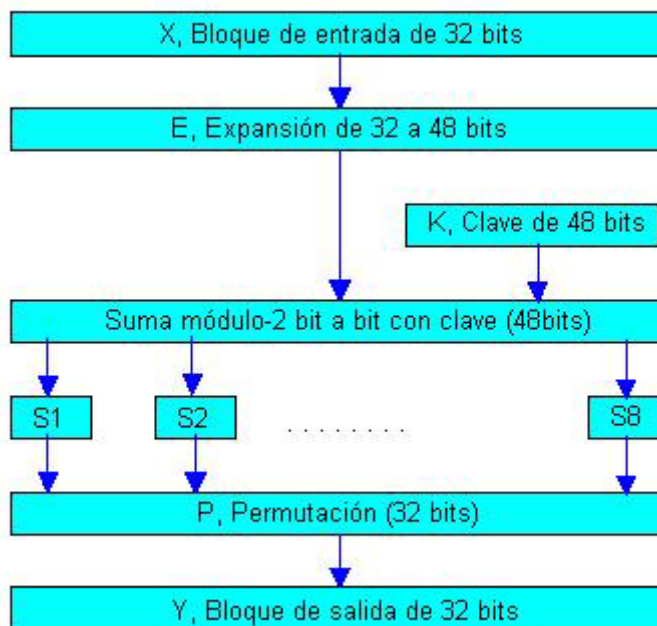


Figura 2.57 Operaciones realizadas por la función F.

Lo primero que se hace es fabricar un vector de 48 bits a partir de los 32 bits iniciales a través de una expansión lineal. Esta expansión es la que se describe a continuación :

Izquierda	32	1	2	3	4	5	4	5	6	7	8	9
Centro izda	8	9	10	11	12	13	12	13	14	15	16	17
Centro dcha	16	17	18	19	20	21	20	21	22	23	24	25
Derecha	24	25	26	27	28	29	28	29	30	31	32	1

Tabla 2.9 Ejemplo de la expansión lineal usada

Después se combina la clave local de 48 bits con la expansión por suma módulo 2 bit a bit, obteniéndose un vector de 48 bits que se divide en 8 grupos de 6 bits. Cada grupo entra en las llamadas “cajas S”. Estas cajas son las responsables de la *no linealidad del DES*. En cada caja entran 6 bits, pero salen únicamente 4 bits. Además los bits centrales se sustituyen en función de los bits laterales. Los principios para la elección de las cajas S no han sido revelados y es información clasificada por el gobierno de los Estados Unidos.

La caja P realiza una permutación lineal fija, esta permutación es la siguiente:

El bloque	16	7	20	21	29	12	28	17	1	15	23	26	5	18	31	10
Se cambia por	2	8	24	14	32	27	3	9	19	13	30	6	22	11	4	25

Tabla 2.10 Ejemplo de la permutación lineal fija usada

### Expansión de claves $K_i$

En DES se manejan claves de 64 bits, pero se le realiza una operación de reducción a 56 bits, eliminando un bit de cada ocho. A continuación se reordenan los bits restantes mediante una permutación fija que carece de significación criptográfica. Después se generan las 16 subclaves necesarias en las 16 vueltas del algoritmo. Cada subclave estará compuesta por 48 bits.

La forma de generar las subclaves es la siguiente:

- Se divide la clave de 56 bits en dos mitades de 28.
- Cada mitad se rota a la izquierda uno o dos bits dependiendo de la vuelta (de 1 a 16).
- Después de las rotaciones se vuelven a unir las mitades teniendo 16 grupos de 56 bits.
- A continuación se realiza una “permutación con compresión”. Esta permutación elige 48 bits de cada grupo formando así las 16 subclaves.

### Modos de uso

En la norma ISO 8372 se definen cuatro modos de uso de cualquier cifrado en bloque:

- ECB (Electronic Codebook): se caracteriza por el uso directo de un cifrador en bloque.
- CBC (Cipher Block Chaining): se carga inicialmente el registro (64 bits) con un vector inicial (VI) que no importe que sea secreto, pero si aleatorio. Sus principales características son que convierten el DES en un cifrador en flujo y puede hacer que cifre mensajes iguales de forma diferente con solo cambiar cada vez el VI.

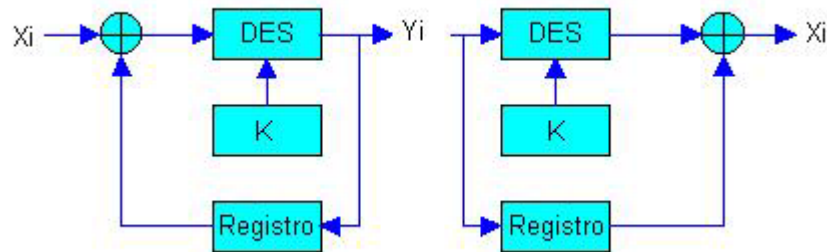


Figura 2.58 Diagrama de bloques del cifrado Cipher Block Chaining CBC

- CFB (Cipher Block Chaining): se carga inicialmente el registro de desplazamiento de 64 bits con un vector inicial (VI) que no importa que sea secreto, pero si aleatorio. Se divide el mensaje en claro en bloques de  $n$  bits. La operación de suma módulo 2 se hace bit a bit sobre bloques de  $n$  bits que pueden variar de 1 y 64. El registro de desplazamiento de 64 bits se desplaza a la izquierda  $n$  bits después de cada operación de cifrado de cada bloque.

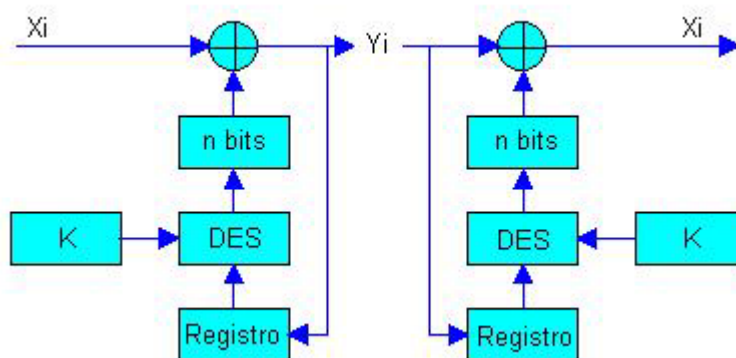


Figura 2.59 Diagrama de bloques del Cipher Block Chaining CFB

- OFB (Output Feedback): el funcionamiento es igual que en CFB, pero ahora el VI si tiene que ser secreto. Su principal característica es que convierte el DES como un generador de secuencia cifrante.

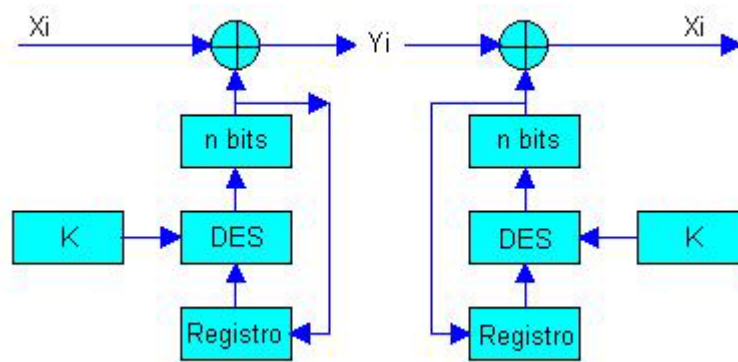


Figura 2.60 Diagrama de bloques del Output Feedback

### Cifrado triple

Es un modo de cifrado para el DES o cualquier otro cifrador en bloque que no llega a ser un cifrado múltiple, porque no son independientes todas las subclaves. Es inmune a un ataque por encuentro a medio camino. Para el DES la longitud efectiva de clave es de 112 bits.

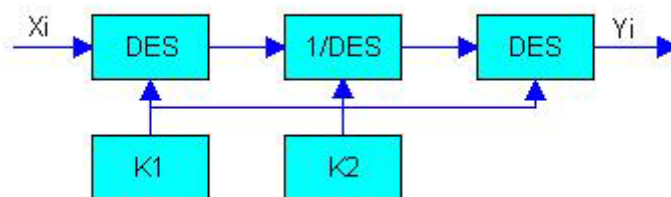


Figura 2.61 Diagrama de bloques del cifrado triple

### 2.13.3 IDEA (International Data Encryption Algorithm)

En este algoritmo, tanto los datos en claro como los cifrados están compuestos por bloques de 64 bits, mientras que la clave consta de 128 bits. Se basa en el concepto de mezclar operaciones aritméticas de grupos algebraicos diferentes (introduce confusión y difusión en el mensaje). Se realizan ocho vueltas de encriptación idénticas seguidas de una transformación de salida. Es decir, como el DES, pero las vueltas son más complejas. En cada vuelta de encriptación, el bloque de datos de entrada es dividido en cuatro sub-bloques de 16 bits. A su vez se utilizan para cada vuelta seis sub-claves.

Este algoritmo es muy seguro porque:

- Claves  $2^{128}$  no se pueden computar actualmente.



- No se le puede aplicar criptoanálisis diferencial a partir de la cuarta vuelta, y este tiene ocho.
- Como inconveniente tiene que si se deducen varios sub-bloques de la clave, se puede deducir la clave.

### 2.13.4 Criptografía de clave pública o asimétrica

En la criptografía de clave secreta se presentan los siguientes problemas:

- **Distribución de claves.** Dos usuarios tienen que seleccionar una clave en secreto antes de empezar a comunicarse, lo que deberá hacer bien personalmente (cosa que no siempre es posible), bien por medio de un canal inseguro.
- **Manejo de claves.** En una red de  $n$  usuarios, cada pareja debe tener su clave secreta particular, lo que hace un total de  $n(n-1)/2$  claves para esa red.
- **Sin firma digital.** En los criptosistemas de clave secreta no hay posibilidad, en general, de firmar digitalmente los mensajes, con lo que el receptor del mismo no puede estar seguro de que quien dice que le envía el mensaje sea realmente quien lo ha hecho. De todos modos, este punto afecta poco a los sistemas RFID ya que no contienen firma digital.

### Cambio de clave de Diffie-Hellman

Para evitar los problemas que se acaban de mencionar, Diffie y Hellman describieron un protocolo por medio del cual dos personas pueden intercambiarse pequeñas informaciones secretas por un canal inseguro. Es el siguiente:

1. Los dos usuarios  $A$  y  $B$ , seleccionan un grupo multiplicativo finito  $G$ , de orden  $n$  ( $Z_n^*$ ) y un elemento  $\alpha \in G$  (generador).
2.  $A$  genera un número aleatorio  $a$ , calcula  $\alpha^a \pmod n$  en  $G$  y transmite este elemento a  $B$
3.  $B$  genera un número aleatorio  $b$ , calcula  $\alpha^b \pmod n$  en  $G$  y transmite este elemento a  $A$
4.  $A$  recibe  $\alpha^b$  y calcula  $(\alpha^b)^a$  en  $G$
5.  $B$  recibe  $\alpha^a$  y calcula  $(\alpha^a)^b$  en  $G$

**Ejemplo:** Sea  $p$  el número primo 53. Supongamos que  $G=Z_{53}^* = \{1,2,\dots,52\}$  y sea  $\alpha = 2$  un generador. El protocolo Diffie-Hellman es el siguiente:

1.  $A$  elige  $a=29$ , calcula  $\alpha^a = 2^{29} \equiv 45 \pmod{53}$  y envía 45 a  $B$ .
2.  $B$  elige  $b=19$ , calcula  $\alpha^b = 2^{19} \equiv 12 \pmod{53}$  y envía 12 a  $A$ .
3.  $A$  recibe 12 y calcula  $12^{29} \equiv 21 \pmod{53}$ .

4. B recibe 45 y calcula  $45^{19} \equiv 21 \pmod{53}$

Ahora una escucha conocerá  $Z_{53}^*$ , 2, 45 y 12, pero no puede conocer la información secreta compartida por A y B que es 21.

## Criptosistema RSA

El protocolo de desarrollo es el siguiente:

1. Cada usuario U elige dos números primos (actualmente se recomienda que tales números primos tengan más de 200 dígitos)  $p$  y  $q$  y calcula  $n=p \cdot q$ . El grupo a utilizar por el usuario U es, entonces,  $Z_n^*$ . El orden de este grupo es  $\varphi(n) = \varphi(p \cdot q) = (p-1)(q-1)$ .
2. Después, U selecciona un entero positivo  $e$ ,  $1 \leq e < \varphi(n)$ , de modo que sea primo con el orden del grupo, es decir, de modo que  $\text{mcd}(e, \varphi(n)) = 1$ .
3. U calcula es inverso de  $e$  en  $Z_{\varphi(n)}$ ,  $d$ ; se tiene entonces  $e \cdot d \equiv 1 \pmod{\varphi(n)}$ , con  $1 \leq d < \varphi(n)$ .
4. La clave pública del usuario U es la pareja  $(n, e)$ , mientras que su clave privada es el número  $d$ . Por supuesto, también deben permanecer secretos los números  $p$ ,  $q$  y  $\varphi(n)$ .

Si un usuario A desea enviar un mensaje  $m$  de  $Z_n$  a otro usuario B, utiliza la clave pública de B,  $(n_b, e_b)$ , para calcular el valor de  $m^{e_b} \pmod{n_b} = c$ , que envía a B. Para recuperar el mensaje original, B calcula  $c^{d_b} = (m^{e_b})^{d_b} = m^{e_b d_b} \equiv m \pmod{n_b}$

**Ejemplo:** Consideremos una codificación del alfabeto que transforme las letras de la A a la Z en los números del 0 al 25 (del alfabeto inglés), y enviamos un mensaje al usuario B.

- El usuario B elige dos primos  $p_b=281$  y  $q_b=167 \rightarrow n_b=281 \cdot 167=46927$  y considera el grupo  $Z_{46927}^*$ .
- Ahora  $\varphi(46927)=280 \cdot 166=46480$  y B elige  $e_b=39423$  y comprueba que  $\text{mcd}(39423, 46480)=1$ .
- A continuación determina el inverso de 39423 módulo 46480  $\rightarrow d_b=26767$ .

**Clave privada=  $d_b=26767$**

**Clave pública=(39424,46927)**

Para enviar un mensaje de A a B, debemos determinar en la longitud del mismo. Como el mensaje ha de ser un elemento del grupo con el que estamos trabajando, su longitud no puede exceder del valor de  $n = 46927$ . Así pues como  $26^3=17576 < n < 456976=26^4$ , el mensaje ha de tener un máximo de tres letras. Si se quiere enviar un mensaje más largo, habrá que romperlo en grupos de tres letras. En la práctica, la longitud del mensaje es mucho mayor dado que  $n$  es un número con muchos dígitos.

$$\text{YES} = Y \cdot 26^2 + E \cdot 26 + S = 16346 = m$$

$$c = m^e_b(\text{mod } n_b) = 16346^{39423}(\text{mod } 46927) = 21166 \text{ [valor que A envía a B]}$$

- Ahora B recibe 21166 la decodificación sería así:

$$m = c^d_b(\text{mod } n_b) = 21166 (\text{mod } 46927^{39423}) = 16346$$

- Se decodifica  $m$  y se obtiene el texto original

$$m = 16346 = 24 \cdot 26^2 + 4 \cdot 26 + 18 = \text{YES}$$

### Características de RSA

Existen algunos **mensajes no cifrables** si  $m^e = m(\text{mod } n)$ .

- El  $e$  suele ser el 3 o  $2^{16}+1$  que son números primos.
- El algoritmo **DES implementado en software es 100 veces más rápido que RSA e implementado en chip es de 1000 a 10000 más rápido**. Por tanto para mensajes cortos se debe utilizar RSA y para los largos DES.
- Lo que se suele hacer es un *envoltorio digital*. El usuario A encripta el mensaje  $m$  con el criptosistema DES mediante una clave aleatoria, y a continuación la clave DES se encripta con RSA. Para recuperar el mensaje, el usuario B describe la clave de DES mediante su clave privada del RSA y luego utiliza la clave obtenida para descifrar el mensaje  $m$ .
- Para romper RSA se necesita conocer  $\varphi(n)$  del cual puede deducir  $d$ . Conocido  $n$  no es fácil determinar  $\varphi(n)$  ya que  $n=p \cdot q$  y no se conoce ni  $p$  ni  $q$ .
- Para que un RSA sea fuerte  $p$  y  $q$  tienen que ser difíciles de adivinar, esto implica:
  - $p$  y  $q$  sólo deben diferir en unos pocos dígitos, aunque no deben ser demasiado cercanos.
  - $(p-1)(q-1)$  deben contener factores primos grandes.
  - El mcd  $(p-1, q-1)$  debe ser pequeño.
  - Una condición indispensable es que  **$p$  y  $q$  sean primos**.

### Algoritmo asimétrico ELGAMAL

Supongamos que los mensajes son elementos de  $G$  y que el usuario A desea enviar un mensaje  $m$  al usuario B. El protocolo utilizado es el siguiente:

1. Se selecciona un grupo finito  $G$  y un elemento  $\alpha$  de  $G$ .
2. Cada usuario A elige un número aleatorio  $a$ , que será su clave privada, y calcular  $\alpha^a$  en  $G$ , que será su clave pública.

Para que un usuario A envíe un mensaje,  $m$ , a otro usuario B, suponiendo que los mensaje son elementos de  $G$ , realiza las siguientes operaciones:

1. A genera un número aleatorio  $v$  y calcula  $\alpha^v$  en  $G$
2. A mira la clave pública de B,  $\alpha^b$ , y calcula  $(\alpha^b)^v$  y  $m \cdot \alpha^{bv}$  en  $G$
3. A envía la pareja  $(\alpha^v, m \cdot \alpha^{bv})$  a B

Para recuperar el mensaje original:

1. B calcula  $(\alpha^v)^b$  en  $G$
2. B obtiene  $m$  sólo con calcular  $\rightarrow m \cdot \alpha^{bv} / \alpha^{vb}$

## 2.14 Control de errores

Cuando se usa el canal móvil para transmitir señales con información útil existe un riesgo muy elevado de pérdida de información si no se implementan métodos que eviten en cierta medida, los errores de transmisión.

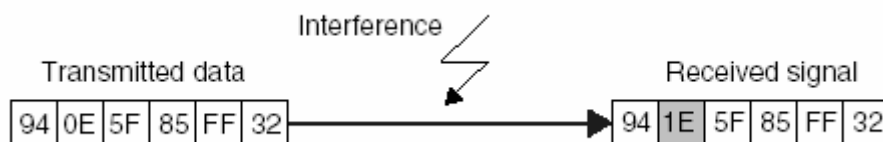


Figura 2.62 Las interferencias durante la transmisión pueden generar errores en los datos transmitidos.

El control de errores se usa para reconocer errores en la transmisión e iniciar medidas de corrección como, por ejemplo, pedir la retransmisión de los bloques de datos erróneos. Las medidas más comunes de control de errores son el control de paridad, la suma XOR y el CRC.

### 2.14.1 Control de paridad

El control de paridad es un muy sencillo y común método para realizar un control de errores eficaz. Este método incorpora un bit de paridad en cada byte transmitido, con un resultado de 9 bits enviados por cada byte de información.

Antes de la transmisión de datos debe tener lugar una decisión para dirimir si se establece una paridad par (even) o impar (odd) para asegurarnos de que emisor y receptor realizan el control de acuerdo con una misma selección. El valor del bit de paridad es fijado de modo que si usamos una paridad par, un número par de '1' debe contarse en los nueve bits. Por otro lado, si la paridad es impar, un número impar de '1' debe poder contarse en los nueve bits. La paridad impar puede ser también interpretada como el control horizontal (módulo 2) de los bits de datos. Este control horizontal también permite el cálculo de los bits de datos usando puertas lógicas OR exclusivas (XOR).

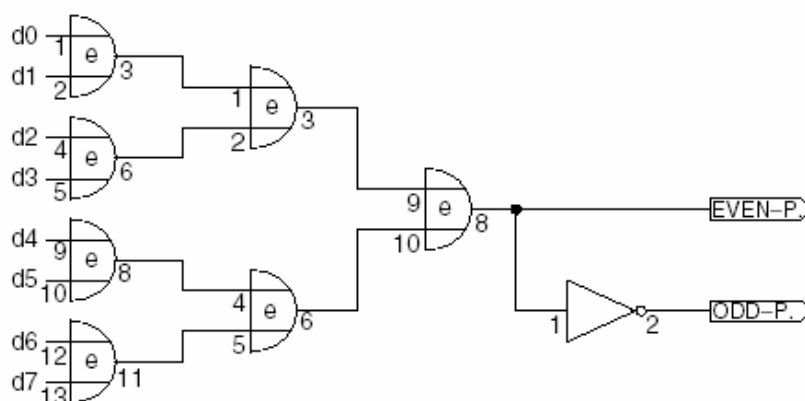


Figura 2.63 El bit de paridad puede ser hallado usando múltiples puertas XOR y realizando operaciones bit a bit.

De todos modos, la simplicidad de este método está contrarrestada por su pobre reconocimiento de errores (Pein, 1996). Si existe un número impar de bits erróneos (1, 3,

5, 7), siempre serán detectados, mientras que si el número de bits erróneos es par (2, 4, 6, 8), unos errores cancelan a los otros y la paridad aparece como correcta.

### 2.1.4.2 Método LRC

La suma de comprobación XOR, conocida como control de redundancia longitudinal (*LRC – Longitudinal redundancy checksum*) puede ser calculado rápida y fácilmente.

La suma de comprobación XOR se genera mediante el puerreo XOR recursivo de todos los bytes de datos en un solo bloque de datos. El byte 1 se pasa por una XOR con el byte 2, la salida de esta OR exclusiva es pasado por una XOR con el byte 3, etcétera. Si el resultado del LRC se añade al bloque de datos que se transmite, entonces un simple control de la transmisión una vez es recibida puede detectar los errores. El método a seguir es generar una suma LRC de todos los bytes recibidos (bloque de datos + resultado LRC añadido) . El resultado de esta operación debe ser siempre cero; cualquier otro resultado nos indica que ha habido errores en la transmisión.

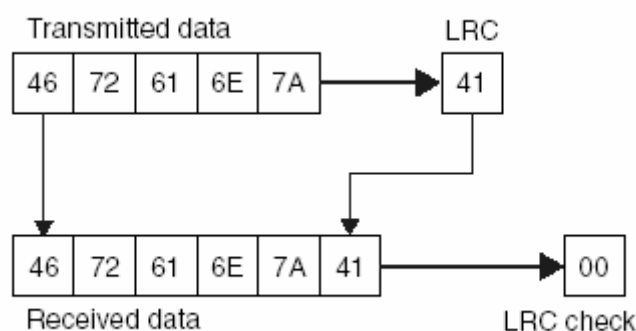


Figura 2.64 Si el LRC es añadido a los datos a transmitir, entonces un nuevo cálculo del LRC de los campos de datos recibido debe resultar 00h (la h indica que trabajamos con números hexadecimales). Esto permite una rápida verificación de los datos sin necesidad de conocer el actual valor de LRC.

Debido a la simplicidad de este algoritmo, los LRCs pueden ser calculados muy simplemente y rápidamente. De todos modos, los LRCs no son muy fiables porque es posible que múltiples errores se cancelen los unos a los otros y lograr así que el control no pueda detectar si se han transmitido con el bloque de datos. Los LRC son usados básicamente para el control rápido de bloques de datos muy pequeños (32 bytes, por ejemplo).

### 2.1.4.3 Método CRC

El CRC (Control de redundancia cíclica) fue originalmente usado en controladores de disco. La gran ventaja es que puede generar una suma de comprobación suficientemente segura para grandes cantidades de datos.

Se puede decir que es un excelente control de errores tanto para transmisiones vía cable (por ejemplo por vía red telefónica) como para radiocomunicaciones inalámbricas (radio, RFID). De todos modos, aunque el control de redundancia cíclica

representa un método muy seguro para reconocer errores, tiene una pega: no puede corregirlos.

Como su propio nombre sugiere, el cálculo del CRC es un proceso cíclico. Así, el cálculo del valor del CRC de un bloque de datos incorpora el valor del CRC de cada uno de los bytes de datos. Cada byte de datos individual es consultado para obtener el valor del CRC del todo el bloque de datos entero.

Matemáticamente hablando, un CRC es calculado dividiendo los datos entre un polinomio usando un llamado *generador de polinomios*. El valor del CRC es el resto obtenido de esta división. Para ilustrar mejor esta explicación, la figura que viene a continuación nos muestra el cálculo de un CRC de 4 bits para un bloque de datos. El primer byte del bloque de datos es 7Fh y el generador de polinomios es  $x^4 + x + 1 = 10011$ :

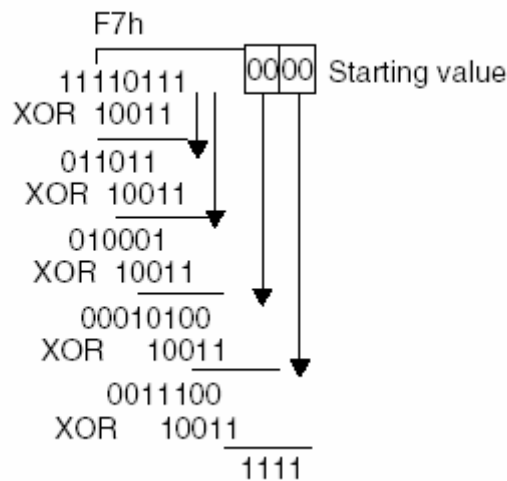


Figura 2.65 Paso a paso del cálculo de un CRC.

Si un CRC que acaba de ser calculado se anexa al final del bloque de datos y se realiza un nuevo cálculo del CRC, el nuevo valor calculado resultará ser cero. Esta característica particular del algoritmo del CRC es explotada para calcular errores en transmisiones de datos en serie.

Cuando un bloque de datos es transmitido, el valor del CRC de los datos es calculado por el transmisor, anexado al final del dicho bloque y transmitido con él. Una vez el bloque de datos es recibido, el receptor calcula el valor del CRC de todo el bloque de datos de modo que, por la propiedad que hemos mencionado anteriormente, el resultado que debe obtener es cero a no ser que exista errores en la transmisión.

Buscar el cero en el CRC del receptor es un método sencillo y rápido de poder comprobar la validez de los datos recibidos. Si no usáramos este método, deberíamos calcular el CRC del bloque de datos útil (es decir, de la información enviada quitándole los últimos bits de CRC) y después comparar el valor obtenido con el CRC recibido, lo que supone un proceso mucho más costoso que realizar el CRC de todo el bloque y buscar un resultado que sea cero.

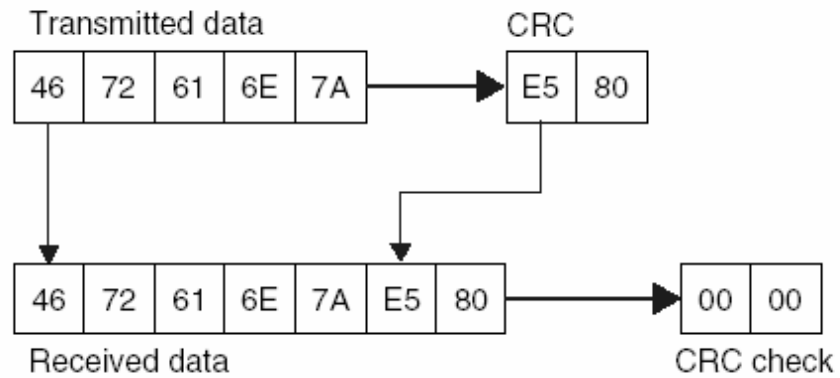


Figura 2.66 Si el valor del CRC se coloca al final del bloque de datos y se transmite todo junto. Al calcular de nuevo el CRC, esta vez de todo el bloque recibido, el resultado debe ser cero; sino existe algún error en la transmisión.

La gran ventaja que presenta el cálculo del CRC es su gran eficacia a la hora de reconocer la existencia de errores realizando un pequeño número de cálculos, incluso cuando existen múltiples errores.

Un CRC de 16 bits es capaz de reconocer los errores de bloques de datos que se encuentran por encima de los 4Kbytes. Un sistema de RFID transmite bloques de menos de 4Kbytes, por lo que los CRC usados pueden incluso ser menores de 16 bits.

A continuación tenemos unos ejemplos de generadores polinomiales:

CRC-8	$x^8+x^4+x^3+x^2+1$
CRC-16 / (controlador de disco)	$x^{16}+x^{15}+x^2+1$
CRC-16 /CCITT	$x^{16}+x^{12}+x^5+1$

Tabla 2.11 Generadores polinomiales



## 2.15 Multiacceso: anticolisión

Muchas veces un sistema de RFID tiene numerosos transponders dentro de su zona de interrogación. En este tipo de situación podemos diferenciar entre 2 principales tipos de comunicación.

La primera es usada para transmitir datos desde el lector a la etiqueta (como vemos en la Figura 2.67, que tenemos a continuación). El flujo de datos enviado es transmitido por todos tags simultáneamente (similar a miles de equipos de radio que reciben la señal desde una estación base). Este tipo de comunicación es la que conocemos como *broadcast*.

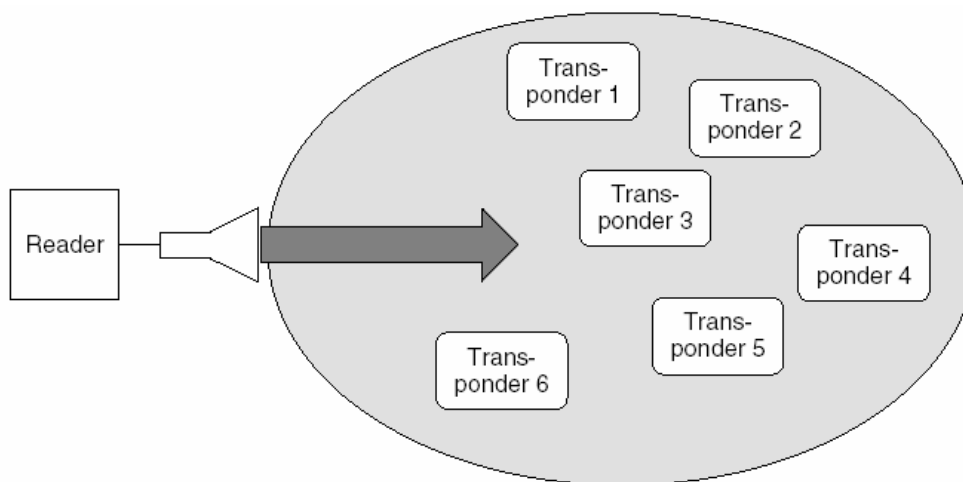


Figura 2.67 Modo *broadcast*: el flujo de datos transmitido por el lector es recibido simultáneamente por todas las etiquetas que se encuentran en la zona de interrogación.

La segunda forma de comunicación supone la transmisión de datos desde muchas etiquetas, que se encuentran en la zona de interrogación, hacia el lector. Esta forma de comunicación es llamada *multiacceso*.

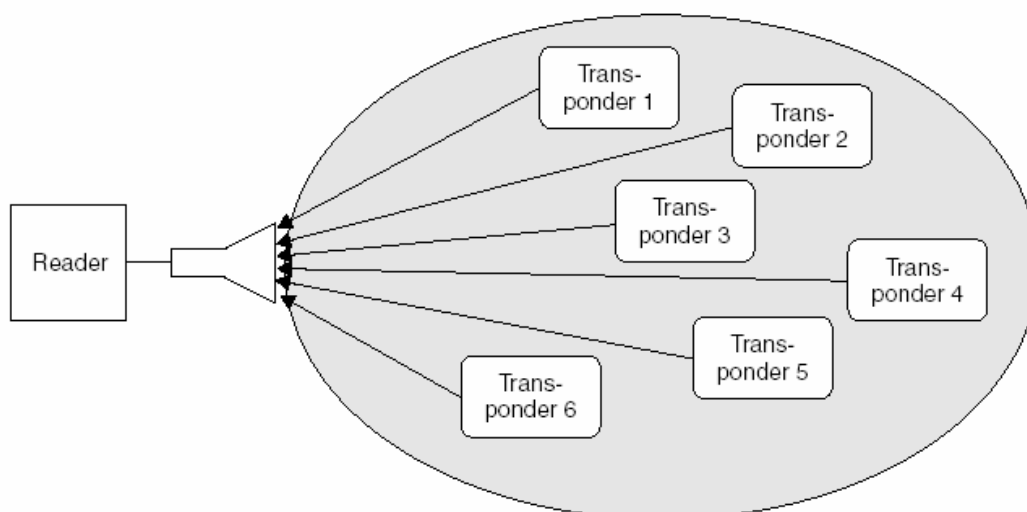


Figura 2.68 Multiacceso: múltiples tags se comunican a la vez con el lector.

Cada canal de comunicación tiene definida la capacidad de canal, la cual es determinada por el ratio máximo de transferencia de dicho canal de comunicación y el tiempo que está disponible.

La capacidad de canal disponible debe ser dividida entre cada participante (etiqueta) y el resultado será la cantidad que puede transmitir cada tag al mismo lector sin que sufran interferencias unos por culpa de los otros (colisión).

El problema del multiacceso ha existido desde hace mucho tiempo en la tecnología radio. Como ejemplo podemos fijarnos en los satélites o en las redes de telefonía móvil donde un gran número de participantes intenta acceder a un mismo satélite o estación base.

Por este motivo han sido desarrollados numerosos métodos con el objetivo de separar la señal de cada participante individual de la de otro cualquiera. Básicamente existen 4 métodos diferentes: acceso múltiple por división de espacio (*space division multiple access, SDMA*), acceso múltiple por división de frecuencia (*frequency domain multiple access, FDMA*), acceso múltiple por división de tiempo (*time domain multiple access, TDMA*), y acceso múltiple por división de código (*code division multiple access, CDMA*); esta última también conocida como técnica del espectro ensanchado (*spread spectrum*).

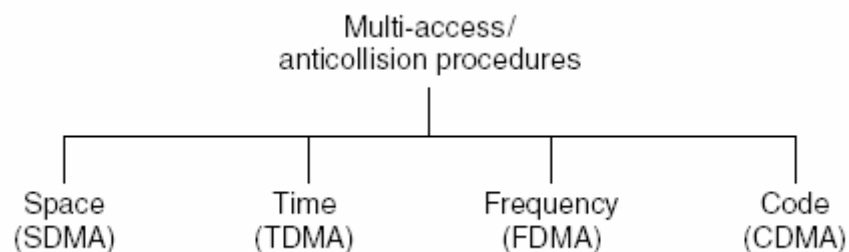


Figura 2.69 Los métodos de multiacceso están divididos en cuatro métodos básicos.

De todos modos, estos métodos clásicos están basados en la suposición de un flujo de datos continuo e interrumpido desde y hacia los participantes. En el momento que se dedica una capacidad de canal, dicha capacidad permanece dedicada hasta que termina la comunicación (p.e. mientras dura una llamada telefónica).

Por otro lado las etiquetas de un sistema RFID se caracterizan por periodos de actividad, intercalados con periodos de inactividad de distinta duración. La capacidad del canal tan sólo se dedica durante el tiempo justo y necesario para establecer un intercambio de datos.

En el contexto de los sistemas RFID, el proceso técnico (protocolo de acceso) que facilita el manejo de múltiples accesos, evitando así las interferencias, es llamado *sistema anticolidión*.

Por motivos de competencia, los fabricantes de sistemas no ofrecen al público los sistemas anticolidión que usan. A continuación vamos a describir los métodos multiacceso que son frecuentemente usados con el fin de ayudar a comprender los métodos anticolidión y, finalmente, expondremos algunos ejemplos de los mismos.

### **2.1.5.1 Acceso múltiple por división de espacio (SDMA)**

El término *acceso múltiple por división de espacio* se refiere a técnicas que rehúsan un cierto recurso (capacidad de canal) en áreas espaciales separadas.

Una opción es reducir significativamente el área de lectura de un único lector, pero para compensarlo entonces se tiene que situar un gran número de lectores y antenas en forma de array de manera que cubran toda el área que antes cubría el lector cuando tenía más alcance.

Otra opción es usar una antena direccionable eléctricamente en el lector. De este modo se puede apuntar a los tags directamente (SDMA adaptativo). De este modo varias etiquetas pueden ser diferenciadas por su posición angular en la zona de interrogación del lector (si el ángulo entre dos transponders es mayor que el ancho de haz de la antena direccional usada, un mismo canal puede ser usado varias veces).

Esto consiste en un grupo de dipolos que forman la antena; por esto mismo el SDMA adaptativo sólo se puede usar en aplicaciones RFID con frecuencias por encima de los 850MHz. Si se usaran frecuencias menores el tamaño de los dipolos sería excesivamente grande. Cada uno de los dipolos está colocado de manera que tiene una fase independiente de los demás dipolos.

El diagrama de radiación de la antena se halla mediante la superposición de los diferentes diagramas de radiación de los dipolos situados en diferentes direcciones.

Para fijar la dirección, los dipolos están alimentados por una señal de alta frecuencia de fase variable, regulada por unos controladores de fase.

Con la intención de cubrir todo el espacio, se deberá escanear el área de interrogación usando la antena direccional hasta que una etiqueta sea hallada dentro del 'foco de búsqueda' del lector.

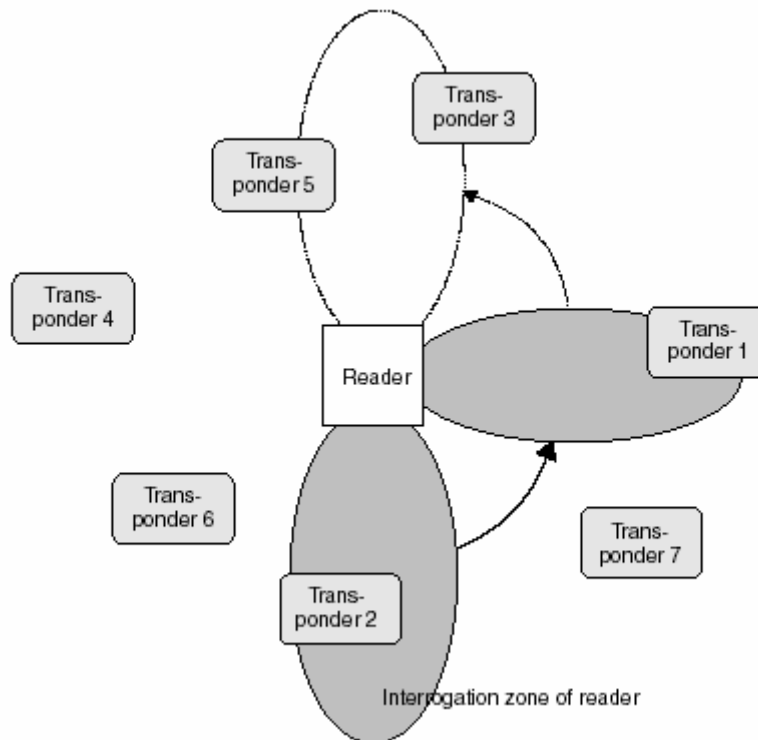


Figura 2.70 SDMA adaptativo con una antena direccionable eléctricamente. El ancho de haz es diseccionado a varias etiquetas; una tras la otra.

Un inconveniente del SDMA es el relativamente alto coste de implementación debido al complicado sistema de la antena. El uso de este tipo de técnica anticollisión queda restringida a unas pocas aplicaciones especializadas.

### 2.15.2 Acceso múltiple por división de frecuencias (FDMA)

El término *acceso múltiple por división de frecuencias* se refiere a las técnicas en las cuales varios canales de transmisión con varias frecuencias portadoras, están disponibles para los participantes en la comunicación.

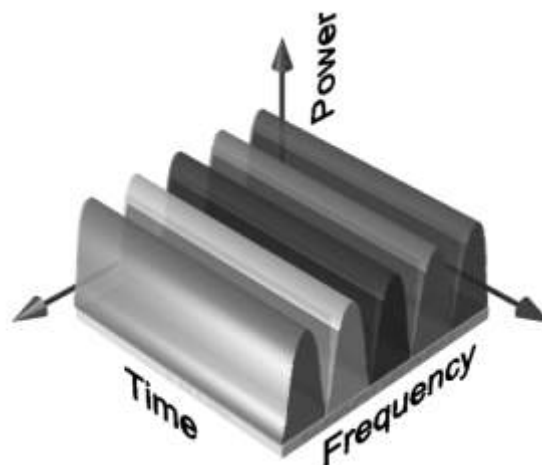


Figura 2.71 En FDMA se tiene varios canales frecuenciales en el mismo instante de tiempo.

En los sistemas RFID esto puede ser logrado una frecuencia de transmisión no harmónica y ajustable libremente. Pueden ser usados varios canales dentro de los rangos de frecuencia definidos por las especificaciones para realizar la transmisión. Esto puede conseguirse usando varias subportadoras de diferente frecuencia cada una.

Una de los inconvenientes de los sistemas que usan FDMA es el coste relativamente elevado que supone para realizar los lectores ya que desde un receptor dedicado tiene que ser posible la recepción para cada canal.

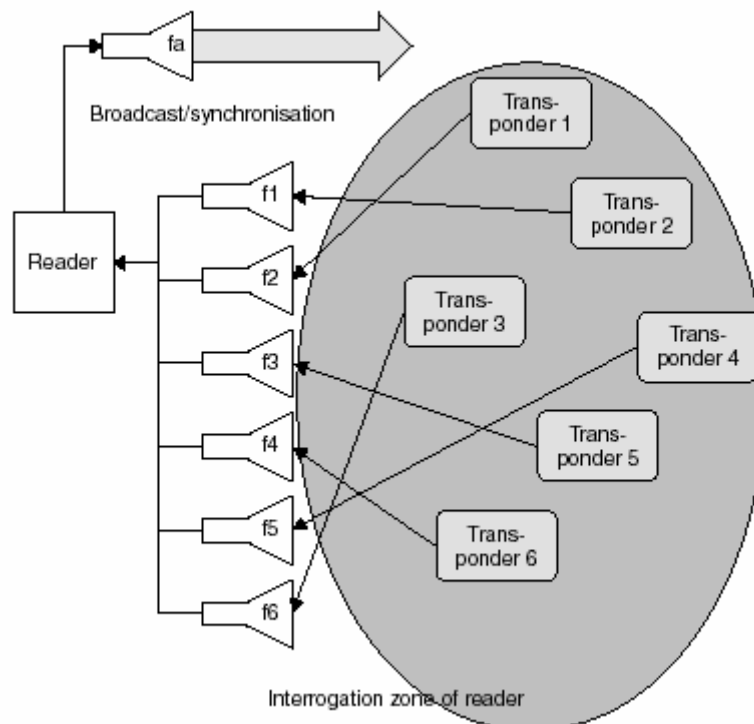


Figura 2.72 En los sistemas que usan FDMA existen varios canales frecuenciales para la transmisión de datos desde las etiquetas al lector.

### 2.15.3 Acceso múltiple por división de tiempo (TDMA)

El término *acceso múltiple por división de tiempo* se refiere a las técnicas de multiacceso en las cuales un canal disponible es dividido cronológicamente entre todos los participantes de la comunicación. El uso de TDMA está particularmente extendido en el campo de los sistemas digitales de radiocomunicaciones móviles.

En los sistemas RFID, TDMA es, de largo, el método usado en un mayor número de técnicas anticolidión.

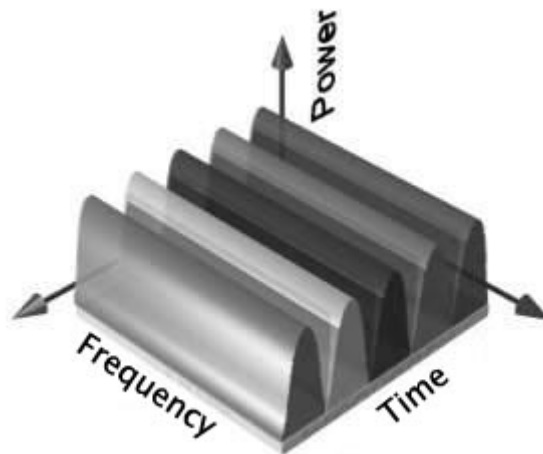


Figura 2.73 En TDMA se usa todo al ancho de banda disponible del canal, repartiéndolo cronológicamente entre todos los usuarios.

Los procedimientos que manejan el transponder son asíncronos, por lo que no existe un control de la transferencia de datos desde el lector. Este es el caso, por ejemplo, del procedimiento *ALOHA*, el cual explicaremos con más detalle a continuación.

Estos procedimientos que controlan la etiqueta son, naturalmente, muy lentos e inflexibles. La mayoría de aplicaciones usan procesos que son controlados por el lector, tomando éste el papel de 'master'. Estos métodos pueden ser considerados como síncronos, ya que todos los tags son controlados y comprobados por el lector simultáneamente.

Un único transponder es primero seleccionado de un gran grupo de transponders en la zona de interrogación del lector usando un algoritmo concreto y entonces la comunicación tiene lugar entre la etiqueta seleccionada y el lector. Una vez acaba la comunicación, ésta se da por finalizada y entonces el lector selecciona otro tag. Sólo una única comunicación puede ser iniciada a la vez, pero los transponder trabajan en una rápida sucesión y parece que todo ocurre en el mismo instante de tiempo. Esta es la finalidad de los métodos TDMA.

Los procedimientos controlados por el lector se pueden subdividir en '*polling*' y '*búsqueda binaria*'. Todos estos métodos están basados en el principio de que todos los transponders son identificados por un único '*número de serie*'.

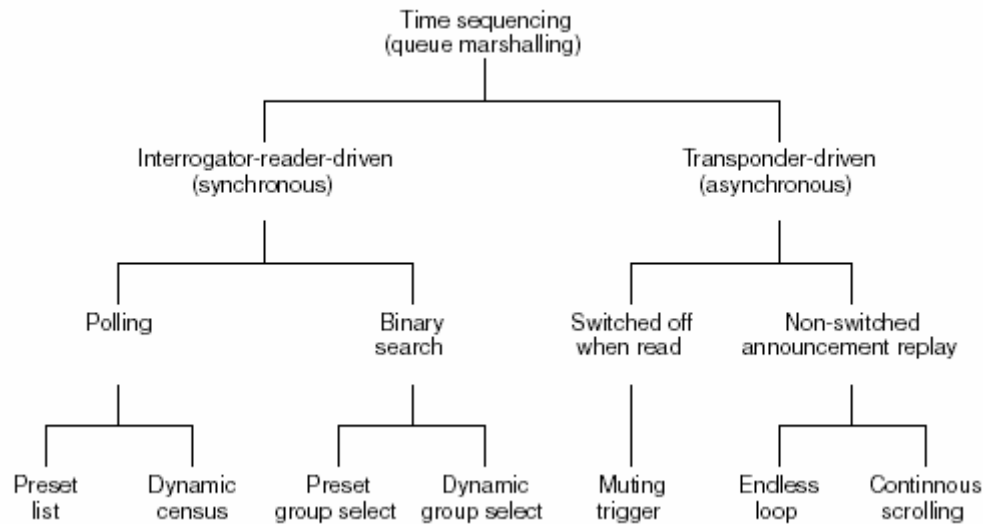


Figura 2.74 Clasificación de los métodos anticolidión TDMA según Hawkes (1997).

El método de ‘*polling*’ requiere una lista de todos los ‘números de serie’ de las etiquetas que pueden encontrarse en todo momento dentro del área de lectura en una aplicación. Todos los códigos de los tags son interrogados por el lector uno a uno hasta que uno de los tags preguntados responde. Este proceso puede ser muy lento dependiendo del posible número de tags que pueda haber en la aplicación; por este motivo este método sólo es aplicable a sistemas que tengan un número pequeño de individuos a identificar.

El método de la *búsqueda binaria* es mucho más flexible además de ser uno de los procedimientos más comunes. Consiste en que el lector provoca, intencionadamente, una colisión con una etiqueta cualquiera, elegida al azar. Si el proceso tiene éxito, es imprescindible que el lector sea capaz de detectar en que precisa posición de todos los bits se ha producido la colisión usando un sistema de codificación conveniente. Una descripción comprensiva del método de la búsqueda binaria es explicado más adelante.

#### 2.15.4 Ejemplos de métodos anticolidión

En los siguientes apartados vamos a explicar algunos de los métodos anticolidión más comúnmente usados. Los algoritmos de los ejemplos están intencionadamente simplificados de tal modo que el principio de funcionamiento puede ser entendido sin innecesarias complicaciones.

##### Método ALOHA

ALOHA es el más simple de todos los métodos anticolidión. Su nombre proviene del hecho de que este método multiacceso fue desarrollado en los años 70 por ALOHANET – una red de radiocomunicaciones de datos de Hawaii.

Este proceso es usado exclusivamente con transponders de sólo-lectura, los cuales generalmente tienen que transmitir sólo una pequeña cantidad de datos (número de serie o código), estos datos que son enviados al lector son una secuencia cíclica.

El tiempo de transmisión de los datos es tan sólo una fracción del tiempo de repetición, ya que hay pausas relativamente largas entre las transmisiones. Sin embargo, los tiempos de repetición para cada etiqueta difieren levemente. Existe una elevada probabilidad de que dos transponders puedan transmitir sus paquetes de datos en tiempos diferentes y, así, de que no colisionen el uno con el otro.

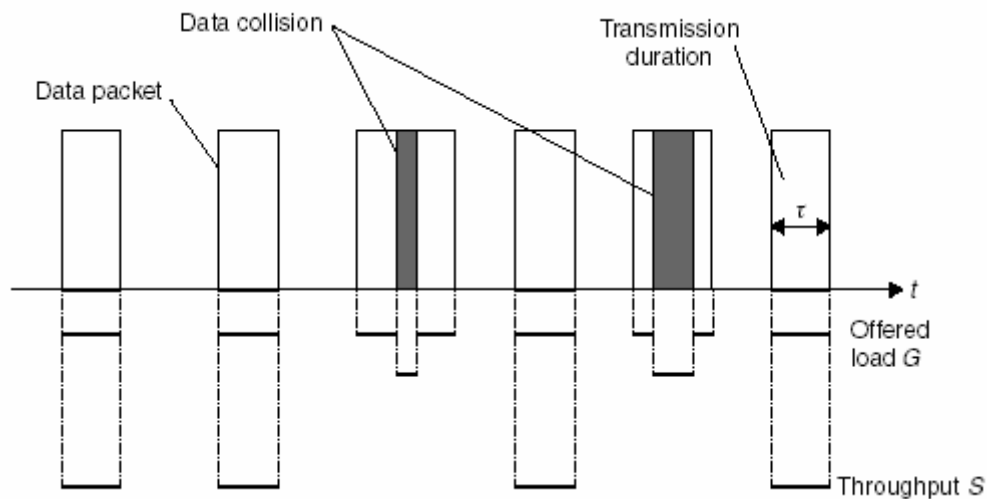


Figura 2.75 Secuencia temporal de una transmisión en un sistema ALHOA.

El tráfico ofrecido  $G$  corresponde al número de etiquetas transmitiendo simultáneamente en un cierto punto temporal  $t_n$ . El tráfico medio ofrecido  $G$  es la media de la observación en un periodo de tiempo  $T$  y es extraordinariamente sencillo de calcular a partir de tiempo de transmisión  $\tau$  de un paquete de datos:

$$G = \sum_1^n \frac{\tau_n}{T} \cdot r_n \quad (2.36)$$

donde  $n=1,2,3,\dots$  corresponde al número de tags en un sistema y  $r_n=0,1,2,\dots$  es el número de paquetes de datos que son transmitidos por el transponder  $n$  durante el periodo de observación.

El throughput  $s$  es 1 por la duración de la transmisión libre de errores (sin colisión) de un paquete de datos. En todos los casos en los que no haya una transmisión sin colisión (no existe transmisión o no se puede leer el paquete de datos por culpa de un error provocado por una colisión) el valor del throughput es 0. El throughput medio  $S$  de un canal de transmisión es hallado a partir del tráfico ofrecido  $G$ :

$$S = G \cdot e^{(-2G)} \quad (2.37)$$

Si consideramos el throughput  $S$  en relación con el tráfico ofrecido  $G$  (ver ecuación 2.37) encontramos un máximo de un 18'4% para una  $G=0,5$ . Para tráfico ofrecido menor, el canal de transmisión permanecerá sin usar la mayoría del tiempo; si



el tráfico ofrecido se incrementa por el número de colisiones entre cada una de las etiquetas entonces  $S$  se incrementaría agudamente.

La probabilidad de éxito  $q$  – la probabilidad de que un único paquete pueda ser transmitido sin colisiones – puede ser calculada a partir del tráfico medio ofrecido  $G$  y el throughput  $S$ :

$$q = \frac{S}{G} = e^{(-2G)} \quad (2.38)$$

Gracias a esta ecuación, algunos datasheets (hojas de especificaciones) incluyen figuras donde se muestra el tiempo necesario para ser capaz de leer todos los transponders que se encuentran en la zona de interrogación – lo que depende, evidentemente, del número de transponders que se encuentren dentro de la zona de interrogación.

La probabilidad  $p(k)$  de que una transmisión observada en un periodo  $T$  tenga  $k$  paquetes libres de errores puede ser calculada a partir del tiempo de transmisión  $\tau$  de un paquete de datos y del tráfico medio ofrecido  $G$ . La probabilidad  $p(k)$  es una distribución de Poisson con valor medio  $G/\tau$ :

$$p(k) = \frac{\left(G \cdot \frac{T}{\tau}\right)^k}{k!} \cdot e^{-\left(\frac{GT}{\tau}\right)} \quad (2.39)$$

### Método ALOHA Ranurado

Una posibilidad para mejorar el relativamente bajo throughput del método ALOHA es el método ALOHA Ranurado, mediante el cual las etiquetas sólo empiezan a transmitir en unos instantes de tiempo definidos y síncronos (*time slots*). La necesaria sincronización de las etiquetas es realizada por el lector.

El periodo de tiempo en el cual una colisión puede ocurrir (intervalo de colisión) es la mitad del mejor de los casos que se pueden dar en el método ALOHA.

Si asumimos que los paquetes de datos tienen todos igual tamaño (y por lo tanto tienen el mismo tiempo de transmisión  $\tau$ ) una colisión puede ocurrir en el método ALOHA si dos transponders quieren transmitir un paquete de datos hacia el lector en un intervalo de tiempo  $T \leq 2\tau$ . Como en ALOHA ranurado sólo pueden transmitirse paquetes en determinados puntos temporales, el intervalo donde se puede tener una colisión queda reducido a  $T = \tau$ . Esto provoca la siguiente relación para el throughput del método ALOHA ranurado:

$$S = G \cdot e^{(-G)} \quad (2.40)$$

Como vemos en la Figura 2.76, si usamos el método ALOHA ranurado podemos llegar a tener un throughput máximo  $S$  de 36,8% para un tráfico ofrecido  $G$ .

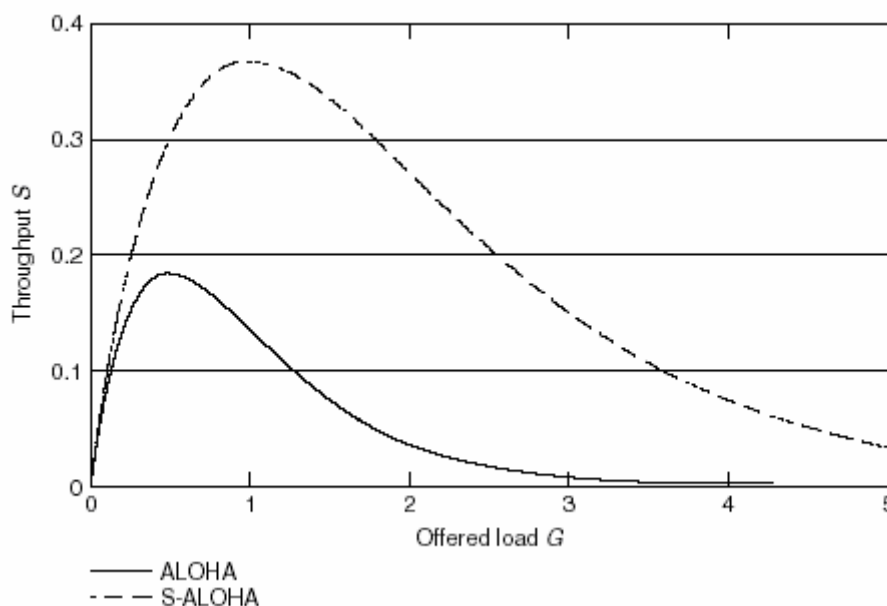


Figura 2.76 Comparación de las curvas del throughput de ALOHA y ALOHA ranurado. En ambos métodos el throughput tiende a cero tan pronto como el punto máximo ha sido sobrepasado.

De todos modos no es necesario que, si varios transponder envían su información al mismo tiempo, exista colisión: si una etiqueta está más cerca del lector que las demás puede ser capaz de imponerse a las demás como resultado de una mejor intensidad de su señal en el lector (debido a la proximidad de ésta al lector). Esto es conocido como el *efecto captura*.

El efecto captura tiene un efecto muy beneficioso en el comportamiento del throughput. Decisivo para esto es el '*threshold*'  $b$  el cual indica como de 'fuerte' es un paquete de datos enviados respecto a los otros para ser detectado por el receptor sin errores.

$$S = G \cdot e^{-\left(\frac{b \cdot G}{1+b}\right)} \quad (2.41)$$

Los principales comandos usados para controlar el proceso de anticollisión son:

REQUEST	Este comando sincroniza todos los transponders en el área de lectura y les solicita que transmitan sus números de serie al lector en uno de los time slots que haya a continuación.
SELECT (SNR)	Envía, como parámetro, un número de serie previamente seleccionado (SNR) al transponder. El transponder que tiene este número se prepara para poder recibir comandos de lectura o escritura. Los transponders con diferente número de serie siguen con el comando REQUEST como acción principal
READ_DATA	El transponder seleccionado envía los datos almacenados al lector (existen sistemas que también tienen comandos de escritura, autenticación, etc.)

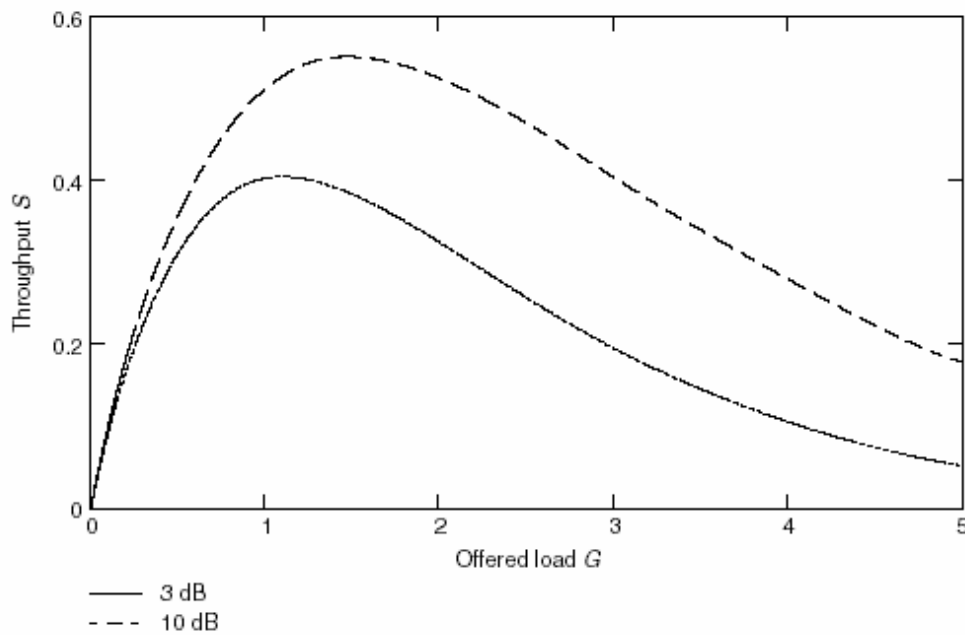


Figura 2.77 Comportamiento del throughput teniendo en cuenta el efecto captura con thresholds de 3 y 10 dB.

En el siguiente gráfico vemos un ejemplo del comportamiento de un sistema con el método ALHOA ranurado:

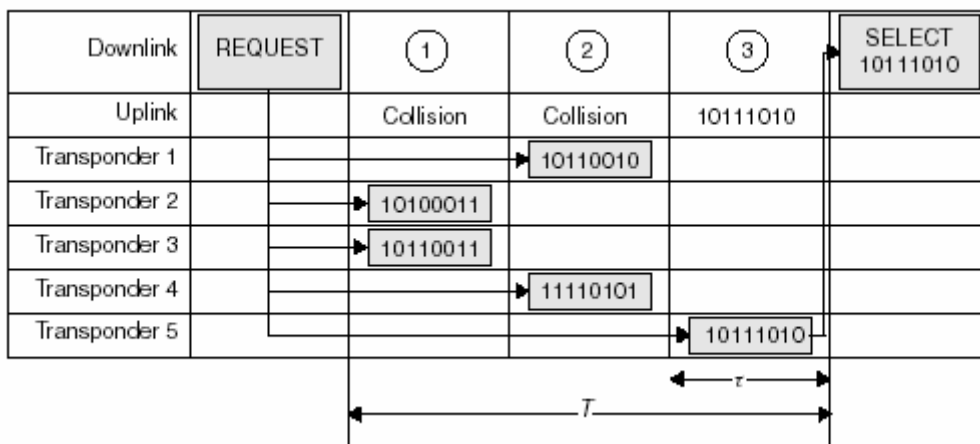


Figura 2.78 Ejemplo de sistema con el método anticollisión ALHORA ranurado

En el ejemplo que tenemos, los transponders tienen códigos de 8 bits, lo que limita a 256 los posibles tags puede haber en el sistema. En el momento en que el lector realiza el “REQUEST”, cada uno de los cinco transponders que se encuentran en el área de interrogación elige un slot temporal de los tres posibles que hay. De este modo vemos como se produce la colisión de dos transponders en los dos primeros slots temporales, mientras que el tag que ha elegido el tercer slot llega al lector, realizando ya el siguiente proceso de “SELECT”.

Este método seguirá hasta que el lector haya realizado las operaciones que pretende realizar y entonces seguirá con los demás tags.

## Algoritmo de búsqueda binaria

La implementación del algoritmo de la búsqueda binaria requiere que el bit preciso donde se produce la colisión sea localizado por el lector. Además, se necesita del uso de una codificación de bit conveniente; por eso vamos primero a comparar el comportamiento en las colisiones de las codificaciones NRZ y Manchester.

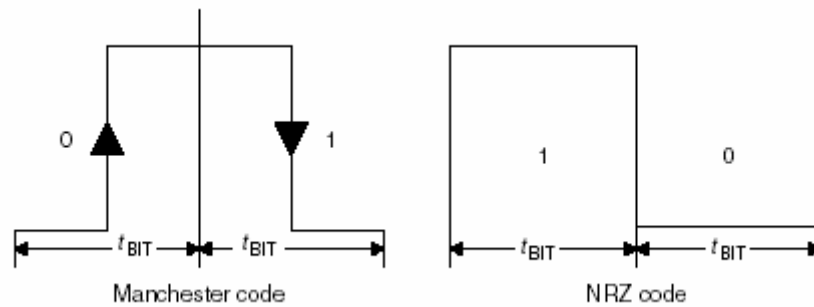


Figura 2.79 Codificación de bit usando códigos Manchester y NRZ

### Código NRZ

El valor de un bit es definido por el nivel estático del canal de transmisión durante una 'ventana de bit' ( $t_{BIT}$ ). En nuestro ejemplo anterior un '1' lógico es codificado por un nivel 'alto' estático, mientras que un '0' lógico lo es por un nivel 'bajo' estático.

Si al menos uno de los dos transponders envía una subportadora, esta es interpretada por el lector como una señal 'alta' y, en nuestro ejemplo, es asignada al valor lógico '1'. El lector no puede detectar si la señal que está recibiendo es una señal proveniente de la superposición de las señales de dos transponders o si, por el contrario, es una señal proveniente de un único tag y, por lo tanto, válida. El uso de un bloque de control de errores (paridad, CRC, etc.) puede encontrar el error en cualquier parte de un bloque de datos. De hecho no lo localiza, simplemente detecta la existencia de un error.

### Código Manchester

El valor de un bit es definido por el cambio de nivel (transición positiva o negativa) durante una ventana de bit ( $t_{BIT}$ ). En el ejemplo anterior un '0' lógico es codificado por una transición positiva; un '1' lógico es codificado por una transición negativa. El estado de 'no transmisión' no está permitido durante la transmisión de datos y es reconocido como un error.

Si dos (o más) transponders transmiten simultáneamente bits de diferente valor, entonces unos cancelan a los otros y lo que sucede es que el lector recibe un valor constante de señal durante todo el periodo de bit, lo que es reconocido como un error ya que este es un estado no permitido por la codificación Manchester. Así es posible detectar la colisión de un bit concreto.

Usaremos el código Manchester en nuestro ejemplo para explicar el algoritmo de búsqueda binaria.

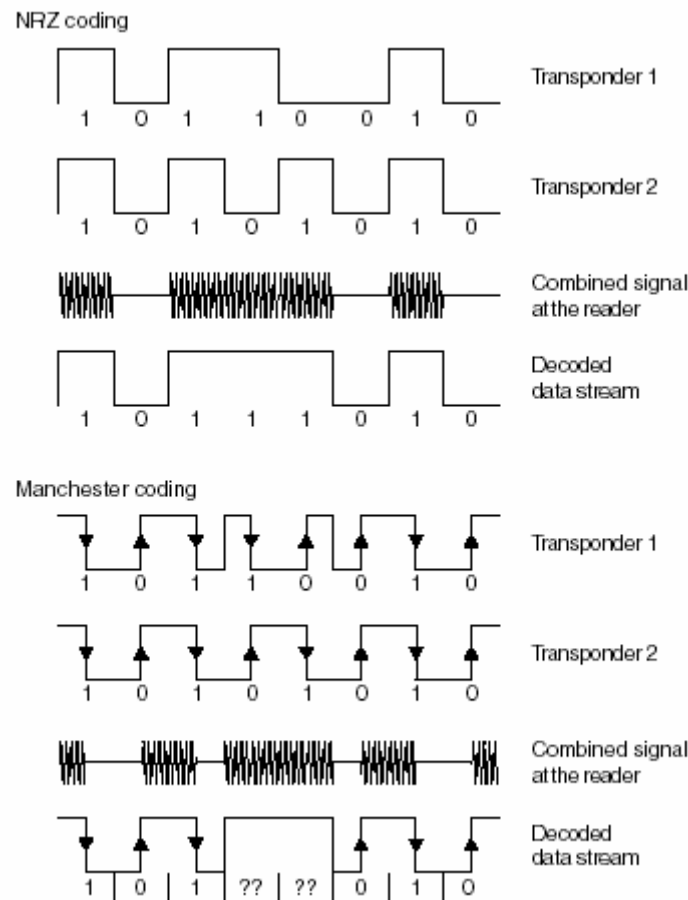


Figura 2.80 Comportamiento de los códigos Manchester y NRZ ante una colisión. El código Manchester hace posible detectar la colisión de un bit concreto.

Un algoritmo de búsqueda consiste en una secuencia predefinida (especificación) de interacciones (comando y respuesta) ente el lector y el transponder con el objetivo de ser capaz de seleccionar un transponder concreto de todos los pertenecientes a un grupo grande.

Para la realización práctica del algoritmo requerimos un conjunto de comandos que puedan ser procesados por el transponder. Además cada transponder debe tener un único número de serie (por ejemplo un código EPC). En el ejemplo que explicamos a continuación usamos un número de serie de 8 bits, por lo que tan sólo podemos garantizar  $2^8$  códigos distintos (256 códigos) y, por lo tanto, tan sólo podrá haber 256 etiquetas en el sistema.

REQUEST	Este comando manda un número de serie a los transponders como parámetro. Si el número de serie del transponder que lo recibe es menor o igual que el número de serie que manda el lector, entonces el transponder manda su propio número de serie hacia el lector. Así el grupo de transponders que responden pueden ser preseleccionados y reducidos.
---------	--

SELECT (SNR)	Envía, como parámetro, un número de serie previamente seleccionado (SNR) al transponder. El transponder que tiene este número se prepara para poder recibir comandos de lectura o escritura. Los transponders con diferente número de serie tan sólo responderán a un REQUEST.
READ_DATA	El transponder seleccionado envía los datos almacenados al lector (existen sistemas que también tienen comandos de escritura, autenticación, etc.)
UNSELECT	La selección de un transponder preseleccionado anteriormente se cancela y el transponder es 'silenciado'. En este estado el tag está completamente inactivo y no responder a los REQUEST. Para reactivarlo, debe ser reseteado apartándolo temporalmente del área del interrogación del lector (lo que es lo mismo que cortarle la fuente de alimentación).

El uso de los comandos que acabamos de definir en el algoritmo de búsqueda binaria será demostrado basado en el funcionamiento de un ejemplo con cuatro etiquetas dentro del área de interrogación. Los transponders de nuestro ejemplo poseen un único número de serie dentro del rango 00 – FFh (= 0 – 255 dec. o 00000000 – 11111111 bin.).

Transponder 1	10110010
Transponder 2	10100011
Transponder 3	10110011
Transponder 4	11100011

Tabla 2.12 Lista de transponders usados.

La primera iteración del algoritmo empieza con la transmisión del comando REQUEST ( $\leq 11111111$ ) por parte del lector. El número de serie 11111111b es el más grande posible, así que con este comando se preguntaría a todos los transponders dentro del área de interrogación.

La precisa sincronización de todas las etiquetas, por lo que empiezan a transmitir todas sus números de serie exactamente en el mismo instante de tiempo, es muy importante para conseguir un funcionamiento seguro del *árbol del algoritmo de búsqueda binaria*. Sólo de este modo es posible una precisa localización de bit donde se ha producido la colisión.

Como vemos en la tabla que viene a continuación, tenemos colisión (X) en los bits 0, 4 y 6 del número de serie recibido como superposición de las diferentes secuencias de los transponder que han respondido. El hecho de que haya una o más colisiones en los números de serie recibidos los lleva a pensar que tenemos más de un tag dentro del área de interrogación. Para ser más precisos, la secuencia de bits recibida 1X1X001X nos indica que tenemos aún ocho posibilidades de números de serie que tienen que ser detectados.

Bit number:	7	6	5	4	3 2 1	0
Received data in the reader	1	X	1	X	001	X
Possible serial number A	1	0	1	0	001	0
Possible serial number B*	1	0	1	0	001	1
Possible serial number C*	1	0	1	1	001	0
Possible serial number D*	1	0	1	1	001	1
Possible serial number E	1	1	1	0	001	0
Possible serial number F*	1	1	1	0	001	1
Possible serial number G	1	1	1	1	001	0
Possible serial number H	1	1	1	1	001	1

Tabla 2.13 Posibles números de serie después de evaluar los datos recibidos y teniendo en cuenta las colisiones (X) que han ocurrido en la primera iteración. Cuatro de las posibles direcciones (\*) son las toman fuerza aquí.

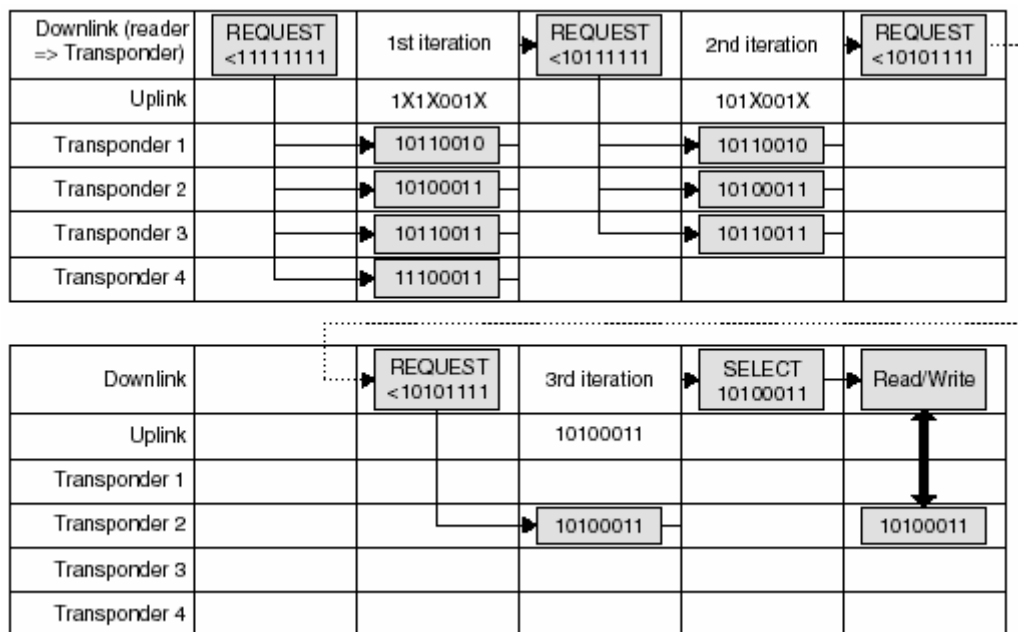


Figura 2.81 Los diferentes números de serie que son devueltos por los transponder en respuesta al comando REQUEST provocan una colisión. Por la restricción selectiva del rango preseleccionado de direcciones en las siguientes iteraciones, finalmente un solo tag responderá.

La regla general para limitar el área de búsqueda (rango) se muestra en la Tabla 2.14

Search command	1st iteration range	nth iteration range =
REQUEST ≥ Range	0	Bit(X) = 1, Bit(0 to X - 1) = 0
REQUEST ≤ Range	SNRmax	Bit(X) = 0, Bit(0 to X - 1) = 1

Tabla 2.14 Regla general para formar el parámetro *dirección* en el árbol de la búsqueda binaria. En cada caso, el bit (X) es el de mayor peso de la dirección recibida desde el transponder en el cual ha ocurrido una colisión en la iteración inmediatamente anterior.

Después de que el lector haya transmitido el comando REQUEST ( $\leq 10111111$ ), todos los transponders que cumplen esta condición responderán enviando su número de serie al lector. En nuestro ejemplo estos son los transponders 1, 2 y 3.

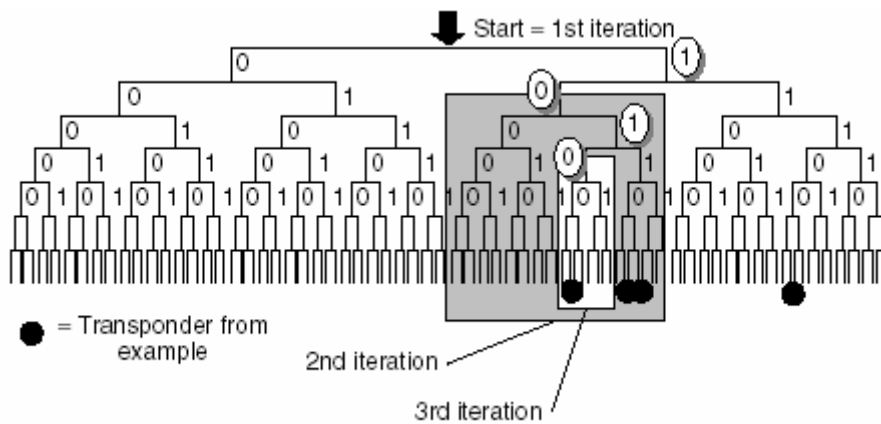


Figura 2.82 Árbol de búsqueda binaria. Un único transponder puede ser seleccionado por sucesivas reducciones del rango de etiquetas posibles.

Ahora hay una colisión (X) de los bits 0 y 4 del número de serie recibido. A partir de esto podemos sacar la conclusión de que hay, al menos, dos transponders en el rango de la segunda iteración. La secuencia recibida 101X001X aún permite 4 opciones para los posibles números de serie a detectar.

Bit number:	7	6	5	4	3	2	1	0
Received data at reader	1	0	1	X	0	0	1	X
Possible serial number A	1	0	1	0	0	0	1	0
Possible serial number B*	1	0	1	0	0	0	1	1
Possible serial number C*	1	0	1	1	0	0	1	0
Possible serial number D*	1	0	1	1	0	0	1	1

Tabla 2.15 Posibles números de serie en el rango de búsqueda después de evaluar la segunda iteración. Los transponders marcados (\*) son los más probables actualmente.

La nueva aparición de colisiones en la segunda iteración requiere una nueva restricción del rango de búsqueda en una tercera iteración. El uso de la regla de la tabla (2.14) nos lleva al rango de búsqueda  $\leq 10101111$ . Ahora el lector vuelve a transmitir a las etiquetas el comando REQUEST ( $\leq 10101111$ ). Esta condición es, finalmente, cumplida sólo por el transponder 2, el cual responde ahora al comando sin que exista colisión posible. Así hemos detectado un número de serie válido – ya no es necesaria una nueva iteración.

Gracias al siguiente comando que hemos explicado (SELECT), el transponder 2 es seleccionado usando la dirección detectada y puede ser ahora leído o escrito sin interferencias por parte de los otros transponders. Todos los tags están ‘callados’ y sólo el seleccionado responde al comando de lectura/escritura – READ\_DATA.

Después de completar la operación de lectura/escritura, el transponder 2 puede ser completamente desactivado usando el comando UNSELECT, de manera que no



responda al próximo comando REQUEST. De este modo el número de iteraciones necesario para seleccionar los demás transponders irá disminuyendo gradualmente.

La media de iteraciones  $L$  necesaria para detectar un único transponder de entre un gran número de ellos depende del número total de transponders  $N$  que se encuentran en el área de interrogación del lector, y puede ser calculada fácilmente:

$$L(N) = \text{ld}(N) + 1 = \frac{\log(N)}{\log(2)} + 1 \quad (2.42)$$

Si tan sólo un transponder se encuentra en la zona de interrogación del lector, entonces tan sólo se requiere una iteración para detectar su número de serie – no existe colisión en este caso. Si hay más de un transponder en la zona de interrogación del lector, entonces el número medio de iteraciones va incrementando gradualmente, siguiendo la curva:

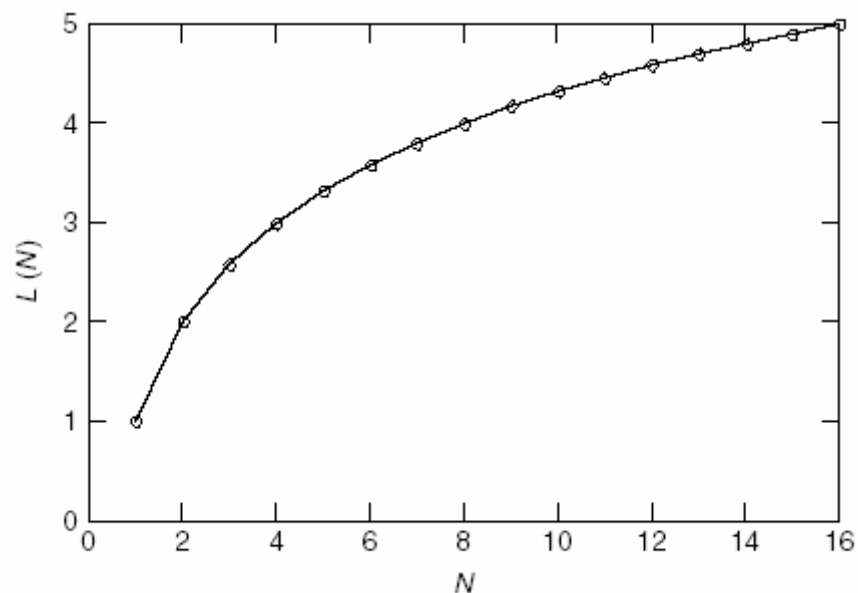


Figura 2.83 El número medio de iteraciones necesitado para determinar la dirección del transponder (número de serie) de un único transponder en función del número total de transponders que se encuentran en el área de interrogación. Cuando tenemos 32 transponders en el área de interrogación hacen falta una media de seis iteraciones, para 65 transponders una media de siete, para 128 transponders una media de ocho iteraciones, etc.

### Algoritmo de la búsqueda binaria dinámica.

En el método de la búsqueda binaria que vamos a explicar, el criterio de búsqueda y el número de serie de los transponders son siempre transmitidos en su longitud total. En la práctica, de todos modos, los números de serie de los transponders no consisten en un solo byte, como en el ejemplo, sino que dependiendo del sistema puede tener más de 10 bytes, lo que significa que toda esta información debe ser transmitida para poder seleccionar un único transponder. Si investigamos el flujo de

datos entre el lector y los transponders individualmente y en más detalle encontramos que:

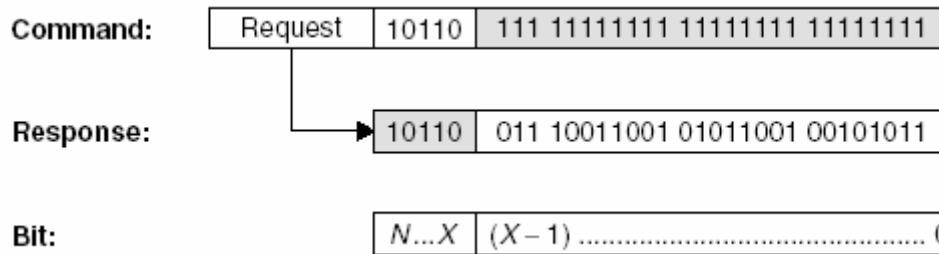


Figura 2.84 El comando del lector (n-ésima iteración) y la respuesta del transponder cuando un número de serie de 4 bytes ha sido seleccionado. Una gran parte de los datos de la solicitud (REQUEST) y de la respuesta (número de serie) es redundante (mostrado en gris). X se usa para situar del bit de mayor peso en el cual ha ocurrido una colisión en la iteración inmediatamente anterior.

- Desde el bit (X-1) al 0 del comando REQUEST no contiene información adicional a partir del momento en que se fijan todos los bits a 1.
- Desde el bit N al X del número de serie en la respuesta del transponder no contiene información adicional para el lector ya que es una información predeterminada y, por lo tanto, conocida.

Por lo tanto vemos que las partes complementarias de la información adicional transmitida son redundantes y que, por eso mismo, no necesitan ser transmitidas. Esto nos muestra rápidamente que podemos encontrar un algoritmo optimizado. En vez de transmitir toda la longitud de los números de serie en ambas direcciones, se puede partir teniendo en cuenta el bit X. El lector ahora tan sólo manda la parte conocida (N - X) del número de serie para ser determinado como el criterio de búsqueda en el comando REQUEST y entonces interrumpe la transmisión. Todos los transponders que coinciden en sus bits N al X con el criterio de búsqueda, responden enviando los bits que faltan, es decir, del X-1 al 0 de su número de serie. Los transponders son informados del número de bits de la subsecuencia por un parámetro adicional (*NVB=número válido de bits*) en el comando REQUEST.

Si nos fijamos en el ejemplo que hemos descrito en el apartado de *Algoritmo de búsqueda binaria* y lo aplicamos ahora, vemos que desde que aplicamos la regla de la tabla (2.14), el número de iteraciones corresponde con las del ejemplo anterior pero, sin embargo, el número de bits transmitidos - y por lo tanto el número de tiempo necesitado - puede ser reducido por debajo del 50%.

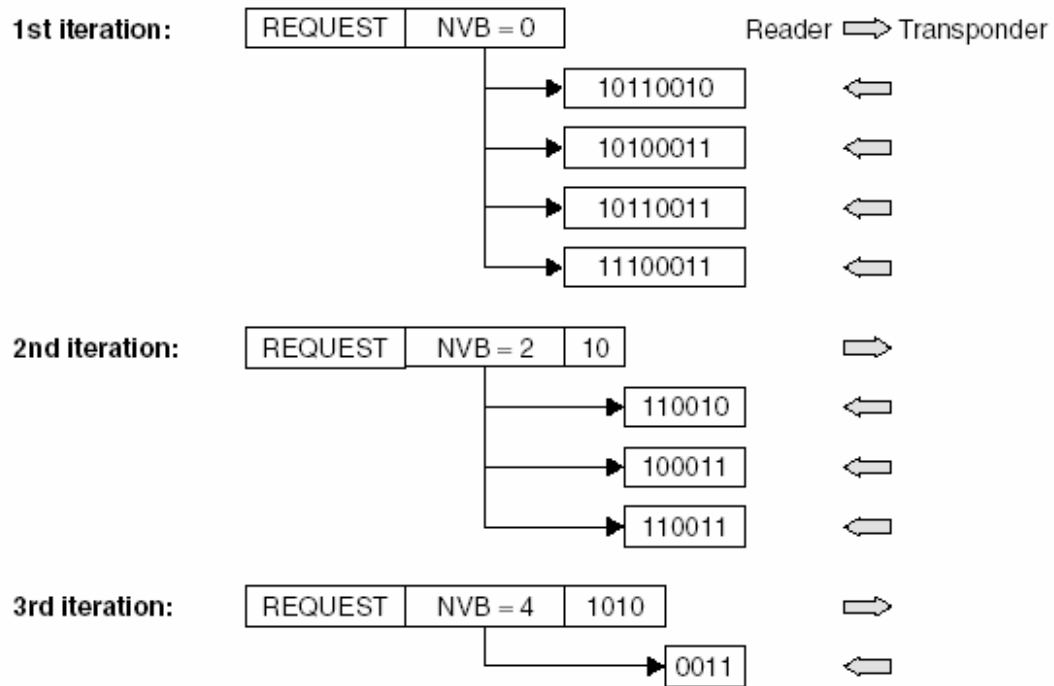


Figura 2.85 El algoritmo de búsqueda binaria dinámico evita la transmisión de partes redundantes del número de serie. El tiempo de transmisión es, así, reducido considerablemente.

## 2.16 Regulación y estandarización

### 2.16.1 Regulación

No existe ninguna administración que se encargue de la regulación a nivel global de la tecnología RFID, sino que cada país tiene sus órganos propios mediante los cuales regula de un modo individual el uso que se hace de las frecuencias y las potencias permitidas dentro de su propio territorio. Algunos de los organismos internacionales que regulan la asignación de frecuencias y potencias para RFID son:

- **EE.UU.:** FCC (*Federal Communications Commission*)
- **Canadá:** DOC (*Departamento de la Comunicación*)
- **Europa:** CEPT (siglas de su nombre en francés *Conférence européenne des administrations des postes et des télécommunications*), ETSI (*European Telecommunications Standards Institute*, creado por el CEPT) y administraciones nacionales. Obsérvese que las administraciones nacionales tienen que ratificar el uso de una frecuencia específica antes de que pueda ser utilizada en ese país
- **Japón:** MPHPT (*Ministry of Public Management, Home Affairs, Post and Telecommunication*)
- **China:** Ministerio de la Industria de Información
- **Australia:** Autoridad Australiana de la Comunicación (*Australian Communication Authority*)
- **Nueva Zelanda:** Ministerio de desarrollo económico de Nueva Zelanda (*New Zealand Ministry of Economic Development*)

En lo que al uso de frecuencias respecta, dependiendo de la banda en la que queramos trabajar, deberemos tener en cuenta que según donde nos encontremos tendremos que guiarnos por las recomendaciones que tenemos a continuación.

Las etiquetas RFID de baja frecuencia (LF: 125 - 134 Khz. y 140 - 148.5 Khz.) y de alta frecuencia (HF: 13.56 MHz) se pueden utilizar de forma global sin necesidad de licencia ya que trabajan dentro de la banda ISM (Industrial – Scientific – Medical). La frecuencia UHF (868 - 928 MHz) no puede ser utilizada de forma global, ya que no hay un único estándar global. En Norteamérica, la frecuencia UHF se puede utilizar sin licencia para frecuencias entre 908 - 928 MHz, pero hay restricciones en la potencia de transmisión. En Europa la frecuencia UHF está permitida para rangos entre 865.6 - 867.6 MHz. Su uso es sin licencia sólo para el rango de 869.40 - 869.65 MHz, pero existen restricciones en la potencia de transmisión (recientemente ha aparecido la nueva norma ETSI que permite hasta 2W de potencia de transmisión). El estándar UHF norteamericano (908-928 MHz) no es aceptado en Francia ya que interfiere con sus bandas militares. En China y Japón no hay regulación para el uso de las frecuencias UHF. Cada aplicación de frecuencia UHF en estos países necesita de una licencia, que debe ser solicitada a las autoridades locales, y puede ser revocada. En Australia y Nueva Zelanda, el rango es de 918 - 926 MHz para uso sin licencia, pero hay restricciones en la potencia de transmisión.

Existen regulaciones adicionales relacionadas con la salud y condiciones ambientales. Por ejemplo, en Europa, la regulación *Waste of electrical and electronic equipment* ("Equipos eléctricos y electrónicos inútiles"), no permite que se desechen las etiquetas RFID. Esto significa que las etiquetas RFID que estén en cajas de cartón deben de ser quitadas antes de deshacerse de ellas.

También hay regulaciones adicionales relativas a la salud; en el caso de Europa acaba de publicarse (por parte de la ETSI) un estándar llamado EN 302 208 que consta de dos partes. Una primera que describe las especificaciones técnicas y una segunda que especifica las condiciones a cumplir en cuanto a directivas europeas se refiere para compatibilidad electromagnética.

Las especificaciones que cumple son:

<b>Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity (R&amp;TTE Directive).</b>
<b>CEPT/ERC/REC 70-03: "Relating to the use of Short Range Devices (SRD)".</b>
<b>ETSI EN 301 489-1: "Electromagnetic compatibility and Radio spectrum Matters (ERM); Electromagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements".</b>
<b>ETSI TR 100 028 (all parts): "Electromagnetic compatibility and Radio spectrum Matters (ERM); Uncertainties in the measurement of mobile radio equipment characteristics".</b>
<b>ETSI EN 302 208-1: "Electromagnetic compatibility and Radio spectrum Matters (ERM); Radio Frequency Identification Equipment operating in the band 865 MHz to 868 MHz with power levels up to 2 W Part 1: Technical requirements and methods of measurement".</b>
<b>ETSI EN 301 489-3: "Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 3: Specific conditions for Short-Range Devices (SRD) operating on frequencies between 9 kHz and 40 GHz".</b>
<b>Council Directive 73/23/EEC of 19 February 1973 on the harmonization of the laws of Member States relating to electrical equipment designed for use within certain voltage limits (LV Directive).</b>
<b>Council Directive 89/336/EEC of 3 May 1989 on the approximation of the laws of the Member States relating to electromagnetic compatibility (EMC Directive).</b>

Tabla 2.16 Especificaciones que cumple la norma EN 302 208

Dentro del proceso de regulación tienen una gran importancia los organismos que desarrollan los diferentes estándares con los que RFID cuenta hoy en día. Algunos de estos organismos son la propia ETSI, EPCglobal o la ISO , dedicados al desarrollo de estándares como:

- ISO 10536
- ISO 14443
- ISO 15693

- ISO 18000
- EPC
- EN 302 208

### **2.16.2 EPC**

El EPC, siglas de Código Electrónico de Producto (Electronic Product Code), nace de las manos de EPCglobal, un consorcio formado por EAN International (European Article Numbering) el cual tiene 101 organizaciones miembro, representadas en 103 países y UCC (Uniform Code Council) propietario del UPC (Universal Product Code), presente en 140 países y ahora llamado GS1 US.

La intención de EPCglobal al crear el EPC no fue otra que la de promover la EPCglobal Network, un concepto de tecnología que pretende cambiar la actual cadena de suministro por otra con un estándar abierto y global, que permita la identificación en tiempo real de cualquier producto, en cualquier empresa de cualquier parte del mundo.

La EPCglobal Network ha sido desarrollada por el Auto-Id Center, un equipo de investigación del MIT (Massachusetts Institute of Technology) que cuenta con laboratorios por todo el mundo. Dicho desarrollo fue llevado a cabo en más de 1000 compañías de alrededor del mundo.

Así mismo, actualmente, todo estándar que desarrolla EPCglobal pasa por la supervisión de la ISO (International Standards Organization), con la única condición de que los estándares concretos que crea ISO sean ratificados y usados en los que cree EPCglobal.

Una vez conocemos de donde proviene el EPC, vamos a hacer un pequeño estudio sobre el estándar para ver que ventajas e inconvenientes nos proporciona.

Las especificaciones del EPC se pueden dividir en:

- Especificaciones para las etiquetas, referentes a los datos almacenados en ellas, a los protocolos de comunicación con el lector y la parte de RF que permite la comunicación.
- Especificaciones para los lectores: protocolo para el interfaz aire y comunicaciones lógicas con las etiquetas.

El estándar EPC divide las etiquetas usadas en seis tipos diferentes, dependiendo de su funcionalidad:

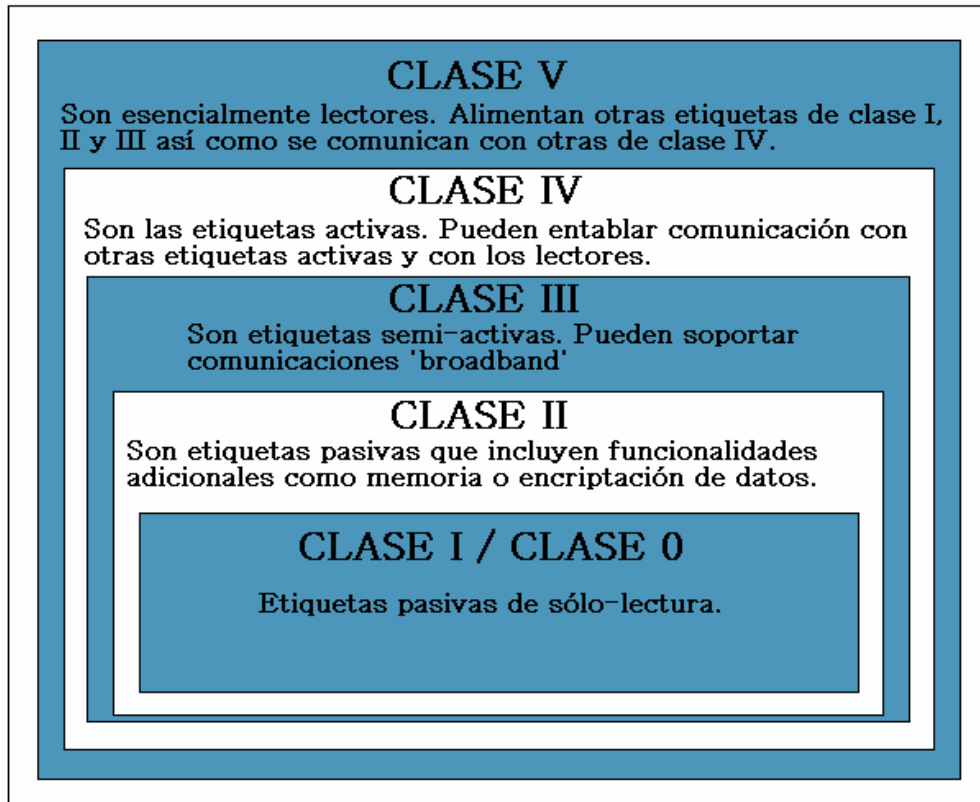


Figura 2.86 Tipos de etiquetas definidos en el EPC.

El pasado mes de enero de 2005, EPCglobal publicó las especificaciones de la última versión de EPC, el ECP Generation 2, versión 1.0.9.

Esta última publicación está llamada a ser el estándar adaptado a nivel mundial en el uso de los sistemas de RFID ya que se ha realizado para cumplir con las necesidades de los consumidores. Para poder suplir las necesidades mencionadas EPCglobal, además de incluir especificaciones no observadas en otras regulaciones realizadas anteriormente, ha pretendido homogeneizar los principales estándares existentes.

En la siguiente tabla podemos observar los estándares que se tienen como pre-requisito en EPC Gen2, los más importantes existentes en la actualidad. Un dato muy importante es que se incluye la norma EN 302 208 de la ETSI, cosa que representa un gran paso para una estandarización única entre Europa y USA, es decir: el EN 302 208 y el EPC Generation 2 se complementan el uno al otro.

<b>EPCglobal™: EPC™ Tag Data Standards</b>
<b>EPCglobal™ (2004): FMCG RFID Physical Requirements Document (draft)</b>
<b>EPCglobal™ (2004): Class-1 Generation-2 UHF RFID Implementation Reference (draft)</b>

<p><b>European Telecommunications Standards Institute (ETSI), EN 302 208:</b> <i>Electromagnetic compatibility and radio spectrum matters (ERM) – Radio-frequency identification equipment operating in the band 865 MHz to 868 MHz with power levels up to 2 W, Part 1 – Technical characteristics and test methods</i></p>
<p><b>European Telecommunications Standards Institute (ETSI), EN 302 208:</b> <i>Electromagnetic compatibility and radio spectrum matters (ERM) – Radio-frequency identification equipment operating in the band 865 MHz to 868 MHz with power levels up to 2 W, Part 2 – Harmonized EN under article 3.2 of the R&amp;TTE directive</i></p>
<p><b>ISO/IEC Directives, Part 2:</b> <i>Rules for the structure and drafting of International Standards</i></p>
<p><b>ISO/IEC 3309:</b> <i>Information technology – Telecommunications and information exchange between systems – High-level data link control (HDLC) procedures – Frame structure</i></p>
<p><b>ISO/IEC 15961:</b> <i>Information technology, Automatic identification and data capture – Radio frequency identification (RFID) for item management – Data protocol: application interface</i></p>
<p><b>ISO/IEC 15962:</b> <i>Information technology, Automatic identification and data capture techniques – Radio frequency identification (RFID) for item management – Data protocol: data encoding rules and logical memory functions</i></p>
<p><b>ISO/IEC 15963:</b> <i>Information technology — Radiofrequency identification for item management — Unique identification for RF tags</i></p>
<p><b>ISO/IEC 18000-1:</b> <i>Information technology — Radio frequency identification for item management — Part 1: Reference architecture and definition of parameters to be standardized</i></p>
<p><b>ISO/IEC 18000-6:</b> <i>Information technology automatic identification and data capture techniques — Radio frequency identification for item management air interface — Part 6: Parameters for air interface communications at 860–960 MHz</i></p>
<p><b>ISO/IEC 19762:</b> <i>Information technology AIDC techniques – Harmonized vocabulary – Part 3: radio-frequency identification (RFID)</i></p>
<p><b>U.S. Code of Federal Regulations (CFR), Title 47, Chapter I, Part 15:</b> <i>Radio-frequency devices, U.S. Federal Communications Commission</i></p>

Tabla 2.17 Los documentos aquí listados son de obligado cumplimiento para poder aplicar la especificación EPC Generation 2.



Las especificaciones de la capa física del EPC Gen2 establecen que en las comunicaciones del lector a la etiqueta deben usarse modulaciones de doble banda lateral ASK (*double sideband amplitude shift keying – DSB-ASK*), simple banda lateral ASK (*simple sideband amplitude shift keying – SSB-ASK*) o de reverso de fase ASK (*phase reversal amplitude shift keying – PR-ASK*), con una codificación de pulso-intervalo (*pulse-interval encoding - PIE*). El lector esperará una respuesta de backscatter (*backscattering reply*).

En la comunicación de la etiqueta al lector se deberá enviar una señal no modulada codificada en formato FM0 o código Miller.

En ambos casos el método usado para comunicarse es Half Duplex.

Para proceder a la identificación de las etiquetas que se encuentran dentro del radio de acción del lector existen 3 operaciones básicas:

- *Select*. Esta operación permite al lector poder ‘ver’ qué población de tags hay disponible en su rango de acción. Se puede decir que este proceso es equivalente a una Select realizada en una sentencia Sql para bases de datos, de ahí su nombre.
- *Inventario*. Es la operación que nos permite identificar las etiquetas. El proceso de inventario se inicia cuando el lector manda un comando *Query*. Entonces uno o más tags pueden responder a esta petición. El lector detecta una única respuesta de un tag y entonces interroga a éste para que le proporcione el código PC (*Protocol Control*), el código EPC y el CRC-16. Este proceso comprende varios comandos y se realiza en una única sesión a la vez.
- *Acceso*. El proceso de acceso comprende varias operaciones de comunicación con la etiqueta (lectura y/o escritura). Una única etiqueta debe ser identificada antes de iniciar el proceso de acceso a la misma.

De todos modos, el proceso de comunicación entre el lector y la etiqueta es mucho más complicado de lo que en un principio puede parecer. En la figura que tenemos a continuación podemos ver un diagrama de estados de una etiqueta. Estos estados representan la situación en la que se encuentra una etiqueta en cada posible momento de una comunicación con el lector.

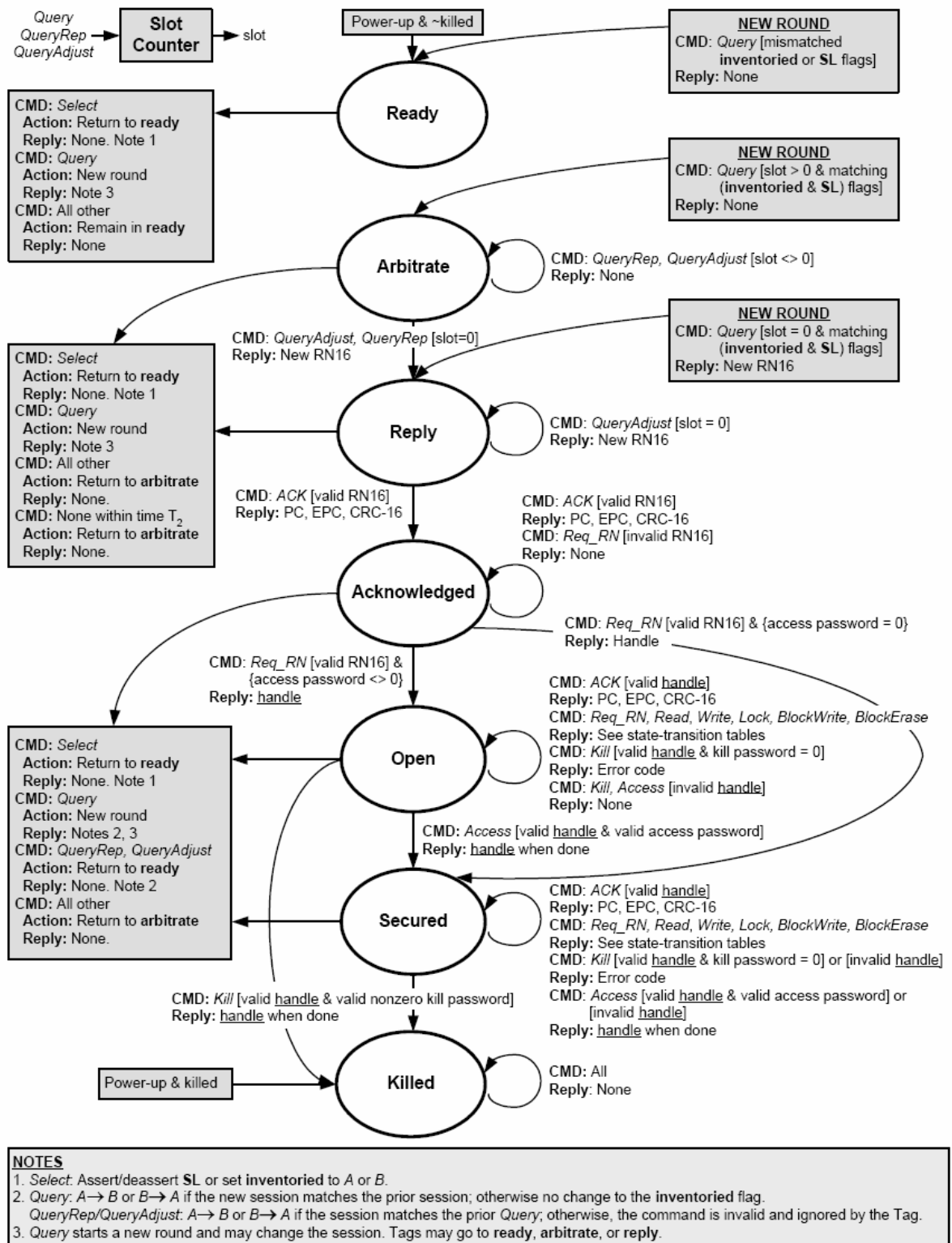


Figura 2.87 Diagrama de estados de una etiqueta que cumple EPC Generation 2.

### 2.16.3 EN 302 208

Actualmente existen limitaciones en Europa en lo que al uso de RFID, dentro de la banda UHF, respecta ya que por el momento se encuentra limitado a frecuencias entre los 869.40 y los 869.65 MHz. debiendo cumplir la norma EN 300 220, la cual no contempla las necesidades de RFID en la banda UHF, con una potencia radiada equivalente menor a 500mW y un ciclo de trabajo inferior al 10%.

La existencia de estas limitaciones dentro de la banda UHF, junto a las necesidades de un mercado que permita la libre circulación de equipos de RFID comunes para los países de la Unión Europea y la no armonización del espectro ha motivado que, en mayo de 2005, la ETSI publicara un nuevo estándar. El EN 302 208.

Este nuevo estándar aumenta la banda frecuencial en la cual pueden trabajar los sistemas RFID hasta los 3MHz. (desde los 865.00MHz. hasta los 868.00MHz.), con una potencia radiada equivalente como vemos en la siguiente figura:

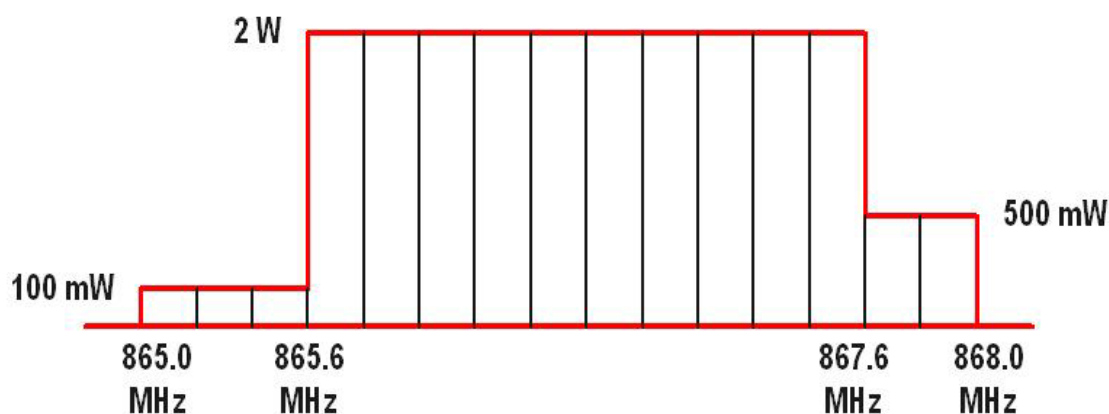


Figura 2.88 Potencia radiada equivalente permitida por la norma EN 302 208.

Dentro de estas ventajas que proporciona la EN 302 208 también existen ciertas condiciones para el uso general de RFID en Europa. Una de ellas es el modo de trabajo que deben tener las etiquetas: “listen before talk”, es decir, el tag deberá permanecer en modo ‘idle’ hasta que el lector no le solicite ningún tipo de información. Esto se puede considerar totalmente lógico si tenemos en cuenta que estamos tratando con etiquetas pasivas, las cuales no tienen una fuente de alimentación propia y, por lo tanto, deben optimizar la energía de la que disponen (campo magnético generado por el lector).

Otras de las condiciones que se incluyen dentro de esta norma de la ETSI son:

- El uso de sub-bandas de 200kHz
- Tiempo de escucha mayor de 5ms.
- Tiempo máximo continuado de transmisión de 4 segundos
- Una pausa obligada de 100ms entre transmisiones repetidas en la misma sub-banda o mover inmediatamente a otra sub-banda que esté libre la transmisión a realizar.

## 2.17 PRIVACIDAD

El uso de RFID está suscitando serias preocupaciones respecto de la protección de la vida privada de los ciudadanos por los nuevos riesgos que plantea para el ejercicio de sus derechos y libertades.

Es cierto que la utilización de esta nueva tecnología puede interferir en el ámbito de las libertades humanas más elementales como la libertad de movimiento, de acción, la dignidad y el libre desarrollo de la personalidad si no se tienen en cuenta, a la hora de implementar los sistemas, la legislación existente en materia de protección de datos.

Hay grupos que se movilizan en contra de la implantación de los sistemas RFID y que identifican los siguientes puntos como los principales riesgos que quedan implícitos en el uso de dichos sistemas.

- La elaboración indiscriminada de perfiles. Este riesgo es inherente a cualquier tecnología que permite recabar datos de carácter personal de forma masiva y ha sido desde los albores de la protección de datos, el objeto de todas las preocupaciones.
- La utilización de los RFIDs con fines de identificación y los problemas que pueda suponer la interceptación fraudulenta de datos y su posterior uso con fines distintos. En particular el problema del "robo de identidad" (*Identity theft*). Este problema ha aparecido estos últimos años en Estados Unidos. Hoy en día, esta figura delictiva se expande a medida de la implantación de las redes de voz IP, pudiendo constituir un problema de entidad para la Unión Europea si no se toman las medidas adecuadas.
- El desarrollo de técnicas de "rastreo" de los movimientos y/o actos realizados por la persona ("Tracking"). Esta tecnología permite localizar en cada momento a los individuos que lo llevan en su ropa, su coche, etc., permitiendo una vigilancia constante. Esta es una nueva característica de los tratamientos masivos de datos, que, más allá de la elaboración de los perfiles de personalidad, permite el seguimiento detallado de todos y cada uno de los pasos que da el individuo.
- La implantación de RFID en personas, que se está dando actualmente en el ámbito de la salud, tiene implicaciones éticas importantes.

Por todo ello se hace necesario delimitar de forma precisa su uso, de acuerdo con los principios de protección de datos implementados tanto por la Directiva 95/46/CE como por la Directiva 2002/58/CE de la Unión Europea. Directivas que son aplicables a los tratamientos de datos de carácter personal (y, por lo tanto, aplicables a RFID pues la diferencia estriba hoy en día en el tipo de soporte utilizado para recabar la información).

La cuestión principal es plantearnos si se hace necesaria la elaboración de unas instrucciones específicas por las Autoridades de Control que guíen la aplicación de sus legislaciones a este tema mientras se estudie, desde la Comisión Europea, la necesidad de elaborar una legislación específica que limite el alcance técnico de la tecnología

RFID, y el de otras tecnologías que en el futuro pudieran aparecer para cumplir iguales finalidades: recabar y tratar información (en el caso que nos ocupa, datos de carácter personal), previniendo en lo posible el amplio abanico de posibilidades que se ofrecen, y respetando en todo caso la legislación específica existente en materia de protección de datos.

## **3. MEMORIA**

### **3.1 *Introducción***

En los apartados que tenemos a continuación vamos a sentar las bases y las aplicaremos para conseguir el diseño de un lector de RFID que pueda ser compatible con etiquetas del tipo EPC Clase 1.

Lo primero que tendremos que hacer para poder lograr una correcta comunicación entre el lector y la etiqueta será seguir las especificaciones de las etiquetas en lo que al ámbito RF respecta. Así veremos qué tipo de modulación será la usada, los tiempos y velocidades de transmisión necesarios para tener éxito en la comunicación y otros aspectos que afectan a este ámbito.

Una vez hayamos seguido estas especificaciones, deberemos ver como trasladamos estas instrucciones a un hardware que las soporte, es decir, deberemos escoger un chip que nos permita implementar físicamente las especificaciones a seguir y una placa donde pueda funcionar de un modo sencillo y cómodo y, finalmente, deberemos entablar una comunicación que permita controlar todo este sistema, por lo que deberemos tener un sistema que controle nuestro sistema RFID (inicialmente un PC), deberemos poder comunicar el sistema de control con el sistema que hemos diseñado y deberemos saber qué comandos debemos usar para poder establecer una ‘conversación’ entre el lector y las etiquetas que se encuentren en su área de interrogación.

Una vez tengamos ya el sistema diseñado, vamos a simular como serían las señales en el canal wireless. Para ello usaremos un software de simulación propiedad de ROHDE & SCHWARZ: el WinIQSim. Este software simulará las señales en banda base (la única diferencia con la señal original sería la de trasladarla en frecuencia hasta la banda UHF) y permitirá añadirle distorsiones que provoca el canal wireless como son interferencias por culpa de señales multicamino o ruido blanco gaussiano.

### 3.2 *Parámetros de diseño del sistema*

Para poder diseñar el lector de etiquetas EPC Clase 1, lo primero que debemos fijar son los parámetros de diseño que nos marcan las especificaciones (*860MHz–930MHz Class I Radio Frequency Identification Tag Radio Frequency & Logical Communication Interface Specification Candidate Recommendation, Version 1.0.1*) de las etiquetas para, así, asegurarnos que la comunicación se realiza de un modo correcto.

Las especificaciones de las etiquetas EPC Clase 1 nos indican que estas tienen un rango de frecuencia desde los 860 a los 930 MHz. En nuestro caso vamos a elegir un rango más restrictivo, el que nos marca la especificación EN 302 208, donde el rango de frecuencias se reduce de los 865 a los 868 MHz, de modo que un sistema RFID no interfiera en la red GSM de telefonía móvil. Esta norma de la ETSI establece que la comunicación deberá establecerse en subbandas de 200KHz, hallándose la de frecuencia más baja en los 865,1MHz.

En las especificaciones también vemos que el rango de lectura que nos permite la norma EPC es de 2m en el peor de los casos y no más de 10m en el mejor de los casos. En este aspecto seremos cautos debido a que no tenemos una implementación física real de nuestro sistema, aunque se puede intuir que el rango que el lector que diseñaremos será mayor debido a que en este aspecto seguiremos las especificaciones del EN 302 208, el cual permite una potencia máxima de transmisión del lector de 2W, lo que aumenta el rango de lectura.

La comunicación se realizará en modo Half-Dúplex. El lector iniciará la comunicación modulando un paquete completo de datos y, una vez lo haya transmitido, deberá seguir emitiendo una señal continua sin modular (*continuous wave – CW*). Esta señal será la que aproveche la etiqueta para transmitir.

La modulación usada será una FSK, de frecuencias  $f_1=865\text{MHz}$  y  $f_2=865,2\text{MHz}$ , de manera que cumpliremos con las especificaciones ya que, siguiendo la ecuación 3.1:

$$f_{\text{CR}} = \frac{f_1 + f_2}{2} \quad \Delta f_{\text{CR}} = \frac{|f_1 - f_2|}{2} \quad (3.1)$$

Vemos que la frecuencia central queda en 865,1MHz, el mínimo que marcan las especificaciones y, lo más importante, lo más alejada posible de GSM, de manera que evitamos cualquier tipo de interferencia con la red de telefonía móvil.

La tasa de transferencia que vamos a usar, de todos modos, será de 15Kbps. A pesar que la capacidad del canal es mucho mayor (200Kbps si aplicamos el teorema de Nyquist), usaremos la que marca las especificaciones. Teniendo en cuenta que la tasa de transferencia podemos obtener de ahí el tiempo de bit:  $6,67\mu\text{s}$  (ya que  $T_0=1/T_1$ ).

El tiempo de salto entre un comando y otro viene definido por la especificación EPC y es de  $83,33\mu\text{s}$  ( $T_{\text{gap}}=1,25*T_0$ ), mientras que el tiempo que se tiene que esperar entre un [EOF] y el tiempo de 'gap' es de 20ms ( $T_{\text{coast}}$ ) como máximo.



Una forma de conseguir resetear los tags que se encuentran en el área de interrogación es disminuir la potencia de transmisión que emite el lector, de manera que sería un proceso similar al de mover los tags fuera del área de interrogación. El tiempo que se tiene que disminuir la potencia para poder resetear los tags  $T_{\text{reset}}=200\mu\text{s}$ .

Seguiremos definiendo los parámetros a partir de los diferentes elementos de los que consta:

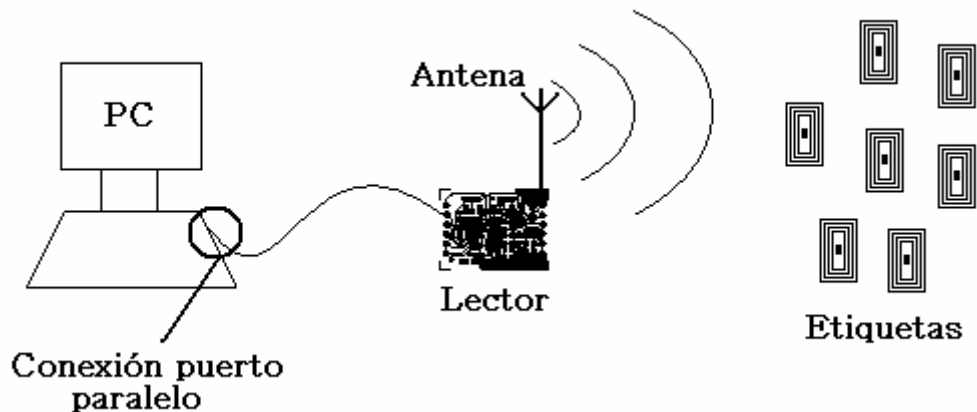


Figura 3.1 Esquema del diseño realizado

Ya hemos hablado de las etiquetas (EPC Clase 1), lo que nos marca unas condiciones que nos restringen en muy alta medida el diseño del interfaz del hardware.

Para poder implementar el sistema hemos elegido, de todos los disponibles, un chip de la marca Chipcon. El modelo es el CC1000 y sus características serán explicadas en un apartado posterior.

Básicamente la elección de este chip se basa en dos motivos:

- Primero porque incorpora en sus especificaciones una placa de evaluación con pocos componentes y que se ajusta totalmente al propósito de nuestro sistema ya que es capaz de modular en FSK usando una codificación Manchester, NRZ o sin codificación.
- Segundo porque la intención inicial del proyecto era desarrollar la placa y el hecho de haber conseguido una muestra gratuita por gentileza de la empresa que distribuye los productos Chipcon en España (Matriz Electrónica) nos ayudó a decidirnos por este chip.

La conexión entre el PC y la placa que usaremos se realiza usando un puerto paralelo debido a la necesidad de tener varios puntos de salida de datos para poder configurar la placa y poder transmitir los datos deseados. Entraremos en más detalle en apartados posteriores.

Como puerta a la transmisión de datos, nos hemos enfrentado a la elección de una antena adecuada para nuestros propósitos. Esta elección ha sido trivial y sencilla, ya que un sistema de las características de nuestro proyecto necesita una antena omnidireccional, con una ganancia relativamente buena y una impedancia de  $50\Omega$ . Por eso nos hemos decantado por un dipolo a  $\lambda/4$ , siguiendo las especificaciones que tenemos de la placa a implementar. Así, el tamaño de nuestra antena será:

$$\lambda = \frac{c}{f} = \frac{3 \cdot 10^8}{865,1 \cdot 10^6} = 0,3467\text{m} \Rightarrow \lambda/4 = 0,087\text{m} \quad (3.2)$$

siendo  $c$  la velocidad de la luz ( $c=3 \cdot 10^8\text{m/s}$ ) y  $f$  la frecuencia de la señal.

Finalmente, como nexo de todos los puntos de diseño, hemos tenido que realizar una descripción a muy alto nivel del software usado para poder controlar todo el sistema. Al igual que todos los puntos de diseño, este punto viene más detallado en un apartado posterior.

### 3.3 Las etiquetas: EPC Clase 1

A continuación vamos a describir los comandos que se ejecutan entre el lector y las etiquetas que hemos elegido para nuestro sistema: EPC clase 1.

Las etiquetas de clase 1 se comunican usando una señal *backscatter* sin modular a no ser que un comando que provenga del lector le indique lo contrario. En nuestro caso no usaremos ningún tipo de modulación en ningún momento para simplificar el sistema.

Para poder comprender mejor las etiquetas veremos como son los datos que contienen, como es la comunicación lógica entre el lector y la etiqueta para poder obtener un correcto funcionamiento del sistema.

#### 3.3.1 Estructura y contenido de los datos de una EPC Clase 1

Una etiqueta EPC Clase 1 contiene un identificador único, un código de detección de errores para el identificador único y un pequeño password como su único contenido de datos externos. El identificador único debe ser un código EPC válido. El código de detección de errores para el identificador único será un código CRC (Código de Redundancia Cíclica). Para el password que representa el contenido de datos externos, no existen restricciones por lo que podemos rellenarlo como más nos interese.

Los datos que encontramos en una etiqueta están almacenados en la Memoria de la Etiqueta Identificadota (*ITM – Identifier Tag Memory*). La organización lógica de la ITM es la de una memoria lineal con el bit de más peso (*MSB – Most Significant Bit*) del CRC situado en la posición de memoria cero (0). El bit de menor peso (*LSB – Least Significant Bit*) está seguido del MSB del código EPC. El LSB del código EPC está seguido del MSB del password, cuyo LSB ocupa la última posición de la ITM.



Figura 3.2 Contenido y organización de la Memoria de la Tarjeta Identificadota (ITM).

### Código EPC

Los diferentes códigos EPC existentes en el mundo son definidos por el Auto-ID Center, por lo que se tiene que solicitar estos códigos a EPCGlobal Inc.

Todos los códigos EPC contienen 4 partes: versión, fabricante, clase de objeto y número de serie, ordenados en este orden de MSB a LSB. Así el MSB del código EPC es el MSB del número de versión.

## CRC

El CRC es calculado con todo el código EPC, siendo el MSB el primer bit en entrar en el algoritmo que calcula el CRC. Para EPC's de menores o iguales que 256 bits se usa el CRC-CCITT, lo que nos proporciona un CRC de 16 bits.

## Password

El Password es un string de datos de 8 bits usado por el comando KILL, explicado a continuación. Aún así, puede tener alguna aplicación extra, dependiendo de cómo se programe el software que controla el sistema.

### 3.3.2 Comunicación lógica entre el lector y la etiqueta EPC

La comunicación entre el lector y la etiqueta ocurre de un modo 'empaquetado', de manera que un simple paquete contiene un comando completo proveniente del lector o una completa respuesta proveniente de la etiqueta. El comando y la respuesta permiten una comunicación Half-Dúplex entre el lector y la etiqueta. Los comandos que provienen del lector permiten la selección de la etiqueta basándose en el CRC y el código EPC.

### Paquetes de comunicación lector-etiqueta

Un paquete completo desde el lector hacia la etiqueta consiste en ocho campos y cinco bits de paridad entre esos campos. Los campos y los bits de paridad tienen el siguiente formato:

[PREAMBL][CLKSYNC][SOF][CMD][P<sub>1</sub>][PTR][P<sub>2</sub>][LEN][P<sub>3</sub>][VALUE][P<sub>4</sub>][P<sub>5</sub>][EOF]

Cada campo y bit de paridad de los comandos del lector son descritos a continuación:

CAMPO BÁSICO DE COMANDO	NÚMERO DE BITS	DESCRIPCIÓN DEL CAMPO
[PREAMBL]	NA	Cada comando viene fijado por un periodo de no transmisión por parte del lector.
[CLKSYNC]	20	Cada comando es prefijado por una serie de 20 ceros binarios para conseguir una apropiada sincronización entre el tag y lector. La circuitería de sincronización usada en la etiqueta usa esta parte del mensaje para establecer su propio reloj de lectura/decodificación y de las respuestas.
[SOF]	1	<i>Start of frame</i> – Marca el inicio de la transmisión de datos por parte del lector. Es un uno binario.
[CMD]	8	Especifica el comando enviado por parte del lector.
[P <sub>1</sub> ]	1	Paridad impar del campo [CMD]

[PTR]	8*	Puntero a una localización (o índice de bit) en el identificador del tag. El índice del bit empieza en el MSB (el valor del [PTR] será cero) y acaba en el LSB. Dependiendo del valor del [PTR], podrá tener 8 bits (para valores menores que 254), 2 bytes (valores entre 255 y 510), etc. [PTR] es el punto de partida para empezar búsquedas de valor especificado en el campo [VALUE].
[P <sub>2</sub> ]	1	Paridad impar del campo [PTR].
[LEN]	8*	Longitud de los datos enviados en el campo [VALUE]. Dependiendo del valor de [VALUE], podrá tener 8 bits (para valores menores que 254), 2 bytes (valores entre 255 y 510), etc. El campo [LEN] debe ser mayor que cero.
[P <sub>3</sub> ]	1	Paridad impar del campo [LEN]
[VALUE]	Variable	Puede variar dependiendo de si estamos transmitiendo el comando <i>ScrollID</i> , <i>PingID</i> , <i>Quiet</i> , <i>Talk</i> o <i>Kill</i> . Estos son los datos que la etiqueta debe encontrar en su identificador (desde [PTR] hasta el LSB). El tag no tendrá en cuenta ningún valor que se encuentre en los últimos 8 bits (password). En el comando <i>ProgramID</i> , este es el valor programado dentro de la ITM.
[P <sub>4</sub> ]	1	Paridad impar del campo [VALUE].
[P <sub>5</sub> ]	1	Paridad impar de los bits de paridad.
[EOF]	1	<i>End of frame</i> - Indica el fin de la transmisión de datos por parte del lector. Es un uno binario

Tabla 3.1 Campos de un paquete de transmisión lector-etiqueta

### Comandos Lector-Etiqueta

Los comandos que el lector envía a la etiqueta se pueden dividir en comandos de requerimiento y comandos de programación del identificador. La etiqueta debe implementar los comandos de requerimiento, mientras que los de programación de identificador depende del tipo de ITM que tenga el tag.

Los comandos de requerimiento del lector a la etiqueta y su correspondiente respuesta, si la hay, son:

Comando	Código comando (de MSB a LSB)	Respuesta del tag
ScrollAllID	0011 0100	ScrollID
ScrollID	0000 0001	ScrollID
PingID	0000 1000	PingID
Quiet	0000 0010	Ninguna
Talk	0001 0000	Ninguna
Kill	0000 0100	Ninguna

Figura 3.3 Comandos de requerimiento del lector a la etiqueta y su respuesta, en el caso de que exista.

Los comandos de programación del identificador y su correspondiente respuesta, si la hay, son:

Comando	Código comando (de MSB a LSB)	Respuesta del tag
ProgramID	0011 0001	Ninguna
VerifyID	0011 1000	VerifyID
LockID	0011 0001*	Ninguna
EraseID	0011 0010	Ninguna

Figura 3.4 Comandos de programación de identificador y su correspondiente respuesta, si existe.

Una etiqueta EPC Clase 1 interpretara los comandos que no aparecen en las figuras anteriores como comandos desconocidos y, por lo tanto, no cambiará su estado si los recibe.

Vamos a ver en que consiste cada comando:

- *ScrollAllID*: Todos los tags responden enviando un preámbulo de ocho bits, seguido del CRC (enviando el MSB primero) y a continuación su código de ID entero (MSB del identificador primero).
- *ScrollID*: Tags que tengan el campo [VALUE] empezando donde marca [PTR] responden enviando un preámbulo de ocho bits, seguido del CRC (enviando el MSB primero) y a continuación su código de ID entero (MSB del identificador primero).
- *PingID*: Tags que tengan el campo [VALUE] empezando donde marca [PTR] responden enviando ocho bits de su identificador, empezando en [PTR]+[LEN].
- *Quiet*: Tags que tengan el campo [VALUE] empezando donde marca [PTR] entran en un modo de reposo durante el cual no responden a ningún comando. Este estado se mantiene hasta que el tag recibe un comando Talk o hasta que se desconecta de la alimentación (es decir, se aparta la etiqueta del área de interrogación) como mínimo un segundo y como máximo diez segundos. Cuando el lector manda un comando Quiet, debe mandar 7 ceros binarios después del campo [EOF] para que el tag ejecute esta instrucción.
- *Talk*: Tags que tengan el campo [VALUE] empezando donde marca [PTR] entran en un modo activo en el cual responden a los comandos que les llegan desde el lector. Este modo de operación se mantiene hasta que otro comando Quiet les llega o hasta que se desconecta de la alimentación (es decir, se aparta la etiqueta del área de interrogación) como mínimo un segundo y como máximo

diez segundos. Cuando el lector manda un comando Talk, debe mandar 7 ceros binarios después del campo [EOF] para que el tag ejecute esta instrucción.

- *Kill*: Los tags que contienen [VALUE] (consistiendo en el completo identificador del tag, el CRC y el password de 8 bits) al principio de [PTR]=0, son desactivados permanentemente y no responderán ni ejecutarán comandos provenientes del lector. Este comando de ‘autodestrucción’ dejará al tag inactivo para siempre.

La transmisión de un comando de programación de identificador debe venir precedida de un tiempo igual a  $8 \cdot T_0$  durante el cual la portadora del tag se encuentra inactiva (o desactivada). Los comandos de programación de identificador que hemos visto en la figura anterior cumplen las siguientes funciones:

- ProgramID: Todos los tags que reciban el comando ProgramID almacenan los datos de [VALUE] en [LEN] bits de la ITM empezando en la posición [PTR]. Este comando programa exactamente 16 bits. [LEN], por lo tanto, tiene un valor decimal de 16.

El campo [PTR] debe ser fijado con un valor múltiple de 16, empezando por cero (0, 16, 32, 48, 64, etc.) siempre que no exceda el tamaño de la ITM ya que, si esto sucede, será ignorado.

Si [PTR] apunta a los 8 últimos bits (es decir al MSB del password), los últimos 8 bits de [VALUE] deben estar fijados a cero (0x00), a no ser que la ITM esté bloqueada (ver comando LockID).

El lector debe mandar ceros lógicos después de [EOF] equivalentes a la duración del tiempo de programación (mínimo 30ms). La operación de programación se termina cuando el tag recibe un uno binario. De todos modos el lector debe transmitir, además siete ‘0’ binarios antes de mandar el ‘1’ que finaliza la programación para poder permitir que se borre la secuencia de programación del tag.

Después de recibir un comando ProgramID válido, el tag ejecutará las secuencias internas requeridas para programar la memoria.

- VerifyID: Todos los tags que reciben correctamente este comando, responden comunicando un preámbulo de 8 bits, seguido del CRC (enviando el MSB primero), seguido de su código de ID entero (empezando por el MSB) y acabando por el password (en este caso, también con el MSB como primer bit enviado). El comando VerifyID es ignorado por los tags que hayan ejecutado correctamente el comando LockID.

- **LockID:** Este comando previene al tag de cualquier posible modificación de sus datos (identificador, CRC o password). Concretamente se trata de un comando que es una versión del comando ProgramID. [PTR] debe contener el valor que apunta al MSB del password. [LEN] debe ser igual a un 16 decimal. Los últimos 8 bits de [VALUE] deben ser igual a 0xA5 (10100101).
- **EraseID:** El comando EraseID pone todos los bits de la ITM a cero. Este comando es ignorado por los tags que han ejecutado satisfactoriamente el comando LockID.

Los datos que contiene el campo [PTR] no tienen importancia a partir del momento en el cual el tag identifica el comando que tiene que ejecutar. [LEN] estará fijado a uno y [VALUE] será cero.

El lector debe mandar ceros lógicos después de [EOF] equivalentes a la duración del tiempo de programación (mínimo 30ms). La operación de programación se termina cuando el tag recibe un uno binario. De todos modos el lector debe transmitir, además siete '0' binarios antes de mandar el '1' que finaliza la programación para poder permitir que se borre la secuencia de programación del tag.

De todos modos existen restricciones en los comandos de programación de la etiqueta, ya que dependen del tipo de memoria usada. Si la memoria es de sólo lectura o si tenemos una memoria de una única escritura, tendremos unas importantes restricciones a la hora de poder ejecutar los comandos de programación.

### **Paquetes de comunicación Etiqueta-Lector**

Las etiquetas no mandan comandos al lector, simplemente ejecutan los que les manda el lector. Tan sólo 4 comandos por parte del lector requieren una respuesta: VerifyID, ScrollAllID, ScrollID y PingID. Los demás únicamente modifican el estado del tag.

#### *Respuesta a VerifyID:*

Las etiquetas que reciben el comando VerifyID responden con un paquete que sigue la siguiente estructura:

[PREAMBL][CRC][TAGID][PASSWRD]

Cada campo se describe a continuación:



CAMPO BÁSICO DE COMANDO	NÚMERO DE BITS	DESCRIPCIÓN DEL CAMPO
[PREAMBL]	8	El tag manda el valor FEh de MSB a LSB como preámbulo.
[TAGID]	Variable	El tag envía el valor de su código EPC de MSB a LSB
[CRC]	16*	El tag envía el CRC de su código EPC de MSB a LSB. Tiene una longitud de 16 bits para EPC's mayores de 256 bits.
[PASSWRD]	8	El tag envía el valor de su password de MSB a LSB.

Tabla 3.2 Respuesta a VerifyID

### Respuesta a ScrollID

Las etiquetas responden del mismo modo a los comandos ScrollID y ScrollAllID. Esta respuesta tiene el siguiente formato:

[PREAMBL][CRC][TAGID]

Cada uno de los campos se describe a continuación:

CAMPO BÁSICO DE COMANDO	NÚMERO DE BITS	DESCRIPCIÓN DEL CAMPO
[PREAMBL]	8	El tag manda el valor FEh de MSB a LSB como preámbulo.
[TAGID]	Variable	El tag envía el valor de su código EPC de MSB a LSB
[CRC]	16*	El tag envía el CRC de su código EPC de MSB a LSB. Tiene una longitud de 16 bits para EPC's mayores de 256 bits.

Tabla 3.3 Respuesta a ScrollID

Para que nos podamos hacer una idea más clara, la Figura 3.5 ilustra los bits enviados por una etiqueta en respuesta a un ScrollID:

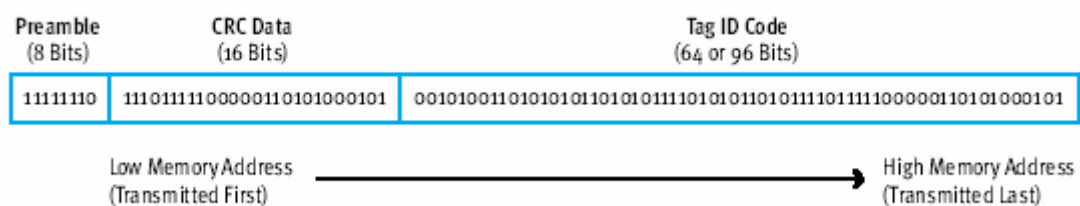


Figura 3.5 Datos transmitidos en respuesta a un comando ScrollID

### Respuesta al comando PingID

La etiqueta responde al comando del lector PingID con 8 bits. Estos 8 bits contienen la información almacenada en las 8 posiciones de memoria de la ITM empezando por [PTR]+[LEN] de MSB a LSB. Estos bits son los correspondientes al password.

La respuesta al PingID se envía en 8 ‘cajones’ de manera que cada bit de los mandados va en un ‘cajón’. Estos ‘cajones’ no son otra cosa que los periodos de bit que el lector asigna al tag para que responda. En la Figura 3.6 vemos como se distribuyen los ‘cajones’ (bins) en la respuesta:

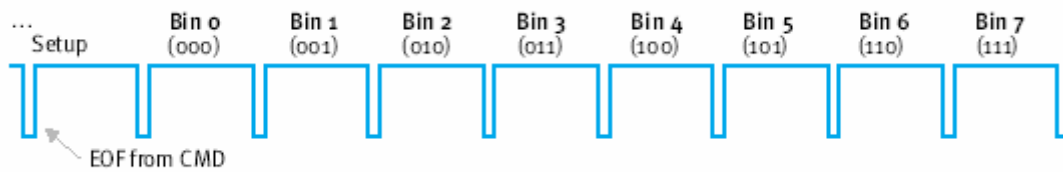


Figura 3.6 Así se distribuyen temporalmente los 8 bits de respuesta al PingID

### Fases de las señales lector-etiqueta

Hay cinco fases en la comunicación lector-etiqueta. La comunicación empieza con un periodo mínimo de  $1,25 \cdot T_0$  de inactividad, o tiempo de gap (primera fase), seguida por un periodo de  $64 \mu\text{s}$  de señal continua (CW, señal emitida no modulada). Esto sucede antes de la modulación (segunda fase). La primera y segunda fases comprenden el comando [PREAMBL] del lector. A partir de este momento el lector modula sus señales emitidas para comunicar los comandos que faltan a la etiqueta, lo que viene referido como Ventana de Modulación de Datos (la tercera fase). Un corto periodo de configuración (cuarta fase) permite que los tags interpreten los comandos y empiecen a ejecutarlos. Finalmente el lector vuelve a emitir una CW durante la cual los tags responden al comando recibido (quinta fase).

La respuesta del tag puede ser una señal continua (CW) o una modulación binaria. Esta modulación binaria la usaremos tan sólo durante el intervalo de respuesta del tag al comando PingID, el cual especifica los ‘cajones’ en los cuales tiene que responder el tag.

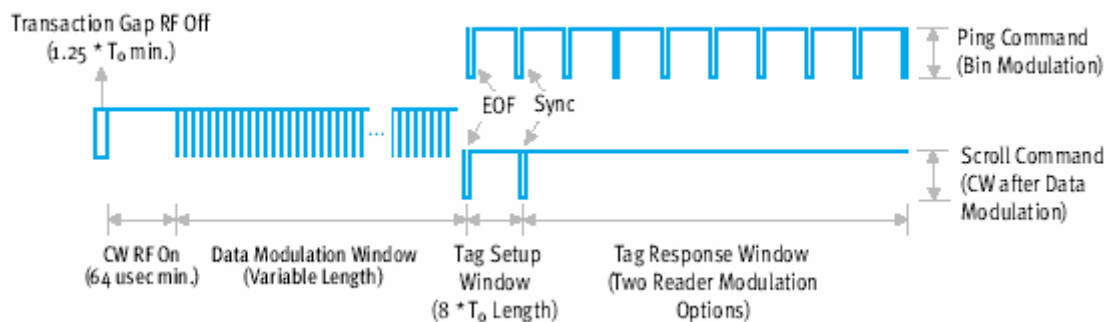


Figura 3.7 Esquema general de la modulación de la señal del lector a la etiqueta

Todas las operaciones empiezan con un ‘gap’,  $T_{\text{gap}}$ , seguido por un mínimo de  $64 \mu\text{s}$  de onda continua (CW) precediendo a la Ventana de Modulación de Datos.

Al principio de la modulación de los datos, el lector provee una señal de reloj maestra para las etiquetas. Este es el periodo [CLKSYNC] del comando que envía el lector.

Una vez se acaba de transmitir la señal de comando, la etiqueta debe estar preparado para recibir el próximo tiempo de gap antes de  $2,5 \cdot T_0$  y ser capaz de detectar un tiempo de gap recibido durante el intervalo  $T_{\text{coast}}$ .

Es necesario que para que la etiqueta sea capaz de detectar el ‘gap’ que hay después de un comando y que precede al siguiente, el lector debe empezar la siguiente transmisión dentro del tiempo  $T_{\text{coast}}$ . Esta restricción no se aplica cuando la portadora ha sido desconectada durante suficiente tiempo como para que la etiqueta pierda su alimentación y se re-sincronice cuando vuelva a ser alimentada.

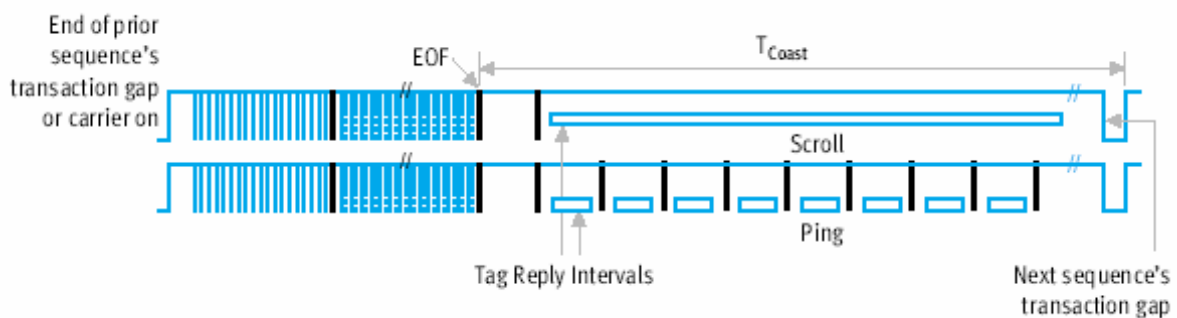


Figura 3.8 Representación gráfica de  $T_{\text{coast}}$

### ***Fases de las señales etiqueta-lector***

Podemos definir unos parámetros que tienen una elevada importancia en la comunicación tag-lector.

El reloj maestro que guía todo el proceso de comunicación de la etiqueta es el mismo que le proporciona el lector ( $T_0=6,67\mu\text{s}$ ), pero si tenemos en cuenta que en la etiqueta el periodo de bit es la mitad que en la transmisión del lector a la etiqueta, obtenemos una tasa de transferencia de 30Kbps. También quedan definidos los tiempos de retardo que se permiten para poder responder a los comandos ScrollID y PingID; este tiempo es de  $267\mu\text{s}$  ( $4 \cdot T_{0\text{max}}$ ). Lo que se mantiene constante en ambos casos (lector-etiqueta, etiqueta-lector) es el  $T_{\text{coast}}$ , que vale 20ms.

### **Retraso de la respuesta al comando ScrollID**

El retraso que debe haber entre un comando ScrollID o VerifyID ( $T_{\text{tagscrollDel}}$ ) se ilustra en la figura que tenemos a continuación:

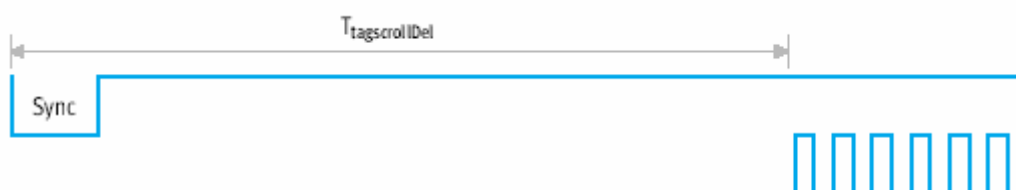


Figura 3.9 Retraso en la respuesta a ScrollID o VerifyID

### Duración de la respuesta del comando ScrollID

La duración de la respuesta es ilustrada en la Figura 3.10:



Figura 3.10 Duración de la respuesta al ScrollID desde el tag al lector

### Retardo de la respuesta al comando PingID

El retraso de un pulso binario al principio de una respuesta al comando PingID es ilustrado en la Figura 3.11:

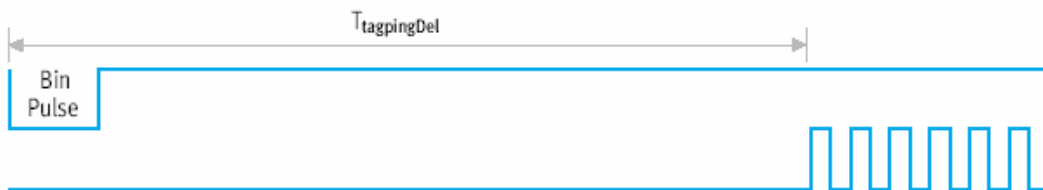


Figura 3.11 Retraso en la respuesta al comando PingID

### 3.4 CHIPCON CC1000

El Transceptor RF CC1000 de la marca CHIPCON, es el integrado que simularemos, básicamente realiza la operación de transmisión y recepción de datos en la frecuencia de RF.

El CC1000 es un chip diseñado para aplicaciones de poca potencia y de pequeño voltaje. Esta basado en la tecnología 0,35 $\mu$ m CMOS. Esta especialmente diseñado para sistemas que usan la modulación FSK y para operar en los rangos de frecuencia de ISM (Industrial, Scientific and Medical) y SRD (Short Range Device), 315, 433, 868 y 915 MHz. Pero es fácilmente programable para operar en otras frecuencias, entre 300-1000 MHz.

Es un chip que puede ser usado conjuntamente a un microcontrolador y pocos componentes externos pasivos. Ente sus características principales destacan un bajo consumo de corriente, una alta sensibilidad, operar con un bajo voltaje que hace posible su utilización con una pila (3 V), su pequeño tamaño, unas velocidades de transmisión superiores a 78,6 kbps.

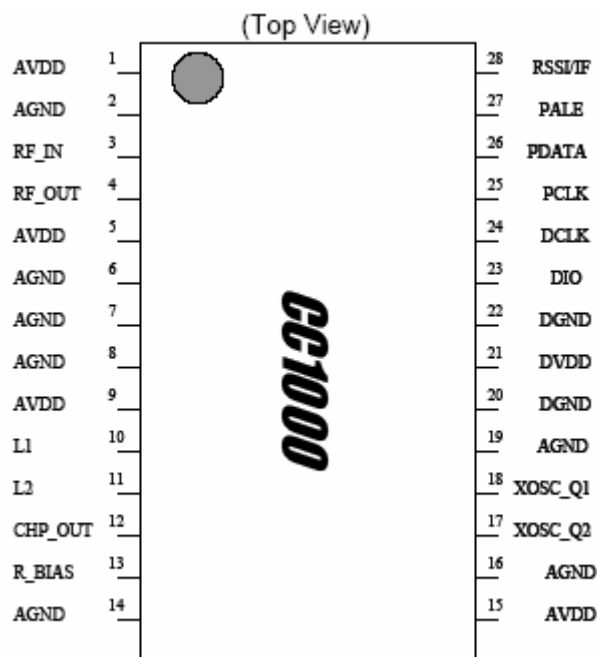


Figura 3.12 Pins del chip CC1000 (En el Anexo 1 aparece la asignación de los pins)

## Descripción del circuito

Podemos observar en la figura 3.13 el diagrama de bloques el funcionamiento del CC1000:

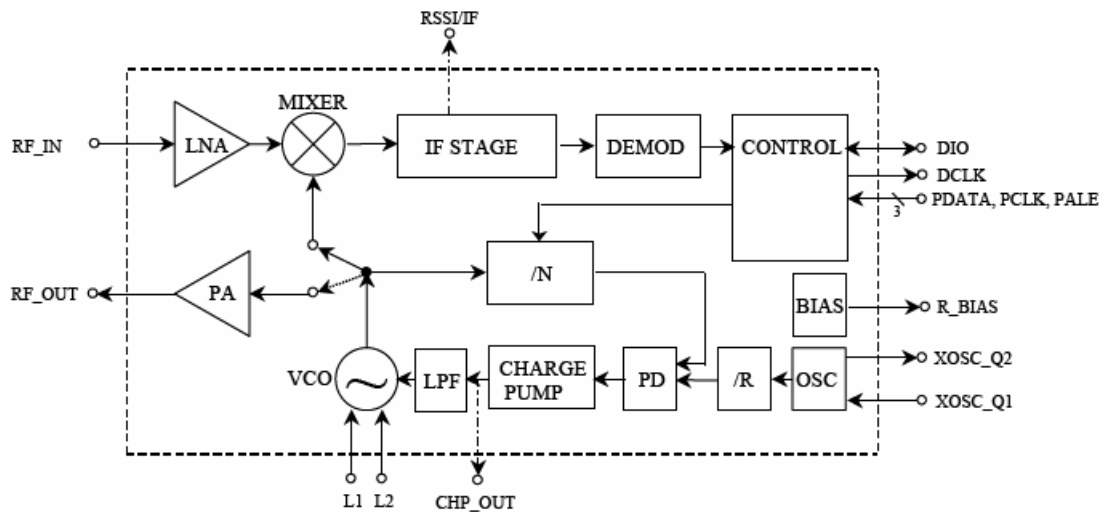


Figura 3.13 Diagrama de bloques simplificados del CC1000

En modo recepción el CC1000 actúa como un receptor superheterodino tradicional. La señal RF de entrada es amplificada por el LNA (Low-Noise Amplification) y bajada de frecuencia por el mezclador que convierte la frecuencia de la señal de entrada a frecuencia intermedia (IF). Después la señal es amplificada y filtrada antes de entrar en el demodulador. Como una opción, existe la posibilidad de extraer la señal antes de ser enviada al demodulador por el pin RSSI/IF. Después de la demodulación los datos se extraen mediante el pin DIO. La sincronización se realiza en el chip mediante el pin DCLK.

En el modo de transmisión la señal del VCO (Voltage Controlled Oscillator) es amplificada por el PA (Power Amplification). La salida RF está modulada en FSK (Frequency Shift Keyed) por el flujo de bits introducidos por el pin DIO.

El sintetizador de frecuencia genera la señal del oscilador local es enviada al mezclador en modo recepción y al amplificador de potencia (PA) en modo de transmisión. El sintetizador de frecuencia consiste en un oscilador de cristal (XOSC), detector de fase (PD), Charge pump, VCO y divisores de frecuencia (/R y /N). El cristal externo debe conectarse al XOSC, y solo se requiere un inductor externo para el VCO. El interfaz de tres entradas digitales (CONTROL) es usado para la configuración.

Como hemos comentado pocos son los componentes exteriores que necesita este chip para funcionar, lo podemos ver en la figura 3.14

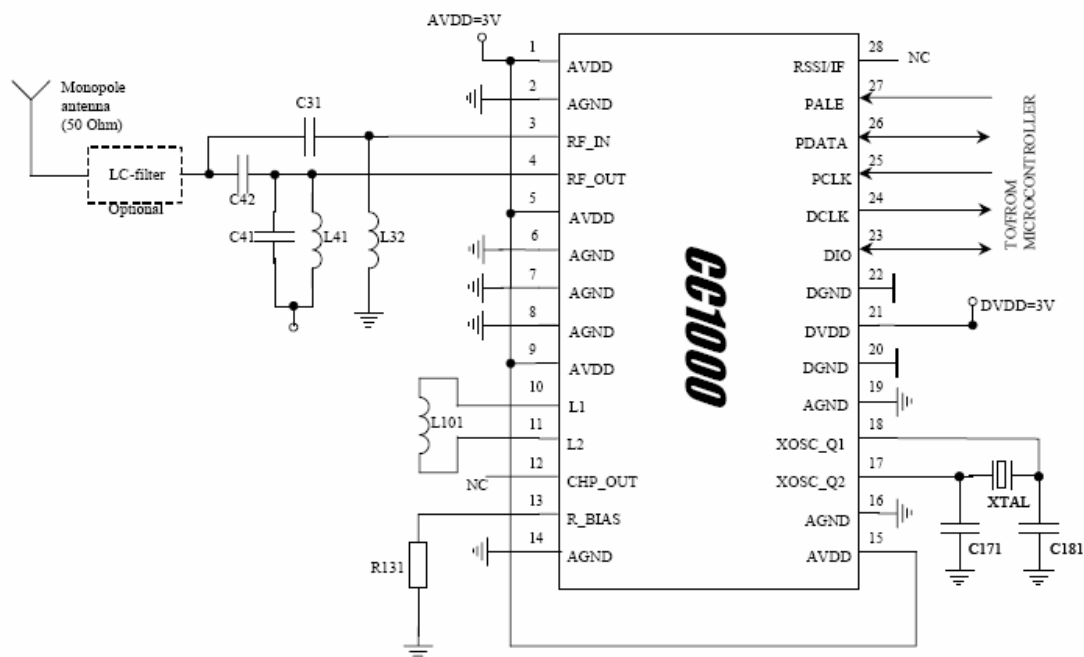


Figura 3.14 Típica aplicación del chip CC1000

Los componentes C31/L32 actúan en la señal de entrada, y C41, L41 y C42 son usadas para transmitir a 50Ω. Un conmutador interno T/R hace posible conectar la entrada y la salida conjuntamente y conectan el CC1000 a la antena de 50Ω. El inductor L101 en el VCO y el cristal de cuarzo XTAL.

Veremos, a continuación, algunas de las características más importantes a la hora de configurar este chip CC1000:

### Interfaz de configuración serie

Este chip ofrece la configuración de una interfaz de tres entradas/salidas (PDATA, PCLK y PALE). Hay 28 registros de 8 bits de datos cada uno y con 7 bits de direcciones. Un bit de Read/Write inicia la operación de lectura o de escritura.

La configuración total del CC1000 requiere el envío de 22 tramas de 16 bits cada una (7 bits direcciones, un bit de lectura/escritura y 8 bits de datos). El tiempo necesario para la configuración total depende de la frecuencia de PCLK. Por ejemplo para una frecuencia de 10 MHz, el tiempo sería menor a 46 μs. La configuración del diseño del CC1000 en la operación de lectura (power down mode) requiere el envío de una única trama que se realiza en un tiempo inferior a 2 μs para que todos los registros del chip sean leíbles, lo que permite una rápida lectura de datos de etiquetas cercanas.

En cada ciclo de escritura 16 bits son enviados por la entrada de PDATA. Los siete bits más significativos (A6:A0) de cada trama son los bits de dirección, el bit A6 es el MSB (Most Significant Bit) es el primer bit enviado. El siguiente bit es el bit de R/W, lectura/escritura, con nivel bajo si es lectura y con nivel alto si es escritura. Durante el envío de los bits de dirección y R/W la entrada PALE (Program Address

Latch Enable) debe permanecer en nivel bajo. Podemos verlo en la Figura 3.15. Los 8 bits siguientes (D8:D0) son los bits de datos.

El tiempo para la programación lo vemos también en la Figura 3.16 en referencia a los parámetros de la Tabla 3.4. Los tiempos para escribir en el chip mediante la entrada PDATA se realizan cuando la señal PCLK está en nivel bajo, en el momento que el último bit de datos D0 está cargado, la palabra de datos se carga en el registro con la dirección especificada.

En la operación de lectura se accede a los registros por la misma interfaz, primero se envían los bits de la dirección de memoria y el bit R/W en nivel bajo, entonces se envían los bits de datos del registro con esa dirección de memoria.

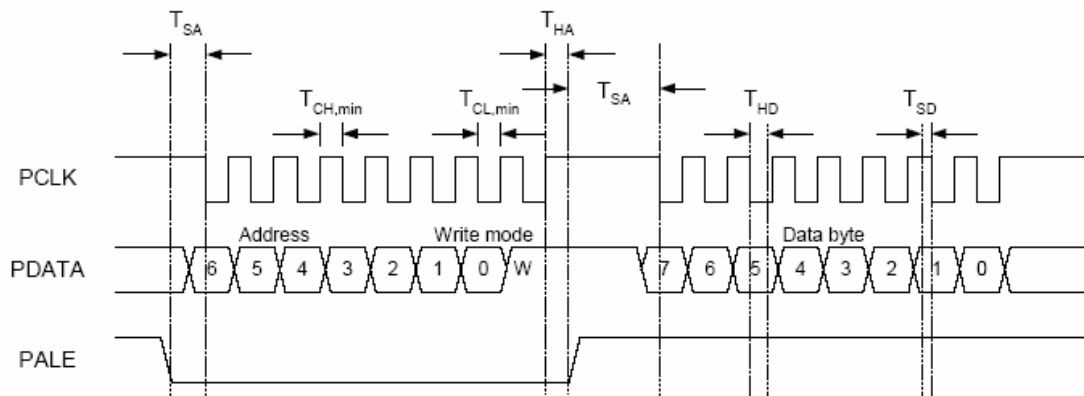


Figura 3.15 Procedimiento de escritura

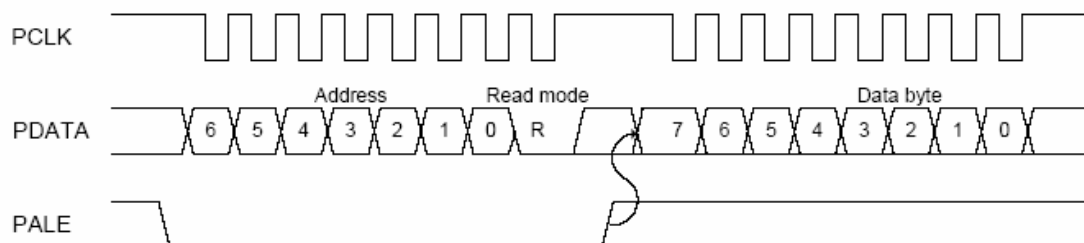


Figura 3.16 Procedimiento de lectura

## Interfaz Microcontrolador

Normalmente el CC1000 es usado con un microcontrolador que realiza las funciones de programar el chip en los diferentes modos mediante los tres pins entrada/salida de la configuración en serie (PDATA, PCLK y PALE). Además realiza funciones de interfaz bidireccional de la sincronización de la señal de datos (DIO y DCLK). Opcionalmente puede realizar la codificación/decodificación de los datos.

El microcontrolador usa 3 pins de salida para configurar el interfaz (PDATA, PCLK y PALE). PDATA es un pin direccional de lectura de datos. Un pin bidireccional es usado para los datos (DIO) que serán transmitidos y recibidos. DCLK produce el tiempo que se conecta a la entrada del microprocesador. Los pins del microcontrolador



conectados a PDATA y PCLD pueden ser utilizados con otros propósitos cuando el interfaz de la configuración no se usa. Podemos ver en la Tabla 3.x los pins en el modo power down.

Pin	Pin state	Note
PDATA	Input	Should be driven high or low
PCLK	Input	Should be driven high or low
PALE	Input with internal pull-up resistor	Should be driven high or high-impedance to minimize power consumption
DIO	Input	Should be driven high or low
DCLK	High-impedance output	

Tabla 3.4 Pins del CC1000 en el modo de lectura

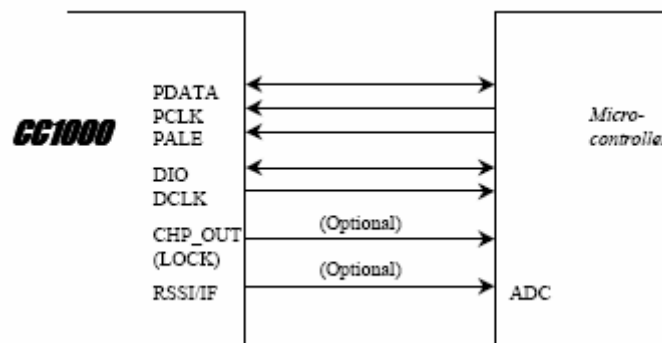


Figura 3.17 Interfaz con el microcontrolador

### Interfaz de señal

El interfaz de señal consiste en DIO y DCLK, y es usado para la transmisión y recepción de los datos. DIO es la línea de bidireccional de datos y DCLK produce un reloj síncrono durante la transmisión y recepción de datos.

El CC1000 puede usar las codificaciones NRZ (Non-Return-to-Zero) o Manchester. También puede sincronizar los datos desde el demodulador y proporcionar el reloj de los datos DCLK.

El CC1000 se puede configurar de tres formatos de datos distintos, dos síncronos los modos NRZ y codificación Manchester y uno asíncrono transparente denominado UART:

- Del modo síncrono NRZ, en transmisión CC1000 produce el reloj de los datos en DCLK y DIO es usado como entrada de datos. Los datos son modulados en RF sin codificación. En el modo de recepción el CC1000 realiza la sincronización y produce el tiempo de reloj de los datos recibidos en DCLK y los datos en DIO. Figura 3.18

- Del modo síncrono de codificación Manchester, en el modo transmisión el CC1000 crea el tiempo de reloj de los datos en DCLK y usa DIO como entrada de datos. Los datos se modulan con codificación Manchester en RF. En el modo de recepción el CC1000 crea la sincronización con el tiempo de reloj en DCLK y DIO es utilizado para la recepción de datos. Figura 3.19
- Del modo asíncrono, que es el modo escogido por nuestro sistema, se puede decir que en el modo de transmisión DIO es usado como entrada de datos. Los datos son modulados en RF sin modulación y sin codificación. En el modo de recepción la ráfaga de datos provenientes del demodulador son enviados a la salida. El pin DCLK se usa como salida de datos en este modo. Podemos verlo en la Figura 3.20

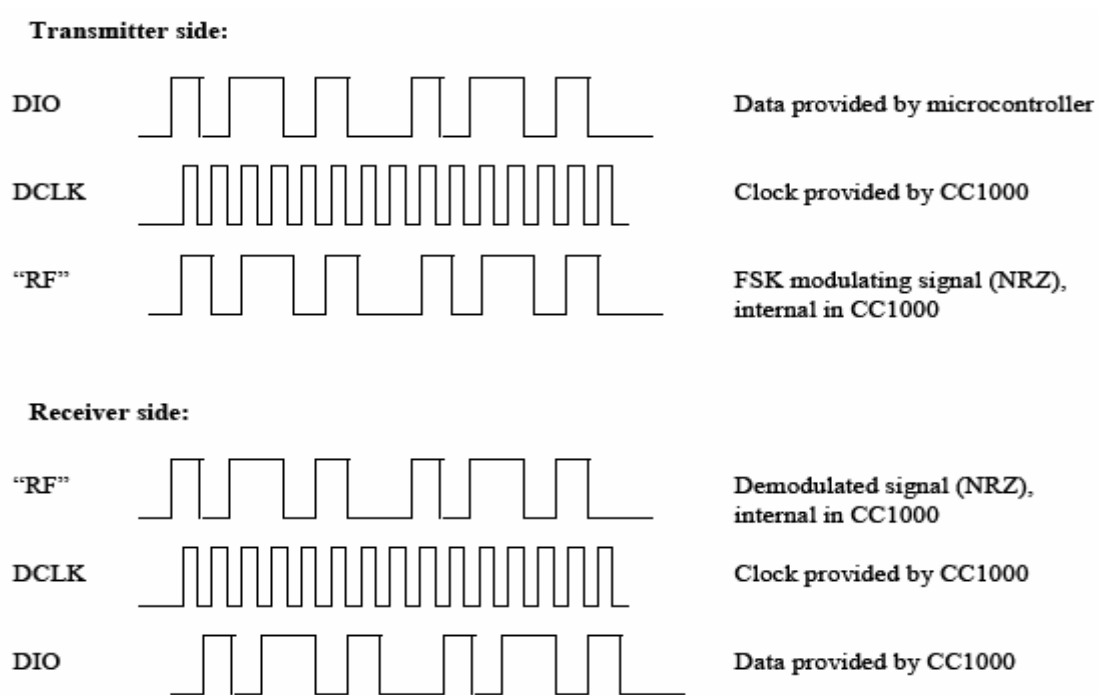


Figura 3.18 Modo síncrono NRZ

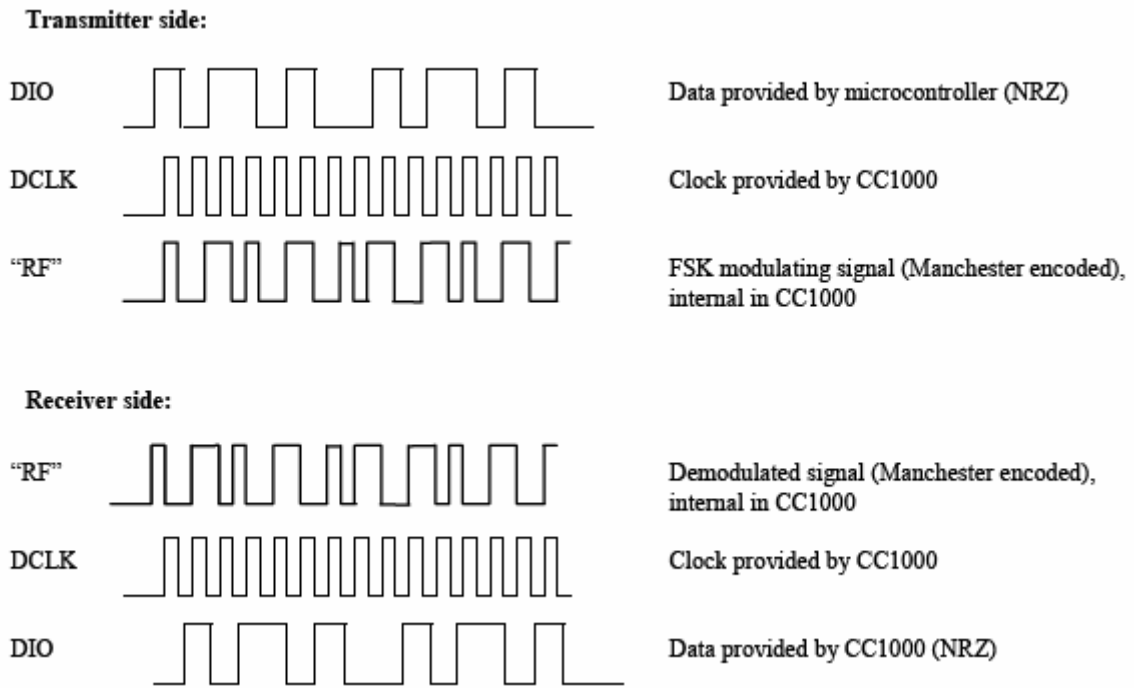


Figura 3.19 Modo síncrono codificación Manchester

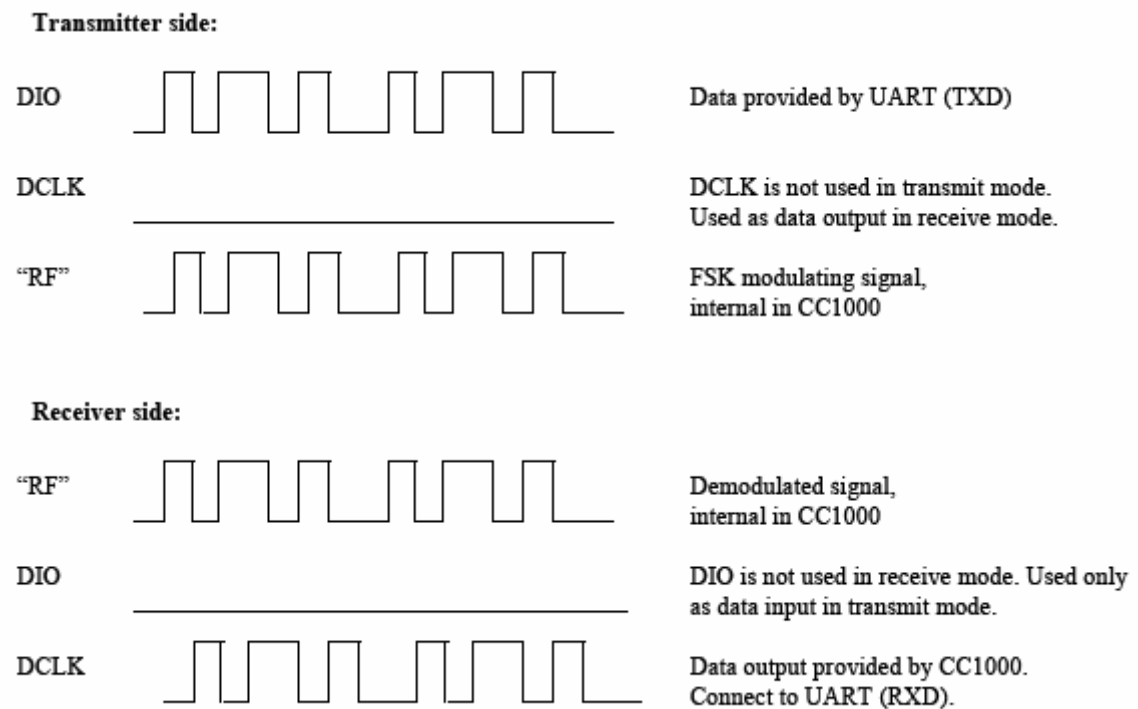


Figura 3.20 Modo asíncrono transparente UART.

### **Sensibilidad receptor**

La sensibilidad del receptor depende del formato de los datos, la velocidad de transmisión, separación frecuencia FSK y la frecuencia RF. Para optimizar la sensibilidad se usan varias configuraciones, como aumentar la separación entre frecuencias debe ser la más grande posible especialmente a velocidades de transmisión elevadas.

En el Anexo 1 encontramos diferentes configuraciones para obtener la sensibilidad del receptor.

### **Programador de frecuencia**

La frecuencia del sintetizador (PLL) es controlado por la palabra de frecuencia en los registros de configuración. Hay dos palabras de frecuencia A y B, las cuales pueden ser programadas en dos frecuencias distintas. Una de las palabras de frecuencia puede ser usada para Rx (frecuencia del oscilador local) y la otra palabra para Tx (frecuencia de transmisión  $f_0$ ). Esto es posible al cambiar rápidamente entre los modos de Tx y Rx.

### **VCO**

Para el correcto funcionamiento de correcto del VCO sólo requiere una bobina externa. El inductor determina el rango de frecuencia de operación del circuito. Es importante ubicar el inductor tan cerca de los pines como sea posible con el fin de reducir desviaciones en el valor de la inductancia. Es recomendable usar un alto valor de Q, y un inductor con baja tolerancia para un diseño óptimo.

### **Oscilador de cristal**

El chip CC1000 tiene un avanzado oscilador de cristal regulador de amplitud. Una elevada corriente se usa para comenzar las oscilaciones. Cuando la amplitud aumenta, el corriente se reduce lo que sea necesario hasta mantener los 600mVpp de amplitud. Esto asegura una rápida puesta en marcha y un mantenimiento del consumo de corriente en el mínimo posible.

Una señal externa de reloj o interna del oscilador de cristal puede ser usada como frecuencia de referencia. La frecuencia del cristal deberá estar en el rango de 3-4, 6-8 o 9-16 MHz. Debido a que la frecuencia del cristal es la usada como referencia en la transmisión de datos (además de otros procesos internos).

El cristal requiere de dos condensadores que añadidos al capacitador parásito, forman el capacitador total del cristal. El valor de la capacidad total de carga depende de la capacidad de carga especificado por el cristal.

La capacidad parásita esta constituida por la capacidad del pin de entrada y por la capacidad provocada por la PCB.

## Filtro LC

Tenemos la posibilidad de añadir un filtro LC, añadido en el kit CC1000PP de Chipcon del que hablaremos en el siguiente apartado, El filtro reduce la emisión de armónicos e incrementa la selectividad del receptor. Podemos ver la topología del filtro en la Figura 3.21 y los valores de los componentes según la frecuencia en la Tabla 3.5

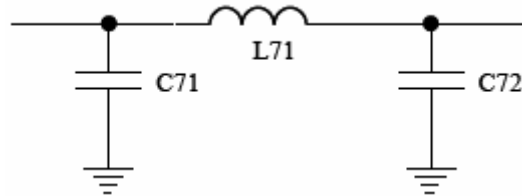


Figura 3.21 Filtro LC opcional

Item	315 MHz	433 MHz	868 MHz	915 MHz
C71	30 pF	20 pF	10 pF	10 pF
C72	30 pF	20 pF	10 pF	10 pF
L71	15 nH	12 nH	5.6 nH	4.7 nH

Tabla 3.5 Componentes del filtro según la frecuencia de operación.

### 3.5. CC1000PP Pulg. and Play Module

En nuestro diseño nos fijamos en el kit CC1000PP diseñado por la misma marca Chipcon como un layout de referencia y un prototipo de un sistema RF. Este kit incorpora, obviamente, el Chip CC1000.

El modulo CC1000PP contiene todos los componentes RF que se requieren para operar. Tiene un tamaño de (28x20 mm). El layout está basado en el económico 2-layer 1.6 mm, con el proceso FR-4 PCB. Los componentes están montados en una sola cara, la cara donde están situados los componentes es usada para guiar la señal y el reverso es usado como plano de masa.

En la Tabla 3.6 tenemos los valores típicos de ajuste para las diferentes frecuencias, en nuestro caso la frecuencia usada es 865,1 MHz con lo que podemos tener una idea de los parámetros en la frecuencia de 868 MHz.

Parameter	CC1000PP-433	CC1000PP-868		Unit
	433 MHz	868 MHz	915 MHz	
Sensitivity, 2.4 kBaud	-111	-107	-105	dBm
Output power, max	8	2.5	0.5	dBm
RF frequency accuracy	± 10	± 10	± 10	ppm
LO leakage	-68	-62	-59	dBm
2 <sup>nd</sup> harmonic	<-36	<-30	<-40 dBc	dBm
3 <sup>rd</sup> harmonic	<-30	<-30	<-40 dBc	dBm
Current consumption, TX	24	23	23	mA
Current consumption, RX	9.7	11.7	11.7	mA
Current consumption, PD	100	100	100	nA

Tabla 3.6 Parámetros típicos a 3V y 25° C.

#### Dimensiones mecánicas y emplazamiento de los componentes

El modulo CC1000PP mide 28x20 mm, y los componentes son montados en una sola cara, por lo que este modulo resulta pequeño y barato a la vez.

Al final de la placa existe una conexión de puerto paralelo para la comunicación con el PC. Podemos ver el dibujo de la PCB en la Figura 3.22

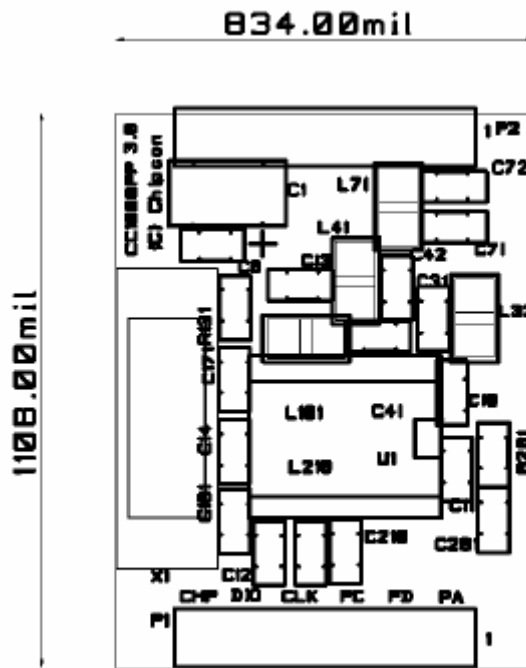


Figura 3.22 Modulo CC1000PP

Para asegurar el diseño optimo RF, la antena externa deberá estar soldada directamente a los terminales de la ante, o a una línea microstrip de 50Ω que deberá conectar el terminal de la antena con el conector externo de la antena.

### Diagrama del circuito

Para la frecuencia en la que trabajaremos tenemos el diagrama del Anexo II que opera en las bandas de 868 MHz y 902-928 MHz. Los valores de los componentes, el inductor VCO y el filtro LC dependerán de la frecuencia de operación.

Para entender los pins de salida para los conectores de la placa, tenemos la Tabla 3.7.

P1		P2	
Pin	Function	Pin	Function
1	PALE	1	GND
2	PDATA	2	ANTENNA
3	PCLK	3	GND
4	DCLK	4	VDD (2.1 – 3.6 V)
5	DIO	5	RSSI / IF
6	CHP_OUT / LOCK	6	GND

Tabla 3.7 Pins de conexión

## Layout

Los circuitos que trabajan a altas frecuencias son muy sensibles a las propiedades físicas de los diseños de las PCB. Por eso los componentes deben estar lo más próximos al chip posible. Podemos ver el diseño de la placa en la Figura 3.23

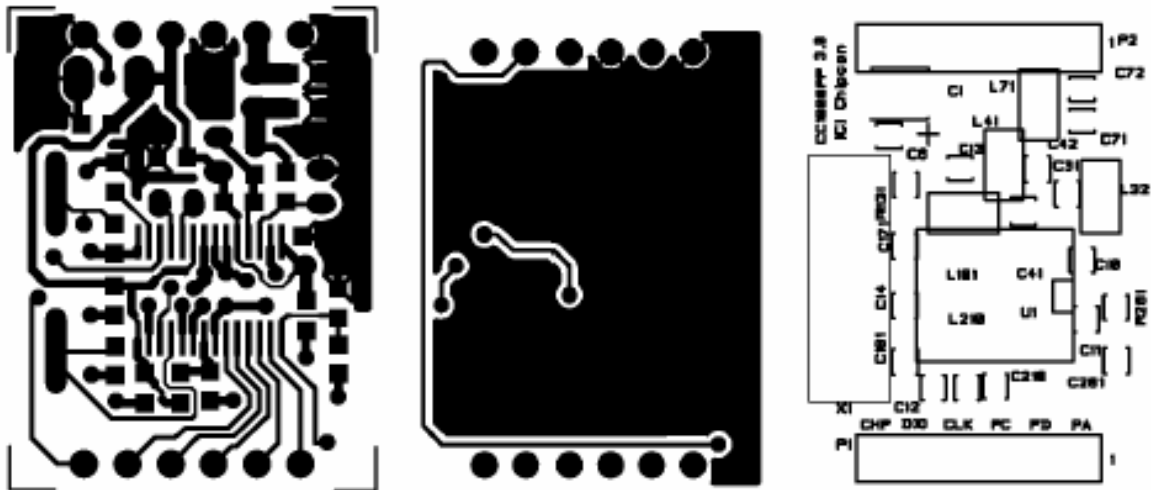


Figura 3.23 Parte superior e inferior del layout de la PCB y esquema de su diseño

## Antenas

El módulo CC1000PP puede usar conjuntamente cualquier tipo de antena. Si la impedancia de la antena no está cerca de los  $50 \Omega$ , se deben usar componentes para aproximar la impedancia a  $50 \Omega$ . Un dipolo  $\lambda/4$  puede ser usado directamente quitando los pines 1,2 y 3 de P2 y soldando una pieza de la longitud correcta. Esta es la opción que hemos tomado nosotros para nuestro diseño.

## Componentes

El kit monta unos componentes pasivos de bajo coste. El componente más crítico es el inductor que acompaña al VCO. Los demás capacitadores e inductores no son problemáticos a la hora de escoger su tolerancia. En la Tabla 3.8 vemos los valores para la frecuencia de 868 MHz.



<b>CC1000PP-868</b>			
<i>Reference</i>	<i>Description</i>	<i>Value</i>	<i>Part</i>
C1	Capacitor, tantal	3.3 $\mu$ F	C_3U3_TAN_B
C6	Capacitor 0603	33nF, 10%	C_33N_0603_X7R_K_25
C10	Capacitor 0603	12pF, 5%	C_12P_0603_NP0_J_50
C11	Capacitor 0603		Do not mount
C12	Capacitor 0603	1nF, 10%	C_1N0_0603_X7R_K_50
C13	Capacitor 0603	330pF, 5%	C_330P_0603_NP0_J_50
C14	Capacitor 0603	8.2pF, $\pm$ 0.25pF	C_8P2_0603_NP0_C_50
C31	Capacitor 0603	10pF, 5%	C_10P_0603_NP0_J_50
C41	Capacitor 0603		Do not mount
C42	Capacitor 0603	4.7pF, $\pm$ 0.25pF	C_4P7_0603_NP0_C_50
C71	Capacitor 0603	8.2pF, $\pm$ 0.25pF	C_8P2_0603_NP0_C_50
C72	Capacitor 0603	6.8pF, $\pm$ 0.25pF	C_6P8_0603_NP0_C_50
C171	Capacitor 0603	18pF, 5%	C_18P_0603_NP0_J_50
C181	Capacitor 0603	22pF, 5%	C_22P_0603_NP0_J_50
C210	Capacitor 0603		Do not mount
C281	Capacitor 0603	1nF, 10%	C_1N0_0603_X7R_K_50
L32	Inductor 0805	120nF, 5%	L_120N_0805_J
L41	Inductor 0805	2.5nH, 5%	L_2N5_0805_J
L71	Inductor 0805	5.6nH, 5%	L_5N6_0805_J
L101	Inductor 0805	4.7nH, 5%	L_4N7_0805_J, KOA KL732ATE4N7C
L210	EMI filter bead		BLM18HG102SN1D, Murata
P1	Pin-row connector		CON6_MALE
P2	Pin-row connector		CON6_MALE
R131	Resistor 0603	82k $\Omega$ , 1%	R_82K_0603_F
R281	Resistor 0603	27k $\Omega$ , 2%	R_27K_0603_G
U1	Single chip transceiver		CC1000
X1	Crystal, HC49-SMD		X14.7456MHz 10/10/10/16, (16pF load)

Tabla 3.8 Materiales para el diseño del CC1000PP a la frecuencia de 868 MHz.

### 3.6 El puerto paralelo

El puerto paralelo de un PC típico utiliza un conector hembra de tipo D de 25 patas (DB-25 S); esto está definido por el estándar **IEEE 1284**. El conector que usaremos es un **1284 tipo A**. El orden de las patas del conector es éste:

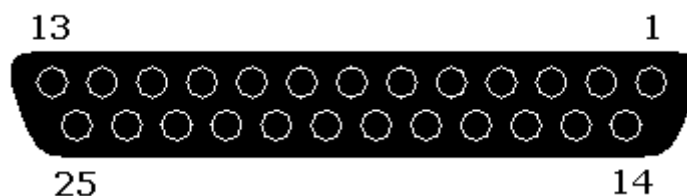


Figura 3.24 Orden de las patas de un conector 1284 tipo A, usado en el puerto paralelo

A continuación describimos la función de cada pata del conector. Hay que tener en cuenta que inicialmente el puerto paralelo fue diseñado por IBM para la gestión de impresoras. Así, podremos usar muchas de las salidas y entradas del puerto para nuestro propósito, sin tener en cuenta que la línea tenga un significado u otro.

Pata	E/S	Polaridad activa	Descripción
1	Salida	0	Strobe
2 ~ 9	Salida	-	Líneas de datos (bit 0/pata 2, bit 7/pata 9)
10	Entrada	0	Línea acknowledge (activa cuando el sistema remoto toma datos)
11	Entrada	0	Línea busy (si está activa, el sistema remoto no acepta datos)
12	Entrada	1	Línea Falta de papel
13	Entrada	1	Línea Select
14	Salida	0	Línea Autofeed
15	Entrada	0	Línea Error (si está activa, hay un error)
16	Salida	0	Línea Init
17	Salida	0	Línea Select input
18 ~ 25	-	-	Tierra eléctrica

Tabla 3.9 Configuración de los pins de un puerto paralelo 1284 Tipo A

Podemos observar que el puerto paralelo tiene 12 líneas de salida (8 líneas de datos, strobe, autofeed, init, y select input) y 5 de entrada (acknowledge, busy, falta de papel, select y error). El estándar IEEE 1284 define cinco modos de operación:

1. Modo compatible
2. Modo nibble
3. Modo byte
4. Modo EPP, puerto paralelo ampliado
5. Modo ECP, puerto de capacidad extendida

Aún así el único modo de funcionamiento que nos interesa para nuestros propósitos es el modo compatible, por lo que tan sólo nos fijaremos en este modo a lo largo de todo el apartado.

Existen tres direcciones de E/S asociadas con un puerto paralelo del PC, estas direcciones pertenecen al **registro de datos**, el **registro de estado** y el **registro de control**. El *registro de datos* es un puerto de lectura-escritura de ocho bits. Leer el registro de datos (en la modalidad unidireccional) retorna el último valor escrito en el registro de datos. Los registros de control y estado proveen la interfaz a las otras líneas de E/S. La distribución de las diferentes señales para cada uno de los tres registros de un puerto paralelo esta dada en las siguientes tablas:

Dirección	Nombre	Lectura/Escritura	Bit #	Propiedades
Base + 0	Puerto de datos	Escritura	Bit 7	Dato 7
			Bit 6	Dato 6
			Bit 5	Dato 5
			Bit 4	Dato 4
			Bit 3	Dato 3
			Bit 2	Dato 2
			Bit 1	Dato 1
			Bit 0	Dato 0

Tabla 3.10 Registro de datos

Dirección	Nombre	Lectura/Escritura	Bit #	Propiedades
Base + 1	Puerto de estado	Sólo Lectura	Bit 7	Busy
			Bit 6	Acknowledge
			Bit 5	Falta de papel
			Bit 4	Select In
			Bit 3	Error
			Bit 2	IRQ (Not)
			Bit 1	Reservado
			Bit 0	Reservado

Tabla 3.11 Registro de estado

Dirección	Nombre	Lectura/Escritura	Bit #	Propiedades
Base + 2	Puerto de control	Lectura/Escritura	Bit 7	No usado
			Bit 6	No usado
			Bit 5	Permite puerto bidireccional
			Bit 4	Permite IRQ a través de la línea acknowledge
			Bit 3	Selecciona impresora
			Bit 2	Inicializa impresora
			Bit 1	Nueva línea automática
			Bit 0	Strobe

Tabla 3.12 Registro de control

Un PC soporta hasta tres puertos paralelos separados, por tanto puede haber hasta tres juegos de registros en un sistema en un momento dado. Existen tres direcciones base para el puerto paralelo asociadas con tres posibles puertos paralelo: 0x3BCh, 0x378h y 0x278h, nos referimos a éstas como las direcciones base para el puerto **LPT1**, **LPT2** y **LPT3**, respectivamente.

El registro de datos se localiza siempre en la dirección base de un puerto paralelo, el registro de estado aparece en la dirección base + 1, y el registro de control aparece en la dirección base + 2. Por ejemplo, para un puerto LPT2 localizado en 0x378h, ésta es la dirección del registro de datos, al registro de estado le corresponde la dirección 0x379h y su respectivo registro de control está en la dirección 0x37Ah.

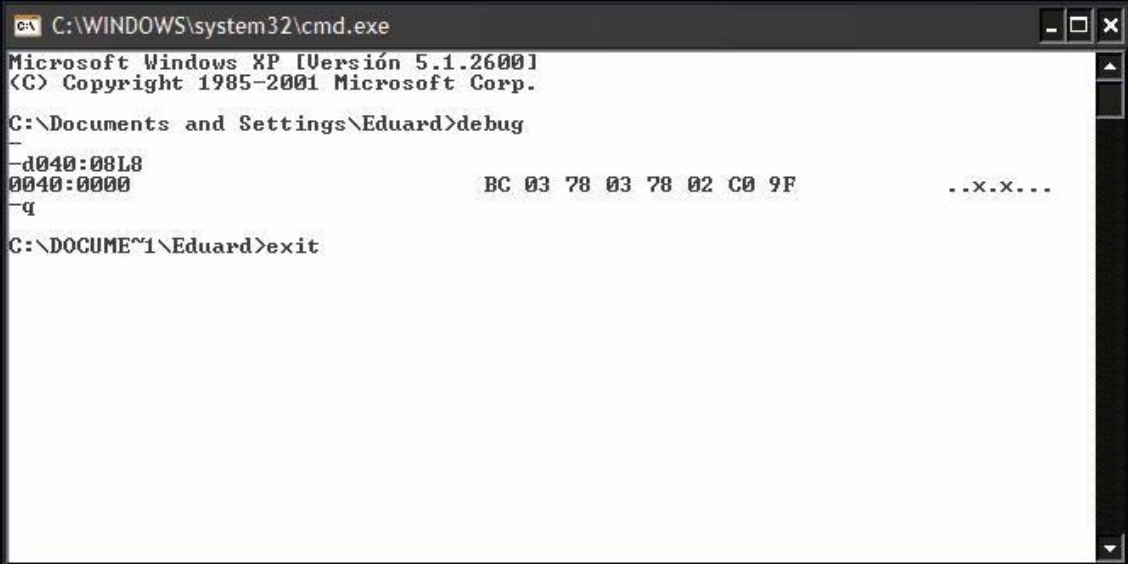
Cuando un PC se enciende, la BIOS ejecuta una rutina para determinar el número de puertos presentes en el sistema asignando la etiqueta LPT1 al primer puerto localizado, si existen más puertos entonces se asignarán consecutivamente las etiquetas LPT2 y LPT3 de acuerdo con:

Dirección inicial	Función
0000:0408	Dirección base para LPT1
0000:040A	Dirección base para LPT2
0000:040C	Dirección base para LPT3
0000:040E	Dirección base para LPT4

Tabla 3.13 Dirección base para los puertos paralelos de un PC

Para trabajar con el puerto paralelo necesitamos en primer lugar conocer la dirección base asignada por la BIOS (estamos hablando de un PC compatible con IBM), podemos utilizar un programa llamado **Debug.exe** que nos indique la(s) dirección(es) asignada(s); si usamos el sistema operativo Windows, yendo al menú *inicio*, en la ventana de ejecutar tecleamos *cmd* y aceptamos, abriremos una ventana de *Símbolo de MS-DOS* y aquí podemos introducir los comandos indicados más abajo.

Si se trabaja en ambiente DOS basta con teclear en la línea de comandos la palabra **debug**, el programa responde colocando un signo menos (-) donde tecleamos, sin dejar espacios en blanco, **d040:08L8** y presionamos la tecla *entrar*; entonces el programa *debug.exe* nos indica en una serie de números la(s) dirección(es) para el (los) puerto(s) paralelo(s) disponibles en nuestro sistema, la siguiente imagen muestra el resultado obtenido en uno de los portátiles donde se ha realizado la prueba:



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Eduard>debug
-
-d040:08L8
0040:0000          BC 03 78 03 78 02 C0 9F          ..x.x...
-q
C:\DOCUME~1\Eduard>exit
```

Figura 3.25 Ejemplo de localización de la dirección base del puerto paralelo en un PC

Se puede observar una serie de números de dos dígitos (ocho en total), se trata del volcado de memoria que empieza en la dirección 40:0008h. Los primeros seis pares de números representan las direcciones base para los puertos instalados, en la imagen de arriba se aprecian varios puertos. El primero (los primeros cuatro dígitos empezando por la izquierda) al puerto paralelo: 0x3BCh (BC 03). Los números están invertidos porque Intel almacena tal información en un formato de "byte de bajo orden - byte de alto orden". El resto de dígitos que aparecen en pantalla se ignoran, ya que el PC tan solo tiene un puerto paralelo disponible. Una vez que obtenemos la información deseada cerramos el programa *Debug.exe* simplemente tecleando la letra **q** y presionando la tecla *entrar*. Para cerrar la ventana de *Símbolo de MS-DOS* tecleamos la palabra **exit** y presionamos la tecla *entrar*.

### Escribiendo datos al puerto paralelo

Con ocho bits podemos escribir en el puerto un total de 256 valores diferentes, cada uno de éstos representa un byte de información y cada byte puede representar una acción concreta que nosotros podemos definir de acuerdo a nuestras necesidades. Un ejemplo de función que permite enviar datos por el puerto paralelo es **outp()**. Esta función requiere dos parámetros, el primero de tipo *unsigned int* que especifica la dirección del puerto paralelo, y el segundo de tipo *char* que especifica el valor a escribir en las líneas de datos de puerto. Una típica llamada a la función *outp()* se parece a esto:

```
outp(0x378, 65);
```

Figura 3.26 Ejemplo de comando para enviar datos al puerto paralelo

Se aprecia la facilidad de manejo de la función, aunque diferentes compiladores dan a sus respectivas funciones nombres diferentes, la mecánica es la misma, se requieren dos parámetros, la dirección del puerto y el valor a escribir en el puerto. Por eso mismo, si tuviéramos que escribir un código que nos permitiera comunicarnos con el puerto paralelo, debería antes consultar las librerías que nos facilitan la entrada y la salida de bits por los pins de este puerto.

### 3.7 *Diseño a alto nivel del software*

Para poder realizar un diseño a alto nivel del software que necesitaremos para poder controlar el sistema, primero deberemos tener claro el esquema que tiene todo el bloque y establecer los tipos de finalidades que tendrá cada parte del programa.

Así podemos dividir el diseño en dos partes diferenciadas:

- Interfaz de usuario
- Interfaz de control

Estas partes se diferencian la una de la otra en la finalidad de su diseño. Mientras que la parte de interfaz de usuario es la ‘cara’ que nuestro programa mostrará al usuario y gestionará sus peticiones, la interfaz de control se limitará a gestionar las peticiones que le realiza la interfaz de usuario, a controlar el funcionamiento del hardware, gestionar los datos de entrada y salida y, finalmente, mostrar los resultados obtenidos al usuario.

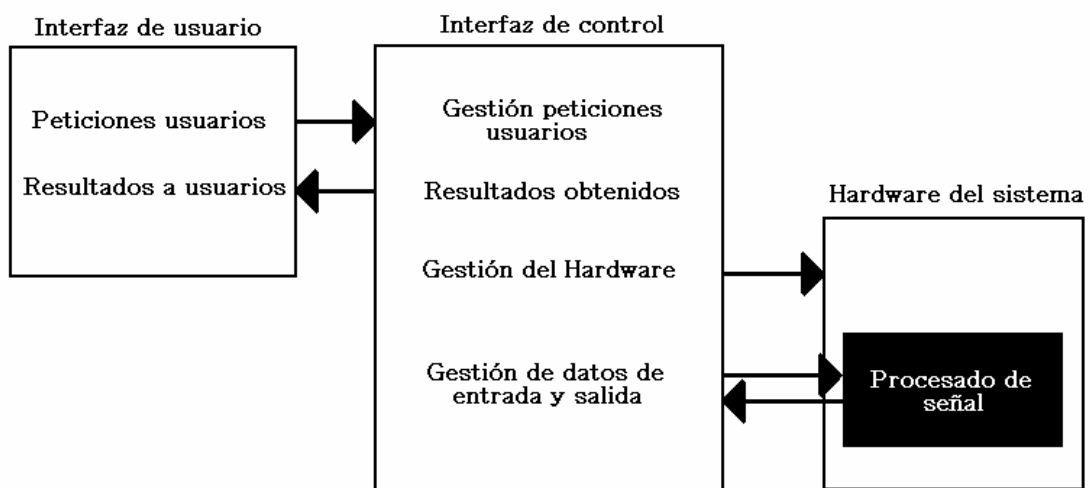


Figura 3.27 Esquema del software del sistema a alto nivel

#### **Interfaz de usuario**

La interfaz de usuario se divide en dos grandes partes: peticiones de los usuarios y resultados obtenidos mostrados a los usuarios. Es evidente que los resultados obtenidos se corresponden directamente con las peticiones que realizan los usuarios, pero desde el punto de vista de la programación es mejor separarlos en dos bloques.

Las peticiones de los usuarios, a su vez, pueden dividirse en varios casos, observando cada uno las posibilidades que ofreceremos como prestaciones a los usuarios.

El objetivo de este sistema es única y exclusivamente el de conseguir identificar las etiquetas EPC de clase 1 que se encuentren dentro del área de interrogación, por lo que tan solo ofreceremos dos opciones a los usuarios:

- Búsqueda de todas las etiquetas que se encuentren dentro del área de interrogación (comando ScrollAllID por parte del lector hacia la etiqueta).
- Búsqueda de una etiqueta concreta dentro del área de interrogación (comando ScrollID del lector a la etiqueta).

Estas prestaciones que son ofrecidas a los usuarios nos proporcionan un grupo de respuestas posibles bastante reducido:

- Listado de todos los tags que se encuentran dentro del área de interrogación: caso favorable.
- Respuesta del tag buscado dentro del área de interrogación: caso favorable.
- No hay respuesta por parte de ningún tag: puede que no haya ninguna etiqueta dentro del área de interrogación.
- Error: puede haber una mala conexión con el hardware o un error del hardware que provoque su mal funcionamiento.

Inicialmente estas son todas las partes que se ofrecerían al usuario para un 'control' de la aplicación que satisfaga las necesidades para las que el sistema es diseñado.

La idea de implementación para este interfaz habría sido de modo gráfico, por lo que el lenguaje de programación usado debería haber sido Visual Basic, que habría estado conectado usando librerías dinámicas (.dll) con el interfaz de control del hardware, programado en C++.

### **Interfaz de control**

La parte del interfaz de control es el grueso del programa. Creado en lenguaje en C++, lo primero que deberemos es crear las clases que nos permitan gestionar todo el volumen de datos del que dispondremos. Inicialmente las clases a crear serán:

- Comando: almacenará los posibles comandos por parte del lector y las funciones que nos permitan configurarlos.
- Paquete de transmisión: Almacenará toda la información que contiene un paquete de transmisión y las funciones que permitan gestionar estos datos.
- Paquete de recepción: Almacenará toda la información que nos proporcione el hardware sobre una respuesta de una etiqueta y las funciones que permitan extraer la información que nos interese para poder pasarla a la clase que tenemos a continuación.
- Familia de etiquetas: Será capaz, de un modo dinámico, de ir guardando la información extraída por las funciones del paquete de recepción de modo que,



al finalizar la transmisión, contenga los datos de todas las etiquetas que hayan respondido (si se trata de un comando ScrollIID, almacenará la información de una sola etiqueta, mientras que si es un comando ScrollAllIID almacenará la información de todas las etiquetas que respondan). También habrá en esta clase las funciones que permitan la gestión de estos datos de manera que puedan ser devueltos al usuario de un modo inteligible.

- Id de etiqueta: almacenará la Id de la etiqueta que busca el comando ScrollIID, de manera que en todo momento pueda ser usada hasta que finaliza la información.
- Configuración del hardware: esta clase albergará la información que permita configurar el hardware para que varíe entre los estados de emisión y recepción.

Estas son las clases que, inicialmente, deberán constar en el programa. Es evidente que por cuestiones prácticas este diseño no puede quedar cerrado debido a que, durante el desarrollo de una aplicación, surgen imprevistos y problemas que a veces requieren crear nuevas clases y funciones, por lo que la decisión final se tiene que tomar en el momento en el que se programa la aplicación.

Con el objetivo de simplificar el diseño que estamos haciendo, en vez de explicar las funciones dentro de las clases que deberían albergarlas, vamos a explicarlas según la finalidad a la que están dirigidas, de modo que su inclusión dentro de una clase u otra queda a elección del programador, aunque la propia definición de cada clase restringe bastante esta libertad.

Para la gestión de las peticiones de los usuarios tendremos en cuenta el diseño de una única función, la cual contemplará la posibilidad de pedir al sistema la ejecución de uno de los dos comandos existentes: ScrollIID o ScrollAllIID.

En lo que respecta a los resultados obtenidos usaremos también una única función que se encargue de gestionar la clase ‘familia de etiquetas’ de manera que, cuando se devuelva esta parte al interfaz de usuario, se puedan extraer de ahí los resultados.

La gestión del hardware contará con varias funciones cuya finalidad será:

- Transferencia de la configuración para pasar a modo ‘emisión’ al hardware. Esta función tiene que contemplar la posibilidad de que puede no haber un hardware con el que comunicarse o, simplemente, que se produzca un error. Esta es, con toda probabilidad, la función con la que se tiene que ser más meticoloso de todo el programa. Una correcta configuración de la placa diseñada (modulación, codificación, etc.) es importante para garantizar una buena calidad de señal, lo que permitirá una mejor comunicación entre el lector y las etiquetas. En esta función usaremos las librerías de control del puerto paralelo.
- Transferencia de la configuración para pasar a modo ‘recepción’ una vez se ha acabado de transmitir los datos. En esta función usaremos las librerías de control del puerto paralelo.

- Transmisión de la trama de transmisión. Esta función tiene que contemplar la posibilidad de que se produzca un error inesperado durante el proceso (por ejemplo, que se desconecte el hardware mientras se está transmitiendo un paquete). En esta función usaremos las librerías de control del puerto paralelo.
- Recepción del paquete de datos proveniente del hardware. Al igual que la función de transmisión, debe contemplar la posibilidad de recibir una trama incompleta, causa de un error en la recepción (colisión) o de un mal funcionamiento del hardware (desconexión, fallo, etc.). En esta función usaremos las librerías de control del puerto paralelo.

Finalmente, la gestión de entrada y salida de datos deberá tener las siguientes funciones para poder conseguir un buen funcionamiento global del programa y, por lo tanto, del sistema.

- Una función que prepare la trama a transmitir para, así, poder directamente enviarla al hardware que se encargará de procesar los datos de manera que el tag los reciba y los interprete según nos interesa. Esta función deberá tener en cuenta que tan solo existen dos posibles tramas posibles ya que sólo hay dos comandos posibles: ScrollID y ScrollAllID. Debemos tener en cuenta que esta es la función que incluirá el CRC dentro de la trama, así que deberá tener en su interior el algoritmo que permita calcularlo (o tenerlo ya calculado para cada trama, puesto que sólo hay dos posibles tramas a transmitir aunque esta opción limita mucho la posibilidad de realizar una versión futura del programa con más funcionalidades).
- Debemos proporcionar la trama creada a la parte de gestión del hardware de manera que pueda hacerla llegar al sistema físico que tenemos diseñado.
- Extracción de la información que llegue en los paquetes de datos recibidos. Es básicamente obtener la ID de cada etiqueta que responda mientras dure el proceso de recepción y comprobar que esta ID obtenida se corresponde con el CRC que lo corrobora.

Una vez tenemos especificadas las funciones del interfaz de usuario y del interfaz de control, ya podríamos empezar a programar.

### 3.8 Simulación del entorno wireless

Para poder hacernos una idea más completa de lo que supone la comunicación entre el lector y las etiquetas, hemos decidido simular la señal que tenemos del lector a la etiqueta y la respuesta de la etiqueta al lector. Dentro de esta simulación nos intentaremos fijar en los parámetros que nos interesen para poder caracterizar las posibles respuestas del sistema al canal wireless.

Un aspecto importante dentro de esta simulación es el software que usaremos para simular el canal. Este software es el WinIQSim v.4.0., propiedad de ROHDE & SCHWARZ.

WinIQSim es un software de simulación de señales I/Q (fase/cuadratura), lo que condiciona la elección de los parámetros para poder interpretar los gráficos de manera que no afecten a la concepción de los resultados.

El interfaz que presenta WinIQSim es gráfico, lo que nos permite una sencilla configuración de todos los puntos del sistema a simular sin necesidad de excesivas complicaciones.

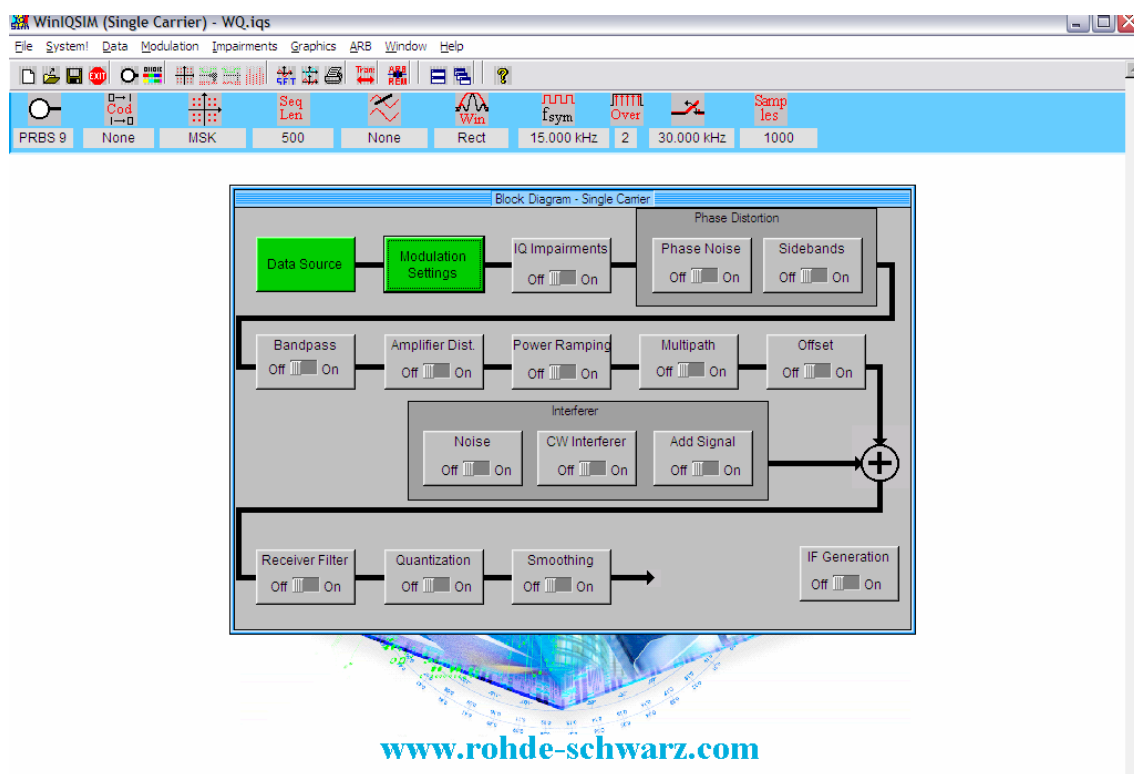


Figura 3.28 Interfaz gráfica de WinIQSim



Estos datos los introduciremos de forma manual dentro de la fuente de datos, quedando del siguiente modo:

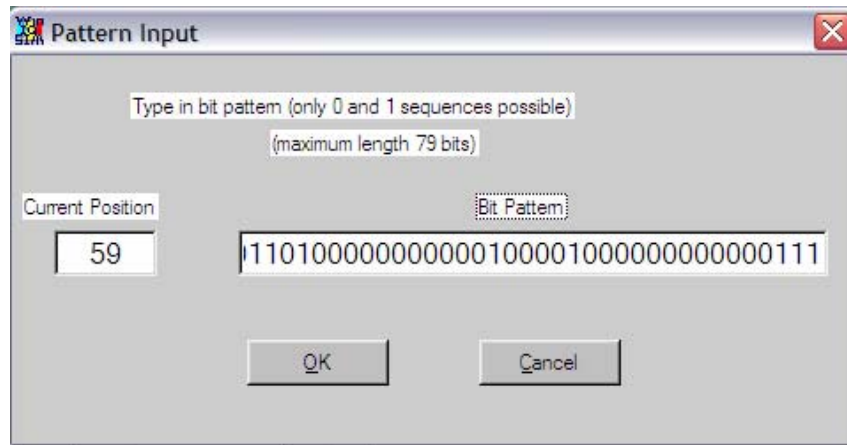


Figura 3.29 Trama de bits introducida en WinIQSim

Una vez hemos introducido los datos a transmitir, debemos configurar la modulación a usar.

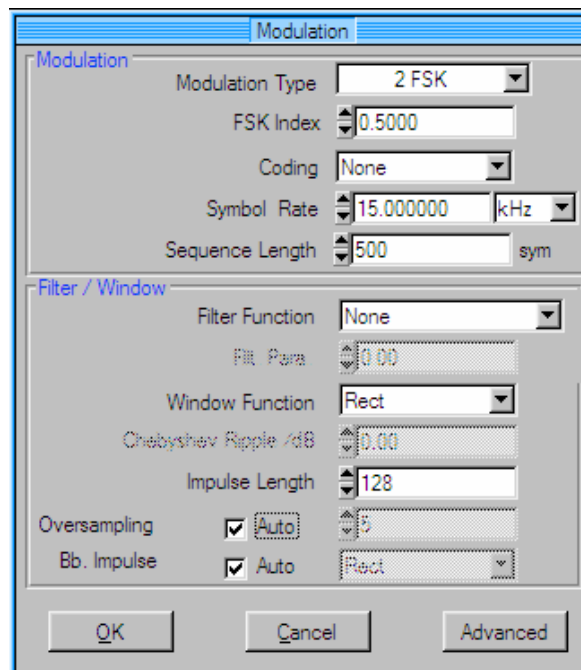


Figura 3.30 Configuración de la modulación usada en WinIQSim

Los campos configurados para la modulación son:

- *Modulation Type*: El tipo de modulación es la que marca las hojas de especificaciones: una 2FSK.
- *FSK Index*: Indica la desviación de frecuencia de la FSK. Elegiremos el máximo que permite el programa para tener los dos símbolos tan separados como sea posible sin llegar a sobrepasar los 200KHz que permiten las especificaciones.
- *Coding*: No usaremos ningún tipo de codificación.
- *Symbol Rate*: Definido en las especificaciones del programa como la tasa de transferencia dividida entre el número de bits por símbolo. Tenemos un bit por símbolo y una tasa de transferencia marcada en las especificaciones como 15Kbps, por lo que nos queda un 'symbol rate' de 15KHz.
- *Sequence Length*: Marca la longitud de la secuencia a enviar. Cuanto mayor, más resolución tendremos. Elegimos el máximo que permite el programa: 500 símbolos.
- *Filter Function*: No usaremos ninguna función como filtro para generar nuestros símbolos. No queda contemplado en las especificaciones del sistema.
- *Window function*: La ventana que usaremos para poder realizar la simulación será una función rectangular, ya que dentro de esta ventana la señal no queda alterada y fuera de la ventana queda truncada.
- *Impulse Length*: Nos marca el tamaño de la ventana usada. Cuanto mayor sea la ventana, mejor resolución tendremos en las gráficas. Optamos por el mayor valor que nos permite el programa: 128.
- *Oversampling*: Indica el número de muestras usado para representar cada símbolo. Lo dejamos en 'auto' de manera que el programa use el número que crea conveniente en cada momento.
- *Baseband pulse*: Indica el tipo de pulso a usar para generar la señal. Si lo dejamos en 'auto', dependerá de los parámetros de la modulación y en cada caso el programa elegirá el que mejor encaje.

Una vez tenemos definidos los datos a usar y la modulación que corresponde según las especificaciones del sistema, vamos a ver las gráficas que estudiaremos en los diferentes casos aplicaremos posteriormente.

### Gráfica de amplitud y frecuencia (r(t), f(t))

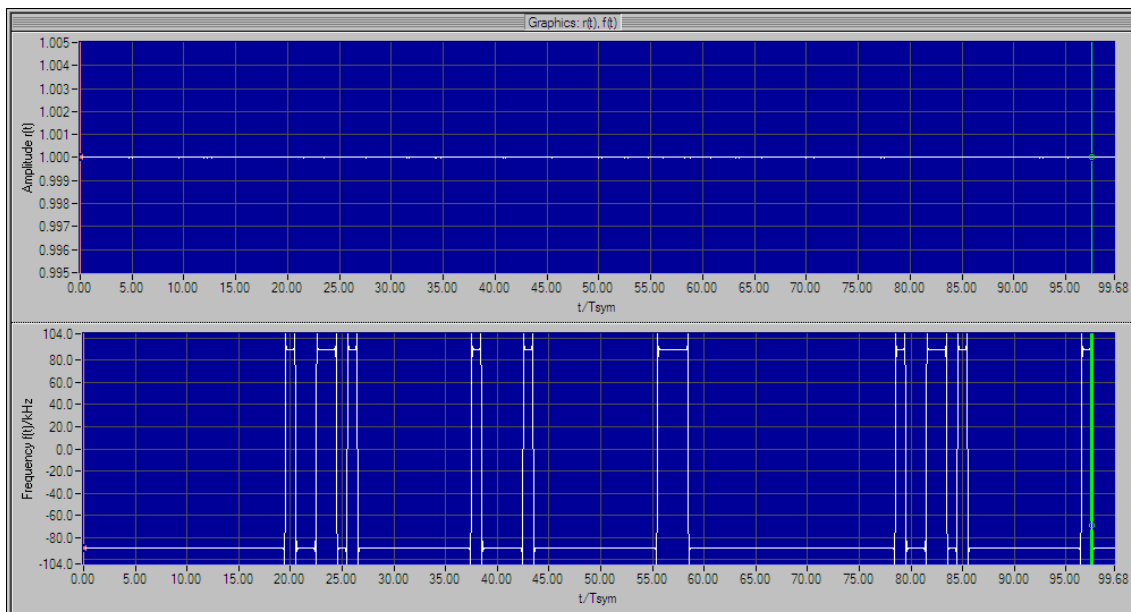


Figura 3.31 Gráfica de amplitud y frecuencia sin ningún tipo de distorsión

Podemos observar en la figura anterior que la amplitud se mantiene constante durante toda la transmisión, mientras que los cambios en la frecuencia debidos al cambio de símbolo enviado son fácilmente observables. A lo largo de todo este apartado observaremos la respuesta que tienen la amplitud y la frecuencia a las distorsiones que le apliquemos. De todos modos, al tratarse de una modulación en frecuencia, los cambios de amplitud afectan en muy poca medida al rendimiento del sistema.

### Constelación

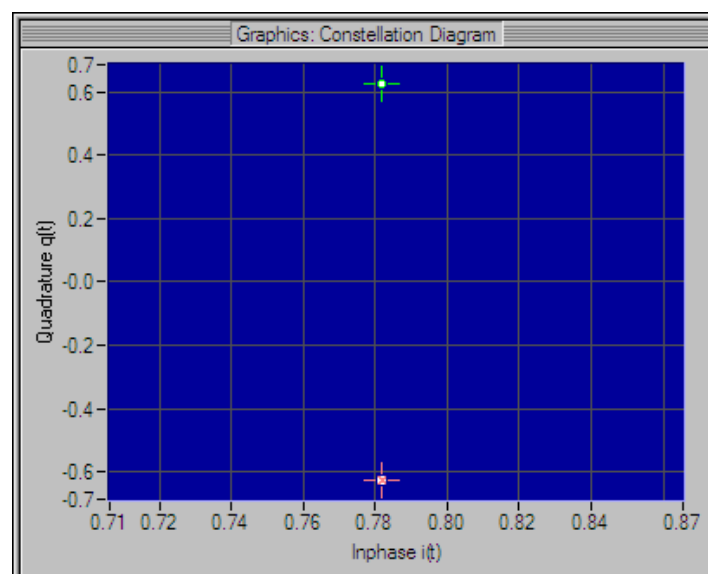


Figura 3.32 Gráfica de la constelación de la señal.

Podemos observar en la gráfica de la constelación como tenemos tan sólo dos símbolos en nuestro sistema. En apartados posteriores veremos como afectan las interferencias a los símbolos que enviamos en nuestro sistema.

### Diagrama de ojo de la frecuencia:

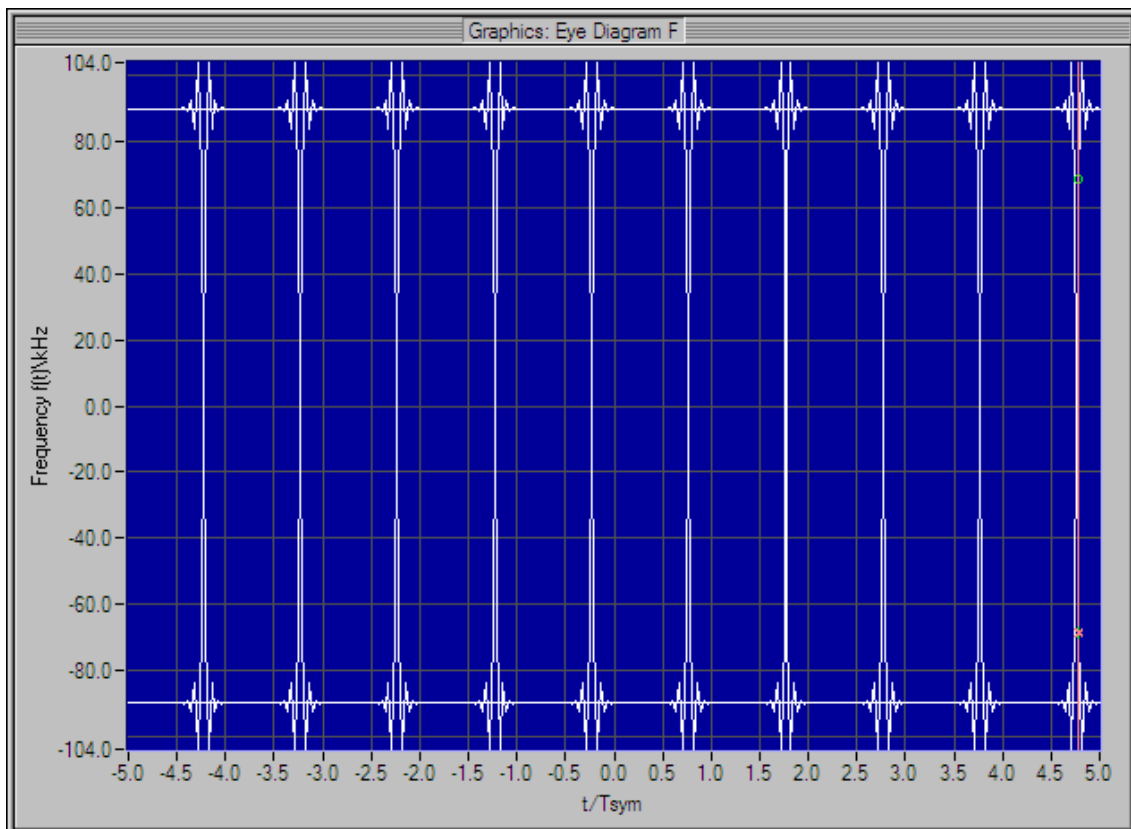


Figura 3.33 Diagrama de ojo de la frecuencia de la señal del sistema.

El diagrama de ojo nos muestra las variaciones que sufre la frecuencia de la señal. Como podemos observar la frecuencia varía tan solo entre dos valores, uno positivo y el otro negativo, lo que nos indica que varía entre en la banda de transferencia de la señal, 865,1MHz, variará entre  $f_1$  y  $f_2$ .

### Gráfica de la FFT MAG (módulo de la FFT)

La gráfica de la FFT MAG nos muestra el módulo de la transformada discreta de Fourier. En esta gráfica podemos comprobar el tipo de respuesta frecuencial que tiene la señal que enviamos. Comprobamos que tiene dos picos simétricos, lo que se debe a la existencia de dos frecuencias en las que trabajamos. Vemos que la señal baja su amplitud a medida que nos desplazamos de las frecuencias en las que trabajamos. Esto nos resulta interesante para poder no interferir en las bandas adyacentes que tenemos.



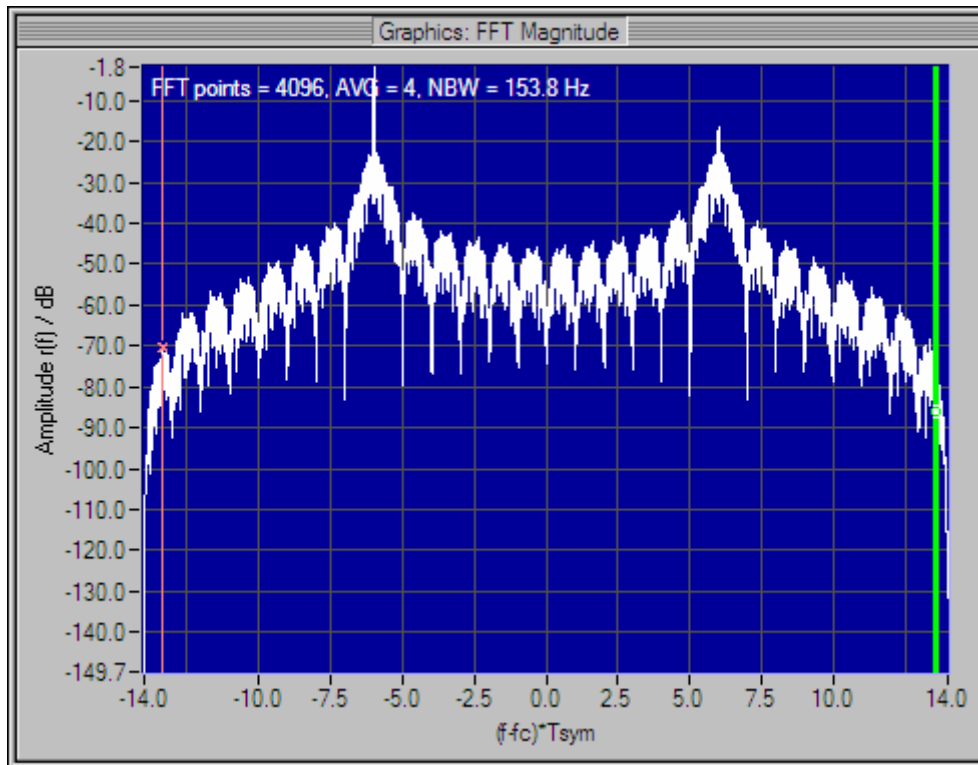


Figura 3.34 Gráfica de la FFT MAG de nuestra señal.

### Propagación multicamino

La propagación multicamino es el principal problema al que nos enfrentamos en nuestro sistema. El hecho de trabajar en espacios cerrados y con muchos objetos en el área de interrogación nos presenta la problemática que vamos a estudiar a continuación.

Hay que tener en cuenta que FSK es una modulación de frecuencia, por lo que para recuperar los símbolos será necesario tan sólo que la frecuencia de la señal no quede alterada, no importando en exceso la influencia que tengan otras señales sobre la amplitud.

La propagación multicamino puede afectar de dos maneras distintas a la señal recibida. Por un lado la amplitud de la señal recibida puede variar. Por otro lado puede que la señal recibida haya cambiado su fase y, al superponerse con la señal buena, la anule.

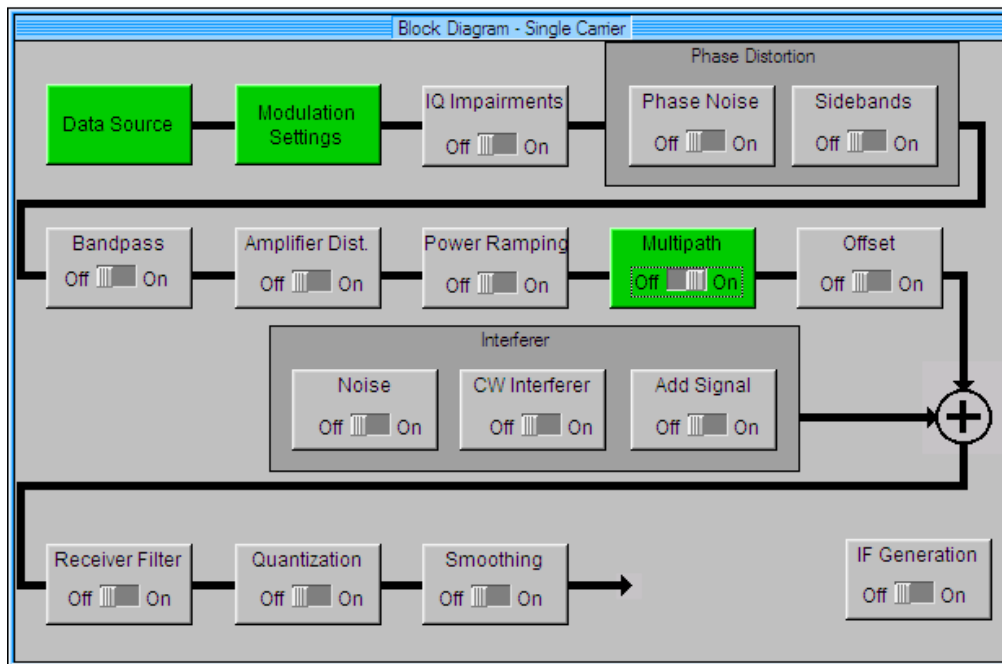


Figura 3.35 Activamos el bloque correspondiente al multicamino

Para observar el efecto de la propagación multicamino sobre la amplitud y sobre la frecuencia, vamos a ver la superposición de la gráfica inicial (rojo) con la que obtenemos al activar la propagación multicamino (azul). Concretamente en estas gráficas tenemos una señal procedente de multicamino con un retardo de  $0,3T$ .

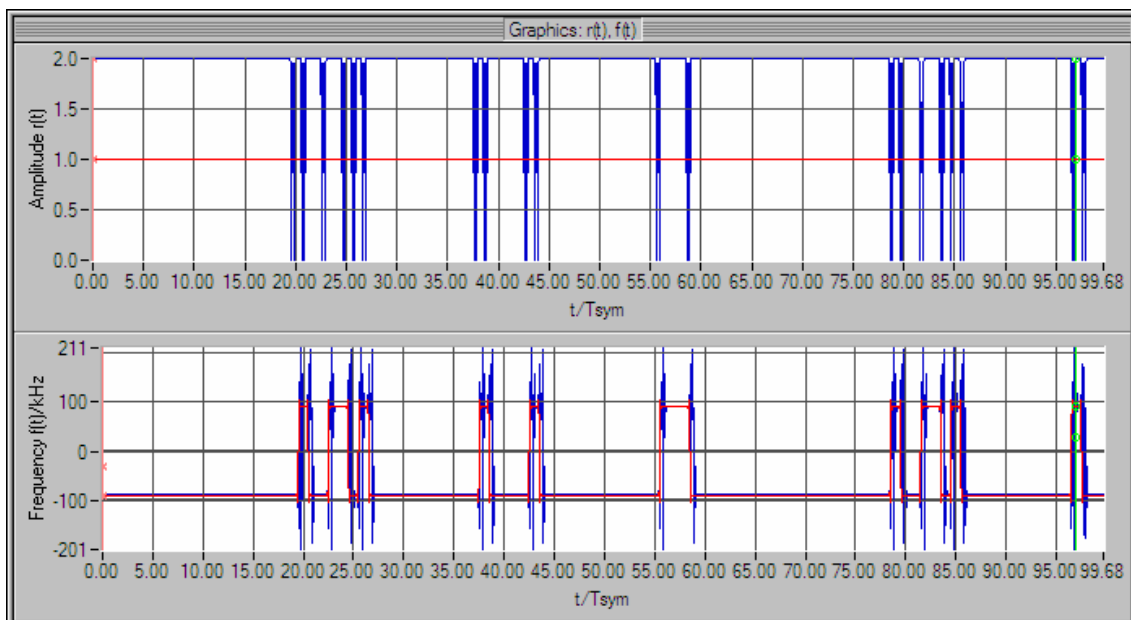


Figura 3.36 Superposición de las gráficas de la amplitud y frecuencia sin (rojo) y con multicamino (azul).

Este es el resultado de superponer señales con un retardo inferior a  $0,35T$ . La señal proveniente de multicamino provoca una distorsión en las transiciones de frecuencia, lo que provoca que estas sean más duraderas. Si aumentáramos el retardo de la señal, las transiciones se superpondrían a la información útil, lo que provocaría que la señal fuera irrecuperable. En cuanto a la amplitud de la señal, no nos afecta para nuestro sistema ya que se trata de una modulación de frecuencia.

Estos resultados se pueden confirmar viendo la constelación y el diagrama de ojo de la señal.

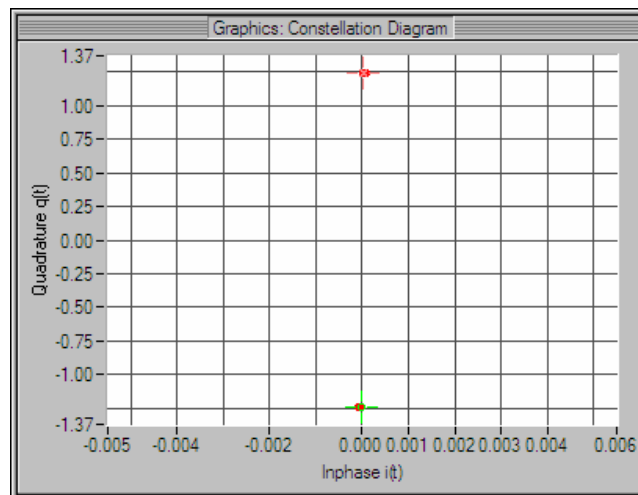


Figura 3.37 Constelación con una señal multicamino con retardo  $0,3T$

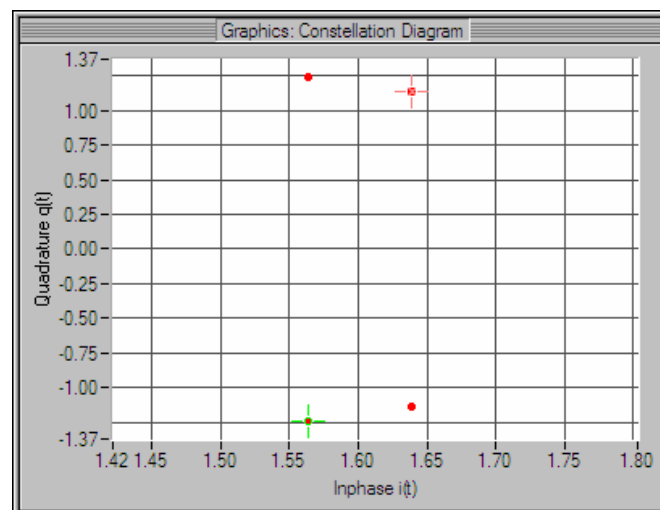


Figura 3.38 Constelación con una señal multicamino con retardo  $0,5T$

La constelación nos muestra como al variar el retardo de la señal proveniente de multicamino, aparecen ya más símbolos de los que deberían inicialmente, lo que provoca un posible error en la recepción de los mismos.

Por lo que al diagrama de ojo respecta, podemos observar exactamente los mismos resultados. Para un retardo  $< 0,3 * T$  podemos distinguir aún las dos frecuencias existentes, mientras que para valores mayores que  $0,3 * T$  la frecuencia pasa a ser indescifrable.

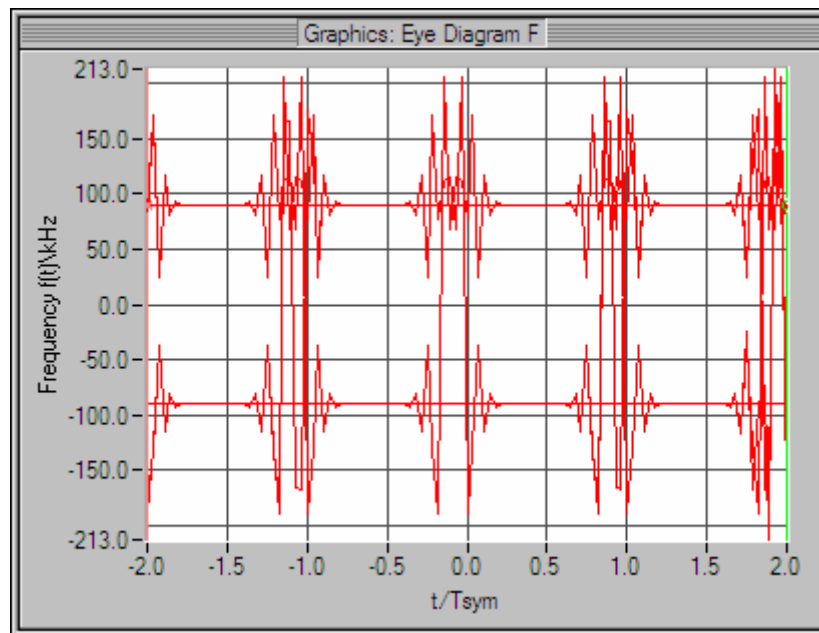


Figura 3.39 Diagrama de ojo de la frecuencia para un retardo de multicamino de  $0,3 * T$

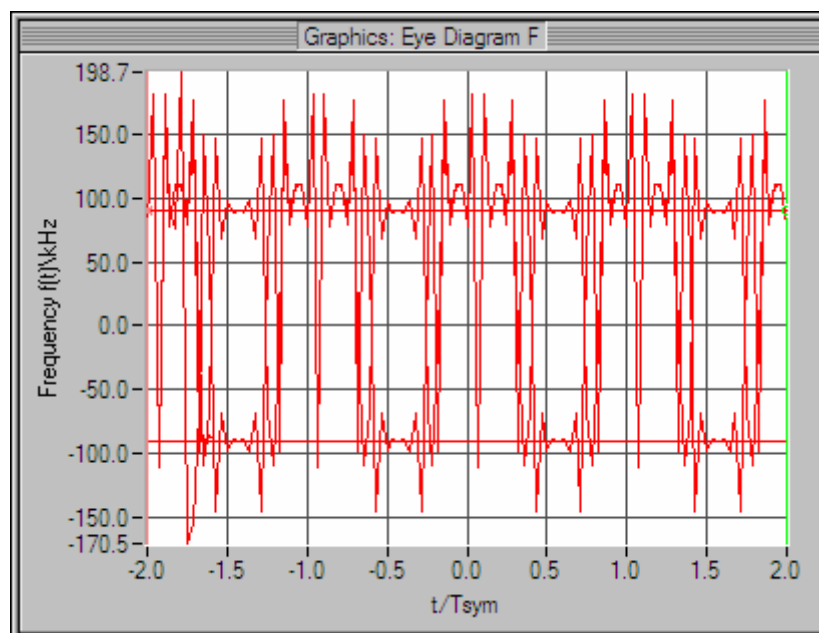


Figura 3.40 Diagrama de ojo de la frecuencia para un retardo de multicamino de  $0,5 * T$

Para la FFT MAG no se observan cambios apreciables.

Si variamos el nivel de señal recibida, es decir, el multicamino provoca una pérdida de potencia sin causar un retardo demasiado elevado en la señal, los cambios que se observan no son susceptibles de provocar un error en la transmisión ya que las señales resultantes son la superposición de la señal recibida sin multicamino y con el nivel adecuado de potencia más la señal que proviene del multicamino con una potencia atenuada, lo que provoca que la señal recibida tenga mayor potencia y no sufra cambios en frecuencia.

Lo mismo sucede cuando la propagación multicamino provoca un cambio de fase en la señal. El único cambio susceptible de ser mencionado es que los puntos de la constelación se desplazan tantos grados como desfase tiene la señal proveniente del multicamino. Así la gráfica con la señal multicamino que tiene un desfase de  $45^\circ$  será:

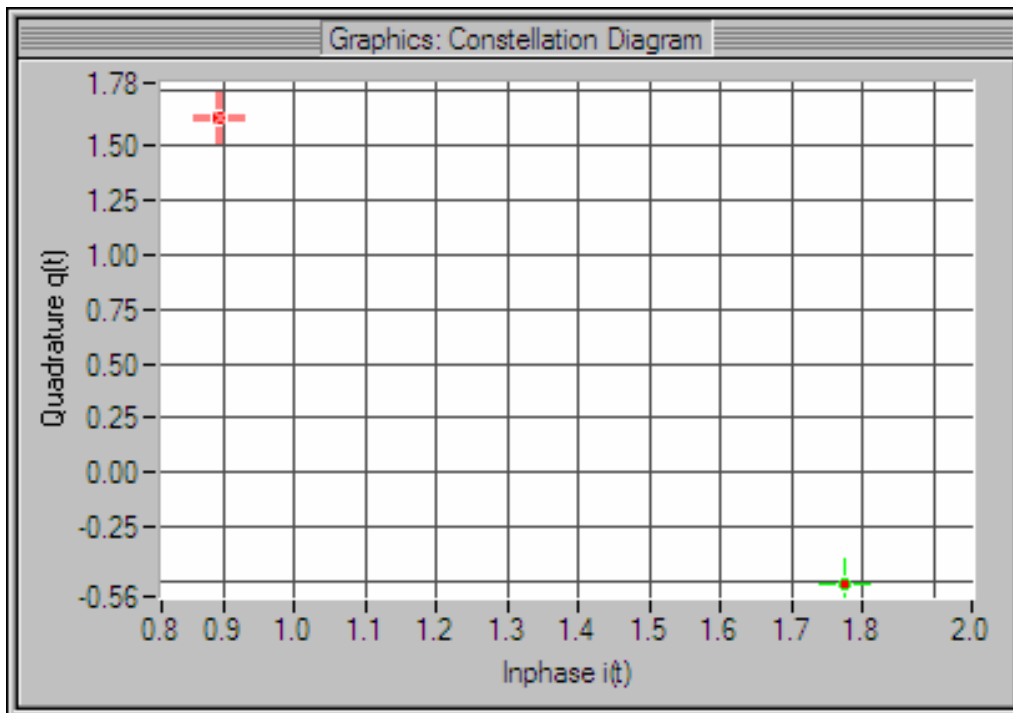


Figura 3.41 Superposición de señales con un desfase de  $45^\circ$

## Ruido

El otro factor que vamos a tener en cuenta a la hora de estudiar el canal wireless en la comunicación lector-etiqueta será el ruido que exista en el ambiente, como algo más genérico pero que afecta a la señal que tiene que recibir el tag y que, por lo tanto, puede producir errores en la comunicación.

Para poder configurar el ruido deberemos activar el bloque 'Noise'. Una vez tengamos elegido este bloque, el cual quedará marcado de color verde, veremos la configuración que le vamos a dar:

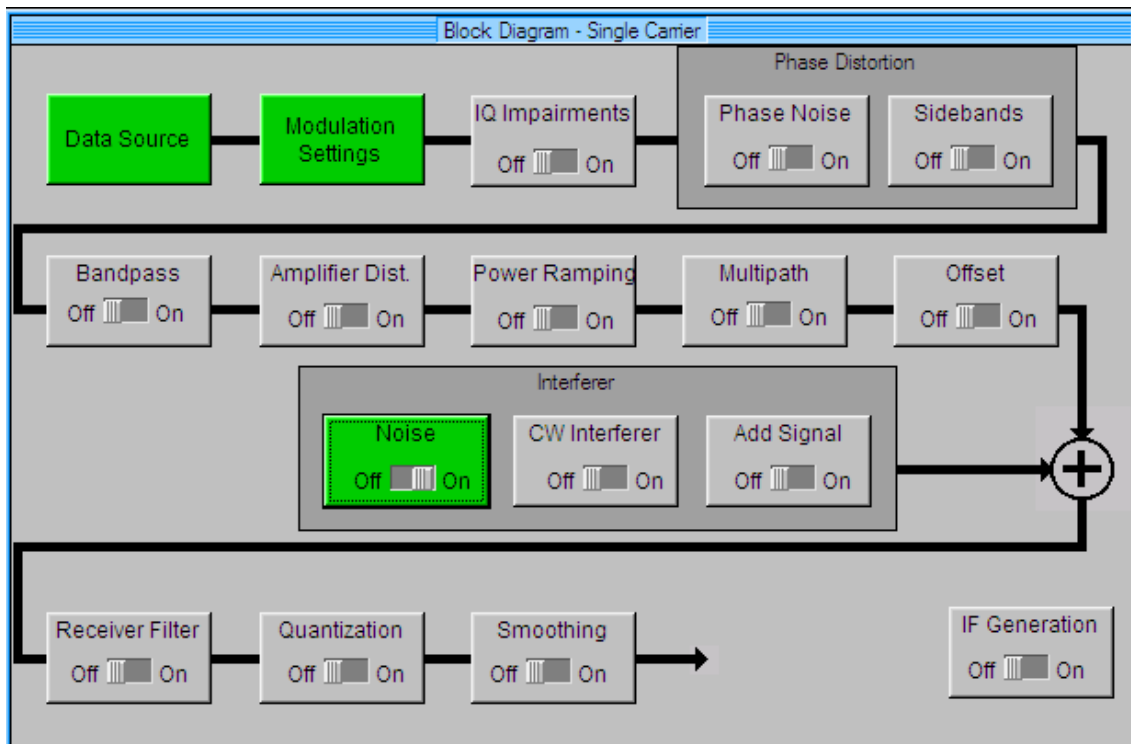


Figura 3.42 Seleccionamos el bloque correspondiente al ruido (Noise) para poder realizar la simulación

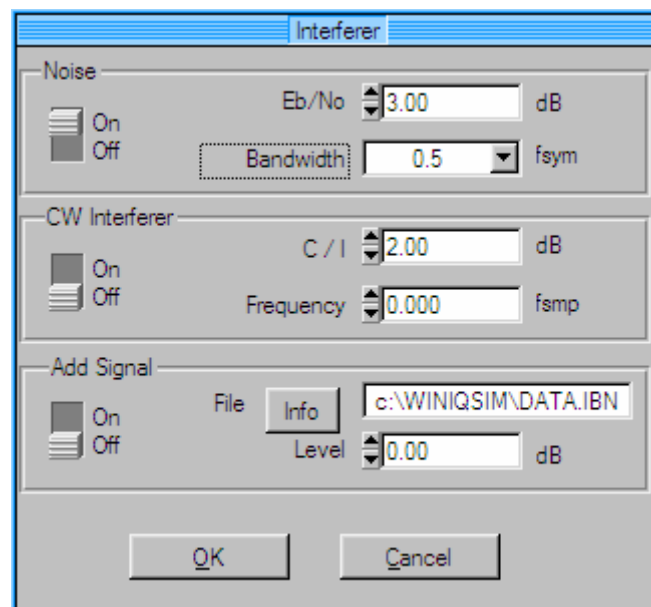


Figura 3.43 Bloque de configuración de interferencias. La parte superior es la referente al ruido, donde podremos variar la relación señal a ruido y el ancho de banda de ruido.

Los parámetros a elegir del bloque 'Noise' son la relación señal a ruido ( $E_b/N_0$ ) y el ancho de banda del ruido (en múltiplos de la frecuencia de símbolo). Variándolos vamos a ver como responde el sistema.

Empezaremos buscando el nivel mínimo de relación señal a ruido que nos permita poder diferenciar las dos frecuencias existentes en el sistema. Dicho nivel es de 18dB. Para niveles inferiores a este valor de  $E_b/N_0$  vemos que no se puede llegar a diferenciar que existen dos frecuencias diferenciadas.

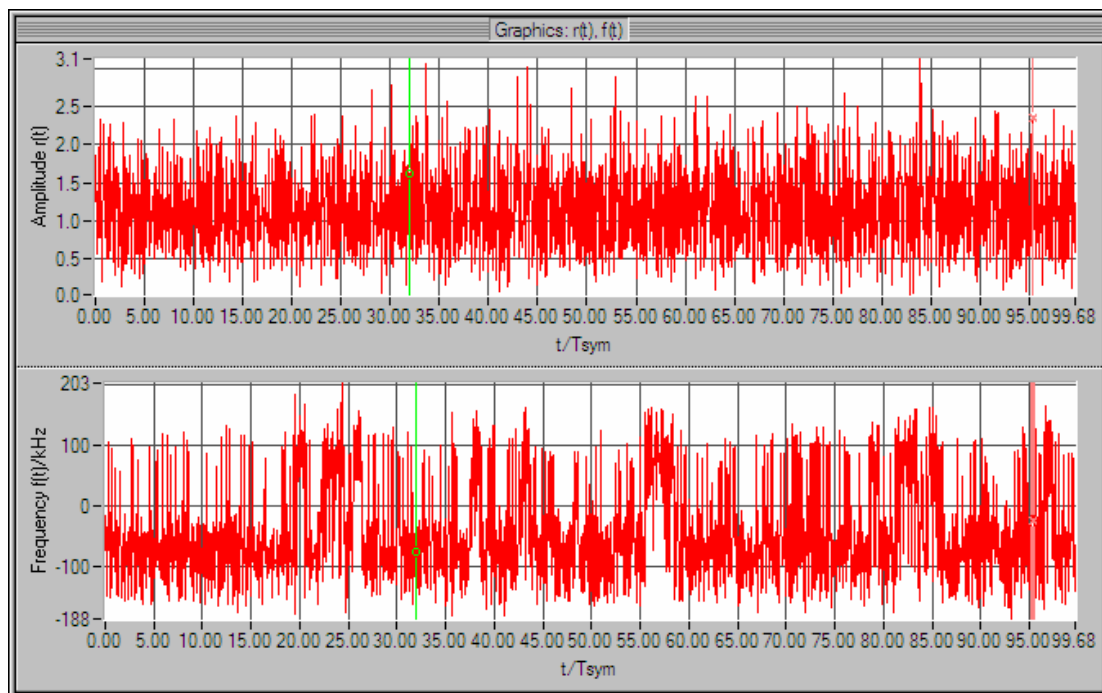


Figura 3.44 La baja relación  $E_b/N_0$  no permite diferenciar las dos frecuencias de sistema

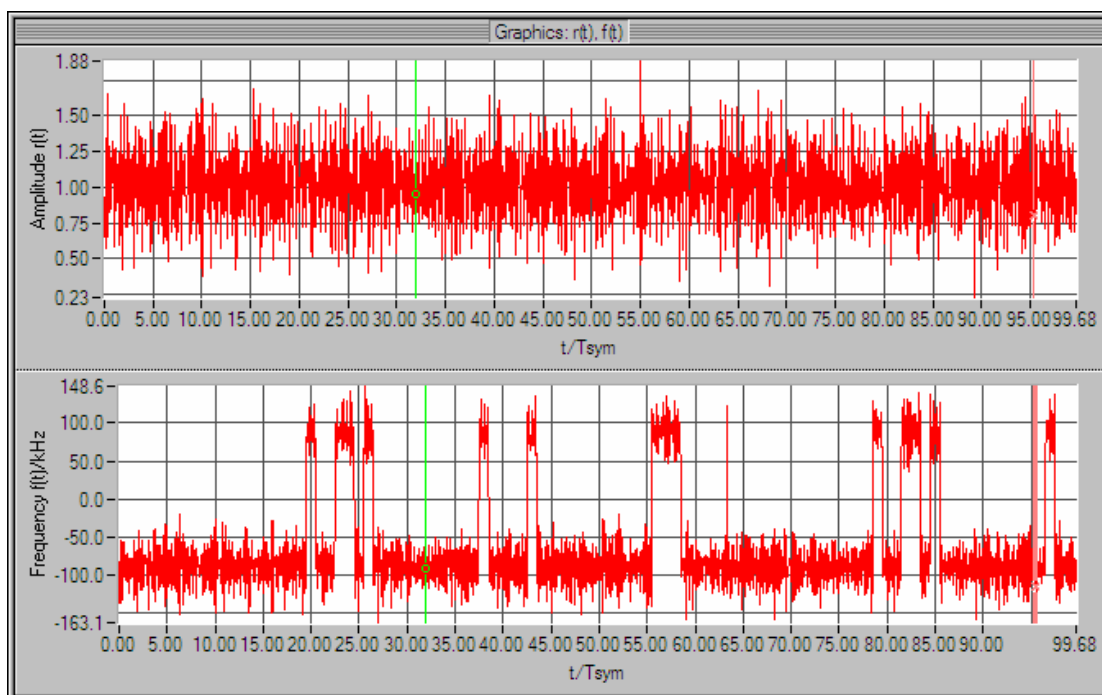


Figura 3.45 Una relación  $E_b/N_0$  superior a 18dB permite diferenciar las frecuencias de nuestro sistema

De todos modos, la calidad de la señal respecto del ruido debe subir para que podamos tener un sistema que funcione correctamente. Con una relación señal a ruido de 30dB existe una calidad lo suficientemente elevada como para poder considerar que el sistema funcionará correctamente.

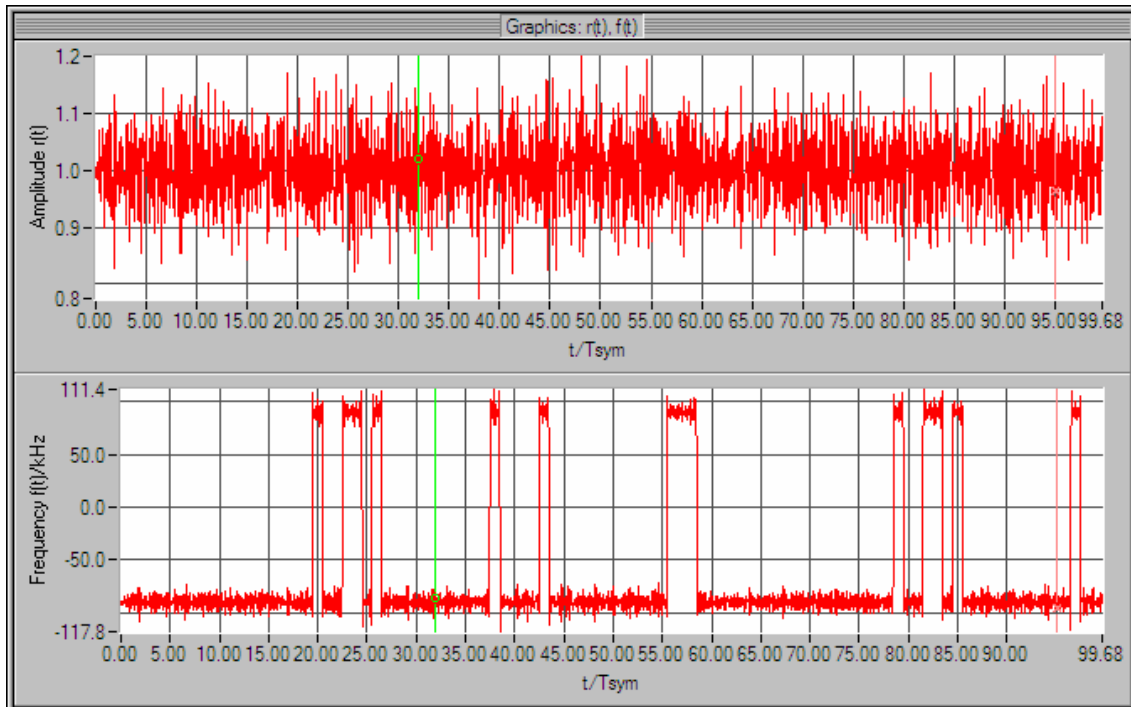


Figura 3.46 Con una relación  $E_b/N_0$  superior a 30dB tenemos una calidad de señal mucho mejor

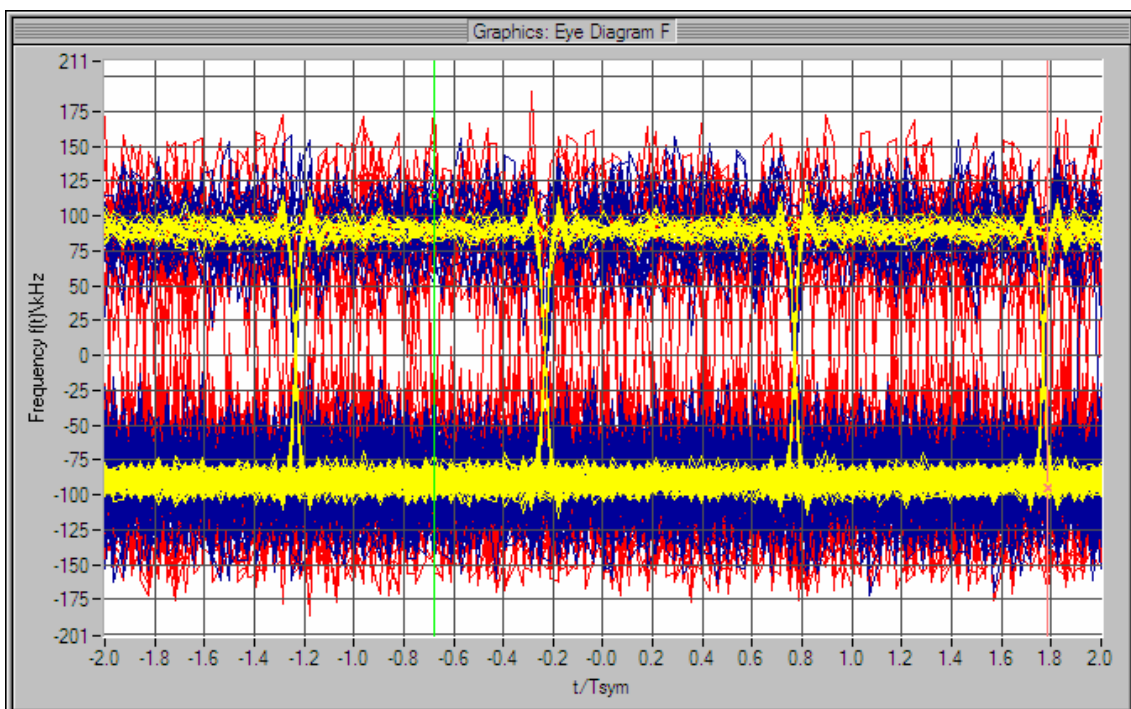


Figura 3.47 La superposición de las gráficas del diagrama de ojo nos muestra que a medida que mejoramos la relación señal a ruido (15dB, rojo; 18dB, azul; 30dB, amarillo), se puede obtener mejor la frecuencia de la señal.



Si lo que variamos es el ancho de banda del ruido, lo que podemos observar es que a igual relación señal a ruido, tenemos más interferencias cuanto mayor es el Bw del ruido. De modo que para obtener una misma calidad de señal, deberemos tener una mejor relación señal a ruido cuanto mayor sea el ancho de banda de éste.

Esto podemos observarlo en las gráficas que tenemos a continuación.

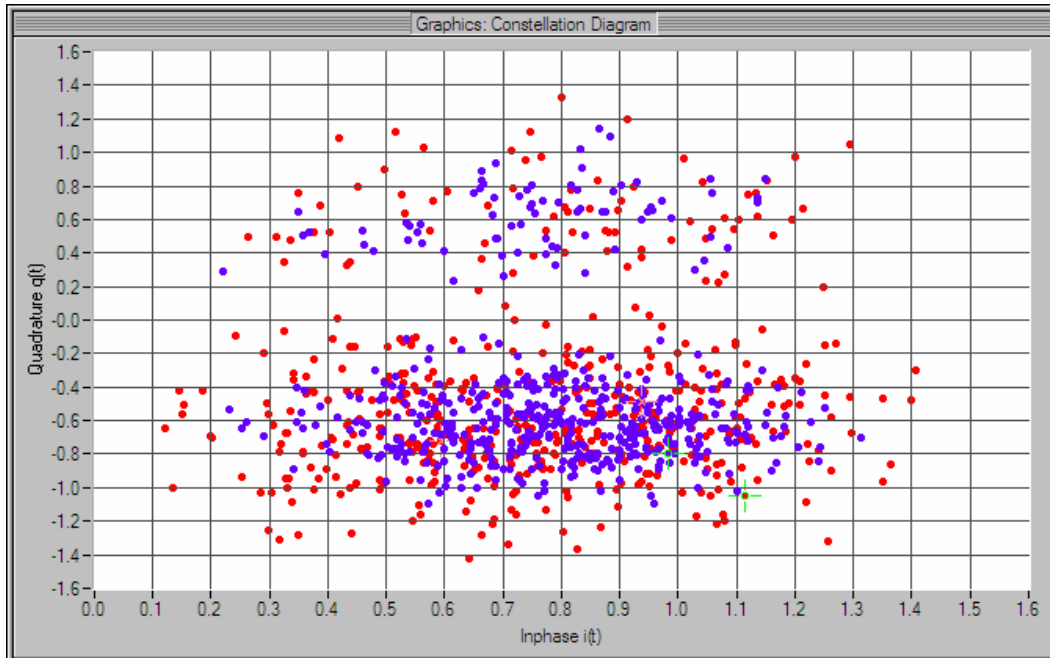


Figura 3.48 Constelación de una señal con 20dB de relación señal a ruido. En la gráfica roja el ruido tiene un ancho de banda de  $8 \cdot f_{sym}$  y en la azul de  $0,5 \cdot f_{sym}$

Donde mejor se observa esta relación es en el diagrama de ojo de la frecuencia.

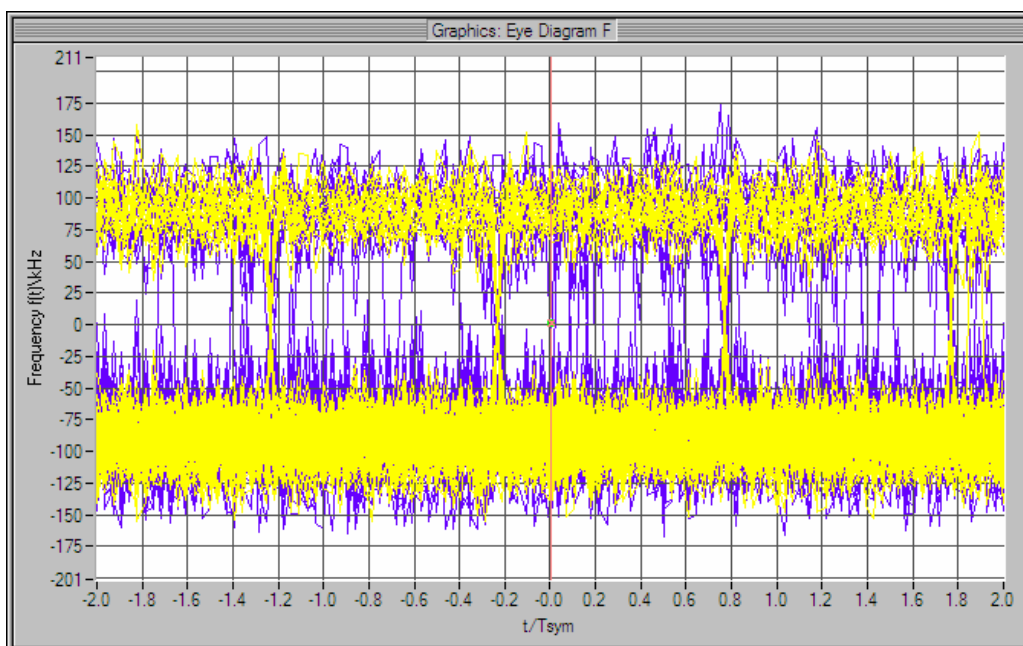


Figura 3.49 Diagrama de ojo de una señal con 20dB de relación señal a ruido. En la gráfica azul el ruido tiene un ancho de banda de  $8 \cdot f_{sym}$  y en la amarilla de  $0,5 \cdot f_{sym}$

Una vez hemos estudiado los dos principales efectos que provoca el canal wireless en nuestro sistema, podemos decir que la modulación usada nos da un buen grado de robustez, lo que nos asegura que en condiciones no óptimas el sistema pueda seguir funcionando.

### 3.8.2 Simulación de la onda continua (CW)

Otro aspecto a tener en cuenta es la señal continua que emite el lector para alimentar las etiquetas mientras estas realizan sus operaciones internas. A continuación vamos a ver como afectan las distorsiones producidas por la propagación multicamino y el ruido.

En el caso que estamos tratando, la señal no tiene una modulación, sino que responde con una onda continua. Vamos a ver el comportamiento de esta onda.

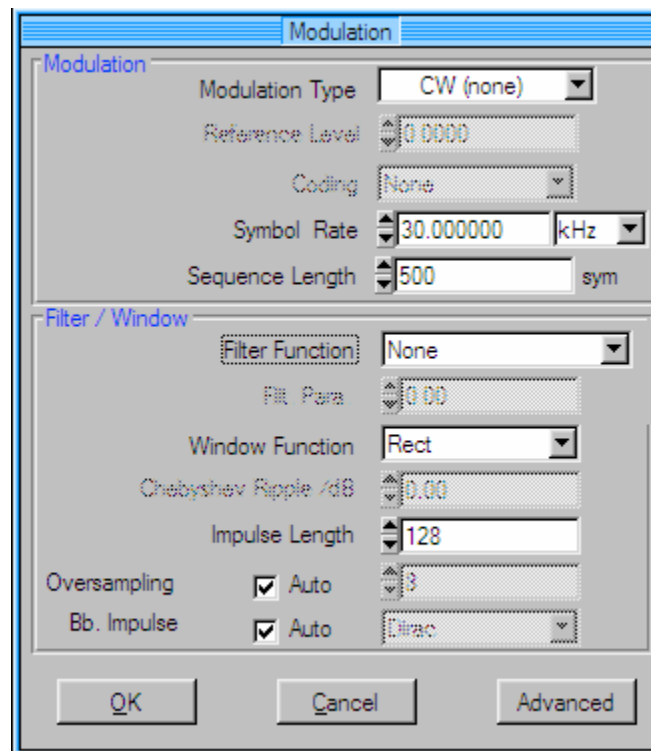


Figura 3.50 Configuración de la modulación usada en WinIQSim

La única diferencia entre esta configuración y la que hemos usado en el apartado anterior es la modulación usada.

Si nos fijamos en las gráficas que nos proporciona el programa sin activar ningún tipo de distorsión, tenemos que:

- La gráfica de amplitud y frecuencia vemos que la señal en amplitud es un pulso triangular y que es constante en frecuencia.

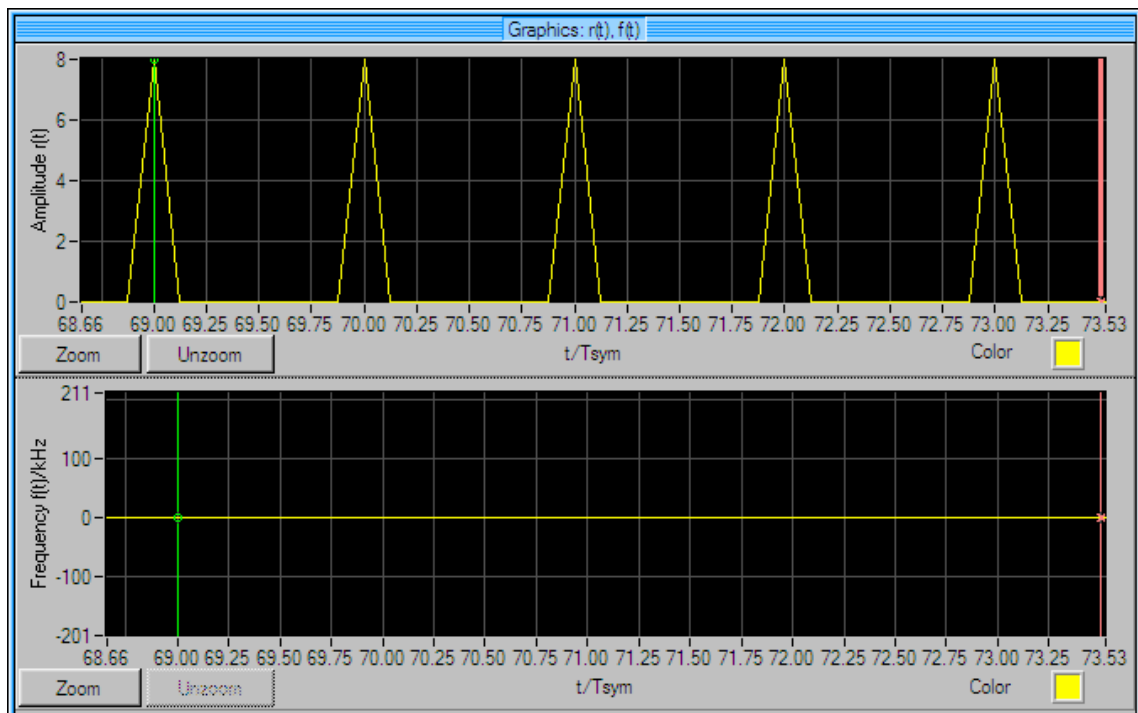


Figura 3.51 Gráfica de amplitud y frecuencia sin ningún tipo de distorsión

- El diagrama de ojo de la frecuencia vemos que se mantiene constante. Es lógico si tenemos en cuenta la representación gráfica de la frecuencia que hemos visto en la figura anterior.

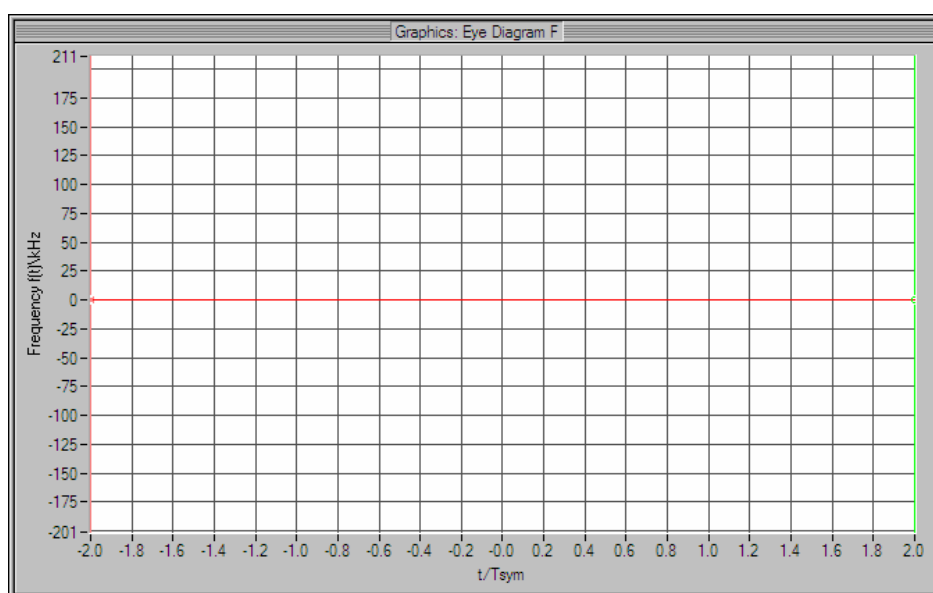


Figura 3.52 Vemos que no hay transiciones de frecuencia en el diagrama de ojo

Con las gráficas de amplitud-frecuencia y el diagrama de ojo de la frecuencia podremos explicar todas las consecuencias que sufre la señal provenientes de la propagación multicamino y la existencia de ruido.

### Propagación multicamino

Al superponerse una señal multicamino (con una cierta atenuación y retraso) con nuestra señal, obtenemos como resultado una variación de la amplitud (ganancia al superponerse las dos señales). La frecuencia sigue siendo constante.

Si nos fijamos en la Figura 3.53 podemos observar las diferencias de amplitud.

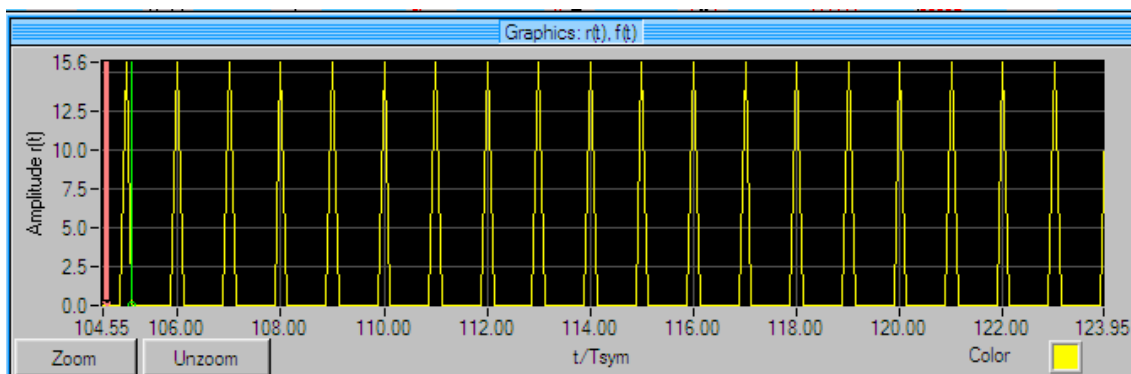


Figura 3.53 Señal después de sufrir la influencia de una señal multicamino con retardo y atenuación. Podemos observar que la amplitud de la señal ha crecido respecto a la misma señal sin la influencia del multicamino.

Sin embargo, si la señal multicamino sufre una distorsión en su fase, observamos que la frecuencia de la señal recibida sufre variaciones.

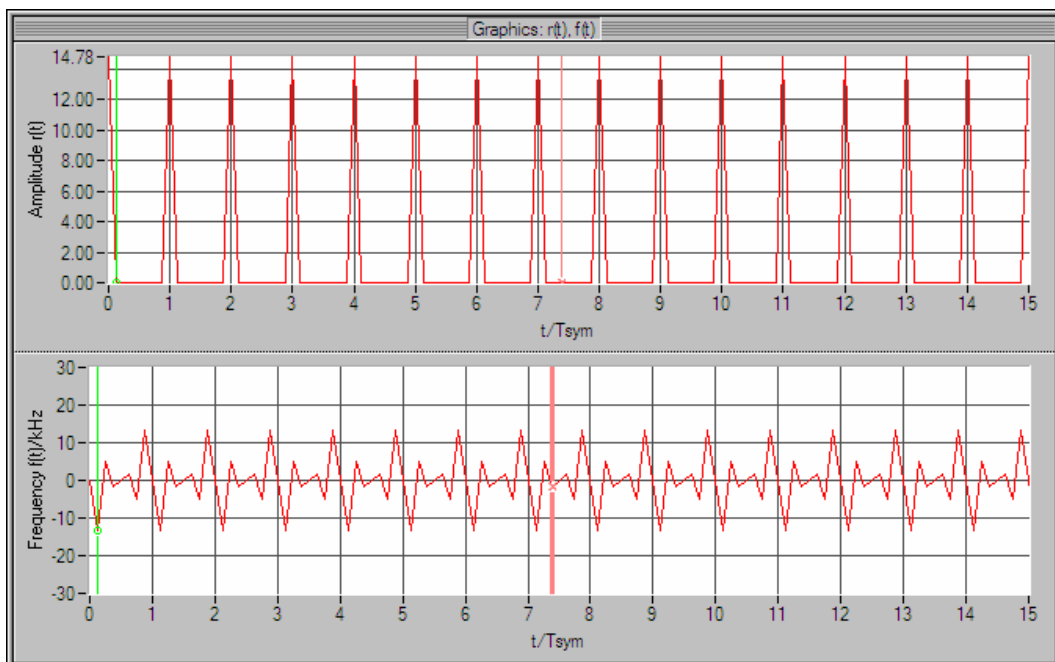


Figura 3.54 Observamos la distorsión en la frecuencia provocada por una señal multicamino con un cierto desfase respecto a la original.

Esta distorsión en la fase no nos provoca un gran inconveniente ya que la frecuencia no afecta a las intenciones de la onda continua y, por otro lado, la ganancia en amplitud provocada por la superposición de las señales nos supone una ventaja ya que así la etiqueta tendrá una potencia mayor para transmitir su respuesta.

### Ruido

La influencia del ruido en la onda continua es pequeña, ya que aún teniendo una relación señal a ruido relativamente baja (15dB) y un ancho de banda del ruido que es igual al de la señal que enviamos, obtenemos como resultado una gráfica que nos muestra como el tag seguirá estando alimentado, sufriendo unas pequeñas fluctuaciones en la potencia recibida (debido a las variaciones que supone el ruido en la amplitud de la señal).

En la gráfica que tenemos a continuación podemos observar:

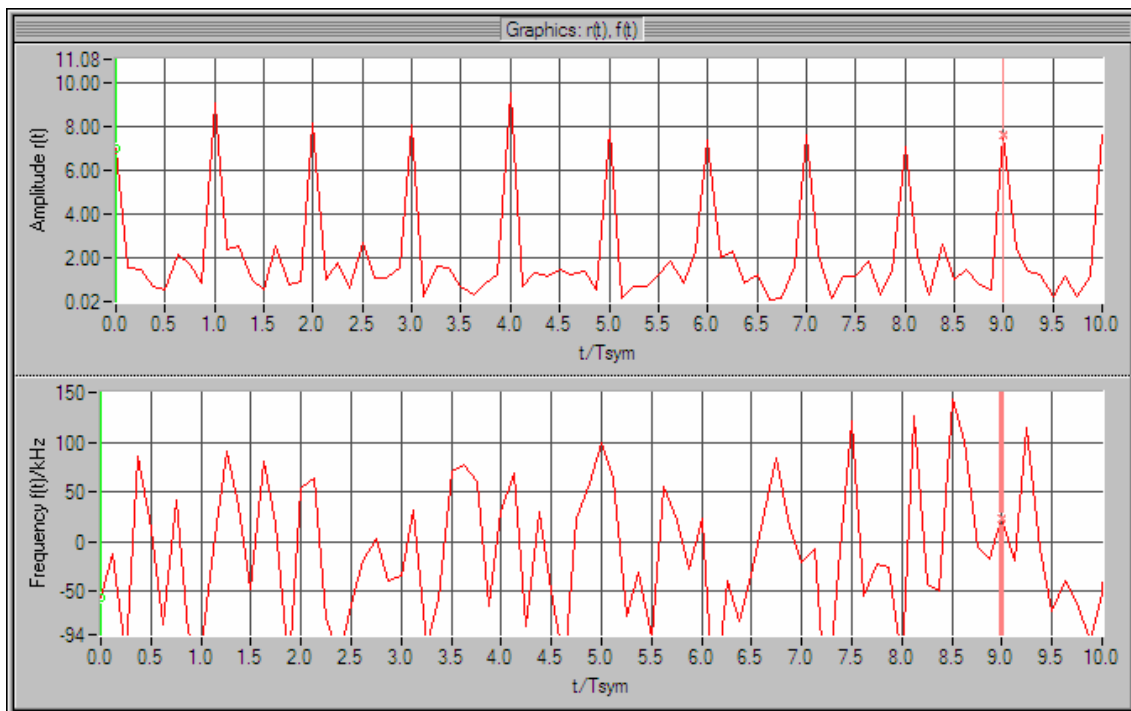


Figura 3.55 Influencia del ruido en la onda continua (CW)

## **4. GLOSARIO**

*AUTO-ID CENTER*: Equipo de investigación del MIT (Massachusetts Institute of Technology) dedicado al estudio de RFID.

*Bit Error Rate (BER)*: La proporción del número de bits recibidos que son considerados erróneos del total de bits transmitidos.

*Cyclic Redundancy Check (CRC)*: Algoritmo de detección de errores que explota las ventajas del módulo-2 aritmético para generarlo.

*EAN (European Article Number)*: Es el principal estándar de código de barras.

*EAS (Electronic Article Surveillance)*: Sistemas basados en un único bit de información en los transponders, usado principalmente como sistema antirrobo en almacenes y establecimientos.

*EEPROM (Electrically Erasable Programmable read-only memory)*: Memoria más usada en los sistemas con acoplamiento inductivo. Tiene unos ciclos de escritura limitados y un consumo alto de batería.

*Effective Isotropic Radiated Power (EIRP)*: El producto de la potencia de entrada de la antena y la ganancia relativa a una fuente isotrópica.

*EPC*: Siglas de Código Electrónico de Producto (Electronic Product Code).

*FRAM (Ferromagnetic Random Acces Memory)*: Memoria usada en sistemas de RFID más complejos que posee mejor tiempo de escritura y mejor consumo que la memoria EEPROM.

*Full Duplex (FDX)*: Canal de comunicaciones que permite la transmisión de datos en ambas direcciones al mismo tiempo.

*Half Duplex (HDX)*: Canal de comunicaciones que permite la transmisión de datos en ambas direcciones pero no al mismo tiempo.

*Modulación Backscatter*: Proceso donde el transponder responde a la señal del lector, modulando y retransmitiendo una señal con la misma frecuencia portadora.

*RAM*: Siglas de Random Access Memory. Memoria de acceso aleatoria y volátil.

*RFID (Radio Frequency IDentification)*: Sistema de identificación automática y capturadora de datos que comprende uno o más lectores y uno más transponders que realizan la comunicación a determinada frecuencia.

*ROM*: Siglas de Read Only Memory. Se trata de memoria de sólo lectura.

*SRAM (Static Random Acces Memory)*: Memoria más utilizada en los sistemas RFID de microondas. Mejor ciclo de escritura a cambio de un suministro de energía continuo por una batería auxiliar.

*TAG*: término sinónimo a transponder, usado especialmente por la AIM.

*TRANSPONDER (TRANSMitter-resPONDER)*: Elemento de los sistemas RFID capaz de recibir la información del lector y de transmitir su información aprovechando la energía del propio lector o con ayuda de una alimentación externa.

*Trazabilidad*: Concepto de seguimiento de datos sobre un producto, desde su fabricación hasta su venta.

*UPC (Universal Product Code)*: Principal estándar de código de barras en EEUU.



## **5. BIBLIOGRAFÍA**

---

*860MHz – 930MHz Class I Radio Frequency Identification Tag Radio Frequency & Logical Communication Interface Specification Candidate Recommendation, version 1.0.1.* Auto-Id Center.

---

*AIM Global Standard for the use of the AIM RFID Mark and Index to Identify RFID Enabled labels,* 2004. AIM Inc.

---

*Antenas,* 1998. Ángel Cardama, Lluís Jofre Roca, Juan Manuel Rius Casals, Jordi Romeu Robert, Sebastián Blanch Boris, Miguel Fernando Bataller. Edicions UPC.

---

*Antenna Circuit Design for RFID Applications,* Youbok Lee. Ph.D. Microchip Technology Inc.

---

*Asignatura “Seguridad en redes telemáticas. Curso 2003/04”* Diatel. UPM

---

*Beyond Passive RFID Tags,* White Paper 2004. Sensitech.

---

*CC1000: Single Chip Very Low Power RF Transceiver, datasheet v.2.2.* Chipcon.

---

*CC1000PP: Reference design v.3.1.* Chipcon

---

*Comentarios al documento de trabajo sobre protección de datos de carácter personal en relación con la tecnología RFID de 19 de Enero de 2005 (WP 105).* Comisión de Libertades e Informática.

---

*Draft Paper on the Characteristics of RFID-Systems,* July 2000. AIM Frequency Forums.

---

*EPC and Radio Frequency Identification (RFID) Standards,* White Paper: Larry Blue, Kevin Powel. Matrics Inc.

---

*EPC Tag Data Standards Version 1.1 Rev. 1.24., Standard Specification 01,* April 2004. EPCglobal Inc.

---

*ETSI EN 302 208-1 v.1.1.1: Electromagnetic compatibility and Radio Spectrum Matters (ERM); Radio Frequency Identification Equipment operating in the band 865MHz to 868MHz with power levels up to 2W; Part 1: Technical requirements and methods of measurement.* ETSI

---

*ETSI EN 302 208-2 v.1.1.1: Electromagnetic compatibility and Radio Spectrum Matters (ERM); Radio Frequency Identification Equipment operating in the band 865MHz to 868MHz with power levels up to 2W; Part 2: Harmonized EN under article 3.2 of the R&TTE Directive.* ETSI.

---

*HF Antenna Design Notes, Technical Application Notes,* 2003. Texas Instruments.

---

*Integrating the Electronic Product Code (EPC) and the Global Trade Item Number (GTIN),* David L. Brock. Auto-Id Center.

---

*ISO 14443, An introduction to the contactless standard for smart cards and its relevance to costumers.* ISO.

---

---

*Multi-Band, Low-Cost EPC Tag Reader*, White Paper: Matthew Reynolds, Joseph Richards, Sumukh Pathare, Harry Tsai, Yael Maguire, Rehmi Post, Ravikanth Pappu, Bernd Schoner. Auto-Id Center.

---

*Passive, Active RFID Tags Linked*. RFID Journal July 2003.

---

*Radio Frecuencia. EPC (Código Electrónico de Producto)*, Marianella Arava Arava. EAN Costa Rica.

---

*RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification, Second Edition*, Klaus Finkenzeller. Copyright 2003 John Wiley & Sons, Ltd.

---

*RFID tags: Big Brother in small packages*, Declan McCullagh, January 2003

---

*Shrouds of Time, The history of RFID*. AIM Inc

---

*Smart tags: RFID becomes the new bar code*, 2003. IBM Business Consulting Service

---

*The physics of RFID*, Matt Reynolds Founding Partner. ThingMagic LLC

---

*The Reader Collision Problem*, Daniel W. Engels. Auto-Id Center.

---

*Tiris Automatic recognition of consumers: Series 5000 Readers system*. Texas Instruments.

---

# ANEXO I

En este anexo se especifican otras características del chip CC1000 y de la placa CC1000PP que son importantes para su implementación.

### Rangos Máximos Absolutos

Parameter	Min.	Max.	Units	Condition
Supply voltage, VDD	-0.3	5.0	V	
Voltage on any pin	-0.3	VDD+0.3, max 5.0	V	
Input RF level		10	dBm	
Storage temperature range	-50	150	°C	
Reflow soldering temperature		260	°C	T = 10 s

### Condiciones de Trabajo

Parameter	Min.	Typ.	Max.	Unit	Condition / Note
RF Frequency Range	300		1000	MHz	Programmable in steps of 250 Hz
Operating ambient temperature range	-40		85	°C	
Supply voltage	2.1	3.0	3.6	V	Note: The same supply voltage should be used for digital (DVDD) and analogue (AVDD) power.

### Especificaciones eléctricas

T<sub>c</sub> = 25°C, VDD = 3.0 V if nothing else stated

Parameter	Min.	Typ.	Max.	Unit	Condition / Note
<b>Transmit Section</b>					
Transmit data rate	0.6		76.8	kBaud	NRZ or Manchester encoding. 76.8 kBaud equals 76.8 kbit/s using NRZ coding. See page 16.
Binary FSK frequency separation	0		65	kHz	The frequency separation is programmable in 250 Hz steps. 65 kHz is the maximum guaranteed separation at 1 MHz reference frequency. Larger separations can be achieved at higher reference frequencies.
Output power 433 MHz 868 MHz	-20 -20		10 5	dBm dBm	Delivered to 50 Ω load. The output power is programmable.

Parameter	Min.	Typ.	Max.	Unit	Condition / Note
RF output impedance 433/868 MHz		140 / 80		$\Omega$	Transmit mode. For matching details see "Input/ output matching" p.31.
Harmonics		-20		dBc	An external LC or SAW filter should be used to reduce harmonics emission to comply with SRD requirements. See p.36.
<b>Receive Section</b>					
Receiver Sensitivity, 433 MHz Optimum sensitivity (9.3 mA) Low current consumption (7.4 mA)		-110 -109		dBm dBm	2.4 kBaud, Manchester coded data, 64 kHz frequency separation, BER = $10^{-3}$
Receiver Sensitivity, 868 MHz Optimum sensitivity (11.8 mA) Low current consumption (9.6 mA)		-107 -105		dBm dBm	See Table 6 and Table 7 page 22 for typical sensitivity figures at other data rates.
System noise bandwidth		30		KHz	2.4 kBaud, Manchester coded data
Cascaded noise figure 433/868 MHz		12/13		dB	
Saturation	10			dBm	2.4 kBaud, Manchester coded data, BER = $10^{-3}$
Input IP3		-18		dBm	From LNA to IF output
Blocking		40		dBc	At +/- 1 MHz
LO leakage			-57	dBm	
Input impedance		88-j26 70-j26 52-j7 52-j4		$\Omega$ $\Omega$ $\Omega$ $\Omega$	Receive mode, series equivalent at 315 MHz at 433 MHz at 868 MHz. at 915 MHz For matching details see "Input/ output matching" p. 31.
Turn on time	11		128	Baud	The turn-on time is determined by the demodulator settling time, which is programmable. See p. 19
<b>IF Section</b>					
Intermediate frequency (IF)		150	10.7	kHz MHz	Internal IF filter External IF filter
IF bandwidth		175		kHz	
RSSI dynamic range	-105		-50	dBm	
RSSI accuracy		$\pm 6$		dB	See p.33 for details
RSSI linearity		$\pm 2$		dB	

Parameter	Min.	Typ.	Max.	Unit	Condition / Note
<b>Frequency Synthesiser Section</b>					
Crystal Oscillator Frequency	3		16	MHz	Crystal frequency can be 3-4, 6-8 or 9-16 MHz. Recommended frequencies are 3.6864, 7.3728, 11.0592 and 14.7456. See page 35 for details.
Crystal frequency accuracy requirement		± 50 ± 25		ppm	433 MHz 868 MHz The crystal frequency accuracy and drift (ageing and temperature dependency) will determine the frequency accuracy of the transmitted signal.
Crystal operation		Parallel			C171 and C181 are loading capacitors, see page 35
Crystal load capacitance	12 12 12	22 16 16	30 30 16	pF pF pF	3-4 MHz, 22 pF recommended 6-8 MHz, 16 pF recommended 9-16 MHz, 16 pF recommended
Crystal oscillator start-up time		5 1.5 2		ms ms ms	3.6864 MHz, 16 pF load 7.3728 MHz, 16 pF load 16 MHz, 16 pF load
Output signal phase noise		-85		dBc/Hz	At 100 kHz offset from carrier
PLL lock time (RX / TX turn time)		200		µs	Up to 1 MHz frequency step
PLL turn-on time, crystal oscillator on in power down mode		250		µs	Crystal oscillator running
<b>Digital Inputs/Outputs</b>					
Logic "0" input voltage	0		0.3*VDD	V	
Logic "1" input voltage	0.7*VDD		VDD	V	
Logic "0" output voltage	0		0.4	V	Output current -2.5 mA, 3.0 V supply voltage
Logic "1" output voltage	2.5		VDD	V	Output current 2.5 mA, 3.0 V supply voltage
Logic "0" input current	NA		-1	µA	Input signal equals GND
Logic "1" input current	NA		1	µA	Input signal equals VDD
DIO setup time	20			ns	TX mode, minimum time DIO must be ready before the positive edge of DCLK
DIO hold time	10			ns	TX mode, minimum time DIO must be held after the positive edge of DCLK
Serial interface (PCLK, PDATA and PALE) timing specification					See Table 2 page 14

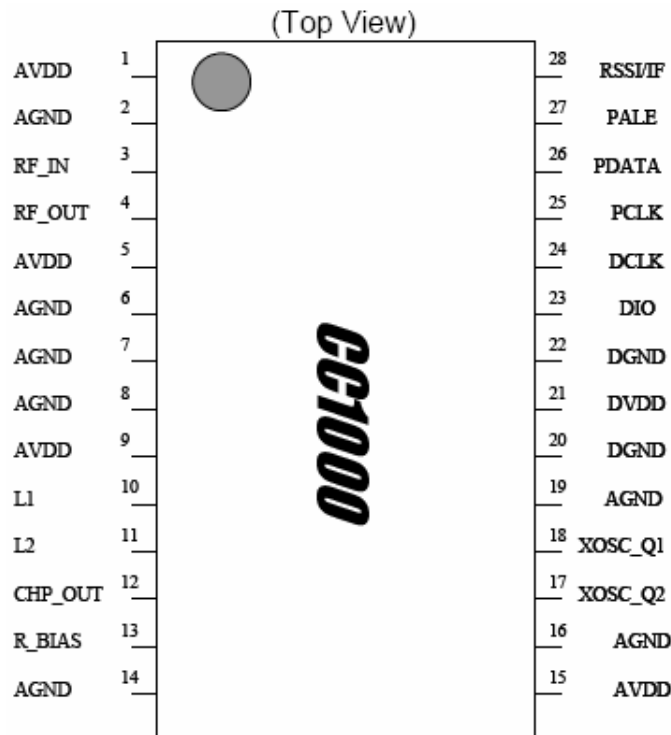
Parameter	Min.	Typ.	Max.	Unit	Condition / Note
<b>Current Consumption</b>					
Power Down mode		0.2	1	μA	Oscillator core off
Current Consumption, receive mode 433/868 MHz		7.4/9.6		mA	Current is programmable and can be increased for improved sensitivity
Current Consumption, average in receive mode using polling 433/868 MHz		74/96		μA	Polling controlled by micro-controller using 1:100 receive to power down ratio
Current Consumption, transmit mode 433/868 MHz:					
P=0.01mW (-20 dBm)		5.3/8.6		mA	The output power is delivered to a 50Ω load, see also p. 32
P=0.3 mW (-5 dBm)		8.9/13.8		mA	
P=1 mW (0 dBm)		10.4/16.5		mA	
P=3 mW (5 dBm)		14.8/25.4		mA	
P=10 mW (10 dBm)		26.7/NA		mA	
Current Consumption, crystal osc.		30 80 105		μA μA μA	3-8 MHz, 16 pF load 9-14 MHz, 12 pF load 14-16 MHz, 16 pF load
Current Consumption, crystal osc. and bias		860		μA	
Current Consumption, crystal osc., bias and synthesiser, RX/TX		4/5 5/6		mA mA	< 500 MHz > 500 MHz



**Asignación de Pins**

Pin no.	Pin name	Pin type	Description
1	AVDD	Power (A)	Power supply (3 V) for analog modules (mixer and IF)
2	AGND	Ground (A)	Ground connection (0 V) for analog modules (mixer and IF)
3	RF_IN	RF Input	RF signal input from antenna
4	RF_OUT	RF output	RF signal output to antenna
5	AVDD	Power (A)	Power supply (3 V) for analog modules (LNA and PA)
6	AGND	Ground (A)	Ground connection (0 V) for analog modules (LNA and PA)
7	AGND	Ground (A)	Ground connection (0 V) for analog modules (PA)
8	AGND	Ground (A)	Ground connection (0 V) for analog modules (VCO and prescaler)
9	AVDD	Power (A)	Power supply (3 V) for analog modules (VCO and prescaler)
10	L1	Analog input	Connection no 1 for external VCO tank inductor
11	L2	Analog input	Connection no 2 for external VCO tank inductor
12	CHP_OUT (LOCK)	Analog output	Charge pump current output The pin can also be used as PLL Lock indicator. Output is high when PLL is in lock.
13	R_BIAS	Analog output	Connection for external precision bias resistor (82 kΩ, ± 1%)
14	AGND	Ground (A)	Ground connection (0 V) for analog modules (backplane)
15	AVDD	Power (A)	Power supply (3 V) for analog modules (general)
16	AGND	Ground (A)	Ground connection (0 V) for analog modules (general)
17	XOSC_Q2	Analog output	Crystal, pin 2
18	XOSC_Q1	Analog input	Crystal, pin 1, or external clock input
19	AGND	Ground (A)	Ground connection (0 V) for analog modules (guard)
20	DGND	Ground (D)	Ground connection (0 V) for digital modules (substrate)
21	DVDD	Power (D)	Power supply (3 V) for digital modules
22	DGND	Ground (D)	Ground connection (0 V) for digital modules
23	DIO	Digital input/output	Data input/output. Data input in transmit mode. Data output in receive mode
24	DCLK	Digital output	Data clock for data in both receive and transmit mode
25	PCLK	Digital input	Programming clock for 3-wire bus
26	PDATA	Digital input/output	Programming data for 3-wire bus. Programming data input for write operation, programming data output for read operation
27	PALE	Digital input	Programming address latch enable for 3-wire bus. Internal pull-up.
28	RSSI/IF	Analog output	The pin can be used as RSSI or 10.7 MHz IF output to optional external IF and demodulator. If not used, the pin should be left open (not connected).

A=Analog, D=Digital



### Especificaciones de tiempo en interfaz serie

Parameter	Symbol	Min	Max	Units	Conditions
PCLK, clock frequency	$F_{\text{CLOCK}}$	-	10	MHz	
PCLK low pulse duration	$T_{\text{CL,min}}$	50		ns	The minimum time PCLK must be low.
PCLK high pulse duration	$T_{\text{CH,min}}$	50		ns	The minimum time PCLK must be high.
PALE setup time	$T_{\text{SA}}$	10	-	ns	The minimum time PALE must be low before negative edge of PCLK.
PALE hold time	$T_{\text{HA}}$	10	-	ns	The minimum time PALE must be held low after the <i>positive</i> edge of PCLK.
PDATA setup time	$T_{\text{SD}}$	10	-	ns	The minimum time data on PDATA must be ready before the negative edge of PCLK.
PDATA hold time	$T_{\text{HD}}$	10	-	ns	The minimum time data must be held at PDATA, after the negative edge of PCLK.
Rise time	$T_{\text{rise}}$		100	ns	The maximum rise time for PCLK and PALE
Fall time	$T_{\text{fall}}$		100	ns	The maximum fall time for PCLK and PALE

Note: The set-up- and hold-times refer to 50% of VDD.

### Sensibilidad de receptor en función de la velocidad e transmisión y separación de frecuencia

Data rate [kBaudo]	Separation [kHz]	433 MHz			868 MHz		
		NRZ mode	Manchester mode	UART mode	NRZ mode	Manchester mode	UART mode
0.6	64	-113	-114	-113	-110	-111	-110
1.2	64	-111	-112	-111	-108	-109	-108
2.4	64	-109	-110	-109	-106	-107	-106
4.8	64	-107	-108	-107	-104	-105	-104
9.6	64	-105	-106	-105	-102	-103	-102
19.2	64	-103	-104	-103	-100	-101	-100
38.4	64	-102	-103	-102	-98	-99	-98
76.8	64	-100	-101	-100	-97	-98	-97
Average current consumption		9.3 mA			11.8 mA		

*Separación de frecuencia 64 KHz.*

Data rate [kBaud]	Separation [kHz]	433 MHz			868 MHz		
		NRZ mode	Manchester mode	UART mode	NRZ mode	Manchester mode	UART mode
0.6	20	-109	-111	-109	-106	-108	-106
1.2	20	-108	-110	-108	-104	-106	-104
2.4	20	-106	-108	-106	-103	-105	-103
4.8	20	-104	-106	-104	-101	-103	-101
9.6	20	-103	-104	-103	-100	-101	-100
19.2	20	-102	-103	-102	-99	-100	-99
38.4	20	-98	-100	-98	-98	-99	-98
76.8	20	-94	-98	-94	-94	-96	-94
Average current consumption		9.3 mA			11.8 mA		

*Separación de frecuencia 20 KHz.*

### Configuración recomendada para frecuencias ISM

ISM Frequency [MHz]	Actual frequency [MHz]	Crystal frequency [MHz]	Low-side / high-side / LO*	Reference divider REFDIV (decimal)	Frequency word RX mode FREQ (decimal)	Frequency word RX mode FREQ (hex)
315	315.037200	3.6864	High-side	3	4194304	400000
		7.3728		6	4194304	400000
		11.0592		9	4194304	400000
		14.7456		12	4194304	400000
433.3	433.302000	3.6864	Low-side	3	5775168	580000
		7.3728		6	5775168	580000
		11.0592		9	5775168	580000
		14.7456		12	5775168	580000
433.9	433.916400	3.6864	Low-side	3	5775360	582000
		7.3728		6	5775360	582000
		11.0592		9	5775360	582000
		14.7456		12	5775360	582000
434.5	434.530800	3.6864	Low-side	3	5783552	584000
		7.3728		6	5783552	584000
		11.0592		9	5783552	584000
		14.7456		12	5783552	584000
868.3	868.297200	3.6864	Low-side	2	7708672	75A000
		7.3728		4	7708672	75A000
		11.0592		6	7708672	75A000
		14.7456		8	7708672	75A000
868.95	868.918800	3.6864	High-side	2	7716864	75C000
		7.3728		4	7716864	75C000
		11.0592		6	7716864	75C000
		14.7456			7716864	75C000
869.525	869.526000	3.6864	Low-side	3	11583488	B0C000
		7.3728		6	11583488	B0C000
		11.0592		9	11583488	B0C000
		14.7456		12	11583488	B0C000
869.85	869.840400	3.6864	High-side	2	7725056	75E000
		7.3728		4	7725056	75E000
		11.0592		6	7725056	75E000
		14.7456		8	7725056	75E000
915	914.998800	3.6864	High-side	2	8126464	7C0000
		7.3728		4	8126464	7C0000
		11.0592		6	8126464	7C0000
		14.7456		8	8126464	7C0000

### Sensibilidad del receptor en fusión del consumo de corriente

RF frequency [MHz]	Current consumption [mA]	Sensitivity [dBm]	CURRENT register			FRONT_END register	
			VCO_CURRENT [3:0]	LO_DRIVE [1:0]	PA_DRIVE [1:0]	BUF_CURRENT	LNA_CURRENT[1:0]
433	9.3	-110	0100	01	00	0	10
433	7.4	-109	0100	00	00	0	00
868	11.8	-107	1000	11	00	1	10
868	9.6	-105	1000	10	00	0	00

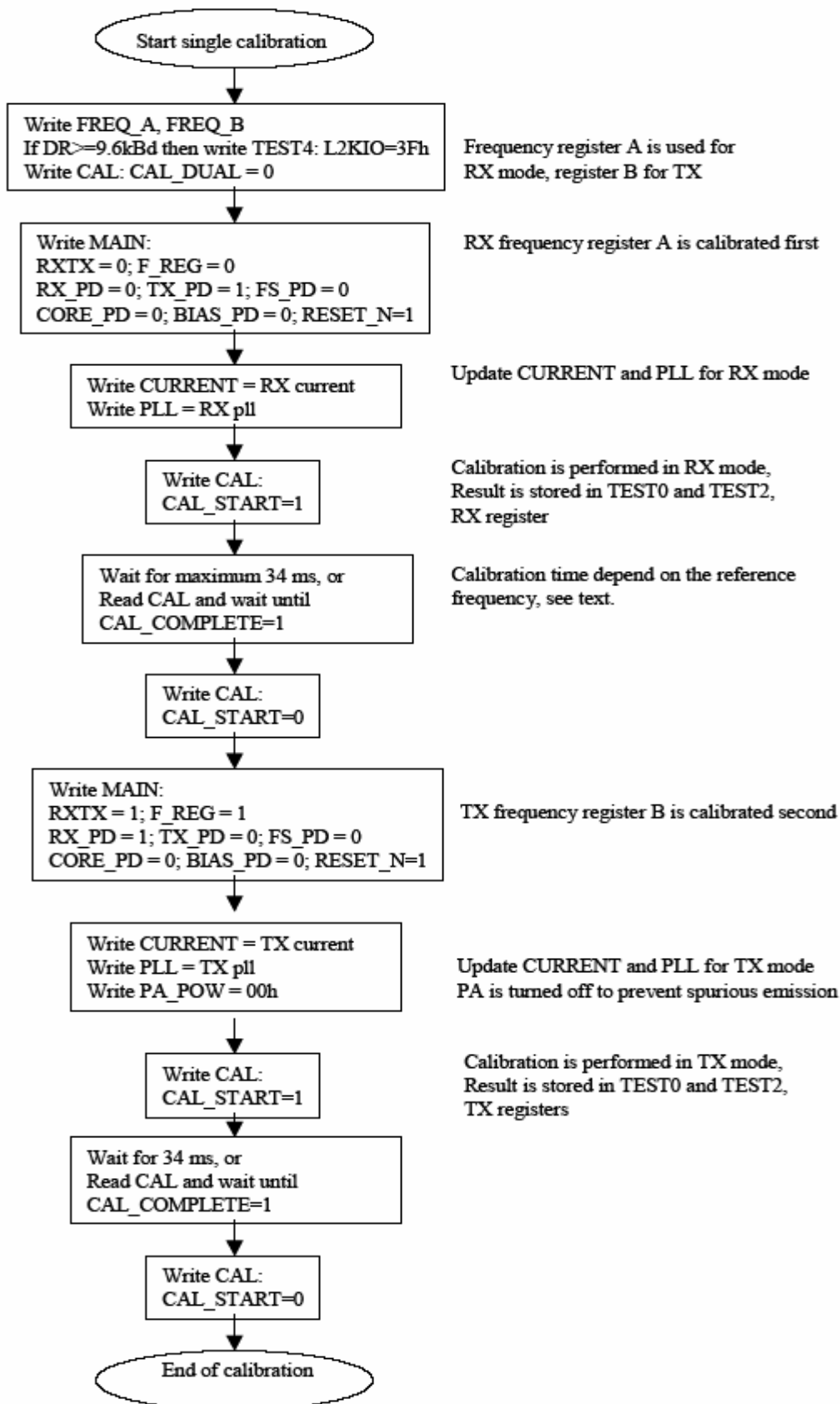
Note: Current consumption and sensitivity are typical figures at 2.4 kBaud Manchester encoded data, BER  $10^{-3}$

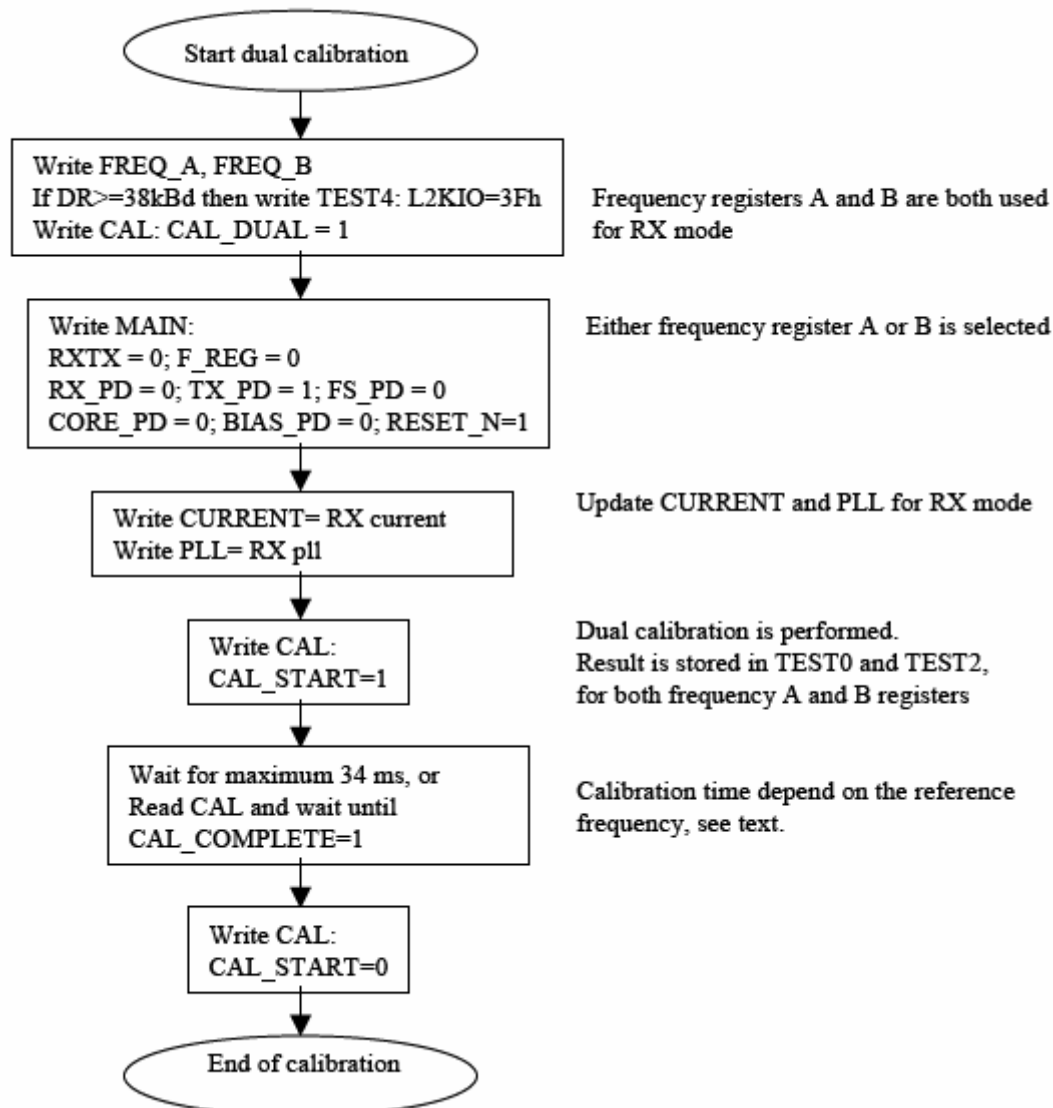
### Potencia de salida y consumo típico

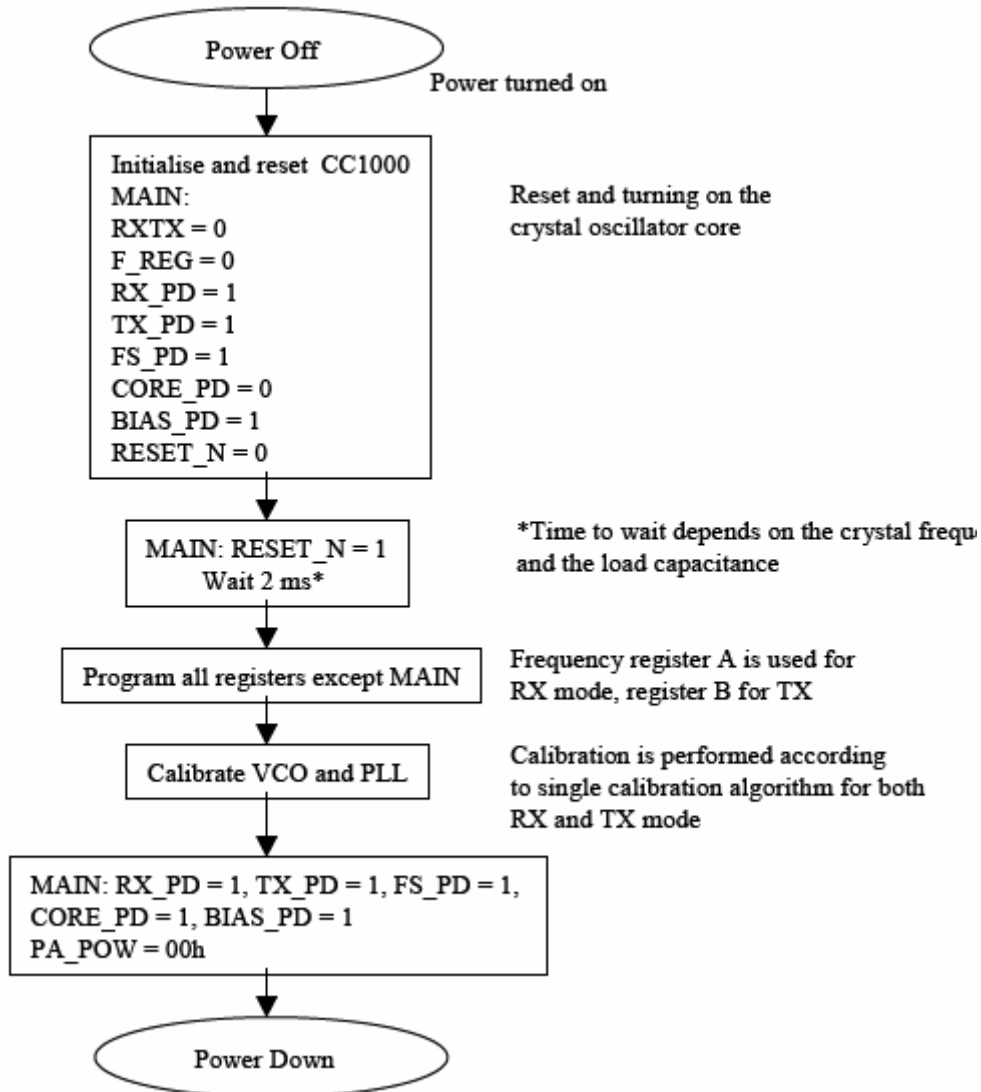
Output power [dBm]	RF frequency 433 MHz		RF frequency 868 MHz	
	PA POW [hex]	Current consumption, typ. [mA]	PA POW [hex]	Current consumption, typ. [mA]
-20	01	5.3	02	8.6
-19	01	6.9	02	8.8
-18	02	7.1	03	9.0
-17	02	7.1	03	9.0
-16	02	7.1	04	9.1
-15	03	7.4	05	9.3
-14	03	7.4	05	9.3
-13	03	7.4	06	9.5
-12	04	7.6	07	9.7
-11	04	7.6	08	9.9
-10	05	7.9	09	10.1
-9	05	7.9	0B	10.4
-8	06	8.2	0C	10.6
-7	07	8.4	0D	10.8
-6	08	8.7	0F	11.1
-5	09	8.9	40	13.8
-4	0A	9.6	50	14.5
-3	0B	9.4	50	14.5
-2	0C	9.7	60	15.1
-1	0E	10.2	70	15.8
0	0F	10.4	80	16.8
1	40	11.8	90	17.2
2	50	12.8	B0	18.5
3	50	12.8	C0	19.2
4	60	13.8	F0	21.3
5	70	14.8	FF	25.4
6	80	15.8		
7	90	16.8		
8	C0	20.0		
9	E0	22.1		
10	FF	26.7		

**Procesos**

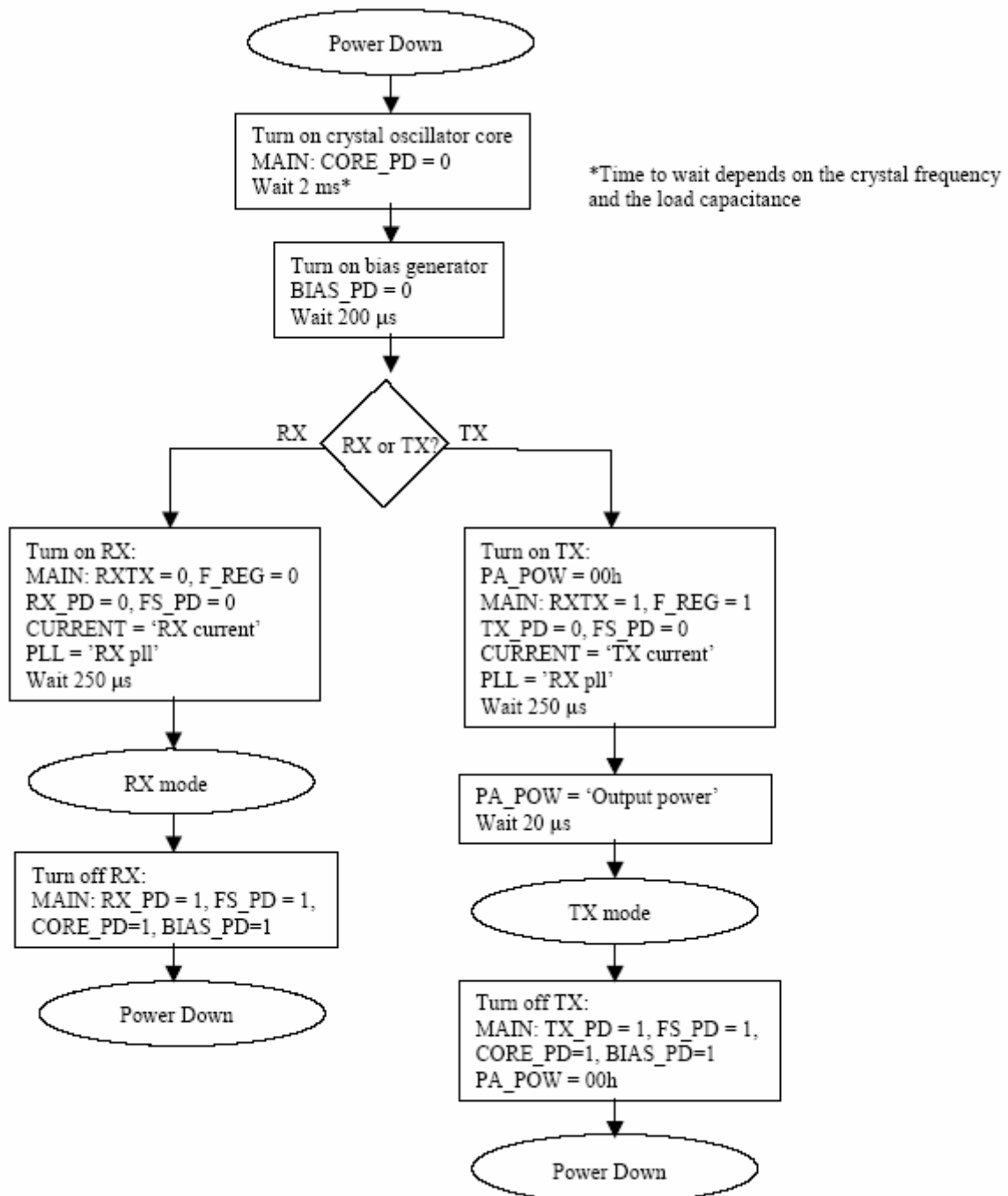
*Algoritmo de calibración de Tx y Rx*



*Calibración dual para Rx*

*Secuencia de inicialización*

Secuencia de activación Rx y Tx





## Registros de configuración

### REGISTER OVERVIEW

ADDRESS	Byte Name	Description
00h	MAIN	MAIN Register
01h	FREQ_2A	Frequency Register 2A
02h	FREQ_1A	Frequency Register 1A
03h	FREQ_0A	Frequency Register 0A
04h	FREQ_2B	Frequency Register 2B
05h	FREQ_1B	Frequency Register 1B
06h	FREQ_0B	Frequency Register 0B
07h	FSEP1	Frequency Separation Register 1
08h	FSEP0	Frequency Separation Register 0
09h	CURRENT	Current Consumption Control Register
0Ah	FRONT_END	Front End Control Register
0Bh	PA_POW	PA Output Power Control Register
0Ch	PLL	PLL Control Register
0Dh	LOCK	LOCK Status Register and signal select to CHP_OUT (LOCK) pin
0Eh	CAL	VCO Calibration Control and Status Register
0Fh	MODEM2	Modem Control Register 2
10h	MODEM1	Modem Control Register 1
11h	MODEM0	Modem Control Register 0
12h	MATCH	Match Capacitor Array Control Register for RX and TX impedance matching
13h	FSCTRL	Frequency Synthesiser Control Register
14h		Reserved
15h		Reserved
16h		Reserved
17h		Reserved
18h		Reserved
19h		Reserved
1Ah		Reserved
1Bh		Reserved
1Ch	PRESCALER	Prescaler and IF-strip test control register
40h	TEST6	Test register for PLL LOOP
41h	TEST5	Test register for PLL LOOP
42h	TEST4	Test register for PLL LOOP (must be updated as specified)
43h	TEST3	Test register for VCO
44h	TEST2	Test register for Calibration
45h	TEST1	Test register for Calibration
46h	TEST0	Test register for Calibration

MAIN Register (00h)

REGISTER	NAME	Default value	Active	Description
MAIN[7]	RXTX	-	-	RX/TX switch, 0 : RX , 1 : TX
MAIN[6]	F_REG	-	-	Selection of Frequency Register, 0 : Register A, 1 : Register B
MAIN[5]	RX_PD	-	H	Power Down of LNA, Mixer, IF, Demodulator, RX part of Signal Interface
MAIN[4]	TX_PD	-	H	Power Down of TX part of Signal Interface, PA
MAIN[3]	FS_PD	-	H	Power Down of Frequency Synthesiser
MAIN[2]	CORE_PD	-	H	Power Down of Crystal Oscillator Core
MAIN[1]	BIAS_PD	-	H	Power Down of BIAS (Global_Current_Generator) and Crystal Oscillator Buffer
MAIN[0]	RESET_N	-	L	Reset, active low. Writing RESET_N low will write default values to all other registers than MAIN. Bits in MAIN do not have a default value, and will be written directly through the configurations interface. Must be set high to complete reset.

FREQ\_2A Register (01h)

REGISTER	NAME	Default value	Active	Description
FREQ_2A[7:0]	FREQ_A[23:16]	01110101	-	8 MSB of frequency control word A

FREQ\_1A Register (02h)

REGISTER	NAME	Default value	Active	Description
FREQ_1A[7:0]	FREQ_A[15:8]	10100000	-	Bit 15 to 8 of frequency control word A

FREQ\_0A Register (03h)

REGISTER	NAME	Default value	Active	Description
FREQ_0A[7:0]	FREQ_A[7:0]	11001011	-	8 LSB of frequency control word A

FREQ\_2B Register (04h)

REGISTER	NAME	Default value	Active	Description
FREQ_2B[7:0]	FREQ_B[23:16]	01110101	-	8 MSB of frequency control word B

FREQ\_1B Register (05h)

REGISTER	NAME	Default value	Active	Description
FREQ_1B[7:0]	FREQ_B[15:8]	10100101	-	Bit 15 to 8 of frequency control word B

FREQ\_0B Register (06h)

REGISTER	NAME	Default value	Active	Description
FREQ_0B[7:0]	FREQ_B[7:0]	01001110	-	8 LSB of frequency control word B

FSEP1 Register (07h)

REGISTER	NAME	Default value	Active	Description
FSEP1[7:3]	-	-	-	Not used
FSEP1[2:0]	FSEP_MSB[2:0]	000	-	3 MSB of frequency separation control

FSEP0 Register (08h)

REGISTER	NAME	Default value	Active	Description
FSEP0[7:0]	FSEP_LSB[7:0]	01011001	-	8 LSB of frequency separation control

CURRENT Register (09h)

REGISTER	NAME	Default value	Active	Description
CURRENT[7:4]	VCO_CURRENT[3:0]	1100	-	Control of current in VCO core for TX and RX 0000 : 150µA 0001 : 250µA 0010 : 350µA 0011 : 450µA 0100 : 950µA, use for RX, f= 400 - 500 MHz 0101 : 1050µA 0110 : 1150µA 0111 : 1250µA 1000 : 1450µA, use for RX, f<400 MHz and f>500 MHz; and TX, f= 400 - 500 MHz 1001 : 1550µA, use for TX, f<400 MHz 1010 : 1650µA 1011 : 1750µA 1100 : 2250µA 1101 : 2350µA 1110 : 2450µA 1111 : 2550µA, use for TX, f>500 MHz
CURRENT[3:2]	LO_DRIVE[1:0]	10		Control of current in VCO buffer for LO drive 00 : 0.5mA, use for TX 01 : 1.0mA, use for RX, f<500 MHz* 10 : 1.5mA, 11 : 2.0mA, use for RX, f>500 MHz *  * LO_DRIVE can be reduced to save current in RX mode. See Table 10 for details
CURRENT[1:0]	PA_DRIVE[1:0]	10		Control of current in VCO buffer for PA 00 : 1mA, use for RX 01 : 2mA, use for TX, f<500 MHz 10 : 3mA 11 : 4mA, use for TX, f>500 MHz

FRONT\_END Register (0Ah)

REGISTER	NAME	Default value	Active	Description
FRONT_END[7:6]	-	00	-	Not used
FRONT_END[5]	BUF_CURRENT	0	-	Control of current in the LNA_FOLLOWER 0 : 520uA, use for f<500 MHz 1 : 690uA, use for f>500 MHz *  *BUF_CURRENT can be reduced to save current in RX mode. See Table 10 for details.
FRONT_END[4:3]	LNA_CURRENT [1:0]	01	-	Control of current in LNA 00 : 0.8mA, use for f<500 MHz * 01 : 1.4mA 10 : 1.8mA, use for f>500 MHz * 11 : 2.2mA  *LNA_CURRENT can be reduced to save current in RX mode. See Table 10 for details.
FRONT_END[2:1]	IF_RSSI[1:0]	00	-	Control of IF_RSSI pin 00 : Internal IF and demodulator, RSSI inactive 01 : RSSI active, RSSI/IF is analog RSSI output 10 : External IF and demodulator, RSSI/IF is mixer output. Internal IF in power down mode. 11 : Not used
FRONT_END[0]	XOSC_BYPASS	0	-	0 : Internal XOSC enabled 1 : Power-Down of XOSC, external CLK used

PA\_POW Register (0Bh)

REGISTER	NAME	Default value	Active	Description
PA_POW[7:4]	PA_HIGHPOWER[3:0]	0000	-	Control of output power in high power array. Should be 0000 in PD mode. See Table 11 page 32 for details.
PA_POW[3:0]	PA_LOWPOWER[3:0]	1111	-	Control of output power in low power array. Should be 0000 in PD mode. See Table 11 page 32 for details.

PLL Register (0Ch)

REGISTER	NAME	Default value	Active	Description
PLL[7]	EXT_FILTER	0	-	1 : External loop filter 0 : Internal loop filter  1-to-0 transition samples F_COMP comparator when BREAK_LOOP=1 (TEST3)
PLL[6:3]	REFDIV[3:0]	0010	-	Reference divider  0000 : Not allowed 0001 : Not allowed 0010 : Divide by 2 0011 : Divide by 3 ..... 1111 : Divide by 15
PLL[2]	ALARM_DISABLE	0	h	0 : Alarm function enabled 1 : Alarm function disabled
PLL[1]	ALARM_H	-	-	Status bit for tuning voltage out of range (too close to VDD)
PLL[0]	ALARM_L	-	-	Status bit for tuning voltage out of range (too close to GND)

LOCK Register (0Dh)

REGISTER	NAME	Default value	Active	Description
LOCK[7:4]	LOCK_SELECT[3:0]	0000	-	Selection of signals to CHP_OUT (LOCK) pin  0000 : Normal, pin can be used as CHP_OUT 0001 : LOCK_CONTINUOUS (active high) 0010 : LOCK_INSTANT (active high) 0011 : ALARM_H (active high) 0100 : ALARM_L (active high) 0101 : CAL_COMPLETE (active high) 0110 : IF_OUT 0111 : REFERENCE_DIVIDER Output 1000 : TX_PDB (active high, activates external PA when TX_PD=0) 1001 : Manchester Violation (active high) 1010 : RX_PDB (active high, activates external LNA when RX_PD=0) 1011 : Not defined 1100 : Not defined 1101 : LOCK_AVG_FILTER 1110 : N_DIVIDER Output 1111 : F_COMP
LOCK[3]	PLL_LOCK_ACCURACY	0	-	0 : Sets Lock Threshold = 127, Reset Lock Threshold = 111. Corresponds to a worst case accuracy of 0.7% 1 : Sets Lock Threshold = 31, Reset Lock Threshold = 15. Corresponds to a worst case accuracy of 2.8%
LOCK[2]	PLL_LOCK_LENGTH	0	-	0 : Normal PLL lock window 1 : Not used
LOCK[1]	LOCK_INSTANT	-	-	Status bit from Lock Detector
LOCK[0]	LOCK_CONTINUOUS	-	-	Status bit from Lock Detector

CAL Register (0Eh)

REGISTER	NAME	Default value	Active	Description
CAL[7]	CAL_START	0	↑	↑ 1 : Calibration started 0 : Calibration inactive CAL_START must be set to 0 after calibration is done
CAL[6]	CAL_DUAL	0	H	1 : Store calibration in both A and B 0 : Store calibration in A or B defined by MAIN[6]
CAL[5]	CAL_WAIT	0	H	1 : Normal Calibration Wait Time 0 : Half Calibration Wait Time  The calibration time is proportional to the internal reference frequency. 2 MHz reference frequency gives 14 ms wait time.
CAL[4]	CAL_CURRENT	0	H	1 : Calibration Current Doubled 0 : Normal Calibration Current
CAL[3]	CAL_COMPLETE	0	H	Status bit defining that calibration is complete
CAL[2:0]	CAL_ITERATE	101	H	Iteration start value for calibration DAC 000 - 101: Not used 110 : Normal start value 111 : Not used

MODEM2 Register (0Fh)

REGISTER	NAME	Default value	Active	Description
MODEM2[7]	PEAKDETECT	1	H	Peak Detector and Remover disabled or enabled 0 : Peak detector and remover is disabled 1 : Peak detector and remover is enabled
MODEM2[6:0]	PEAK_LEVEL_OFFSET[6:0]	0010110	-	Threshold level for Peak Remover in Demodulator. Correlated to frequency deviation, see note.

Note:  $PEAK\_LEVEL\_OFFSET[6:0] = \frac{F_s}{IF_{low}} - \frac{F_s}{IF_{low} + \Delta f} \cdot \frac{5}{8}$  where  $F_s = \frac{f_{xosc}}{XOSC\_FREQ + 1}$

and  $IF_{low} = 150kHz - 2 \cdot f_{rf} \cdot XTAL\_accuracy$  and  $\Delta f$  is the separation

MODEM1 Register (10h)

REGISTER	NAME	Default value	Active	Description
MODEM1[7:5]	MLIMIT	011	-	Sets the limit for the Manchester Violation Flag. A Manchester Value = 14 is a perfect bit and a Manchester Value = 0 is a constant level (an unbalanced corrupted bit)  000 : No Violation Flag is set 001 : Violation Flag is set for Manchester Value < 1 010 : Violation Flag is set for Manchester Value < 2 011 : Violation Flag is set for Manchester Value < 3 100 : Violation Flag is set for Manchester Value < 4 101 : Violation Flag is set for Manchester Value < 5 110 : Violation Flag is set for Manchester Value < 6 111 : Violation Flag is set for Manchester Value < 7
MODEM1[4]	LOCK_AVG_IN	0	H	Lock control bit of Average Filter  0 : Average Filter is free-running 1 : Average Filter is locked
MODEM1[3]	LOCK_AVG_MODE	0	-	Automatic lock of Average Filter  0 : Lock of Average Filter is controlled automatically 1 : Lock of Average Filter is controlled by LOCK_AVG_IN
MODEM1[2:1]	SETTLING[1:0]	11	-	Settling Time of Average Filter  00 : 11 baud settling time, worst case 1.2dB loss in sensitivity 01 : 22 baud settling time, worst case 0.6dB loss in sensitivity 10 : 43 baud settling time, worst case 0.3dB loss in sensitivity 11 : 86 baud settling time, worst case 0.15dB loss in sensitivity
MODEM1[0]	MODEM_RESET_N	1	L	Separate reset of MODEM

MODEM0 Register (11h)

REGISTER	NAME	Default value	Active	Description
MODEM0[7]	-	-	-	Not used
MODEM0[6:4]	BAUDRATE[2:0]	010	-	000 : 0.6 kBaud 001 : 1.2 kBaud 010 : 2.4 kBaud 011 : 4.8 kBaud 100 : 9.6 kBaud 101 : 19.2, 38.4 and 76.8 kBaud 110 : Not used 111 : Not used
MODEM0[3:2]	DATA_FORMAT[1:0]	01	-	00 : NRZ operation. 01 : Manchester operation 10 : Transparent Asynchronous UART operation 11 : Not used
MODEM0[1:0]	XOSC_FREQ[1:0]	00	-	Selection of XTAL frequency range 00 : 3MHz - 4MHz crystal, 3.6864MHz recommended Also used for 76.8 kBaud, 14.7456MHz 01 : 6MHz - 8MHz crystal, 7.3728MHz recommended Also used for 38.4 kBaud, 14.7456MHz 10 : 9MHz - 12MHz crystal, 11.0592 MHz recommended 11 : 12MHz - 16MHz crystal, 14.7456MHz recommended

MATCH Register (12h)

REGISTER	NAME	Default value	Active	Description
MATCH[7:4]	RX_MATCH[3:0]	0000	-	Selects matching capacitor array value for RX, step size is 0.4 pF 0001: Use for RF frequency > 500 MHz 0111: Use for RF frequency < 500 MHz
MATCH[3:0]	TX_MATCH[3:0]	0000	-	Selects matching capacitor array value for TX, step size is 0.4 pF

FSCTRL Register (13h)

REGISTER	NAME	Default value	Active	Description
FSCTRL[7:4]	-	-	-	Not used
FSCTRL[3:1]				Reserved
FSCTRL[0]	FS_RESET_N	1	L	Separate reset of frequency synthesizer

PRESCALER Register (1Ch)

REGISTER	NAME	Default value	Active	Description
PRESCALER[7:6]	PRE_SWING[1:0]	00	-	Prescaler swing. Fractions for PRE_CURRENT[1:0] = 00  00 : 1 * Nominal Swing 01 : 2/3 * Nominal Swing 10 : 7/3 * Nominal Swing 11 : 5/3 * Nominal Swing
PRESCALER[5:4]	PRE_CURRENT [1:0]	00	-	Prescaler current scaling  00 : 1 * Nominal Current 01 : 2/3 * Nominal Current 10 : 1/2 * Nominal Current 11 : 2/5 * Nominal Current
PRESCALER[3]	IF_INPUT	0	-	0 : Nominal setting 1 : RSSI/IF pin is input to IF-strips
PRESCALER[2]	IF_FRONT	0	-	0 : Nominal setting 1 : Output of IF_Front_amp is switched to RSSI/IF pin
PRESCALER[1:0]	-	00	-	Not used

TEST6 Register (for test only, 40h)

REGISTER	NAME	Default value	Active	Description
TEST6[7]	LOOPFILTER_TP1	0	-	1 : Select testpoint 1 to CHP_OUT 0 : CHP_OUT tied to GND
TEST6 [6]	LOOPFILTER_TP2	0	-	1 : Select testpoint 2 to CHP_OUT 0 : CHP_OUT tied to GND
TEST6 [5]	CHP_OVERRIDE	0	-	1 : use CHP_CO[4:0] value 0 : use calibrated value
TEST6[4:0]	CHP_CO[4:0]	10000	-	Charge_Pump Current DAC override value

TEST5 Register (for test only, 41h)

REGISTER	NAME	Default value	Active	Description
TEST5[7:6]	-	-	-	Not used
TEST5[5]	CHP_DISABLE	0	-	1 : CHP up and down pulses disabled 0 : normal operation
TEST5[4]	VCO_OVERRIDE	0	-	1 : use VCO_AO[2:0] value 0 : use calibrated value
TEST5[3:0]	VCO_AO[3:0]	1000	-	VCO_ARRAY override value

TEST4 Register (for test only, 42h)

REGISTER	NAME	Default value	Active	Description
TEST4[7:6]	-	-	-	Not used
TEST4[5:0]	L2KIO[5:0]	100101	h	Constant setting charge pump current scaling/rounding factor. Sets Bandwidth of PLL. Use 3Fh for 9.6 kBaud and higher



TEST3 Register (for test only, 43h)

REGISTER	NAME	Default value	Active	Description
TEST3[7:5]	-	-	-	Not used
TEST3[4]	BREAK_LOOP	0	-	1 : PLL loop open 0 : PLL loop closed
TEST3[3:0]	CAL_DAC_OPEN	0100	-	Calibration DAC override value, active when BREAK_LOOP =1

TEST2 Register (for test only, 44h)

REGISTER	NAME	Default value	Active	Description
TEST2[7:5]	-	-	-	Not used
TEST2[4:0]	CHP_CURRENT [4:0]	-	-	Status vector defining applied CHP_CURRENT value

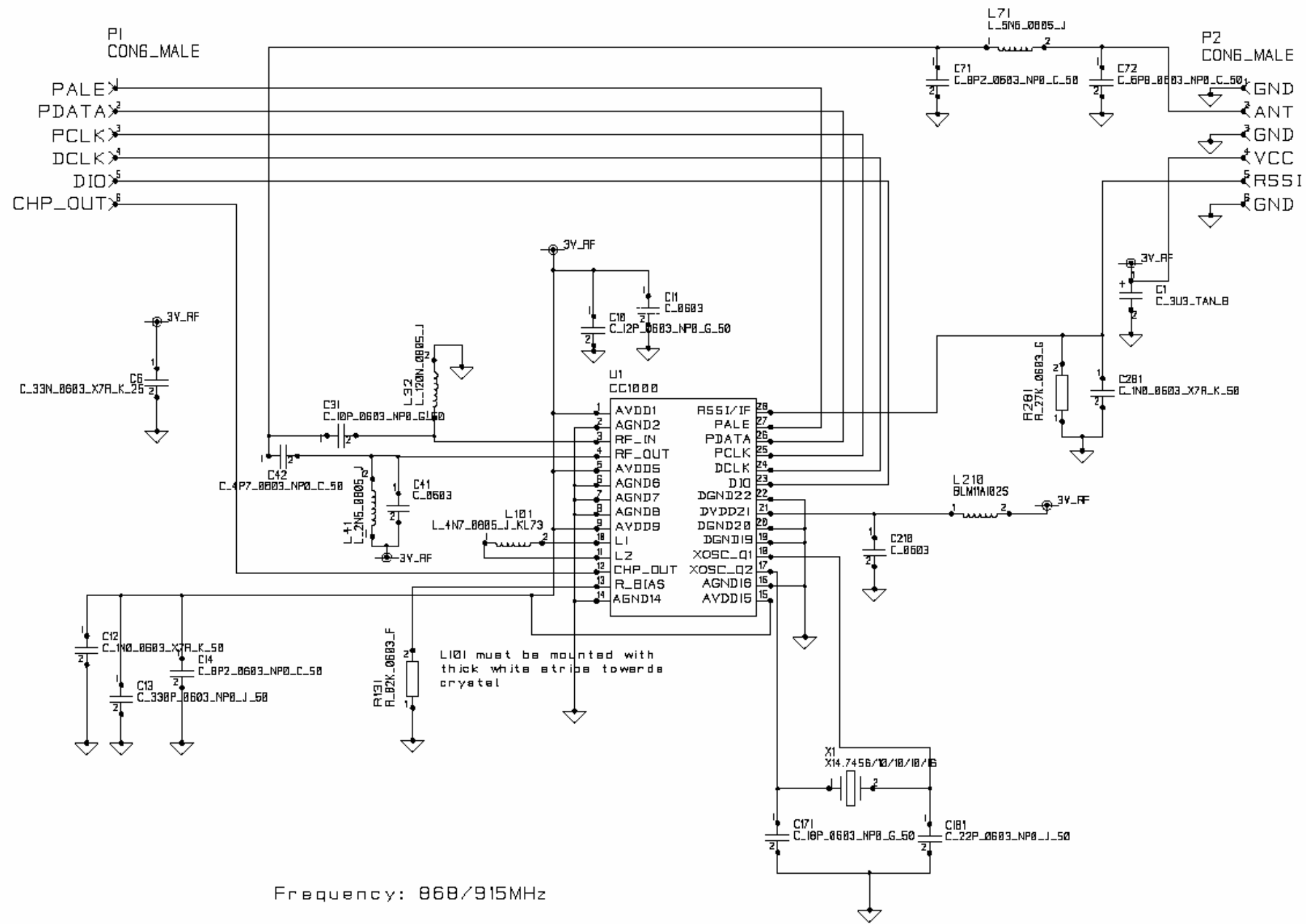
TEST1 Register (for test only, 45h)

REGISTER	NAME	Default value	Active	Description
TEST1[7:4]	-	-	-	Not used
TEST1[3:0]	CAL_DAC[3:0]	-	-	Status vector defining applied Calibration DAC value

TEST0 Register (for test only, 46h)

REGISTER	NAME	Default value	Active	Description
TEST0[7:4]	-	-	-	Not used
TEST0[3:0]	VCO_ARRAY[3:0]	-	-	Status vector defining applied VCO_ARRAY value

# **ANEXO II**



PROJECT NO. 02519		COMPANY NAME CHIPCON A5			
APPROVALS	DATE	DWG CC1000PP 868/915MHz			
DRAWN	KHT	SIZE A3	FSCM NO.	DWG NO.	REV. 3.1
CHECKED		SCALE			SHEET 1/1
ISSUED					

Esquema de la placa