



UNIVERSIDAD NACIONAL  
AUTÓNOMA DE  
MÉXICO

UNIVERSIDAD NACIONAL AUTÓNOMA  
DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES  
ARAGÓN

**“CONVERGENCIA E INTEROPERABILIDAD  
DE LOS SISTEMAS MOVILES HANDHELD  
3G CON EL RFID EN EL PROTOCOLO NFC”**

**T E S I S**

QUE PARA OBTENER EL TÍTULO DE:  
INGENIERO MECÁNICO ELECTRICISTA  
(AREA ELECTRICA-ELECTRONICA)

P R E S E N T A:  
LUIS DANIEL RAMIREZ ROJAS

ASESOR: ING. PABLO LUNA ESCORZA



FES Aragón

MEXICO 2008



Universidad Nacional  
Autónoma de México

Dirección General de Bibliotecas de la UNAM

**Biblioteca Central**



**UNAM – Dirección General de Bibliotecas**  
**Tesis Digitales**  
**Restricciones de uso**

**DERECHOS RESERVADOS ©**  
**PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL**

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

## **AGRADECIMIENTOS**

A mi todo: Valery Ivett, gracias por tu amor, comprensión y por el tiempo que deje de convivir contigo para la culminación de este sueño.

A mi familia, especialmente a mi hermano Gabriel, porque sin su apoyo no hubiera logrado cumplir esta meta, pero sobre todo a mi madre, por ser mi ejemplo a seguir y porque a ella debo todo lo que soy.

Al maestro Carlos Reyes Martínez por su apoyo académico, sus valiosos comentarios y paciencia en la revisión de este texto.

A mi amiga Ana Rosa, porque sin saberlo, es un ejemplo profesional para mi, por sus consejos y apoyo a lo largo de mi vida.

Por último, a Francisco, por impulsarme, su cariño y por darme un motivo más para seguir adelante.

## *Agradecimiento especial.*

*Dedicado a la memoria de mi padre el Sr. Sergio Ramírez y de mi hermano Raúl a quienes les debo muchos recuerdos, valores y enseñanzas sin las cuales no habría podido entender lo trascendental de una actitud en la vida. Papá, espero puedas estar viendo todo desde donde estás, espero puedas estar orgulloso de todos nosotros, me has hecho falta. Hermano te nos adelantaste en el camino pero siempre estuviste peleando contra las adversidades, gracias por aclararnos un poco la ruta y enseñarnos esa fuerza de carácter y voluntad para cambiar las cosas y hacer la diferencia. Sé que al final podré verlos de nuevo, mientras tanto aquí esta un pequeño homenaje...*

*Mamá, gracias por estar siempre ahí señora incansable, te agradezco por que a pesar de tus enfermedades siempre has tenido fe y has dado tu vida entera sin vacilación por nosotros, te debo muchas cosas y quizá nunca te podré pagar pero lo que sí puedo hacer es quererte mucho Regina Rojas.*

*Hermano Pato representas al hermano mayor y me has apoyado como un padre, solo puedo agradecerte y espero no defraudarte nunca, me hago ingeniero debido a tu ejemplo profesional, gracias Ingeniero Fausto Sergio. Hermana Roxana, gracias por quererme tanto y apoyarme siempre, me diste las llaves de tu hogar en el que me sentí como en mi propia casa cuando lo necesité. En general tengo que agradecer a todos mis hermanos quienes de una u otra forma me han brindado su apoyo en este largo trayecto y que tanto han hecho por mí .....sólo puedo mencionarlos a continuación: Roxana, Sergio, Laura, Miguel, Claudia, Raúl y Lilitiana, ustedes saben por lo que hemos pasado, Dios los bendiga a ustedes y sus familias, gracias por todo.*

*Deseo también agradecer a Dios por todas las personas con las que he vivido diferentes etapas y aprendizajes; mis amigos, cada uno de ustedes sabe lo que significa el valor de esa categoría por eso es que así los considero. Clara, gracias por ser el estímulo y motor de esta importante etapa eres mi persona favorita, ¡que bueno conocerte!*

*A la Universidad Nacional Autónoma de México y los profesores que ahí laboran, cada uno de ellos hace posible el desarrollo de esta institución de la cual todos estamos orgullosos.*

*Por mi raza hablará el espíritu...*

# **CONVERGENCIA E INTEROPERABILIDAD DE LOS SISTEMAS MOVILES HANDHELD 3G CON EL RFID EN EL PROTOCOLO NFC**

## **INDICE GENERAL**

OBJETIVO GENERAL.....	1
JUSTIFICACIÓN.....	2
INTRODUCCIÓN.....	3

### **Capítulo 1. Introducción al RFID**

1.1 Contexto del RFID.....	7
1.2 Espectro de Frecuencia y Pérdidas por Propagación Atmosférica.....	8
1.3 Aplicaciones Inalámbricas .....	11
1.4. Sistemas Celulares en los Estados Unidos, Europa y Japón .....	15
1.5 Telefonía Inalámbrica.....	21
1.6 Sistemas Wireless LAN.....	25
1.7 Sistemas de Comunicación Satelital.....	26
1.8 Sistemas Inalámbricos del Futuro .....	30

### **Capítulo 2. IC y los Tipos de Modulación**

2.1 Introducción.....	39
2.2 Circuitos Integrados (IC).....	41
2.3 Fabricación de un Circuito Integrado.....	44
2.4 Tipos de Chip o Integrado .....	48
2.5 Modulación.....	51

### **Capítulo 3. Historia del RFID en las Comunicaciones**

3.1 Introducción.....	65
3.2 El Siglo XX.....	66
3.4 Visión Histórica de la Comunicación Satelital.....	70
3.5 Génesis de Una Idea .....	75
3.6 De los años 60's a los 80's: RFID se vuelve una realidad .....	75
3.7 La Década de los 90 .....	77
3.8 La Actualidad del RFID .....	79

## **Capítulo 4. Bases RFID**

4.1 Introducción.....	83
4.2 Radio Frequency Identification Devices (RFID) .....	84
4.3 La Interface Aérea y la Comunicación Inalámbrica.....	85
4.4 Las Frecuencias Portadoras .....	87
4.5 Tasa de Transferencia de Datos y Ancho de Banda .....	88, 89
4.6 Rango (alcance) y Niveles de Potencia .....	89
4.7 Transponders o Tags .....	91
4.8 El Lector o Interrogador .....	104
4.9 Los Programadores de Transponder.....	104
4.10 Categorías en los sistemas RFID.....	105
4.11 Estandarización. ....	106

## **Capítulo 5. El RFID en las comunicaciones 3G, protocolo NFC**

5.1 Introducción.....	109
5.2 Requerimientos RFID Actuales.....	110
5.3 Las Aplicaciones RFID .....	148
5.4 Near Field Communications (NFC) .....	138

## **Capítulo 6. Codificación y Modulación**

6 Codificación y Modulación .....	159
6.1 Codificación en Banda Base.....	159
6.2 Procedimientos de Modulación Digital .....	162
6.3 Integridad de Datos .....	165
6.4 Seguridad de los Datos .....	175

## **Capítulo 7. Áreas Abiertas a Discusión**

7.1 Introducción.....	183
7.2 Amenazas a la Privacidad y las Libertades Civiles.....	183
7.3 Limitaciones de la tecnología RFID: Mito y Realidad.....	187
7.4 Valoración de las soluciones propuestas en la industria .....	189

CONCLUSIONES.....	193
BIBLIOGRAFÍA.....	194
I. GLOSARIO DE TERMINOS.....	196
I.A. TERMINOS GENERALES RFID.....	196
I.B. TERMINOS ESPECÍFICOS NFCIP-1 .....	201
II. ACRÓNIMOS EN NFCIP-1.....	203

## **OBJETIVO GENERAL.**

El presente trabajo esta hecho con la finalidad de presentar al protocolo NFC como un potencial impulsor de distintos servicios de valor agregado para muchas de las compañías de telefonía celular que implementen 3G no sin antes dar un panorama del desarrollo de los sistemas de identificación electrónicos, su evolución y principios que han llegado a dar forma a los mas evolucionados sistemas de identificación, seguimiento y control así como a ingeniosas variantes de estas tecnologías para dar pie a soluciones complejas de interactividad tecnológica que involucra a distintas disciplinas del área de las telecomunicaciones como por ejemplo la ya antes mencionada tercera generación de telefonía móvil.

Específicamente en las siguientes páginas nos referiremos a la tecnología RFID cuyas siglas en inglés significan "Identificación por Radiofrecuencia" y su relación con la telefonía móvil que es otra tecnología que implica a las señales radiales para su operación pero que a diferencia de RFID, ahora se encuentra bastante bien establecida y aceptada en el mercado mundial. El NFC es una tecnología derivada del RFID y es el protocolo en donde convergen e interactúan tanto la tecnología telefónica así como la tecnología de identificación por radio, sus siglas en inglés significan comunicación de campo cercano.

Así pues, el NFC bien puede ser aplicado desde prepago para el metro o también como monedero electrónico y muchas aplicaciones y servicios que solo la imaginación puede establecer como límite debido a que es una tecnología sencilla pero muy versátil y compatible con otras tecnologías actualmente existentes.

De lo anterior que el presente tratado introduzca parcialmente en cada capítulo las tecnologías que han tenido que ver con la historia de las comunicaciones y haga énfasis en la implementación y adopción de NFC ya que este protocolo no es mas que el siguiente paso hacia sistemas de comunicación mas automatizados y seguros a su vez. Lo que se sustenta a continuación es el NFC como una tecnología alterna que servirá para hacer transferencias de archivos, prepagos para el transporte público, pago de servicios, monedero electrónico...etc, todo con la facilidad de acercar un dispositivo con esta capacidad a otro y sin que la persona deba efectuar ninguna configuración extra o conocer el manejo del otro dispositivo al que se requiere conectar o incluso sin configurar el propio dispositivo de la persona, lo cual en inglés se define mas fácilmente como "touch and go".

## JUSTIFICACIÓN.

La tendencia a la convergencia hacia sistemas electrónicos y automatizados ya no es una novedad, en la actualidad se está viviendo una realidad global que abarca diferentes aspectos de la vida cotidiana. Desde la explosión de la televisión, la telefonía, las aplicaciones móviles y el internet se han venido originando sucesos en la historia de las telecomunicaciones que han marcado de una forma positiva los ámbitos en donde operan.

En el caso de la tecnología NFC que aquí se justifica, tenemos actualmente muy pocas referencias prácticas aún, sin embargo la teoría es muy sólida y en la parte de implementación ha habido un crecimiento significativo en los últimos años, tan es así que principalmente en Europa en donde ya se ha implementado algunos sistemas similares se tiene ya pensado que los mismos serán una herramienta imprescindible hacia finales de esta década y que marcará un hito en las comunicaciones tal como ha sido el caso del internet.

Por lo tanto parte del objetivo de este tratado es el de dar un vistazo a las posibilidades que se tienen con esta tecnología y se justifica por sí solo al contemplar las bondades que tiene como medio de mejora en almacenamiento, intercambio e identificación por nombrar las principales características. Por ejemplo cuando se tiene la necesidad de adquirir un bien, cuando se tiene la necesidad de compartir información, cuando se tiene necesidad de disponer de efectivo o incluso cuando queramos ver algún video en el televisor desde nuestro iPod, por supuesto que todo lo anterior no es ninguna novedad, lo que sí es novedad es que todo lo antes mencionado se pueda hacer con un solo dispositivo de manera inalámbrica y sin tener que configurar ninguno de los aparatos electrónicos involucrados en los procesos mencionados, en cambio lo único que se deberá hacer será acercar un dispositivo a pocos centímetros del otro para que se pueda dar la comunicación entre dichos dispositivos.

## INTRODUCCIÓN.

Las largas filas en los centros comerciales, son una de las grandes quejas del público en general acerca de la tarea del consumidor, no obstante llegan a convertirse en grandes pérdidas económicas en algunas temporadas donde la gente hace compras de pánico o visitas regulares a los autoservicios, por ejemplo en época navideña. Bien, estas largas filas pueden muy pronto ser parte de un pasado el cual nos agrada recordar como una cómica anécdota de primitivas formas de comercio, todo esto será posible gracias a que el hasta ahora funcional código UPC de barras será reemplazado por etiquetas inteligentes, también llamadas *Dispositivos de Identificación por Radiofrecuencia (RFID)*, que servirán entre otras cosas para que usted pueda al terminar de hacer sus compras, caminar directamente hacia la puerta de salida del establecimiento, sin tener ninguna clase de problemas judiciales, por ejemplo.

Imagine las posibilidades, usted se encuentra comprando dentro de un establecimiento que cuenta con las certificaciones para RFID, entonces, usted podrá tener acceso desde su organizador personal o teléfono celular al estado de su despensa, con lo cual, el organizador le sugerirá que artículos ingresar al carrito de compras, así como también el poder llevar la contabilidad de su dinero, y las posibilidades de adquisición de cierto artículo, incluso podrá cargársele a su cuenta bancaria el monto total de los artículos una vez finalizada su compra.

Todo lo anterior podría formar parte de un panorama muy amplio de posibilidades que nos da el utilizar este tipo de etiquetas inteligentes en los productos que se ofrecen al consumidor, conjugando la tecnología de tercera generación celular con cierto protocolo llamado NFC, sin embargo en el uso de estas, existen riesgos de los cuales se pueden deducir muy fácilmente algunos y se pueden prevenir, aunque siempre existirá un cierto porcentaje de incertidumbre, esta incertidumbre es la que ha llevado a grandes controversias acerca del uso de esta tecnología. RFID es una tecnología con profundas implicaciones sociales, usada indiscriminadamente puede atentar seriamente la privacidad del consumidor, reducir o eliminar el anonimato del comprador y amenazar las libertades civiles.

Es por esto que las organizaciones y los individuos se han unido al afán de buscar una solución para estas limitantes al despliegue completo de la tecnología, el propósito de éste tratado, es pues, en esencia poner sobre la mesa los argumentos tecnológicos más adecuados con los que se cuenta en la actualidad, para así ayudar a tomar un criterio respecto de esta tecnología, que tarde o temprano irremediamente será adoptada en la mayor parte del planeta, debido en gran parte al afán de muchos desarrolladores y la gente involucrada por proporcionar un servicio de proyección futurista, pero que, tecnológicamente podemos hablar de una realidad.

Entonces surge la pregunta -¿qué es RFID?-, la respuesta es que se trata de una tecnología basada en la capacidad de obtener mas información, de una forma fácil de usar, no importa de qué tipo de información estemos hablando, identificación de personas, cosas, seguimiento de objetos, u otros aspectos que requieran de la fácil disponibilidad de datos.

Cabe destacar que RFID no es aún un reemplazo para los códigos de barras, hoy en día un código de barras impreso en una caja de cornflakes por ejemplo, es prácticamente gratis, la tinta extra para pintar la simbología de código de barras es despreciable y no dispara el costo del producto tan considerablemente como una etiqueta inteligente RFID, además un código de barras hace un gran trabajo cuando se trata de identificar productos, la identificación de productos es una aplicación con licencia que no cambia de un paquete de cornflakes a otro.

En un futuro con el desarrollo de la tecnología de microchips y generación de radiofrecuencia, la perspectiva de las etiquetas es que posiblemente podrá tener una reducción en los costos conforme aumente la tecnología de fabricación, técnicas en las cuales ya trabajan las principales compañías del mundo como Texas Instruments por citar alguna.

Por ahora si consideramos una etiqueta RFID, podremos ver la gran flexibilidad que ofrece la etiqueta y el valor agregado que se puede notar al utilizarlo en conjunto con el sistema de código de barras, sin embargo como mencionamos anteriormente, éste no es el mayor problema al que se enfrenta la tecnología, al aplicarla, se tienen que tomar en cuenta algunas implicaciones sociales que consideraremos aquí.

En las siguientes páginas se estará dando una descripción más profunda y detallada acerca de los elementos que conforman al RFID, las interfaces de interacción con el medio, así como también se asentarán las bases de las tarjetas inteligentes de no-contacto que son esenciales para entender el funcionamiento del protocolo NFC (Near Field Communications) que permite conjugar la funcionalidad del RFID con los servicios de telefonía celular o mercados de consumo en general, todo lo anterior como parte de la integración, convergencia e interoperabilidad de los mencionados sistemas entre sí, también se tomará en cuenta algunas de las sugerencias y medidas que se han establecido para fines de mejorar un futuro servicio y podremos ver algunas de las diversas aplicaciones de esta tecnología.

# ***CAPÍTULO 1***

## **CONTEXTO DEL RFID EN LAS COMUNICACIONES**

1.1 Contexto del RFID.....	7
1.2 Espectro de Frecuencia y Pérdidas por Propagación Atmosférica .....	8
1.3 Aplicaciones Inalámbricas .....	11
1.3.1 El Espectro Radioeléctrico.....	12
1.3.2 Sistemas de comunicación celular .....	12
1.3.3 Telefonía inalámbrica .....	14
1.3.4 Sistemas satelitales.....	15
1.4. Sistemas Celulares en los Estados Unidos, Europa y Japón ....	15
1.4.1. Sistemas celulares análogos.....	16
1.4.2 Sistema digital celular.....	17
1.4.2.1 Global System Mobile .....	17
1.4.2.2 NADC .....	19
1.4.2.3 Personal Digital Cellular.....	19
1.4.3 Sistemas de Acceso Múltiple por División de Código.....	20
1.4.3.1 Modo de operación Dual de CDMA .....	21

1.5 Telefonía Inalámbrica .....	21
1.5.1 Teléfonía Inalámbrica Analógica.....	22
1.5.2 Telefonía inalámbrica digital .....	22
1.5.2.1 Sistemas CT2/CT2+ .....	22
1.5.2.2 Sistema DECT .....	23
1.5.2.3 Sistema Personal Handyphone (PHS).....	24
1.5.3 WACS/PACS.....	24
1.5.4 DCS 1800.....	25
1.6 Sistemas Wireless LAN .....	25
1.7 Sistemas de Comunicación Satelital .....	26
1.7.1 Sistema Iridium.....	26
1.7.2 Sistema Globalstar .....	29
1.7.3 El Sistema ICO-P.....	30
1.8 Sistemas Inalámbricos del Futuro .....	30
1.8.1 Sistemas Bluetooth.....	31
1.8.2 Sistemas PCN/PCS .....	33
1.8.3 Tercera Generación de Sistemas Celulares .....	34
1.8.4 MMDS/LMDS.....	36

## 1.1 CONTEXTO DEL RFID

El objetivo de este capítulo es el de mostrar, de una manera práctica la tecnología RFID, la cual pertenece al grupo de las comunicaciones inalámbricas que han estado en un avance constante en las últimas décadas. Las tecnologías de las comunicaciones personales inalámbricas y la de comunicación de datos son, sin duda de las tecnologías que crecerán más rápidamente en las próximas dos décadas. Desde que el sistema celular móvil llegó en los 80's, se sobrevino en la industria una serie de cambios revolucionarios. Tan sólo en los estados unidos, el número de suscriptores de teléfonos celulares se ha incrementado de 200,000 en 1985 a 73.3 millones en 1999. La tasa de crecimiento que se ha dado en los últimos años es de poco más de 25 % anual para estos usuarios de telefonía celular. El fácil acceso a una forma móvil y rentable en el aspecto de comunicaciones, ha cambiado drásticamente nuestra vida cotidiana. Diversos sistemas satelitales se encuentran en desarrollo para proveer de servicios de comunicación de voz y datos. Aunque al hablar de comunicaciones inalámbricas se puede pensar en primera instancia en aquellas que ocupan en su mayor parte tecnología de radiofrecuencia y microondas, también se hace extensivo este término para sistemas de radar, sensores, navegación, senseo remoto, vigilancia, transmisión, autos compactos y carreteras y por supuesto la tecnología radio frequency identification (RFID).

La era de las comunicaciones inalámbricas dio inicio gracias a dos científicos europeos, James Clerk Maxwell y Heinrich Rudolf Hertz. En el año de 1864, Maxwell presentó sus ecuaciones con la combinación de los trabajos de Lorentz, Faraday, Ampere y Gauss. Maxwell predijo el fenómeno de la propagación de las ondas electromagnéticas en el espacio libre a la velocidad de la luz. Su teoría no fue del todo aceptada sino hasta 20 años después cuando Hertz validó con sus trabajos la propagación de la onda electromagnética. Hertz demostró la generación, propagación y recepción de radiofrecuencia (RF) en el laboratorio. El trabajo de Hertz estuvo catalogado como una curiosidad de laboratorio y se le confino ahí por casi dos décadas, hasta que un joven italiano, Guglielmo Marconi, tuvo la suficiente visión para crear un método para enviar y recibir información. Marconi comercializó el uso de la propagación electromagnética para la telegrafía inalámbrica lo cual permitió la transferencia de información de un continente a otro sin la necesidad de una conexión física. El telégrafo se volvió sinónimo de comunicaciones rápidas. Las llamadas de auxilio desde el trasatlántico Titanic tuvieron un gran impacto en el público, remarcando así la gran importancia de las comunicaciones inalámbricas.

Ya para principios de los años 1900s, la mayor parte de las transmisiones inalámbricas fueron hechas con longitudes de onda muy largas. En los 1920s, fue hecha una transmisión unidireccional para las patrullas y patrulleros en Detroit. El uso de ondas de radio para la transmisión inalámbrica, comunicaciones entre estaciones móviles y fijas, sistemas de seguridad pública, servicios marítimos móviles y los sistemas de transporte terrestre se incrementaron drásticamente. Durante la segunda guerra mundial, las radiocomunicaciones se hicieron indispensables en el ambiente militar para los campos de batalla y para las maniobras de las tropas. La segunda guerra mundial además creó una necesidad urgente de sistemas de radar (*radio detection and ranging*). La resolución de un radar (el mínimo tamaño de objeto que puede ser detectado) es proporcional a la longitud de onda. Entonces, las longitudes de onda más pequeñas o altas frecuencias (por ejemplo las frecuencias de

microondas) son requeridas para detectar objetos más pequeños como los aviones de combate.

Los métodos de comunicación inalámbricos como los telégrafos, transmisiones, teléfonos, y comunicaciones punto a punto ya estaban disponibles antes de la segunda guerra mundial. El uso de estos métodos de comunicación se aceleró y se extendió durante y después de la guerra. Para las comunicaciones inalámbricas de larga distancia, los sistemas de relevo, básicamente punto a punto y los de halo troposférico fueron utilizados. Después de 1960, los sistemas satelitales emergieron para cubrir las necesidades de comunicaciones globales. Un satélite usa un sistema banda ancha de alta frecuencia (normalmente en gigahertz) que puede simultáneamente soportar miles de usuarios telefónicos, decenas o cientos de canales de televisión, y muchos enlaces de datos. Empezando en los ochentas, los teléfonos inalámbricos se volvieron populares y han gozado de un rápido crecimiento en las últimas dos décadas. Recientemente, los sistemas de comunicación personal (PCS) que operan a altas frecuencias con amplios anchos de banda, han emergido ofreciendo una combinación de varios servicios como los de correo de voz, correo electrónico, video, mensajería, datos y servicios computacionales en línea.

Las aplicaciones de radiofrecuencia y microonda han experimentado un tremendo crecimiento desde que la guerra fría se terminó en 1990. Muchos libros han sido publicados en respuesta a las necesidades de un fuerte mercado. De cualquier manera, muchos de estos libros han sido escritos con un énfasis en sistemas. El objetivo del presente capítulo es el de describir las principales características de las aplicaciones inalámbricas en general, dejando ver claramente que no se trata de tecnologías divergentes que se trabajan aisladamente, sin tener nada que ver unas con otras. Entonces veamos pues como las distintas tecnologías han logrado avanzar tendenciosamente hacia la convergencia, si bien no de la tecnología como tal, sí en cuanto a los servicios que se ofrecen actualmente.

## **1.2 ESPECTRO DE FRECUENCIA Y PERDIDAS POR PROPAGACIÓN ATMOSFÉRICA**

Los espectros de frecuencia para microondas van de los 300 MHz a los 30 GHz con una correspondiente longitud de onda de 100 a 1 cm. Antes del espectro de microondas, se encuentra el espectro de radiofrecuencia y arriba del de microondas el espectro de ondas milimétricas. Arriba del espectro de ondas milimétricas se encuentra el espectro de las ondas submilimétricas, el infrarrojo y el espectro óptico. Las ondas milimétricas (30-300 GHz), cuyo nombre se deriva de las dimensiones de su longitud de onda (de 10 a 1mm), pueden ser clasificadas como microondas desde que se utiliza para éstas la misma tecnología o similar que para el caso de las microondas. La figura 1.1 muestra a grandes rasgos el espectro electromagnético. Por conveniencia, las microondas y las ondas milimétricas son además divididas en muchas bandas de frecuencia, la figura 1.1 muestra algunas de las bandas de microondas, y la tabla 1.1 muestra algunas de las bandas milimétricas. El espectro de radiofrecuencia está definido vagamente, uno puede considerar el espectro de frecuencia menor de 300 MHz como el espectro de radiofrecuencia. Pero la literatura frecuentemente usa el término radiofrecuencia hasta para frecuencias arriba de 2 GHz o incluso más altas.

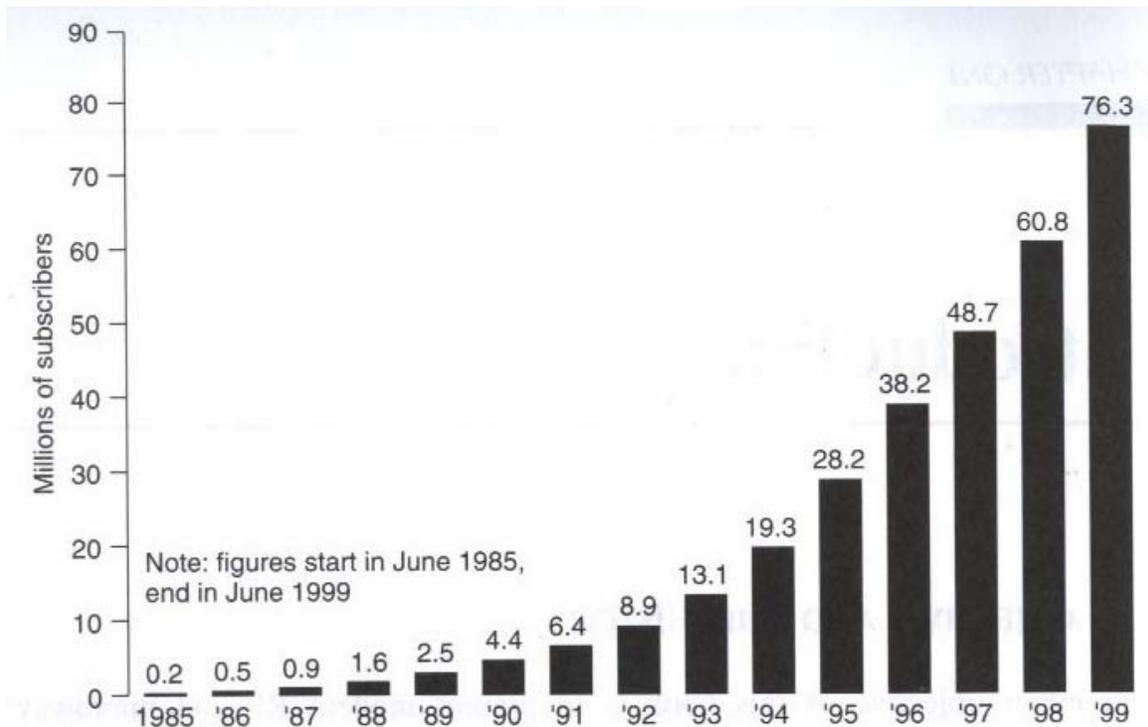
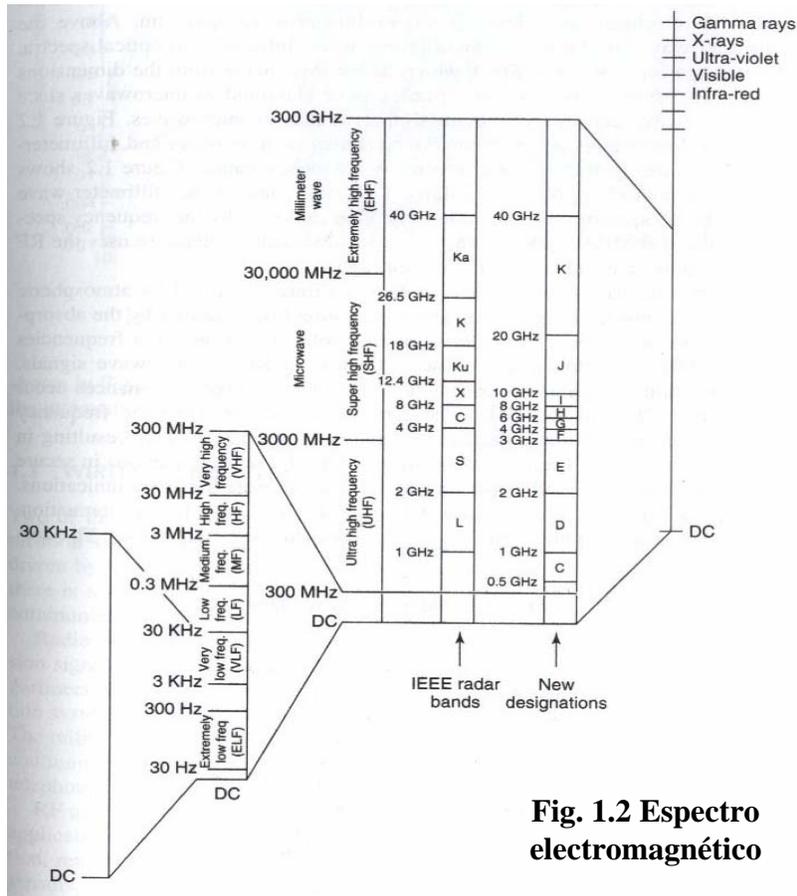


Fig 1.1 Crecimiento de suscriptores celulares

El rendimiento de un sistema inalámbrico está fuertemente afectado por la absorción atmosférica como se muestra en la figura 1.2. Las pérdidas por propagación son causadas por la absorción de la energía de microondas por vapor de agua y oxígeno molecular. Para frecuencias debajo de 10 GHz, la atmósfera causa tan sólo una pequeña pérdida tanto para la radiofrecuencia como para las señales de microondas. La atenuación es entonces alta a frecuencias arriba de 30 GHz. Distintas resonancias ocurren a frecuencias de 22.2, 60, 120, y 183 GHz. Estas resonancias ocurren cuando la frecuencia coincide con una de las resonancias moleculares del agua u oxígeno, dándonos por resultado la máxima absorción. La alta atenuación a 60 GHz tiene aplicaciones en la seguridad de las comunicaciones en las redes de área local (LAN) y comunicaciones intersatelitales. También hay varias “ventanas” a los 35, 94, y 140 GHz con menor atenuación por supuesto. Algunas aplicaciones de radar o radio están centradas en estas últimas frecuencias. Los datos mostrados en la figura 1.2 son para condiciones limpias de clima, la lluvia y tormentas aumentan la atenuación drásticamente.

Designación	Rango de Frecuencia (GHz)
Banda Q	33-50
Banda U	40-60
Banda V	50-75
Banda E	60-90
Banda W	75-110
Banda D	110-170
Banda G	140-220
Banda Y	220-325

**TABLA 1.1 Designación de la banda milimétrica**



**Fig. 1.2 Espectro electromagnético**

### 1.3 APLICACIONES INALÁMBRICAS

Dos de las más importantes aplicaciones de RF/microondas históricamente son los sistemas de comunicación y radar, pero existen otros tantos. Actualmente, el mercado es conducido por el fenómeno de crecimiento de los sistemas de comunicación personal, aunque también hay una demanda en incremento por los sistemas basados en satélite de video, teléfono y sistemas de comunicación de datos.

Las ondas de radio y las microondas juegan un importante papel en la vida moderna, las señales de televisión son transmitidas alrededor del globo por los satélites con ayuda de las microondas. Los aviones son guiados desde el despegue hasta el aterrizaje por radar de microondas y sistemas de navegación. Los teléfonos y datos son transmitidos usando estaciones de microondas de relevo. Los militares usan las microondas para la supervisión, navegación, control remoto, comunicaciones, identificación en tanques y aeroplanos. Los teléfonos celulares los encontramos donde quiera.

Como podemos ver, las tecnologías inalámbricas RF y microondas tienen muchas aplicaciones comerciales y militares. Las áreas de mayor aplicación incluyen las comunicaciones, radar, navegación, sensores remotos, *RF identification*, transmisiones (AM, FM, TV, DBS), automóviles y carreteras, vigilancia, medicina, astronomía y exploración del espacio.

Los servicios portátiles inalámbricos tienen sus raíces en las radio comunicaciones móviles. La aplicación inicial de la radio fueron los servicios fijos, en los cuales tanto receptores como emisores estaban fijos en una locación. La demanda de sistemas más pequeños, eficientes y rudos, se incrementó con el advenimiento de las comunicaciones dúplex en vehículos en movimiento, cruceros y aviones. La tecnología de semiconductores se alzó al reto, de tal forma que el tamaño y peso se redujo considerablemente. Para cuando la idea de combinar la radio de dos vías y los servicios telefónicos se materializó, las oportunidades de mercado para productos portátiles se alzaron significativamente. El potencial de los teléfonos desde un vehículo en movimiento dio inicio a un totalmente nuevo mercado para la tecnología inalámbrica, así como el número de suscriptores a este servicio se incrementó, la capacidad radial bidireccional se usó más y el concepto de sistema de radio celular nació. Los diseñadores de sistemas de radio celular desarrollaron nuevas técnicas para el aprovechamiento de frecuencias y así se implementaron los primeros sistemas análogos. Las agencias reguladoras han establecido diversas bandas de frecuencia para distintas aplicaciones inalámbricas a lo largo de los años. Durante la última década, muchos productos para comunicación portátiles han sido introducidos con una dramática reducción en peso, tamaño y costo. La diferencia en las reglas estipuladas por las agencias reguladoras en diferentes países nos conducen a tener distintos estándares alrededor del mundo.

Otro segmento de mercado que está emergiendo muy rápidamente es en el de las aplicaciones inalámbricas de corto alcance. Un nuevo sistema llamado Bluetooth fue iniciado gracias a un grupo de interés especial de cuatro grandes compañías en 1998, en 1999 un consorcio fue creado y ahora tiene más de 2500 participantes. Se espera del anterior mercado que sea una porción significativa del mercado total en cuanto a

comunicaciones inalámbricas se refiere en los próximos años. Muchas compañías además están diseñando productos que podrían integrar a los teléfonos celulares con la tecnología Bluetooth.

Así como la tecnología inalámbrica ha avanzado en los sistemas terrestres, también los sistemas de comunicación que utilizan satélites han sido propuestos. Con estos sistemas satelitales, voz, datos y video digital podrán ser transmitidos desde cualquier lugar en el mundo a cualquier hora y a cualquier parte. El sistema Iridium propuesto por Motorola fue el primero de su tipo que utilizó satélites de órbita baja para proveer de comunicación instantánea alrededor del mundo.

En las siguientes líneas discutiremos los sistemas terrestres y satelitales inalámbricos de diferentes tipos.

### **1.3.1 El Espectro Radioeléctrico**

El espectro radioeléctrico es la denominación que se le da al conjunto de las distintas bandas que conforman las locaciones para los diferentes sistemas inalámbricos, estas locaciones son reguladas por las distintas agencias en los diferentes países, en México la encargada de regularlas es la Secretaría de Comunicaciones y Transportes (SCT)-COFETEL.

### **1.3.2 Sistemas de comunicación celular**

El primer estándar análogo para sistemas de comunicación celular implementado en los Estados Unidos se conoce como el Advanced Mobile Phone Service (AMPS). AMPS es también utilizado en Canadá, Sudamérica y Australia. Algunos de los más grandes estándares para comunicación celular usados en Europa son los TACS (Total Access Communication Systems), NMT (Nordic Mobile Telephones) y Radiocom. 2000. En Japón, el primer celular análogo fue introducido en 1979. La tabla 1.2 muestra el resumen de los sistemas análogos de comunicación celular, su banda y la región geográfica donde son utilizados.

El sistema celular digital, también conocido como sistema celular de segunda generación, se levantó debido al éxito de los sistemas de primera generación (análoga), y fue construido en base a algunas de las experiencias en cuanto a lo técnico, comercial, político y regulatorio que arrojó el sistema analógico. Técnicamente había la necesidad de mejorar la eficiencia del espectro y de adoptar la codificación digital de la voz y la modulación digital de la portadora. El desarrollo de las técnicas de codificación digital de voz hizo completamente viable al sistema celular. Esta segunda generación de sistema celular podía soportar más usuarios por estación base por mega hertz de espectro. Un sistema digital celular conocido como Groupe Special Mobile (GSM) fue presentado en 1982 para responder a la necesidad de alojar un creciente número de usuarios en Europa.

Standard	Frecuencia de Transmisión (MHz)	Frecuencia de Recepción (MHz)	Espacio entre Canal (kHz)	Número de Canales	Región
AMPS	824-849	869-894	30	832	USA
TACS	890-915	935-960	25	1000	Europa
ETACS	872-905	917-950	25	1240	Reino Unido
NMT 900	890-915	935-960	12.5	1999	Europa
NTT	925-940	870-885	2.5/6.25	600/2400	Japón
	915-918.5	860-863.5	6.25	5650	
JTACS/NTACS	915-925	860-870	2.5/12.5	400/800	Japón
	898-901	843-846	2.5/12.5	120/240	
	918.5-922	863.5-867	12.5	280	

**Tabla 1.2 Estándares de comunicación telefónica celular**

Los sistemas GSM (ahora conocidos como Global System Mobile) fueron originalmente pensados para la operación en la banda de 900 MHz, en 1989, el departamento británico de comercio e industria asignó 150 MHz de espectro en la banda de 1800 MHz para las redes de comunicación personal (personal communication networks PCN). El estándar escogido para esta aplicación también fue GSM y este sistema es conocido también como sistema digital celular 1800 o DCS 1800 por sus siglas en inglés.

Para responder a la incesante demanda de radio celulares en áreas de alta densidad en los Estados Unidos, un sistema celular fue propuesto en 1992. La asociación de la industria electrónica (EIA) y la asociación de la industria de telecomunicaciones (TIA) adoptaron el estándar Interim 54 (IS-54) basado en TDMA para el sistema digital celular. Este último estándar digital retuvo el espacio de canal de 30 kHz que se tenía en AMPS (para mantener la evolución del sistema análogo). El estándar IS-54 permitió un modo dual de operación en el sentido de que las operaciones análogas y digitales pueden coexistir. El EIA/TIA además adoptó otro estándar conocido como IS-95 basado en CDMA, este estándar permite a los usuarios compartir un canal común para la transmisión. Este último estándar (IS-95) tiene distintos beneficios incluyendo el incremento en capacidad, flexibilidad para adaptarse a distintas tasas de transmisión, rango variable de codificación de voz y control de energía. Con lo anterior se puede operar en el modo CDMA o en el AMPS.

En Japón, un sistema celular digital conocido como sistema celular personal digital (PDC) fue introducido en 1992, como en el caso del IS-54, PDC está basado en la tecnología TDMA y tiene un espaciado entre canal de 25 kHz; además emplea  $\pi/4$  del esquema de modulación DQPSK. El sistema PDC opera en dos juegos de bandas de frecuencia que van de los 800 a 900 MHz y de 1400 a 1500 MHz. La tabla 1.3 resume los estándares digitales celulares.

### 1.3.3 Telefonía inalámbrica

La telefonía inalámbrica convencional opera en la banda receptora de 46.6-47.0 MHz y la banda transmisora de 49.6-50.0 MHz, el FM análogo es usado para la señal de voz y el poder irradiado efectivo es de alrededor de 20  $\mu$ W. Incluso aunque teléfonos inalámbricos de alto poder que operan en la banda ISM han sido introducidos recientemente, la popularidad de los teléfonos de 49 MHz es aún muy fuerte. Un sistema de teléfono inalámbrico, conocido como CT1 y la versión mejorada CT1+, han sido muy exitosos en Europa, estos sistemas operan en el rango de bandas de 914-915 MHz y 959-960 MHz para transmisión y recepción respectivamente. En Japón los teléfonos análogos inalámbricos operan bajo la asignación, hablamos de 254 MHz para transmisión y 380 MHz para la recepción.

Standard	Acceso Múltiple	Frecuencia de Recepción (MHz)	Frecuencia de Transmisión (MHz)	Espacio entre canales (kHz)	Esquema de Modulación	Región
<b>DAMPS (IS-54)</b>	TDMA/FDMA	869-894	824-849	30	$\pi/4$ DQPSK	USA
<b>GSM</b>	TDMA/FDMA	935-960	890-915	200	GMSK	Europa
<b>CDMA (IS-95)</b>	CDMA/FDMA	869-894	824-849	1250	BPSK/QPSK	USA
<b>JDC</b>	TDMA/FDMA	940-956 1447-1489 1501-1513	810-826 1429-1441 1453-1465	25	$\pi/4$ QPSK	Japón
<b>W-CDMA</b>	CDMA	Emergente		40,000	M-PSK	USA
<b>ISM</b>	TDMA/CDMA /FDMA	902-928	902-928	10,000	BPSK	USA
<b>DCS-1800</b>	TDMA/FDMA	1895-1907	1710-1785	200	GFSK	UK
<b>CT2</b>	FDMA	864-868	864-868	100	GFSK	UK Europa Asia
<b>DECT</b>	TDMA/FDMA	1800-1900	1800-1900	1728	GFSK	Europa
<b>PHS</b>	TDMA/FDMA	1895-1907	1895-1907	300	$\pi/4$ DQPSK	Japón
<b>PACS</b>	TDMA/FDMA	1850-1910	1930-1990	300	$\pi/4$ DQPSK	USA

**Tabla 1.3 Estándares para comunicación celular digital y telefonía inalámbrica**

Los teléfonos inalámbricos digitales en Norteamérica estuvieron operando en la banda ISM (industrial, scientific, and medical), en Estados Unidos y Canadá, la banda ISM incluye los siguientes rangos de frecuencia 902-928, 2400-2483.5 y 5725-5820 MHz. A los teléfonos inalámbricos que operan en esta banda no licitada usando las frecuencias estipuladas o directamente la de la secuencia de la tecnología spread spectrum, se les permite tomar arriba de 1 W para su potencia de transmisión. Lo anterior debido a que se trata de una banda no licitada y no existe mucha regulación de la misma, por lo tanto los fabricantes tienen considerables ventajas de libertad en los diseños. En el Reino Unido, un sistema

digital inalámbrico, conocido como CT2 fue introducido como el remedio a algunas de las deficiencias de los sistemas análogos. Un estándar europeo DECT (digital European cordless telecommunications) también se presentó como una interfaz flexible para proveer de servicios de comunicación económicamente efectivos. La tabla 1.3 muestra un resumen de los sistemas de inalámbricos de telefonía y sus bandas de frecuencia. Una comparación de características importantes del sistema celular digital y el sistema inalámbrico de telefonía se lista en la tabla 1.4

<b>Características</b>	<b>Telefonía Inalámbrica Digital</b>	<b>Telefonía Digital Celular</b>
Tamaño de Celda	Pequeña (50-500 m)	Grande (0.5-30 km)
Elevación de Antena	Baja ( $\leq 15$ m)	Alta ( $\geq 15$ m)
Velocidad de Movilización	Baja ( $\leq 6$ kph)	Alta (arriba de 250 kph)
Cobertura	Zonal	Área amplia continua
Complejidad del Aparato	Baja	Moderada
Complejidad de la Estación Base	Baja	Alta
Acceso al Espectro	Compartido	Exclusivo
Promedio de Potencia Tx en el Aparato	5-10 mW	100-600 mW

**Tabla 1.4 Comparación de características entre telefonía inalámbrica y celular**

#### 1.3.4 Sistemas satelitales

Los sistemas satelitales permiten la comunicación global. Estos sistemas operan bajo bandas de frecuencia específicas. Los servicios MSS (Mobile Satellite Systems) pueden ser ampliamente divididos en tres categorías basadas en la altitud de los satélites usados en el sistema. Los satélites geoestacionarios orbitan a una altitud de cerca de 35,800 km. Los satélites de órbita media, orbitan a una altitud de cerca de 10,000 km. Los satélites de órbita baja están a una altitud de alrededor de 1000 km.

#### 1.4. SISTEMAS CELULARES EN LOS ESTADOS UNIDOS, EUROPA Y JAPÓN

Los laboratorios Bell fueron los pioneros en el diseño de sistemas celulares en los 70's. El éxito de la radio celular es el resultado de la capacidad automática de conmutación de la red telefónica en la actualidad. En la operación de sistemas celulares, el área a cubrir se relaciona con lo que hay en una red de celdas de radio contiguas. La red celular idealizada es una estructura hexagonal, cada celda tiene una estación base y un juego asociado de canales de radio para conectar efectivamente a cualquier unidad móvil localizada en la celda. Cada sistema tiene una operación full-duplex y capacidad para la búsqueda de canal. Los canales de control son usados para transferir información de control del sistema desde la estación base al radio móvil. Los canales de voz proveen el enlace para la voz propiamente y para la transmisión de datos. Las estaciones base están conectadas por cables

terrestres o enlaces de microondas a una central móvil de conmutación, es esta central la que controla la conexión entre unidades móviles.

Un área geográfica determinada es cubierta por un patrón de celdas; cada una con un juego asignado de canales de control y de voz. Un grupo de celdas adyacentes se comparten entre todos los canales de frecuencia disponibles, además de que las mismas frecuencias pueden ser nuevamente usadas en la misma área pero en otro grupo de celdas. Una ventaja mas grande del sistema celular es la capacidad *cell splitting*, es decir que es posible incrementar la capacidad del sistema con el simple hecho de separar (splitting) las largas celdas y convertirlas en pequeñas celdas, tal sistema puede emplear celdas de distintos tamaños, dependiendo de la densidad y distribución del tráfico.

Otra característica importante de la radio celular es la capacidad hand-off, que permite al usuario del radio móvil desplazarse entre celdas sin la interrupción del servicio. Durante la conversación telefónica, las estaciones base monitorean el nivel de la señal recibida desde los móviles y ajustan su potencia transmitida como sea necesario. Si la señal recibida cae debajo del nivel predeterminado mas bajo, las bases adyacentes entonces están encomendadas para monitorear la fuerza de la señal y la llamada es deslindada estación base que recibió la señal en un principio.

#### **1.4.1. Sistemas celulares análogos**

El primer estándar celular análogo implementado en los Estados Unidos se conoce como el AMPS. En AMPS hay un total de 50 MHz de espectro, repartido en 25 MHz para la banda de transmisión de los 824-849 MHz y otros 25 MHz para la banda de 869-894 MHz en la recepción destinados para las aplicaciones radio celulares. Cada espectro de 25 MHz se divide en 832 canales con 30 kHz de ancho. El código de voz es logrado por una modulación en frecuencia con 8 kHz de desviación en frecuencia. El canal de señalización usa modulación FSK con una tasa de bits de 10 kbps. Una versión expandida del sistema AMPS que se introdujo después se conoce como EAMPS.

El primer sistema celular análogo desplegado en el Reino Unido se conoce como TACS. Otros diferentes sistemas fueron introducidos a lo largo de toda Europa (ver tabla 1.2), todos estos sistemas usan FM para la voz y FSK para señalización. El espaciamiento de canal es de 25 MHz para TACS, NMT-450 y RTMS, y 10 kHz para NMT 900 y Radiocom. 2000. En japon los teléfonos análogos operaron a la frecuencia de transmisión de 825-940 MHz y la frecuencia de recepción de 870-885 MHz.

El teléfono celular se ha probado a si mismo y ha justificado su utilidad en un mundo lleno de alternativas en el tema de comunicaciones inalámbricas. El mundo esta cubierto por sistemas celulares de radio operando en distintas bandas de frecuencia y usando distintos protocolos. El explosivo crecimiento de suscriptores al servicio celular en la década pasada ha desencadenado la firme expansión de las redes celulares. Las instalaciones y la expansión llevan hacia mas cobertura y capacidad. Pero así como el número de suscriptores se incrementa, la acumulación en las capacidades celulares se incrementa especialmente en áreas metropolitanas donde la densidad de suscripción y volumen de tráfico son altos. Debido a la limitada disponibilidad de espectro, nuevas tecnologías han sido propuestas.

Estas soluciones han sido desde radios de banda delgada, microceldas y técnicas de multiplexaje en tiempo digitales. La radio analógica tiene el defecto de dejar pasar los disturbios físicos en los enlaces de radio transmisión directamente en la vía de audio de la banda de recepción. Los disturbios como las disminuciones, interferencias y señales falsas se manifiestan en los canales de audio como estática, zumbidos, siseos, ruido de fondo y sensaciones de alejamientos. Con las técnicas digitales, la señal de audio no se transmite como tal, sino que se transforma a los patrones para datos digitales, estas y otras razones de carácter regulatorio guiaron al desarrollo de los sistemas de segunda generación, el cual se conoce como el sistema de radio celular digital.

## **1.4.2 Sistema digital celular**

El papel de líderes en la segunda generación de teléfonos celulares fue tomado por Europa con la creación de el comité GSM por la Post and Telecommunication Operator's Organization. GSM se dio a la tarea de desarrollar un sistema de comunicación móvil que pudiese operar con el mismo estándar en toda Europa y que permitiera a los usuarios el acceso y uso del sistema independientemente de la ubicación del usuario o del equipo usado.

Lo paralelo del otro lado del planeta, en Estados Unidos, fue el desarrollar un estándar AMPS de modo dual ó dual mode AMPS (DAMPS) en respuesta a la creciente necesidad de incrementar la capacidad celular en áreas de alta demanda. Otro estándar que emergió en 1993 es el sistema CDMA, también conocido como el sistema IS-95. Las bandas de frecuencia para todos los teléfonos inalámbrico y celulares se muestran en la tabla 1.3.

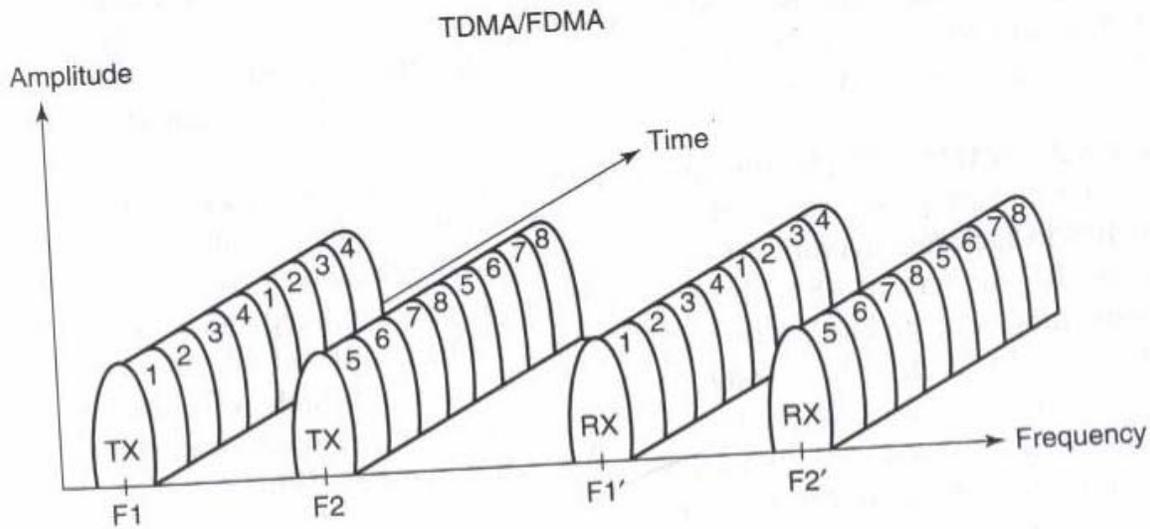
### **1.4.2.1 Global System Mobile**

GSM fue originalmente usado como el acrónimo de un comité, el Groupe Special Mobile, que fue formado para desarrollar el estándar *mobile communication systems* en Europa. En 1982, las autoridades europeas de telecomunicaciones reservaron dos bandas de frecuencia primarias, 890-915 MHz y 935-960 MHz para aplicaciones celulares. Antes de ese periodo, el mercado celular Europeo se caracterizó por tener un gran número de estándares análogos incompatibles, incluyendo TACS y NMT. Tal como los subscriptores de servicio celular y su movilidad por toda Europa se incrementó, los sistemas celulares análogos que tenían un límite territorial en sus servicios, tenían también un serio inconveniente. Todo esto condujo a la siguiente generación de sistemas digitales Europeos basados en el modo de operación banda estrecha TDMA. *Time División Multiplexing Access* tiene la ventaja de ofrecer una mucho mas grande variedad de servicios en comparación con los sistemas celulares análogos. Adicionalmente TDMA tiene la capacidad para ISDN, la posibilidad de seccionamiento de canal y una avanzada codificación de voz.. Los mas grandes requerimientos operacionales desarrollados para el GSM incluyen:

- Alta calidad de voz e integridad del enlace
- Alta eficiencia del espectro

- Sistemas idénticos para toda Europa
- Alto grado de flexibilidad
- Integración con ISDN
- Bajo costo en infraestructura

GSM usa tanto el TDMA como el FDMA para transmitir y recibir información. Una estructura típica de trama TDMA/FDMA se muestra en la figura 1.3. Estos sistemas usan paquetes de datos en específicos intervalos de tiempo, en frecuencias específicas. Por lo anterior diversas conversaciones pueden tomar lugar simultáneamente en la misma frecuencia en diferentes intervalos de tiempo (time slots). Una vez que la frecuencia dúplex se usa en GSM, las transmisión y recepción se vuelven concurrentes. El sistema GSM tiene ocho time slots por canal, y el espacio entre portadoras es de 200 kHz. El ancho de banda de GSM es de 25 MHz, lo cual permite 125 portadoras, cada una de las cuales tiene un ancho de banda de 200 kHz (ver tablas 1.3 y 1.5).



**Fig 1.3 Estructura típica de una trama TDMA/FDMA**

El método de modulación adoptado para GSM es *Gaussian minimum shift keying* (GMSK). Esto facilita el uso de ancho de banda estrecho y una capacidad de detección coherente. En el esquema GSMK, los pulsos rectangulares se pasan a través de un filtro Gaussiano antes de ser pasados por un modulador. La tasa de datos de 270.8 kbps, en suma con el espaciamiento de portadoras de 200 kHz, tiene como consecuencia una eficiencia espectral de 1.35 b/s/Hz para el sistema GSM. La tasa de datos de 270.8 kbps que se divide entre ocho usuarios en GSM, produce una tasa de 33.85 kbps. El codificador de voz *regular pulse excitation with long-term predictor* (RPE-LPT), convierte la voz en 13 kbps. En un futuro cercano, el esquema de codificación de rango completo (full-rate) será reemplazado por un esquema de medio rango (half-rate) que daría como resultado una codificación de 7 kbps. Existen tres diferentes categorías de unidades de telefonía móvil especificadas por el GSM, los rangos de potencia especificados son 0.8, 2, 5, 8, y 20 watts con la capacidad de

variación del nivel de potencia entre 3.7 mW y 20 W. Las unidades de 8 y 20 W respectivamente son para uso de montaje en vehículo o para estación portátil.

#### 1.4.2.2 NADC

El *North American Digital Cellular* (NADC) adoptó el estándar IS-54 basado en TDMA. Este retuvo el espaciamiento de 30 kHz por canal de AMPS para facilitar la evolución del análogo al digital de lo análogo a lo digital y, en adición proveer de un rango de bits RF de 48 kb por canal, este estándar utilizó el esquema de modulación  $\pi/4$  DQPSK y cada canal de frecuencia tenía un rango de bit RF de 48.6 kbps. La capacidad es dividida en seis intervalos de tiempo (time slots), dos de los cuales se asignaban a cada usuario. Cada par de frecuencia de 30 kHz podía servir para tres usuarios simultáneamente. El IS-54 proveía del triple de capacidad en relación a los sistemas AMPS. Con el advenimiento de codificadores de voz de medio rango (half-rate), la capacidad pudo superar seis veces a los sistemas análogos. Desde que este sistema soportó tanto a los sistemas análogos como a los digitales, se le ha conocido como el sistema de modo dual AMPS ó DAMPS. Atributos importantes del IS-54 se muestran en la tabla 1.5

Estándar	Potencia de Transmisión (mW)	Codificación de Voz (kHz)	Bit Rate (kbps)	Conversaciones por canal	Tasa de bits por canal (kbps)	Codificación de Canal
DAMPS (IS-54)	600	VSELP	8	3	48.6	Rango ½ convolución
GSM	1000	RPE-LPT	13	8	270.8	Rango ½ convolución
CDMA (IS-95)	600	QCELP	1-8	12	1228.3	CRC
PDC		VSELP	8	3	42	Rango 1/2 , 1/3 conv.
DCS-1800	1000	RPE-LTP	13		270.8	Rango ½ convolución
CT-2	10	ADPCM	32	1	640	Ninguno
DECT	250	ADPCM	32	12	96	CRC
PHS	80	ADPCM	32	4	72	CRC
PACS	250		32	4	72	

**Tabla 1.5 Especificaciones de sistemas Celular Digital y Telefonía Inalámbrica**

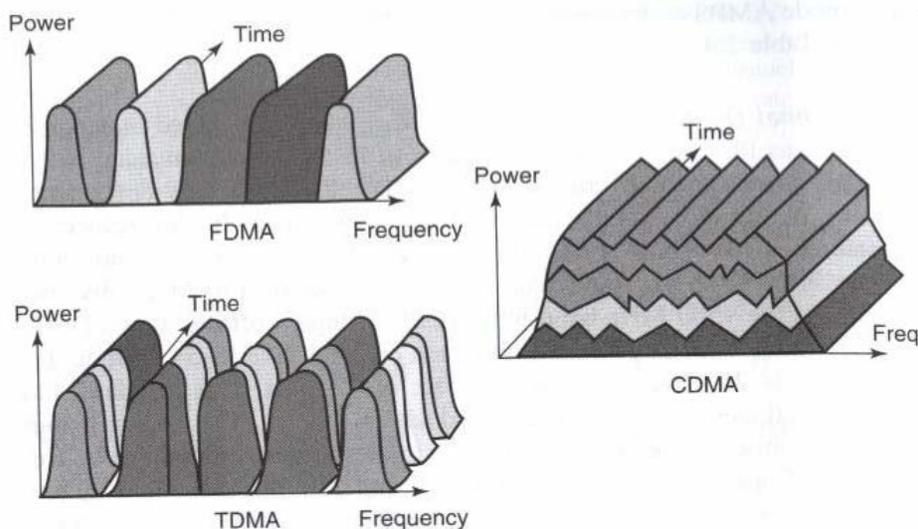
#### 1.4.2.3 Personal Digital Cellular

El sistema digital establecido en Japón en 1991 se conoce como sistema PDC. Este es similar a los sistemas IS-54 de muchas formas. Mientras que el NADC se diseñó para coexistir con AMPS, el PDC se diseñó para reemplazar a muchos de los sistemas análogos incompatibles en Japón, a este respecto su implementación es como en GSM. PDC ofrece tres juegos de bandas de frecuencia, uno se encuentra en la banda de 800-900 MHz con una compensación dúplex de 130 MHz y los otros dos se encuentran en la banda de 1500 MHz con 48 MHz de compensación dúplex. Está basada en TDMA y tiene tres intervalos de tiempo multiplexados en cada canal como en el caso del sistema IS-54. El espaciamiento de

canal es de 25 kHz, con una tasa de bits RF de 42 kbps. Este estándar como el IS-54 utiliza el esquema de modulación  $\pi/4$  DQPSK. La única característica de PDC es la asistencia móvil menos libres que facilita el uso de celdas pequeñas. Los atributos clave en PDC se resumen en las tablas 1.4 y 1.5.

### 1.4.3 Sistemas de Acceso Múltiple por División de Código

El reuso de frecuencia en los sistemas celulares requirió del desarrollo de diferentes técnicas de acceso que permitieran a los usuarios compartir la misma banda de frecuencia, las dos técnicas más sencillas son FDMA, la cual relaciona a cada usuario de un área geográfica determinada con un canal específico de frecuencia; y TDMA que asigna a diversos usuarios con una banda de frecuencia común, pero se transmite en una base rotativa durante ranuras de tiempo (time slots) específicas asignadas. Otra técnica es CDMA, un sistema que usa la técnica CDMA permite que muchos usuarios transmitan al mismo tiempo con la misma banda de frecuencia, a cada usuario se le asigna un código único ó secuencia de “sintonía” con el sistema CDMA. Esta secuencia de código permite al transmisor generar una señal, la cual puede ser únicamente reconocida por el supuesto receptor. La figura 1.4 ofrece una descripción gráfica de FDMA, TDMA y CDMA.



**Fig 1.4**  
**Descripción**  
**gráfica de**  
**los esquemas**  
**FDMA,**  
**TDMA y**  
**CDMA**

La tecnología CDMA, desarrollada en un principio por QUALCOMM, se avoca a un canal de banda ancha con un ancho de banda de 1.23 MHz para usarse en cada celda, lo cual es equivalente a 42 canales de 30 kHz de banda. Cada canal es compartido por muchos usuarios con diferentes códigos. Aún cuando existen muchos sistemas CDMA en el mundo, uno de los más ampliamente utilizados es la versión IS-95 de CDMA, la cual es el resultado de un comprensivo esfuerzo de QUALCOMM en cooperación con AT&T, Motorola y otros. Un canal sencillo de CDMA es típicamente de 1.23 MHz y una docena de usuarios comparten simultáneamente el canal completo.

Algunas de las ventajas de un sistema CDMA son:

- Mayor resistencia a la interferencia
- Rendimiento mejorado en movilidad activa
- Mayor capacidad en el reutilización de frecuencia y
- Mayor seguridad

De cualquier manera el sistema CDMA, impuso demandas sustanciales para la microelectrónica para procesar datos.

Una de las suposiciones fundamentales del sistema CDMA es que las señales para cada usuario llegan al receptor con la misma potencia. Si una señal de interferencia llega al receptor con un nivel de señal mayor al de la señal de información, podría causar degradación en el rendimiento. Como resultado de lo anterior, los sistemas prácticos de CDMA tienen que incorporar elaborados algoritmos de control de potencia. Otro muy importante problema es la sincronización, los requerimientos de temporización de los sistemas CDMA son en mucho, mas indispensables en éste que para otros tipos de sistemas de comunicación, así que el receptor debe estar en sincronía para determinar el tiempo preciso de llegada de la señal deseada. Existen algunas muy buenas técnicas disponibles para sobrellevar este tipo de dificultades de implementación, muchas de estas soluciones requieren de componentes microelectronicos complejos que incrementan el costo del teléfono. Los mayores retos de la tecnología CDMA son:

- La velocidad de procesamiento de datos
- Los altos niveles de integración y miniaturización
- El bajo consumo de potencia y
- Flexibilidad

Estos retos, han en parte facilitado el desarrollo de la microelectrónica, teniéndose ahora un bajo consumo de potencia y alta eficiencia.

#### **1.4.3.1 Modo de operación Dual de CDMA**

CDMA no comparte ninguna de las características que se tienen para fuentes AMPS, a excepción de que ocupan la misma banda de frecuencia. Cuando un teléfono CDMA accede a un sistema que soporta el protocolo CDMA, éste gana el acceso al modo CDMA. Si, por otro lado el sistema servidor no soporta el protocolo CDMA, el protocolo reconoce la firma perdida para CDMA y se vuelve un teléfono convencional AMPS.

### **1.5 TELEFONÍA INALÁMBRICA**

Los sistemas telefónicos inalámbricos ofrecen al usuario una movilidad muy limitada cuando se les compara con los sistemas celulares, la telefonía inalámbrica se caracteriza por un rango radial más corto. Los rangos típicos son de 50 – 300m dependiendo de la aplicación y el estándar implementado, por otro lado, el costo operativo para el usuario es significativamente más bajo que para el caso de los sistemas celulares. La aplicación mas extendida es en telefonía inalámbrica residencial. Cabe señalar que los teléfonos inalámbricos constan de su estación base y el dispositivo móvil como tal o auricular. Los

teléfonos inalámbricos en Europa consisten en los estándares CT2, CT2+, y DECT. En Japón los teléfonos inalámbricos están establecidos bajo el estándar PHS (*Personal Handyphone System*).

### **1.5.1 Telefonía Inalámbrica Analógica**

Desde 1984, los teléfonos inalámbricos en los Estados Unidos operaron en dos bandas separadas, una de estas bandas en el rango de 46.6 – 47 MHz que a su vez se dividían en 10 rangos de frecuencia para recibir las señales del auricular portátil. La otra banda se encontraba comprendida en 49.6 – 50.0 MHz, que tenía también otros 10 correspondientes rangos de frecuencia para transmitir las señales. El ancho de banda permitido fue de 20 kHz y la potencia radiada efectiva fue de 20  $\mu$ W. El FM analógico fue usado como señal de voz y la codificación digital de la señal se usó con fines de seguridad. Debido a la popularidad de este tipo de teléfonos, la existencia de los 10 pares de frecuencias se volvieron inadecuados, particularmente en las áreas de mayor demanda. En 1995, la FCC designó 15 pares de frecuencia cercanos a la banda de los 44 MHz para el equipo fijo y de cerca de 49 MHz para transmisión de señal en los equipos móviles (auricular). A pesar de la reciente introducción de teléfonos digitales inalámbricos que operan a altas frecuencias, los teléfonos análogos operando a 49 MHz continúan siendo muy populares debido a su bajo costo.

Los teléfonos inalámbricos fueron en un inicio importados a Europa desde los Estados Unidos y el lejano oriente. El primer estándar británico, similar al de EUA, permitía ocho pares de canales. Estos equipos contaban con una frecuencia de recepción cercana a 1.7 MHz y la frecuencia de transmisión cercana a 47.5 MHz, un estándar similar se adoptó en Francia de la misma manera. El estándar del que hablamos es comúnmente conocido como el estándar CT0. En el resto de Europa, la demanda de teléfonos inalámbricos se direccionó hacia el desarrollo de un estándar conocido como CT1. Este último provisto de 40 canales dúplex de 25 kHz cada uno, en las siguientes bandas de frecuencia: 914-915/959-960 MHz. En una versión mejorada conocida como CT1+, 80 pares se asignaron en las bandas de frecuencia 885-887/930-932 MHz. La adopción de la forma de DCA (*dynamic channel assignment*) permitía la selección de uno de los cuarenta (u ochenta para CT1+) pares de frecuencia dúplex al inicio de cada una de las llamadas.

Para el caso de Japón se utilizaban 89 canales dúplex cercanos a los 254 MHz para la transmisión, y cerca de los 380 MHz para la recepción. El espaciamiento entre canales de 12.5 kHz y el límite de potencia irradiada de 10 mW.

### **1.5.2 Telefonía inalámbrica digital**

#### **1.5.2.1 Sistemas CT2/CT2+**

Las deficiencias como el limitado número de canales y alta probabilidad de bloqueo de la telefonía inalámbrica estimularon el desarrollo de una tecnología alternativa conocida como CT2-Common Air Interface (CT2-CAI). CT2 está basado en una tecnología digital que usa a su vez, una combinación de las técnicas de transmisión de división de frecuencia y

división de tiempo. El esquema de modulación es GMSK. El espectro CT2 consiste de 40 canales FDMA con un espaciamiento de 100 kHz en la banda de 864-868 MHz., la potencia de transmisión es de 10 mW y el rango típico es de 30-100 m. CT2 soporta datos en adición a la transmisión de voz, CT2 se introdujo como un estándar de telepunto en el cual las redes telepunto usaban estaciones base para establecer un servicio telefónico de paga inalámbrico. Después de la inicial y exitosa aceptación de los usuarios, hubo más tarde una baja en la popularidad, a medida que en el lejano oriente se incrementaba. En Canadá una versión mejorada de CT2, conocida como CT2+ operando en 944-948 MHz se implemento para la telefonía inalámbrica, lo último con el objetivo de proveer algo de las funciones de administración-movilidad que no se tenía hasta ese momento. Estas cinco portadoras se reservaron para señalización, y cada portadora incluyendo 12 canales comunes usando TDMA, éstos últimos (canales) soportando los registros locales, las actualizaciones locales y el compaginado de ambos.

### 1.5.2.2 Sistema DECT

El sistema DECT se diseñó como un interface flexible para proveer de un servicio económicamente efectivo en las áreas de alta demanda utilizando las picoceldas. Es rentable para telefonía residencial, acceso público y enlaces locales. Se diseñó para ser de un bajo costo y flexible en operación en cualquier ambiente. DECT es mas similar al sistema celular que cualquier otro sistema de telefonía inalámbrica clásico. La estación base para el DECT puede por consiguiente manejar múltiples dispositivos simultáneamente con un transceiver sencillo, DECT además es compatible con GSM, lo cual conduce a una capacidad de red adicional.

DECT funciona con TDMA y TDD (*time división duplex*) como esquemas de transmisión, la frecuencia operativa para este sistema está en el rango de 1800-1900 MHz, la banda se divide en 10 portadoras y cada una de las portadoras se divide a su vez en 24 ranuras de tiempo (time slots), 12 en cada dirección. La voz se codifica con 32 kbps con una modulación PCM adaptativa diferencial (ADPCM) con un rango de canal de 1.152 kbps sobre una un ancho de canal de 1.728 MHz, el cual provee una eficiencia de ancho de banda de 0.67 b/s/Hz. El rango de datos de voz es mucho mayor que aquel usado en el estándar digital celular y como resultado provee una calidad de voz comparable con cualquier sistema convencional de telefonía. Los detalles de la estructura de tramas y el time slot de un sistema DECT se muestra en la figura 1.5. Como se puede ver en la figura, la duración total de la trama de 10 ms se divide equitativamente entre dos segmentos de 5 ms para comunicación en cada dirección. Cada segmento de 5 ms se divide a su vez en 12 time slots, representando 12 canales. Un rango de datos total de 1.152 Mbps se proporciona, comparado con los equipos CT2, DECT tiene el doble del rango de transmisión (20-200 m para interiores y arriba de 300 m para ambientes externos). El estándar DECT incluye provisiones de seguridad tales como el encriptamiento de la radio transmisión y la autenticación del dispositivo portátil. El estándar DECT es obligatorio en Europa, además tiene un amplio soporte en la industria y el primer sistema comercial se implementó en 1993. DECT también proyecta mucho interés desde fuera de Europa. Un estándar basado en DECT esta empezando a ser adoptado en los Estados Unidos para su aplicación en las bandas PCS.

### 1.5.2.3 Sistema Personal Handyphone (PHS)

En Japón PHS se lanzó en 1989 para proveer capacidad para el hogar, oficina y el acceso público. La asignación PHS consiste de 77 canales, 300 kHz de ancho, en la banda 1895-1918 MHz, la banda 1906.1-1918.1 MHz fue designada para los sistemas públicos y la banda 1895-1906.1 MHz es usada para aplicaciones de hogar u oficina. Tal como DECT (fig. 1.5), PHS utiliza TDMA y TDD, pero tiene cuatro canales dúplex en vez de doce.

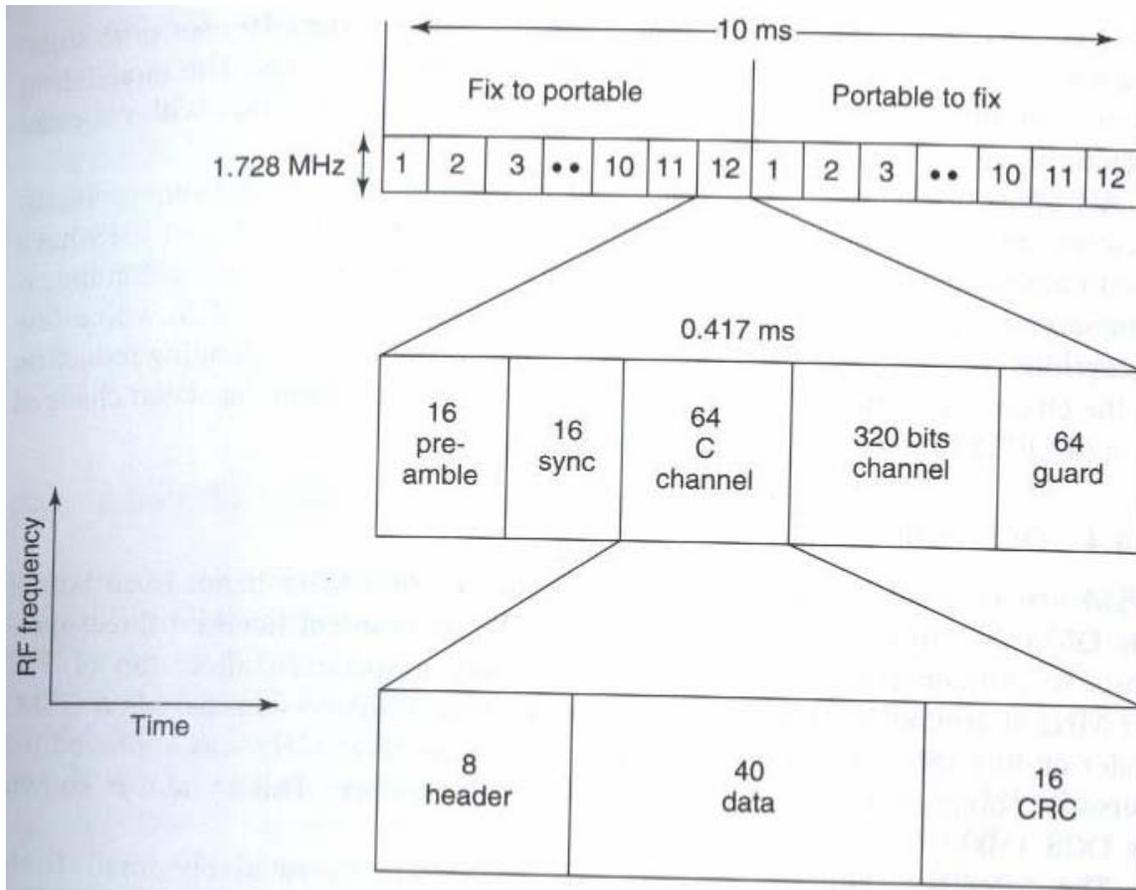


Fig. 1.5 Estructura de trama y ranura de tiempo (time slot) del sistema DECT

### 1.5.3 WACS/PACS

En los Estados Unidos, Bellcore desarrolló un interface aérea para los sistemas de comunicación inalámbricos (*wireless access communication systems*) WACS, este interface provee de conectividad inalámbrica a una portadora local de intercambio, la aplicación objetivo para esta tecnología fue los dispositivos portátiles de baja velocidad. Para el caso de las estaciones base se tuvo pensado que fueran como pequeñas cajas montadas en los polos del teléfono y separadas por cerca de 600 m. WACS usa frecuencia dúplex de división (*frequency división duplex*) FDD en lugar de TDD como en el caso de los sistemas

DECT. Cada frecuencia portadora de 10 time slots de usuario. La codificación de voz es de 32 kbps y la duración de trama de 2 ms. El esquema de modulación adoptado para esto es el QPSK (*quadrature phase shift keying*) con detección coherente.

Así como el estándar de Estados Unidos para 2 GHz, PCS se estableció, de la misma forma los atributos del sistema WACS y PHS se combinaron y crearon un nuevo estándar conocido como PACS (*personal access communication services*). PACS retuvo muchos de los atributos de WACS con algunas excepciones. Primero los time slots se redujeron de 10 a 8, con la correspondiente reducción en el ancho de banda y tasa de bits en el canal, el esquema de modulación se cambió a  $\pi/4$  QPSK.

#### **1.5.4 DCS 1800**

GSM inicialmente se diseñó para operar en la banda de los 900 MHz , antes de que el sistema GSM se volviera operacional, el gobierno británico dio licencia a tres operadores de proveer servicios usando un espectro de asignación de 2x75 MHz a cerca de 1800 MHz, los proveedores se basaron en GSM, después esta misma banda de 150 MHz de espectro cercana a los 1800 MHz fue aprobada para PCN (*personal communication network*) por toda Europa, este sistema es conocido como DCS 1800.

Las diferencias entre GSM y DCS 1800 son relativamente pocas. Ambas estan basadas en una modulación idéntica y pueden ofrecer el mismo rango de servicios. La disponibilidad del espectro está incrementada en DCS 1800, y soporta sólo dispositivos handheld de bajo poder, opuestamente a La capacidad GSM para un amplio rango de quipo de bajo y alto poder.

### **1.6 SISTEMAS WIRELESS LAN**

Los sistemas de datos inalámbricos se diseñaron para su operación en conmutación de paquetes, opuestamente al caso de la operación por conmutación de circuitos convencional. Los operadores de los sistemas de mensajería de área extensa usan un espectro con licencia, y de esta manera venden sus servicios a los consumidores, por otro lado las redes de area local inalámbricas son operadas por el propietario con privacidad e independencia en su manejo. Esto provee de una alta tasa de datos en la comunicación sobre un área pequeña. Las redes LAN no necesitan licencia y operan en la banda ISM (*industrial, scientific, and medical*).

Las redes LAN inalámbricas son la mayoría de veces usadas para comunicación de espacios cerrados a una tasa de bits igual o mayor a 1 Mbps. Los estándares para LAN inalámbrica están cubiertos en la recomendación IEEE 802.11. Para el caso de Europa se tiene contemplado en el estándar HyperLAN, el cual usa una banda dedicada de 5.150-5.3 GHz, mientras que el IEEE 802.11 contempla la banda ISM de 2.4 GHz. Para Japón se4 han implementado dos tipos de redes LAN inalámbricas, una es para rangos de datos medios en 256 kbps – 2Mbps y la otra para rangos mayores a 10 Mbps. La primera opera en la banda de 2.4 GHz ISM, mientras que la segunda usa la banda de 18 GHz.

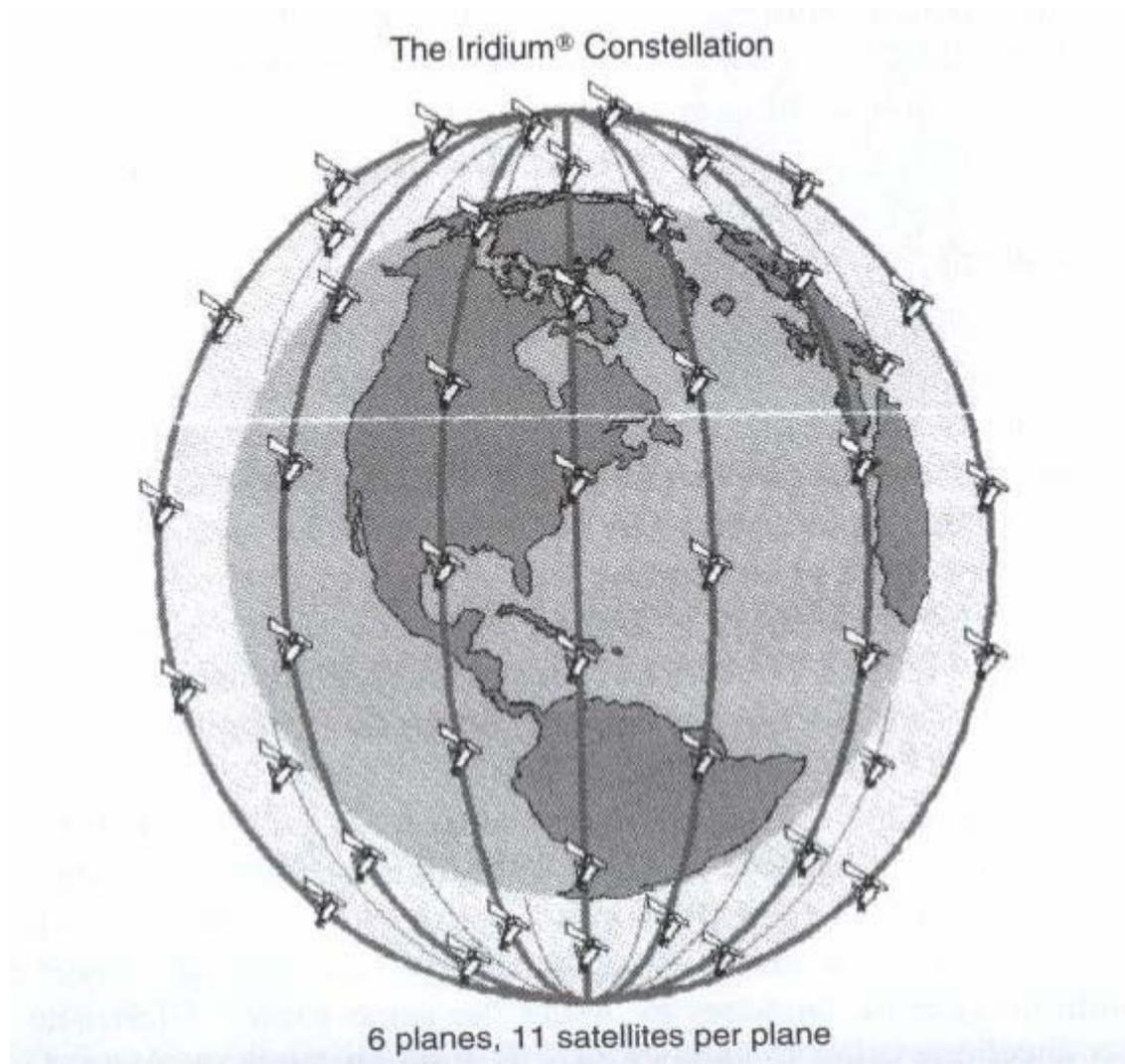
## 1.7 SISTEMAS DE COMUNICACIÓN SATELITAL

La industria de la comunicación satelital, ha experimentado un crecimiento muy significativo en las últimas décadas. Los satélites proveen de una plataforma para relevar las señales de radio entre puntos en la tierra. Un satélite es capaz de desempeñar el papel de un repetidor de microondas para las estaciones terrenas que se localizan y operan en un área determinada. Existen tres tipos básicos de orbitas para los satélites artificiales: a) Low Earth Orbiting Systems (LEOS), o de orbita baja; b) Medium Earth Orbiting Systems (MEOS), o de orbita media; c) Geostacionary or Geosynchronous Orbit Systems (GEOS), o geostacionarios. Los MEOS son también conocidos como ICOS (*intermediate circular orbit systems*). Un satélite del tipo GEO puede cubrir una tercera parte de la superficie terrestre con excepción de las zonas polares. De esta forma un mínimo de tres satélites se requieren para una cobertura mundial, sin embargo en la actualidad existen mas de una veintena de satélites comerciales GEO en operación. De 35,800 km arriba del ecuador los satélites proyectan servicios como la televisión, la distribución de servicios a las estaciones emisoras terrestres, comunicaciones marítimas, entre otros. LEOS y MEOS requieren de más satélites para cubrir la superficie terrestre. Los satélites en LEOS están típicamente en los 500-1500 km sobre la superficie terrestre, mientras que los MEOS se encuentran en 5000-12000 km. Debido al hecho de que el satélite se mueve en relación a la tierra, un completo número de satélites llamados en conjunto constelación son requeridos para proveer cobertura continua. Pero los satélites de orbita baja son mas pequeños, ligeros y menos caros. La fricción atmosférica y la radiación del cinturón interno de Van Allen, como es de esperarse, limita la vida útil de los satélites LEO (típicamente de 5 a 7 años). Los satélites MEOS tienen una vida de cerca de 12 años, el costo por lanzar un satélite LEO es significativamente menor que para el caso de satélites más pesados como los MEO o GEO. La longitud del camino para el caso de los LEOS es menor que para cualquier otro y esto conduce al tiempo de propagación más bajo. El tiempo de propagación de un sistema GEO es cerca de 260 ms, comparado a los 10 ms para un sistema LEO como Iridium por ejemplo. Las frecuencias del enlace de subida y de bajada caen en manos de la asignación que tenga el organismo internacional ITU. Los enlaces de subida de teléfonos para los satélites de órbitas baja y media, estan dentro de la banda de 1610-1626.5 MHz. Los enlaces de bajada están en la banda de 2483.5-2500 MHz..

### 1.7.1 Sistema Iridium

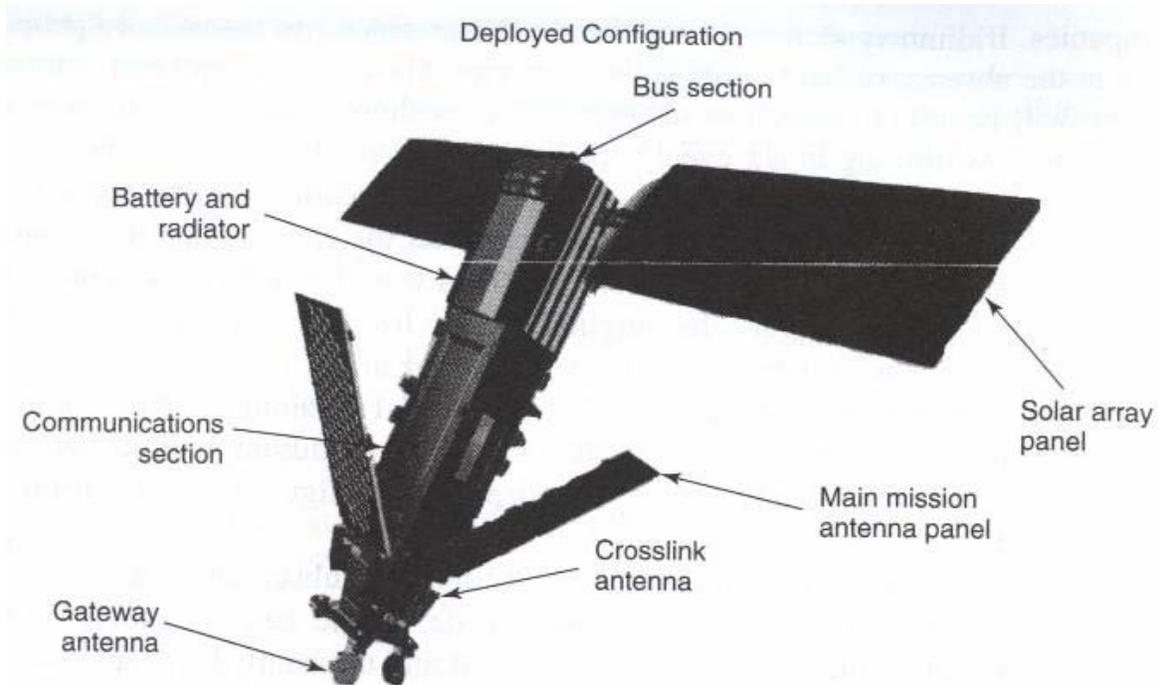
El sistema Iridium, propuesto por primera vez por Motorola, se considera como el mas ambicioso en términos de tamaño y complejidad, actualmente el sistema Iridium es operado por *Iridium LLC*, un consorcio internacional de cerca de 20 compañías industriales y de telecomunicaciones. El sistema Iridium busca extender el servicio celular a mucha mayor gente, incluso en la ausencia de un sistema celular basado en estaciones de retransmisión, los usuarios del sistema convencional celular serían de esta forma capaces de pasar al servicio satelital sin ninguna interrupción. El sistema consiste de 66 satélites orbitando en seis orbitas espaciadas longitudinalmente a partir de los polos a 780 km de la Tierra, Iridium fue originalmente propuesto como un sistema de comunicaciones que debía consistir de 77 satélites, el sistema se bautizó Iridium ya que el elemento tiene como numero atómico el 77. Un estudio minucioso demostró que 66 satélites serían suficientes para proveer de una cobertura global (de cualquier forma , el nombre Iridium se mantuvo).

La figura 1.6 muestra la constelación que se mantuvo y que se implementa en el sistema Iridium, cada satélite es triangular en forma, 4.5 m de longitud y 1 m a través de su base, de tal manera que puede caber en cualquier vehículo propulsor sencillo. Un satélite Iridium pesa alrededor de 690 libras (313 kg) cuando se encuentra completamente cargado. La configuración en despliegue de un satélite Iridium se muestra en la figura 1.7.



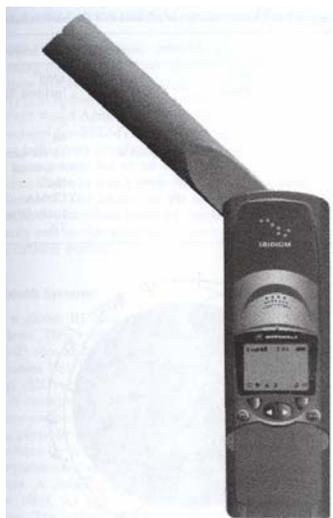
**Fig 1.6 Constelación satelital del sistema Iridium**

Una llamada de un suscriptor Iridium a otro es transmitida directamente por satélite a su destino en cualquier lugar del mundo, si la llamada es desde una fiesta con teléfonos convencionales, se convertirá y transmitirá por el sistema. El primer juego satelital se lanzó en Mayo de 1997, y la red telefónica Iridium fue ofrecida al público en Noviembre de 1998. Motorola y Kyocera desarrollaron teléfonos de mano para la aplicación en Iridium. Una fotografía de un teléfono de mano Motorola se muestra en la figura 1.8.



**Fig 1.7 Configuración en despliegue de un satélite Iridium**

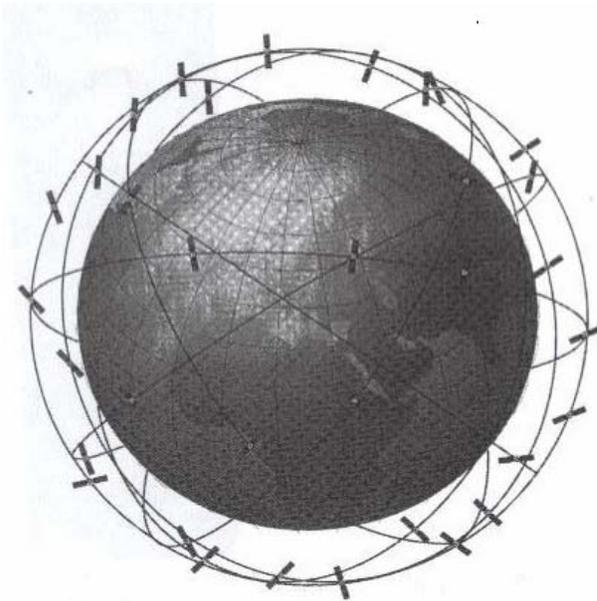
A pesar de la innovación tecnológica y excelencia en ingeniería, el mercado para los sistemas telefónicos Iridium no se desarrolló como originalmente se pensaba. El aparato de mano era demasiado pesado para portarlo y requería además de una línea de vista satelital para su correcta operación. El costo del aparato telefónico y el tiempo aire cargado fueron muy altos, debido a estas razones y al explosivo crecimiento de nuevos sistemas celulares de bajo costo y las otras razones de comunicaciones, la demanda por el servicio Iridium fue muy baja. La compañía Iridium LLC se declaró en bancarrota en 1999.



**Fig 1.8  
Fotografía  
del  
aparato  
telefónico  
Motorola-  
Iridium**

### 1.7.2 Sistema Globalstar

El sistema Globalstar utiliza una constelación de 48 satélites, que se ubican en 8 órbitas circulares a 1414 km de altitud. Otros ocho satélites sirven como repuestos. Las orbitas están inclinadas  $52^\circ$  con respecto al ecuador y espaciadas entre si con  $45^\circ$  a lo largo del círculo mayor de la tierra. El sistema Globalstar es capaz de proveer información entre  $70^\circ$  norte y  $70^\circ$  al sur del ecuador, pero no cubre las regiones polares. La primer batería de satélites del sistema Globalstar se lanzó en 1998. La figura 1.9 muestra la constelación de satélites Globalstar. El sistema Globalstar tampoco tiene capacidad de procesamiento por si mismo ni tampoco puede establecer enlaces intersatelitales. En cambio, muchas funciones incluyendo procesamiento de llamada y operaciones de conmutación se realizan desde la tierra. Un satélite Globalstar por lo tanto tiene menos peso (450 lb/204 kg) comparado con un satélite Iridium. Una comparación entre las características clave entre el sistema Globalstar e Iridium se presente en la tabla 1.6



**Fig 1.9**  
**Constelación**  
**Satelital del**  
**sistema**  
**Globalstar**

Los satélites Globalstar se diseñaron con una forma trapezoidal y esto permite a múltiples satélites ser lanzados usando el mismo cohete. El sistema Globalstar no conecta directamente por satélites un llamante con otro usuario, en vez de eso los requerimientos de enlace descendente recibidas por el satélite desde el enlace fuente, se van a una compuerta, las llamadas son procesadas en la compuerta y ruteadas a través de la infraestructura terrestre. Pero si la parte llamada es otro usuario Globalstar, la llamada será subida desde la compuerta, Globalstar requiere mas compuertas que Iridium, éste último usa 11 compuertas, mientras que para Globalstar se utilizan 78 compuertas. El sistema Globalstar empezó a operar en 1999. El aparato de usuario para este sistema es muy pequeño y el futuro de este sistema es aún muy incierto.

Atributos	Iridium	Globalstar
Altitud de Orbita (km)	900	1389
Geometría	Polar	Inclinada 52°
Número de Orbitas	6	8
Satélites por órbita	11	6
Número total de Satélites	66 (+repuestos)	48
Emisiones por Satélite	48 de la tierra al espacio en banda L	48 de la tierra al espacio en banda L
Enlace Intersatelital	Banda k	Ninguno
Acceso Múltiple	TDMA	CDMA
Cobertura	Global	Latitud superior a 70°
Vida Útil del Satélite (años)	6	7.5

**Tabla 1.6 Resumen de las principales características de los sistemas Iridium y Globalstar**

### 1.7.3 El Sistema ICO-P

El sistema ICO-P es propiedad de *ICO Global Communications Inc.*, se formó en 1995 como un vástago de Inmarsat, el consorcio de 80 naciones que provee de comunicaciones satelitales móviles a terminales marítimas. El sistema ICO provee de la comunicación mundial con el despliegue de 10 satélites MEOS u orbita circular intermedia (ICO), por sus siglas en inglés. Este satélite orbita en dos planos ortogonales inclinados a 45° y 135° con respecto al ecuador, a una altitud de 10,355 km. Los satélites ICO son enlazados a estaciones terrenas con múltiples antenas y capacidades de conmutación. Estas estaciones se localizan alrededor del mundo para proveer la cobertura global. El satélite pesa alrededor de 2750 kg,

### 1.8 SISTEMAS INALÁMBRICOS DEL FUTURO

Las comunicaciones personales inalámbricas ofrecen muchas posibilidades, parte de los retos en la planeación de los sistemas de comunicación inalámbricos del futuro, es el de determinar los servicios que ellos deben soportar, uno de los campos de mayor empuje en la ITU-Radio (ITU-R) es el de definir los sistemas futuros de comunicación inalámbrica terrestre (*future public land mobile telecommunication systems*) FPLMTS, la conferencia de la administración mundial de radio de 1992 (*World Administration Radio Conference-WARC'92*) asignó el espectro de frecuencia para FPLMTS en una base internacional. Los rápidos avances en los componentes tecnológicos en conjunto con el desarrollo de la ingeniería de servicio y administración de red, condujo a un creciente deseo por combinar

las redes fijas y móviles. También existe un gran deseo de desarrollar un aparato “handheld” capaz de soportar múltiples aplicaciones, lo cual se podría ver ya próximamente. El éxito de la segunda generación de tecnología celular con sus soluciones económicamente viables desemboca en la lógica probabilidad a futuro de que alcanzará una temprana saturación en cuanto a servicio y a capacidad, por lo cual este mercado esta forzando a que se despliegue a nivel mundial la tercera generación de tecnología celular.

### **1.8.1 Sistemas Bluetooth**

Bluetooth es una solución global de conectividad basada en radiofrecuencia, de corto alcance para dispositivos personales portátiles, este sistema provee conectividad inalámbrica en tres áreas: puntos de acceso de datos y voz, reemplazo del cable y, *ad hoc* networking.

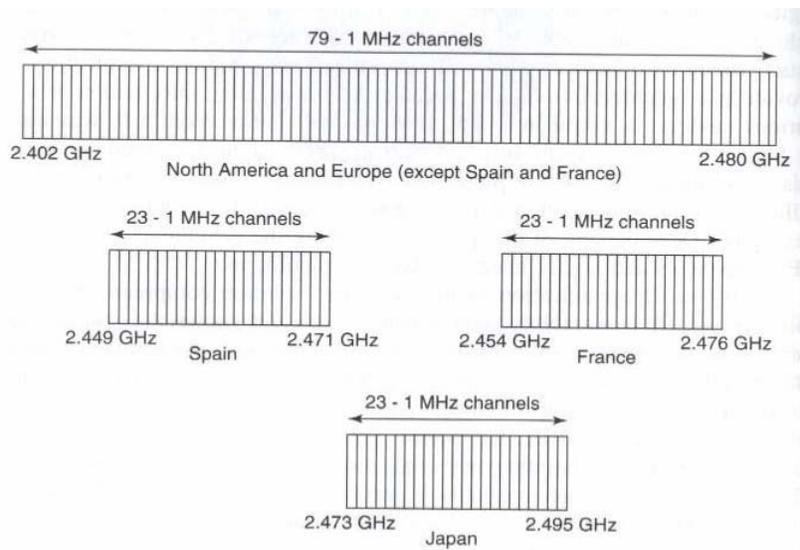
Cinco compañías (Intel, Nokia, IBM, Ericsson y Toshiba) formaron un grupo especial de interés (SIG) en 1998 para formular un protocolo para usar la arquitectura Bluetooth. Un consorcio fue posteriormente creado para atender la creación de un protocolo digital inalámbrico sencillo con el fin de dirigirlo hacia la necesidad de conectividad inalámbrica de PC's, dispositivos handheld, teléfonos portátiles, pagers, PDA's, notebooks, etc. La transferencia de datos entre estos dispositivos requiere de sincronización, la especificación Bluetooth provee esta sincronización y un protocolo para transmisión de información entre varios dispositivos. Una especificación muy comercial llamada Bluetooth 1.0 fue un tópico en 1999, de la misma forma para julio del 2000, mas de 1800 firmas adoptivas se unieron a el consorcio inicial. Las perspectivas de volumen para transceivers Bluetooth es de mas de un billón de unidades y el objetivo en cuanto a costo para un modulo sencillo de chip esta por debajo de \$5.00. El desarrollo de este producto esta conduciendo a al consiguiente desarrollo de componentes de RF de bajo costo y tecnologías RFIC altamente integradas.

La especificación Bluetooth define una solución sistemática que comprende hardware, software y requerimientos de interoperabilidad. La tabla 1.7 muestra las especificaciones para el sistema Bluetooth. Los dispositivos para aplicaciones Bluetooth operan en 2.4 GHz en la banda ISM y es capaz de transmitir datos a una distancia mayor a 10 metros bajo condiciones normales de operación. Hay tres clases de operación dependiendo de la potencia de transmisión, para la clase III, la operación normal por default, la potencia de transmisión es de 0 dBm (100 mW). Las otras dos son clases mas altas de operación opcionales, en la operación en clase II y clase I, la potencia de transmisión es de 4 dBm (2.5 mW) y 20 dBm (1.0 mW), respectivamente, mientras que la distancia de transmisión va de 10 m a 100m correspondientemente. La potencia de transmisión es autorregulable, si el transmisor detecta que un receptor esta en la cercanía, el transmisor ajustara el nivel de potencia para coincidir en el rango. También tiene la capacidad para ir a un estado de “sleep mode” cuando el volumen de tráfico es bajo. Estas características del sistema Bluetooth reducen el consumo de potencia a menos de 3% de lo que lo hace un teléfono móvil.

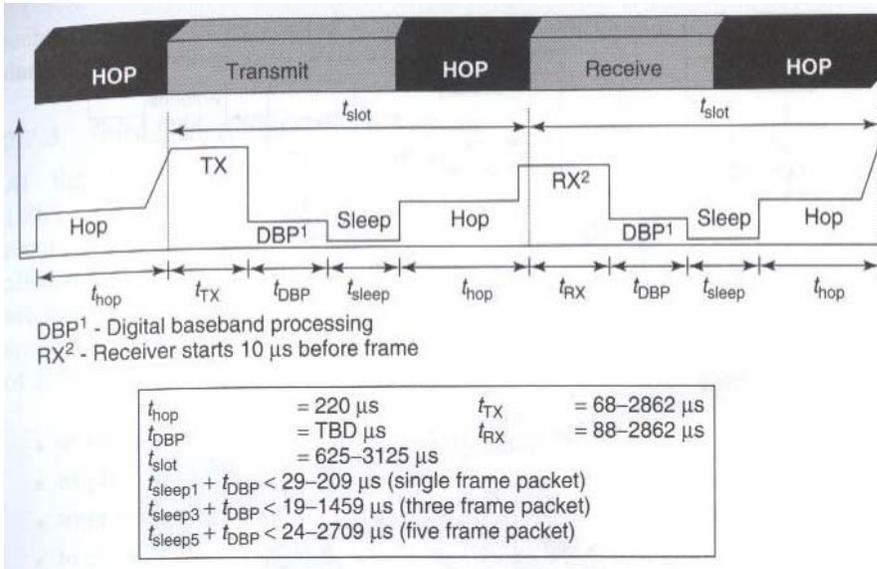
<b>Frecuencia</b>	2.4-2.5 GHz (banda ISM)
<b>Ancho de Banda de Señal</b>	1 MHz
<b>Frecuencia Máxima de Error</b>	25 kHz
<b>Potencia de Transmisión</b>	
Clase I	0-20 dBm (1-100 mW)
Clase II	-6.0-4.0 dBm (0.25-4 mW)
Clase III	0 dB (1 mW)
<b>Ruido de Fase</b>	-124 dBc/Hz (3 MHz distante)
<b>Sensibilidad del Receptor (con BER&lt;0.1%)</b>	-70 dBm
<b>Rechazo en Banda Imagen</b>	-9.0 dB ( $C/I_{mag}$ )
<b>Máximo ruido del Sistema</b>	33 dB

**Tabla 1.7 Especificaciones del sistema Bluetooth**

El nivel mínimo de sensibilidad del receptor es de  $-70$  dBm y la máxima tasa de bits de 1 Mbps. El protocolo estipula conmutación de paquetes basado en un esquema de frecuencia de hop de 1600 hops/s. En la comunicación full dúplex esta permitido usar TDD como la técnica de acceso. La codificación de voz se logra usando la técnica de modulación CVSD (*continuously variable slope delta*). La seguridad para la transmisión es provista por las técnicas de encriptado y autenticación. La corriente de espera es de  $30 \mu\text{A}$  y el máximo de corriente de consumo es de  $300 \mu\text{A}$ . La figura 1.10 muestra el plan de frecuencia para el estándar Bluetooth y la figura 1.11 muestra la secuencia de radio timing.

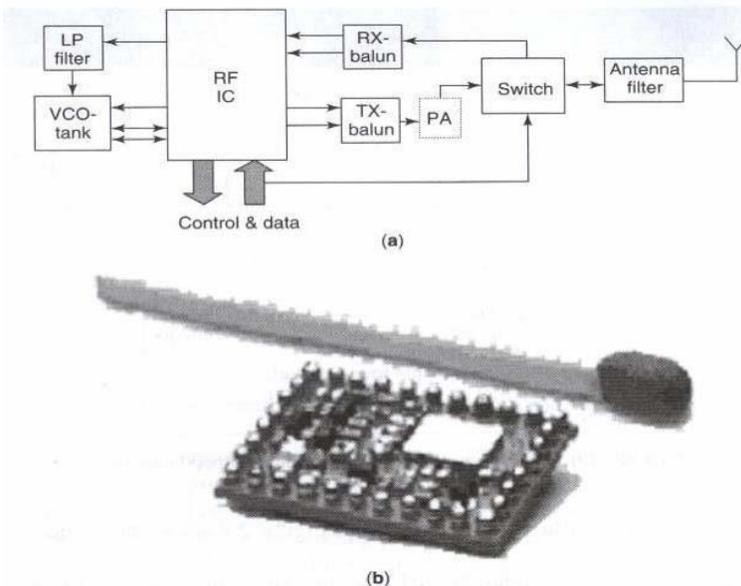


**Fig 1.10 Estándares de frecuencia para módulos Bluetooth**



**Fig 1.11**  
**Especificaciones**  
**radio timing para**  
**Bluetooth.**

Los desarrollos de chip sencillos RFIC's para esta aplicación esta conduciendo a la tecnología de silicón BiCMOS. La figura 1.12a muestra un diagrama a bloques de un modulo de chip sencillo y la figura 1.12b muestra una fotografía de un prototipo de módulo Bluetooth. RFIC's altamente integrados están siendo desarrollados por diferentes compañías y los productos Bluetooth actualmente se encuentran en el mercado.



**Fig 1.12**

**a) Diagrama a**  
**bloques de**  
**modulo**  
**Bluetooth**

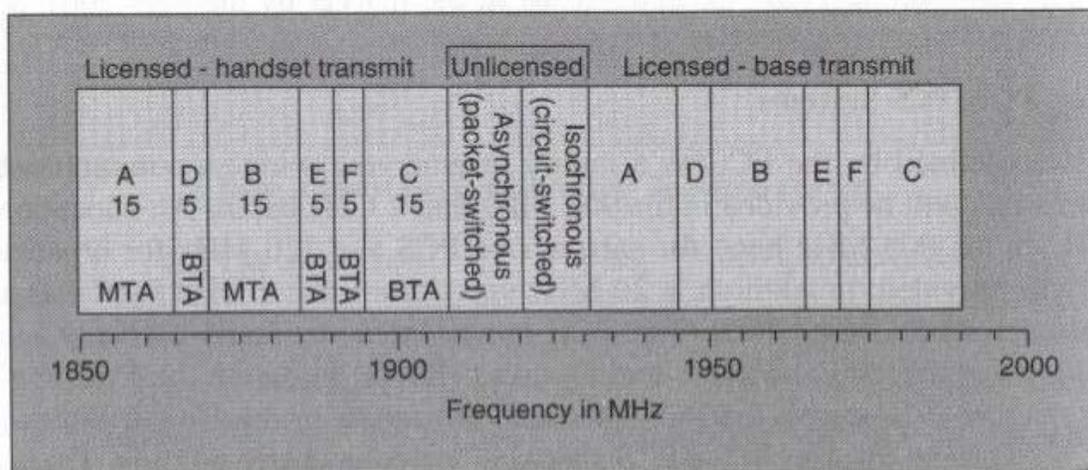
**b) Prototipo de**  
**radio**  
**Bluetooth**

### 1.8.2 Sistemas PCN/PCS

PCS fue definida por la FCC como una familia de servicios inalámbricos de comunicación emergente que se proveería en las bandas de 900 MHz y 2 GHz, se asignaron 3 MHz en la banda de los 900 MHz para banda angosta PCS y 120 MHz para banda ancha PCS.

También se asignó un espectro de 20 MHz en la banda de 2 GHz para PCS sin licencia. La FCC adoptó el método Rand McNally- major trading areas (MTAs) y basic trading areas (BTAs) para definir las áreas del servicio PCS. La figura 1.13 muestra el espectro asignado a PCS para el caso de Estados Unidos. La FCC esta reservando licencias en el espectro PCS vía oferta competitiva. No hay lineamientos oficiales aún en cuanto a como desarrollar la arquitectura del sistema y el interface aéreo, no hay estándares establecidos para los sistemas que estarán operando en el espectro de 2 GHz Tanto TDMA como CDMA se emplean para sistemas móviles de área amplia. Muchas propiedades de las tecnologías de acceso se implementan para los sistemas móviles de área pequeña.

En Europa, el objetivo grosso modo en general es un sistema de telecomunicaciones móvil universal (UMTS) por sus siglas en inglés, que unifique las tecnologías celular, inalámbrica, wireless LAN, radio trunking y navegación. El objetivo es el de especificar una tercera generación de comunicación móvil, la cual se presente, en cuanto a terminales compacta, liviana y teniendo una calidad y rango de servicios compatible con las redes de nuestros tiempos, una alta capacidad de infraestructura y cobertura de todos los sistemas tanto para el consumidor como para las unidades de negocios.



**Fig 1.13 Asignación del espectro PCS en Estados Unidos**

En Japón, un nuevo comité de estandarización y grupos de trabajo relacionados se han establecido en conjunto con el trabajo de FPLMTS. Las tecnologías CDMA y TDMA avanzado están siendo estudiadas con el propósito de contribuir con las actividades de estandarización de la ITU-R

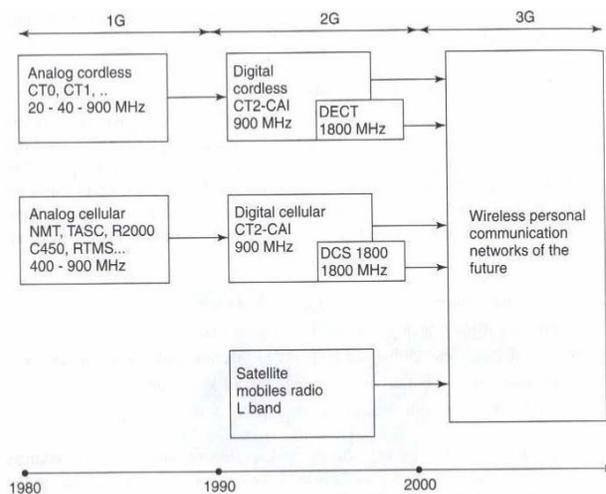
### 1.8.3 Tercera Generación de Sistemas Celulares

En el encuentro WARC del ITU en 1992, las bandas globales entre 1.885-2025 GHz y 2.110-2.2 GHz se establecieron para las FPLMTS las cuales se renombraron ya hora son IMT-2000 (International Mobile Telecommunication 2000), ésta última asignación incluye

la banda existente de 1980-2010 MHz y la de 2170-2200 MHz para comunicación satelital. La tercera generación de sistemas celulares proveerá de una velocidad de transmisión de datos alta y capacidad multimedia, en adición a la transmisión de voz. Los objetivos de IMT-2000 son:

- Integrar servicios residenciales, de oficina y celulares
- Proveer de calidad de voz, comparable a las líneas terrestres
- Proveer cobertura global de radio, ofreciendo un amplio rango de servicios
- Proveer servicios de muy alta tasa de datos (>144 kbps), y
- Crear accesos satelitales directos

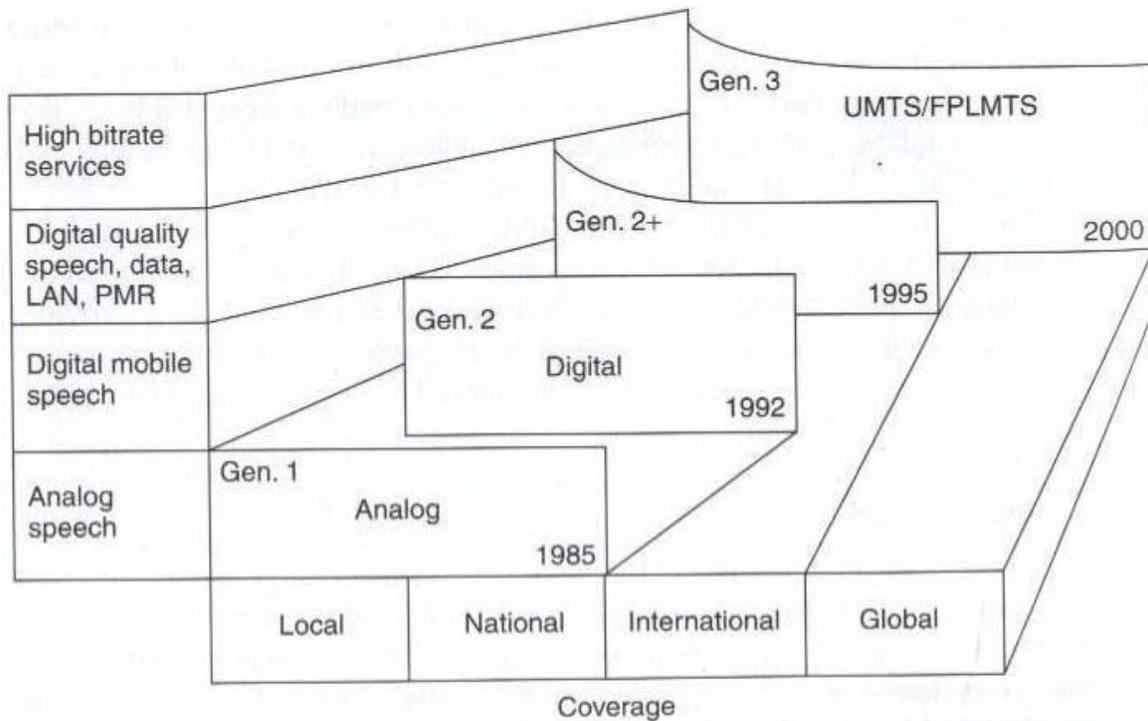
Los esfuerzos se hacen en Estados Unidos, Europa y Japón para llegar a estas metas. En los Estados Unidos, el sistema US-PCS ocupa una porción de la banda de frecuencia identificada en IMT-2000. Dos esquemas de acceso múltiple se han propuesto para direccionarse hacia los objetivos del IMT-2000, éstos esquemas son CDMA de banda ancha (W-CDMA) y el time división CDMA (TD-CDMA). En la reunión de 1998 de ETSI, un acuerdo se alcanzó que bosquejaba el uso de estas dos tecnologías de acceso, el nuevo estándar se nombró UMTS radio acceso terrestre (UTRA), este estándar es básicamente una aproximación del W-CDMA modificado para asegurar que trabajara con GSM, provee para FDD/TDD un modo dual, y cabe dentro del espectro estadounidense.



**Fig 1.14**

**La evolución de las diferentes generaciones de teléfonos celulares**

La tercera generación de celulares debe ser capaz de manejar diferentes rangos de datos con respecto a la demanda y de comprender un efectivo transporte de paquetes ya que la transición de datos en conmutación de circuitos a datos en conmutación de paquetes puede también ocurrir. Los datos en conmutación de paquetes provee de una mejor utilización del ancho de banda disponible. La evolución de las diferentes generaciones de telefonía celular se puede ver bosquejada en la figura 1.14 y sus capacidades se ilustran en la figura 1.15.



**Fig 1.15 Capacidades de las diferentes generaciones de telefonía celular**

### 1.8.4 MMDS/LMDS

Actualmente varios sistemas inalámbricos para la entrega de información de video están en avanzados procesos de desarrollo. MMDS (multichannel multipoint distribution systems), LMDS (local multipoint distribution systems) y MVDS (multichannel video distribution systems) son los sistemas más prominentemente lanzados para el servicio comercial. El mercado de distribución de video casero es el servicio de banda ancha más grandemente extendido en los Estados Unidos con un rédito anual que sobrepasa los 26 billones de dólares. Los métodos de entrega son el cable, satélite y cable inalámbrico, MMDS, LMDS y MVDS caen dentro de la categoría de cable inalámbrico. MMDS es una alternativa simple analógica de televisión por cable, los sistemas unidireccionales han estado en operación en Estados Unidos, Irlanda, Europa oriental y oriente medio por algún tiempo, ellas operan a 2.5 GHz con un ancho de banda de 100 MHz. MMDS emplea el sistema unidireccional AM/QM análogo. La estación base tiene un rango de alcance de alrededor de 60 km y es una forma económica de entregar señal de televisión para esparcirla en áreas pobladas. LMDS opera en el rango de 28-29 GHz, este sistema tiene una capacidad de comunicación unidireccional o bidireccional, en los Estados Unidos el ancho de banda completo de 1 GHz está asignado para este servicio.



# ***CAPÍTULO 2***

## **EL IC Y LOS TIPOS DE MODULACIÓN**

2.1 Introducción .....	39
2.2 Circuitos Integrados (IC) .....	41
2.2.1 Mejoras e Inconvenientes de los IC .....	41
2.2.2 Mejoras Gracias a los IC .....	43
2.2.3 Clasificación de los IC .....	43
2.3 Fabricación de un Circuito Integrado.....	44
2.3.1 Aislamiento de los elementos de un Circuito Integrado ..	46
2.3.2 Tecnología de Película Delgada y Gruesa .....	47
2.4 Tipos de Chip o Integrado.....	48
2.4.1 Integrados.....	48
2.4.2 Los Integrados Según sea su Aplicación.....	49
2.4.3 Tipos de Chip o Integrados .....	49
2.4.3.1 Circuitos Lineales Analógicos .....	50
2.4.3.2 Circuitos Digitales de Bit a Bit .....	50
2.4.3.3 Circuitos Integrados Híbridos .....	50

2.5 Modulación .....	51
2.5.1 ¿Porque se Modula? .....	52
2.5.2 ¿ Como se Modula ? .....	54
2.5.3 Tipos de Modulación y Relación Señal-Canal-Ruido.....	54
2.5.3.1 ¿ Que tipos de modulación existen ?.....	54
2.5.3.2 ¿ Como afecta el canal a la señal ?.....	55
2.5.3.3 ¿ Que relación existe entre la modulación y el canal ?	
.....	55
2.5.4 Modulación en Amplitud (AM) .....	55
2.5.4.1 La envolvente de AM.....	56
2.5.4.2 Recepción de AM.....	56
2.5.4.2.1 Detector de Picos .....	57
2.5.4.3 Índice de Modulación.....	58
2.5.4.4 Desventajas y Ruido.....	59
2.5.5 Modulación en Frecuencia (FM).....	60
2.5.5.1 Ventajas y desventajas de la Modulación de	
Frecuencia.....	60
2.5.5.2 Bandas laterales e índice de modulación en FM .	62
2.5.5.3 Ancho de banda en FM	63

## 2.1 Introducción

El circuito integrado ha sido (desde la aparición del transistor) el hito a considerar en lo que se refiere a la electrónica y sus grandes áreas, las cuales, de una forma u otra se interrelacionan como ramificaciones de un tronco muy sólido de conocimiento adquirido que tiene sus grandes raíces en la ciencia. La microelectrónica actual ha sido desarrollada a partir de todos estos avances que de una u otra forma han sido tomados de la abstracción del pensamiento y espíritu humano que en su intento irrefrenable por ganar una carrera de mejoras constantes, comodidades, dinero o simplemente la creatividad consumada, ha sabido llevar a buen término muchos de los componentes de toda esta era digital.

La microelectrónica de alta integración es una realidad en nuestros días, los semiconductores se encuentran en todas partes, desde pequeños, los seres humanos ya estamos en contacto con la tecnología digital, sin darnos cuenta algunas veces, otras muchas concientemente, en tareas tan cotidianas como programar un despertador, poner el tiempo al microondas y ajustar el nivel de potencia, los juegos de video...etc.

Las técnicas aplicadas a la fabricación de dispositivos semiconductores están siendo continuamente revisadas, modificadas y mejoradas. En años recientes, se ha hecho énfasis principalmente en aumentar la tasa de rendimiento (cantidad de elementos buenos en un lote), expandir los niveles de automatización (menor necesidad de mano de obra) y aumentar los niveles de densidad. La secuencia de pasos para la fabricación de circuitos integrados IC (microcircuitos de alta densidad con millones de elementos) no ha cambiado dramáticamente. Sin embargo, la forma de hacer cada paso ha experimentado un cambio radical en la última década.

Este capítulo pretende simplemente dar una imagen general del ciclo de producción y funcionamiento de los circuitos integrados, presenta algunas de las fases más importantes de producción y la terminología que se aplica. Un análisis más detallado de cualquier paso del ciclo requeriría de todo un libro. En la segunda parte de este capítulo también estaremos analizando algunas de las características de la modulación y los tipos de modulación más usuales. Todo lo anterior debido a que nuestro estudio de las características del RFID no puede dejar de lado todas estas nociones, ya que éstas son la base del estudio de ésta y otras muchas técnicas de radiocomunicación, y en general de las telecomunicaciones, como lo habíamos mencionado.

Durante la década pasada el circuito integrado (IC) ha llegado a ser por su uso cada vez mayor y por los diversos medios de difusión, un producto cuya función y objetivos básicos son comprendidos por cualquier persona. La característica más notable de un IC es su tamaño, por que es miles de veces más pequeño que una estructura semiconductor construida de la forma más usual con componentes discretos.

Los circuitos integrados rara vez necesitan de alguna reparación, esto es, si un solo componente del IC falla, se reemplaza la estructura completa (circuito completo); por tanto, resulta un método mucho más económico. En la actualidad, existen tres tipos de IC disponibles comercialmente a gran escala; incluyen los IC's monolíticos, los de película delgada o gruesa y los híbridos.

Durante la última década la cantidad de pasos en el proceso de fabricación se ha incrementado dos o tres veces, y cada proceso es más sofisticado. En los primeros días el fabricante de IC diseñaba, construía y mantenía el equipo empleado en el ciclo de producción. Sin embargo, hoy día han aparecido nuevas industrias que han asumido la responsabilidad de introducir los últimos avances tecnológicos en el equipo de proceso. El resultado es que el fabricante puede concentrarse en el diseño, control de calidad, mejor funcionamiento y características de confiabilidad y una mayor miniaturización.

La automatización está llegando a ser cada vez más importante en el ciclo de producción. Una gran cantidad de controles basados en microprocesador, introducidos en forma de “direccionamiento por casete”, ha reducido significativamente la posibilidad de errores debidos a transferencia incorrecta de información a la unidad de procesamiento. También tiene una sensibilidad al proceso que se está desarrollando que no está disponible por medio de la curva de respuesta humana. Para un control de proceso mayor y un seguimiento, la mayor parte de la fabricación ha pasado a operaciones de computadora sin pape, con terminales junto al equipo de procesamiento o hasta con el equipo conectado directamente a la computadora anfitrión. El mayor nivel de automatización también reduce la cantidad de manejo y contacto con la oblea, reduciendo, por tanto, la cantidad de fuentes contaminantes y aumentando el nivel de producción.

Los avances de la última década han dado como resultado una aceptación general por la industria de que la densidad de los IC casi se duplica cada dos años. En un tiempo, las dimensiones se proporcionaban en mils y mils cuadrados. Ahora es el micrón o micrómetro (un millonésimo de un metro, mm) la medida estándar.

El incremento de la densidad y los mejores niveles de producción se deben a una maquinaria más sofisticada en el ciclo de producción, métodos mejorados para detectar y corregir fallas, mayores niveles de limpieza, mayores niveles de pureza en los materiales de procesamiento, mejores materiales de fabricación y una cantidad mayor de pasos de procesamiento.

## 2.2 Circuitos Integrados (IC)

Los circuitos integrados son circuitos "comprimidos" en una microplaqueta (chip) que realizan la misma función que un circuito compuesto de transistores, diodos, resistencias, etc., cuyo número puede llegar a superar el millón de componentes. Con la aparición de los circuitos integrados (IC) a finales de la década de 1950 se ha producido un cambio total en la forma de fabricar los circuitos electrónicos. El factor más importante de este cambio es la gran reducción que se ha conseguido en el tamaño de dichos circuitos (fig 2.1).



**Fig. 2.1 Clases de CI's**

**a) CI monolítico**

**b) Procesadores**



Esta reducción ha traído consigo que todos los aparatos electrónicos sean mucho más pequeños y más manejables para todo el mundo y de ahí viene el gran "bum" de los ordenadores en las últimas décadas, así como de las calculadoras, relojes, etc. Pero ¿qué es exactamente un IC?. Se denomina IC a un circuito electrónico metido en una cápsula de dimensiones muy reducidas, y que está constituido por un conjunto de diodos, transistores, resistencias y condensadores. Se fabrica todo sobre un substrato común y en un mismo proceso según diferentes técnicas que más adelante se mostrarán. Lo importante es que cada IC puede desempeñar una función concreta sin interesarnos los componentes que contiene en su interior.

### 2.2.1 Mejoras e Inconvenientes de los IC

Además de su reducido tamaño, los circuitos integrados tienen numerosas ventajas. Una de las consecuencias de la implantación de los CI, a la que apenas se le ha dado importancia, es que ahora las personas que se dedican a diseñar, fabricar, manipular aparatos electrónicos han tenido que cambiar por completo su mentalidad y su preparación. Ya no es tan necesario saber perfectamente de que está compuesto el circuito, ni hay que preocuparse de las múltiples conexiones que antes tenía cualquier aparato, sin embargo hay que saber manejar aparatos más sofisticados, como osciloscopios, computadoras, etc. Dentro de un solo circuito integrado van "integrados", como su nombre indica, numerosos componentes, resistencias, transistores, diodos, etc., que juntos desempeñan una función. Pues bien, de ese IC sólo interesa saber la función que realiza y cómo se acopla al aparato que se esté fabricando, y prácticamente no interesa nada sobre cómo está constituido internamente, ni sus conexiones, ni los elementos que lo forman, ni la función que desempeña cada uno de ellos individualmente. Por lo tanto, los IC forman parte de circuitos electrónicos cuyo coste total es más barato al ser más fácil su diseño.

Como ha visto, un circuito integrado contiene muchos componentes electrónicos y, aunque la fabricación de cada CI resulte más cara que la de un componente discreto, es tal la popularidad de los CI debido a sus grandes ventajas, que se construyen un número muy elevado de ellos cada vez, consiguiendo así que el precio de cada unidad sea bastante bajo.

Otra de las metas que continuamente tienen los diseñadores de circuitos electrónicos es conseguir aumentar la velocidad de respuesta de sus componentes. Esto, como cabe esperar, se consigue totalmente con los CI, ya que, al estar todos los elementos en un espacio tan reducido, las señales pasan rápidamente de unos a otros aumentándose así la velocidad considerablemente.

Los aparatos realizados con CI son los más fiables por varios motivos; primero, porque en los fabricados con componentes discretos se tiene que juntar la fiabilidad de cada uno de los elementos que componen el circuito para obtener la fiabilidad total que tiene; segundo, porque se utilizan técnicas de fabricación muy modernas, muy estudiadas y se fabrican con mucha minuciosidad en cada una de las fases por las que pasan. Al ser mucho más reducido el espacio de interconexión, las posibilidades de fallo son mucho menores y, por último, se debe pensar en el encapsulado de este tipo de CI que hace que estén mucho más protegidos.

Al sustituir los circuitos integrados a un montón de "piezas" dentro de un circuito se consiguen varias cosas: primero se produce una reducción muy importante en los errores de montaje, ya que éste suele ser sencillo y con pocas conexiones, al producirse una avería se puede localizar mucho mejor y no es necesario tener un montón de repuestos de cada elemento. Por último, y aunque en principio pueda parecer un inconveniente, se sabe que cuando se produce una avería en un CI es muy difícil de solucionar y suele ser necesario reemplazarlo por otro nuevo, esto supone una ventaja debido al tiempo, materiales y conocimiento del funcionamiento interno que se ahorra y, como se ha visto antes, el coste de un CI no es muy elevado.

A pesar de su enorme utilización, no todo son ventajas en estos diminutos elementos. Existen algunos inconvenientes, aunque no tan importantes como para conseguir influir en la enorme popularidad de los circuitos integrados. Entre los inconvenientes se puede decir que no todos los elementos discretos que se conocen pueden ser integrados en un CI. Así, las bobinas o inductores no se pueden integrar, y con las resistencias y los condensadores se tienen limitaciones en los valores que pueden alcanzar, debido a que cuanto mayor sea el CI mucho mayor será su coste. Por esta razón, una resistencia suele estar limitada a tener como mucho 50 kW y un condensador 100 pf. Debido a esta limitación, estos elementos, condensadores y resistencias, se sacan muchas veces fuera de los CI y al montar el circuito se montan exteriormente. También se produce un inconveniente al no ser muy recomendable integrar juntos transistores PNP y NPN, ya que hay muchos circuitos que están compuestos de ambos tipos de transistores. La tensión que se le puede aplicar también está limitada, siendo recomendable que el valor de ésta no exceda los 20 V. Se ha dicho que el precio de un circuito integrado es bastante reducido y esto no es cierto del todo, ya que para que esto sea verdad se tiene que cumplir una condición y es que el circuito integrado se debe fabricar en grandes cantidades, pues si se desea un CI adaptado a necesidades particulares resultará muy costosa su fabricación.

Por último, dentro de los inconvenientes se puede tener problemas con la potencia disipada, ya que, al estar los elementos tan juntos, las corrientes grandes pueden producir calor y, al aumentar mucho la temperatura, se puede llegar a estropear el circuito.

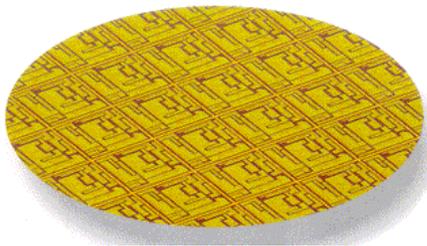
### 2.2.2 Mejoras Gracias a los IC

Una de las aplicaciones de los CI que ha crecido más espectacularmente en los últimos años ha sido la de los microprocesadores. Un microprocesador es un CI compuesto por una de las partes más importantes de un computador: la CPU, unidad central de proceso. Como todos los CI el microprocesador tiene un tamaño muy reducido. Gracias al tamaño reducido, y a otros avances tecnológicos, se ha conseguido pasar en pocos años de las grandes computadoras (que ocupaban habitaciones enteras y que son difíciles de manejar por lo que necesita de profesionales muy calificados que dediquen muchas horas para hacer pequeñas operaciones), a los ordenadores personales, PC, mucho más pequeños, manejables, fáciles de usar y económicos, por lo que han pasado a formar parte de todas las facetas de la vida: medicina, banca, industria, investigación, etc.

La importancia de los CI es incalculable y cada día que pasa se van reduciendo más sus dimensiones y aumentando su velocidad de respuesta.

### 2.2.3 Clasificación de los IC

Se puede hacer varios tipos de clasificaciones según el criterio que se use. Una de estas clasificaciones está basada en el tipo de transistores que se emplee. Así, se puede tener un CI bipolar, si se fabrica a base de transistores bipolares, NPN y PNP, y circuitos integrados MOS, si lo que se usan son transistores de efecto campo más conocidos como MOS. Según la manera de fabricar un CI se puede encontrar circuitos integrados monolíticos, en los cuales se forman todos los componentes a la vez en el substrato semiconductor. Circuitos integrados multiláminas formados por capas gruesas, o circuitos integrados de capas delgadas. Y, por último, dentro de esta clasificación se pueden encontrar los circuitos híbridos que combinan la fabricación monolítica con la de multilamina o la de capas delgadas (fig 2.2).



**Fig. 2.2 Vista Microscópica de una oblea semiconductor en un Circuito Integrado**

Según el número de componentes que contengan se puede dividir los circuitos integrados en SSI (Small Scale Integrated), formados por pocos componentes, MSI (Medium Scale Integrated), varios cientos de componentes, LSI (Large Scale Integrated), miles de componentes y los VLSI (Very Large Scale Integrated), que han superado el millón de componentes.

Por último, si se tiene en cuenta el tipo de señales con las que van a trabajar los circuitos integrados, se puede encontrar CI digitales que, como su nombre indica, trabajan con señales digitales y los CI analógicos, que trabajan con señales analógicas.

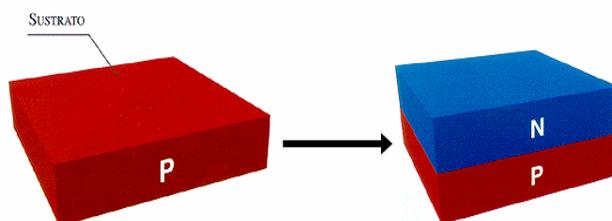
## 2.3 Fabricación de un Circuito Integrado

En los circuitos integrados monolíticos todos los componentes se encuentran en una sola pastilla de silicio. Para fabricar un circuito integrado monolítico se parte de una lámina de silicio denominada "oblea" la cual a su vez está dividida en un gran número de plaquetas cuadradas o chips, cada uno de los cuales va a constituir un CI. Por lo tanto, con una oblea se puede fabricar a la vez un montón de CI.

Se suele partir de un semiconductor tipo P y por la técnica epitaxial<sup>1</sup> se coloca encima una capa de silicio tipo N.

En los circuitos integrados monolíticos todos los componentes se encuentran en una sola pastilla de silicio. Para fabricar un circuito integrado monolítico se parte de una lámina de silicio denominada "oblea" la cual a su vez está dividida en un gran número de plaquetas cuadradas o chips, cada uno de los cuales va a constituir un CI. Por lo tanto, con una oblea se puede fabricar a la vez un montón de CI.

Se suele partir de un semiconductor tipo P y por la técnica epitaxial<sup>1</sup> (fig 2.3) se coloca encima una capa de silicio tipo N.



**Fig. 2.3 Técnica Epitaxial**

Para este proceso se utiliza un horno epitaxial<sup>1</sup>. Este tipo de crecimiento va a asegurar que la región tipo N que se acaba de añadir tiene estructura de un solo cristal, al igual que la región tipo P.

Seguidamente, le se coloca una capa de óxido a la oblea, para ello se introduce en un horno de oxidación formándose una capa delgada de dióxido de silicio ( $\text{SiO}_2$ ) que recubre a la oblea y cuyas funciones más importantes van a ser la de proteger al circuito contra la contaminación.

La siguiente etapa se denomina fotoprotección. Consiste en colocar una sustancia orgánica que sea sensible a la luz ultravioleta, denominada fotoprotector, sobre la capa de óxido.

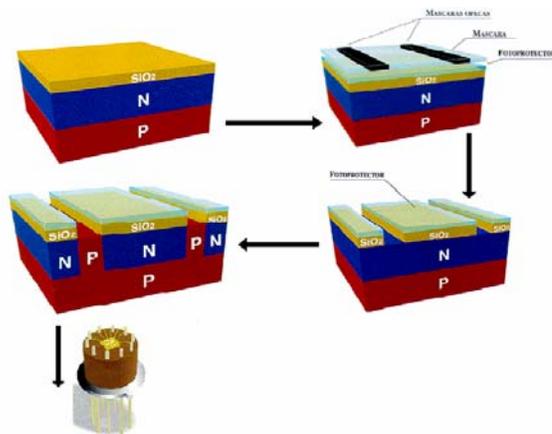
En esta capa se coloca una máscara que tiene unas ventanas opacas en la zona donde se va a realizar la siguiente difusión (por ejemplo, se quiere integrar un transistor NPN se tiene que tener bien definidas tres regiones: el colector, la base y el emisor. Estas tres zonas determinarán cómo será la máscara y dónde tendrá las ventanas opacas). Se expone la oblea a rayos ultravioleta y el barniz fotosensible que había debajo de las ventanas opacas se va a eliminar y va a aparecer la capa de dióxido de silicio.

Después se ataca a la oblea con ácido fluorhídrico y las zonas de SiO<sub>2</sub> que han quedado al descubierto se van a destruir quedando ahora al descubierto la capa de material tipo N.

El siguiente paso es realizar una difusión tipo P. Se introduce la oblea en un horno de difusión y se dopa con gran cantidad de impurezas tipo P. Así se convierte en tipo P la zona que queda al descubierto de la capa epitaxial<sup>1</sup> tipo N. Se ha conseguido aislar una zona tipo N, que ha quedado rodeada por semiconductor tipo P y por dióxido de silicio. Si se estuviese haciendo un transistor esta zona aislada podría ser, por ejemplo, el colector. Se repite el proceso de oxidación y de fotoprotección y se colocan unas máscaras diferentes, por ejemplo, para formar la base. Se difunde nuevamente impurezas tipo P. Para formar el emisor se podrían repetir todos los pasos pero con la diferencia de que al final se añaden impurezas tipo N.

Para conectar todas las regiones "n" y "p" se suele usar una película delgada de un material conductor por ejemplo el aluminio. Se coloca nuevamente una capa de oxidación y un fotoprotector y la máscara que pone ahora tiene ventanas que van a permitir que se realicen las conexiones eléctricas, por ejemplo, entre la base y el colector. Después de realizar la metalización y una vez que las conexiones eléctricas se hayan hecho, se cortan los diferentes chips de la oblea.

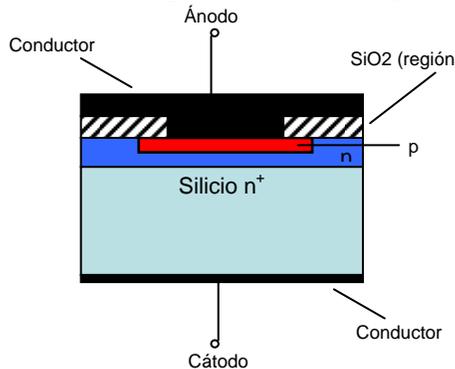
Después de separarlos, se realizan las conexiones necesarias de cada chip con los pines de la cápsula que va a contener el circuito integrado, estas conexiones se realizan soldando hilo de aluminio muy delgado. Para acabar, se introduce el chip dentro de la cápsula que lo va a proteger, y así termina el proceso de fabricación de un CI (fig 2.4).



**Fig. 2.4 Proceso de fabricación**

## \*1 Crecimiento epitaxial

El término epitaxial se deriva de las palabras griegas *epi* que significa “sobre” y *taxis* que significa “arreglo”. Una oblea base de material  $n^+$  se conecta a un material metálico, tal como se muestra en la figura 2.5. La  $n^+$  indica un nivel de dopado muy alto para una característica de resistencia reducida. Su propósito es actuar como una extensión semiconductor del conductor y no como el material tipo n de la unión p-n. La capa tipo n se depositará sobre esta capa usando un proceso de difusión, como lo indica la figura 2.5. Esta técnica de utilizar una base  $n^+$  da al fabricante ventajas definitivas de diseño. Luego se aplica el silicio tipo p usando una técnica de difusión y se agrega el conector metálico del ánodo, como se puede ver en la figura.

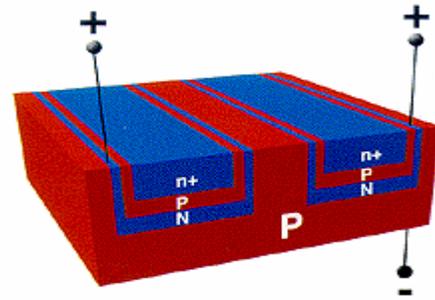


**Fig. 2.5 Diodo semiconductor de crecimiento epitaxial**

### 2.3.1 Aislamiento de los elementos de un Circuito Integrado

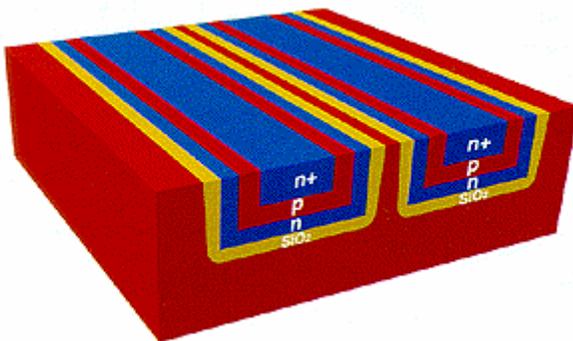
Dentro de un circuito integrado puede encontrarse una gran cantidad de componentes. Estos componentes pueden ser de diferentes tipos: resistencias, transistores, condensadores, etc., o del mismo tipo. Una de las necesidades que se presenta es separar los elementos, no físicamente ya que todos forman parte del mismo circuito integrado, sino que han de ser aislados eléctricamente para que cada uno pueda seguir comportándose según sus características, es decir, que, por ejemplo, los transistores sean exactamente iguales y cumplan las mismas propiedades que tiene un transistor discreto (que no forma parte de un circuito integrado).

Hay varias formas de conseguir el aislamiento eléctrico entre los diferentes elementos que componen un circuito integrado: la más usada de todas ellas, debido a lo económica que resulta, es la denominada "aislamiento de unión" (fig 2.6). Supóngase que se quieren separar dos transistores, este método consiste en polarizar inversamente las regiones N y P y, al no circular corriente, se produce el deseado aislamiento eléctrico entre los dos transistores.



**Fig. 2.6 Técnica de Aislamiento de Unión**

Otra forma es usando dióxido de silicio,  $\text{SiO}_2$ , recubriendo cada región de colector de cada uno de los transistores, el dióxido de silicio se comporta como un aislante. Por último, hay un tipo de aislamiento denominado "tipo viga" que es parecido al aislamiento de unión. La diferencia radica en que en el tipo viga, al realizar la metalización, se forma una capa muy gruesa encima de la oblea (fig. 2.7). Después se remueve el silicio que sobra en el sustrato tipo P. Se forma una estructura con los circuitos conectados semirrígidamente y todos los elementos separados unos de otros.



**Fig. 2.7 Aislamiento Tipo Viga**

### 2.3.2 Tecnología de Película Delgada y Gruesa

Las características, propiedades y apariencia generales de los circuitos integrados de película delgada y gruesa son similares, aunque ambos difieren en muchos aspectos de los circuitos integrados monolíticos. No se forman dentro de una oblea semiconductor, sino sobre la superficie de un sustrato aislante, como vidrio o un material cerámico adecuado. Además solamente se forman elementos pasivos (resistencias, capacitores) por medio de técnicas de película delgada o gruesa en la superficie aislante. Después de que se forman los elementos pasivos, los elementos activos (transistores, diodos) se añaden como elementos discretos sobre la superficie de la estructura. Los dispositivos activos discretos se producen la mayoría de las veces gracias al proceso monolítico.

En los circuitos integrados monolíticos se ha visto que se forman todos los componentes a la vez en un sustrato semiconductor. En la tecnología de película delgada y en la de película gruesa no ocurre lo mismo. Las resistencias y condensadores de valores pequeños

se fabrican en el sustrato, pero las resistencias y los condensadores de valores grandes y algunos circuitos monolíticos son exteriores al chip y se conectan formando un circuito híbrido. Este tipo de circuitos tiene la peculiaridad de que no se forman sobre la superficie de un semiconductor sino que lo hacen sobre un material aislante que puede ser vidrio o un material cerámico.

La principal diferencia entre las técnicas de película delgada y gruesa es el proceso empleado para formar los componentes pasivos y el patrón de conducción metálica. El circuito de película delgada aprovecha una técnica de evaporación o de dispersión por cátodo, y el circuito de película gruesa emplea técnicas de serigrafía. En general, los componentes pasivos de los circuitos integrados de película pueden formarse con un amplio rango de valores y tolerancias en comparación con los IC monolíticos. El uso de los elementos discretos también incrementa la flexibilidad del diseño de circuitos integrados de película, aunque el circuito resultante será mucho más grande. El costo de los circuitos integrados de película con una gran cantidad de elementos es también considerablemente mayor que el de los circuitos integrados monolíticos.

La técnica de fabricación de películas delgadas consiste en ir haciendo una deposición por medio de una evaporación al vacío o pulverización catódica. La superficie que contiene el sustrato actúa como el ánodo, y el material que se va depositando por la deposición como cátodo. Los pasos para el procesamiento de un circuito integrado por tecnología de película delgada son muy similares a los que se han explicado de los circuitos monolíticos.

En la tecnología de película gruesa se utiliza un circuito impreso sobre el cual se van a depositar las resistencias, condensadores, etc. Una de las ventajas de esta tecnología es que resulta más barata que la de película delgada.

## **2.4 Tipos de Chip o Integrado**

### **2.4.1 Integrados**

Puede parecer complicado al principio, pero el tema de las normalizaciones que rodea al mundo de los integrados, bien en encapsulados o bien en cuanto a zócalos y conexiones, es sencillo si se enfoca desde un punto de vista práctico.

Toda la gama de circuitos integrados disponibles se engloba dentro de cierta familia o apartado. Podemos ver una primera subdivisión de los circuitos integrados en función de su aplicación específica. Una segunda clasificación podría ser aquella que nos permite clasificar los chips según estos se dividan por el tipo de encapsulado. Pero a pesar de existir cierta norma, los fabricantes suelen hacer sus propias subclasificaciones, lo cual suele desembocar en un más que aparente caos.

Antes de continuar con este tema conviene aclarar que la forma en que se aplican encapsulados a los circuitos integrados ha motivado en los últimos años la aparición en el mercado electrónico de conjuntos de componentes discretos típicos -como, por ejemplo, las resistencias- que han aprovechado la "normativa" impuesta por los chips en su propio

beneficio, acogiendo a los tamaños y encapsulados de aquellos, lo cual simplifica diseños y facilita la colocación de ingentes cantidades de componentes en un espacio bastante reducido. Por esta razón no debe sorprendernos encontrar un "aparente" chip o circuito integrado dentro de un moderno circuito y que tal chip no es más que un conjunto de 8 ó 10 resistencias de idéntico valor óhmico, con lo que esto representa en cuanto a ahorro, tanto en la parte económica como en la de espacio, cuestión a tener muy en cuenta en el diseño electrónico moderno.

#### **2.4.2 Los Integrados Según sea su Aplicación**

Podríamos decir que por cada aplicación específica que se nos ocurra y que haya sido diseñada en forma de componentes discretos -esto es, no integrados- existe un circuito monolítico capaz de implementar la misma función. Esto, como es lógico, no deja de ser una pequeña exageración pero lo que no es menos cierto es que la evolución tecnológica y el abaratamiento de costes de los circuitos integrados hacen que aparezcan más y más modelos de circuitos integrados cada día.

No es extraño que la evolución tecnológica tienda a esto: ¿a quién no le encantaría realizar una pequeña aplicación electrónica y meterla luego dentro de un encapsulado único y fácil de colocar en cualquier circuito? Podemos avanzar que esto es ya una realidad para el aficionado a la electrónica, pero esto... es ya otra historia.

#### **2.4.3 Tipos de Chip o Integrados**

Dentro de la familia de los circuitos integrados disponibles hoy en día en el mercado -no olvidemos que esto varía en horas- podemos encontrar tres apartados fundamentales:

1. Circuitos Integrados Lineales
2. Circuitos Integrados Digitales
3. Circuitos de Tipo Híbrido

Puede que esta no sea la división más exacta, pero si es la más completa y a grosso modo esos son los principales tipos de IC's que se ocupan actualmente en el mercado.

De un lado tenemos los circuitos lineales, denominación que normalmente se aplica a circuitos integrados de uso específico y que no se englobe en el amplio grupo de las aplicaciones digitales. Puede decirse que esta gama de circuitos reproduce comportamientos implementables con circuitería analógica de tipo discreto. Por poner un ejemplo, los amplificadores operacionales pueden ser reproducidos transistor a transistor de forma independiente, lo cual, hoy en día, parece un asunto fuera de toda lógica.

Por otro lado, los circuitos integrados digitales se dedican a trabajar con señales de tipo "todo o nada" o "cero y uno", asunto este dedicado, casi en exclusividad, al mundo de los ordenadores y la informática.

En último lugar aparecen una gama de circuitos integrados a los que hemos dado en denominar híbridos. Esta familia abarca toda la gama de integrados que no puede colocarse de forma contundente a un lado u otro dentro de los dos grupos anteriores.

Para poder tener una idea más clara de a qué grupo pertenece cada circuito integrado vamos a abordar unos ejemplos dentro de cada grupo comentado.

#### **2.4.3.1 Circuitos Lineales Analógicos**

Queda claro que las aplicaciones de carácter analógico han precedido, de forma histórica, a las de carácter digital. Por esta razón cabría pensar que la realización de integrados de tipo analógico pasa sólo por el trámite de colocar un circuito que opere correctamente con componentes discretos y encapsularlo en un formato monolítico. Además de esto es preciso que dicho circuito sea rentable, tanto en el campo económico como en el de la prosperidad de futuras aplicaciones para el mismo.

Como ejemplo ya mencionado destaca el amplificador operacional, pero hay otros tan interesantes como éste. Podemos mencionar los amplificadores integrados que equipan tanto los modernos equipos de radiocasete para coche como los equipos Hi-Fi caseros. También destacan los integrados destinados a los equipos de recepción (y emisión) de radio, TV y comunicaciones en general.

Otro campo de aplicación de los integrados lineales es el de los sensores integrados, aunque este apartado lo comparten con los circuitos de tipo híbrido que luego comentaremos.

#### **2.4.3.2 Circuitos Digitales de Bit a Bit**

La parte mínima de un circuito digital está introducida en un chip y responde a la denominación de puerta lógica. Es posible, cómo no, implementar esta misma puerta en modo de componentes discretos.

Una puerta lógica, como ya veremos, realiza la parte más sencilla de la operativa de un circuito digital. Por ejemplo, cuando introducimos un cero lógico (p. ej. cero voltios) en una puerta que realice la función lógica "inversor" obtendremos en la salida de dicho chip un uno lógico ( +5 V si trabajamos en norma TTL ). Además de estas sencillas funciones los circuitos digitales pueden contener:

Funciones lógicas complejas, memoria volátil y no volátil, Unidad Central de Proceso o CPU, microcontroladores, registros de desplazamiento, etc.

#### **2.4.3.3 Circuitos Integrados Híbridos**

Para finalizar este breve repaso por los circuitos integrados existentes en el mercado vamos a abordar el apartado que hemos dado en llamar "circuitos híbridos".

El término circuito integrado híbrido se aplica a una amplia variedad de circuitos integrados formados por varios microcircuitos, y también en aquellos formados por una combinación de las técnicas de película y de IC monolítico. Un circuito integrado por varios microcircuitos emplea las técnicas monolítica o de película para crear los diversos componentes, o juegos de circuitos individuales, que luego se interconectan sobre un sustrato aislante y son encapsulados juntos. En un tipo más sofisticado de circuito integrado híbrido, primero se forman los dispositivos activos dentro de una oblea semiconductor, cubierta después con una capa aislante, como el  $\text{SiO}_2$ . Después se emplean las técnicas de película para formar los elementos pasivos sobre la superficie de  $\text{SiO}_2$ . Las conexiones se hacen de la película hacia la estructura monolítica a través de “ventanas” cortadas en la capa de  $\text{SiO}_2$ . A este apartado pertenecen circuitos tales como los convertidores de nivel, los convertidores A/D o sus homónimos D/A.

Un convertidor de nivel será, por ejemplo, aquel que está destinado a compatibilizar las diferentes familias lógicas. Por comentar un caso claro, la familia de circuitos digitales denominada TTL responde a niveles lógicos típicos de 0 = cero voltios y 1 = cinco voltios, mientras que los niveles típicos de la familia lógica CMOS son de 0 = cero voltios y 1 = depende de la alimentación.

Queda claro que para intercambiar datos entre un formato y otro deberemos utilizar un tipo de chip que nos permita convertir niveles, con lo cual queda clara la aplicación de éstos.

En resumen hemos visto las características básicas de la fabricación de IC's, un estudio mas detallado de los mismos, requeriría todo un libro completo, lo cual no es la intención de este tratado. Sin embargo se han descrito las técnicas que han permitido desarrollar la mayoría de estos circuitos hasta un grado de integración inimaginable y con mejoras constantes a los arreglos clásicos para dar como resultado los potentes procesadores de hoy en día y, sin dejar de lado, por supuesto a los dispositivos osciladores integrados, tecnologías de grabación MOS...etc, los cuales han dado pie a la tecnología RFID.

## **2.5 MODULACIÓN**

Muchas señales de entrada no pueden ser enviadas directamente hacia el canal, como vienen del transductor. Para eso se modifica una onda portadora, cuyas propiedades se adaptan mejor al medio de comunicación en cuestión, para representar el mensaje.

Para el caso de los dispositivos de identificación por radiofrecuencia (RFID) nos encontramos en la misma necesidad de enviar los datos desde el chip portador de la información que necesitamos acerca de algún determinado producto, hacia el lector para tener una comunicación óptima entre ambos dispositivos. Para tal efecto los métodos de modulación empleados para alterar la portadora codificada en estos dispositivos son diversos. Se emplea desde la modulación en amplitud (AM), la modulación de fase (PM), la modulación de frecuencia (FM) y otro tipo de modulaciones derivadas de las anteriores y que sirven como técnicas de codificación para transformar señales digitales a señales análogas, estamos hablando de técnicas como FSK, PPM, PDM o incluso CW (continuous wave) en la que debemos establecer un punto y aparte.

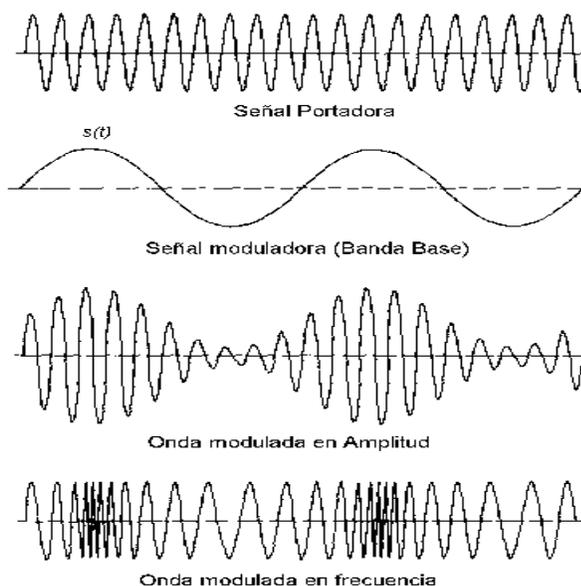
A continuación una descripción detallada de los principales tipos de modulación que se emplean comúnmente. Un estudio mas exhaustivo puede ser consultado en la bibliografía presentada. La intención de esta sección es presentar solamente las bases de la modulación analógica. Un estudio más amplio de los procedimientos para la modulación digital, integridad de datos y seguridad se verá en secciones posteriores.

Definiciones:

"La modulación es la alteración sistemática de una onda portadora de acuerdo con el mensaje (señal modulada) y puede ser también una codificación"

"Las señales de banda base producidas por diferentes fuentes de información no son siempre adecuadas para la transmisión directa a través de un a canal dado. Estas señales son en ocasiones fuertemente modificadas para facilitar su transmisión."

Una portadora es una senoide de alta frecuencia, y uno de sus parámetros (tal como la amplitud, la frecuencia o la fase) se varía en proporción a la señal de banda base  $s(t)$ . De acuerdo con esto, se obtiene la modulación en amplitud (AM), la modulación en frecuencia (FM), o la modulación en fase (PM). La siguiente figura muestra una señal de banda base  $s(t)$  y las formas de onda de AM y FM correspondientes. En AM la amplitud de la portadora varía en proporción a  $s(t)$ , y en FM, la frecuencia de la portadora varía en proporción a  $s(t)$  (ver figura 2.8).



**Fig. 2.8 Señales para Modulación**

Es interesante hacer hincapié en que muchas formas de comunicación no eléctricas también encierran un proceso de modulación, y la voz es un buen ejemplo. Cuando una persona habla, los movimientos de la boca ocurren de una manera mas bien lenta, del orden de los 10 Hz, que realmente no pueden producir ondas acústicas que se propaguen. La transmisión de la voz se hace por medio de la generación de tonos portadores, de alta frecuencia, en las cuerdas vocales, tonos que son modulados por los músculos y órganos de la cavidad oral. Lo que el oído capta como voz, es una onda acústica modulada, muy similar a una onda eléctrica modulada.

### 2.5.1 ¿Porque se Modula?

Existen varias razones para modular, entre ellas:

- Facilita la PROPAGACIÓN de la señal de información por cable o por el aire.
- Ordena el RADIOESPECTRO, distribuyendo canales a cada información distinta.
- Disminuye DIMENSIONES de antenas.
- Optimiza el ancho de banda de cada canal
- Evita INTERFERENCIA entre canales.
- Protege a la Información de las degradaciones por RUIDO.
- Define la CALIDAD de la información transmitida.

Modulación para facilidad de radiación: Una radiación eficiente de energía electromagnética requiere de elementos radiadores (antenas) cuyas dimensiones físicas serán por lo menos de 1/10 de su longitud de onda (ver fórmula). Pero muchas señales, especialmente de audio, tienen componentes de frecuencia del orden de los 100 Hz o menores, para lo cual necesitarían antenas de unos 300 km de longitud si se radiaran directamente. Utilizando la propiedad de traslación de frecuencias de la modulación, estas señales se pueden sobreponer sobre una portadora de alta frecuencia, con lo que se logra una reducción sustancial del tamaño de la antena. Por ejemplo, en la banda de radio de FM, donde las portadoras están en el intervalo de 88 a 108 MHz, las antenas no deben ser mayores de un metro.

$$\lambda = \frac{c}{f}$$

Donde,

$\lambda$  es la longitud de onda (m),

c es la velocidad de la luz ( $3 \times 10^8$  m/s),

f es la frecuencia (Hz).

Modulación para reducir el ruido y la interferencia: Se ha dicho que es imposible eliminar totalmente el ruido del sistema. Y aunque es posible eliminar la interferencia, puede no ser práctico. Por fortuna, ciertos tipos de modulación tiene la útil propiedad de suprimir tanto el ruido como la interferencia. La supresión, sin embargo, ocurre a un cierto precio; generalmente requiere de un ancho de banda de transmisión mucho mayor que el de la señal original; de ahí la designación del ruido de banda ancha. Este convenio de ancho de banda para la reducción del ruido es uno de los intereses y a veces desventajosos aspectos del diseño de un sistema de comunicación.

Modulación por asignación de frecuencia: El propietario de un aparato de radio o televisión puede seleccionar una de varias estaciones, aún cuando todas las estaciones estén transmitiendo material de un programa similar en el mismo medio de transmisión. Es posible seleccionar y separar cualquiera de las estaciones, dado que cada una tiene asignada una frecuencia portadora diferente. Si no fuera por la modulación, solo operaría una estación en un área dada. Dos o más estaciones que transmitan directamente en el mismo medio, sin modulación, producirán una mezcla inútil de señales interferentes.

Modulación para multicanalización: A menudo se desea transmitir muchas señales en forma simultánea entre dos puntos. Las técnicas de multicanalización son formas intrínsecas de modulación, permiten la transmisión de múltiples señales sobre un canal, de tal manera que cada señal puede ser captada en el extremo receptor. Las aplicaciones de la multicanalización comprenden telemetría de datos, emisión de FM estereofónica y telefonía de larga distancia. Es muy común, por ejemplo, tener hasta 1,800 conversaciones telefónicas de ciudad a ciudad, multicanalizadas y transmitidas sobre un cable coaxial de un diámetro menor de un centímetro.

Modulación para superar las limitaciones del equipo: El diseño de un sistema queda generalmente a la disponibilidad de equipo, el cual a menudo presenta inconvenientes en relación con las frecuencias involucradas. La modulación se puede usar para situar una señal en la parte del espectro de frecuencia donde las limitaciones del equipo sean mínimas o donde se encuentren más fácilmente los requisitos de diseño. Para este propósito, los dispositivos de modulación se encuentran también en los receptores, como ocurre en los transmisores.

### 2.5.2 ¿ Como se Modula ?

Frecuentemente se utilizan dispositivos electrónicos semiconductores con características no lineales (diodos, transistores, bulbos), resistencias, inductancias, capacitores y combinaciones entre ellos. Estos realizan procesos eléctricos cuyo funcionamiento es descrito de su representación matemática.

$$s(t) = A \sin(\omega t + \theta)$$

Donde,

A: Amplitud de la señal moduladora (volts)

w: Frecuencia angular de la portadora (rad/s)

$\theta$ : ángulo de fase de la portadora (rad)

Hay que recordar que la expresión anterior tiene que ver con el hecho de que las señales de información deben ser transportadas entre un transmisor y un receptor sobre alguna forma de medio de transmisión. Sin embargo, las señales de información pocas veces encuentran una forma adecuada para la transmisión. No hay que olvidar que la modulación se define como el proceso de transformar información de su forma original a una forma más adecuada para la transmisión. Demodulación es el proceso inverso. La modulación se realiza en el transmisor en un circuito llamado modulador, y el proceso inverso se lleva a cabo en el receptor, específicamente el demodulador.

### 2.5.3 Tipos de Modulación y Relación Señal-Canal-Ruido

#### 2.5.3.1 ¿ Que tipos de modulación existen ?

Existen básicamente dos tipos de modulación: la modulación ANALÓGICA, que se realiza a partir de señales analógicas de información, por ejemplo la voz humana, audio y video en su forma eléctrica y la modulación DIGITAL, que se lleva a cabo a partir de señales generadas por fuentes digitales, por ejemplo una computadora.

Modulación Analógica: AM, FM, PM  
Modulación Digital: ASK, FSK, PSK, QAM

### **2.5.3.2 ¿ Como afecta el canal a la señal ?**

Depende del medio o canal, ya que hay unos mejores que otros, aunque también depende del tipo de modulación y aplicación. Los principales efectos que sufre la señal al propagarse son:

- Atenuación
- Desvanecimiento
- Ruido Blanco aditivo
- Interferencia externa
- Ruido de fase
- Reflexión de señales
- Refracción
- Difracción
- Dispersión

### **2.5.3.3 ¿ Que relación existe entre la modulación y el canal ?**

El canal influye fuertemente en la elección del tipo de modulación de un sistema de comunicaciones, principalmente debido al ruido.

CANAL: Ruido, Distorsión, Interferencia y Atenuación.

MODULACIÓN: Inmunidad al ruido, Protege la calidad de la información, Evita interferencia.

### **2.5.4 Modulación en Amplitud (AM)**

Modulación de amplitud (AM es el proceso de cambiar la amplitud de una portadora de frecuencia relativamente alta de acuerdo con la amplitud de la señal modulante (información). Las frecuencias que son lo suficientemente altas para radiarse de manera eficiente por una antena y propagarse por el espacio libre se llaman comúnmente radiofrecuencias o simplemente RF. Con la modulación de amplitud, la información se imprime sobre la portadora en la forma de cambios de amplitud. La modulación de amplitud es una forma de modulación relativamente barata y de baja calidad de modulación que se utiliza en la radiodifusión de señales de audio y video. La banda de radiodifusión comercial AM abarca desde 535 a 1605 kHz. La radiodifusión comercial de TV se divide en tres bandas (dos de VHF y una de UHF). Los canales de la banda 1 entre 2 y 6 (54 a 88

MHz), los canales de banda alta de VHF son entre 7 MHz) y los canales de UHF son entre 14 a 83 (470 a 890 MHz). La modulación de amplitud también se usa para las comunicaciones de radio móvil de dos sentidos tal como una radio de banda civil (CB) (26.965 a 27.405 MHz). Un modulador AM es un aparato no lineal con dos señales de entrada de información: una señal portadora de amplitud constante y de frecuencia sencilla, y la señal de información. La información actúa sobre o modula la portadora y puede ser una forma de onda de frecuencia simple o compleja compuesta de muchas frecuencias que fueron originadas de una o más fuentes. Debido a que la información actúa sobre la portadora, se le llama señal modulante. La resultante se llama onda modulada o señal modulada.

#### **2.5.4.1 La envolvente de AM**

Varias formas o variaciones de modulación de amplitud son posibles de generar. Aunque matemáticamente no es la forma más sencilla, la portadora de AM de doble banda lateral (AM DSBFC) se discutirá primero, puesto que probablemente sea la forma más utilizada de la modulación de amplitud. AM DSBFC se le llama algunas veces como AM convencional. La onda modulada de salida contiene todas las frecuencias que componen la señal AM y se utilizan para llevar la información a través del sistema. Por lo tanto, a la forma de la onda modulada se le llama la envolvente. Sin señal modulante, la onda de salida simplemente es la señal portadora amplificadas. Cuando se aplica una señal modulante, la amplitud de la onda de salida varía de acuerdo a la señal modulante. Observe que la forma de la envolvente de AM es idéntica a la forma de la señal modulante. Además el tiempo de un ciclo de la envolvente es el mismo que el periodo de la señal modulante. Consecuentemente, la relación de repetición de la envolvente es igual a la frecuencia de la señal modulante. Espectro de frecuencia de AM y ancho de banda Como se estableció anteriormente, un modulador AM en un dispositivo no lineal, Por lo tanto, ocurre una mezcla no lineal y la envolvente de salida es una onda compleja compuesta de un voltaje de cd, la frecuencia portadora y las frecuencias de suma y diferencia (es decir, los productos cruzados). La suma y diferencia de frecuencias son desplazadas de la frecuencia portadora por una cantidad igual a la frecuencia de la señal modulante. Por lo tanto, una envolvente de AM contiene componentes en frecuencia espaciados por  $f_m$  Hz en cualquiera de los lados de la portadora. Sin embargo, debe observarse que la onda modulada no contiene un componente de frecuencia que sea igual a la frecuencia de la señal modulante. El efecto de la modulación es trasladar la señal de modulante en el dominio de la frecuencia para reflejarse simétricamente alrededor de la frecuencia del conducto.

#### **2.5.4.2 Recepción de AM**

La recepción de AM es el proceso inverso de la transmisión de AM. Un receptor de AM convencional, simplemente convierte una onda de amplitud modulada nuevamente a la fuente original de información (o sea, demodular la onda AM). Cuando se demodula una onda AM, la portadora y la porción de la envolvente que lleva la información (o sea, las bandas laterales) se convierten (se "bajan ") o se trasladan del espectro de radio frecuencia a la fuente original de información. El propósito de este capítulo es describir el proceso de

demodulación de AM y mostrar varias configuraciones del receptor para poder realizar este proceso. Un receptor debe ser capaz de recibir, amplificar, y demodular una señal de RF. Un receptor también debe ser capaz de limitar las bandas del espectro Total de radio frecuencias a una banda específica de frecuencias. En muchas aplicaciones el receptor debe de ser capaz de cambiar el rango (banda) de frecuencia que es capaz de recibir. A este proceso se le llama sintonizar el receptor. Una vez que una señal de RF se recibe, se amplifica, y se limitan las bandas, deberá convertirse a la fuente original de información. A este proceso se le llama demodulación. Una vez demodulada, la información podría requerir de mayor limitación de las bandas y una amplificación, antes de considerarse lista para usar. Para entender completamente el proceso de demodulación, primero es necesario tener una comprensión básica de la terminología utilizada para describir las características de los receptores y de los circuitos del receptor. La figura siguiente (2.9) muestra un diagrama a bloques simplificado de un típico receptor de AM. La sección de RF es la primera etapa y, por lo tanto, frecuentemente se llama la parte frontal. Las funciones principales de la sección de RF son: detectar, limitar las bandas y amplificar las señales RF recibidas. En esencia, la sección de RF establece el umbral del receptor (o sea, el nivel mínimo para la señal de RF que el receptor puede detectar y demodular a una señal de información útil).

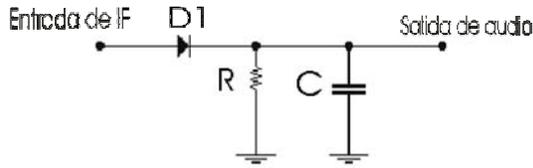


**Fig. 2.9 Diagrama básico de un receptor AM**

La sección de RF abarca uno o más de los siguientes circuitos: antena, red de acoplamiento de la antena, filtro ( pre-selector ), y uno o más amplificadores de RF. La sección de mezclador / convertidor reduce las frecuencias de RF recibidas a frecuencias intermedias (IF). La sección de IF generalmente incluye varios amplificadores en cascada y los filtros pasa-bandas. Las funciones principales de la sección de IF son la amplificación y selectividad. El detector de AM demodula la onda de AM y recupera la información de la fuente original. La sección de audio simplemente amplifica la información recuperada a un nivel utilizable.

#### **2.5.4.2.1 Detector de Picos**

La función de un detector de AM es demodular la señal de AM, recuperar y reproducir la información de la fuente original. Y debe tener las mismas características relativas de amplitud. La siguiente figura (2.10) “detector de picos” muestra un diagrama esquemático para un demodulador de AM sencillo no coherente, que se llama comúnmente detector de picos.



**Fig. 2.10 Detector de Picos**

Debido a que el diodo es un dispositivo no lineal, ocurre una mezcla no lineal en D1 cuando dos o más señales se aplican a su entrada. Por lo tanto, la salida contiene las frecuencias de entrada originales, sus armónicas, y sus productos cruzados. Esencialmente, la diferencia entre un modulador de AM y un demodulador de AM es que la salida de un modulador se sintoniza con las frecuencias de suma (convertidor de altas frecuencias), mientras que la salida de un demodulador se sintoniza a las frecuencias de diferencia (convertidor de baja frecuencia). El circuito demodulador mostrado en la figura 1 se le llama común mente detector de diodos puesto que el dispositivo no lineal es un diodo, o un detector de picos, porque detecta los picos de la envolvente de entrada, o un detector de envolvente o de figura porque detecta la figura de la envolvente de entrada. Esencialmente, la señal de la portadora captura el diodo y lo obliga a activarse y desactivarse (rectificar) sincrónicamente (tanto frecuencia como fase). Así las frecuencias laterales se mezclan con la portadora, y se recuperan las señales de banda base original. La red RC que sigue al diodo en un detector de picos es un filtro de pasa - bajas. La pendiente de la envolvente depende tanto de la frecuencia de la señal modulante como del coeficiente de modulación (m). Por lo tanto, la pendiente máxima ocurre cuando la envolvente está cruzando su eje cero en la dirección negativa. La frecuencia de la señal modulante más alta que puede demodularse por un detector de picos sin atenuarse se da como:

$$f_{m(\text{máx})} = \frac{\sqrt{\frac{1}{m^2} - 1}}{2\pi RC}$$

Donde,

$f_{m(\text{máx})}$ : Frecuencia máxima de la señal modulante (Hz)

m: Coeficiente de modulación sin unidades

RC: Constante de tiempo (s)

Para 100% de modulación, el numerador de la ecuación anterior tiende a cero, que esencialmente significa que todas las frecuencias de la señal modulante son atenuadas cuando se demodula.

El mezclado no lineal ocurre cuando dos o mas señales se combinan en un dispositivo no lineal tal como un diodo o amplificador de señal grande. Con el mezclado no lineal, las señales de entrada se combinan de una manera no lineal y producen componentes de frecuencias adicionales.

### 2.5.4.3 Índice de Modulación

Se denomina "índice de modulación" a la relación que existe entre la amplitud máxima de la señal modulante y la amplitud máxima de la portadora. Matemáticamente se expresa porcentualmente y representa en qué proporción la señal modulante modula a la portadora. La expresión matemática es:

$$E = EM/E_p \times 100 [\%]$$

M = índice de modulación porcentual.

EM = amplitud máxima de la señal modulante.

E<sub>p</sub> = amplitud máxima de la señal portadora.

Los transmisores, generalmente, operan cerca del cien por ciento de modulación, ya que para valores por encima de éste, se produce una distorsión de la señal de AM (sobremodulación) originando armónicas cuyas frecuencias pueden producir bandas laterales que interfieren los canales adyacentes. También debemos recordar que la relación señal a ruido aumenta con "M".

### 2.5.4.4 Desventajas y Ruido

Como un medio para transmitir información, la modulación de amplitud tiene muchas ventajas; sin embargo, también presenta algunas desventajas que, en ciertas condiciones, limitan su utilidad y obligan a buscar otras formas de modulación. La desventaja principal de la modulación de amplitud estriba en que la afectan fácilmente diversos fenómenos atmosféricos (estática), señales electrónicas con frecuencias parecidas y las interferencias ocasionadas por los aparatos eléctricos tales como motores y generadores. Todos estos ruidos tienden a modular en amplitud la portadora, del mismo modo que lo hace su propia señal moduladora. Por lo tanto se convierten en parte de la señal modulada y subsisten en ella durante todo el proceso de demodulación. Después de la demodulación se manifiestan como ruido o distorsión, que si es bastante fuerte, puede sobreponerse a toda la información y hacer completamente inaprovechable la señal demodulada. Aun si aquellos no son tan acentuados como para tapar parte de la información, sí pueden ser extremadamente molestos.

El ruido constituye un problema grave en todos los receptores de radio. Hay diferentes tipos de ruido, como el zumbido, un tono constante de baja frecuencia (unas dos octavas por debajo del do), producido generalmente por la frecuencia de la fuente de alimentación de corriente alterna (por lo común 60 Hz) que se superpone a la señal debido a un filtrado o un apantallamiento defectuoso; el siseo, un tono constante de alta frecuencia, y el silbido, un tono limpio de alta frecuencia producido por una oscilación involuntaria de frecuencia audio, o por un golpeteo. Estos ruidos se pueden eliminar mediante un diseño y una construcción adecuados. Sin embargo, ciertos tipos de ruidos no se pueden eliminar. El más importante en los equipos normales de AM de baja y media frecuencias es el ruido parásito, originado por perturbaciones eléctricas en la atmósfera. El ruido parásito puede proceder del funcionamiento de un equipo eléctrico cercano (como los motores de automóviles o

aviones), pero en la mayoría de los casos proviene de los rayos y relámpagos de las tormentas. Las ondas de radio producidas por estas perturbaciones atmosféricas pueden viajar miles de kilómetros sin sufrir apenas atenuación, y, dado que en un radio de algunos miles de kilómetros respecto del receptor de radio siempre hay alguna tormenta, casi siempre aparecen ruidos parásitos. Los ruidos parásitos afectan a los receptores FM en menor medida, ya que la amplitud de las ondas intermedias está limitada mediante circuitos especiales antes de la discriminación, lo que elimina los efectos de los ruidos parásitos. Otra fuente primaria de ruido es la agitación térmica de los electrones. En un elemento conductor a temperatura superior al cero absoluto, los electrones se mueven de forma aleatoria. Dado que cualquier movimiento electrónico constituye una corriente eléctrica, la agitación térmica origina ruido al amplificarlo en exceso. Este tipo de ruido se puede evitar si la señal recibida desde la antena es notablemente más potente que la corriente causada por la agitación térmica; en cualquier caso, se puede reducir al mínimo mediante un diseño adecuado. Un receptor teóricamente perfecto a temperatura ordinaria es capaz de recibir la voz de forma inteligible siempre que la potencia de la señal alcance los  $4 \times 10^{-18}$  W; sin embargo, en los receptores normales se precisa una potencia de señal bastante mayor.

### **2.5.5 Modulación en Frecuencia (FM)**

La modulación de frecuencia o FM, es uno de los métodos de transmisión de información más populares de nuestro tiempo. La principal razón de esta popularidad es la recepción prácticamente libre de ruido que este sistema provee, especialmente si se compara con la modulación de amplitud (AM), su competidor más próximo. La modulación de frecuencia se utiliza tanto en radioafición como en radio difusión comercial o "broadcasting". El sonido de TV en VHF y UHF también se transmite en FM.

Las estaciones de radiodifusión comerciales en FM transmiten en la banda de 88 a 108 MHz. A cada emisora se le asigna un ancho de banda de 200KHz. Para los radioaficionados se han destinado ciertas bandas específicas. La más conocida es la de 2 metros, la cual comprende frecuencias alrededor de 144MHz. Otras bandas de radioafición muy populares son las de 52 a 54 MHz, 146 a 148 MHz, 222 a 225MHz y 440 a 450 MHz, todas en el espectro de VHF. En la presente sección estudiaremos los fundamentos de la modulación frecuencia, sus orígenes, ventajas y desventajas y otros temas de interés. Conoceremos también cómo están estructurados, en términos generales, un transmisor y un receptor de FM. Todo esto nos servirá cómo base para emprender en el futuro el estudio completo de un receptor experimental de FM que Ud. mismo podrá construir, analizar y reparar paso a paso.

#### **2.5.5.1 Ventajas y desventajas de la Modulación de Frecuencia.**

La principal ventaja de la modulación de frecuencia es su habilidad para producir una alta relación de señal a ruido (SNR) cuando recibe un señal de moderada intensidad. En otras palabras, la recepción en FM está prácticamente exenta de ruido e interferencia.

Por esta razón, la modulación de frecuencia es el modo elegido por los servicios de comunicaciones móviles y las emisoras que difunden programas de calidad, en especial emisiones musicales.

En su camino del transmisor al receptor, un señal de RF puede incorporar ruido natural o ruido hecho por el hombre (MMN). El primero proviene de descargas atmosféricas y el segundo de aparatos generadores de chispas, como motores eléctricos, avisos luminosos de neón y sistemas de ignición de automóviles y bicicletas.

Todo ruido, cualquiera que sea su origen, modula en amplitud una onda viajera de RF. Por consiguiente, el ruido afecta la reproducción de la información en transmisiones de AM. La información transmitida puede ser sonido, imagen o otro tipo. La anterior es la razón por la cual los receptores de radio de AM y de TV son muy susceptibles a los ruidos e interferencias provenientes de electrodomésticos, automóviles, aviones, luces, etc. La información de la imagen en TV se envía modulada en amplitud. El ruido no afecta la recepción de FM porque los circuitos de detección de información responden solamente a las variaciones de frecuencia e ignoran las variaciones de amplitud. El ruido inducido en una señal modulada de RF puede también interferir con la frecuencia de la portadora, desviándola de su valor central.

Este problema se soluciona en los sistemas de FM utilizando, en el transmisor, un circuito de "preénfasis" a la entrada de audio del modulador y, en el receptor un filtro de "deénfasis" a la salida del detector o demodulador. El circuito de preénfasis o de preacentuación atenúa las frecuencias más bajas de audio y el de deénfasis las restablece a sus valores originales.

En contraste con la alta inmunidad al ruido, la señales de FM requieren de un gran ancho de banda y experimentan una severa distorsión cuando se propagan a través de la ionosfera. En radioafición, esta última circunstancia limita el uso de la modulación de frecuencia a bandas como la de 10 metros y a varios sectores del espectro de VHF, como las bandas de 52 a 54 MHz, 146 a 148 MHz y otras.

El amplio ancho de banda requerido en FM es otro de los factores determinantes de la alta calidad de reproducción de sonido que se consigue por este sistema. En radiodifusión por FM (88 a 108 MHz), las estaciones transmiten información dentro de un ancho de banda de 150 KHz, con 25 KHz de tolerancia. En total, disponen de 200 KHz.

Este ancho de banda (BW) veinte veces más grande que el utilizado en radiodifusión por AM (530 a 1600KHz), donde se dispone de sólo de 10 KHz para enviar una gama muy limitada de tonos. La utilización de BW tan amplio permite introducir en la señal de FM toda la gama audible de sonidos (20Hz a 20KHz), incluyendo a sus armónicos. Estos últimos son los que le dan el timbre distintivo a cada sonido, imprimiéndole fidelidad y realismo a cada audición.

En condiciones normales sin señal de entrada, la amplitud y frecuencia de la portadora permanecen constantes. Cuando se aplica la señal de modulación, la frecuencia de la portadora varía por encima y por debajo de su valor central de acuerdo a la amplitud y polaridad de la señal de modulación o de audio aplicada.

Específicamente, la frecuencia de la portadora se incrementa durante los semiciclos positivos de la señal de modulación y se reduce durante los negativos. La frecuencia de la portadora es máxima o mínima cuando la señal de modulación alcanza su valor pico positivo o negativo, respectivamente.

Si observáramos una onda FM veríamos que si se nota que existen más ciclos de RF (más alta frecuencia) cuando la señal de modulación es positiva y menos ciclos (más baja frecuencia) cuando la señal de modulación es negativa.

El cambio o desviación de frecuencia de la portadora con respecto a su valor central es proporcional al valor instantáneo de la señal de modulación. La desviación es mínima cuando la señal de modulación vale cero y máxima cuando alcanza su valor pico, negativo o positivo.

La desviación máxima o pico se llama  $\Delta f_c$  ("delta fc") y su valor lo define el transmisor. Las estaciones de radiodifusión de FM que transmiten en la banda de 88 a 108 MHz utilizan una desviación máxima de  $\pm 75$  KHz.

En televisión,  $\Delta f_c = \pm 25$  KHz. Entre otros sistemas de FM menos conocidos,  $\Delta f_c = \pm 15$  KHz

Para aclarar este concepto daremos un ejemplo. Si se modula una portadora de 100MHz con una onda senoidal de 1 KHz y 1Vp de amplitud en un sistema que tiene una desviación extrema de  $\pm 15$  KHz, la frecuencia de la portadora oscilaría 1000 veces por segundo entre 99.985 KHz y 100.015 KHz. Una señal de modulación de 2Vp y 1KHz causaría una desviación máxima de  $\pm 30$ KHz. Una señal de 2Vp y 2KHz provocaría también una desviación pico de  $\pm 30$  KHz pero a una tasa de cambio de 2000 veces por segundo.

En conclusión, en una señal de FM:

- La amplitud máxima en una señal de modulación controla la desviación pico de la frecuencia de la portadora.
- La frecuencia de la señal de modulación controla la tasa de cambio de la frecuencia de la portadora.
- La amplitud de la portadora permanece constante, independientemente de la frecuencia y la amplitud de la señal de modulación.

### **2.5.5.2 Bandas laterales e índice de modulación en FM**

La modulación en frecuencia de una portadora de RF con una señal de audio produce un gran número de bandas laterales.

La modulación de amplitud sólo produce dos bandas laterales. La separación entre bandas laterales adyacentes es igual a la frecuencia de la señal de modulación y su amplitud disminuye progresivamente a medida que se alejan de la portadora. Las bandas laterales más próximas a la portadora son las más fuertes o significativas y las más alejadas, las más débiles.

Por ejemplo, si se modula en frecuencia una portadora de 100 MHz con un tono de 2 KHz, el primer par de bandas laterales estará ubicado en 99.998 MHz y 100.002 MHz, respectivamente, el segundo en 99.994 MHz y 100.004 MHz, el tercero en 99.996 MHz y 100.006 MHz, y así sucesivamente.

La amplitud de la portadora y de las bandas laterales depende del "índice de modulación" del proceso. En FM el índice de modulación ( $m$ ) se define como la relación entre la

máxima desviación de frecuencia de la portadora ( $f_c$ ) y la frecuencia de la señal de modulación ( $f_m$ ). Esto es:

$$\text{Índice de modulación}(m) = \Delta f_c / f_m$$

Por ejemplo, si la desviación máxima es 15 KHz, el "índice de modulación" con una frecuencia de 10 KHz será  $m = 15/10 = 1.5$ , con una frecuencia de 5 KHz sería  $m = 15/5 = 3$ , con una frecuencia de 1 KHz sería  $m = 15/1 = 15$ , y así sucesivamente.

### 2.5.5.3 Ancho de banda en FM

Por definición, el ancho de banda de una señal modulada es la separación de frecuencia entre las bandas laterales más alejadas de la portadora. En FM el número de bandas laterales es muy grande. Por consiguiente, desde el punto de vista teórico, el ancho de banda de una señal de FM es ilimitado. En la práctica se omiten las bandas laterales menos significativas, es decir, las más alejadas de la portadora. Desde este punto de vista, BW de una señal de FM se define, en forma aproximada, como sigue:

$$B = 2 \Delta f_c + f_{\max}$$

En esta expresión,  $\Delta f_c$  es la desviación pico de la portadora, en Hz y la máxima frecuencia presente en la señal de modulación en Hz. Por ejemplo si  $\Delta f_c = \pm 75$  KHz y  $f_{\max} = 20$  KHz entonces  $B = 2 \times 75 + 20 = 150$  KHz + 20 = 170 KHz

Las estaciones de radiodifusión en FM utilizan un ancho de banda de 200 KHz. En consecuencia, la máxima frecuencia de modulación que pueden transmitir es 50 KHz, muy superior a la máxima frecuencia audible (20KHz). En AM, la máxima frecuencia que se puede transmitir es de 5KHz. La voz humana tiene muchas frecuencias componentes y por lo tanto, cuando se emite un sonido o una palabra, cada frecuencia componente genera numerosas bandas laterales, de diversa intensidad y distanciadas de manera diferente en cada instante. El número de bandas laterales significativas está también cambiando permanentemente. El resultado es un espectro continuo de bandas laterales a cada lado de la portadora.

Nótese que el BW de una señal de FM depende tanto de la amplitud como de la frecuencia de la señal de modulación. Esto es particularmente importante cuando se modula la voz humana. Dos voces nunca exhiben las mismas características de amplitud y frecuencia. En consecuencia, ambas tienen efectos diferentes en el BW. Por esta razón, para enviar el máximo de información de audio, el control de desviación del transmisor debe ajustarse de acuerdo a las características de voz del locutor. Esta operación puede resultar incómoda e imprecisa. Para minimizar este problema los equipos de FM utilizan un circuito denominado "clipper" o limitador en la sección procesadora de audio del transmisor. En este circuito, un resistor R1 establece el nivel de limitación o recorte de la amplitud de la señal de audio y un resistor R2 la cantidad de desviación deseada. El filtro minimiza la distorsión de la señal de salida. La operación de recorte de los picos de audio la realizan dos diodos D1 y D2.

# ***CAPÍTULO 3***

## **HISTORIA DEL RFID EN LAS COMUNICACIONES**

3.1 Introducción .....	65
3.2 El Siglo XX.....	66
3.4 Visión Histórica de la Comunicación Satelital .....	70
3.5 Génesis de Una Idea.....	75
3.6 De los años 60's a los 80's: RFID se vuelve una realidad .....	75
3.7 La Década de los 90 .....	77
3.8 La Actualidad del RFID.....	79

### 3.1 Introducción

Muchas cosas están ocultas en el tiempo. La tarea de trazar la historia y la genealogía es ardua y retadora, sin embargo al final de cuentas apremiante. Nuestro pasado puede abrir puertas a nuestro futuro, si nos damos cuenta RFID es una parte integral de nuestras vidas, RFID es usada por cientos, sino es que miles de aplicaciones como tecnología antirrobo de automóviles, podría ser también el registro del peaje sin necesidad de parar, la administración del tráfico (en algunos países se analiza la puesta en práctica de carreteras automatizadas auto controladas en donde los viajeros solo tengan que ceder el mando a sus automóviles, por supuesto el RFID solo entraría como auxiliar en esta nueva forma de viajar por carreteras ya que para el propósito antes mencionado se requieren de distintas tecnologías mas), el registro de entradas a un edificio, estacionamientos automáticos, el control de accesos a vehículos a comunidades privadas, aeropuertos, campos universitarios, la distribución de bienes, seguimiento de libros de biblioteca, compra en autoservicios, y la oportunidad creciente de rastrear los insumos en el manejo de una cadena de servicios.

Podemos trazar la genealogía del RFID remontándonos al principio del tiempo. La ciencia y la religión parecen coincidir en que en los primeros momentos de la creación existía energía electromagnética, citando un pasaje de la Biblia del libro del Génesis: “y Dios dijo hágase la luz y la luz se hizo”, antes de la luz todo estaba vacío y sin forma, antes que todo, hubo energía electromagnética.

El pensamiento humano resume que el universo fue creado en un instante con el Big Bang, la gran explosión de donde partió todo lo que conocemos hasta ahora, debatible o no, este pensamiento deduce que todo esta en las cuatro fuerzas fundamentales que se unificaron y que fueron la gravedad, el electromagnetismo y las fuerzas de fusión y fisión nuclear. La primera forma en el universo fue la energía electromagnética. Durante los primeros segundos del universo, los protones, neutrones y electrones empezaron a formarse cuando los protones (el elemento cuántico de la energía electromagnética) colisionaron convirtiendo energía en masa. El remanente electromagnético del Big Bang sobrevive hasta nuestros días como un siseo de microondas en el ruido del universo.

Ahora nos preguntamos por que de la importancia de todo esto y ¿que tiene que ver con el RFID?, pues bien toda esta energía es la fuente del RFID, pudo tomar más de 14 billones de años o incluso antes para que nosotros nos diésemos cuenta de como delimitar la energía electromagnética en la región radial, y aplicar este conocimiento al desarrollo de RFID.

Los chinos fueron probablemente los primeros en observar y usar los campos magnéticos en forma de magnetitas en el siglo I antes de Cristo, el entendimiento científico progresó muy lento hasta mas o menos el siglo XV. De los años 1600's a 1800's hubo una explosión de conocimiento observacional de la electricidad, la óptica y el magnetismo, acompañados por un creciente desarrollo de las matemáticas, uno de los pioneros de la electricidad en el siglo XVIII fue Benjamín Franklin.

El siglo XVIII marcó el inicio del entendimiento fundamental de la energía electromagnética. Michael Faraday un notorio experimentalista ingles, propuso en 1846 que tanto la luz como las ondas de radio son parte de la energía electromagnética. En 1864,

casi paralelo a los trabajos de Faraday, pero en otro lugar del mundo James Clerk Maxwell, un físico escocés publicó su teoría en campos electromagnéticos y concluyó que la energía eléctrica y magnética viaja en ondas transversales que se propagan a una velocidad igual a la de la luz. Poco después en 1887, Heinrich Rudolf Hertz, científico alemán confirmó la teoría electromagnética de Maxwell y produjo ondas electromagnéticas (las cuales estudio) de radio, las cuales demostró que son largas ondas transversales que viajan a la velocidad de la luz y pueden ser reflejadas, refractadas y polarizadas tal como también para el caso de la luz. Hertz es reconocido como el primero en transmitir y recibir ondas de radio y sus demostraciones fueron rápidamente seguidas por Aleksandr Popov en Rusia.

En 1896, Guglielmo Marconi demostró una exitosa transmisión de radiotelegrafía a través del Atlántico y el mundo a partir de entonces no volvió a ser el mismo. Las ondas de radio de Hertz, Popov y Marconi se diseñaron para la telegrafía o los puntos y líneas.

### **3.2 El Siglo XX**

En 1906, Ernest F. W. Alexanderson demostró la primera radio generación de onda continua y la transmisión de señales de radio. Estas señales logradas fueron el principio de la radio comunicación moderna, donde todos los aspectos de las radio ondas son controlados.

A principios del siglo XX, aproximadamente 1922, se considera el nacimiento del radar. El trabajo en radar durante la segunda guerra mundial fue tan significativo para la historia del RFID en cuanto a desarrollo tecnológico como lo fue el proyecto Manhattan en el laboratorio científico de Los Alamos, y fue crítico en el éxito para los aliados. El radar envía ondas de radio para detectar y localizar un objeto por la reflexión de las ondas de radio. Esta reflexión puede determinar la posición y velocidad de un objeto. La significancia del radar se entiende rápidamente en ambientes militares, muchos de los avances en aquellas épocas fueron celosamente mantenidos en secreto.

Desde mediados del siglo XX, la electrónica se convirtió en parte intrínseca de las modernas telecomunicaciones, al grado que hoy es difícil determinar donde empiezan y donde terminan algunos componentes electrónicos o de telecomunicación.

La electrónica creó un sin fin de elementos electrónicos como interruptores, resistencias, aislantes y transformadores, que fueron interconectados con tubos de vacío para producir sistemas completos de comunicaciones. En sus inicios, esos sistemas se montaban en mástiles de madera y más tarde se colocarían en artefactos de metal. El tubo de vacío, inventado en 1906 por Lee De Forest para transmitir y amplificar señales eléctricas, tuvo una influencia crucial para el desarrollo de las comunicaciones por radio y televisión. Sin embargo, mostró serias limitaciones de funcionamiento cuando se usó en máquinas más complejas como las computadoras y cuando se juntaban varios paneles, la probabilidad de que un tubo fallara era muy grande, por lo que para inicios de los cuarenta ya se trabajaba para reemplazarlo por dispositivos más pequeños como el transistor, cuyo tamaño original era 100 veces menor que el tubo de vacío.

De esta manera es que el RFID es la combinación de la transmisión de radio y el radar, es de esperarse que la convergencia entre estas dos disciplinas y el RFID ocurran en el contexto del desarrollo del radar.

Para 1947, con la invención del transistor en los Laboratorios Bell en Estados Unidos, se inició una asombrosa carrera por la miniaturización del equipo transmisor y receptor de telecomunicaciones. Sus características de no emisión de calor y bajos requerimientos de energía, permitieron abrir el camino a sistemas telefónicos compactos y eficientes.

El transistor es un dispositivo compuesto por materiales conocidos como semiconductores por sus especiales propiedades eléctricas, tales como el germanio, silicio, selenio y arseniuro de galio. Usando un pequeño cristal de silicón, los científicos de Laboratorios Bell en Estados Unidos, descubrieron que el cristal podía reaccionar a la corriente eléctrica casi de la misma manera que el tubo de vacío. Los primeros modelos de transistores no eran más grandes que un grano de arena, por lo que al sustituir los voluminosos y pesados tubos de vacío, el transistor marcó el camino hacia la masificación en el uso de la computadora y aparatos electrónicos como cámaras de televisión y receptores portátiles. Igualmente, los sistemas de conmutación telefónicos, al utilizar el transistor, reemplazaron a los dispositivos electromecánicos que producen ruido y son afectados por el polvo. La reducción masiva del peso y volumen de los equipos electrónicos, facilitó el desarrollo de la astronáutica y telecomunicaciones vía satélite. Fue tal su trascendencia que sus inventores, los científicos norteamericanos John Bardeen, Walter Brattain y William Shockley recibieron el Premio Nobel de física en 1956 por su contribución al desarrollo de los semiconductores.

El transistor fue solamente el primer paso de la vertiginosa miniaturización, ya que después de medio siglo de iniciada esta tendencia tecnológica, continúan lográndose asombrosos descubrimientos con ese mismo objetivo. Hacia 1958 la electrónica se transformó realmente en microelectrónica con la creación del circuito integrado, cuyo propósito principal es la integración a escala.

Un circuito integrado normal, construido comúnmente a base de silicio, consta de una pequeña placa de tamaño variable -cuyo estándar es de 25,41 mm por 12,7 mm- que contiene millares de transistores y otros circuitos elementales. La densidad y capacidad de los circuitos ha venido multiplicándose exorbitantemente. A inicios de los sesenta se consiguió integrar doce circuitos (pequeña escala) en una pastilla o chip de silicio; para finales de esa década fueron 100 (media escala); a principios de los setenta se dió la integración a gran escala con 1000; y, a fines de esa década se colocaron 50 mil circuitos lógicos llamados digitales que son usados en los ordenadores o computadoras.

No obstante la alta capacidad de integración lograda hace quince años, con los desarrollos de los circuitos digitales existe la impresión de estar cada vez frente al inicio de una nueva fase de la integración. Es maravilloso constatar que si bien es cierto que para 1987 un circuito contenía más de un millón de transistores (en comparación de uno en 1959), esa integración se aprecia modesta en relación a la que se pretende obtener para el año 2000, que podrá ser de mil millones. Los semiconductores de hoy contienen complejos circuitos integrados que se adaptan con facilidad para usos múltiples que abarcan desde juguetes,

relojes, calculadoras, procesadores de textos, hasta sistemas expertos que diseñan aviones. Sin los circuitos integrados y la amplia variedad de tecnología de estado sólido desarrollada desde hace 25 años sería poco probable que tuviéramos satélites para comunicaciones, sistemas de centrales electrónicas y toda la capacidad de transmisión que hoy poseen las redes.

Por su versátil aplicación, el desarrollo y fabricación de circuitos integrados ha pasado a ser una de las industrias más dinámicas y competidas en Estados Unidos, Japón, Suecia, la Comunidad Europea, Inglaterra, Alemania, Francia y Holanda. En febrero de 1988 por ejemplo, se tenían registrados 3,244 diseños de circuitos solamente en Estados Unidos, 1,376 en Japón y 25 en Alemania Federal. En los dos primeros países existen regiones y ciudades enteras cuya actividad central es la investigación, innovación y manufacturación de semiconductores.

### **3.3 El Espectro Radioeléctrico y las Microondas**

En los últimos años, las modernizaciones del sistema telefónico y las telecomunicaciones avanzan a pasos agigantados también gracias a la explotación tecnológica de las microondas y las fibras ópticas. Aunque las microondas se empezaron a utilizar desde la segunda guerra mundial, fue hasta hace dos décadas que inició su más cabal aprovechamiento.

Los avances de la telecomunicación inalámbrica están asociados al descubrimiento y explotación de la radiación electromagnética, que es energía radial con forma de ondas invisibles que se propagan por el espacio y la materia. La radiación es óptimamente utilizada para transmisiones electrónicas (u otros usos), dentro del espectro radioeléctrico en diferentes longitudes e intensidad. Por ello, el espectro se ha dividido en nueve bandas y en diferentes longitudes e intensidad. Cada banda cubre una década de frecuencia, o sea el número de ondas radiadas que pasan por cierto punto en determinado tiempo (estos son los Hertz). La longitud de onda del espectro útil abarca de los tres mil metros a un milímetro en ruta descendente.

Las microondas son ondas de radio generadas a frecuencias muy altas a través de un tubo oscilador llamado magnetrón. A diferencia de la longitud de 3,200 metros que alcanzan las ondas en la frecuencias bajas del espectro, las microondas obtienen longitudes que van de los 100 centímetros a un milímetro. Además de usarse en la radiodifusión, radiotelegrafía, televisión, satélites, tienen aplicaciones en intervenciones quirúrgicas, laboratorios de física, hornos de uso industrial y doméstico, combaten plagas, etcétera.

La emisión de microondas para telecomunicaciones se realiza a través de torres transmisoras, instaladas en línea visual en puntos elevados a distancias entre 30 y 50 kilómetros; se enfocan en haces direccionales, pueden reflejarse en aviones, naves marítimas, patrullas de policía, carros de bomberos y otros objetos. Utilizan repetidoras para reforzar las señales periódicamente. Comúnmente se emplean dos y cuatro antenas en cada estación para recepción y retransmisión.

El uso de las microondas ha sido históricamente controvertido. No obstante que su localización en el espacio atmosférico impide su apropiación física, la sobreexplotación y saturación de las bandas de transmisión es un problema siempre presente.

Para prever la explotación irracional del espectro y el uso indiscriminado de equipo, se han establecido normas técnicas internacionales para controlar el uso de frecuencias y artefactos por los particulares. Aunque estas reglas tienen como objetivo evitar el caos en el uso de las microondas, su violación es un problema latente, sobre todo por aquellas empresas o gobiernos que tienen capacidad tecnológica y poder suficiente para dominar en un momento determinado el espectro radioeléctrico, traspasando incluso las fronteras nacionales sin autorización de los gobiernos. Tal es el caso del equipo que emplea el proyecto T.V. Martí de Estados Unidos que envía desde 1990 sonido e imagen a la televisión cubana, aún cuando el gobierno de este país no admite dichas transmisiones.

En épocas de guerra las microondas son cruciales por la alta capacidad transmisiva y por la ventaja de no tener que emplear cables conductores. En la primera guerra mundial se usó el radioteléfono trasatlántico para las comunicaciones con los barcos navieros y mercantes, después que los cables que unían a Alemania y Gran Bretaña fueron cortados al estallar el conflicto en 1914. Durante la segunda guerra mundial, la tecnología de microondas sirvió de base para el radar. Las primeras instalaciones del radar eran limitadas y poco confiables; conforme los militares exigieron mejor definición y certeza hacia el final de las hostilidades, los tecnólogos fabricaron equipo que permitía blancos precisos, usando las partes más altas del espectro.

Durante la guerra del Golfo Pérsico en 1991, el espectro radial sirvió de cauce para controlar, mediante computadoras enlazadas a satélites, poderosos artefactos de guerra como los misiles teledirigidos. Los aliados emplearon redes de satélites para vigilar las comunicaciones y movimientos de las fuerzas iraquíes, para localizar a los aviadores derribados en el desierto, así como para orientar a sus aviones, barcos y fuerzas de tierra. Los alcances de los satélites espías dejan pasmado a cualquier persona: se especula que el Big Bird del Pentágono estadounidense leía los titulares del diario ruso Pravda y los números de placas de los automóviles en la Plaza Roja, cuando aquello era una fortaleza.

Las microondas también son el medio para que a través de los satélites artificiales, y no precisamente en épocas de guerra, se tenga acceso a información sobre cuestiones como instalaciones y posesión de armamentos, espionaje, investigación de la tierra e interacción educativa a distancia.

La irrefrenable explosión tecnológica para el aprovechamiento del espectro electromagnético ha alcanzado tal magnitud que vivimos diariamente en un mar lleno de energías anormales producidas por infinidad de aparatos electrónicos: relojes digitales, cables de alta tensión, televisores, teléfonos celulares, portones automáticos, hornos de microondas, cámaras de circuito cerrado. Las consecuencias de esto aún están por conocerse. Algunos experimentos han mostrado que pueden impactar negativamente en la salud pública. Ya se han detectado algunos casos de enfermedades provocadas por radiaciones tolerables. En España, se descubrió que los embriones de pollos durante la formación de su sistema nervioso y corazón no se desarrollaron completamente después de

ser expuestos brevemente a un campo electromagnético muy similar al generado por terminales de video. Estos y otros fenómenos anormales detectados en relación directa con el uso de radiaciones de intensidad variable debieran ser ya motivo de serias investigaciones. En breve tendremos que solicitar que, así como se monitorea el aire de las grandes urbes para registrar los niveles de partículas contaminantes que flotan en el aire, también se monitoreen los niveles de radiación en zonas de alta densidad de transmisiones inalámbricas.

Las microondas son el soporte de dos de las formas de transmisión de mayor éxito en la actualidad: las comunicaciones vía satélite y la radiotelefonía móvil celular, que a su vez han evolucionado hacia las redes de comunicación personales, cuya base técnica primordial es la no supeditación a redes de cable inmóviles.

### **3.4 Visión Histórica de la Comunicación Satelital**

El afán por ampliar las comunicaciones y abarcar todos los rincones de la tierra, ha conducido a los científicos a buscar medios cada vez más complejos para lograrlo. La exploración terrestre y atmosférica no ha sido suficiente. El objetivo de ir más arriba, a 36 mil kilómetros de altura sobre el nivel del mar se ha cumplido. Allí la ubicación es idónea para que los satélites artificiales logren, con unos cuantos artefactos, llevar comunicaciones e información a todos los puntos de la tierra.

Las redes satelitales se componen por una serie de estaciones terrenas conectadas entre sí por medio de satélites colocados en una órbita espacial que retransmisten señales por microondas a través del espacio atmosférico. El equipo instalado dentro de un satélite recibe las señales enviadas desde una estación terrestre, las amplifica y transmite a otra estación terrestre que las distribuye por pares de cables, cables coaxiales, guías de onda, fibras ópticas y sistemas de repetición de microondas.

La transmisión espacial fue concebida con más de diez años de anticipación al lanzamiento de los primeros satélites artificiales. En 1945 el científico inglés Arthur C. Clarke propuso el uso de un satélite terrestre para radiocomunicación entre varios puntos de la superficie terrestre. Clarke sugirió en una publicación el diseño de una nave espacial tripulada que podría lanzarse como un cohete. La nave se posicionaría a una altitud aproximada de 35,900 kilómetros, giraría junto con la tierra (sería síncrono) y habría receptores y equipo de transmisión terrestres que llevarían las señales a una determinada parte de la tierra. Fue tal el acierto del científico inglés que su mecanismo es en esencia el mismo con el que funcionan los sistemas satelitales geosíncronos de la actualidad. En su memoria, la órbita geoestacionaria se conoce también como Cinturón de Clarke.

El lanzamiento de los satélites artificiales inició el cuatro de octubre de 1957, cuando la Unión Soviética envió al espacio el Sputnik I, con el objeto de realizar experimentos biológicos; pesaba 80 kilogramos y gravitó alrededor de la tierra hasta el cuatro de enero de 1958. Inmediatamente el Congreso Norteamericano aprobó el otorgamiento de fondos para proyectos satelitales, y al año siguiente ese país lanzó el Explorer I, de 14 kilogramos de peso, que permaneció en órbita cinco años.

La generación de satélites comerciales para comunicaciones empezó en 1965 con el lanzamiento del satélite "El pájaro madrugador" (Intelsat I), que medía sólo 71 por 58 centímetros, pesaba 39 kilogramos y tenía capacidad para manejar 250 llamadas telefónicas internacionales. Este sería el primero de una serie de doce propiedad de Intelsat.

La fuerte demanda de servicios satelitales, han propiciado la multiplicación de satélites a tal grado que la órbita espacial sobre el ecuador, donde se estacionan, está casi saturada. Muy pronto diferentes países empezaron a lanzar satélites, a través de empresas privadas o los propios gobiernos. Canadá fue el tercero en disponer satélites para comunicaciones, pero únicamente a nivel nacional. En 1972 puso en servicio el primero de cinco generaciones llamados Anik. Entre otros países que cuentan con sistemas de satélites domésticos están: Brasil, Francia, Rusia, India, Japón, China, Australia, Gran Bretaña, Italia, Panamá, México y Argentina.

Los satélites artificiales cubrieron regiones donde la comunicación por redes terrestres es prácticamente imposible, o sumamente costosa. Se vencieron las barreras físicas que aislaban zonas enteras de los cinco continentes, como desiertos, montañas, océanos, selvas y polos glaciares. Se incorporaron a las comunicaciones localidades de Asia, Africa y América que de haberse esperado a tender redes alámbricas no tuviesen, aún a la fecha, acceso a circuitos de canales para telefonía, telegrafía y televisión.

La ventajas de utilizar satélites de comunicaciones radica en que eluden las barreras naturales, permiten planear su uso a requerimientos reales, acortan los tiempos de instalación y complementan las redes terrestres para transmisiones internacionales, posibilitando el cubrimiento total de la tierra. Con ellos se pueden establecer transmisiones con equipo móvil desde puntos geográficos donde no existe infraestructura para telecomunicaciones.

Los satélites son insensibles a las distancias. Todos los enlaces se hacen aproximadamente a 71,800 kilómetros (satélites geosíncronos) donde quiera que se ubiquen los artefactos emisores y receptores. Se necesitan unas cuantas estaciones terrestres movibles de acuerdo a las necesidades, y la señal las sigue. Es común ver que cuando ocurre un acontecimiento relevante en cualquier parte del mundo, inmediatamente se desplazan plataformas móviles llevando antenas parabólicas y equipo de transmisión, que envían señales para televisión de determinado fenómeno en vivo a todos los rincones de la tierra.

Algunas desventajas en las transmisiones satelitales es que están sujetas a demoras de propagación, se debilitan con las lluvias intensas, nieve y manchas solares que afectan a las estaciones terrestres, también sufren interferencias de radio, microondas y aeropuertos. Además los costos de fabricación y lanzamiento son muy elevados. Los ahorros de costos una vez que están en órbita, son máximos cuando la distancia entre los puntos excede a 1,800 kilómetros comparados con los de microondas y los 190 kilómetros con los de fibras ópticas.

Los satélites pueden ser ubicados a distintas distancias de la tierra y a velocidades diferentes de la de rotación, lo que permite coberturas locales, regionales y globales. De

acuerdo a estos requerimientos se han desarrollado diferentes generaciones de satélites de comunicaciones. A continuación veamos los más conocidos.

Los satélites de órbita elíptica (high earth orbit, HEO), fueron los primeros satélites diseñados especialmente para comunicaciones. Se desplazan a diferente velocidad de la tierra, y se alejan y acercan a ella en diferentes momentos. Tardan 12 horas en completar una revolución y ofrecen mejores condiciones de uso en las telecomunicaciones cuando su altitud es de 40 mil kilómetros.

Los satélites geoestacionarios (geosynchronous earth orbit, GEO) se ubican sobre el ecuador a 36 mil kilómetros de la tierra y viajan a su misma velocidad (de ahí su nombre de síncronos), por lo que parecen estar estacionados o inmóviles y completan su recorrido en 24 horas. Tienen una área de cobertura aproximada de ocho mil kilómetros que proporciona una capacidad visual hasta de una tercera parte de la tierra. Tres satélites de este tipo, colocados en forma equidistante, pueden transmitir instantáneamente señales de radio o televisión a casi el área completa de la tierra. Son los más utilizados para servicios de transmisión de datos, señales de televisión y telefonía, requieren de grandes estaciones terrenas fijas, pero también sirven para comunicaciones con unidades móviles como las de navegación aérea, marítima y terrestre. La órbita geoestacionaria es la más congestionada ya que en ella están colocados no nada más satélites para comunicaciones, sino otros de aplicaciones diversas como meteorológicos, experimentales y militares.

Otra generación de satélites son los de órbita terrestre baja (low earth orbit, LEO). Estos han provocado serias controversias sobre todo con los consorcios y países que tienen satélites GEO para comunicaciones, pues aducen que sus objetivos no están bien definidos y entrarán a hacerles una fuerte competencia sobre todo por los bajos costos que están manejando en comparación con los GEO.

Los LEO se ubican a una altitud entre 900 y 1300 kilómetros y son no geoestacionarios, o sea, registran una velocidad distinta a la de rotación de la tierra. Su área de cobertura terrestre es de un radio promedio de 5,500 kilómetros, por lo que tienen que colocarse muchos microsátélites con trayectorias diferentes para brindar cobertura local, regional y mundial. Dado que los satélites LEO, (que admiten en frecuencias inferiores a un gigahertz), necesitan estaciones terrenas sencillas, terminales portátiles, así como antenas y fuentes de poder reducidas, (a diferencia de los geoestacionarios que requieren infraestructura terrena pesada), permiten una gran flexibilidad en su uso, pues pueden aprovecharse varias decenas de microsátélites de acuerdo a las necesidades de cobertura o servicio.

Estos satélites se encuentran en vías de experimentación. Aunque pueden utilizarse en zonas que ya cuentan con comunicaciones desarrolladas, por la facilidad de transportación de las antenas receptoras, son aprovechables también en zonas que carezcan por completo de sistemas de telecomunicaciones. Han despertado gran interés en diferentes empresas que ven la posibilidad de usarlos para redes de telecomunicaciones y brindar servicios de información inalámbricos no nada más a grandes consorcios sino a usuarios particulares (para viajes de negocios o placer, operadores de botes, ingenieros y médicos que trabajan en áreas remotas). Otros creen que podrán solucionar problemas de comunicación en áreas

rurales con servicios deprimidos, en zonas cuya ubicación está a dos horas de donde existe teléfono, donde vive aproximadamente la mitad de la población mundial.

Los proyectos LEO, encabezados por consorcios norteamericanos, se iniciaron incluso antes de que el Congreso de ese país asignara frecuencias en mayo de 1994. Veamos cuales son esos proyectos:

- Proyecto 21: Es propiedad de Inmarsat y parte de la cuarta generación de satélites de este organismo. Su costo es de más de un mil millones de dólares.
- Iridium: Son una constelación de 66 satélites. Su diseño incluye líneas intersatélite y el costo es de 3.4 mil millones de dólares. Son propiedad del consorcio formado por 18 empresas de diferentes países encabezados por Motorola. (Fig. 1.6)
- Globalstar: Se compondrá de 24 a 48 satélites con cobertura global y en Estados Unidos. Está diseñado con código de acceso por división múltiple (CDMA code division multiple acces) y con un costo de 1.8 mil millones de dólares. (Fig. 1.9)
- Odyssey: Es una constelación de 12 satélites que orbitarán en tres planos. Su costo es de 1.3 mil millones de dólares y es propiedad de TRW, Inc. un consorcio de manufacturación de tecnología aeroespacial.
- Elipso I y II: Comprende de 6 a 18 satélites en dos planos para proveer servicio nacional solamente. Su costo son 180 millones de dólares y son propiedad de 6 compañías norteamericanas de comunicaciones móviles, manufactureras de electrónica y tecnología inalámbrica y del banco inglés Barclays.
- Aries: Son 48 satélites de órbita polar en cuatro planos. Su costo es de 292 millones de dólares y es propiedad de inversionistas privados y empresas de comunicaciones de Estados Unidos.
- Teledesic. Son 840 satélites del tamaño de un refrigerador basados en el diseño de Strategic Defense Initiative. Su costo es de 9 mil millones de dólares y es propiedad de Craig McCaw, William Gates, McCaw Development y Kinship Partners.

La participación de grandes consorcios multinacionales de telecomunicaciones, junto con grupos financieros, manufactureros electrónicos y de cohetes, entre otros, refleja el alto grado de mercantilización de los satélites, que inicialmente fueron concebidos para solventar necesidades básicas de comunicaciones.

De acuerdo a la cobertura que tienen en tierra, existen tres sistemas de satélites para comunicaciones: 1. Internacionales: Intelsat, Intersputnik, Inmarsat; 2. Regionales: Eutelsat que cubre a los países europeos, Arabsat a países árabes, Panamsat a países americanos; 3: Nacionales: Telesat de Canadá, Telecom de Francia, Satcom, Comstar, Westar, SBS, Gstar de Estados Unidos, Palapa de Indonesia, Molnya-3, Statsionar, Loutch de Rusia, Sakura,

CS y Ayame de Japón, Radugae e Insat de India, Morelos y Solidaridad de México y Nahuel de Argentina, entre otros.

Además de los satélites para comunicaciones, existe otra amplia gama de satélites con diferentes objetivos, entre ellos: meteorológicos, de exploración marina, oceanográfica, terrestre, del espacio, astronómica, con misiones biológicas y médicas. Aproximadamente cinco mil se encuentran en órbita, de los cuales 175 ocupan la órbita geoestacionaria para servicios comerciales y uso doméstico.

México cuenta con un sistema de satélites para comunicaciones desde 1985. El Morelos I entró en órbita en junio de 1985 y el Morelos II en noviembre de 1989. El primero fue reemplazado en 1994 por el Solidaridad I y en ese mismo año se lanzó el Solidaridad II. El Morelos II saldrá de órbita en 1998. A partir de 1994, con el lanzamiento de los Solidaridad, el sistema tendrá una cobertura más amplia que el Morelos. Está programado para enviar más de 50 mil llamadas telefónicas simultáneamente, o más de 50 canales de televisión y datos a altas velocidades; permitirá la comunicación con unidades del autotransporte de carga y pasaje durante su tránsito por las carreteras, así como para las embarcaciones de cabotaje que navegan por los litorales mexicanos. Se prestarán servicios a los países del Caribe centroamericano, Venezuela, Colombia, Ecuador, Perú y diferentes ciudades de Estados Unidos como Los Angeles, San Francisco, Houston, Dallas, Chicago, Nueva York, Washington, Miami, Tampa e incluso a Toronto, Canadá. Enviará también señales especiales a Buenos Aires, Montevideo y Santiago de Chile. Con el Morelos II y el Solidaridad se cubrirá la demanda de señales de México y esas regiones hasta el año 2006.

Indudablemente el sistema satelital con más alcance, aunque muy cuestionado por operar como monopolio estadounidense, es Intelsat. Se fundó en agosto de 1964 como una empresa de riesgo. Su creación se previó en la Ley de Satélites de Comunicaciones de 1962 de Estados Unidos, que ordenó el establecimiento de un sistema de comunicaciones por satélite comercial, pero no prescribió claramente los asuntos para las comunicaciones nacionales.

Para la fundación de Intelsat firmaron únicamente once países; inició con el lanzamiento del Early Bird pero fue tal la aceptación que para 1980 ya poseía cerca de 400 estaciones terrestres con 12 satélites. En 1987 Intelsat contaba con 113 países signantes, 17 satélites que unían a aproximadamente 170 países, distintos territorios y corporaciones alrededor del mundo a través de 739 estaciones terrestres.

Las principales normas que lo rigen son: Intelsat es dueño de los satélites y del segmento espacial de frecuencias y las estaciones terrenas son propiedad de cada uno de los países; los estados miembros se comprometen a utilizar los satélites de Intelsat para comunicación con el extranjero; los países tienen, en Comsat (el órgano administrador), un número de votos proporcional al porcentaje del capital total invertido en los servicios de satélites.

Con base en la Ley de Comunicaciones por Satélites de 1962, el Congreso de Estados Unidos creó Comsat y se adjudicó, a ese país, el monopolio de las comunicaciones internacionales por satélite. Fue creada como corporación privada, con un propósito nacional. Su estructura fue resultado de un fuerte debate congresional y público alrededor

de la Ley de Comunicaciones por Satélite. Hubo dos posiciones contrarias para que se formara como empresa pública o como empresa privada. Finalmente resultó un híbrido público-privado. Comsat funge como intermediario entre consorcios norteamericanos de comunicación (American Telephone and Telegraph -AT&T-, General Telephone and Electronics -GTE-, Radio Corporation of America -RCA-) y el gobierno de Estados Unidos, es responsable del diseño, desarrollo y mantenimiento del segmento espacial del sistema global de telecomunicaciones.

### **3.5 Génesis de Una Idea**

Existe un viejo adagio que dice que el éxito tiene muchos padres, pero el fracaso es un huérfano. El desarrollo de la tecnología es caprichoso, el potencial para un infinito número de cosas está presente, aún las más amplias decisiones humanas determinan como se desenvolverá la tecnología para los años venideros. En el desarrollo tecnológico no existe la claridad, no existe el libro de texto perfecto o una progresión lógica y muy seguido los desarrollos adelantados al tiempo no se reconocen hasta después de muchos años incluso, si es que se reconocen. Así es como ha pasado con el RFID.

Un trabajo pionero, si no el primero, explorando RFID es "*Communication by Means of Reflected Power*" de Harry Stockman el cual constituye un hito y citamos un renglón del mismo pp1196-1204, octubre 1948, Stockman declaró entonces que "Evidentemente, un trabajo considerable de investigación y desarrollo tiene que ser hecho antes de que los remanentes de problemas básicos en cuanto a comunicación con potencia reflejada se solventaran, y antes de que el campo de aplicación útil sea explorado".

Treinta años debieron pasar antes de que la visión de Harry empezará a rendir frutos, otros desarrollos se necesitaron: el transistor, el circuito integrado, el microprocesador, el desarrollo de las redes de comunicación y que cambiara la manera de hacer negocios. Lo anterior una tarea nada fácil, como en muchos aspectos el tiempo lo decide todo y el éxito del RFID debe esperar aún un poco más.

Mucho ha pasado en los 53 años subsecuentes desde el trabajo de Harry S., los 50's fueron una época de exploración de las técnicas RFID siguiendo a los desarrollos técnicos en radio y radar llevados a cabo en los 30's y 40's. Diferentes tecnologías relacionadas al RFID han sido exploradas como por ejemplo sistemas de transponder de largo alcance de identificación "identification friend or foe" (IFF) para aeronaves. Los desarrollos en los 50's incluyen trabajos tales como "*Application of the Microwave Homodyne*" de F.L. Vernon, y el trabajo de D.B. Harris "*Radio Transmisi3n Systems with Modulatable Passive Transponder*". Las ruedas del desarrollo de RFID est3n rodando nuevamente.

### **3.6 De los a3os 60's a los 80's: RFID se vuelve una realidad**

Los 60's fueron el preludio para la explosi3n en los 70's, R.F. Harrington estudi3 la teor3a electromagn3tica relacionada con el RFID en sus publicaciones "*Field Measurements Using Active Scatterers*" y "*Theory of Loaded Scatterers*" en el periodo 1963-1964. Los inventores estuvieron muy ocupados en cuanto a temas relacionados al RFID como por ejemplo los siguientes trabajos: de Robert Richardson "*Remotely Activated Radio*

*Frequency Powered Devices*” en el año de 1963, también el trabajo de Otto Rittenback “*Communication by Radar Beams*” en 1969, J.H. Vogelmann’s “*Passive Data Transmission Techniques Utilizing Radar Beams*” en 1968 y “*Interrogator-Responder Identification System*” de J.P. Vinding en 1967.

Las actividades comerciales empezaron en los 60’s. Sensormatic y Checkpoint se fundaron a finales de aquella década, estas compañías junto con otras como Knogo, desarrollaron el equipamiento de *supervisión electrónica de artículo* (EAS) para el control contra robo. Todos los tipos anteriores de sistemas usualmente utilizaban etiquetas de “1 bit” (sólo la presencia o ausencia de una etiqueta se podía detectar), pero estas etiquetas eran económicamente atractivas y además proveían de efectividad en cuanto a medidas antirrobo, estas últimas utilizaban tanto tecnología inductiva o incluso microondas. EAS es tal vez el primero y el más popular uso comercial de RFID.

En los años 70’s los desarrolladores, inventores compañías, instituciones académicas y laboratorios del gobierno estuvieron activamente trabajando en el RFID, de esta forma notables avances se fueron haciendo en los laboratorios de investigación y en instituciones académicas como en el laboratorio científico *Los Alamos*, la universidad *Northwestern* y el *Microwave Institute Foundation* en Suecia entre otros. Un temprano e importante desarrollo fue el trabajo del laboratorio Los Alamos que fue presentado por Alfred Koelle, Steven Depp y Robert Freyman y que tuvo por título “*Short-Range Radio-Telemetry for electronic Identification Using Modulated Backscatter*” en 1975.

Grandes compañías estuvieron también desarrollando la tecnología RFID, como la popular Raytheon con “Raytag” en el año de 1973. RCA y Fairchild estuvieron muy activos en sus esfuerzos para desarrollar un “Sistema de Identificación Electrónica” con Richard Klensch de RCA encabezando en 1975 y posteriormente F. Sterzer de RCA desarrollando una “Licencia Electrónica de Plataforma para Vehículos Motorizados” en 1977. Thomas Meyers y Ashley Leigh de Fairchild también desarrollaron un “Transponder de Codificación Pasiva de Microondas”.

La autoridad portuaria de Nueva York y Nueva Jersey estuvo también probando sistemas construidos por General Electric, Westinghouse, Philips y Glenayre, los resultados fueron favorables, pero la primer aplicación exitosa al transporte de RFID, nos referimos a la aplicación de colección de peaje electrónico, no estuvo lista aún para el día de su presentación.

Los 70’s estuvieron caracterizados principalmente por el desarrollo experimental, las aplicaciones en mente eran las de rastreo de mascotas, rastreo de vehículos y automatización industrial. Algunos ejemplos de los esfuerzos en el etiquetamiento animal fueron los sistemas de microondas en Los Alamos y los sistemas inductivos en Europa. El interés en el etiquetamiento animal resultó muy fuerte en Europa. Compañías como Alfa, Laval, Nedap y otras estuvieron desarrollando sistemas RFID en ese periodo.

Los esfuerzos en cuanto a aplicaciones al transporte incluyeron los trabajos en Los Alamos y también los trabajos del *International Bridge Turnpike and Tunnel Association* (IBTTA) y el *United States Federal Highway Administration* que básicamente son organismos

administradores de carreteras, autopistas y puentes en los Estados Unidos, los últimos patrocinaron una conferencia en 1973 el cual concluyo sin atraer ningún interés nacional en el desarrollo de un estándar para la identificación electrónica de vehículos. Esta era una importante decisión en el sentido que podría permitir una variedad de sistemas a desarrollar lo cual sería por supuesto muy bueno ya que la tecnología RFID estaba en su infancia.

Alrededor de esta época, nuevas compañías empezaron a tocar este tópico, una de ellas Identronix, una extensión del Laboratorio de Los Alamos y otras del equipo de Los Alamos, Amtech fue fundado (después adquirido por Intermecc y actualmente vendido a TransCore) en los 80's. Por ahora el número de compañías individuos e instituciones que trabajan en RFID se multiplica, un signo positivo, el potencial de RFID se volvió obvio.

Los 80s vinieron a ser la década de una implementación completa del RFID, aunque los desarrollos se dieron a final de cuentas de diferentes maneras en diferentes partes el mundo. El gran interés en los Estados Unidos fue en cuanto a transportación, acceso de personal y un poco menos extendido para los animales. En Europa en cambio, el mayor interés fue el de sistemas de corto alcance para animales, el área industrial y de negocios, como herramienta se equiparon los caminos en Italia, Francia, España, Portugal y Noruega con tecnología RFID.

En Norteamérica, la Asociación de Ferrocarriles Americana y el Programa Cooperativo del Manejo de Contenedores fueron entidades activas con en cuanto a iniciativas RFID. Pruebas de RFID para el cargo de peajes se han estado llevando a cabo durante muchos años y la primer aplicación comercial empezó en Europa en el año de 1987 específicamente en Noruega y fue seguida rápidamente en los Estados unidos por el Dallas North Turnpike en 1989. Además durante este tiempo, la autoridad portuaria de Nueva Cork y Nueva Jersey comenzaron la operación comercial de RFID para los autobuses que atraviesan el túnel Lincoln. RFID encontró un hogar en el cargo de peajes electrónico y nuevamente el interés crecía a diario.

### **3.7 La Década de los 90**

Los 90's fueron una década de gran significancia para el RFID ya que se vio el despliegue y crecimiento a gran escala de la colecta electrónica de peaje en los Estados Unidos. Para empezar se dio continuidad a algunas importantes aplicaciones incluyendo diferentes innovaciones en cuanto a el cargo electrónico de peaje. El primer sistema de carretera abierto para el cargo de peaje abrió en Oklahoma en el año de 1991, constaba de vehículos que pasaban los puntos de colecta de peaje en las autopistas sin la necesidad de hacer las filas en las casetas o barreras reductoras y con videocámaras además para reforzar la seguridad. El primer sistema combinado de colecta de peaje y administración de tráfico se instaló en el área de Houston por la Autoridad Estatal de Caminos de Cuota Harris en 1992. También otro pionero fue el sistema instalado en la autopista Kansas usando un sistema basado en el Título 21 del estándar con lectores que además podían operar con las etiquetas del vecino del sur, Oklahoma. Para continuar seguiría el Georgia 400 que actualizó su equipamiento con lectores que podían comunicar con las novedosas etiquetas Título 21 de la misma forma que las etiquetas existentes. En realidad, las últimas dos que mencionamos

fueron las primeras en implementar una capacidad multiprotocolo en cuanto a las aplicaciones de peaje electrónico.

En el Noreste de Estados Unidos, siete agencias regionales de peajes formaron el E-Z Pass Interagency Group (IAG) en el año de 1990 para desarrollar un sistema de peaje electrónico regional compatible, el sistema anterior es el modelo del uso de una etiqueta sencilla y una cuenta sencilla por vehículo para acceder a las autopistas de diferentes autoridades en cuanto a peaje (estatales).

El interés también fue muy persistente para las aplicaciones RFID en Europa durante la década de los noventa, tanto tecnologías de microondas e inductivas para RFID encontraron un uso para el cargo de peaje electrónico, control de acceso y una amplia variedad de otras aplicaciones en el comercio.

Un nuevo esfuerzo que se hizo fue el desarrollo de Texas Instruments (TI) TIRIS system, usado en los automóviles para el control del motor de marcha del vehículo. El sistema TIRIS (y otros como el de Mikron, ahora parte de Philips) desarrolló nuevas aplicaciones para el abasto de combustible, chips de juegos, pases de esquí, acceso de vehículos, y muchas otras aplicaciones.

Adicionalmente algunas compañías en Europa se volvieron muy activas en la carrera RFID como por ejemplo los desarrollos alcanzados por Microdesign, CGA, Alcatel, Bosch y Philips Combitech, P. Baumer y P. Tagmaster. Un estándar Pan Europeo se necesitó para las aplicaciones de peaje electrónico en Europa y muchas de estas compañías (y otras) estuvieron trabajando en el estándar CEN para peaje electrónico.

Las aplicaciones de peaje y ferrocarriles también aparecieron en muchos países incluyendo Australia, China, Hong Kong, Filipinas, Argentina, Brasil, México, Canadá, Japón, Malasia, Singapur, Tailandia, Corea del Sur, Sudáfrica y Europa por supuesto.

Con el éxito del cargo electrónico de peajes, otros avances se dieron como por ejemplo el primer uso múltiple de etiquetas a través de diferentes segmentos de negocios (ámbitos). Ahora una etiqueta sencilla (con cargo de cuenta dual o sencillo) se podía usar para el cargo electrónico de peajes, acceso a estacionamientos y pago de tarifas, acceso a comunidades exclusivas y acceso a campus universitarios por ejemplo. En el Dallas Ft. Worth metroplex, un primer logro se dio cuando una etiqueta sencilla de peaje, TollTag® en un vehículo, se pudo usar para el cargo de peaje en la autopista de peaje del norte de Dallas, acceso a estacionamientos y pago de tarifas en el aeropuerto internacional Ft. Worth en Dallas (uno de los aeropuertos de mas demanda mundial), el cercano Love Field y muchos estacionamientos en el centro de la ciudad así como el acceso a comunidades exclusivas y centros corporativos.

La investigación y el desarrollo no fue lento durante los 90's, una vez que nuevos desarrollos tecnológicos pudieron expandir la funcionalidad de RFID. Por primera vez los útiles diodos Schottky de microondas se fabricaron en un circuito integrado regular con tecnología CMOS, todo este desarrollo permitió la construcción de etiquetas RFID de microondas que contenían solo un circuito integrado, una capacidad anteriormente limitada a los transponders de acople inductivo RFID. Las compañías activas en esta empresa fueron

IBM (la tecnología después adquirida por Intermec) Micron, y Sistemas de Chip Sencillos (SCS). La tabla 3.1 resume algo de lo que acabamos de describir.

Década	Evento
1940-1950	<ul style="list-style-type: none"> <li>• El radar se refino y se desplegó en la Segunda Guerra Mundial.</li> <li>• El RFID se inventó en 1948.</li> </ul>
1950-1960	<ul style="list-style-type: none"> <li>• Se dieron las primeras exploraciones del RFID y los experimentos de laboratorio.</li> </ul>
1960-1970	<ul style="list-style-type: none"> <li>• Se desarrolló la teoría del RFID.</li> <li>• Inicio de las aplicaciones (intentos de campo).</li> </ul>
1970-1980	<ul style="list-style-type: none"> <li>• Explosión del desarrollo RFID.</li> <li>• Las pruebas del RFID se aceleraron.</li> <li>• Adopciones en implementación muy tempranas del sistema RFID.</li> </ul>
1980-1990	<ul style="list-style-type: none"> <li>• Las aplicaciones comerciales del RFID se vuelven convencionales.</li> </ul>
1990-2000	<ul style="list-style-type: none"> <li>• Surgimiento de estándares.</li> <li>• Amplio despliegue de RFID.</li> <li>• RFID se vuelve una parte de la vida diaria.</li> </ul>

**Tabla 3.1 Las décadas del RFID**

Con el creciente interés del RFID en la aplicación de administración de artículos y la oportunidad de RFID de trabajar en conjunto con el código de barras, se torna difícil en la última parte de la década el contar el número de compañías que entran en este mercado, muchas han llegado y se han ido, muchas han llegado para quedarse, muchas han surgido y existen muchas opciones, diariamente existe una nueva actualización técnica, diariamente hay quienes adquieren esta tecnología, hay muchos jugadores en este juego.

### **3.8 La Actualidad del RFID**

La carrera de la identificación por radiofrecuencia (RFID) y métodos de rastreo esta iniciada ya que mucha de la tecnología de hoy , cadenas de abastecimiento y los líderes logísticos ven el RFID como la inversión de la década , incluso tal como lo fue el Internet en su momento, además el desarrollo en cuanto a estándares y competitividad en precios también se ha ido dando. En cuanto a iniciativas se refiere el líder es el Departamento de Defensa (DOD) y el gigante de los complejos comerciales Wal-Mart, ambos convencidos que el RFID en sus cadenas de abastecimiento internas y externas podría ahorrarles billones

de dólares. El DOD estadounidense usará tecnología RFID para volverse mas fluido y eficiente dentro de lo que son sus retos de logística para el despliegue de tropas, equipos y abastecimiento de una forma rápida a todos los lugares del planeta en tiempos de crisis.

Tanto el DOD como Wal-Mart han dado ordenes a sus principales proveedores de estar preparados para convertirse totalmente a la tecnología RFID por enero del 2005. estos mandatos dieron como resultado reacciones encontradas por parte de sus proveedores, quienes contemplaron que sus inversiones en esta tecnología y los recursos para cumplir con las iniciativas RFID son muy prematuras y que es muy improbable que puedan ofrecer económicamente una recuperación para ellos como proveedores.

Por otro lado, el empuje de el DOD y Wal-Mart ha generado un gran interés de parte del sector tecnológico. Muchos de los pesos pesados en cuanto a tecnología como IBM, Microsoft, Texas Instruments, Oracle, Cisco Systems y Alien Technologies junto con un conglomerado de compañías, a la cabeza en iniciativas, han tomado sus roles de compañerismo en el desarrollo, investigación y soporte de la tecnología RFID.

A principios de abril de 2004, el DOD anunció un acuerdo con IBM para consultar y colaborar en la tecnología RFID por los próximos tres años. Microsoft además recientemente formó su propio grupo RFID que estará proveyendo una plataforma en la cual sus socios pueden crear productos y servicios basados en RFID. Similarmente, Sears Logistics se ha asociado con IBM, Symbol Technologies y Zebra Technologies para el desarrollo de tecnologías RFID más avanzadas que serán orientadas hacia la planeación estratégica y soporte en entregas directas y sistemas logísticos.

Aunque la tecnología RFID está en sus primeras etapas (a pesar de que como hemos visto se viene dando desde hace ya algunos años) y con muchas barreras que superar como la estandarización y temas de eficiencia en costos, muchos de los sectores privados interesados están de acuerdo que los beneficios de RFID, una vez establecido, permitirá mayores mejoras a través de las cadenas de abastecimiento enteras y procesos logísticos. De hecho, Eric Michielsen, un analista destacado con investigación ABI y que es quién se encarga del mercado RFID dice al respecto que “la tecnología prevalecerá por mucho tiempo y cuando las piezas encajen juntas (y lo harán pronto) se dará la explosión”.

# ***CAPÍTULO 4***

## **BASES RFID**

4.1 Introducción .....	83
4.2 Radio Frequency Identification Devices (RFID) .....	84
4.3 La Interface Aérea y la Comunicación Inalámbrica .....	85
4.4 Las Frecuencias Portadoras.....	87
4.5 Tasa de Transferencia de Datos y Ancho de Banda.....	88, 89
4.6 Rango (alcance) y Niveles de Potencia.....	89
4.7 Transponders o Tags .....	91
4.7.1 Características Básicas de un Transponder RFID .....	91
4.7.1.1 Energizado de los Tags .....	93
4.7.1.2 Opciones de transporte de datos.....	96
4.7.1.3 Rango de lectura de datos .....	96
4.7.1.4 Opciones de programación de datos .....	97
4.7.1.5 Forma física .....	97
4.7.1.6 Costos.....	103
4.8 El Lector o Interrogador.....	104
4.9 Los Programadores de Transponder .....	104
4.10 Categorías en los sistemas RFID. ....	105
4.11 Estandarización. ....	106

## 4.1 Introducción

La aplicación, estandarización e innovación en la tecnología RFID se encuentran en constante cambio, en general la tecnología se está moviendo hacia las tendencias más convenientes para las grandes compañías que buscan una aplicación económica y eficiente a la vez. La adopción del RFID sigue siendo relativamente nueva aún, por lo que existen distintas características de la tecnología que no han sido del todo entendidas por el público en general. Los desarrollos en la tecnología RFID continúan y se dirigen hacia una mayor capacidad de almacenaje en memoria, más amplios rangos de lectura y un procesamiento más rápido.

No es del todo cierto que la tecnología RFID finalmente reemplazará a la codificación de barras, puesto que, incluso con el decremento inevitable en costo de los materiales semiconductores en crudo, ya que el circuito integrado en una etiqueta de radiofrecuencia nunca será tan económicamente efectivo como un etiquetamiento de código de barras, en donde solamente para algunos casos sólo se gasta en la tinta. De cualquier manera RFID continuará creciendo en los nichos que ha establecido hasta la fecha, en donde el código de barras u otras tecnologías ópticas no son efectivas. Si algunos de los estándares en pie se logran comunemente, de manera que el equipamiento RFID de diferentes fabricantes se pueda usar de forma intercambiable o genérica, el mercado probablemente crecerá exponencialmente.

Una analogía que tiene que ver con lo que hoy son las altas tasas de transferencia de datos que invaden el mundo de las redes y que relaciona lo que es la estandarización con la implementación y las antiguas técnicas con las nuevas, sería lo relativo a las tecnologías de acceso como DSL que hace uso de los métodos de transmisión digital en la línea portadora que generalmente existe entre una central local y la línea de abonado. El asunto es que las líneas existentes de cableado en par trenzado están ahí debido y como parte de la infraestructura gradualmente construida para soportar comunicación de voz, así que desde que este sistema se expandió lentamente a lo largo del siglo pasado, no es de sorprender que las necesidades de velocidad se han vuelto el principal criterio del diseño de estas redes. Esto ha ayudado a mejorar la calidad de servicios de voz sobre la red y permitió la comunicación interpersonal en una base global.

En referencia a lo anterior tenemos que las técnicas de comunicación están en constante cambio, primeramente para ser capaces de comunicar más rápido y sobre grandes distancias. Usar este sistema a lo largo de un siglo se puede considerar ahora mucho tiempo, de cualquier manera, sistemas previos finalizaron después de cientos, incluso miles de años. En la actualidad estamos enfrentados a ciclos decrecientes en tiempo, donde las necesidades de la red van a tener muy diferentes requerimientos. Esto no significa de cualquier forma que las viejas técnicas de comunicación simplemente desaparecerán. La gente aún sigue haciendo llamadas, escribiendo, telegrafando y usan el servicio telefónico convencional. Lo anterior es cierto también para la infraestructura que se pone a efecto para soportar estos servicios. No es económicamente (o, de alguna manera, política y socialmente) posible el echar fuera toda el viejo cableado y reemplazarlo con el método “en boga”, o reemplazar el viejo equipo con nuevo. Entonces las nuevas técnicas deben coexistir con las antiguas e influenciar la habilidad de hacer uso de las estructuras

existentes para soportar las nuevas, esto también es aplicable a las tecnologías como el RFID que no ha encontrado hasta la fecha un amplio campo para el despliegue de todo el potencial que involucra esta tecnología. Sin embargo es el propósito de este documento y bajo este contexto que examinaremos las principales características de un sistema RFID.

Por un momento uno piensa sobre las emisiones de radio comercial, o los teléfonos móviles y uno prontamente puede apreciar los beneficios de la comunicación inalámbrica. Haciendo también extensivos estos beneficios a la comunicación de datos, a y desde portadores de datos de bajo costo, y también se puede estar cerca de apreciar la naturaleza y potencial de la identificación por radiofrecuencia (RFID). RFID es un área de identificación automática que ha ganado momentum en años recientes y se ve ahora como una manera radical de mejorar los procesos de manejo de datos, complementario en muchos aspectos a otras tecnologías de captura de datos como el código de barras. Un rango de dispositivos y sistemas asociados están disponibles para satisfacer un siempre amplio rango de aplicaciones. A pesar de esta diversidad, los principios sobre los cuales se basa la tecnología son evidentes, incluso aunque la tecnología y sus tecnicismos en lo que concierne a la manera en la que la éstos operan es muy sofisticada, cabe decir que uno no necesita conocer éstos tecnicismos, tal como uno no necesita conocer los de un teléfono móvil o una PC para operarlos, no es necesario tampoco conocer los tecnicismos del RFID para saber los principios, consideraciones y el potencial para esta tecnología. De cualquier manera una apreciación técnica por más pequeña que ésta sea, puede dar una ventaja en la determinación de los requerimientos del sistema y en lo que se refiere a la consultoría y proveedores.

## **4.2 Radio Frequency Identification (RFID)**

El objetivo de cualquier sistema de identificación por radiofrecuencia es el de cargar datos en unos circuitos integrados convenientes para tal fin o “transponders”, también conocidos como etiquetas inteligentes<sup>1</sup>, además de portar los datos en un dispositivo de estas características, el sistema también debe ser capaz de recuperar esos datos por medio de máquinas de lectura, en un tiempo y lugar específicos para satisfacer las necesidades particulares de aplicación. Lo anterior de manera que los datos que se almacenan en las etiquetas puedan proveer información sobre casos especiales como en la producción de bienes, traslado de valores, una locación, la identidad de un vehículo, un animal o una persona, entre otras aplicaciones. Si se incluyen datos adicionales, la prospección se torna hacia el soporte de aplicaciones en las que se necesita información específica o instrucciones que estarían disponibles inmediatamente a la hora de la lectura de la etiqueta, ejemplos de lo anterior podrían ser instrucciones acerca del color de la pintura de un automóvil en la línea de producción cuando entra en un área de pintado con spray, las instrucciones de configuración para una célula de manufactura flexible, o en el rastreo de un embarque de bienes.

---

<sup>1</sup> A partir de este momento utilizaremos indiferentemente para mencionar estas etiquetas los términos: transponder RFID, chip inteligente, tag...etc. De forma estricta las “Etiquetas Inteligentes” son etiquetas con dispositivos RFID ultra delgados que son llamados comúnmente “inlays”.

El sistema también requiere en adición a las propias etiquetas algo que tenga que ver con la lectura o interrogación de las mismas y algo que haga las veces de comunicación de los datos a un host o un sistema de administración de información. También incluirá alguna facilidad para ingresar o programar información o datos en la etiqueta, si es que esto no ha sido proporcionado por el fabricante. A veces la antena en estos dispositivos se mira como una cuestión aparte (o como si lo fuere) de un sistema RFID, sin embargo su importancia radica en que se debe ver como una característica que no puede faltar en todo sistema de esta tipo, ya que está presente tanto en lectores como en las etiquetas, es esencial para la comunicación entre ambos.

El RFID utiliza señales de radio de baja potencia para intercambiar datos sin la necesidad de hacer interconexiones (físicas) entre los chips y los lectores, no se necesita una línea de vista entre la etiqueta y el dispositivo de lectura/escritura, eliminando así mucho de la orientación de otro tipo de sistemas hacia la presentación del artículo en las otras formas de colecta de datos automatizada. Los lectores RFID a su vez, son capaces de reconocer y procesar simultáneamente cientos de etiquetas con sus respectivos campos de lectura.

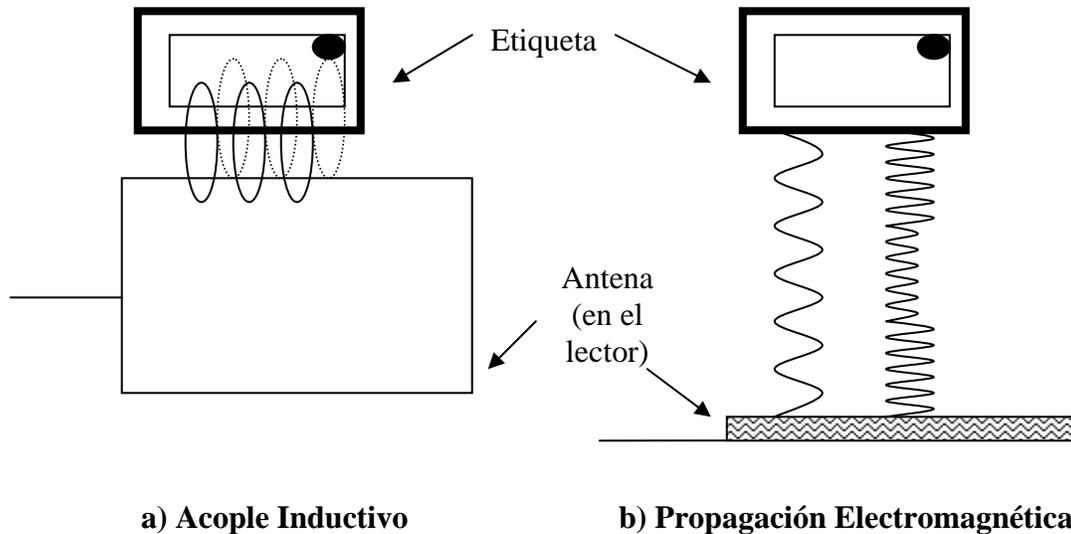
Para entender y apreciar las capacidades de los sistemas RFID, es necesario considerar las partes que constituyen el sistema. También será necesario el considerar los requerimientos de flujo de datos que influyen y determinan en algunos casos la elección de sistemas y las practicidades de la comunicación a través del espacio o interface aérea, si se consideran los componentes del sistema y su función junto con la cadena de datos de flujo es posible el considerar a muchos de los temas importantes que influyen en la aplicación directa del RFID. De cualquier manera es muy conveniente el empezar considerando brevemente la manera en la cual la comunicación inalámbrica se logra, así como las técnicas involucradas que tienen un impacto importante desde el diseño de los propios componentes.

### **4.3 La Interface Aérea y la Comunicación Inalámbrica**

La comunicación de datos entre las etiquetas y un lector es por comunicación inalámbrica. Dos métodos son los que distinguen y categorizan principalmente a los sistemas RFID, uno basado en la proximidad electromagnética o acople inductivo y el otro se basa en la propagación de ondas electromagnéticas. El acople se hace vía estructuras de “antena” que conforman una característica integral, tanto en los lectores como en las etiquetas, debemos mencionar que el término antena es generalmente considerado más apropiado para los sistemas de propagación no obstante también es aplicado a los sistemas inductivos. En la figura 4.1 se puede ver bosquejada la idea anterior.

La transmisión de datos esta sujeta a los caprichos e influencias del medio o canal a través del cual los datos fluyen, incluyendo por supuesto la interface aérea. El ruido, la interferencia y la distorsión son las fuentes de corrupción de datos que se debe tomar en cuenta y que deben considerarse con la necesidad de canales de comunicación fiables que deben proteger contra estos efectos en la búsqueda de lograr una recuperación de datos libre de errores, ya que primordialmente lo que se maneja en este tipo de sistemas es una

capacidad de procesamiento y transferencia altas y con una fiabilidad de datos que corresponda a lo anterior y a las demandas de identidad única e irrepetible de cada etiqueta.



**Fig 4.1 Tipos de Sistemas RFID**

Más aún, se debe considerar la naturaleza de los procesos de comunicación de datos, que pueden ser tanto síncronos como asíncronos, y que requieren una atención en cuanto a la forma en la que los datos se transfieren, de manera que se debe estructurar la cadena de bits para dar acomodo a estas necesidades, lo que se utiliza comúnmente para dar solvencia a estas necesidades se llama codificación de canal y aunque transparente al usuario del sistema RFID, el esquema de codificación de canal debe aparecer en las especificaciones del sistema. Muchos esquemas de codificación se pueden distinguir de aquí, cada uno de los cuales exhibe diferentes características de rendimiento.

Para transferir datos eficientemente vía aérea o del espacio que separa ambos componentes de comunicación, se requiere que los datos sean superpuestos, en algo que comúnmente se denomina modulación, y varios esquemas están disponibles para este propósito, cada uno teniendo atributos particulares que favorecen su uso. Estos esquemas están esencialmente basados en los cambios de valor de alguna de las características principales de una fuente alternada sinusoidal, su amplitud, frecuencia o fase en concordancia con la cadena de datos de la portadora. Con esta base uno puede tener los esquemas amplitud shift keying (ASK), frequency shift keying (FSK) y phase shift keying (PSK).

En adición a la transferencia de datos de no-contacto, la comunicación inalámbrica también puede permitir la comunicación no-línea de vista. De cualquier manera, con sistemas de muy alta frecuencia la mayor directividad es evidente y se tiene que considerar ahora la necesidad de un apropiado diseño de antena.

#### 4.4 Las Frecuencias Portadoras

En los sistemas de comunicación con cables las restricciones de las conexiones físicas permiten a los enlaces de comunicación y redes el ser efectivamente aislados unos de otros, la aproximación que se toma generalmente para los canales de comunicación en radio frecuencia es la de separarlos en base a su asignación de banda. Lo anterior requiere, y es generalmente cubierto por las entidades gubernamentales de cada país y su legislación, con las diferentes partes del espectro electromagnético siendo asignados para diferentes propósitos. Las asignaciones pueden diferir dependiendo el entorno de los gobiernos, requiriendo especial atención al considerar las aplicaciones RFID en diferentes países. Los esfuerzos de estandarización están buscando hacer obvios los problemas a este respecto.

Principalmente tres rangos de frecuencia se distinguen para este tipo de sistemas y son: sistemas RFID de baja frecuencia (LFRFID), sistemas de alta frecuencia (HFRFID) o intermedia para este tipo de sistemas y los sistemas de ultra-alta frecuencia (UHFRFID). De manera que las principales características para estos sistemas serían las siguientes:

Low Frequency RFID systems: Operan cerca de la banda de los 125 kHz con un rango de lectura típico de arriba de 508 mm (20 in).

High Frequency RFID systems: Operando en los 13.56 MHz con un máximo rango de lectura de arriba de 1 metro (3 ft).

Ultra-High Frequency RFID systems: Opera en múltiples frecuencias, incluyendo los 868 MHz (en Europa), una banda centrada en 915 MHz y otra en 2.45 GHz (microondas). El rango de lectura es de típicamente 1 a 3 metros (3 a 10 ft), pero los sistemas que operan en la banda de 915 MHz pueden lograr rangos de lectura de hasta 6 metros (20 ft) o más.

La tabla 4.1 resume las principales características de estos sistemas:

Banda de Frecuencia	Características	Aplicaciones Típicas
Baja Frecuencia 100-500 kHz	Rango de lectura de Corto a Medio. Barata. Baja velocidad de Lectura.	Control de Acceso Identificación Animal Control de inventarios Inmovilizador de Automóvil
Alta Frecuencia 10-15 MHz	Rango de lectura de Corto a Medio. Potencialmente barato. Velocidad de lectura Media.	Control de Accesos Tarjetas Inteligentes
Ultra-Alta Frecuencia 850-950 MHz 2.4-5.8 GHz	Rango de Lectura Largo. Alta velocidad de Lectura. Se requiere línea de vista. Caro.	Monitoreo de vagones de tren Sistemas de Colecta de Cuotas

**Tabla 4.1 Bandas de Frecuencia y Aplicaciones**

Un nivel de uniformidad es buscado para el uso de frecuencia portadora, a través de tres áreas de regulación que son: Región 1 Europa y África, Región 2 Norte, Sudamérica y el lejano oriente y la Región 3 en Australia y partes de Asia. Cada país administra sus asignaciones de frecuencia en base a las guías establecidas para las tres regiones. Desafortunadamente no ha habido muy poca o inconsistente acentuación en lo que a asignación se refiere, y también hay muy pocas frecuencias que están disponibles a nivel mundial para esta tecnología. Esto cambiará con el tiempo, así como los países sean orillados a mejorar la uniformidad al respecto para el 2010 aproximadamente.

Las etiquetas y los dispositivos de lectura/escritura deben compartir más que tan solo la frecuencia portadora para comunicarse. Los algoritmos de encriptamiento y decodificación, contenido de datos y formato, protocolos de interface y otras especificaciones técnicas deben ser completamente compatibles para los sistemas para que funcionen correctamente. Actualmente hay distintas iniciativas para la industria y la estandarización para facilitar el desarrollo de sistemas interoperables.

Tres frecuencias portadoras que han recibido especial énfasis con anterioridad son las representativas baja frecuencia, alta frecuencia y ultra-alta frecuencia, cuyos rangos típicos son de 125 kHz, 13.56 MHz y 2.45 GHz, respectivamente, sin embargo existen ocho bandas de frecuencia en uso en el mundo para aplicaciones RFID, las aplicaciones que usan estas bandas de frecuencia se listan en la tabla 4.2.

No todos los países en el mundo tienen acceso a todas las bandas que se listan en la tabla 4.2, así como no todos los países han asignado estas bandas para este uso. Para cada país y para cada rango de frecuencia existen regulaciones específicas que gobiernan el uso de la frecuencia. Estas regulaciones se pueden aplicar a niveles de potencia e interferencia así como a tolerancias de frecuencia.

#### **4.5 Tasa de Transferencia de Datos y Ancho de Banda**

La elección de la frecuencia de la onda de campo o la portadora es de primordial importancia en la determinación de la tasa de transferencia de datos. En términos prácticos la tasa de transferencia de datos es influenciada principalmente por la frecuencia de la onda portadora o variando el campo usado para llevar los datos entre la etiqueta y el lector. En general, a altas frecuencias, alta tasa de transferencia, o más grandes son los caudales de datos que se pueden lograr. Lo anterior se encuentra íntimamente relacionado con el ancho de banda o rango disponible con el espectro de frecuencia para el proceso de comunicación.

El ancho de banda de canal debe ser al menos dos veces el valor de la tasa de bits requerida para la aplicación en mente (ver el teorema de Nyquist), de aquí que las asignaciones de banda angosta pueden llevar a una consideración importante en cuanto a lo que es la tasa de transferencia, es muy claro que cuando menos alguna aplicación en donde amplios anchos de banda están envueltos se debe considerar. Usando la banda Spread Spectrum de 2.4-2.5 GHz, por ejemplo, rangos de 2 Mbps se pueden lograr, con una inmunidad al ruido agregada que provee la aproximación de modulación Spread Spectrum (espectro ensanchado) por su naturaleza.

Sin tomar en cuenta el Spread Spectrum, incrementando el ancho de banda se permite el incremento en el nivel de ruido y una reducción en la relación señal a ruido, de manera que generalmente es necesario el asegurar que una señal este por arriba del nivel de ruido para una aplicación en específico, el ancho de banda es una consideración importante en este sentido.

<b>Rango de Frecuencia</b>	<b>Aplicaciones y Comentarios</b>
Menos de 135 kHz	Una amplia variedad de productos disponibles para satisfacer una amplia variedad de aplicaciones, incluyendo etiquetamiento animal, control de accesos y seguimiento y ruteo. Los sistemas transponder los cuales operan en esta banda no necesitan estar licitados en muchos países.
1.95 MHz, 3.25 MHz, 4.75 MHz, y 8.2 MHz	Sistemas de Vigilancia Electrónica de Artículo (EAS) utilizados en algunas tiendas departamentales.
Aprox. 13 MHz, 13.56 MHz	Para sistemas EAS e ISM (Industrial, Scientific and Medical)
Aprox. 27 MHz	Aplicaciones ISM
430-460 MHz	Aplicaciones ISM especialmente en Región 1
902-916 MHz	Aplicaciones ISM específicamente en Región 2. En los Estados Unidos esta banda esta muy bien organizada con diferentes tipos de aplicaciones y con distintos niveles de prioridad, lo anterior incluye camiones de carga y Peaje electrónico. Esta banda ha sido dividida en fuentes de banda pequeña y fuentes de banda ancha (del tipo Spread Spectrum). En la región 1 las mismas frecuencias se utilizan por la red telefónica GSM.
918-926 MHz	En Australia se usa para sistemas RFID con transmisores con un EIRP no mayor de 1 watt.
2350-2450 MHz	Una banda reconocida en muchas partes del mundo como ISM. El IEEE 802.11 reconoce esta banda aceptable para comunicaciones en radiofrecuencia y tanto Spread Spectrum con sistemas de banda angosta son utilizados.
5400-6800 MHz	Esta banda esta asignada para uso futuro  Se le ha pedido al FCC que provea una asignación de 75 MHz en la banda de 5.85-5.925 GHz para servicios de Transportación Inteligente.  En Francia el sistema TIS esta basado en el pre-estandar Europeo propuesto (preENV) para vehículos en el tramo carretero, con comunicación vía microondas operando a 5.8 GHz.

**Tabla 4.2 Bandas de Frecuencia y Aplicaciones a nivel Mundial**

#### **4.6 Rango (alcance) y Niveles de Potencia**

El alcance que puede ser logrado con los sistemas RFID esta determinado esencialmente por:

- La potencia disponible en el lector/interrogador para comunicarse con las etiquetas.
- La potencia disponible en la etiqueta propiamente para responder.
- Las condiciones ambientales y estructurales, la forma se empieza a hacer significativa a altas frecuencias, incluyendo la razón señal a ruido.

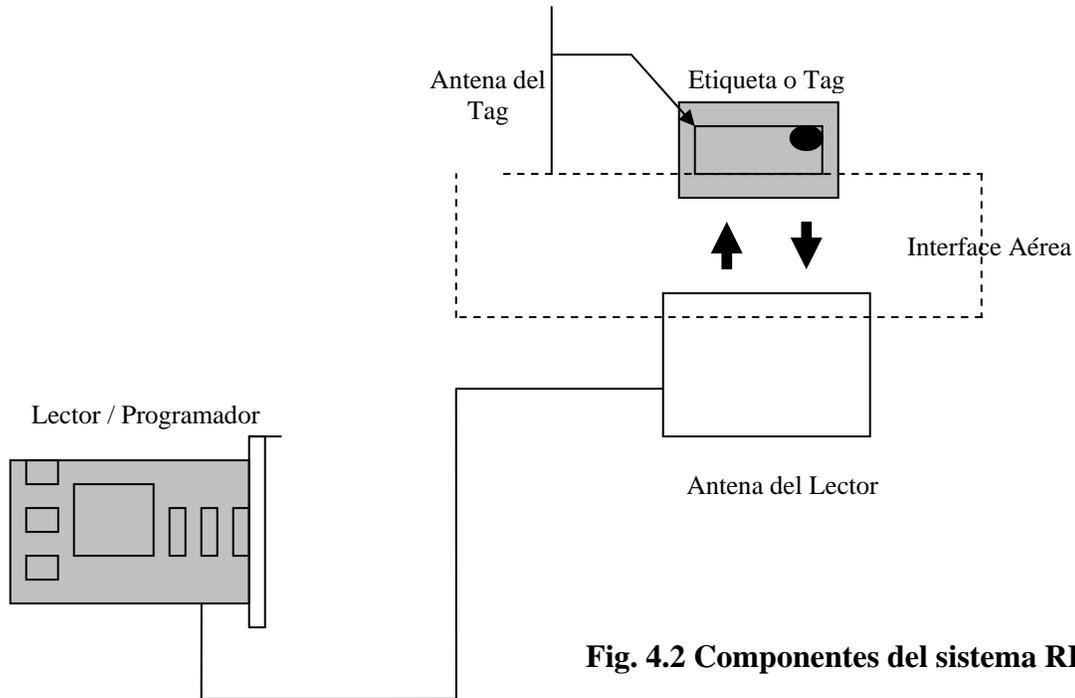
Aunque el nivel de potencia disponible es un factor determinante del rango y de cierta manera la eficiencia con la cual la potencia se despliega, también es influido por el rango. El campo u onda entregado desde una antena se extiende al espacio alrededor del mismo y su fuerza disminuye con respecto a la distancia. El diseño de antena determinará la forma del campo u onda de propagación entregada por la misma, así que el alcance también será influenciado por el ángulo subtendido entre la etiqueta y la antena.

En el espacio libre de obstrucciones o mecanismos de absorción, la fuerza del campo se reduce en proporción inversa al cuadrado de la distancia. Para una onda que se propaga a través de una región en la cual los reflejos pueden levantarse desde el suelo y desde obstáculos, la reducción en fuerza puede variar considerablemente, algunas veces como una cuarta potencia de la distancia inversa. Cuando existen diferentes caminos en este aspecto, se le denomina al fenómeno “atenuación multi-path”. A mas altas frecuencias, la absorción debida a la presencia de humedad puede influir en el alcance, por lo que es entonces importante en muchas de las aplicaciones el determinar que tanto el ambiente, interno o externo, puede influenciar el alcance de comunicación. Cuando un número de “obstáculos” reflectores metálicos y demás se encuentran en donde se va a considerar una aplicación y que además pueden variar en numero y de tiempo, también suele ser necesario el establecer las implicaciones de tales cambios a través de una apropiada evaluación del medio.

La potencia de las etiquetas es generalmente hablando mucha menos que la de los lectores, requiriendo además estos últimos de capacidad de detección sensitiva para manejar las señales de regreso. En algunos sistemas el lector constituye un receptor y esta separado de la fuente de interrogación o transmisor, particularmente si la portadora “uplink” (del transmisor al tag) es diferente de la del “downlink” (del tag al lector)

Aunque es posible el seleccionar niveles de potencia para satisfacer las diferentes necesidades de cada aplicación, no es posible sin embargo el ejercicio de completa libertad de elección, así como las restricciones en las frecuencias portadoras son por legislación en cada país limitantes en cuanto a niveles de potencia. Mientras que los valores de 100-500 mW son frecuentemente ocupados para los sistemas RFID, los valores actuales deben ser confirmados con la autoridad regulatoria, en los países donde se va a aplicar la tecnología. Estas autoridades además deben ser capaces de indicar la forma en la cual la potencia es entregada, por pulsos o continua, y los valores asociados permitidos.

Teniendo ahora alguna noción de los parámetros de comunicación de datos y sus valores asociados, es apropiado el considerar, en detalle, los componentes de un sistema RFID. Como podremos ver a continuación en la figura 4.2



**Fig. 4.2 Componentes del sistema RFID**

## 4.7 Transponders o Tags

La palabra transponder, derivada de TRANSMitter (transmisor) y resPONDER (receptor), revela la función del dispositivo, la etiqueta responde a una petición transmitida o comunicada por los datos que porta, el modo de comunicación entre el lector y la etiqueta (tag) es por vía inalámbrica a través del espacio o interface aérea entre ambos. El término además sugiere los componentes esenciales que componen un sistema RFID, los tags (etiquetas) y un lector o interrogador, donde el interrogador es usualmente aplicado como alternativa al lector, la diferencia estriba en que un lector en conjunto con un decodificador vienen a conformar lo que es el interrogador.

Los componentes básicos de un transponder se pueden representar como se muestra en la siguiente sección. Hablando en términos generales, los transponder se fabrican como circuitos integrados de baja potencia con capacidad de interface a devanados externos, o utilizando tecnología de “devanado en chip” para la transferencia de datos y generación de potencia (en modo pasivo).

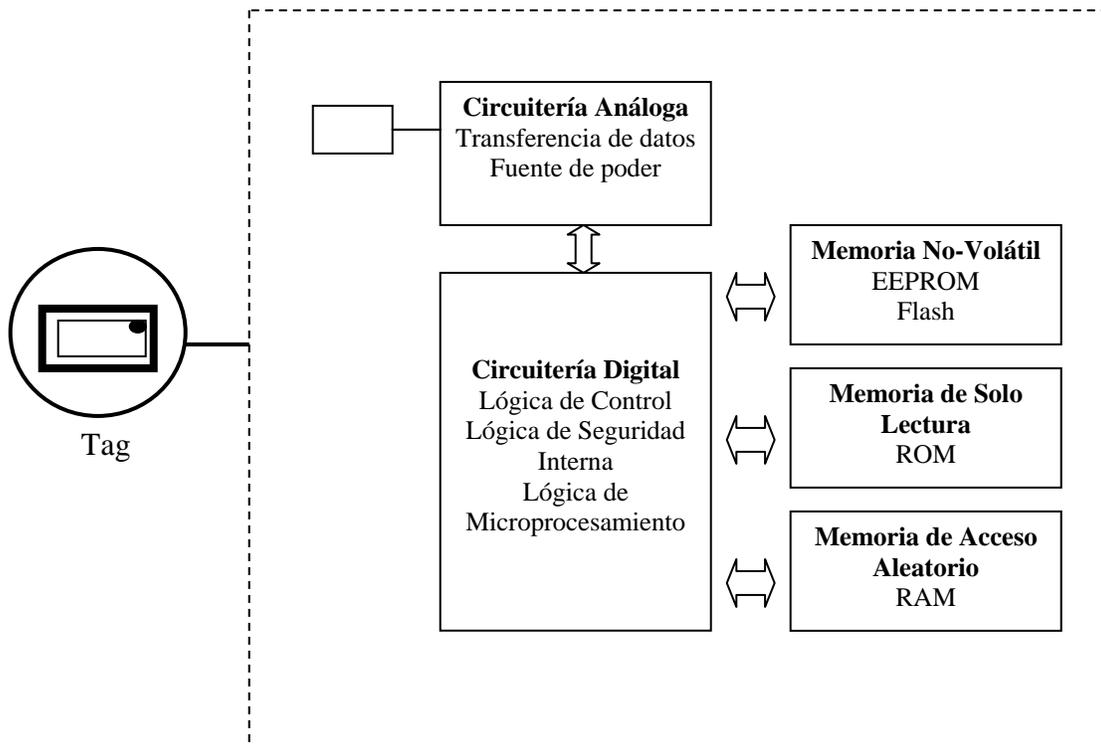
### 4.7.1 Características Básicas de un Transponder RFID

La memoria del transponder puede comprender desde memorias de sólo lectura (ROM), de acceso aleatorio (RAM) y memorias programables de almacenamiento no-volátil para el almacenaje de datos, dependiendo de el tipo y sofisticación del dispositivo. La memoria basada en ROM es usualmente empleada para el almacenaje de datos de seguridad y de

sistema operativo del transponder el cual contiene las instrucciones que, en conjunto con el procesador o con lo que se refiere a lógica de procesamiento son los elementos que negocian con las funciones internas (house keeping functions) tales como tiempo de respuesta o retardo, control reflujo de datos y la conmutación de fuente de poder. Los chips basados en memoria RAM son usados para facilitar el almacenamiento temporal de los datos durante la interrogación al transponder y la respuesta.

La memoria programable no volátil puede tomar varias formas, con la memoria de sólo lectura eléctricamente reprogramable (EEPROM) siendo la más típica. Esta última es usada para almacenar los datos de transponder y las necesita ser no-volátil para asegurar que los datos son retenidos cuando el dispositivo se encuentra en su estado inmóvil o de ahorro de energía (sleep).

Los buffers de datos son más que solo componentes de la memoria, son usados para el almacenamiento temporal de datos de entrada que después pasan a ser demodulados y a los datos de salida para la modulación que actúa como interface para la antena del transponder. La circuitería de la interface provee la facilidad de direccionamiento y distribución de la energía de campo para propósitos de potencia en los transponder pasivos, además del disparo en cuanto a la respuesta del transponder. La programación brinda las facilidades que deben ser provistas para aceptar la señal modulada de datos y realizar los procesos necesarios para la demodulación y transferencia de datos, ver figura 4.3.



**Fig. 4.3 Componentes de un Transponder (etiqueta)**

La antena del transponder es para cuando el dispositivo sensa el campo interrogatorio y cuando es apropiado, el campo de programación que a su vez sirve como transmisor del transponder en respuesta a la interrogación.

Un número de características en adición a la frecuencia portadora, distinguen a los transponders RFID y forman la base de las especificaciones del dispositivo, que incluyen:

- En lo que se refiere a la manera en que el transponder es energizado
- Las opciones de portadora de datos
- La tasa de lectura
- Las opciones de programación
- La forma física
- Los costos

#### **4.7.1.1 Energizado de los Tags**

Para que las etiquetas (tags) operen, al igual que muchos dispositivos, requieren de energía aunque los niveles no varíen mucho (del orden de micro a miliwatts). Cabe recordar que los tags pueden ser tanto activos como pasivos (puede agregarse semipasivos), la designación se determina completamente por la manera en la cual deriva la energía del dispositivo.

Los tags activos son energizados por una batería interna y son generalmente dispositivos de lectura-escritura, usualmente estos dispositivos contienen una *célula* que exhibe una alta razón de potencia-peso y es usualmente capaz de operar sobre un rango de temperatura de -50 °C a +70 °C. El uso de una batería significa que un transponder activo sellado tiene una vida finita. De cualquier modo una celda conveniente acoplada a una conveniente circuitería de baja potencia puede asegurar funcionalidad en 10 o mas años, dependiendo del las temperaturas de operación, ciclos de lectura/escritura y el uso. El <sup>2</sup>trade off (las desventajas a cambio de algunas ventajas sustanciales)es que pueden ser de un tamaño mayor y también son más costosos comparados con los tags pasivos.

En términos generales, los transponders activos permiten un amplio rango de comunicación del que se puede esperar para el caso de los dispositivos pasivos, además de una mejor inmunidad al ruido, y altas tasas de transmisión de datos cuando es usado para energizar un modo de respuesta en alta frecuencia.

Los tags pasivos operan sin una fuente interna o batería, derivando la potencia de operación al campo generado por el lector. Los tags pasivos son consecuentemente mucho mas livianos que los dispositivos activos, menos caros y ofrecen un tiempo operacional virtualmente ilimitado. El <sup>2</sup>trade off en este caso es que los tags pasivos tienen menos rango de lectura que los tags activos y requieren además de un lector altamente energizado.

---

<sup>2</sup> El término trade off viene a significar en los dispositivos electrónicos, el precio pagado en cuanto a características técnicas a cambio de otro tipo de beneficios tanto técnicos como económicos.

Los tags pasivos además están restringidos en su capacidad de almacenamiento de datos y en la capacidad de operar bien en ambientes de ruido electromagnético.

La sensibilidad y orientación de estos dispositivos también puede estar restringida en cuanto a la potencia disponible. Debido a todas estas limitaciones, los transponders pasivos ofrecen algunas ventajas en términos de costos y longevidad, éstos además tienen un indefinido periodo de vida y son generalmente mas bajos en precio que los transponders activos.

Es muy conveniente también el clasificar a los tags de acuerdo a la funcionalidad que tienen. El centro MIT de auto identificación ha separado así a cinco clases de acuerdo a la funcionalidad, veremos a continuación una clasificación similar (Ver tabla 4.3).

Tags de **Clase 0**: Los tags de clase 0 son de los más primitivos, estos ofrecen tan solo la vigilancia electrónica de artículo (EAS) como funcionalidad. Los tags de clase 0 solamente anuncian su presencia y no contienen alguna identificación única de chip. Los tags de clase 0 pueden no contar con ningún chip, esto es que no contengan ninguna clase de lógica, se les puede encontrar principalmente en los libros de biblioteca o en los discos compactos.

Tags de **Clase 1**: Estos contienen datos de identificación únicos que son almacenados en memorias del tipo solo lectura (ROM) o del tipo solo una escritura y muchas lecturas (WORM). Los tags de clase 1 típicamente son pasivos aunque pueden presentarse como semi-pasivos o activos, éstos tags actúan como simples medios de identificación.

Tags de **Clase 2**: Los tags de clase 2 poseen memorias de lectura-escritura, lo cual les permite actuar como dispositivos de anotación. Los tags de clase 2 se pueden reciclar y reutilizarse para identificar distintos artículos durante su periodo de vida. Aunque la clase 2 puede ser pasiva, son más comunes los dispositivos semi-pasivos o activas.

Tags de **Clase 3**: Esta clase de tags contiene sensores ambientales de a bordo. Estos pueden grabar tanto la temperatura, como la aceleración ,movimiento o radiación, para poder ser más eficientes que un sensor sin memoria. Los tags de clase 2 requieren de memoria de escritura, ya que la lectura de sensores se toma en ausencia de un lector. Los tags clase 3 son necesariamente semi-pasivos o activos.

Tags de **Clase 4**: Los tags de clase 4 pueden establecer redes inalámbricas de tipo ad-hoc con otros tags y ya que pueden iniciar una comunicación, necesariamente deben ser dispositivos activos. La funcionalidad de estos dispositivos reside en la visión de computadoras ubicuotas o el llamado “polvo inteligente” (smart dust).

Clase	Nombre Genérico	Memoria	Fuente de Energía	Características
0	Tags anti-robo	Ninguna	Pasiva	Vigilancia de Artículo
1	EPC	Sólo Lectura	Cualquiera	Solo Identificación
2	EPC	Lectura-Escritura	Cualquiera	Datos de Anotación
3	Tags de Sensor	Lectura-Escritura	Semi-pasiva/Activa	Sensores de Ambiente
4	Smart Dust	Lectura-Escritura	Activa	Redes Ad-Hoc

**Tabla 4.3 Funcionalidad en Clases de Tags**

En resumen lo que podríamos decir de los tags o etiquetas es que son dispositivos de microelectrónica usados para el almacenaje de datos y de carácter operacional, tienen además un elemento de acople como una antena para comunicación. Los tags además pueden tener una superficie de contacto como se puede encontrar en las tarjetas inteligentes. La memoria del tag puede ser del tipo solo lectura, de una sola escritura y muchas lecturas o completamente reescribibles, ver comparativo en tabla 4.3.

Una clasificación clave para estos dispositivos es en función de su fuente de energía. Los tags pueden venir en tres variedades: activos, semi-pasivos y pasivos. Los dispositivos activos contienen una fuente de energía de a bordo, por ejemplo una batería, así como la habilidad de poder iniciar sus propias comunicaciones, posiblemente con otros tags. Los tags semi-pasivos, contienen una batería, pero solo pueden responder a comunicaciones entrantes. Los dispositivos pasivos reciben toda la energía del lector y nunca pueden iniciar una comunicación.

Para dar una analogía a lo que es el proceso de energizado pasivo, uno puede pensar en los lectores como si estuviesen “gritando” a los tags pasivos y después extrayendo datos del eco resultante, los tags pasivos se encuentran completamente inactivos en la ausencia de un lector.

Una fuente de energía en un tag determina tanto su rango como su costo (como veremos adelante). Los tags pasivos son los mas baratos en manufactura e incorporados en su empaque también tienen el menor rango de lectura. Los tags semi-pasivos tienen un costo y rango moderados, mientras que los tags activos tienen el mayor rango de lectura y costo, vea la tabla 4.4 para una comparación de los diferentes tipos.

	Pasivos	Semi-Pasivos	Activos
<b>Fuente de Energía</b>	Pasivo	Batería	Batería
<b>Transmisor</b>	Pasivos	Pasivos	Activos
<b>Rango Máximo</b>	10 m	100 m	1000 m

**Tabla 4.4 Tags Activos, Semi-Pasivos y Pasivos**

#### 4.7.1.2 Opciones de transporte de datos

Los datos almacenados en la (etiqueta) portadora de datos invariablemente requieren de algo de organización y agregados, tales como las características de identificación de datos y los bits de detección de errores para satisfacer necesidades de recuperación. Este proceso es usualmente referido como *codificación de fuente*. Sistemas de numeración estándar como el UCC/EAN y elementos asociados de definición de datos también se pueden aplicar a los datos almacenados en las etiquetas. La cantidad de datos dependerá por supuesto de la aplicación y requiere de un tag apropiado para satisfacer esa necesidad. Básicamente los tags se pueden usar para portar:

- Identificadores en los cuales una cadena numérica o alfanumérica se almacena para propósitos de identificación, o como una llave de acceso para el almacén de datos en otra parte como en una computadora o un sistema de administración, o también
- Archivos portátiles de datos, en los cuales la información se puede organizar para comunicación o para iniciar acciones sin tener que hacer un redireccionamiento, o en combinación con los datos almacenados en otro lugar.

En términos de capacidad de datos, las etiquetas pueden satisfacer necesidades desde un solo bit hasta kilobits. Los dispositivos de almacenaje de un solo bit son esencialmente para propósitos de vigilancia. La vigilancia electrónica de artículo (EAS por sus siglas en inglés) de las tiendas o cadenas comerciales es la aplicación típica para tales dispositivos, siendo usados en ese caso para activar una alarma cuando se detecta en el campo de interrogación, además se les puede encontrar en contadas aplicaciones.

Los dispositivos caracterizados por capacidades de almacenaje de arriba de 128 bits son suficientes para retener un número de serie o identificación completo, y hasta posiblemente, con bits de chequeo de paridad, tales dispositivos pueden ser programados por el fabricante o programables por el usuario. Los tags con capacidades de almacenaje de datos de arriba de 512 bits son invariablemente programables por el usuario y rentables al hablar de capacidades para alojar en memoria datos de identificación y otros datos como podrían ser números de serie, contenido del empaque, instrucciones clave de procesamiento o posiblemente resultados de transacciones tempranas de interrogación o respuesta.

Las etiquetas caracterizadas por capacidades de almacenamiento de cerca de 64 kilobits se pueden considerar como dispositivos para archivos de datos portátiles. Con la capacidad incrementada las facilidades pueden ser provistas para organizar datos dentro de campos o páginas que deberán ser interrogadas selectivamente durante el proceso de lectura.

#### 4.7.1.3 Rango de lectura de datos

Ya se ha mencionado anteriormente que la tasa de transferencia de datos está esencialmente ligada a la frecuencia portadora de la siguiente manera, a más alta frecuencia, más alta será la tasa de transferencia, generalmente hablando. Esto también debe ser contemplado que la

lectura o transferencia de datos requiere de un periodo finito de tiempo, incluso cuando sea en el orden de los milisegundos, y puede ser una consideración importante en aplicaciones donde un tag es pasado rápidamente a través de un campo o zona de interrogación o lectura.

#### **4.7.1.4 Opciones de programación de datos**

Dependiendo del tipo de memoria una etiqueta que contiene datos puede ser de solo lectura, de una sola escritura y muchas lecturas WORM (Write Once Read Many) o de lectura/escritura. Las etiquetas de sólo lectura, invariablemente son dispositivos de baja capacidad programados de manufactura, usualmente con un número de identificación. Los dispositivos WORM son dispositivos programables por el usuario, los dispositivos de lectura/escritura son también programables por el usuario, pero además permitiendo al usuario el cambio de los datos almacenados en un tag. Los programadores portátiles se pueden reconocer ya que también permiten programación del tag dentro del campo de lectura/interrogación mientras éste se encuentra adjunto al objeto, siendo identificado.

#### **4.7.1.5 Forma física**

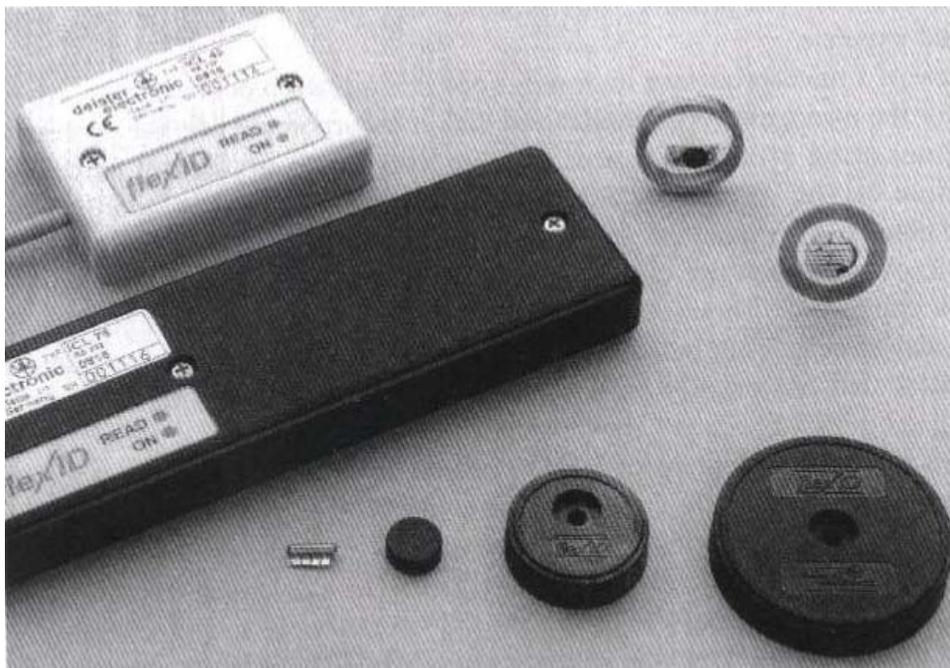
Los tags RFID vienen en una amplia variedad de formas, figuras, tamaños y empaques protectores. Los tags de seguimiento animal, insertados debajo de la piel, pueden ser tan pequeños como un puntilla de lápiz en diámetro y 10 milímetros de longitud. Los tags pueden ser forma de tornillo de manera que se puedan identificar árboles o elementos forestales, o con forma de tarjeta de crédito para el uso en aplicaciones de acceso. Los tags con plástico duro antirrobo que se adjuntan a la mercancía en las tiendas también son tags RFID, así como también los hay para fines mas pesados como por ejemplo los transponders rectangulares de 120 x 100 o 50 milímetros usados para el seguimiento de contenedores intermodales o maquinaria pesada, camiones y vagones de tren para aplicaciones de mantenimiento y seguimiento. A continuación se presenta una breve descripción de las principales formas de construcción de los tags.

**Discos y Monedas:** El formato de construcción más común es en *Disco* (moneda), en él se encuentra un transponder en un alojamiento moldeado redondo de inyección (ABS), cuyo rango de alcance (diámetro) va de unos cuantos milímetros a 10 cm (figura 4.4). Usualmente poseen un hueco en el centro para atornillado. Como alternativa al moldeado de inyección (ABS), el polystyrol o incluso una resina epóxica pueden ser usados para lograr un rango de temperatura mas amplio.

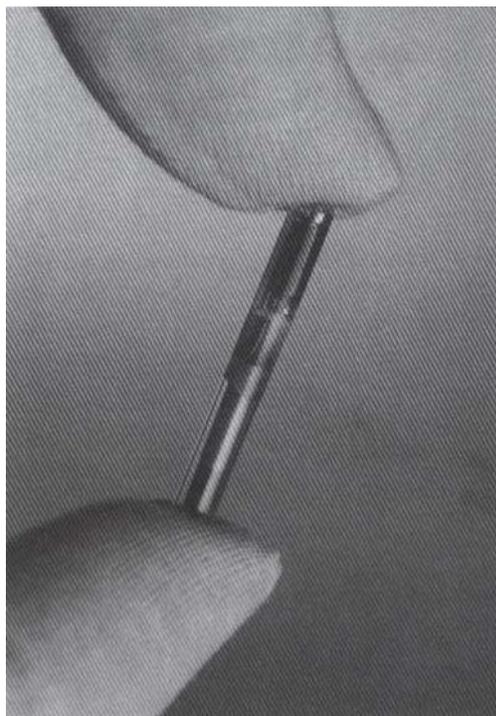
**Alojamiento de Cristal:** Los transponders de *Cristal* (figura 4.5) se han desarrollado de manera que puedan ser inyectados bajo la piel de animales para propósitos de identificación.

Los tubos de cristal de tan solo 12-32 mm contienen un microchip montado en un portador (PCB) y un chip capacitor para filtrar el suministro de corriente obtenido. El devanado del transponder, incorpora cable de solo 0.03 mm de espesor hendido en un núcleo de ferrita.

Los componentes internos se empotran en un adhesivo suave para lograr una estabilidad mecánica. (fig 4.6)



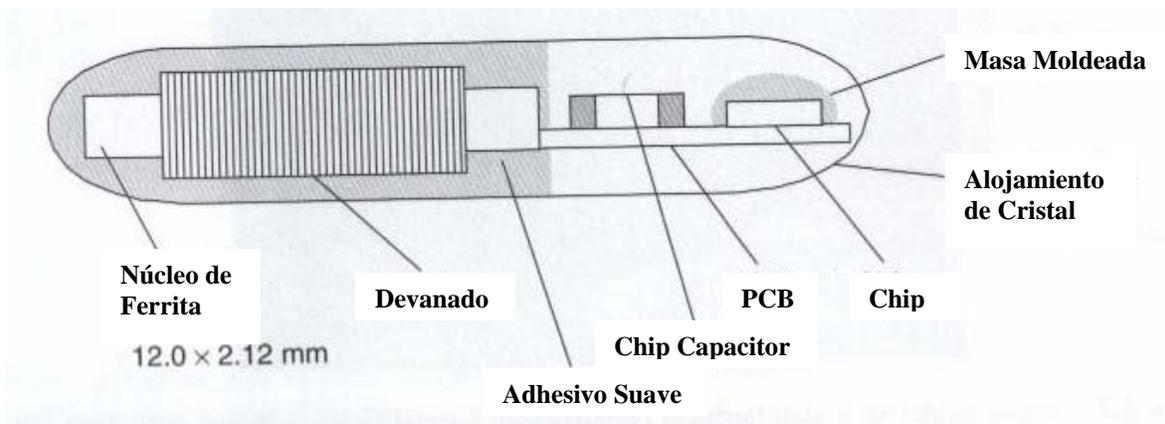
**Fig. 4.4** Diferentes formatos de construcción de los transponders de disco. A la derecha el devanado del transponder y el chip antes de ser colocado en el alojamiento; a la izquierda, diferentes formatos de construcción de antenas lectoras.



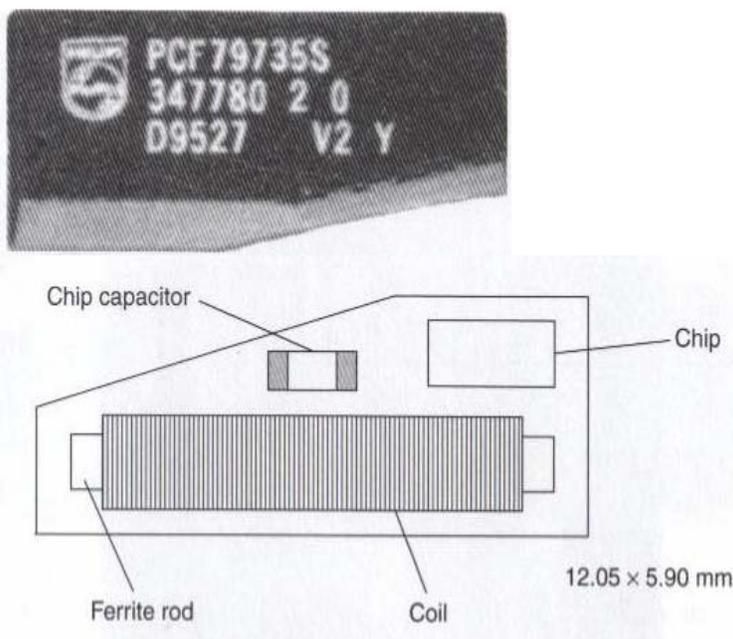
**Fig. 4.5** Acercamiento a un transponder de Cristal de 32 mm para la identificación de animales o para el procesamiento para otros formatos de construcción (Texas Instruments)

**Alojamiento Plástico:** Este alojamiento plástico (plastic package, PP) se desarrolló para aplicaciones que involucran demandas mecánicas particularmente altas, este alojamiento se puede integrar fácilmente a los productos como por ejemplo las llaves de auto para sistemas de inmovilización electrónica (fig 4.7).

La pieza, hecha de una sustancia moldeable (compuesto típico IC), contiene casi los mismos componentes que el alojamiento de cristal, pero su devanado más largo le da un rango funcional más elevado (fig 4.7). Algunas otras ventajas son su habilidad para aceptar chips más grandes y su gran tolerancia a las vibraciones mecánicas, la cual es requerida por la industria automotriz por ejemplo. El transponder PP se ha probado con resultados completamente satisfactorios con relación a los requerimientos de calidad, como los ciclos de temperatura o pruebas de caída.

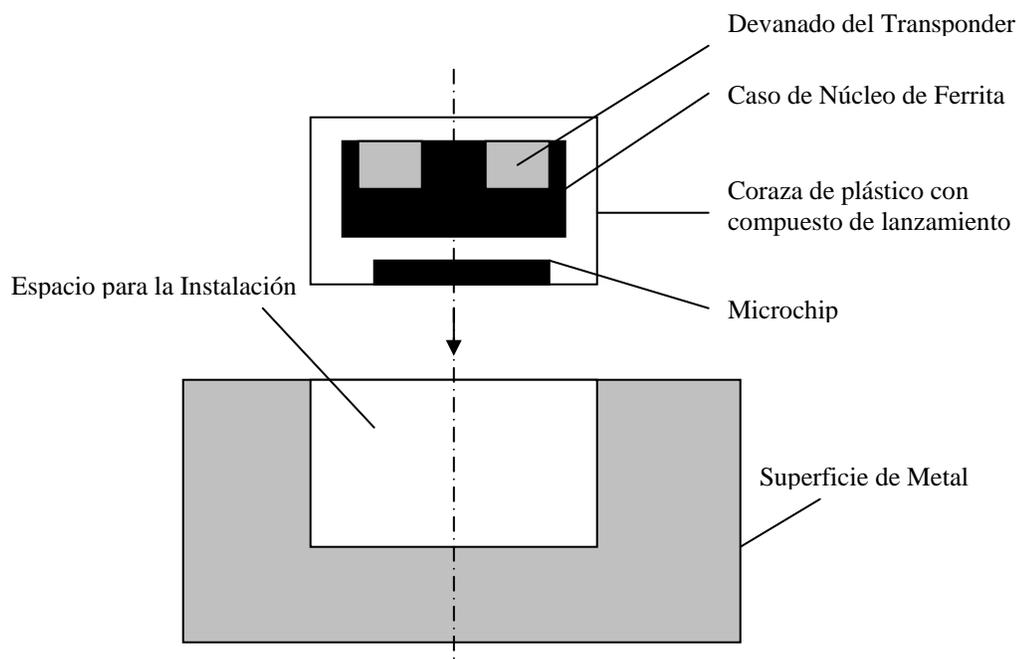


**Fig. 4.6 Esquema Mecánico de un Transponder de Cristal**



**Fig. 4.7 Transponder de Alojamiento Plástico. Esquema del transponder, El alojamiento tiene tan solo 3 mm de espesor.**

**Para herramientas e identificación de cilindros de gas:** Algunos formatos especiales de construcción se han desarrollado para la instalación de transponders de acople inductivo dentro de superficies metálicas. Para esto el devanado del transponder se encuentra hendido en un núcleo de ferrita. El chip del transponder se monta en la parte posterior del núcleo de ferrita y contactado con el devanado del transponder, en pro de obtener suficiente estabilidad mecánica, de vibración y tolerancia al calor, el chip del transponder y el núcleo de ferrita son lanzados dentro de un alojamiento plástico (plastic package shell PPS) usando resina epóxica. Las dimensiones externas del transponder y su área de encaje se han estandarizado en ISO 69873 para la incorporación dentro de una tuerca o afilamiento de descarga rápida para la identificación de herramientas. Diferentes diseños son utilizados para la identificación de cilindros de gas. La figura 4.8 muestra el esquema mecánico de un transponder para encajar en una superficie metálica.



**Fig. 4.8 Esquema mecánico de un transponder para encajar en superficies metálicas. El devanado de transponder esta hendido alrededor de un núcleo de ferrita en forma de U y después lanzado a la coraza de plástico. Se instala con la abertura del núcleo en primer lugar.**

**Transponders para llaves y llaveros:** Los transponders también se integran en las llaves para inmovilizadores o aplicaciones de seguro de puertas con los sistemas particulares de alta seguridad. Estos están generalmente basados en un transponder dentro de un alojamiento plástico, el cual es lanzado o inyectado en el llavero.

El diseño de transponder en llave ha probado ser muy popular para los sistemas al proveer accesos a oficinas y áreas de trabajo.

**Transponders en relojes:** Este formato de construcción se desarrolló a principios de los 90's por la compañía austriaca Ski-Data y se usó primeramente en pases de esquí, estos relojes de no contacto también eran capaces de ganar terreno en sistemas de control de acceso. El reloj contiene un marco de antena con un pequeño número de bobinados impresos sobre un delgado circuito impreso, el cual sigue al alojamiento del reloj tan cerca como puede para maximizar el área encerrada por el devanado de la antena y de esta forma... el rango.

**Tarjetas inteligentes Formato ID-1:** El formato ID-1 familiar por las tarjetas de crédito y tarjetas telefónicas (85.72 mm x 54.03 mm x 0.76 mm  $\pm$  tolerancias) se está volviendo incrementalmente importante para las tarjetas inteligentes de no contacto en los sistemas RFID. Una ventaja de este formato para sistemas RFID de acople inductivo es la gran área de devanado, la cual incrementa el rango de las tarjetas.

Las tarjetas inteligentes de no contacto se producen por la laminación de un transponder entre 4 láminas de PVC, los laminados individuales se cocinan a alta presión y temperaturas arriba de los 100 °C para producir una atadura permanente.

Las tarjetas inteligentes de no contacto de diseño ID-1 están excelentemente adaptadas para portar anuncios y usualmente tener estampados muy artísticos, como los de las tarjetas telefónicas, por ejemplo (fig 4.9).

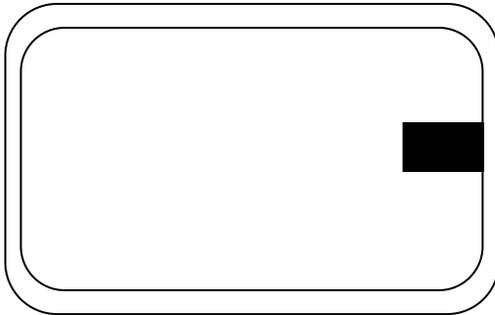
De cualquier manera, no siempre es posible el adherir el máximo espesor de 0.8 mm especificado para tarjetas ID-1 en el ISO 7810 . Los transponders de microondas en particular requieren de un diseño más grueso, ya que en este diseño el transponder es típicamente insertado entre dos corazas de PVC o empaçados usando un procedimiento de moldeado de inyección (ABS).

**Tarjetas Inteligentes:** El término *tarjeta inteligente* se refiere a un formato de transponder de papel delgado. En los transponders de estas características el devanado de los mismos se aplica a un forro plástico de tan solo 0.1 mm de espesor por apantallamiento o grabado. Este forro es usualmente laminado usando una capa de papel y su recubrimiento trasero con adhesivo. Los transponders son surtidos en la forma de stickers auto adhesivos en su presentación final, son delgados y suficientemente flexibles para pegarse al equipaje, empaques y bienes de todos tipos (figs 4.10 y 4.11). Las etiquetas pegadas pueden ser sobreimpresas, tan solo se relacionan los datos almacenados a un código de barras adicional al frente de la etiqueta.



**Fig. 4.9**

**Tarjeta inteligente de no contacto semitransparente. La antena del transponder se puede ver claramente a lo largo del borde de la tarjeta.**



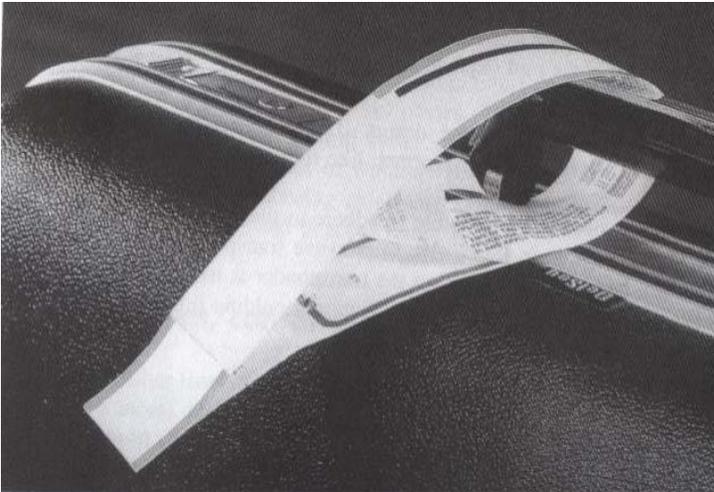
**Esquema de una tarjeta inteligente de no contacto**

**Vista Frontal**

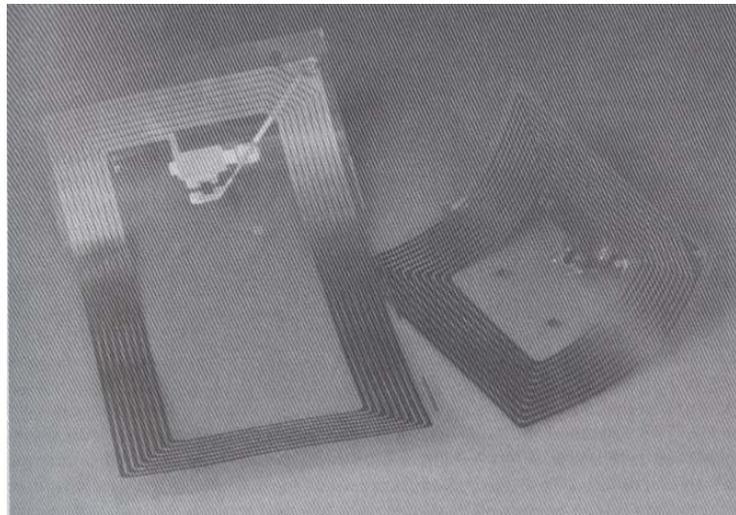
**Devanado en Chip:** En los formatos de construcción mencionados anteriormente, los transponders consisten de un devanado que funciona como una antena y un chip transponder separado (tecnología híbrida). El devanado del transponder es unido al chip transponder en la manera convencional. Un paso adelante obvio en la miniaturización es la integración del devanado en chip (devanado en chip). Esto se hace posible gracias a un proceso microgalvánico que puede tener lugar en una oblea CMOS normal. El devanado se coloca directamente en el aislante del chip de silicio en la forma de un arreglo de espiral planar (capa sencilla) y contactado al circuito de debajo de acuerdo a las aberturas convencionales en la capa de pasivación. El camino del conductor y sus anchos caen en los rangos de 5 – 10  $\mu\text{m}$  con un espesor de capa de 15 – 30  $\mu\text{m}$ . Una pasivación final sobre una base de polyamide se lleva a cabo para garantizar la capacidad de carga mecánica del módulo de memoria de no contacto basado en tecnología de devanado en chip (coil-on-chip).

El tamaño del chip de silicio, y del transponder también es de tan solo 3 mm x 3 mm. Los transponders son frecuentemente pegados a una coraza plastica por conveniencia y a las dimensiones de 6 mm x 1.5 mm ya son casi los más pequeños dispositivos de este tipo que se pueden hallar al mercado disponibles entre los de tecnología RFID.

**Otros formatos:** En adición a los principales diseños que hemos presentado, distintos diseños para aplicaciones específicas también se fabrican, por ejemplo los tags que se usan en las carreras de palomas “*racing pigeon transponder*” o el “*champion chip*” para eventos deportivos de precisión. Los transponders se pueden incorporar dentro de cualquier diseño que requiera el cliente. Las opciones preferidas son los transponders de vidrio o los de plástico PP, los cuales son entonces procesados mas allá para obtener la forma final



**Fig. 4.10 Tarjeta inteligente que son suficientemente delgadas y flexibles para ser adjuntadas a maletas en forma de etiqueta auto adhesiva.**



**Fig. 4.11 Una etiqueta inteligente consiste principalmente de una película delgada de plástico laminado con lo que el devanado y el chip se pueden aplicar.**

#### **4.7.1.6 Costos**

Los costos de un tag obviamente dependen del tipo y cantidades que se adquieran. Para cantidades muy grandes (decenas de miles) el precio puede oscilar de menos de unos cuantos centavos para tags extremadamente sencillos a miles de pesos para los sistemas más grandes y sofisticados.

La complejidad creciente de las funciones de los circuitos, la construcción y la capacidad de memoria influirá también en los costos tanto de transponders como de lectores/programadores.

La manera en la cual el transponder se empaca para formar una unidad también será un factor limitante en el costo. Algunas aplicaciones en las que se pueden esperar ambientes ásperos de alguna forma, como en molinos de acero, minas y car body paint shops, requerirá empaques mecánicamente robustos, químicamente tolerantes y tolerantes en factores como la temperatura. Dicho empaquetado indudablemente representará una porción significativa del costo total del transponder.

Generalmente los transponders de baja frecuencia son más baratos que los dispositivos de alta frecuencia así como los transponders pasivos son baratos usualmente, a diferencia de los dispositivos activos.

#### **4.8 El Lector o Interrogador**

Los dispositivos lectores o de interrogación pueden diferir considerablemente en complejidad, dependiendo del tipo tags que soportan y las funciones que deben satisfacer. De cualquier forma, la mayor función es la de proveer comunicación con los tags y facilitar la transferencia de datos, las funciones que son realizadas por el lector pueden incluir un condicionamiento de señal sofisticado, verificación de error de paridad y corrección. Una vez que las señales del transponder se han recibido correctamente y decodificado, los algoritmos se pueden aplicar para decidir cuando la señal es una transmisión repetida y entonces poder comandar al transponder para dejar de transmitir.

Lo anterior se conoce como el protocolo *Command response* y es usado para sobrellevar los problemas de lectura de múltiples tags en un corto espacio de tiempo. Al usar interrogadores de esta manera es a veces referido como *Hands Down Polling*. Una alternativa, que ofrece además mayor seguridad, pero una menor técnica para sondeo de tags se llama *Hands Up Polling* (Sondeo Manos Arriba) que involucra que el interrogador busque algún tag de identidad específica y los interroge por turnos entonces. Esto es una técnica de sondeo-respuesta o administración de la disputa por el espacio de transmisión (del tipo token en ambientes LAN), y una variedad de técnicas han sido desarrolladas para mejorar el proceso de barrido de lectura en lotes. En un enfoque diferente que va un poco más allá, también se pueden utilizar lectores múltiples, multiplexados en un interrogador, pero, por supuesto con significativos incrementos en costos.

#### **4.9 Los Programadores de Transponder**

Los programadores de transponder actúan en el sentido en que los datos son entregados para escribir una vez, leer muchas veces (WORM) y tags de lectura-escritura. La programación es generalmente llevada a cabo en una forma *off-line* (fuera de línea) al principio de un lote en línea de producción, por ejemplo.

Para algunos sistemas la reprogramación se debe llevar a cabo de manera *on-line*, particularmente si esta se usa como un archivo portátil interactivo de datos en un ambiente de producción por ejemplo. Los datos deben ser grabados durante cada proceso. Quitando el transponder al final de cada proceso para leer el proceso de datos previo y para programar los nuevos datos, naturalmente incrementará el tiempo de procesamiento y podría disminuir sustancialmente la flexibilidad que se intentaba obtener para la aplicación. Si se combinan las funciones de un lector/interrogador y un programador, los datos se pueden adjuntar o alterar en el transponder como sea requerido, sin comprometer a la línea de producción.

El rango sobre el cual la programación se puede lograr es generalmente menos que el rango de lectura y, en algunos casos el posicionamiento de cercanía de contacto es requerido. Los programadores son también generalmente diseñados para manejar un tag a la vez. De cualquier manera, los desarrollos están ahora satisfaciendo la necesidad de programación selectiva de un número de tags presente en el rango del programador.

#### **4.10 Categorías en los sistemas RFID.**

Los sistemas RFID se pueden agrupar en cuatro categorías a grosso modo que son:

- Sistemas para vigilancia electrónica de artículo EAS por sus siglas en inglés.
- Sistemas portátiles de captura de datos.
- Sistemas de red.
- Sistemas de posicionamiento.

Los sistemas para vigilancia electrónica de artículo EAS son típicamente sistemas de un solo bit usados para censar la presencia o ausencia de un artículo. El más amplio uso que se le da a esta tecnología es en las tiendas departamentales donde cada artículo es etiquetado y un amplio número de antenas lectoras son colocadas en cada salida de las tiendas para detectar la salida sin autorización de cualquier producto (robo).

Los sistemas portátiles de captura de datos se caracterizan por el uso de terminales de datos portátiles con lectores RFID integrales y que se usan en aplicaciones donde un alto grado de variabilidad en cuanto a los requerimientos de datos de fuente desde los artículos etiquetados se puede llegar a dar. Los lectores hand-held o terminales de datos portátiles capturan los datos que son entonces transmitidos directamente a un sistema host de administración de información por medio de una comunicación de datos en radio frecuencia (RFDC-radio frequency data communication) o pueden también ser retenidos para su posterior entrega en un enlace en línea al host en un proceso de lotes.

Las aplicaciones para sistemas en red pueden generalmente caracterizarse por lectores de posición fija desplegados en un determinado lugar y conectados directamente a un sistema en red de administración de información. Los transponder se colocan en artículos en movimiento o móviles de alguna manera, o gente, dependiendo de la aplicación.

Los sistemas de posicionamiento usan transponders para facilitar la localización automática y apoyo a la navegación para vehículos de comando. Los lectores se posicionan en los vehículos y se comunican a la vez a una computadora de a bordo en un enlace RFDC al sistema host de administración, los transponders se empotran al piso del ambiente operativo y se programan con los datos apropiados de identificación y locación, la antena lectora es usualmente alojada bajo el vehículo para permitir la mayor proximidad con los transponders.

#### **4.11 Estandarización.**

Si las únicas buenas noticias para RFID son las ventajas y su flexibilidad, entonces la proliferación de estándares incompatibles RFID serían la malas noticias, ya que los más grandes fabricantes y vendedores de esta tecnología ofrecen sistemas de su propia autoría, lo que arroja el resultado de que varias aplicaciones e industrias han comprado estándares de diferentes vendedores RFID con las consecuentes frecuencias de operación y protocolos, que varían entre sí debido a la competencia. El actual estado de los estándares RFID se encuentra severamente desordenado, los estándares para los que se tiene esta situación comprenden desde los ferrocarriles, camiones, control de tráfico aéreo y la captación de peajes. El sistema estadounidense de transportación inteligente (Intelligent Transportation System) y el sistema de visibilidad total del recurso (Total Asset Visibility) del departamento de defensa del mismo país (DoD) se encuentran entre las aplicaciones de especial interés.

La ausencia de sistemas abiertos intercambiables ha hecho cojear severamente el crecimiento de la industria RFID en su totalidad, además de desacelerar la disminución en precios resultante del despliegue de estándares para la tecnología en la industria. De cualquier manera, un número importante de organizaciones han estado trabajando en las resoluciones para llegar en el mediano plazo a una convención en lo que compete a los sistemas RFID, tanto en Europa como en Estados Unidos en donde el mercado RFID ha hecho las mas importantes incursiones. Mientras eso sucede, en Estados Unidos, el grupo X3T6 de ANSI, que comprende el mayor de los fabricantes y usuarios de RFID, está actualmente desarrollando un documento de proyecto para sistemas basados en frecuencias de operación de 2.45 GHz, el cual esta en proceso de ser adoptado por ISO. ISO actualmente ha adoptado algunos estándares RFID para el seguimiento de animales, estos estándares son el ISO 11784 e ISO 11785.

Así como la estandarización permitió el tremendo crecimiento y despliegue del código de barras, la cooperación entre los fabricantes de RFID será necesaria para promover los desarrollos tecnológicos y refinamientos que permitirán una amplia base para el crecimiento de la aplicación.

# ***CAPÍTULO 5***

## **EL RFID EN LAS COMUNICACIONES 3G, PROTOCOLO NFC**

5.1	Introducción .....	109
5.2	Requerimientos RFID Actuales. ....	110
5.2.1	¿Que problema de negocio estoy tratando de resolver? .....	110
5.2.2	¿Cuál es la diferencia entre RFID y el código de barras?.....	111
5.2.3	¿Qué buena razón tengo para usar el RFID? .....	111
5.2.4	¿Cuales son los beneficios para mi negocio?.....	112
5.2.5	¿Cuáles estándares y consideraciones regulatorias aplicar? .....	114
5.2.6	¿Qué cambios a la infraestructura de sistemas informáticos se requieren para .....	116
5.2.7	¿Qué cambios a los procesos de etiquetado y empaquetado debo tener en cuenta para cumplir con los requerimientos? .....	116
5.2.8	¿Qué tipo de pruebas antes de la aplicación se requieren? .....	117
5.3	Las Aplicaciones RFID .....	148
5.3.1	Aplicaciones potenciales .....	121
5.3.1.1	Gen 2 .....	121
5.3.1.2	Identificación de pacientes.....	122
5.3.1.3	Tráfico .....	122
5.3.2	TARJETAS INTELIGENTES .....	122
5.3.3	Aplicaciones Específicas para Tarjetas Inteligentes .....	124
5.3.4	Transporte Público .....	126
5.3.4.2	Boletaje.....	133
5.3.4.3	Metrobús-Ciudad de México .....	134
5.3.5	Características principales para Tarjetas Inteligentes .....	135
5.4	Near Field Communications (NFC).....	138
5.4.1	Introducción a NFC .....	138
5.4.2	Near Field Communication Interface and Protocol 1 (NFCIP-1)...	141

5.4.2.1 Campo de Radiofrecuencia (RF).....	141
5.4.2.2 Interface Aérea .....	142
5.4.2.3 Flujo General del Protocolo .....	144
5.4.2.4 Inicialización .....	146
5.4.2.4.1 Modo de comunicación Pasivo .....	146
5.4.2.4.2 Modo de comunicación Activo .....	150
5.4.2.5 Protocolo de Transporte .....	151
5.4.2.5.1 Flujo de sucesos para la activación en el modo de comunicación pasivo.....	
5.4.2.5.2 Flujo de sucesos para la activación en el modo de comunicación activo .....	153
5.4.2.5.3 Comandos del Protocolo .....	154
5.4.3 Near Field Communication Interface and Protocol 2 (NFCIP-2)...	154
5.4.4 Módulo de transmisión Philips para comunicación no-contacto a 13.56 MHz .....	155
5.4.5 Interface Philips S <sup>2</sup> C para NFC.....	156

## 5.1 INTRODUCCIÓN

Una vez que hemos revisado las principales características de los diferentes sistemas RFID y su clasificación de acuerdo a las características técnicas (necesaria para entender las bases de la tecnología propuesta), vamos a entrar en este capítulo a más detalle en lo que respecta a la tecnología de tarjetas inteligentes de no-contacto, debido a que estas tarjetas son las que se ocupan principalmente para la interoperabilidad de los dispositivos handheld (PDA's, Teléfonos...etc) con la tecnología RFID de punta.

Lo anterior se lleva a cabo por algunas firmas transnacionales visionarias (Philips, Nokia, Sony...) que actualmente están empeñando muchos recursos en cuestión de desarrollo e investigación de tecnologías como el NFC (Near Field Communications) que permitan el desenvolvimiento de las características de la comunicación de este nuevo milenio, siendo congruentes con las necesidades de transporte, medios de pago, acceso a la información entre otras, que de hecho ha sido lo que ha impulsado grandemente a estos desarrollos.

A pesar de que estas tecnologías han sido enfocadas a la solución de problemas como los que se mencionaban, no quedan exentas del interés interdisciplinario de otro tipo de compañías, por supuesto que se habla de las compañías para las cuales estos desarrollos tienen algún tipo de validez en cuanto a mejoras en el servicio que ofrecen, esto además redundando en el usuario final que no tiene que saber los tecnicismos, ni el costo que han tenido estos desarrollos sino solamente es un espectador en cuanto a la forma como estos desarrollos mejoran su vida, dándole los elementos para que en este mundo que exige movilidad se pueda también tener una comunicación al nivel de los tiempos actuales en que el argumento es la información.

A continuación se mencionan tan sólo algunas de las características de las tarjetas inteligentes, observando los estándares actuales para esta tecnología, para posteriormente ahondar en el tema de la convergencia que se ha dado entre la comunicación celular de tercera generación y la tecnología RFID, visionando las características de las siguientes generaciones de comunicación.

De esta forma comenzaremos dando una mirada a lo que actualmente se está aplicando en el ambiente industrial para los dispositivos RFID, de manera tal que podremos tener una perspectiva de las conexiones de esta tecnología y el impacto que puede llegar a darse si se considera el potencial de una filosofía de comunicación global en la que se “automaticen” los medios de pago, el surtido de recetas médicas, la información de inventarios y demás situaciones que a lo largo de este tratado hemos mencionado y que veremos a más detalle a continuación.

Ya teniendo la perspectiva de todo lo anterior, podemos así dar paso al estudio de los medios por los cuales actualmente podemos hablar de la convergencia e interoperabilidad de las características de una tecnología inalámbrica para la identificación de objetos y/o bienes con las tecnologías de comunicación personal que cada vez están adaptando mayores servicios y por consiguiente anchos de banda a su infraestructura.

## 5.2 REQUERIMIENTOS RFID ACTUALES.

El crear un sistema de identificación por radiofrecuencia puede llegar a ser un reto pero también es altamente gratificante. El reto comienza cuando para implementar uno de estos sistemas se debe empezar desde cero para satisfacer una necesidad del cliente en vez de tan sólo enfocarlo a las mejoras para la eficiencia interna de un negocio. Los sistemas que son cuidadosamente planeados pueden ofrecer tanto las mejoras como la necesidad original del cliente como veremos.

### 5.2.1 ¿Que problema de negocio estoy tratando de resolver?

La primera pregunta que debe surgir al tratar de implementar cualquier tecnología para la mejora de un ambiente en específico debe ser ¿Qué problema de negocio estoy tratando de resolver?, para muchos la respuesta no va mas lejos de “mantener al cliente”, los cumplimientos de los mandatos de etiquetamiento (RFID) colocan un claro requerimiento de lo que un sistema RFID debe ser, las compañías que solamente desean cumplir con los requerimientos del cliente y no hacer ningún otro uso del RFID no necesitan preocuparse por considerar como el RFID puede mejorar el inventario, almacenaje, distribución, logística y seguridad. De cualquier manera, los mismos tags y sistemas usados para satisfacer los requerimientos del usuario, también pueden ser usados para la mejora de estas y otras operaciones. El implementar un sistema que cumpla con el etiquetamiento que necesita el cliente requerirá cambios a las operaciones, las compañías deberían usar entonces la ocasión para investigar el cómo los cambios pueden proveer algunos beneficios internos.

Algunos fabricantes de productos consideraron el etiquetamiento con código de barras en los embarques una molestia y una carga cuando las cadenas comerciales y los minoristas empezaron a requerir de estas impresiones. Hoy en día, muchos de esos mismos fabricantes ni siquiera piensan en prescindir de los códigos de barras en sus centros de distribución debido a la comprobada eficiencia que la tecnología les brinda. RFID mantiene el mismo potencial para mejorar las operaciones, el RFID no reemplazará a la tecnología de código de barras, pero puede eficientemente ampliar las prestaciones de los sistemas de colección de basados en código de barras en donde una visibilidad adicional o proceso automatizado es deseable.

Muchas compañías cumplirán con los requerimientos de etiquetamiento con *etiquetas inteligentes*, que consisten, como se ha dicho, del RFID inlay (la combinación de la antena y el chip) contenidos en una etiqueta adhesiva. Las impresoras de etiquetas inteligentes codifican el chip RFID dentro el material de la etiqueta y pueden imprimir texto, códigos de barras y gráficas por la parte de afuera. Cabe destacar que las compañías que están forjando las iniciativas de etiquetamiento RFID no están diciendo que ésta misma tecnología reemplazará a los códigos de barras, sino por lo contrario opinan que *la información visible al ser humano* y los datos en código de barras requieren caminar juntos haciendo del RFID una excelente y obvia elección con la cual comenzar el etiquetamiento de radiofrecuencia.

---

### 5.2.2 ¿Cuál es la diferencia entre RFID y el código de barras?

Es importante el comprender las diferencias significativas entre la tecnología RFID y la de código de barras para apreciar los beneficios que la identificación por radiofrecuencia puede ofrecer. El código de barras y el RFID son ambas tecnologías de identificación que retienen datos que son accesados después por algún tipo de lector. En la actualidad ambas tecnologías se complementan muy bien una a otra y pueden ser usadas efectivamente en conjunto para muchas aplicaciones. El código de barras es una tecnología óptica, mientras que el RFID es una tecnología de radio, la formas en las que estas tecnologías transfieren datos nos marca muchas de las diferencias entre el RFID y el código de barras y nos ayuda a determinar donde se aplica mejor cada una de estas tecnologías.

Como cualquier tecnología de radio el RFID no requiere de la línea de vista entre el lector y el transponder para su operación. Los tags RFID entonces pueden leer a través de empaques que incluyen empaques de cartón y el plástico. El RFID está sujeto a interferencia de cualquier manera, particularmente del metal, de manera que potenciales fuentes de interferencia pueden ser reconocidas y se deben tomar en cuenta a la hora de la planeación.

A causa de que no se requiere línea de vista, los objetos etiquetados pueden ser leídos indistintamente de su orientación por medio del uso de sistemas RFID optimizados. Los objetos no tienen que ser colocados forzosamente con la cara hacia arriba sobre los contenedores para poder ser leídos, solucionando así el problema del mal manejo de éstos. Si los trabajadores suelen colocar los objetos en los contenedores, serán mas productivos si no tienen que posicionar y alinear las etiquetas cuando manejan los objetos.

Los lectores RFID automáticamente pueden reconocer y diferenciar todas las etiquetas RF en su campo de lectura. Esta capacidad de *procesamiento simultáneo* provee de flexibilidad adicional para el manejo de materiales, empacamiento y una suerte de operaciones más debido a que no se necesita mantener un espaciamiento entre los objetos para asegurar que serán leídos. La habilidad de leer docenas o incluso cientos de etiquetas por segundo hace al RFID ideal para aplicaciones de alta velocidad de recepción entre otras. La *capacidad de datos* de las etiquetas RFID les permite el almacenaje de la misma información que los códigos de barras e incluso más. Tal como el código de barras, los tags RFID están disponibles con diferentes tamaños de memoria y opciones de codificación.

### 5.2.3 ¿Qué buena razón tengo para usar el RFID?

Los usuarios pueden tomar ventajas de las características de rendimiento RFID para crear sistemas de lectura y de organización que trabajan con intervención mínima de operador o no requieren de operadores. Los rasgos del RFID son especialmente valorados en las aplicaciones de alta velocidad y operaciones de línea de producción en donde la labor manual es usualmente la mayor de las limitaciones en la velocidad de caudal y precisión en el procesamiento. Para algunas ideas de cómo el RFID puede mejorar un negocio, se deben revisar las operaciones para determinar si existe algún punto de choque característico o procesos que requieran del excesivo manejo humano, como por ejemplo el colocar etiquetas de una cierta forma en un contenedor, todos estos problemas deben ser candidatos

a ser automatizados con el RFID, el cual puede proveer de una buena retribución en investigación ya que reduce los requerimientos de labor y mejora la eficiencia.

Existen muchas posibilidades para tomar ventaja del manejo desatendido y una de las mas prometedoras es para el monitoreo desatendido, por ejemplo los fabricantes pueden usar el RFID para reducir su trabajo de inventario un 10% de acuerdo a un estudio de una firma consultora –Accenture-. Los lectores RFID se pueden colocar estratégicamente, tanto ocultos como visiblemente para hacer zonas de seguridad con algunas facilidades. Los lectores pueden constantemente y a discreción monitorear el inventariado de los bienes terminados, componentes, herramientas, equipamiento y otros objetos de valor por medio de la lectura de las etiquetas en todos los objetos dentro de la zona de lectura. Las etiquetas en los objetos pueden disparar alarmas o una notificación discreta a un supervisor si intentan un removimiento de las mismas sin autorización.

#### **5.2.4 ¿Cuales son los beneficios para mi negocio?**

El etiquetamiento RFID puede producir diferentes beneficios al mismo tiempo que le permite mantener sus clientes. Los lineamientos del etiquetamiento están creciendo para una variedad de industrias ya que las organizaciones se han convencido que el RFID puede reducir la distribución y los costos de manejo, además de reducir los niveles de inventario por medio de una mejora en la “visibilidad”. Estos beneficios están disponibles para las compañías que deben proveer de bienes ya etiquetados para los clientes que las reciben y que también lo necesitan. Esto ha sido comprobado una y otra vez con diferentes lineamientos para códigos de barras, y se cree que mejoras en la eficiencia de procesos se pueden lograr al usar el RFID.

Existen muchas formas en que las compañías que están etiquetando pueden satisfacer los requerimientos de estándar para tomar ventaja también de la etiquetas RFID para operaciones internas. La mejor aproximación es el empezar a evaluar una aplicación sencilla y pequeña y expandirla posteriormente ya que los beneficios y la experiencia hayan sido obtenidos, de cualquier manera haciendo siempre las observaciones cuidadosas de las actividades de fuera de su organización para ver hacia donde se mueven las tendencias en la industria, especialmente con respecto a la selección de tecnología y estándares. El RFID puede potencialmente beneficiar a cualquier proceso en donde los artículos deban ser identificados, rastreados o movidos. Una solución sería trabajar como respaldo en donde las etiquetas se necesiten aplicar para encontrar los lugares mas fáciles y lógicos para así empezar el uso interno.

El área de envío podría ser un buen lugar para empezar, debido a que muchas de las compañías podrían imprimir y aplicar las etiquetas justo antes del envío. Como sean cargados los embarques, los tags RFID en estuches, cartones y paletas de madera se podrán leer para desactivar los artículos y construir un documento de envío. Si se hace interface entre el sistema RFID y las aplicaciones de envío o de administración de órdenes, los embarques se pueden verificar para tener una exactitud usando los lectores RFID para asegurar que todos los artículos que se requerían hayan sido cargados en la cantidad exacta. Procesos similares se pueden desarrollar para apresurar la entrega y recepción.

---

Actualmente muchas organizaciones manejan la verificación de envíos por medio del escaneo de las etiquetas en código de barras y se debe esperar que sean cargados los artículos, lo cual previene de algunos errores. El cambiar a una verificación basada en RFID permitiría a los embarques ser procesados más rápido ya que los lectores de radiofrecuencia pueden capturar datos de docenas de empaques simultáneamente indiferentemente de su orientación. La verificación por código de barras de los embarques requiere de operadores para escanear cada etiqueta, lo que da pie a la posibilidad de que los artículos puedan extraviarse y no se tomen en cuenta por la misma razón.

Haciendo tan sólo una mejora pequeña e incremental a la exactitud del envío puede producir grandes beneficios, tal como el siguiente cálculo lo ilustra. Varios análisis han establecido que los errores de envío le cuestan a las empresas entre \$600 y \$2500 para resolverlos, dependiendo de las proporciones de labor, costos de envío y la cantidad de tiempo de oficina y administrativo que sea necesario. Por consiguiente, cada mejora del 1% en la exactitud del envío podría reducir los gastos de envío entre \$600 y \$2,500 por cada 100 embarques. Para una compañía que embarca 100 ordenes diario, cada mejora del 1% en exactitud del embarque produciría ahorros anuales de entre \$156,000 y \$650,000.

Procesos similares podrían ser implementados en el lado de la recepción de mercancía para mantener la exactitud del inventario y reducir los requerimientos de labores. Se debe considerar que si se usa el RFID en el nivel de cartón o estuche, la recepción puede ser manejada, salvo excepciones, con reportes automáticos de lo que haya sido recibido y comparándolos con la información recibida en una notificación de embarque previamente recibida, en vez del laborioso escaneo de un estuche o cartón a la vez.

La verificación de embarque es sólo una manera en que los fabricantes pueden tomar ventaja del etiquetamiento RFID aplicados a satisfacer las necesidades del cliente. Los fabricantes pueden ganar en lo descrito en cuanto a seguridad y beneficios de reducción (tiempos, labores...) si etiquetan el inventario de los bienes finalizados o crean un sistema de seguridad para monitorear las puertas de los muelles y otros puntos de salida. Las etiquetas RFID se pueden usar como una forma de autenticación para encarar al creciente problema de la falsificación, de lo cual la Cámara de Comercio Internacional estima sumas del 8% del comercio global. Las etiquetas inteligentes en empaques proveen de un método para auditar los canales de distribución para detectar embarques falsos o desviados. Las etiquetas en los productos pueden proveer de una autenticación mas avanzada y una forma de verificar la elegibilidad para garantizar el servicio.

La EPC global, una organización formada para comercializar y dar soporte al sistema RFID de código electrónico de producto (EPC) que se desarrolló originalmente en el centro MIT Auto-ID, ofrece una serie de casos de negocios sobre RFID y sus análisis en su página web [www.epcglobalinc.org](http://www.epcglobalinc.org). Resulta de particular interés un estudio titulado "*Auto-ID On Demand: The Value of Auto-ID Technology in Consumer Packaged Goods Demand Planning*". Este estudio encuentra que los sistemas RFID pueden mejorar la planeación de la demanda previendo la exactitud para el consumidor y los productos empacados por el fabricante en un 10 a 20 por ciento. Otros beneficios proyectados incluyen un 10 a 30 por ciento de reducción en los niveles de requerimiento de inventario y un 1 a 2 por ciento en mejoras en ventas atribuible a la reducción de los apilamientos de artículos. Otros estudios

en esa serie ilustran diferentes maneras en que las compañías se pueden beneficiar del etiquetamiento RFID a través de la cadena de abastecimiento.

Muchas compañías de mala gana tuvieron su primera experiencia con los códigos de barra y los sistemas electrónicos de comercio en respuesta a las necesidades del cliente por las etiquetas de barras y las comunicaciones EDI. Los abastecedores comúnmente resentían estos programas y eran escépticos de los beneficios con los que podían contar, pero al transcurrir el tiempo aprendieron como tomar ventaja de estos para las operaciones internas. Esos primeros sistemas de cumplimiento en etiquetamiento y sistemas EDI se volvieron los fundamentos para muchas de los sistemas altamente eficientes de captura de datos y sistemas de comunicación en la cadena de abastecimiento de hoy en día. El RFID seguirá una evolución similar y los pioneros en adoptarla alcanzarán los mejores beneficios.

### **5.2.5 ¿Cuáles estándares y consideraciones regulatorias aplicar?**

Los distribuidores en cumplimiento con las relaciones de etiquetamiento deben cumplir con las necesidades de rendimiento en etiquetamiento del cliente y los requerimientos de datos, además cumplir con todas las regulaciones internacionales relevantes que gobiernan los dispositivos electrónicos y las comunicaciones de radio. Afortunadamente, estos requerimientos raramente se contradicen uno al otro, aunque deben ser revisados cada vez que las operaciones RFID sean extendidas dentro de diferentes países. Así como en las etiquetas en código de barras para envío, las compañías deben desarrollar formatos de cumplimiento de propietario o requerimientos base en estándares internacionales o industriales.

Los dos programas más grandes de etiquetamiento anunciados a la fecha –por el líder mundial de las cadenas comerciales y el departamento de defensa de los Estados Unidos– especifican el uso de tecnología EPC RFID. Se cree que otros de los grandes usuarios finales como Metro AG, el líder alemán de cadenas comerciales, quienes han recientemente anunciado su intento por desplegar RFID para el rastreo de cartón y paletas de madera, se adoptarán las especificaciones y estándares que se están desarrollando por el EPCglobal. Al respecto de los sistemas de identificación automática y captura de datos, el sistema EPC define estructuras de datos para producir números ID (de identificación) únicos y además define las especificaciones técnicas para las comunicaciones lector a etiqueta y el rendimiento de la etiqueta (o el subsistema lector). El sistema EPC (*Electronic Product Code*) asigna un número ID a cada etiqueta para identificar únicamente al artículo etiquetado. El código EPC sirve como un número serial o un certificado virtual de nacimiento y puede usarse para identificar para distinguir un artículo (que puede ser una paleta, estuche, cartón o un producto individual) de otros similares.

El EPC es un “código de licencia de placa”, el cual no describe el artículo o a su propietario, sino que provee de un único identificador para las bases de datos que almacenan la información, así como las placas de licencia en automóviles. Los códigos EPC son similares en estructura a los códigos estandarizados bajo el sistema EAN.UCC, el cual es la base de mucho del comercio global y que es creado y mantenido por EAN (European Article Number) Internacional y el Uniform Code Council (UCC).

---

El identificador único es la base del sistema EPC y es una constante en todas las especificaciones EPC. Lo anterior representa una buena diferencia de los sistemas de identificación EAN.UCC ya que estos pertenecen al comercio del menudeo, el cual incluye los códigos de barras UPC/EAN usados en los bienes del consumidor alrededor del globo. Los símbolos UPC/EAN típicamente solo identifican al fabricante y al tipo de producto. Si el producto es una escoba, cada instancia de esa escoba hecha por el fabricante tendrá el mismo número UPC. En el sistema EPC, cada escoba tendría un único número de identificación ID, el cual facilitará el rastreo a nivel de artículo. La identificación única también es útil para la trazabilidad, beneficia en autorización y procesamiento, garantizar y administración de servicio y más. Lo último muy útil para el tipo de aplicaciones que estaremos tratando en este capítulo en lo que respecta a las comunicaciones NFC y lo que podrían ser las transacciones de productos en supermercados, posters...etc, como veremos mas adelante.

Las especificaciones EPC difieren en las frecuencias operativas, funcionalidad de la etiqueta y protocolos de comunicación. Para tests pilotos, el líder de minoristas esta permitiendo a sus proveedores el usar la banda UHF (860-930 MHz) versiones EPC tanto de etiquetas Clase 0 ó Clase 1. Los Clase 0 son etiquetas de sólo lectura que operan en la banda mencionada anteriormente. Las etiquetas de Clase 1 se pueden escribir hasta una vez después de que son programadas en la fábrica, pero operan en la misma banda de frecuencia que la Clase 0.

Existen diferentes versiones (también conocidas como generaciones) de especificaciones EPC en adición a las diferentes clases. Las especificaciones, estándares y terminología están continuamente siendo actualizados. Para asegurar el cumplimiento con los requerimientos de los clientes, se debe considerar las especificaciones y otra documentación de programa provista por el propio cliente como la guía a la que se debe apegar más.

En adición a cubrir las necesidades del cliente, los sistemas RFID deben cumplir con todas las regulaciones establecidas. Los gobiernos regulan las frecuencias disponibles, potencias de salida, emisiones y otras características de rendimiento. Las regulaciones RFID caen bajo la autoridad de la Comisión Federal de Telecomunicaciones en México y otros muchos cuerpos alrededor del mundo.

Los estándares RFID creados por la Organización Internacional de Estandarización (ISO) cumplen con todos los requerimientos regulatorios de manera que los usuarios pueden asegurar que sus sistemas están disponibles para uso mundial. De cualquier forma, los requerimientos RFID hechos por compañías de forma individual pueden no cumplir con los estándares ISO y pueden no ser convenientes para su uso extendido. Los estándares ISO de la serie 18000 se están empezando a considerar para muchas cadenas comerciales y sistemas de etiquetamiento. El ISO 18000-parte 6 se ha ratificado ya como un estándar para el RFID en la banda de 860-930 MHz. Otro número de estándares RFID ISO se han ratificado (con la serie 18000 como la más apropiada para aplicaciones de identificación de artículos). Muchos estándares más están por venir una vez que se tenga un consenso final.

Las especificaciones EPC están ahora en el proceso de ser convertidas en estándares, debido a los procesos, bajo el auspicio de EPCglobal el cual es una unión con el sistema de barras UPC/EAN usados en los bienes de consumo alrededor del mundo. De esta forma EPCglobal esta idealmente posicionado y equipado para comercializar y estandarizar las especificaciones técnicas EPC, las estructuras de datos las guías de uso y continúa el desarrollo.

### **5.2.6 ¿Qué cambios a la infraestructura de sistemas informáticos se requieren para usar RFID?**

El RFID podría cambiar mas que la manera en que se recuperan los datos, también debe proveer de nuevas tipos de información ejecutable que cree las oportunidades para hacer las cosas de diferente forma y más eficientemente. El RFID puede dar visibilidad dentro de las operaciones que antes eran inaccesibles debido a las limitaciones del código de barras y otras tecnologías de colección de datos. Las organizaciones pueden así tomar ventaja de la habilidad de seguimiento de artículos en más lugares, sin la intervención humana, para crear nuevas características y aplicaciones. Estas capacidades son de alguna forma nuevas, así que la aplicaciones software también se necesitan modificar o desarrolladas para tomar ventaja de ello, y la infraestructura de telecomunicaciones podría ser extendida para soportar las operaciones RFID.

Los lectores RFID pueden detectar automáticamente e identificar todas las etiquetas que se encuentren en su rango de lectura, lo que puede potencialmente producir cientos de lecturas por segundo. Cada lectura representando un punto de datos que el sistema de información empresarial pueda necesitar procesar. De ahí que la identificación de datos y los datos de identificación evento-relación (como el tiempo y ubicación) necesitarán ser intercalados y filtrados usando reglas flexibles, antes que empezar a orillarlos a una aplicación de negocios o sometidos en respuesta a una necesidad de datos. Por otra parte, el sistema RFID puede producir muchos datos y no la suficiente calidad de información.

Middleware (software de marca registrada) se ha desarrollado específicamente para soportar los sistemas RFID y filtrar datos para los sistemas de información de legado (que se encontraban ya en operación) y las aplicaciones software. Algunos proveedores líderes en software ERP (enterprise resource planning) y WMS (warehouse management system) también ofrecen Middleware u otros módulos de software para soportar el uso del RFID con sus aplicaciones. El software de etiquetamiento podría también ser modificado como discutiremos a continuación.

### **5.2.7 ¿Qué cambios a los procesos de etiquetado y empaquetado debo tener en cuenta para cumplir con los requerimientos?**

Las etiquetas inteligentes pueden ser aplicadas para cumplir con los más actuales requerimientos de etiquetado, las etiquetas inteligentes son una opción conveniente, ya que se pueden producir sobre demanda y una etiqueta sencilla puede cumplir con los requerimientos RFID, código de barras y de marcado de texto. De cualquier manera se deben hacer mas cosas para cumplir con el etiquetamiento que sólo imprimir un nuevo tipo

---

de etiqueta de envío, los dictámenes exitosamente satisfactorios en el etiquetamiento requieren además de planeación para la codificación de la etiqueta, selección de medio RFID, colocación del etiquetado y los cambios al software.

Un impresor/codificador de etiquetas inteligentes programa la etiqueta RFID que se adjunta a la etiqueta inteligente de manera efectiva mientras que la misma se imprime, todo esto extiende la flexibilidad de impresión sobre demanda para cumplir las necesidades de codificación. Información variable, como números de orden, notificaciones...etc, pueden ser convenientemente codificados e impresos sobre demanda con impresoras para etiquetas inteligentes. Las impresoras térmicas se usan también para el etiquetamiento inteligente, estas impresoras están disponibles como las tradicionales impresoras de etiquetas o máquinas de impresión para su uso con aplicadores automáticos para integrarse en una variedad de procesos de empaque y etiquetamiento de embarque. El software de etiquetamiento necesitará ser agregado o modificado para soportar el etiquetamiento inteligente y la codificación RFID.

Lo que se debe siempre considerar es que para cumplir con el buen etiquetamiento, los proveedores pueden cambiar el lugar en donde colocan las etiquetas en los paquetes ya sea de cartón o madera, debido a que la tecnología de RFID es obviamente una tecnología de radio por lo que está sujeta a algunas perturbaciones en la señal, particularmente debido a metales ya que éstos reflejan las señales, y los líquidos que las absorben. Colocando las etiquetas en diferentes áreas de los empaques puede influir en el rendimiento del lector, además del tamaño de la etiqueta, la frecuencia y la orientación de la misma, todo esto afecta y podría necesitar de ajustes para etiquetar diferentes tipos de objetos.

Las organizaciones podrían necesitar utilizar diferentes tipos de etiquetas inteligentes para la identificación de diferentes objetos o para lidiar con las incompatibles especificaciones de diferentes clientes. En esa situación, es muy importante que las impresoras puedan soportar todos los medios requeridos y los procedimientos se establezcan para prevenir a estos mismos medios de ser usados en intercambio.

Los procesos deben además establecerse para prevenir que las etiquetas que no se pueden leer o erróneas sean colocadas a los embarques. Las etiquetas inteligentes ocasionalmente no se leen debido a componentes defectuosos o daño constante durante su manejo y a veces la información codificada está incompleta o no es muy exacta. Estos problemas son indetectables la mayoría de veces a menos que la etiqueta sea leída después de su impresión para validar la legibilidad y el contenido. Si los problemas se detectan, los procesos se deben llevar a cabo para desviar la etiqueta y prevenir así futuras fallas, hasta que el problema sea resuelto.

### **5.2.8 ¿Qué tipo de pruebas antes de la aplicación se requieren?**

Los proyectos piloto y las pruebas pre-despliegue deben descubrir cualquier problema de interferencia, calidad o rendimiento que necesite ser resuelto antes de que el sistema sea desplegado. Así como con cualquier sistema de etiquetamiento, el medio y adhesivo deben soportar todas las condiciones de ambiente y uso a las que la etiqueta será expuesta a través

de la cadena de abastecimiento. Es crucial el probar todos los diferentes artículos que serán etiquetados bajo tantas condiciones como sea posible para asegurar el correcto funcionamiento.

En adición a las condiciones de prueba discutidas anteriormente, una serie de pruebas a gran escala se deben conducir para determinar si el sistema de etiquetamiento inteligente puede mantenerse a la par de los requerimientos de volumen de etiquetado durante las peores condiciones para garantizarlos también en condiciones normales. Las etiquetas inteligentes toman un poco más de tiempo en producirse que las etiquetas normales de envío, y en un ambiente de etiquetado automatizado a alta velocidad, esto se debe considerar para asegurar la adecuada capacidad de caudal informático.

Algunas pruebas más extensivamente funcionales se requerirían si el RFID se usara para operaciones internas. La interferencia es la principal preocupación; un proveedor de soluciones experimentado en RFID puede dar una valoración de la potencial interferencia y sugerir remedios al respecto, la valoración es similar a la supervisión de sitio que se lleva a cabo antes de que una red LAN inalámbrica sea instalada. La interferencia se puede prevenir o mitigar usando diferentes tipos o tamaños de antenas RFID y etiquetas, y experimentando con diferentes frecuencias, niveles de potencia de salida y opciones de montaje de tags, todo con el objetivo definido por los requerimientos de la aplicación. No hay que olvidar, si lo que conduce al uso del RFID para operaciones internas es una directiva generada externamente para el etiquetamiento, entonces ciertas elecciones que usted de otra forma podría elegir libremente ya estarán definidas.

Con el RFID tal vez no se puedan hacer muchas pruebas, existen muchas variables para probar y contingencias que planear. Los puntos muertos, donde la lectura de etiquetas no es posible, pueden aparecer misteriosamente un día en un almacén y al siguiente, desaparecer debido a los diferentes materiales que se encuentran en los estantes donde los productos etiquetados descansan. Las pruebas pueden no revelar cada barrera, pero a través de una completa planeación se pueden superar estos problemas.

Como conclusión podríamos decir que el implementar un sistema completo de RFID puede parecer sumamente intimidante, pero es muy manejable cuando se tiene un claro entendimiento de los requerimientos y opciones. Lo que se ha presentado aquí nos dan un excelente punto de partida desde el cual podemos empezar a identificar las áreas para futura investigación y desarrollar preguntas específicas para avanzar en un proyecto, aunque no es la intención principal de este capítulo, sin embargo se ha tomado en cuenta ya que nos ofrece una visión de lo que puede interactuar en cierta forma con nuestra vida y principalmente para ubicar a la tecnología NFC de Philips como tal en el amplio contexto RFID. Regresando a lo anterior y ya por último hay que decir que el mantener una buena comunicación con los clientes, los demás comerciantes, los proveedores de tecnología y los departamentos internos afectados por los cambios y permitiendo un largo periodo para que se asiente el sistema (periodo de pruebas y refinamiento), nos conducirá a hacer un proyecto exitoso.

Una vez que hemos analizado lo que se debe preguntar una empresa para implementar RFID, veremos a continuación el como lo implementan actualmente, el potencial de

mercado para el RFID y por qué se ha convertido en una punta de lanza para tecnologías como el NFC que estará facilitando mucha de la actividad comercial en los siguientes años.

### 5.3 LAS APLICACIONES RFID

Las etiquetas RFID de baja frecuencia se utilizan comúnmente para la identificación de animales, seguimiento de barricas de cerveza, y como llave de automóviles con sistema antirrobo. En ocasiones se insertan en pequeños chips en mascotas, para que puedan ser devueltas a su dueño en caso de pérdida. En los Estados Unidos se utilizan dos frecuencias para RFID: 125 kHz (el estándar original) y 134,5 kHz, el estándar internacional. Las etiquetas RFID de alta frecuencia se utilizan en bibliotecas y seguimiento de libros, seguimiento de pallet, control de acceso en edificios, seguimiento de equipaje en aerolíneas y seguimiento de artículos de ropa. Un uso extendido de las etiquetas de alta frecuencia como identificación de insignias, substituyendo a las anteriores tarjetas de banda magnética. Sólo es necesario acercar estas insignias a un lector para autenticar al portador.

Las etiquetas RFID de UHF se utilizan comúnmente de forma comercial en seguimiento de pallets y envases, y seguimiento de camiones y remolques en envíos. Las etiquetas RFID de microondas se utilizan en el control de acceso en vehículos de gama alta.

Algunas autopistas, como por ejemplo la *FasTrak* de California, el sistema *I-Pass* de Illinois y la *Philippines South Luzon Expressway E-Pass* utilizan etiquetas RFID para recaudación con peaje electrónico. Las tarjetas son leídas mientras los vehículos pasan; la información se utiliza para descontar el peaje de una cuenta prepago. El sistema ayuda a disminuir el tráfico causado por las cabinas de peaje (fig 5.1).



**Fig. 5.1 Una etiqueta RFID empleada para la recaudación de peaje electrónico**

Sensores como los sísmicos pueden ser leídos empleando transmisores-receptores RFID, simplificando enormemente la recolección de datos remotos.

En enero de 2003, *Michelin* anunció que había comenzado a probar transmisores-receptores RFID insertados en neumáticos. Después de un período de prueba estimado de 18 meses, el fabricante ofrecerá neumáticos con RFID a los fabricantes de automóviles. Su principal objetivo es el seguimiento de neumáticos en cumplimiento con la *United States Transportation, Recall, Enhancement, Accountability and Documentation Act* (TREAD Act).

Las tarjetas con chips RFID integrados se usan ampliamente como dinero electrónico, como por ejemplo la tarjeta *Octopus* en Hong-Kong y en los Países Bajos como forma de pago en transporte público y ventas menores.

Comenzando con el modelo de 2004, está disponible una "llave inteligente" como opción en el *Toyota Prius* y algunos modelos de *Lexus*. La llave emplea un circuito de RFID activo que permite que el automóvil reconozca la presencia de la llave a un metro del sensor. El conductor puede abrir las puertas y arrancar el automóvil mientras la llave sigue estando en la cartera o en el bolsillo.

En agosto de 2004, el Departamento de Rehabilitación y Corrección de Ohio (ODRH) aprobó un contrato de 415.000 dólares para ensayar la tecnología de seguimiento con *Alanco Technologies* en cárceles. Los internos portan unos transmisores del tamaño de un reloj de muñeca que puede detectar si los presos han estado intentando quitárselas y enviar una alarma a los ordenadores de la prisión. Este proyecto no es el primero que trabaja en el desarrollo de chips de seguimiento en prisiones estadounidenses. Instalaciones en Michigan, California e Illinois emplean ya esta tecnología.

Los chips RFID implantables, diseñados originalmente para el etiquetado de animales se están utilizando y se está contemplando también para los seres humanos. *Applied Digital Solutions* propone su chip "*unique under-the-skin format*" (formato bajo-la-piel único) como solución a la usurpación de la identidad, al acceso seguro a un edificio, al acceso a un ordenador, al almacenamiento de expedientes médicos, a iniciativas de anti-secuestro y a una variedad de aplicaciones. Combinado con los sensores para supervisar diversas funciones del cuerpo, el dispositivo *Digital Angel* podría proporcionar supervisión de los pacientes. El Baja Beach Club en Barcelona (España) utiliza un *Verichip* implantable para identificar a sus clientes VIP, que lo utilizan para pagar las bebidas. El departamento de policía de Ciudad de México ha implantado el *Verichip* a unos 170 de sus oficiales de policía, para permitir el acceso a las bases de datos de la policía y para poder seguirlos en caso de ser secuestrados.

Amal Graafstra, un empresario natural del estado de Washington, tenía un chip RFID implantado en su mano izquierda a principios de 2005. El chip medía 12 mm de largo por 2 milímetros de diámetro y tenía un radio de acción para su lectura de dos pulgadas (50 milímetros). La implantación fue realizada por un cirujano plástico, aunque el nombre del doctor no fue develado. Cuando le preguntaron qué pretendía hacer con el implante, Graafstra respondió: "estoy escribiendo mi propio software y estoy soldando sobre mi propia materia, prácticamente esto es lo que deseo. Bueno, de forma más precisa, algo que tengo el tiempo y la inspiración para poder hacerlo. En última instancia sin embargo, pienso

que el verdadero acceso sin llave requerirá un chip implantable con un sistema muy fuerte de cifrado; ahora tan sólo veo este tipo de cosas en un contexto personal."

### **5.3.1 Aplicaciones potenciales**

Las etiquetas RFID se ven como una alternativa que reemplazará a los códigos de barras UPC o EAN , puesto que tiene un número de ventajas importantes sobre la arcaica tecnología de código de barras. Quizás no logren sustituir en su totalidad a los códigos de barras, debidos en parte a su coste relativamente más alto. Para algunos artículos con un coste más bajo la capacidad de cada etiqueta de ser única se puede considerar exagerado, aunque tendría algunas ventajas tales como una mayor facilidad para llevar a cabo inventarios.

También se debe reconocer que el almacenamiento de los datos asociados al seguimiento de las mercancías a nivel de artículo ocuparía muchos terabytes. Es mucho más probable que las mercancías sean seguidas a nivel de pallet usando etiquetas RFID, y a nivel de artículo con producto único, en lugar de códigos de barras únicos por artículo.

Los códigos RFID son tan largos que cada etiqueta RFID puede tener un código único, mientras que los códigos UPC actuales se limitan a un solo código para todos los casos de un producto particular. La unicidad de las etiquetas RFID significa que un producto puede ser seguido individualmente mientras se mueve de lugar en lugar, terminando finalmente en manos del consumidor. Esto puede ayudar a las compañías a combatir el hurto y otras formas de pérdida del producto. También se ha propuesto utilizar RFID para comprobación de almacén desde el punto de venta, y sustituir así al encargado de la caja por un sistema automático que no necesite ninguna captación de códigos de barras. Sin embargo no es probable que esto sea posible sin una reducción significativa en el coste de las etiquetas actuales. Se está llevando a cabo una investigación sobre la tinta que se puede utilizar como etiqueta RFID, que reduciría costes de forma significativa. Sin embargo, faltan todavía algunos años para que esto dé sus frutos.

#### **5.3.1.1 Gen 2**

Una organización llamada EPCglobal está trabajando en un estándar internacional para el uso de RFID y EPC en la identificación de cualquier artículo en la cadena de suministro para las compañías de cualquier tipo de industria, en cualquier lugar del mundo. El consejo superior de la organización incluye representantes de *EAN International*, *Uniform Code Council*, *The Gillette Company*, *Procter & Gamble*, *Wal-Mart*, *Hewlett-Packard*, *Johnson & Johnson*, *Checkpoint Systems* and *Auto-ID Labs*. Algunos sistemas RFID utilizan estándares alternativos basados en la clasificación ISO 18000-6.

El estándar gen 2 de EPCglobal fue aprobado en diciembre de 2004, y es probable que llegue a formar la espina dorsal de los estándares en etiquetas RFID de ahora en adelante. Esto fue aprobado después de una contención de *Intermec* por la posibilidad de que el estándar pudiera infringir varias patentes suyas relacionadas con RFID. Se decidió que el estándar en sí mismo no infringía sus patentes, sino que puede ser necesario pagar derechos

a Intermec si la etiqueta se leyera de un modo particular. EPC Gen2 es la abreviatura de "EPCglobal UHF Generation 2".

### **5.3.1.2 Identificación de pacientes**

En julio de 2004, la *Food and Drug Administration* (Administración de Comida y Medicamentos) hizo pública la decisión de comenzar un proceso de estudio que determinará si los hospitales pueden utilizar sistemas RFID para identificar a pacientes y/o para permitir el acceso por parte del personal relevante del hospital a los expedientes médicos. El uso de RFID para prevenir mezclas entre esperma y óvulos en las clínicas de fecundación in vitro también está siendo considerado. Además, la FDA aprobó recientemente los primeros chips RFID de EE.UU. que se pueden implantar en seres humanos. Los chips RFID de 134,2kHz, de VeriChip Corp., una subsidiaria de Applied Digital Solutions Inc., pueden incorporar información médica personal y podrían salvar vidas y limitar lesiones causadas por errores en tratamientos médicos, según la compañía. La aprobación por parte de la FDA fue divulgada durante una conferencia telefónica con los inversionistas. También se ha propuesto su aplicación en el hogar, para permitir, por ejemplo, que un frigorífico pueda conocer las fechas de caducidad de los alimentos que contiene, pero ha habido pocos avances más allá de simples prototipos.

### **5.3.1.3 Tráfico**

Otra aplicación propuesta es el uso de RFID para señales de tráfico inteligentes en la carretera (Road Beacon System o RBS).

## **5.3.2 TARJETAS INTELIGENTES**

Una tarjeta inteligente es un sistema electrónico de almacenamiento de datos, posiblemente con capacidad adicional de cómputo (tarjeta de microprocesador), las cuales por conveniencia se incorporan dentro de una tarjeta plástica del tamaño de una tarjeta de crédito. Las primeras tarjetas inteligentes en forma de tarjetas telefónicas de prepago se lanzaron en 1984. Las tarjetas inteligentes son colocadas en un lector el cual hace una conexión galvánica a la superficie de contacto de la tarjeta inteligente que usa conectores también (para el caso de las de contacto), la tarjeta inteligente es alimentada con energía y pulsos de reloj desde el lector vía las superficies de contacto. La transferencia de datos entre el lector y la tarjeta toma lugar usando una interface serial bidireccional (I/O port), es posible el diferenciar entre los dos tipos básicos de tarjetas inteligentes basándose en la funcionalidad interna de los mismos, así tenemos: la tarjeta de memoria y la tarjeta de microprocesador.

Una de las principales ventajas de la tarjeta inteligente es el hecho de que los datos almacenados en ella se pueden proteger contra acceso no deseado (lectura) y manipulación. Las tarjetas inteligentes hacen de todos los servicios que se relacionan con la información u operaciones financieras más simples, seguros y baratos, por esta razón, 200 millones de tarjetas inteligentes se emitieron mundialmente en 1992, para 1995 esta figura se elevó a 600 millones de los cuales 500 millones eran tarjetas de memoria y 100 millones eran

tarjetas de microprocesador. El mercado de tarjetas inteligentes entonces representa uno de los subsectores de crecimiento rápido en la industria de la microelectrónica.

Una desventaja de las tarjetas inteligentes de contacto es la vulnerabilidad de los contactos a la portación, corrosión y suciedad. Los lectores que se usan frecuentemente son caros para mantener debido a su tendencia al mal funcionamiento. En adición, los lectores que son accesibles al público (casetas telefónicas) no se pueden proteger contra el vandalismo.

### **Tarjetas de Memoria**

En las tarjetas de memoria, la memoria (usualmente una EEPROM) es accesada usando una lógica secuencial (máquina de estado). Es también posible el incorporar algoritmos de seguridad simple para el uso de este sistema. La funcionalidad de la tarjeta de memoria en cuestión es optimizada usualmente para una aplicación específica. La flexibilidad de la aplicación es altamente limitada pero, por otro lado, las tarjetas de memoria son muy económicas, por esta razón, estas tarjetas son utilizadas predominantemente aplicaciones sensibles al precio, de gran escala.

### **Tarjetas de Microprocesador**

Como sugiere su nombre, estas tarjetas contienen un microprocesador, el cual es conectado a una memoria segmentada (segmentos ROM, RAM y EEPROM).

La máscara ROM programada incorpora un sistema operativo para el microprocesador y es insertada durante la manufactura del chip. Los contenidos de ROM son determinados durante ésta etapa, son idénticos para todos los microchips del mismo lote de producción y no pueden ser sobrescritos.

Los chip EEPROM contienen datos de aplicación y un código de programa relacionado. La lectura o escritura a esta área de memoria es controlada por el sistema operativo.

La RAM es la memoria de trabajo temporal del microprocesador, los datos almacenados en ella se pierden cuando el voltaje de alimentación se desconecta o se pierde.

Las tarjetas e microprocesador son muy flexibles, en los modernos sistemas de tarjetas inteligentes es además posible el integrar diferentes aplicaciones en una tarjeta sencilla (multi-aplicación). Las partes específicas de aplicación del programa no se cargan dentro de la EEPROM sino hasta después de su manufactura y se pueden iniciar vía sistema operativo.

Las tarjetas de microprocesador son principalmente usadas en aplicaciones sensibles a la seguridad, algunos ejemplos son las tarjetas inteligentes para teléfonos móviles GSM y las tarjetas EC (electronic cash). La opción de programar las tarjetas de microprocesador también facilitan la rápida adaptación a nuevas aplicaciones.

### 5.3.3 Aplicaciones Específicas para Tarjetas Inteligentes

Ya que hemos visto el panorama RFID de forma global y generalizada en cuanto a los rangos para cada sistema, las frecuencias, y que tenemos en mente los campos en los que el RFID ha incursionado con éxito (dejando de lado otras muchas aplicaciones), vamos a acercarnos esta vez a las aplicaciones específicas de la tecnología de tarjetas inteligentes, que como se ha mencionado anteriormente es lo que de alguna manera antecede a los teléfonos RFID y la tecnología que se aplica a su vez en ellos, además de la tecnología propia del NFC-Philips que estaremos analizando mas adelante.

Las primeras tarjetas plásticas aparecieron en los Estados Unidos a principios de la década de los 50's, cuando el PVC económico reemplazó al cartón, en los años que siguieron, las tarjetas de crédito plásticas se volvieron de uso común. Curiosamente, las primeras tarjetas de crédito se emitieron por el Diners Club en 1950.

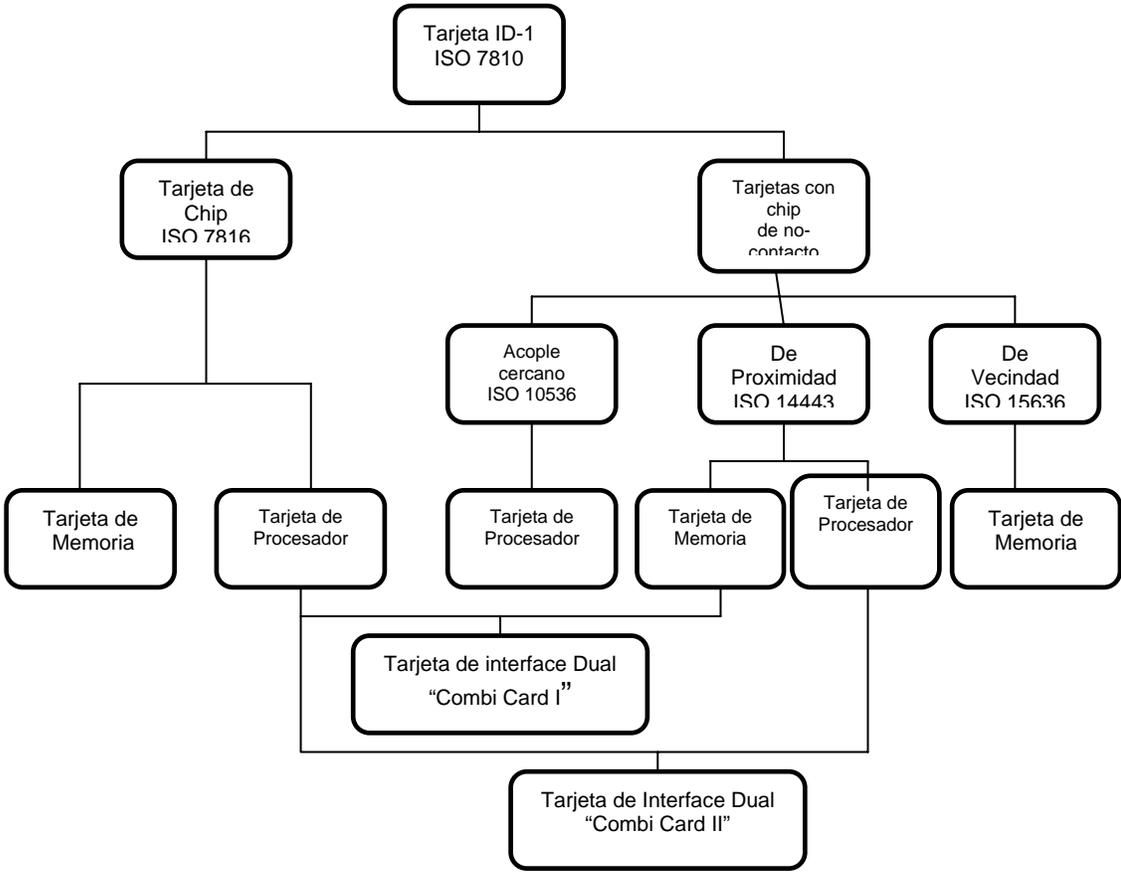
El rápido desarrollo de la tecnología de semiconductores hizo posible el integrar una memoria de datos y una lógica de protección en un solo chip de silicio en los años 70's. La idea de incorporar tal chip de memoria integrado dentro de una tarjeta de identificación se patentó en 1968 por Jurgen Dethloff y Helmut Grotrupp en Alemania. De cualquier manera no fue sino hasta 15 años después que el gran paso se logró con la introducción de la tarjeta inteligente telefónica por la compañía francesa PTT. Muchos millones de tarjetas inteligentes telefónicas estuvieron en circulación durante 1986 en Francia. Esta primera generación de tarjetas inteligentes fueron tarjetas de memoria de contacto. Una mejora significativa se logró cuando los microprocesadores se integraron exitosamente en un chip de silicio y estos chips se incorporaron en las tarjetas de identificación. Esto hizo posible el correr algún software en una tarjeta inteligente, esto abrió la posibilidad de lanzar aplicaciones de alta seguridad. Entonces fueron lanzadas las tarjetas inteligentes para telefonía móvil y las nuevas tarjetas bancarias (EC con chip) usando exclusivamente tarjetas con microprocesador.

Desde mediados de los 80's, intentos repetidos se han hecho para lanzar las tarjetas inteligentes de no-contacto al mercado. La frecuencia operativa de 135 kHz que era normal en ese tiempo y el alto consumo de potencia de los chips de silicio en el mercado, necesitaron devanados en transponder con cientos de vueltas. La resultante, una gran sección de cruce de devanado, y los capacitares adicionales que usualmente se requerían impidieron su fabricación en el formato ID-1 de tarjetas plásticas y los transponders fueron usualmente lanzados dentro reinconvenientes corazas e plástico. Debido a esta limitación, las tarjetas inteligentes de no-contacto jugaron un papel menor en el mercado de las tarjetas inteligentes por un largo rato.

En la primera mitad de los 90's, sistemas de transponder se desarrollaron con una frecuencia operativa de 13.56 MHz. Los transponders que se requerían para estas aplicaciones sólo necesitaban de cinco vueltas en su devanado, por primera vez fue posible producir sistemas transponder en el formato ID-1 de 0.76 mm de espesor. El gran avance en Alemania ocurrió en 1995 con la introducción de la tarjeta de cliente en formato ID-1 "Viajero Frecuente" por la compañía alemana *Lufthansa AG*. Vale la pena hacer notar que estas tarjetas, fabricadas por la compañía de Munich *Giesecke & Devrient*, continuaban

teniendo una tira magnética, un holograma y estaban grabados con el nombre y número de cliente. Veremos una descripción mas detallada de este sistema mas adelante.

Hoy en día las tarjetas inteligentes de no-contacto han sido divididas en tres grupos basados en los estándares aplicables (figura 5.2) a las tarjetas inteligentes, acoplamiento cercano, acoplamiento remoto (acople inductivo) y acople de vecindad (acople inductivo). Mientras que las tarjetas de acople de vecindad están solamente disponibles en la forma de tarjetas de memoria, las tarjetas de microprocesador han estado disponibles en la forma de tarjetas acopladas inductivamente en pequeños proyectos piloto desde 1997.



**Fig. 5.2 La gran Familia de Tarjetas Inteligentes, incluyendo el estándar ISO**

Actualmente los campos más importantes de aplicación de tarjetas inteligentes de no-contacto son en sistemas de pago (transporte público y boletaje) o pases (tarjetas de identificación, credenciales de empleado en compañías). A largo plazo podríamos esperar que estas tarjetas inteligentes de no-contacto reemplazarán por mucho a las tarjetas de contacto en sus clásicas aplicaciones (tarjetas telefónicas, tarjetas EC-Eurocheque o Electronic Cash). En adición, la tecnología inalámbrica permitirá a las tarjetas inteligentes ser usadas en completamente nuevos campos, de los cuales tal vez nunca nos hayamos imaginado.

### 5.3.4 Transporte Público

El transporte público es una de las aplicaciones en donde existe un gran potencial para el uso de sistemas RFID, particularmente tarjetas inteligentes de no-contacto. En Europa y Estados Unidos las asociaciones de tránsito continúan operando con grandes pérdidas, algunas veces tanto como el 40% de su producción, lo cual debe resanarse con los subsidios de la comunidad o país en cuestión. Debido al incremento en la escasez de recursos, soluciones a largo plazo deben ser buscadas para cortar estas pérdidas, reduciendo costos e incrementando las ganancias. El uso de las tarjetas electrónicas de no-contacto como pases electrónicos de viajero podrían hacer una importante contribución para mejorar la situación (AFC-automatic fare collection “*colecta automática de tarifas*”). En particular en el campo d administración de las tarifas existe un gran negocio y mucha tela de donde cortar.

#### El punto de partida

La situación financiera menos sana de las compañías de transporte, naturalmente puede tener distintas causas, de cualquier manera los siguientes factores son importantemente mencionados en relación con los pases electrónicos de viajero:

- Las compañías de transporte incurren en altos costos debido a la venta de boletos de viaje por los despachadores automáticos. Por ejemplo, la venta de un pase de viaje por medio de un despachador automático en Zurich cuesta Sfr 0.45, donde el precio de venta promedio es de Sfr 2.80, en otras palabras el 16% del precio de venta se pierde por el debido aprovisionamiento del mismo despachador, el mantenimiento y las reparaciones (deben rellenarse con notas y monedas, reparaciones y daño por vandalismo).
- En vehículos, se requieren además impresoras electrónicas de boletos muy caras, a veces los boletos son vendidos incluso por el conductor, lo que causa largos tiempos de espera cuando los pasajeros abordan, además del riesgo de seguridad que se presenta por la continua distracción del conductor.
- Los boletos de papel se tiran después de ser usados, aunque la fabricación de boletos a prueba de fraude para las compañías de transporte, son cada vez más caros.
- En las ciudades alemanas en particular, pérdidas arriba de 25% se deben tomar en cuenta debido a los que eluden las tarifas, esto es porque las compañías de transporte alemanas son muy liberales en cuanto a las condiciones de viaje y permiten la entrada al sistema subterráneo y autobuses sin que los boletos sean verificados antes.
- Los descuentos para asociaciones sólo pueden ser calculados en base a cuentas aleatorias costosas lo que conduce a la imprecisión de cálculos.

## Requerimientos

Los sistemas de administración de tarifas tienen que llenar muy altas expectativas y requerimientos, particularmente con respecto a la resistencia, degradación, uso, velocidad de escritura-lectura y facilidad de uso, estas expectativas pueden ser únicamente satisfactorias con los sistemas RFID. El más común de los formatos de tarjetas inteligentes es el formato ID-1 y recientemente en relojes de pulso.

### *Tiempo de transacción*

El tiempo que se toma para la compra o verificación de un boleto de viaje es particularmente crítica en los sistemas de transporte en los cuales el boleto sólo puede ser verificado dentro del vehículo. Este es un problema particular de los autobuses y tranvías. En los trenes subterráneos, los boletos pueden ser verificados en los torniquetes. Una comparación de diferentes métodos nos arrojan la clara superioridad de sistemas RFID en términos de tiempos de transacción (ver tabla 5.1).

<b>Tecnología</b>	<b>Tiempo de Procesamiento de Pasajero (s)</b>
RFID I (acople remoto)	1.7
Verificación visual del conductor	2.0
RFID II (acoplamiento cercano)	2.5
Tarjeta Inteligente con contactos	3.5
Efectivo	> 6

**Tabla 5.1 Tiempos de procesamiento de pasajeros para diferentes tecnologías**

### *Resistencia a la degradación, tiempo de vida y conveniencia*

Las tarjetas inteligentes de no-contacto están diseñadas con un tiempo de vida de 10 años o más. La lluvia, frío, suciedad y polvo no son un problema ni para la tarjeta ni para el lector. Las tarjetas inteligentes se pueden mantener en una cartera o bolsa de mano y por lo tanto son extremadamente convenientes de usar (especialmente en la ciudad de México debido a la delincuencia). Los transponders también pueden ser colocados dentro de relojes de pulsera.

### **Beneficios de los sistemas RFID**

El reemplazo de boletos convencionales de papel por modernos sistemas de administración de tarifas electrónicos basados en las tarjetas inteligentes de no-contacto provee una multitud de beneficios para todos los involucrados. Aunque los costos de compra de una tarjeta inteligente de no-contacto siguen siendo más altos que aquellos de un sistema convencional (por lo mismo se han desarrollado sistemas telefónicos con RFID), la inversión se debería auto-reparar en un periodo corto de tiempo. La superioridad de

sistemas de no-contacto se demuestra por los siguientes beneficios para usuarios y operadores de compañías de transporte público.

#### *Beneficios para Pasajeros*

- El efectivo ya no será necesario, las tarjetas electrónicas de no-contacto se pueden cargar con grandes cantidades de dinero, los pasajeros no tienen que cargar con el pasaje exacto.
- Las Tarjetas electrónicas de no-contacto en prepago permanecen vigentes incluso cuando las tarifas se cambien.
- El pasajero no necesita conocer la tarifa precisa, el sistema automáticamente deduce de la tarjeta la tarifa correcta.
- Mensualmente los boletos pueden iniciar en cualquier día del mes, el periodo de validez empieza después de la primer deducción de la tarjeta de no-contacto.

#### *Beneficios para el Conductor*

- Los boletos ya no son vendidos al momento, lo que resulta en una menor distracción del personal operador.
- El vehículo no maneja efectivo.
- Se elimina el conteo diario de ingresos.

#### *Beneficios para la Compañía de Transporte*

- Se reducen los costos de operación y mantenimiento de los despachadores de ventas y la devaluación de boletos.
- Muy seguros en contra del vandalismo.
- Es muy fácil el cambiar tarifas, no se necesitan imprimir nuevos tickets.
- La introducción de sistema electrónico cerrado, en el cual todos los pasajeros deben producir un boleto de viajero válido, puede significativamente reducir el número de personas que no pagan.

#### *Beneficios para la asociación de Transportes*

- Es posible el calcular el rendimiento de socios individualmente en la asociación. Debido a que datos precisos son obtenidos automáticamente en los sistemas de administración electrónica de tarifas, el descuento para la asociación se puede calcular usando figuras precisas.
- Se pueden obtener datos estadísticos muy claros.

#### *Beneficios para los Tesoreros*

- La reducción de la necesidad de subsidios debido a la reducción en costos.
- El mejor uso del transporte público debido al servicio mejorado tiene un efecto positivo en los ingresos y en el ambiente.

## Sistemas Tarifarios usando Pago Electrónico

Las regiones de asociaciones de transporte se encuentran generalmente divididas en diferentes zonas de tarifa y zonas de pago, además existen diferentes tipos de pases de viaje, zonas de tiempo de espera y numerosas posibles combinaciones. El cálculo de las tarifas puede ser de esta manera extremadamente complicado en sistemas convencionales de pago y puede incluso ser una fuente de desconcierto para los clientes locales.

Los sistemas de administración electrónica de tarifas, por otro lado, facilitan el uso de completamente nuevos procedimientos para el cálculo y pago de tarifas. Existen cuatro modelos básicos para el cálculo electrónico de tarifas como se muestra en la tabla 5.2

Sistema Tarifario 1	El pago tiene efecto al inicio de la jornada. Una cantidad fija se deduce de la tarjeta electrónica de no-contacto, a pesar de la distancia recorrida.
Sistema Tarifario 2	Al inicio de la jornada, le punto de entrada (verificador de entrada) se graba en la tarjeta de no-contacto. En el desembarque en la estación final (verificador de salida), la tarifa por la distancia recorrida es calculada automáticamente y deducida de la tarjeta. En adición, la tarjeta se puede verificar en cada punto de cambio previniendo la existencia de una entrada válida. Para prevenir intentos de manipulación, la ausencia de un punto de verificación de salida se puede penalizar con la deducción de la tarifa máxima al inicio de la próxima jornada.
Sistema Tarifario 3	Este modelo es el más rentable para redes entrelazadas, en las cuales la misma ruta puede recorrerse usando diferentes sistemas de transporte a diferentes tarifas. Cada vez que el pasajero cambia de vehículos una cantidad predeterminada se deduce de la tarjeta, los bonos para los viajeros de grandes distancias y gente que cambia muchas veces se pueden tomar automáticamente a cuenta.
Cálculo del Mejor Precio	En este sistema todas las jornadas que se hacen son grabadas en la tarjeta de no-contacto por un mes. Si un cierto número de jornadas superaron el límite diario o mensual en su totalidad, entonces la tarjeta de no contacto puede automáticamente ser convertida en una tarjeta mas económica de 24 horas o mensual, esto da al usuario máxima flexibilidad y las mejores tarifas posibles. El <i>Cálculo del Mejor Precio</i> mejora las relaciones con el cliente y hace una mayor contribución a la satisfacción del cliente.

**Tabla 5.2 Diferentes Sistemas Tarifarios para pagos con Tarjetas de no-contacto**

### Potencial de Mercado

Se estima que alrededor del 50% de todas las tarjetas de no-contacto que se venden, se usan en el sector de transporte público. Las mayores áreas de implementación son las grandes

urbes en Asia (Seúl, Hong Kong, Singapur, Shanghai) y ciudades Europeas (París, Londres, Berlín).

En 1994 y 1995 cerca de un millón de tarjetas inteligentes de no-contacto se produjeron por año a nivel mundial para aplicaciones del transporte público. En el periodo de 1996 a 1997 el volumen alcanzó alrededor de 40 millones de tarjetas por año. El volumen estimado para 1998 solamente, fue de 100 millones de tarjetas a nivel mundial para el mismo fin. Dado la tasa de crecimiento de 60% o más, podemos esperar que la demanda anual por tarjetas de no-contacto aumente a 250 millones en este nuevo siglo.

La alta tasa de crecimiento para tarjetas inteligentes de no-contacto en aplicaciones de transporte público será en el área Asia-Pacífico, debido a las nuevas infraestructuras creadas ahí para estas nuevas tecnologías.

#### **5.3.4.1 Proyectos Ejemplares**

##### **Seúl-Corea**

El más largo sistema de pase de viajero electrónico (AFC) que usa las tarjetas de no-contacto se comisionó al inicio de 1996 en la metrópolis de Seúl, Corea el Sur. La tarjeta coreana “*Bus Card*” es una tarjeta de prepago al igual que la del Metrobus, y con un valor de aproximadamente 17 euros, las tarifas se calculan a partir del sistema tarifario 1. Una jornada en autobús cuesta en promedio aproximadamente 0.35 euros, pero cada vez que el pasajero cambia de vehículos debe pagar nuevamente.

La tarjeta se puede usar en todas las 453 líneas y recargada en kioscos específicos como sea requerido. La asociación de transportes, Seoul Bus Union se compone de 89 compañías operadoras autónomas con un total de más de 8700 autobuses, los cuales se equiparon con terminales de no-contacto a mediados de 1996. Cuando la provincia Kyung-ki que rodea la ciudad capital se incluyó en el esquema, mas de 4000 autobuses y un total de 3500 puntos de carga que se equiparon con terminales en 1997, la tecnología RFID usada en este proyecto es el sistema MIFARE® (acople inductivo, 10 cm, 13.56 MHz), el cual es muy popular en aplicaciones de transporte público.

Cerca de 4 millones de “*Bus Cards*” estuvieron en circulación a finales de 1997. El gran éxito de este sistema ha convencido al gobierno de Seúl para introducir un sistema compatible para el sistema férreo subterráneo.

##### **Luneburg, Oldenburg- Alemania**

Uno de los primeros proyectos de tarjetas inteligentes en el transporte público de Alemania es el proyecto *Fahrsmart* en la asociación de transporte KVG Luneburg-VWG Oldenburg. El proyecto piloto subsidiado *Fahrsmart* fue lanzado por el *Ministerio para la Educación e Investigación* en esta área en 1990/91. Cerca de 20 000 tarjetas inteligentes de contacto se usaron con los clientes para este proyecto. De cualquier modo, fallas significativas en los sistemas instalados se volvieron evidentes durante este proyecto piloto, el mayor problema

fue el tiempo de registro de más de tres segundos por pasajero, lo cual se consideró excesivo.

A inicios de 1996 un nuevo campo de pruebas se lanzó, el sistema Fahrsmart II basado en tarjetas inteligentes de no-contacto, la tecnología utilizada una vez mas fue el sistema MIFARE® de Philips/Mikron. La integración del sistema, por ejemplo la comisión del sistema entero se concesionó a Siemens VT (Berlín).

El sistema Fahrsmart calcula automáticamente el precio más bajo para el cliente (garantía de mejor precio). El pasajero debe verificar al inicio de la jornada usando su tarjeta inteligente personal, así como verificar al termino de la misma, los datos de la jornada obtenidos se colectan en la computadora de a bordo y almacenados en la tarjeta inteligente para verificación.

Cuando el vehículo regresa al depósito al final del día, los datos del día en cuestión son enviados de la computadora del vehículo al servidor de estación, vía una interface infrarroja. Los datos procesados se transfieren entonces al servidor central Fahrsmart por medio de una red interna. Para calcular la factura mensual, el servidor Fahrsmart analiza el perfil de uso de cada pasajero y calcula el boleto más barato para la distancia recorrida (jornada individual, pase semanal, pase mensual etc.).

### **Proyectos en Estados unidos – ICARE y CALYPSO**

Algunos de los proyectos de transporte local mencionados arriba que usan tarjetas inteligentes de no-contacto, como casi todos los proyectos realizados hasta hoy, también son llamados *sistemas de intercambio cercano*. En la práctica esto significa que las tarjetas inteligentes son “cargadas” con dinero, pero que sólo se pueden usar dentro del transporte público en cuestión como un boleto o en el sentido de pagos de cuentas no muy grandes, por ejemplo en las maquinas de bebidas operadas por la misma compañía de transporte. Estas tarjetas no pueden ser usadas en otras tiendas o como un pase electrónico de viajero en otras localidades. Todo esto significa que el portador de tal tarjeta debe almacenar información para una aplicación específica en el sistema colecta electrónica de cercanía y no tendrá acceso a esta para una aplicación diferente (tarjeta inteligente telefónica o tarjeta de prepago no-contacto pase de viajero para el restaurante de la compañía).

Lo anterior es el resultado de la tecnología empleada en la tarjeta, ya que las tarjetas que han sido utilizadas hasta hoy sólo tienen un chip de memoria y de esta forma no satisfacen los estrictos requerimientos de seguridad de las instituciones crediticias para los sistemas automatizados abiertos de intercambio financiero.

Los sistemas abiertos de intercambio financiero basados en un chip de microprocesador han sido introducidos exitosamente en el campo de las tarjetas electrónicas de no-contacto, en Alemania estos sistemas son tarjetas de pago de *Telekom*, VISA-Cash-Karte y el “ec-Karte mit Chip”, el último contando con la base de usuarios más grande con aproximadamente 50-55 millones de tarjetas en uso. Estas tarjetas se diseñaron para pagos de sumas pequeñas y se pueden usar donde sea que los lectores convenientes se encuentren. Desde el punto de vista de usuario, podría ser ideal si la tarjeta de débito se pudiera usar como un boleto para

el transporte público local, debido al alto tiempo de transacción de tarjetas electrónicas de contacto (ver tabla 5.1), las tarjetas electrónicas para efectivo aún no son capaces de establecerse a sí mismas como un pase electrónico de viajero en las asociaciones de transporte público locales.

Se han propuesto varias soluciones que ayudan a combinar lo amigable para el usuario de los boletos de no-contacto con la seguridad de los sistemas de intercambio de contacto, y todo esto para mejorar la aceptación de tales sistemas por parte de los usuarios. La tarjeta híbrida es la combinación de una tarjeta inteligente de no-contacto con un chip adicional de contacto en la misma tarjeta, no existe de cualquier manera, conexión eléctrica entre ambos chips, esto significa que puede ser posible el transferir sumas de dinero de un chip a otro, en máquinas especiales, debido a esta limitación, la tarjeta híbrida también se puede considerar como una solución provisional.

La tarjeta de interface dual (o tarjeta Combicard, ver figura 5.2) que resulta de la combinación de interfaces de contacto y no-contacto en una sola tarjeta de chip es actualmente la solución ideal para la combinación de un pase electrónico de viajero con un sistema de intercambio financiero abierto. De cualquier manera, la cuestión de cuando la colecta electrónica de la alemana ZKA (ec-card) estará disponible como una tarjeta de interface dual y en que cantidades existirá seguirá pendiente y sin respuesta por el momento, de cualquier manera VISA ya ha anunciado que integrará su *VISA cash chip* basado en tecnología de contacto, en un combichip en Madrid.

Una solución a la vista llamada “*sobre*” (envelope) en la cual un adaptador de no-contacto convierte la tarjeta de contacto en un pase de no-contacto (la tarjeta de contacto entra en el sobre como una carta), ofrece la ventaja sobre las antes mencionadas variantes de que las tarjetas con microprocesador que se encuentran en circulación se pueden hacer útiles como tarjetas de no-contacto sin cambiar las tarjetas en sí.

El *sobre* tiene como referencia a ICARE-*Integration of contactless technologies into public transport environment* (Integración de tecnologías de no-contacto en el ambiente transporte público), este proyecto apoyado por Estados Unidos está orientado hacia el uso de sistemas de intercambio electrónico abierto en los sistemas de transporte locales, el campo de pruebas para este proyecto, el cual inició temprano en 1996, se desarrollará en varias regiones europeas.

En París, la más grande zona conurbana, 40 000 miembros del personal RATP y 4 000 pasajeros se han equipado con esta solución (*sobre*). Como una característica adicional, se ha desarrollado una llamada de emergencia que actualmente se ha probado en el metro. Esta característica se podría disparar como el desarrollo tecnológico en sí (*sobre*). Adicionalmente al concepto de *sobre*, al desarrollo de un boleto disponible se le ha dado alguna prioridad en París.

En Venecia, una población con un alto porcentaje de visitantes diarios, muchas estaciones terrestres se han equipado con lectores de no-contacto. A parte de la función de boleto no-contacto, una característica central en Venecia es la multifuncionalidad del concepto, la tarjeta puede ser usada en museos, hoteles, o como un boleto de estacionamiento. En el

distrito de Constanza en el lago del mismo nombre, después de un intento en el otoño de 1996, un segundo campo de aplicación de prueba se inició en enero de 1998, en este segundo intento, la tarjeta de efectivo del banco de ahorro local se usó en conjunto con un *sobre* para formar el “FlexPass”, el cual se puede usar en el transporte local. Una antena *handsfree* con rango de 1m permite que los datos estadísticos de la tarjeta sean usados para grabar sin que el cliente tenga que sujetar el *sobre* cerca del lector.

En Lisboa, una ciudad capital de tamaño medio en Europa con un complicado sistema de transporte y numerosas compañías operarias públicas y privadas, el desarrollo de una antena *handsfree* también es un proyecto por demás importante.

Desde 1998, actividades de búsqueda han estado activas bajo el proyecto estadounidense CALYPSO-Contact And contactLess environments Yielding a citizen Pass integrating urban Services and financial Operations (ambientes de contacto y no-contacto actuando como pase ciudadano, integrando servicios urbanos y operaciones financieras). Las compañías de transporte han incrementado sus esfuerzos para construir una cooperativa con los operadores de sistemas automáticos de intercambio. Entre otras compañías de la industria de crédito alemana, la compañía Deutsche Sparkassen-und Giroverband (DSGV) ha sido reclutada como socio.

El objetivo del proyecto CALYPSO es el pase flexible “FlexPass”, la intención es que éste reemplazará tanto al boleto de papel como al dinero en efectivo usado por los clientes para pagar. Un nuevo aspecto del proyecto es la introducción de mas servicios en el sobre, por ejemplo un servicio de información dinámica de pasajeros (tiempos de salida y conexiones se muestran en pantalla), el uso en estacionamientos o en la integración de servicios de emergencia también están siendo considerados.

A largo plazo, la inclusión de mas aplicaciones en los campos de estacionamientos, turismo, administración pública o incluso compartir auto en el “FlexPass” se considera.

#### **5.3.4.2 Boletaje**

##### **Millas Lufthansa y otras tarjetas**

El proyecto de Lufthansa “Ticketless flying” es el proyecto en escarapate para los sistemas de tarjetas inteligentes sin-contacto. La prueba piloto que envuelve a 600 vuelos regulares de mayo a diciembre de 1995 corrió tan fácilmente que para Marzo de 1996 el programa “Miles & More” se hizo extensivo a todas las tarjetas Lufthansa (HON Club, SENATOR y Frequent Traveller), y la compañía propietaria del servicio Lufthansa, AirPlus se estableció. Desde el otoño de 1996, todos los aproximadamente 250 000 pasajeros regulares tenían la nueva “ChipCard” sin-contacto. Esta nueva tarjeta inteligente sin-contacto (en conjunto con la computadora central Lufthansa en Munich-Erding) reemplazó tanto al viejo boleto de papel como al convencional pase de abordaje.

El sistema RFID seleccionado para este proyecto fue el sistema MIFARE® de Philips/Mikron. Las terminales se desarrollaron por Siemens-Nixdorf, mientras que las tarjetas inteligentes de no-contacto se fabricaron por la compañía de Munich Giesecke & Devrient, además de un módulo transponder de no-contacto, las tarjetas tenían incorporado también una cinta magnética, letras levantadas, cinta para firmar, holograma y un chip telefónico (de contacto) opcional.

Desde el punto de vista del pasajero, el sistema opera como sigue: el propietario de la tarjeta reserva un vuelo por vía telefónica con un agente, proporcionando su número individual de tarjeta, con las nuevas tarjetas, la reservación debía tomar una hora antes de la salida, posteriormente se crea un boleto electrónico que combina datos personales e información del vuelo y todo esto se salva en la computadora Lufthansa. Para verificar la tarjeta en el aeropuerto (de último minuto), el propietario de la tarjeta inteligente solo tiene que presentar su tarjeta inteligente brevemente en la *terminal de chip*, normalmente se hace esto sin sacar la tarjeta de la billetera, el sistema verifica la reservación y la fecha del vuelo aparece en pantalla (de la Terminal de chip). Ya para este punto, al pasajero se le da la opción de confirmar el vuelo, incluyendo reservación de asiento o seleccionando un vuelo alternativo en el monitor *touch screen*, al pasajero se le da un recibo impreso especificando su número de asiento y puerta de abordaje además de otros detalles. Todo este procedimiento permite al pasajero el verificar con su equipaje de mano en menos de 10 segundos, lo cual ayuda a prevenir las filas en la Terminal. Cuando el pasajero llega a la puerta de abordaje el solo presenta su ChipCard una vez mas y entonces puede abordar.

La nueva solución de ChipCard beneficia tanto a pasajeros como Lufthansa y Airplus, los pasajeros ahorran tiempo en el aeropuerto, tienen la capacidad de reservar en un corto tiempo y una conveniente y simple operación. Un claro éxito de la racionalización puede verse en Lufthansa y Airplus, todo lo dicho se debe al autoservicio del cliente, el cual reduce significativamente la intensa labor de manejo y verificación. Además, de que la habilidad para aceptar las reservaciones de última hora se ve incrementada por el ahorro de tiempo en tierra, de esta forma se incrementa la competitividad comparada con opciones alternativas de viaje.

#### **5.3.4.3 Metrobús-Ciudad de México**

La Ciudad de México vive una situación crítica de contaminación y tráfico por el abandono del transporte público. Las ventas de automóviles casi se han duplicado en los últimos doce años, pasando de 168,167 automóviles vendidos en 1992 a alrededor de 270 mil en 2004 (datos de la Asociación Mexicana de la Industria Automotriz). Con el aumento del parque vehicular, del cual no existen datos oficiales para el Área Metropolitana, el tráfico se ha agudizado. Al aumentar el tiempo de traslado han aumentado las emisiones de contaminantes por kilómetro recorrido. Para Greenpeace la solución a esto se encuentra en mejorar el sistema de transporte público, volviéndolo eficiente, disminuyendo los tiempos de traslado, haciéndolo un sistema seguro y cómodo, pero el asunto es ¿cómo lograrlo?, pues bien la tecnología RFID nos pudiera servir de mucha ayuda en respuesta a esta pregunta como veremos.

Desde 1997 se han presentado distintas propuestas para mejorar el sistema de transporte de la ciudad de México, el Metrobús es una de ellas, sin embargo esta sería una de las primeras opciones para liberar el tránsito de principales avenidas en la ciudad. Con ayuda de la electrónica, no solo se proporcionaría calidad de servicio sino también comodidad a la hora de manejar el efectivo (tarjetas prepagadas) , especialmente cuando se tienen los índices delictivos tan altos para el robo en transporte público. Todo lo anterior conduce al principal objetivo de proyectos como este: planificar y regular el transporte público y establecer áreas libres de automóviles.

Y es que la Ciudad de México tiene uno de los peores sistemas de transporte público ya que la mayor parte de los viajes-persona-día se realizan en microbuses. Desde su origen, los microbuses demostraron que agravarían los problemas de transporte debido a que son unidades no diseñadas para el transporte público de pasajeros, tienen baja capacidad de pasaje y el salario de los conductores depende de la cantidad de pasajeros que suben.

Alrededor de 80 por ciento de los habitantes de la Ciudad utiliza el transporte público, de ahí que éste deba tener prioridad sobre el automóvil privado, pues contamina mucho menos por pasajero transportado y ocupa menos espacio vial por pasajero.

La opción del metrobús es la más viable porque es la más económica y eficiente. En cálculos realizados en 1997 el costo de un kilómetro de Metro era suficiente para instalar 200 kilómetros de metrobús, esto sin considerar el tiempo e impacto urbano que implicaba la construcción de Metro. Incluso el tranvía o el trolebús son más caros que el metrobús. Sin embargo, una vez construidos los carriles exclusivos para este último, posteriormente pueden ser utilizados por un sistema eléctrico de transporte como cualquiera de los mencionados.

Para resaltar, lo importante del metrobús dentro del esquema de nuestro estudio, tiene que ver con los lectores de tarjetas inteligentes que se instalaron (no de inicio) para que los usuarios puedan comprar este tipo de tarjetas que tienen las mismas características que lo que se define en el estandar 14443 (consultar más adelante), lo cual no tiene precedente en la ciudad de México (en la ciudad de León, Gto. Se ha aplicado con éxito) y es un esfuerzo mas por mejorar el transporte público de la misma. Así pues un poco de lo que se propone en este capítulo es ejemplificado con este servicio urbano en México, que si bien, el usar las tarjetas inteligentes ya es un adelanto, pues también cabe la posibilidad de alargar las opciones de reducción de tiempos y demás beneficios, si se toma en cuenta una tecnología como la que aquí se desglosa (NFC), para futuras aplicaciones como ésta y otras muchas como las que ya se han visto antes en el capítulo.

### **5.3.5 Características principales para Tarjetas Inteligentes**

Si clasificamos los sistemas RFID de acuerdo al rango de información y funciones de procesamiento de datos ofrecidos por el transponder y el tamaño de su memoria de datos, obtenemos un amplio espectro de variantes. Este espectro va desde los más simples sistemas Low-end (como los sistemas EAS), sistemas mid-end y los sistemas mas avanzados “*high-end*” a los cuales pertenecen las aplicaciones de tarjetas inteligentes sin-contacto.

El segmento high-end se compone de los sistemas con microprocesador y un sistema operativo de tarjeta inteligente (smart card OS). El uso de microprocesador facilita la realización de algoritmos de encriptación y autenticación significativamente más complejos que pueden ser posibles usando la lógica altamente orientada a cables de una máquina de estado. En lo más alto de los sistemas high-end es ocupado por las modernas tarjetas inteligentes de interface dual, las cuales contienen un coprocesador criptográfico. La enorme reducción en tiempos de cómputo que resulta del uso de un coprocesador significa que las tarjetas inteligentes sin-contacto pueden incluso ser usadas para aplicaciones que imponen altos requerimientos en la encriptación segura de la transmisión de datos, tal como los sistemas de colecta electrónica o de boletaje en los sistemas de transporte público. Los sistemas high-end son casi exclusivamente operados en la frecuencia de 13.56 MHz, la transmisión de datos entre el transponder y el lector se describe en el estándar ISO 14443.

Como habíamos mencionado con anterioridad, las tarjetas inteligentes son sistemas que pueden contar con distintos tipos de acople y como tal, cumplen con las siguientes características en resumen:

*Alimentación para el transponder:* Los sistemas de acople cercano se diseñaron para rangos de entre 0.1 cm y un máximo de 1 cm, el transponder es entonces insertado en un lector o colocado en una superficie delimitada (*touch & go*) para su operación.

Insertando el transponder dentro del lector, o colocándolo en el mismo, permite al devanado del transponder el ser posicionado de forma precisa en el hueco de aire de un núcleo de forma de anillo o de uno de forma de U. El bosquejo funcional del devanado de transponder y de lector corresponden al de un transformador (fig.5.3), el lector representa al devanado primario y el arrollamiento del transponder representa el devanado del secundario. Una corriente alterna de alta frecuencia en el devanado primario genera un campo magnético de alta frecuencia en el núcleo y hueco de aire del arreglo, el cuál además fluye hacia el devanado del transponder, esta energía es rectificadora para proveer energía al chip.

Debido a que el voltaje  $U$  inducido en el devanado del transponder es proporcional a la frecuencia  $f$  de la corriente de excitación, la frecuencia elegida para la transferencia de energía debe ser tan alta como sea posible. En la práctica, las frecuencias en el rango de 1-10 MHz se usan, a favor de mantener las pérdidas en el núcleo del transformador bajas, se debe seleccionar, como material de núcleo, un material de ferrita que sea conveniente para tal frecuencia.

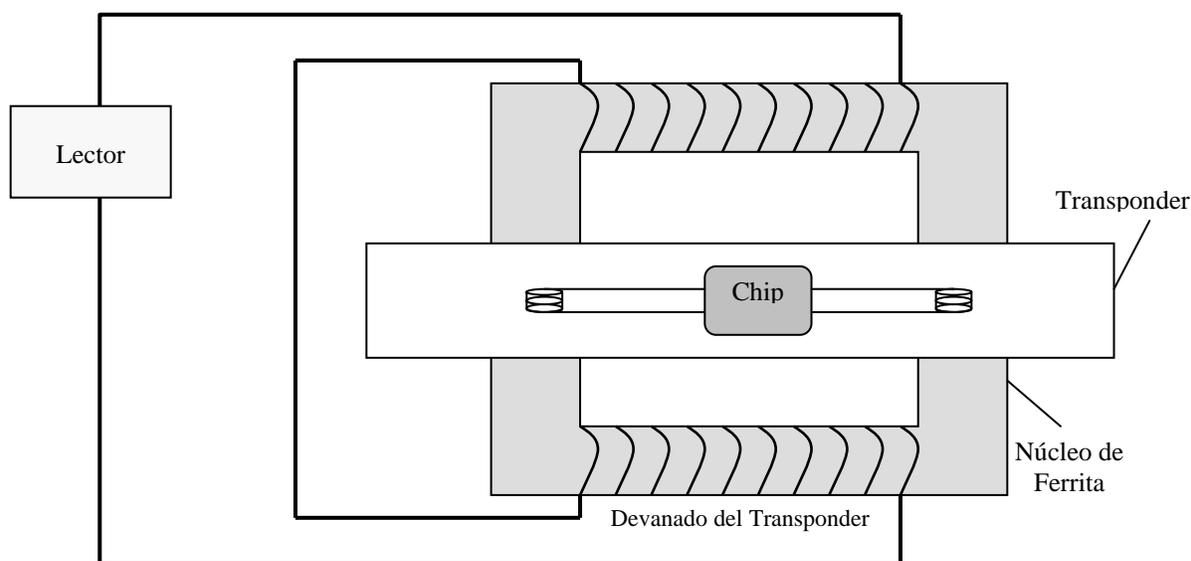
Ya que en contraste a los sistemas de acople inductivo o de microondas, la eficiencia de la transferencia de energía desde el lector al transponder es muy buena, los sistemas de acople cercano son excelentemente convenientes para la operación de chips de alto consumo de potencia. Lo anterior incluye microprocesadores, los cuales aún requieren 10 mW de potencia para su operación, por esta razón todos los sistemas de tarjeta chip acople cercano en el mercado contienen microprocesadores.

Los parámetros mecánicos y eléctricos de las tarjetas chip acople cercano de no-contacto se han definido en su propio estándar, ISO 10536. Para otros diseños los parámetros de operación se pueden definir libremente.

#### *Transferencia de datos transponder – lector*

*Acople Magnético:* La modulación de carga con subportadora se usa también para transferencias de datos magnéticamente acopladas desde el transponder al lector en los sistemas de acople cercano. La frecuencia de subportadora y modulación se especifican en ISO 10536 para las tarjetas chip de acoplamiento cercano.

*Acople Capacitivo:* Debido a la corta distancia entre el lector y el transponder, los sistemas de acoplamiento cercano pueden emplear además el *acoplamiento capacitivo* para la transmisión de datos. Los capacitores de plato resultan de acoplar superficies aisladas una de otra, y que se arreglan en el transponder y el lector de tal manera que cuando un transponder se inserta, se encontrará paralelo al lector y viceversa. Este procedimiento también se usa en tarjetas inteligentes de acople cercano. Las características mecánicas y eléctricas de estas tarjetas, también se definen en ISO 10536.



**Fig. 5.3 Transponder de Acople cercano en un lector de inserción con devanados magnéticamente acoplados**

Lo anterior principalmente es válido, como se puede observar para los sistemas de acople cercano, sin embargo los estándares propuestos para la tecnología NFC incluyen otra clase de acoplamientos como los que veremos para el caso del estándar ISO 14443 (incluido en la parte de estandarización).

## **5.4 Near Field Communications (NFC)**

La tecnología NFC es una evolución de las tecnologías de RFID y tecnologías de interconexión, opera en el rango de frecuencia de los 13.56 MHz, en una distancia típica de tan sólo unos cuantos centímetros. La tecnología NFC está estandarizada en ISO 18092, ECMA 340 y ETSI TS 102 190. La tecnología NFC es además compatible como mencionábamos con anterioridad con algunas tecnologías para tarjetas inteligentes de no-contacto como el ampliamente establecido estándar ISO 14443 (por ejemplo la tarjeta MIFARE® de Philips y la tarjeta FELICA® de Sony).

Estos dispositivos NFC se pueden comunicar con tasas de datos de 106, 212 y 424 kbps, a continuación se dará una breve explicación de lo que el estándar permite, pero que sin embargo no especifica acerca de la comunicación y aplicaciones en productos en red y equipo de consumidor (PDA's, Teléfonos...).

Primeramente estaremos revisando entonces algunas características de esta tecnología en cuanto a la interface y el protocolo en sí, para una descripción más detallada se deberán revisar los estándares antes mencionados además de sus complementarios (para el caso de ECMA, revisar 352, 356 y 362). Esta parte del tratado es fundamental en el mismo ya que mantiene una relación directa con la propuesta de este proyecto, así que sin mas preámbulo, deberemos entrar a una breve descripción.

En general los ya mencionados estándares definen modos de comunicación y para la interface y protocolos de comunicaciones de campo cercano que se le ha llamado NFCIP para interconexión con periféricos computarizados.

### **5.4.1 Introducción a NFC**

El estado actual de los consumibles electrónicos puede ser caracterizado como en transición, de dispositivos de propósito sencillo a dispositivos multifuncionales, de la misma forma una transición de dispositivos aislados a dispositivos en red, en relación a lo segundo, es importante que la gente no lidie directamente con las complejidades de establecer conexiones de red entre dispositivos, penosamente las configuraciones para red pueden tratarse dentro del mundo computacional, pero ciertamente no sucede así para el caso del mundo de los consumibles electrónicos.

Lo anterior es la principal tarea para el protocolo de comunicación cercana NFC interface y protocolo (NFCIP-1), el cual se enfoca hacia los consumibles electrónicos que permitan al usuario tener seguridad en cuanto a la comunicación entre diferentes dispositivos sin tener que ejercer mucho esfuerzo intelectual en configurar “su red”. El concepto es notablemente simple, en función de hacer que dos dispositivos se comuniquen se deben acercar el uno al otro o tocarse. Lo anterior enganchará a las interfaces de los dispositivos inalámbricos NFCIP-1 y los configurará para establecer una comunicación con el modelo par a par de red. Ya que toda la información ha sido intercambiada usando NFC, los dispositivos se pueden programar y continuar la comunicación a una mayor distancia (rango) y con protocolos mas rápidos como el caso de Bluetooth y Ethernet inalámbrico (WiFi).

El protocolo se basa en una interface inalámbrica donde siempre existen dos partes a comunicar, de manera que el protocolo también es conocido como *protocolo de comunicación par a par*. El protocolo establece comunicaciones de red inalámbricas entre aplicaciones de red y dispositivos consumibles electrónicos.

Las interfaces operan en el espectro no regulado de 13.56 MHz, lo cual significa que no se aplica ninguna restricción y no se necesita ninguna licencia para el uso de dispositivos NFC entro de esta frecuencia. Desde luego, cada país impone ciertas limitaciones en cuanto a las emisiones electromagnéticas en esta banda, estas limitaciones en la práctica indican las limitaciones de distancia a la que los dispositivos pueden conectarse y puede variar. Generalmente se consideran las distancias de 0-20 cm.

Como es usualmente el caso para los dispositivos que comparten una misma banda de radiofrecuencia, la comunicación es half-duplex, los dispositivos además ocupan la política de *escucha antes de hablar*, esto es, cualquier dispositivo debe primero escuchar a la portadora y empezar a transmitir una señal solamente si no se encuentra ningún otro dispositivo transmitiendo.

El protocolo NFC distingue entre el Iniciador y el Blanco de una comunicación, así que cualquier dispositivo puede ser cualquiera de los dos. El *Iniciador* como se puede deducir de su nombre, es el dispositivo que inicia y controla el intercambio de datos. El *Blanco* es el dispositivo que responde a las peticiones del iniciador.

EL protocolo NFC también distingue entre dos modos de operación: el *modo pasivo* y el *modo activo*, y todos los dispositivos soportan ambos modos de operación, con las siguientes características:

- En el *modo activo* de comunicación ambos dispositivos generan su propio campo de radiofrecuencia para llevar sus datos.
- En el *modo pasivo* de comunicación sólo uno de los dispositivos en cuestión genera el campo de radiofrecuencia, mientras el otro utiliza la modulación de carga para transferir los datos. El protocolo especifica que el Iniciador es responsable de generar el campo de radiofrecuencia.

La aplicación coloca la velocidad inicial de transferencia en 106, 212 o 424 kbit/s, subsecuentemente la aplicación y/o el ambiente de comunicación puede requerir de adaptación de velocidades, lo cual se puede hacer durante la misma comunicación.

NFCIP-1 usa diferentes esquemas de modulación y codificación de bit, dependiendo de la velocidad. Mientras establece la comunicación, el Iniciador principia la comunicación en un modo particular a una velocidad particular. A su vez el Blanco determina la velocidad actual y el protocolo asociado de bajo nivel automáticamente y responde de acuerdo a esas condiciones. La comunicación puede finalizar cuando se da un comando desde aplicación o cuando los dispositivos se encuentren fuera de rango.

### **Características únicas del protocolo**

Lo que hace a las comunicaciones entre dispositivos tan fácil es que el protocolo NFC provee de algunas características que no se encuentran en otros protocolos de propósito general.

Primero que todo, se trata de un protocolo de muy corto rango, soporta comunicaciones medidas en centímetros, los dispositivos tienen que estar literalmente casi tocándose para establecer un enlace entre ellos, esto tiene dos importantes consecuencias:

1. Los dispositivos se pueden apoyar en el protocolo para estar inherentemente seguros, ya que deben ser colocados muy cerca del otro. Es muy sencillo controlar cuando ambos dispositivos comunican o no, simplemente colocándolos uno cerca del otro o separándolos.
2. El procedimiento para establecer comunicación del protocolo es inherentemente familiar a la gente, quieres que algo se comunique –*tócalo*-. Lo anterior permite que la conexión de red entre dispositivos se complete automáticamente y suceda de una manera transparente. El proceso completo es como si los dispositivos se reconocieran el uno al otro por el *toque* y se conectaran una vez que esto sucede.

Otra característica importante de este protocolo es que soporta un modo pasivo de comunicación, esto es muy importante para los dispositivos de baterías que deben cuidar el consumo de energía como prioridad. El protocolo permite a dispositivos tales como un teléfono móvil el operar en modo de ahorro de energía (el modo pasivo de la comunicación NFC), este modo no requiere que ambos dispositivos generen el campo de radiofrecuencia y permite que toda la comunicación sea energizada desde un solo lado. Por supuesto, el dispositivo en sí seguirá necesitando ser energizado internamente pero, no tendrá que “desperdiciar” batería en energizar la interface de comunicación RF.

Además el protocolo puede usarse fácilmente en conjunto con otros protocolos para seleccionar dispositivos y automáticamente configurar una conexión, como veremos en el siguiente ejemplo, los parámetros de otros protocolos inalámbricos pueden ser intercambiados permitiendo la configuración automática de otros protocolos de mayor rango. La dificultad al usar protocolos de largo rango como Bluetooth o Wireless Ethernet se da al seleccionar el dispositivo correcto fuera de la multitud de dispositivos en el rango y proveer los parámetros correctos a la conexión, al usar NFC todo el procedimiento es simplificado a acercar un dispositivo a otro.

El protocolo NFC es además compatible con los ampliamente usados protocolos para tarjetas inteligentes FeliCa™ y Mifare™. Los Dispositivos NFC son capaces de trabajar con las tarjetas inteligentes y los lectores de las mismas, conforme a los mismos protocolos y de forma parecida, de esta manera no solo se puede acoplar una tarjeta con un dispositivo NFC sino también un dispositivo NFC se puede utilizar en vez de una tarjeta inteligente.

## 5.4.2 Near Field Communication Interface and Protocol 1 (NFCIP-1)

Para empezar a definir este protocolo de comunicación, empezaremos por recalcar que se trata de un estándar en la banda de los 13.56 MHz además de las siguientes características que nos permitirán describirlo.

El estándar define los modos de comunicación pasivo y activo de la siguiente manera:

- En el modo de comunicación activa, tanto el Iniciador como el Blanco deben usar su propio campo RF para permitir la comunicación, el Iniciador empieza la comunicación NFCIP-1, el Blanco responde a un comando iniciador en este modo usando una modulación de campo RF auto generado.
- En el modo de comunicación pasivo, el Iniciador genera el campo RF e inicia la comunicación, el Blanco responde a un comando iniciador en este modo usando un esquema de modulación de carga.

La comunicación sobre la interface aérea en el modo activo y pasivo debe incluir, por supuesto: esquemas de modulación, velocidades de transferencia y codificación de bit. Además debe incluir el inicio de comunicación, el fin de comunicación, la representación de bit y/o byte, detección de trama y error, detección de dispositivo (SDD), selección de protocolo y parámetros, intercambio de datos y de-selección de dispositivos NFCIP-1.

Todos los dispositivos NFCIP-1 deben tener capacidades de comunicación en el rango de los 106, 212 y 424 kbps en cada uno de los cuales pueden permanecer o conmutar a otra cualquiera de estas tres tasas de transferencia.

El modo de comunicación (activo ó pasivo) no se debe cambiar durante una transacción sino hasta la desactivación del Blanco o cuando se aparte el mismo, incluso cuando la velocidad de transferencia del Iniciador al Blanco o viceversa no sean las mismas. Se puede hacer el cambio de velocidad de transferencia durante una transacción mediante un procedimiento de cambio de parámetro.

Por último se especifica que la transacción se inicia por inicialización de dispositivo y terminada por de-selección de dispositivo (o equivalente).

### 5.4.2.1 Campo de Radiofrecuencia (RF).

La frecuencia portadora para este caso debe ser de 13.56 MHz, donde el campo RF mínimo no modulado debe ser  $H_{\min}$  con un valor de 1.5 A/m rms, mientras que para el caso del campo máximo RF no modulado se tiene  $H_{\max} = 7.5$  A/m rms. Además de las condicionantes establecidas para los modos de comunicación activo y pasivo.

Para el modo de comunicación pasivo, el Iniciador deberá producir un campo RF para energizar al Blanco, éste último deberá operar continuamente entre los valores  $H_{\min}$  y  $H_{\max}$ .

En el modo de comunicación activo tanto el Iniciador como el Blanco deberán generar alternadamente un campo al menos con un valor  $H_{\min}$  pero sin exceder  $H_{\max}$  en las posiciones especificadas por el fabricante.

Los dispositivos NFCIP-1 deben detectar campos RF externos a 13.56 MHz con un valor mayor a  $H_{\text{umbral}}$  cuando sensan campos externos RF. El valor  $H_{\text{umbral}}$  es:

$$H_{\text{umbral}} = 0.1875 \text{ A/m}$$

#### 5.4.2.2 Interface Aérea

Se debe antes de todo definir una duración de bit para los modos de comunicación (ver tabla 5.3). La duración de bit  $bd$  se calcula con la siguiente fórmula:

$$1 \text{ bd} = 128 / (D \times f_c)$$

Donde los valores del divisor D dependen de la tasa de datos y se dan en la tabla 5.3,  $f_c$  es la frecuencia portadora definida (13.56 MHz).

Modo de comunicación	Kbps	Divisor D
<b>Activo o Pasivo</b>	<b>106</b>	<b>1</b>
<b>Activo o Pasivo</b>	<b>212</b>	<b>2</b>
<b>Activo o Pasivo</b>	<b>424</b>	<b>4</b>
<b>Activo</b>	<b>847</b>	<b>8</b>
<b>Activo</b>	<b>1695</b>	<b>16</b>
<b>Activo</b>	<b>3390</b>	<b>32</b>
<b>Activo</b>	<b>6780</b>	<b>64</b>

Tabla 5.3 Definición del Divisor D

Nota: Para comenzar una comunicación el Iniciador es quien elige la tasa de bit inicial.

A continuación describiremos las principales características de cada una de las velocidades en que el NFCIP-1 opera, sólo para el *modo de comunicación activo* en el cual la especificación de dirección no importa, puesto que si es de Iniciador a Blanco o al revés se ocupan las mismas reglas.

#### **MODO DE COMUNICACIÓN ACTIVO 106 KBPS.**

La tasa de bits para la transmisión durante la inicialización y detección de dispositivo (SDD) debe ser  $f_c/128$  (106 kbps).

La comunicación desde el Iniciador a un Blanco y viceversa para una velocidad de 106 kbps debe usar el principio de modulación ASK 100% del campo RF operativo para crear un “pulso” cuyas características se explican mejor en el estándar ecma-340.

#### **Representación de bit y codificación**

La representación de bit y codificación deben ser como sigue:

*Inicio de comunicación:* Al principio de la duración de bit un “pulso” debe ocurrir

*Uno*: Después de transcurrido un tiempo de pulso de la mitad de duración de bit.

*Cero*: En la duración total de bit no debe aparecer modulación salvo las siguientes excepciones

- Si existen dos o más ceros contiguos, desde que aparece el segundo debe aparecer también un pulso al inicio de la duración de bit.
- Si el primer bit después de un inicio de comunicación es cero, entonces debe haber un pulso al inicio de la duración de bit.

*Fin de comunicación*: Cero seguido de una duración de bit sin modulación

*Sin información*: Deberá codificarse con al menos dos periodos de bit completos sin modulación.

La codificación de byte que se emplea es la de primero el bit menos significativo (lsb first).

### **MODO DE COMUNICACIÓN ACTIVO 212 Y 424 KBPS.**

La tasa de bits para la transmisión durante la inicialización y detección de dispositivo (SDD) debe ser respectivamente de  $f_c/64$  (212 kbps) y  $f_c/32$  (424 kbps).

El Iniciador y el Blanco deberán usar una modulación ASK con un índice de 8 a 30% del campo operativo, esta modulación se debe mantener en transmisión durante la inicialización y SDD debe ser la misma.

#### **Representación de bit y codificación**

Se debe emplear la codificación Manchester con niveles lógicos definidos como sigue:

*Cero lógico*: La primera mitad de un bit es una portadora de amplitud baja, mientras que la segunda mitad del bit debe ser una portadora de alta amplitud in modular.

*Uno lógico*: La primera mitad de *bd* es una señal de alta amplitud sin modular, mientras que la segunda mitad del bit será una señal de baja amplitud.

Una polaridad inversa en amplitud se permite, la polaridad se deber detectar a partir de la sincronización. La codificación de byte es msb first.

### **MODO DE COMUNICACIÓN PASIVO 106 KBPS**

#### **Iniciador a Blanco**

La tasa de bits de Iniciador a Blanco es la misma que para el caso en modo activo, dada por  $f_c/128$ . El esquema de modulación tampoco tiene cambios (se emplea el mismo que para el caso del modo activo). Para la representación de bit y codificación durante la inicialización y detección de dispositivo (SDD) se utilizan los mismos métodos que para el caso de la comunicación en modo activo. La codificación de byte es lsb first (primero el bit menos significativo).

### **Blanco a Iniciador**

La tasa de bits obviamente es de  $f_c/128$ , mientras que para el caso de modulación, el Blanco debe responder al Iniciador por medio de un área de acoplamiento inductivo donde la frecuencia portadora es cargada para generar una subportadora de frecuencia  $f_s$ , ésta subportadora debe ser generada conmutando una carga en el Blanco. La amplitud de la modulación de carga debe ser al menos  $30/H^{1.2}$  (mV pico), donde  $H$  es el valor (rms) del campo de fuerza magnético en unidades A/m. La frecuencia  $f_s$  de la subportadora deberá ser  $f_c/16$ .

En cuanto a la modulación de subportadora podemos decir que cada periodo de bit debe iniciar con una relación de fase definida a la subportadora y el periodo de bit debe iniciar con el estado de carga de la subportadora. La subportadora se debe modular con el esquema de representación de bit y codificación que se estableció para el caso de la interface en modo activo de 212 y 424 kbps, es decir codificación Manchester (no se permite una polaridad inversa). La codificación de bytes es lsb first (primero el bit menos significativo).

## **MODO DE COMUNICACIÓN PASIVO 212 Y 424 KBPS.**

### **Iniciador a Blanco**

Nuevamente la tasa de bits se define igual que para el caso de las comunicaciones en modo activo, tampoco cambian la representación de bit y los esquemas de codificación o modulación para la transmisión durante inicialización y SDD. La codificación de bytes se basa en lsb first.

### **Blanco a Iniciador**

La tasa de bits se define como hemos visto (no cambia) para el caso de la comunicación en modo activo. En cuanto a modulación, el Blanco debe ser capaz de comunicarse con el Iniciador por medio de un área de acople inductivo donde la frecuencia portadora se carga para generar una codificación Manchester con duración de bit  $bd$ . La amplitud de la modulación de carga debe ser al menos  $30/H^{1.2}$  (mV pico), donde  $H$  es el valor (rms) del campo de fuerza magnético en unidades A/m. La codificación de byte que se emplea es msb first.

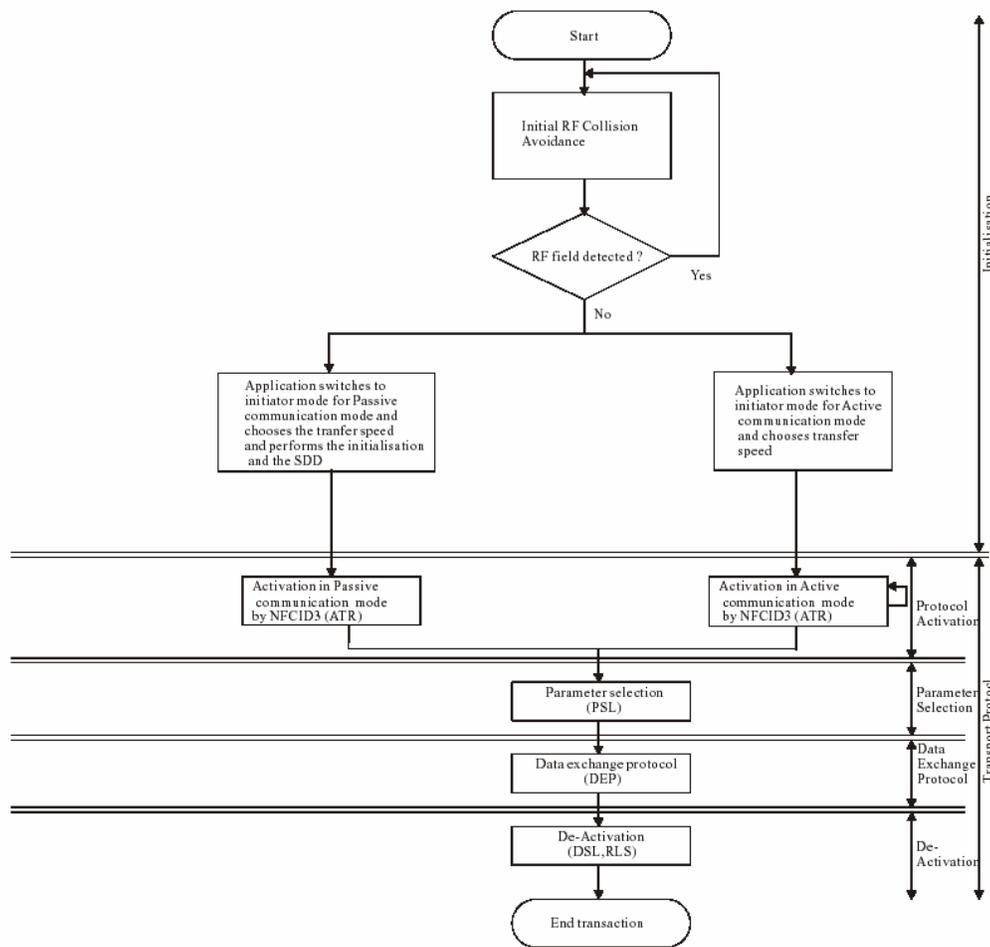
### **5.4.2.3 Flujo General del Protocolo**

El flujo general del protocolo entre dispositivos NFCIP-1 se debe conducir sobre las siguientes operaciones consecutivas:

- Cualquier dispositivo NFCIP-1 debe por default estar en modo Blanco.
- Cuando está en modo Blanco, no debe generar campo RF, y deberá esperar silenciosamente por un comando desde el iniciador.
- El dispositivo NFCIP-1 se debe cambiar a modo Iniciador sólo si así lo requiere la aplicación.
- La aplicación se encargará de determinar el modo (activo o pasivo) y la velocidad de transferencia de datos.

- El Iniciador debe comprobar si existe algún campo RF presente y no deberá activar su propio campo si un campo externo es detectado.
- Si no se detecta un campo externo, el Iniciador deberá activar su campo RF.
- El Blanco se deberá activar con el campo RF del Iniciador.
- La transmisión de comandos por parte de un Iniciador tanto en el modo activo como en el pasivo debe hacerse a las velocidades de transferencia seleccionadas.
- Se transmite una respuesta por parte de un Blanco en cualquiera de los modos (activo o pasivo). El modo de comunicación y la velocidad deben ser los mismos que los del Iniciador.

La figura 5.4 muestra el flujo de inicialización y detección de dispositivo para los modos de comunicación activo y pasivo a diferentes velocidades de transferencia.



**Fig 5.4 Flujo general para la Inicialización y SDD entre dispositivos NFCIP-1**

#### 5.4.2.4 Inicialización

A continuación describiremos los protocolos de inicialización y detección de colisión para Blancos en el modo pasivo y activo. El Iniciador debe detectar cualquier colisión, cuando al menos dos Blancos estén transmitiendo patrones de bit con una o dos posiciones de donde se transmiten los valores complementarios.

#### Prevención de colisión RF

En función de no perturbar alguna otra comunicación NFC o a cualquier infraestructura corriendo en la misma frecuencia portadora, el Iniciador no debe generar su propio campo RF cuando sea detectado otro campo RF.

#### Prevención de colisión inicial.

Para iniciar la comunicación con un Blanco tanto en el modo activo como pasivo, el Iniciador debe buscar continuamente la presencia de un campo externo RF. Si el Iniciador no detecta un campo RF en un tiempo definido, el campo RF del mismo puede cambiar a “encendido”.

Debemos recalcar que el campo RF que se genera por el Iniciador se debe “apagar” en el modo de comunicación activo. Para el caso del modo de comunicación pasivo el campo RF del Iniciador no se debe apagar.

En adición a la prevención de colisión inicial descrita antes, una prevención de colisión respuesta debe darse durante la activación en el modo de comunicación activo, para prevenir la colisión de datos por una respuesta simultánea de mas de un Blanco.

#### 5.4.2.4.1 Modo de comunicación Pasivo

#### Inicialización y SDD a 106 kbps

Aquí se describe el formato de trama y tiempo usado durante la inicialización y SDD en el modo de comunicación pasivo a 106 kbps. Antes que la comunicación inicie, el Iniciador debe accionar el modo de prevención de colisión inicial.

Las tramas se deben transferir en pares, es decir, el iniciador comienza la comunicación seguido por la respuesta del Blanco...y así sucesivamente. Tanto la trama del Iniciador como la del Blanco contienen los campos de *Inicio de comunicación*, *Información* y *Fin de comunicación* (Ver fig 5.5). En esta comunicación entre Iniciador y Blanco se define también un *Tiempo de Respuesta de Trama (FRT)*, en la parte FRT de Blanco a Iniciador, existe un traslape con el fin de comunicación del Iniciador.

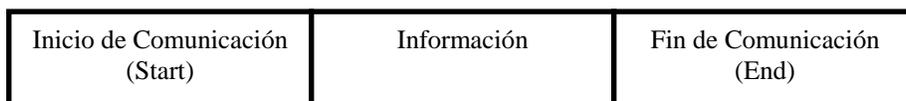


Fig.5.5 Formato de Trama en comunicación NFC (para Iniciador y Blanco)

El tiempo de respuesta de trama es el tiempo que transcurre entre el final del último pulso transmitido por el Iniciador y el primer borde de modulación, dentro del bit de inicio, transmitido por el Blanco. La tabla 5.4 define valores para  $n$  (múltiplo entero) y FRT dependiendo del tipo de comando y de la lógica de estado del último bit de datos transmitido con este comando

Tipo de Comando	$n$ (Valor entero)	FRT	
		Último bit Pulsado = Uno	Último bit Pulsado = Cero
SENS_REQ	9	$(n \times 128 + 84) / f_c$	$(n \times 128 + 20) / f_c$
ALL_REQ			
SDD_REQ			
SEL_REQ			
Todos los demás comandos	$\geq 9$		

**Tabla 5.4 FRT Iniciador-Blanco**

El valor  $n=9$  significa que todos los Blancos en el campo deben responder de forma síncrona, lo cual es necesario para detección de dispositivo SDD. Para todos los demás comandos, el Blanco debe asegurarse que el primer borde de modulación en el bit de inicio se encuentra alineado con la delimitación de bit de acuerdo a la definición de la tabla 5.4.

En cuanto al *tiempo de respuesta de trama Blanco-Iniciador*, éste se define como el tiempo de la última modulación transmitida por el Blanco y la primera pausa transmitida por el Iniciador y debe ser al menos  $1172 / f_c$ .

### **Formatos de Trama**

Se pueden distinguir los siguientes tipos de trama:

- **Trama corta:** La trama corta se debe usar para iniciar una comunicación y consiste de un *inicio de comunicación*, 7 bits de transmisión (*lsb*) y un *fin de comunicación* sin bit de paridad (ver fig 5.6).
- **Trama estándar:** Se deben utilizar para el intercambio de datos y consisten de un campo *inicio de comunicación*, un campo de *información* que estará dado por  $n \times$  (8 bits datos + bit de paridad impar) con  $n \geq 1$  y el bit menos significativo de cada byte se transmite primero, a cada byte le debe seguir un bit de paridad impar, éste bit de paridad P debe colocarse cuando el número de UNOS sea impar dentro del byte (bit 0 a bit 7, P) ver fig 5.6.
- **Trama orientada a bit para selección de dispositivo:** Las colisiones se deben detectar cuando al menos dos Blancos transmitan diferentes patrones de bit al Iniciador. En este caso, la frecuencia portadora se debe modular junto con la subportadora durante la duración de bit completa por al menos un bit.

	bit 0	bit 1	bit 2	bit 3	bit 4	bit 5	bit 6	
Start	Command							End

(a) Trama Corta

	Byte 0						Byte 1						..	Byte n						
Start	bit 0	bit 1	..	bit 6	bit 7	P	bit 0	bit 1	..	bit 6	bit 7	P	...	bit 0	..	bit 7	P	End		
	Command or Data						Data						..	Data						

(b) Trama Estándar

**Fig. 5.6 Formatos de Trama**

***Trama orientada a bit para selección de dispositivo SDD***

Las tramas orientadas a bit SDD sólo se deben usar durante la trama SDD y deben dividirse en dos partes para el caso de las tramas estándar con longitud de 7 bytes: La parte 1 para la transmisión de Iniciador a Blanco y la parte 2 para la transmisión de Blanco a Iniciador.

Para la longitud de la trama, sólo se aplican tres reglas:

- Regla 1: La suma de bits de datos debe ser 56.
- Regla 2: La longitud mínima de la parte 1 debe ser de 16 bits de datos.
- Regla 3: la longitud máxima de la parte 1 debe ser de 55 bits de datos.

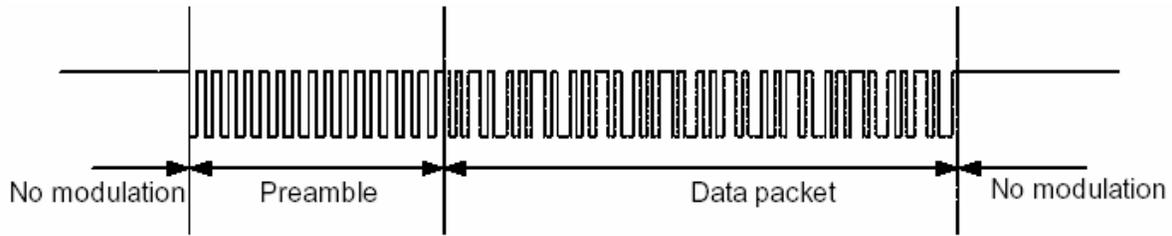
Como consecuencia, la longitud mínima de la parte 2 debe ser de 1 bit de datos y la longitud máxima deben ser 40 bits de datos (ver ecma-340 ó ISO 18092).

El CRC que se ocupa para la comunicación activa y pasiva en el modo 106 kbps es el CRC-16/CCITT (ver siguiente capítulo secc 6.3.1.3). En los estándares mencionados anteriormente también se incluyen los estados de los Blancos (Power-off state, sense state, sleep state...) específicos para el protocolo de detección de colisión, los Blancos deben reaccionar solamente a las tramas válidas, no se debe enviar ninguna respuesta cuando se detectan errores de transmisión.

**Inicialización y SDD a 212 y 424 kbps**

El inicio para la comunicación pasiva debe estar señalizado con la presencia de modulación en la frecuencia portadora. La comunicación debe iniciar con una secuencia preámbulo de 48 bits mínimo y con un CERO lógico codificado. El final de la comunicación debe resultar de la longitud de campo de la trama (ver fig 5.7).

Después que un dispositivo NFCIP-1 ha finalizado una comunicación, el otro deberá demorar un periodo de al menos  $8 \times 64/f_c$  antes de empezar la transmisión con una secuencia de preámbulo.



**Fig. 5.7 Inicio y fin de comunicación (212 y 424 kbps)**

### Formato de Trama

Consiste de un preámbulo, sincronía, longitud, payload y CRC (ver fig 5.8). El campo preámbulo debe ser de 48 bits mínimo todos como CERO lógico. El campo de sincronía (SYNC) debe consistir de 2 bytes. El campo Length debe ser de 8 bits y se le debe ajustar al número de bytes a ser transmitidos en el campo Payload mas 1, el rango del campo Length será de 2 a 255.

El campo Payload consiste de  $n$  8-bit-bytes de datos, donde  $n$  esta dado por el número de bytes de datos. El CRC se debe calcular de acuerdo al CCITT CRC-16.



**Fig. 5.8 Formato de Trama (212 y 424 kbps)**

### SDD a 212 y 424 kbps

La técnica básica del procedimiento SDD deberá ser el método de Time Slot que consiste en lo siguiente: El número de slot debe ser un entero mayor de cero, el Iniciador deberá enviar peticiones de sondeo, el Blanco deberá responder aleatoriamente en cada time slot controlable. El Iniciador será capaz de leer los datos NFCID2 del Blanco(s) en diferentes time slots.

Después de obtener los datos NFCID2 del Blanco(s) en el campo operativo, el Iniciador puede comunicarse con múltiples Blancos. Mas de 16 time slots se pueden ocupar por acuerdo entre las partes que intercambian datos. El número de time slots se debe indicar con el valor TSN en la trama de petición (sondeo) del Iniciador (ver fig 5.9).

Un blanco, que ya está energizado, responde al Iniciador de acuerdo a las siguientes reglas después que ha recibido las peticiones de poleo (sondeo) del Iniciador:

1. El Blanco debe generar un numero aleatorio R en el rango de 0 a TSN.
2. El Blanco debe esperar hasta que el time slot concuerde con R, entonces enviará la trama de respuesta de sondeo y esperará por la siguiente petición. Un blanco puede ignorar una petición para prevenir las colisiones de respuestas.

La comunicación entre Iniciador y Blanco se debe iniciar como sigue:

1. El Blanco obtiene energía del campo operativo generado por el Iniciador.
2. EL Blanco debe estar listo para recibir una petición del Iniciador en 2 segundos a partir de ser energizado como máximo.
3. El Blanco debe esperar por una petición del Iniciador. El Iniciador puede enviar una petición sin esperar a que el Blanco este listo.
4. Si el Iniciador no recibe ninguna respuesta a su petición, entonces puede enviar otra petición de nuevo. El Iniciador del modo pasivo de comunicación debe mantener la energizado el campo RF mientras ejecuta el procedimiento SDD.

La demora  $T_d$  entre el inicio de la trama de petición y el primer time slot debe ser de  $512 \times 64/f_c$ . La unidad Time Slot (Ts) debe tener un valor de  $256 \times 64/f_c$ .

### **Contenidos NFCID2**

El NFCID2 debe ser un número de 8 bytes para identificar dispositivos NFCIP-1. El código prefijo de 2 bytes debe ser seguido por un número de 6 bytes en el NFCID2. El código prefijo definirá las características del número de 6 bytes.

El número de 6 byte deberá ser generado aleatoriamente, mientras que el código prefijo es (01) (FE) entre otros.

Preamble (48 bit min.)	SYNC (16 bit)	Length (8 bit)	Payload					CRC (16 bit)
			(00)	(FF)	(FF)	(00)	TSN	

(a) Trama de Petición

Preamble (48 bit min.)	SYNC (16 bit)	Length (8 bit)	Payload			CRC (16 bit)
			(01)	NFCID2	Pad	

(b) Trama de Respuesta a la Petición

**Fig 5.9 Formatos de Trama de Sondeo y de Respuesta**

#### **5.4.2.4.2 Modo de comunicación Activo**

### **Inicialización a 106, 212 y 424 kbps**

La aplicación cambia a modo Iniciador para el modo de comunicación activo y puede elegir cualquiera de las velocidades, para este protocolo (106, 212, 424 kbps).

### **Procedimiento anticolidión RF en el modo activo de comunicación**

El método anticolidión RF se deberá ejecutar de acuerdo a la siguiente cronología:

- El iniciador deberá ejecutar el procedimiento anticolidión inicial.

- El primer comando ejecutado por el Iniciador es ATR\_REQ en el modo de comunicación activo en un rango de velocidad específico.
- El Iniciador deberá apagar el campo RF.
- El Blanco ejecuta un procedimiento anticolidión de respuesta.
- El Blanco envía el ATR\_RES como respuesta al ATR\_REQ a la misma velocidad que recibió este último y apaga su campo RF.
- El iniciador hace un procedimiento anticolidión de respuesta con indicadores de tiempo jitter en  $n=0$ .
- El Iniciador envía el PSL\_REQ en orden de cambiar algún parámetro o envía el DEP\_REQ para iniciar el protocolo de intercambio de datos.

En caso de que 2 Blancos o más se encuentren en el campo, aquel con el mas bajo valor  $n$  contestará primero y el otro no lo hará. Para el caso de 2 Blancos o más contestando en el mismo periodo de tiempo, el Iniciador detectará una colisión y éste reenviará el comando ATR\_REQ el cual se describe en los estándares ISO 18092, ECMA 340 y ETSI TS 102 190.

Después de que la primer respuesta del Blanco es detectada por el Iniciador el indicador de parámetro de tiempo jitter  $n$  se colocará en cero para futuras comunicaciones.

#### 5.4.2.5 Protocolo de Transporte

El protocolo de transporte se debe manejar en tres partes:

- a) La activación del protocolo, lo que incluye la petición de atributos (REQ\_ATR) y la selección de parámetros (PSL).
- b) El protocolo de intercambio de datos.
- c) La desactivación del protocolo, incluyendo Deselect y Release.

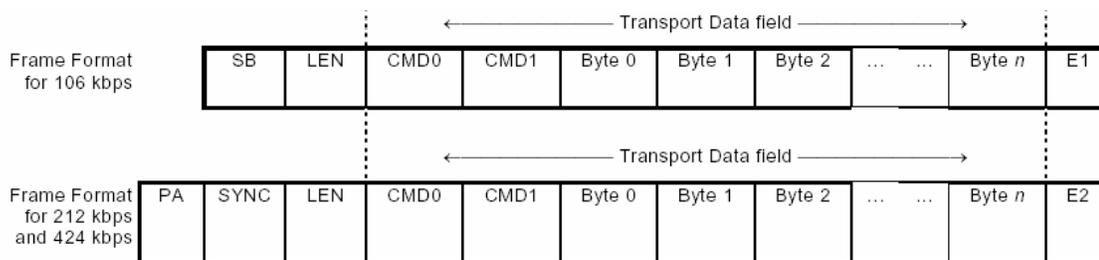
En general la *activación del protocolo* se basa en la petición de atributos que hace el Iniciador al Blanco con todos sus bytes de parámetro, cuando el Iniciador ha enviado una petición de atributo y recibe respuesta, se procede con las operaciones como se verá más adelante. En cualquier otro caso el Iniciador deberá retransmitir la petición antes de usar una secuencia de desactivación, en caso de falla de la desactivación, se envía una petición de “sueño”.

El *protocolo de intercambio de datos* esta basado en el comando DEP\_REQ y su respectiva respuesta, debiendo ser una comunicación half dúplex orientada a bloques y con manejo de errores. Para los datos que no caben en una sola trama se ocupa un mecanismo de encadenamiento definido.

Después del intercambio de datos, el Iniciador debe aplicar una *desactivación* del protocolo de intercambio de datos, después de una exitosa desactivación tanto el Iniciador como el Blanco deberán permanecer en el modo inicial elegido, pero el Iniciador puede escoger una de las velocidades de transferencia definidas para reactivación. Cuando se ha desactivado exitosamente, el Blanco no debe responder a las

subsecuentes peticiones de atributo. El comando Release en su forma de petición deberá cambiar al Blanco nuevamente a el estado “encendido”, en este estado, el Blanco deberá responder a todos los esquemas iniciales de comunicación y también a las peticiones de atributo (ATR\_REQ)

Los datos de usuario se deben transportar en el campo de Transporte de Datos en el formato de trama (fig. 5.10). La estructura de trama para 106 kbps se muestra en la misma figura, el byte de inicio SB debe colocarse en (F0), el byte LEN se debe ajustar a la longitud del campo de transporte de datos más uno en un rango de 3 a 255. El campo E1 es el código CRC para la trama. Para 212 y 424 kbps se describen además los campos de preámbulo (PA) y los bits de patrón de sincronía (SYNC), en éste último caso E2 es el CRC para la trama.



**Fig. 5.10 Definición del Formato de Trama de Transporte**

El campo de Transporte de Datos contiene los campos de bytes de comando CMD0 y CMD1 junto con los bytes cero a  $n$ . El contenido de los bytes 0 a  $n$  depende del comando CMD1 y pueden contener información, en cuyo caso son comandos, los bits de datos son opcionales.

#### 5.4.2.5.1 Flujo de sucesos para la activación en el modo de comunicación pasivo

Se debe aplicar la siguiente secuencia de activación:

1. El Iniciador deberá hacer la secuencia inicial anticolidión RF como se definió anteriormente.
2. El Iniciador deberá hacer la inicialización y SDD para el modo pasivo de comunicación a una velocidad definida como se vio antes.
3. El soporte para el protocolo NFCIP-1 deberá verificarse a diferentes tasas de velocidad de acuerdo a lo descrito anteriormente para la petición de atributos (ATR\_REQ).
4. El Blanco debe regresar al modo inicialización y SDD si ningún ATR\_REQ es soportado.
5. El ATR\_REQ debe ser enviado por el Iniciador como siguiente comando después de conocer que una petición de atributo está disponible.
6. El Blanco debe enviar su ATR\_RES en respuesta a la petición de atributo enviada por el Iniciador. El Blanco sólo debe responder a la petición de atributo si el mismo (ATR\_REQ) es recibido directamente después la selección.

7. Si el Blanco soporta cualquier parámetro intercambiable en la petición de atributo (ATR\_REQ), entonces se debe usar una petición de selección de parámetro (PSL\_REQ) por parte del Iniciador como siguiente comando después de recibir el ATR\_REQ para cambiar parámetros.
8. El Blanco debe enviar una respuesta (PSL\_RES) a la petición de selección de parámetro (PSL\_REQ).
9. Un Blanco no necesita complementar la selección de parámetro, si éste no soporta cualquiera de los diferentes parámetros en el ATR\_RES.
10. Los datos transparentes se deben enviar usando el protocolo de intercambio de datos.

#### **5.4.2.5.2 Flujo de sucesos para la activación en el modo de comunicación activo**

Se debe aplicar la siguiente secuencia de activación del protocolo en el modo activo de comunicación:

1. El Iniciador debe hacer la secuencia inicial anticolidión RF como se ha definido anteriormente.
2. El Iniciador deberá conmutar al modo activo de comunicación y seleccionará la velocidad de transferencia.
3. El Iniciador deberá enviar la petición de atributos (ATR\_REQ).
4. El Blanco debe enviar su ATR\_RES en respuesta al ATR\_REQ, después de una exitosa respuesta el dispositivo es seleccionado.
5. Si el Iniciador detecta una colisión de datos, se debe reenviar el comando ATR\_REQ.
6. Si el Blanco soporta cualquier parámetro variable en el ATR\_REQ, se debe usar entonces el PSL\_REQ por parte del Iniciador como siguiente comando después de recibir el ATR\_RES para cambio de parámetros.
7. El Blanco debe enviar un comando PSL\_RES en respuesta al PSL\_REQ.
8. Un Blanco no necesita complementar la selección de parámetro toda vez que no soporte cualquiera de los diferentes parámetros en el ATR\_RES.

### 5.4.2.5.3 Comandos del Protocolo

Los bytes de comando consisten de dos bytes. El primer byte debe ser CMD0 y el segundo debe ser CMD1. El código para los bytes de comando debe especificar la petición y respuesta de acuerdo a la tabla 5.5

Mnemónico	Bytes de Comando		Definición
	CMD0	CMD1	
ATR_REQ	(D4)	(00)	Attribute Request (Enviado por Iniciador)
ATR_RES	(D5)	(01)	Attribute Response (Enviado por Blanco)
WUP_REQ	(D4)	(02)	Wakeup Request (Enviado por Iniciador)
WUP_RES	(D4)	(03)	Wakeup Reponse (Enviado por Blanco)
PSL_REQ	(D5)	(04)	Parameter selection Request (Enviado por Iniciador)
PSL_RES	(D4)	(05)	Parameter selection Response (Enviado por Blanco)
DEP_REQ	(D5)	(06)	Data Exchange Protocol Request (Enviado por Iniciador)
DEP_RES	(D4)	(07)	Data Exchange Protocol Response (Enviado por Blanco)
DSL_REQ	(D5)	(08)	Deselect Request (Enviado por Iniciador)
DSL_RES	(D4)	(09)	Deselect Response (Enviado por Blanco)
RSL_REQ	(D5)	(0A)	Release Request (Enviado por Iniciador)
RSL_RES	(D4)	(0B)	Release Response (Enviado por Blanco)

Tabla 5.5 Set de Comandos para el NFCIP-1

Para mas detalles acerca de los comandos y campos específicos de los mismos, referirse a la documentación expedida por los organismos internacionales, específicamente ISO 18092, ECMA 340 y ETSI TS 102 190.

### 5.4.3 Near Field Communication Interface and Protocol 2 (NFCIP-2)

En el 2002, ECMA internacional formó el grupo de tarea 19 del comité técnico 32 para especificar las señales, interfaces y protocolo NFC. La asamblea general de diciembre de 2002 adoptó el NFCIP-1 como el estándar ECMA-340.

Aunque los estándares ECMA-340 (NFCIP-1), ISO/IEC 14443 e ISO/IEC 15693 especifican una frecuencia de operación de 13.56 MHz, también especifican distintos modos de comunicación, estos se definen como NFC (Near Field Communication), PCD

(Proximity Coupling Device) y VCD (Vicinity Coupling Device), respectivamente estandarizados en ECMA-340, ISO/IEC 14443 e ISO/IEC 15693.

El protocolo NFCIP-2 especifica el mecanismo para detectar y seleccionar un modo de comunicación de los anteriores tres posibles. Además NFCIP-2 requiere que un comportamiento subsecuente especifique el estándar acentuando el modo de comunicación seleccionado.

Los estándares para NFC, PCD y VCD especifican la interface de RF, inicialización, anticolidión y los protocolos para interconexión inalámbrica de dispositivos de acople de cercanía y el acceso a tarjetas de circuito integrado sin-contacto operando en los 13.56 MHz.

Este estándar especifica el mecanismo de selección de modo de comunicación y está diseñado para no irrumpir en cualquier comunicación en curso a 13.56 MHz para dispositivos implementando NFC y la funcionalidad de lectura para tarjetas de circuito integrado que cumplen con ISO/IEC 14443 ó ISO/IEC 15693. Este estándar requiere de implementaciones para ingresar a un modo de comunicación seleccionado como se ha especificado en el estándar respectivo. Las especificaciones del modo de comunicación, en todo caso, se encuentran fuera del objetivo de este estándar NFCIP-2.

#### **5.4.4 Módulo de transmisión Philips para comunicación no-contacto a 13.56 MHz**

Actualmente en el mercado podemos encontrar los módulos de transmisión para una adaptación directa de los dispositivos que así lo requieran, especialmente como objeto de nuestro estudio, los teléfonos móviles. Los módulos altamente integrados para transmisión en comunicación no-contacto PN511 y el PN531 de Philips<sup>®</sup> actúan ya directamente con sobresalientes conceptos de modulación y demodulación integrados completamente para diferentes métodos de comunicación no-contacto y protocolos en la banda de los 13.56 MHz.

El PN511 ocupa el concepto anterior de integración para diferentes tipos de métodos de comunicación pasivos y protocolos en los 13.56 MHz, además soporta tres diferentes modos de operación.

- Modo lectura/escritura para tarjetas FeliCa<sup>™</sup> e ISO14443A
- Soporta el modo Tarjeta para FeliCa<sup>™</sup> e ISO14443A/MIFARE en combinación con un microcontrolador seguro.
- Modo NFCIP-1

Para ser más claros, puede actuar como lector o transponder en los estándares para tarjetas inteligentes de no-contacto como los mencionados en los puntos anteriores, además de ofrecer la posibilidad de comunicación directa a diferentes dispositivos NFC habilitados en el modo NFCIP-1, el modo NFC también ofrece diferentes tasas de velocidad de más de 424 kbit/s, la parte digital maneja completamente el tramado y detección de errores NFC.

El PN531 además de todas las características que tiene su hermano integrado, cuenta con una funcionalidad de microcontrolador basada en un núcleo 80C51 con 32 kbytes de ROM y 1 kbyte de RAM. Este módulo de transmisión basado en  $\mu$ -controlador combina un sobresaliente concepto de modulación y demodulación completamente integrado para diferentes métodos de comunicación no-contacto y protocolos en los 13.56 MHz con la facilidad de usar firmware para los diferentes modos que soporta y las respectivas interfaces de host (teléfonos móviles, PDA's, Laptop's...etc.). El firmware adjunto maneja el protocolo de lectura ISO14443A y MIFARE® así como un elemental FeliCa™ en lectura y el protocolo completo NFCIP-1.

Además de todo esto, el firmware junto con el hardware interno soportan el manejo y los protocolos de host para las diferentes interfaces como por ejemplo: USB 2.0, I2C, SPI y UART serial. El PN531 con su microcontrolador integrado permite un rápido y conveniente diseño en combinación con un bajo gasto de recursos en el lado del controlador de host.

En resumen, cualquiera de estos módulos de transmisión están diseñados para satisfacer los requerimientos de las diversas aplicaciones que usan la comunicación no-contacto, basadas en NFCIP-1 ó lectura de protocolos ISO14443 y FeliCa™ en donde el costo-efectividad, tamaño y alto rendimiento en general es debido. Compatibles con la actual infraestructura RFID, la tecnología NFC en éstos dispositivos ofrece un nuevo tipo de comunicación directa entre dos dispositivos, ya que la comunicación par a par permite el intercambio de datos. Esta tecnología esta diseñada para encontrarse con los requerimientos para los mercados de consumo así como los de handheld y de computadoras.

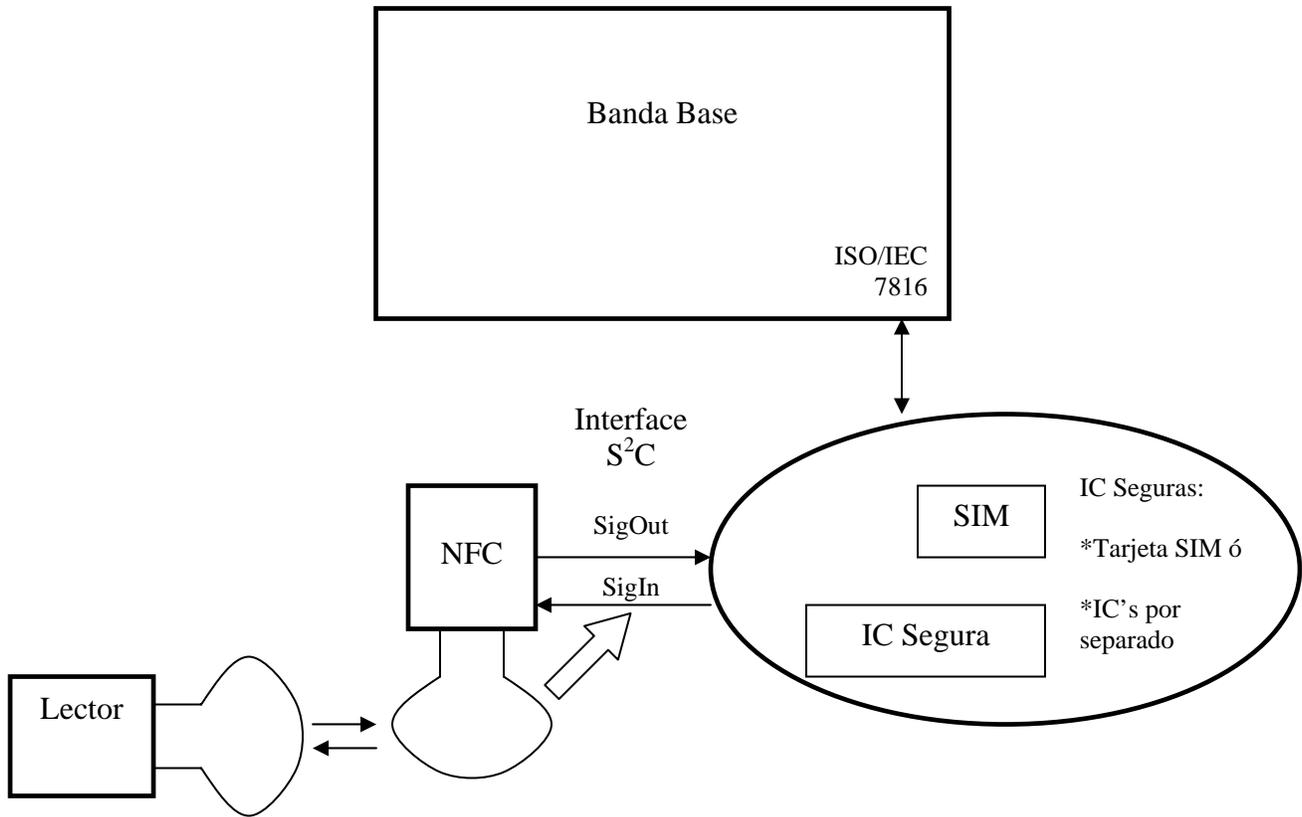
#### **5.4.5 Interface Philips S<sup>2</sup>C para NFC**

Otra de las tecnologías desarrolladas por Philips es en lo que respecta a las tecnologías de seguridad agregada, específicamente la interface S<sup>2</sup>C (SigIn-SigOut-Conection) para NFC, preocupados por las mismas causas que la sociedad y algunos organismos, ésta compañía se dio a la tarea de desarrollar un aditamento de seguridad de tipo interface de propósito general entre NFC y *Tarjetas IC (Integrated Circuit) Seguras* para permitir una comunicación de *seguridad NFC*.

Para nuestros propósitos tendríamos como principio de esta tecnología lo siguiente:

NFC + Tarjetas IC Seguras en un teléfono móvil = NFC seguro

En general, el NFC seguro agrega seguridad al NFCIP-1, el cual por sí mismo no provee de funciones de seguridad, por lo que provee aplicaciones seguras en una Tarjeta IC Segura (típicamente una tarjeta inteligente de acople inductivo) con la interface de no-contacto NFC, cuya combinación actúa como lo haría una tarjeta inteligente. La interface S<sup>2</sup>C permite la interconexión de dispositivos seguros como tarjetas SIM o tarjetas inteligentes sin-contacto por separado (ver fig 5.11).



**Fig. 5.11 Interface S<sup>2</sup>C**

De la figura 5.11 podemos observar las principales dos señales para la interface S<sup>2</sup>C, que son SigOut y SigIn:

- SigIn: Provee datos desde la IC Segura
- SigOut: Provee el reloj y datos a la IC Segura

Se puede ver además que el NFCIP-1 hace las veces de puente para la información entre el lector externo y la IC Segura, usando las dos señales digitales: SigIn, SigOut. Además tres diferentes estilos de codificación (A, B, F) cumplen con todos los modos, tipos y tasas de datos de ECMA-340 (ISO/IEC 18092) e ISO/IEC 14443.

En resumen la interface S<sup>2</sup>C (SigIn-SigOut-Connection) requiere de un reloj a 13.56 MHz solamente en el lado de NFC, cumple totalmente y se acopla directamente con todos los modos, tipos y tasas de datos de los antes mencionados protocolos sin necesitar de alguna adaptación adicional o conversión de protocolo, cuenta con dos conexiones alámbricas para el intercambio de datos, es un concepto probado y conveniente, factible para su inmediata implementación.

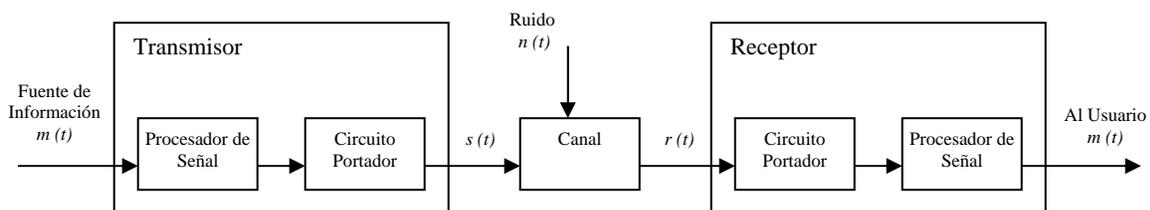
# ***CAPÍTULO 6***

## **CODIFICACIÓN Y MODULACIÓN**

6 Codificación y Modulación .....	159
6.1 Codificación en Banda Base .....	159
6.2 Procedimientos de Modulación Digital.....	162
6.2.1 Modulación por desplazamiento de amplitud ASK.....	162
6.2.2 Modulación 2 FSK .....	163
6.2.3 Modulación 2 PSK .....	164
6.2.4 Procedimientos de modulación con subportadora .....	164
6.3 Integridad de Datos .....	165
6.3.1 El procedimiento Checksum .....	165
6.3.1.1 Chequeo de paridad.....	166
6.3.1.2 Procedimiento LRC.....	166
6.3.1.3 Procedimiento CRC .....	166
6.3.2 Técnicas de Acceso múltiple y Anticolisión.....	167
6.3.2.1 Acceso Múltiple por División de Espacio (SDMA) .....	170
6.3.2.2 Acceso Múltiple en el Dominio de la Frecuencia (FDMA).....	172
6.3.2.3 Acceso Múltiple en el Dominio del Tiempo (TDMA) .....	173
6.3.2.4 Procedimientos anticolisión .....	174
6.4 Seguridad de los Datos .....	175
6.4.1 Autenticación Simétrica Mutua .....	176
6.4.2 Autenticación por medio de Claves Derivadas.....	178
6.4.3 Transferencia de Datos Encriptados .....	178
6.4.3.1 Cifrado Continuo.....	179

## 6 CODIFICACIÓN Y MODULACIÓN

El diagrama a bloques de la figura 6.1 describe un sistema digital de comunicación, de manera similar, la transferencia de datos entre lector y transponder en un sistema RFID requiere de tres principales bloques funcionales. De lector a transponder (la dirección de transferencia de datos) éstos bloques son: codificación de señal (*procesamiento de señal*), el modulador (*circuito portador*) en el lector (*transmisor*), el medio de transmisión (*canal*) y el demodulador (*circuito portador*) con el decodificador de señal (*procesamiento de señal*) en el transponder (*receptor*).



**Figura 6.1 Flujo de señal y datos en un sistema digital de comunicaciones**

Un sistema de código de señal toma el mensaje a transmitir y su *representación como señal* y los adecua óptimamente a las características del medio de transmisión. Este proceso implica proveer al mensaje con un grado de protección contra interferencia o colisión, incluso contra modificación intencional de ciertas características de señal. La codificación de señal no debe ser confundida con la modulación, por este motivo se le conoce como *codificación en banda base*.

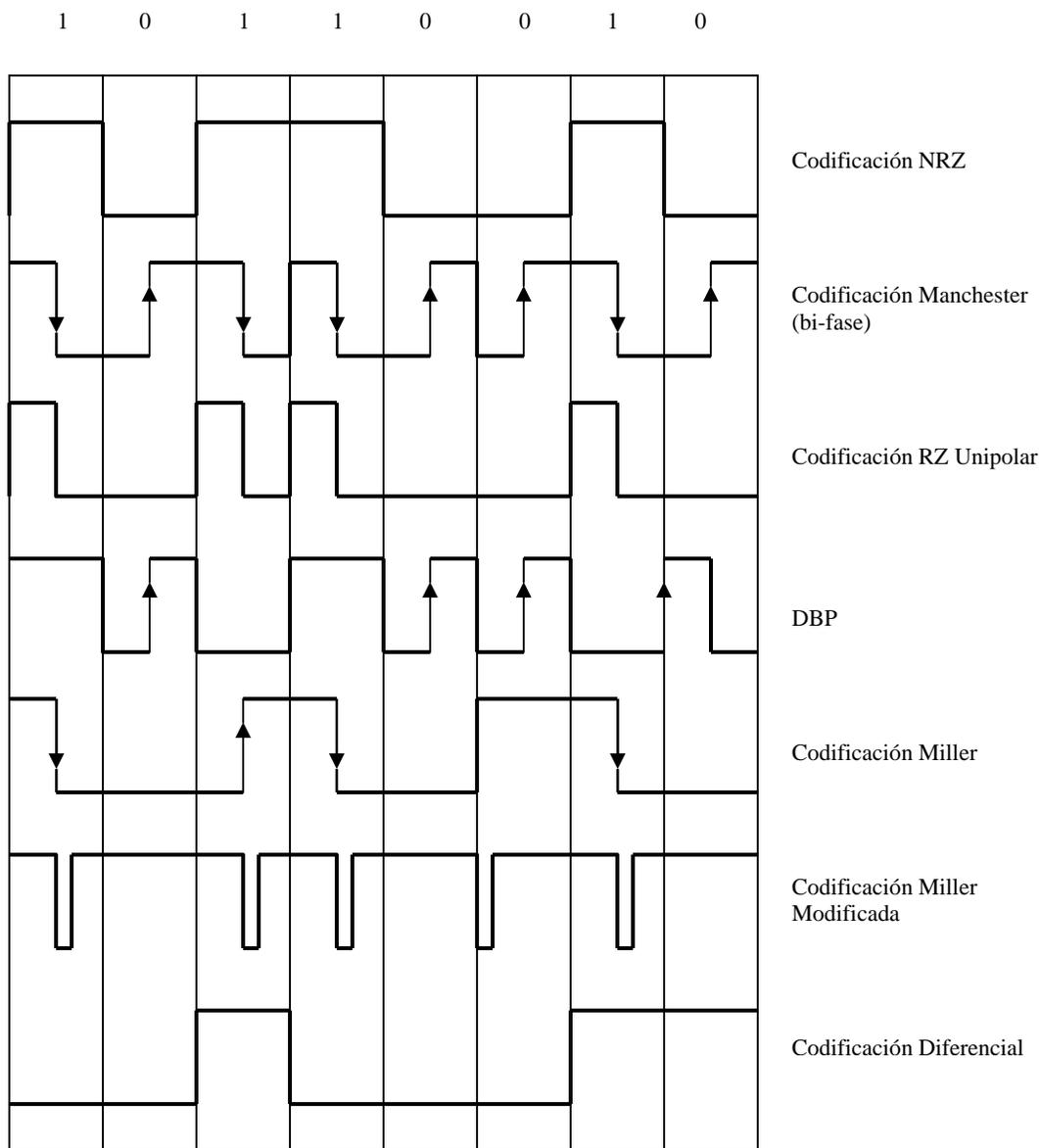
Como veíamos en capítulos anteriores, la modulación es el proceso de alterar los parámetros de una señal con una portadora de alta frecuencia, por ejemplo su amplitud, frecuencia o fase, en relación con una señal modulada o señal de banda base. El medio de transmisión transmite el mensaje sobre una distancia predeterminada. El único medio de transmisión usado en los sistemas RFID como sabemos son los campos magnéticos (acople inductivo) y las ondas electromagnéticas (microondas).

La *demodulación* es un proceso adicional a la modulación con el fin de reclamar la señal en banda base. Ya que usualmente existe una *fuerza de información* (entrada) tanto en el transponder como en el lector, una información es transmitida de manera alterna en ambas direcciones, estos componentes contienen tanto un *modulador* como un *demodulador*, a lo cual se le llama *módem*, un término que describe la configuración normal. La tarea de la decodificación de señal es la de reconstruir el mensaje original de la señal recibida codificada en banda base y el reconocer cualquier error de transmisión y *abanderarlos* como tal.

### 6.1 Codificación en Banda Base

Los ceros y unos binarios pueden ser representados en diferentes *códigos de línea*. Los sistemas RFID normalmente usan uno de los siguientes procedimientos de codificación:

NRZ, Manchester, RZ Unipolar, DBP (bi-fase diferencial), Miller, codificación Diferencial o codificación PP (ver fig 6.2).



**Fig 6.2 Codificación de Señal para sistemas RFID con frecuente cambio en códigos de línea**

**Codificación NRZ:** El 1 binario se representa con una señal “alta” y el 0 binario es representado con una señal “baja”. El código NRZ (No Retorno a Cero) se usa casi exclusivamente con modulación FSK o PSK.

**Codificación Manchester:** El 1 binario se representa con una transición negativa a la mitad del periodo de bit, mientras que el 0 binario es representado por una transición positiva. El código Manchester es también conocido como *split-phase coding* (codificación por división

de fase). El código Manchester es usado muy seguido para transmisiones de datos desde el transponder al lector, basándose en modulación de carga usando subportadora.

**Codificación RZ Unipolar:** El 1 binario se representa por una señal “alta” durante la primer mitad del periodo de bit, un 0 binario se representa con una señal “baja” que faltaría para completar la duración de bit entera.

**Codificación DBP:** El 0 binario se codifica como una transición de cualquier tipo en el medio periodo de bit, el binario 1 se codifica por la ausencia de transición. Además, el nivel es invertido al inicio de cada periodo de bit, de modo que el pulso de bits pueda ser reconstruido fácilmente en el receptor (si es necesario).

**Codificación Miller:** El 1 binario se representa por una transición de cualquier tipo en el medio periodo de bit, el 0 se representa por la continuidad del nivel de 1 sobre el siguiente periodo de bit. Una secuencia de ceros crea una transición al inicio de un periodo de bit, de manera que el pulso de bits pueda ser reconstruido fácilmente en el receptor (si es necesario).

**Codificación Miller Modificada:** En esta variante del código Miller, cada transición se reemplaza por un pulso “negativo”. El código Miller modificado es altamente conveniente para su uso en sistemas RFID acoplados inductivamente para la transferencia de datos del lector al transponder. Debido al corto periodo de duración de pulso ( $t_{\text{pulso}} \ll T_{\text{bit}}$ ) es posible asegurar un fuente de energía continua al transponder desde el campo HF del lector incluso durante la transferencia de datos.

**Codificación Diferencial:** En la codificación diferencial, cada binario 1 a transmitir causa un cambio (toggle) en el nivel de señal, donde el nivel de señal permanece sin cambio por un cero binario. La codificación diferencial se puede generar fácilmente de una señal NRZ usando una compuerta XOR y un flip-flop D.

**Codificación Pulso-Pausa:** EN la codificación pulso-pausa (PPC) el 1 binario se representa por una pausa de duración  $t$  antes que el pulso siguiente; el 0 binario se representa por una pausa de duración  $2t$  antes que el pulso siguiente. Este procedimiento de codificación es popular en sistemas RFID acoplados inductivamente para transferencia de datos del lector al transponder.

Debido a los muy cortos periodos de bit ( $t_{\text{pulso}} \ll T_{\text{bit}}$ ) es posible el asegurar una fuente de energía continua al transponder desde el campo HF del lector, incluso durante la transferencia de datos.

Varias consideraciones limitantes deben hacerse a la hora de seleccionar un sistema de señalización conveniente para un sistema RFID. La más importante consideración es el espectro de señal después de la modulación y la susceptibilidad a la transmisión de errores. Además, en el caso de transponders pasivos, la fuente de energía no se debe interrumpir por una inapropiada combinación de codificación de línea o procedimientos de modulación.

## 6.2 Procedimientos de Modulación Digital

La energía que es irradiada desde una antena a el área que la rodea en la forma de ondas electromagnéticas. Si cuidadosamente influimos en tres de los parámetros de la señal (potencia, frecuencia o fase) de una onda electromagnética, los mensajes se pueden codificar y transmitirse a cualquier punto dentro de esa área. Al procedimiento de influir en una onda electromagnética con mensajes (datos) se le llama *modulación*, y a una onda electromagnética no modulada se le llama portadora.

Analizando las características de una onda electromagnética en cualquier punto del área, podemos también reconstruir el mensaje midiendo el cambio en la potencia, frecuencia o posición de fase de recepción, éste proceso es conocido como demodulación.

La tecnología clásica de radio esta ampliamente ocupada por los procedimientos de modulación analógica, podemos diferenciar entre *modulación de amplitud*, *modulación en frecuencia* y *modulación de fase*, siendo éstas las principales tres variables de una onda electromagnética, todos los demás procedimientos demodulación derivan de algunos de estos tres tipos (ver capítulo 2). Son procedimientos que se emplean en sistemas RFID son los procedimientos digitales ASK (amplitude shift keying), FSK (frequency shift keying) y PSK (phase shift keying).

En cada procedimiento de modulación, productos modulados simétricos llamados, también llamados *bandas laterales* son generados alrededor de la portadora. El espectro y amplitud de las bandas laterales son influidos por el espectro de la señal codificada en banda base y por el proceso de modulación, de esta forma podemos diferenciar entre una banda lateral superior e inferior.

### 6.2.1 Modulación por desplazamiento de amplitud ASK

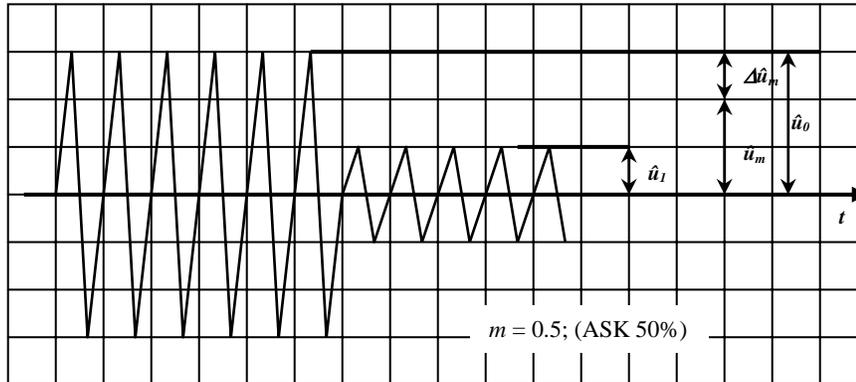
En la modulación por desplazamiento de amplitud, la amplitud de una oscilación portadora es conmutada entre dos estados  $u_0$  y  $u_1$  (desplazamiento) por un código binario de señal.  $U_1$  puede tomar valores entre  $u_0$  y 0. La razón de  $u_0$  a  $u_1$  es conocida como el factor de modulación  $m$  ó *duty factor* (para el caso de modulaciones digitales). Para hallar este factor de modulación  $m$  calculamos el valor aritmético de la amplitud codificada y no-codificada (keyed & unkeyed) de la señal portadora:

$$\hat{u}_m = \frac{\hat{u}_0 + \hat{u}_1}{2} \quad (6.1)$$

El factor de modulación es ahora calculado de la razón de cambio de amplitud  $\hat{u}_0 - \hat{u}_m$  al valor significativo  $\hat{u}_m$ :

$$m = \frac{\Delta \hat{u}_m}{\hat{u}_m} = \frac{\hat{u}_0 - \hat{u}_m}{\hat{u}_m} = \frac{\hat{u}_0 - \hat{u}_1}{\hat{u}_0 + \hat{u}_1} \quad (6.2)$$

En un 100% de ASK la amplitud de la oscilación de portadora es conmutada entre los valores de amplitud de portadora  $2\hat{u}_m$  y 0 (codificación encendido-apagado) ver fig 6.3. En la modulación en amplitud, usando una señal analógica (sinusoidal), esto podría corresponder con un factor de modulación de  $m = 1$  (ó 100%).



**Fig 6.3 En la modulación ASK, la amplitud de la portadora se desplaza entre dos estados por una señal binaria**

El procedimiento descrito para calcular el factor de modulación es el mismo que el que se usa para calcular el factor de modulación para AM, usando señales analógicas. De cualquier manera, existe una significativa diferencia entre la modulación digital y la analógica, en la digital, una portadora toma la amplitud  $\hat{u}_0$  en el estado no-modulado, mientras que en la modulación analógica, la señal portadora toma la amplitud  $\hat{u}_m$  en el estado no-modulado. En la literatura el factor de modulación digital “*duty factor*” es referido a veces como *reducción de porcentaje de portadora*  $m'$  durante la codificación, esta dado por:

$$m' = 1 - \frac{\hat{u}_1}{\hat{u}_0} \quad (6.3)$$

### 6.2.2 Modulación 2 FSK

En la modulación 2 *frequency shift keying* (*desplazamiento de frecuencia*), la frecuencia de una oscilación portadora es conmutada entre dos frecuencias  $f_1$  y  $f_2$  por una señal binaria codificada. La frecuencia portadora  $f_{CR}$  se define como el valor aritmético de las dos frecuencias características  $f_1$  y  $f_2$ . La diferencia entre la frecuencia portadora y las frecuencias características es en términos de la desviación de frecuencia  $\Delta f_{CR}$ :

$$f_{CR} = \frac{f_1 + f_2}{2}; \Delta f_{CR} = \frac{|f_1 - f_2|}{2} \quad (6.4)$$

En función del tiempo, la señal 2 FSK se puede considerar como la composición de dos señales desplazadas en frecuencia y con valores  $f_1$  y  $f_2$ . El espectro de una señal 2 FSK se obtiene entonces superponiendo el espectro de ambas señales desplazadas en amplitud. La codificación en banda base usada en los sistemas RFID produce una frecuencia asimétrica desplazada y codificada:

$$\tau \neq \frac{T}{2} \quad (6.5)$$

En estos casos siempre hay una distribución asimétrica de espectro en relación a la frecuencia media  $\Delta f_{CR}$

### 6.2.3 Modulación 2 PSK

En la modulación por desplazamiento de fase (*phase shift keying*), los estados binarios 0 y 1 de una señal codificada son convertidos en los correspondientes estados de fase de la oscilación portadora en relación a una fase de referencia. En 2 PSK la señal es conmutada entre los estados de fase  $0^\circ$  y  $180^\circ$ .

Matemáticamente hablando, el desplazamiento de la posición de fase entre  $0^\circ$  y  $180^\circ$ , corresponde con la multiplicación de la señal portadora por 1 y  $-1$ .

El espectro de potencia de una 2PSK se puede calcular como sigue para una relación marca-espacio  $\tau/T$  de 50%:

$$P(f) = \left( \frac{P \cdot T_s}{2} \right) \cdot \left[ \text{senc}^2 \pi(f - f_0)T_s + \text{senc}^2 \pi(f + f_0)T_s \right] \quad (6.6)$$

Donde P es la potencia de transmisión,  $T_s$  es la duración de bit ( $=\tau$ ),  $f_0$  es la frecuencia central y  $\text{senc}(x) = (\text{sen}(x)/x)$ .

La envolvente de las dos bandas laterales alrededor de la frecuencia portadora  $f_0$  cumple la función  $(\text{sen}(x)/x)^2$ . Esto conduce a cero posiciones en las frecuencias  $f_0 \pm 1/T_s$ , 90% de la potencia de transmisión es transmitida.

### 6.2.4 Procedimientos de modulación con subportadora

El uso de una *subportadora* modulada es muy amplio en las tecnologías de radio. En las emisiones VHF, una subportadora estéreo con una frecuencia de 38 kHz es transmitida a lo largo del canal de tono en banda base, la banda base contiene solamente la señal monótono. La señal diferencial “L-R” izquierda-derecha requerida para obtener los canales de tono L(izquierdo) y R(derecho) puede ser transmitido “silenciosamente” con la modulación de la subportadora estéreo. Entonces el uso de una subportadora representa una *modulación multinivel*. Esto para nuestro ejemplo es, la subportadora primero es modulada con la señal diferencial, en orden de que finalmente se module el transmisor VHF una vez más con la señal subportadora modulada.

En los sistemas RFID, los procedimientos de modulación usando una subportadora son principalmente utilizados en sistemas inductivamente acoplados en rangos de frecuencia de 6.78 MHz, 13.56 MHz ó 27.125 MHz y en la modulación de carga para transferencias de datos desde el transponder al lector. La modulación de carga de un sistema RFID inductivamente acoplado tiene un efecto similar a la modulación ASK de voltaje HF en la antena del lector. En vez de conmutar la *resistencia de carga* entre encendido y apagado al tiempo con una señal en banda base codificada, una subportadora de frecuencia bajase modula primero por la señal de datos codificados en banda base. La modulación ASK, FSK o PSK se puede seleccionar como el procedimiento de modulación para la subportadora. La *frecuencia de subportadora* en si misma es normalmente obtenida por la división binaria de la frecuencia operacional. Para los sistemas de 13.56 MHz, son usualmente usadas las frecuencias de subportadora de 847 kHz ( $13.56 \text{ MHz} \div 16$ ), 424 kHz ( $13.56 \text{ MHz} \div 32$ ) ó 212 kHz ( $13.56 \text{ MHz} \div 64$ ). La señal subportadora modulada es utilizada en este caso para conmutar el resistor de carga a los estados encendido y apagado.

La gran ventaja de utilizar una subportadora sólo se clarifica cuando consideramos el espectro de frecuencia generado. La modulación de carga con subportadora inicialmente genera dos líneas espectrales a una distancia de  $\pm$  la frecuencia de subportadora  $f_H$  alrededor de la frecuencia operacional. La información actualizada es hora transmitida en las bandas laterales de las dos líneas subportadoras, dependiendo de la modulación de la subportadora con la cadena de datos codificados en banda base. Si la modulación de carga en banda base fuere usada, por otro lado, las bandas laterales de la cadena de datos quedaría directamente al lado de la señal portadora a la frecuencia de operación.

En sistemas muy pobremente acoplados, la diferencia entre la señal portadora del lector  $f_T$  y las bandas laterales recibidas de la modulación de carga varían en función del rango (de 80-90 dB). Uno de los dos productos de modulación subportadora puede ser filtrado y demodulado desplazando la frecuencia de las bandas laterales de la cadena de datos modulada. Es irrelevante aquí si las frecuencias  $f_T + f_H$  ó  $f_T - f_H$  son usadas, debido a que la información es contenido de cualquiera de las bandas laterales.

## 6.3 Integridad de Datos

### 6.3.1 El procedimiento Checksum

Cuando se transmiten datos usando tecnología inalámbrica, es muy probable que se encuentre interferencia que causa cambios no deseados a los datos transmitidos, lo cual conduce a errores de transmisión.

Un procedimiento *checksum* se puede usar para reconocer errores de transmisión e iniciar medidas de corrección, por ejemplo la retransmisión de los bloques de datos erróneos. El más común de los procedimientos checksum son los chequeos de paridad, suma XOR y CRC.

### 6.3.1.1 Chequeo de paridad

El chequeo de paridad es un procedimiento muy simple y por lo tanto muy popular, en éste se incorpora un *bit de paridad* a cada byte y se transmiten juntos, con el resultado de que se transmiten 9 bits por cada byte. Antes de que la transferencia de datos tome lugar se debe tomar una decisión en cuanto a que tipo de paridad se tomará en cuenta (paridad par o impar), para asegurar que el remitente y destinatario verifiquen en base al mismo método.

El valor del bit de paridad se coloca de forma tal que si la paridad impar se utiliza, un número impar de los nueve bits debe tener como valor 1 y si se utiliza una paridad par, un número par de bits deben ser 1. La paridad par se puede interpretar además como la suma (checksum) horizontal *módulo 2* de los bits de datos. Esta suma horizontal también permite el cálculo de la OR exclusiva o compuerta lógica XOR de los bits de datos.

De cualquier manera, la simplicidad de este método se contrapone con su pobre reconocimiento de errores. Un número impar de bits invertidos (1, 3, 5,...) será detectado siempre, pero si existe un número par de bits invertidos (2, 4, 6,...) los errores se cancelan unos a otros y el bit de paridad aparecerá de manera correcta.

### 6.3.1.2 Procedimiento LRC

El checksum XOR conocido como *longitudinal redundancy check*- código de redundancia longitudinal se puede calcular rápida y fácilmente.

La suma XOR se genera por la compuerta recursiva XOR de todos los bits de datos en un bloque. El byte 1 se opera en XOR con el byte 2, el resultado de esta operación se opera a su vez en XOR con el byte 3 y así sucesivamente. Si el valor LRC se añade a un bloque de datos y se transmite con el, entonces una simple verificación para errores de transmisión se puede hacer en el receptor para generar un LRC a partir del bloque de datos más el byte LRC. El resultado de esta operación debe ser siempre cero; cualquier otro resultado indica que han ocurrido los errores de transmisión.

Debido a la simplicidad del algoritmo, los LRC se pueden calcular simple y rápidamente. De cualquier forma, los LRC's no son muy convenientes debido a la posibilidad de errores múltiples para cancelarse mutuamente y la verificación puede no detectar si los bytes han sido transpuestos en un bloque de datos, los LRC's son principalmente usados para el rápido chequeo de muy pequeños bloques de datos.

### 6.3.1.3 Procedimiento CRC

El procedimiento CRC *cyclic redundancy check*- código de redundancia cíclica se usó originalmente en los drives de disco y puede generar una suma de comprobación que es suficientemente rentable aún para cantidades muy grandes de datos. De cualquier forma es excelentemente conveniente para reconocimiento de errores en transferencia de datos vía cableado (teléfono) o interfaces inalámbricas (radio, RFID). El procedimiento CRC representa un método altamente rentable de reconocimiento de errores de transmisión, aunque no pueda corregirlos.

Tal como lo sugiere el nombre, el cálculo del CRC es un procedimiento cíclico, de manera que el cálculo del CRC incorpora el valor CRC del byte de datos a ser calculado más los valores CRC de todos los bytes de datos previos. Cada byte individual en un bloque de datos es verificado para obtener el valor CRC para todo el bloque de datos. Matemáticamente hablando, una suma de comprobación CRC se calcula dividiendo un polinomio usando un *generador polinomial*. El valor CRC es entonces el residuo obtenido de esta división.

Cuando se transmite un bloque de datos, el valor CRC de los mismos se calcula en el transmisor y ese valor se anexa al final de el bloque de datos para ser transmitido junto, El valor CRC de los datos recibidos, incluyendo el byte CRC anexado se calcula en el receptor. El resultado siempre es cero, a menos que existan errores de transmisión en el bloque recibido. La verificación de cero es un método muy simple de análisis del checksum CRC y evita el costoso proceso de comparación de checksums. De cualquier manera es necesario asegurarse de que ambos cálculos CRC comiencen con el mismo valor inicial.

La gran ventaja del CRC es la rentabilidad de reconocimiento de errores que se logra en un pequeño número de operaciones, incluso donde se presentan múltiples errores. Un CRC de 16 bits es conveniente para verificar la integridad de datos de bloques mayores de 4KB, arriba de este valor el rendimiento cae dramáticamente. Los bloques de datos que se transmiten en sistemas RFID son considerablemente más pequeños que 4KB, lo cual significa que los CRC's de 12 y 8 bits se pueden usar también adicionalmente al de 16 bits. Algunos ejemplos de diferentes polinomios generadores son:

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

Cuando los algoritmos CRC se desarrollaron en un principio como controladores de disco, la prioridad se le dio a la realización de un simple procesador CRC en la forma de circuito hardware, esto dio paso a un procesador CRC hecho de *registros de desplazamiento* acoplados espalda-espalda y compuertas XOR que son muy fáciles de implementar.

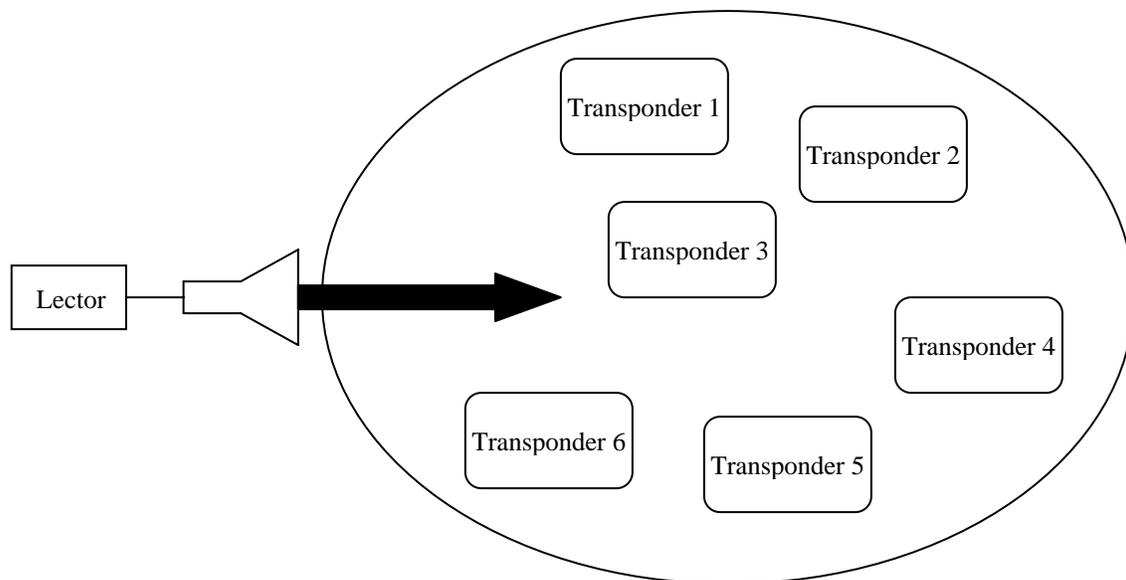
Cuando se calcula el CRC-16 usando registros de desplazamiento, el registro de desplazamiento de 16 bits se coloca primeramente en su valor inicial, entonces el cálculo comienza desplazando los bits de datos, empezando con el de menor valor, dentro del registro de desplazamiento espalda-espalda y uno después del otro. La división espalda-espalda o polinomial se basa en los bits CRC operados lógicamente en XOR. Cuando todos los bits se han desplazado a través del registro, el cálculo está completo y el contenido del registro CRC de 16 bits representa el CRC deseado.

### 6.3.2 Técnicas de Acceso múltiple y Anticolisión

La operación de sistemas RFID usualmente implican situaciones en que numerosos transponders están presentes en la zona de interrogación de un solo lector al mismo tiempo. En tales sistemas (que consiste de una *estación de control*, el lector y un número de

*participantes*, los transponders) podemos diferenciar entre dos principales formas de comunicación.

La primera se usa para transmitir datos desde un lector a los transponders (fig 6.4), la cadena de datos transmitida se recibe por todos los transponders simultáneamente, esto es comparable con la recepción simultánea de cientos de radio receptores de un programa de noticias transmitido por una estación de radio. A éste tipo de comunicación se le conoce como *broadcast*.

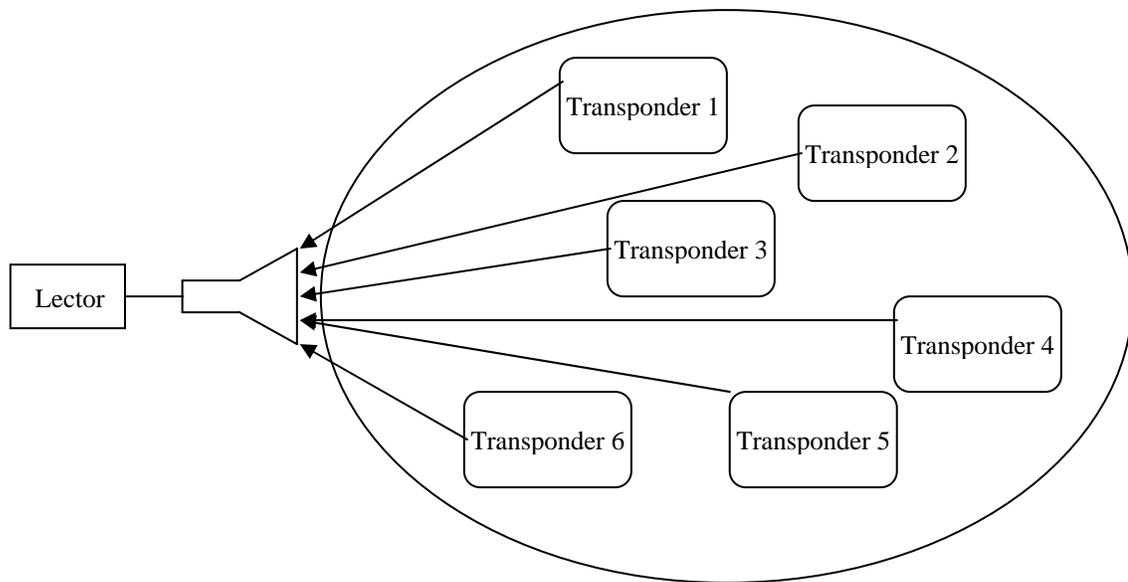


**Fig. 6.4 Modo Broadcast; los datos transmitidos por un lector son recibidos simultáneamente por todos los transponders en la zona de interrogación**

La segunda forma de comunicación implica la transmisión de datos desde muchos transponders individuales en la zona de interrogación del lector hacia el lector. Esta forma de comunicación es llamada *multi-acceso* (fig 6.5).

Cada canal de comunicación tiene una capacidad de canal definida, la cual se determina con la máxima tasa de datos de este canal de comunicación y el tiempo de disponibilidad del mismo. La capacidad disponible de canal debe dividirse entre los participantes (transponders) individualmente, de manera que los datos se puedan transferir desde varios transponders a solo un lector sin interferencia mutua (colisión).

En un sistema RFID inductivo, por ejemplo, sólo la sección receptora en el lector esta disponible para todos los transponders en la zona de interrogación como un canal común para transferencia de datos hacia el lector. La máxima tasa de datos se encuentra del ancho de banda efectivo de las antenas en el transponder y lector.



**Fig. 6.5 Acceso múltiple al lector; varios transponders intentan transferir datos al lector simultáneamente**

El problema del acceso múltiple ha estado presente desde hace ya un tiempo en la tecnología de radio. Los ejemplos incluyen a los satélites de noticias y redes telefónicas móviles, donde un número de participantes tratan de acceder a un mismo satélite o estación base (fig6.5). Por esta razón, numerosos procedimientos se han desarrollado con el objetivo de separar a las señales individuales que participan de otras. Básicamente, existen cuatro diferentes procedimientos *acceso múltiple por división de espacio (SDMA)*, *acceso múltiple por división de frecuencia (FDMA)*, *acceso múltiple por división de tiempo (TDMA)* y el *acceso múltiple por división de código (CDMA)*, este último también conocido como *espectro ensanchado*. De cualquier manera estos procedimientos clásicos se basan en asumir una cadena de datos ininterrumpida desde y hacia los participantes, una vez que la capacidad del canal ha sido separada, así permanece hasta que la comunicación finalice.

Los transponders RFID por otro lado, se caracterizan por breves periodos de actividad esparcidos en pausas de longitud desigual. Una tarjeta inteligente de no-contacto en forma de una tarjeta de transporte público, la cual es llevada dentro de la zona de interrogación de un lector, tiene que ser autenticada, leída y grabada dentro de unos pocos milisegundos, a lo cual puede seguir un periodo largo en el cual ninguna tarjeta inteligente entre a la zona de interrogación. Como sea, este ejemplo no debe llevarnos a la conclusión de que el acceso múltiple no es necesario para este tipo de aplicación. La situación en que un pasajero posee dos o tres tarjetas inteligentes de no-contacto del mismo tipo en su cartera, la cual el mantiene colocada hacia la antena de un lector, se debe tener en cuenta. Un procedimiento poderoso de acceso múltiple es capaz de seleccionar la tarjeta correcta y deducir la tarifa sin ninguna demora detectable, incluso en estos casos. La actividad en un canal de transmisión entre el lector y el transponder posee un muy alto factor de ráfaga, y entonces hablamos también de un procedimiento de acceso a paquetes.

La capacidad del canal se separa sólo lo que es necesario (p.ej. durante la selección de un transponder en la zona de interrogación del lector). La realización técnica de un procedimiento de acceso múltiple en sistemas RFID propone unos cuantos retos para el transponder y el lector, ya que se tiene que prevenir convenientemente a los datos de transponder (paquetes) de colisionar unos con otros en el receptor del lector y de esta forma volverse ilegibles, sin que esto cause una demora perceptible. En el contexto de sistemas RFID, un procedimiento técnico (protocolo de acceso) que facilita el manejo del acceso múltiple sin ninguna interferencia es llamado *sistema anticolidión*.

El hecho de que un paquete de datos enviado a un lector para un solo transponder (p.ej en modulación de carga) no pueda ser leído por todos los demás transponders en la zona de interrogación de este lector, propone un reto particular para casi todos los sistemas RFID. De esta forma, un transponder no puede de primera instancia detectar la presencia de otros transponders en la zona de interrogación del lector.

Por razones de competitividad, los fabricantes de sistemas no están generalmente preparados para publicar los procedimientos anticolidión que utilizan. De cualquier manera, se puede encontrar poco en este asunto en la literatura técnica, por lo que un estudio exhaustivo para comprender este asunto no es, desafortunadamente, posible en este punto. Más adelante vamos a ver una breve descripción de lo que son los más importantes procedimientos empleados.

### **6.3.2.1 Acceso Múltiple por División de Espacio (SDMA)**

El término *acceso múltiple por división de espacio* tiene relación con las técnicas que reusan un cierto recurso (capacidad de canal), en áreas espacialmente separadas.

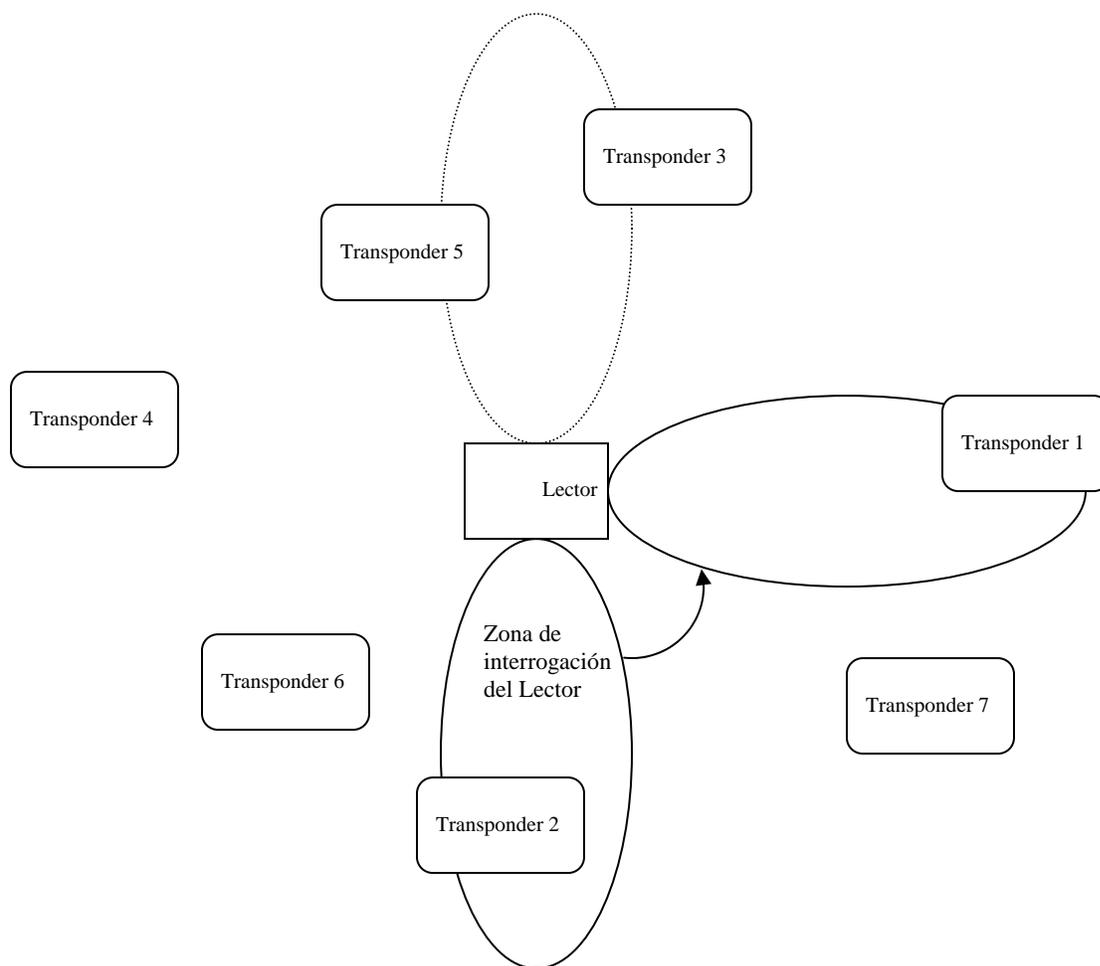
Una opción es la de reducir significativamente el rango de un solo lector, pero compensarlo juntando un gran número de lectores y antenas para formar un arreglo, de manera que se provea la cobertura a un área. Como resultado, la capacidad del canal para conjuntar lectores se hace disponible repetidamente. Tales procedimientos han sido exitosamente utilizados en eventos de maratón de gran escala para detectar los tiempos de carrera de atletas con transponders. En esta aplicación un número de antenas lectoras son insertadas en una *mat<sup>1</sup> tartan*. El corredor viajando sobre la mat “porta” su transponder sobre la zona de interrogación de unas cuantas antenas que forman parte del bosquejo completo. Un amplio número de transponders pueden así ser leídos simultáneamente como resultado de la distribución espacial de los corredores sobre la vista completa.

Otra opción es usar una antena direccional electrónicamente controlada en el lector, por la directividad de la antena, ésta se puede apuntar hacia un transponder (SDMA adaptativo).

---

<sup>1</sup> Arreglo de antenas lectoras que se colocan dentro de los delgados *mat* y entonces pueden ser colocados en el suelo y estar protegidos de todas las influencias del ambiente. Las dimensiones de mat sencilla son 2.10m x 1.00m. en velocidad de carrera normal, una resolución de red de  $\pm 1$  s. La exactitud para los atletas mejora los  $\pm 0.2$  s.

De manera que varios transponders puedan ser diferenciados por su posición angular en la zona de interrogación del lector. Arreglos de antenas en fase son usados como antenas direccionales electrónicamente controladas, estas consisten de varias antenas de dipolo, y por consiguiente el SDMA adaptativo sólo puede ser ocupado para aplicaciones RFID en frecuencias arriba de los 850 MHz (típicamente 2.45 GHz) como resultado del tamaño de las antenas. Cada uno de los elementos del dipolo es llevado hasta cierta posición de fase independiente. El diagrama direccional de la antena se encuentra de las diferentes superposiciones de las ondas individuales de los elementos dipolo en diferentes direcciones. En ciertas direcciones los campos individuales de la antena dipolo se superponen en fase, lo cual conduce a la amplificación del campo. Para colocarlos en dirección, los elementos individuales son alimentados con un voltaje HF (alta frecuencia) de fase variable y ajustable por modificadores controlados de fase. En orden de direccionar un transponder, el espacio alrededor del lector debe ser escaneado usando una antena direccional, hasta que un transponder se detecta con la “búsqueda ligera” del lector (fig 6.6).



**Fig. 6.6 SDMA adaptativo con una antena direccional electrónicamente controlada. La cobertura direccional es apuntada a los diferentes transponders uno tras otro**

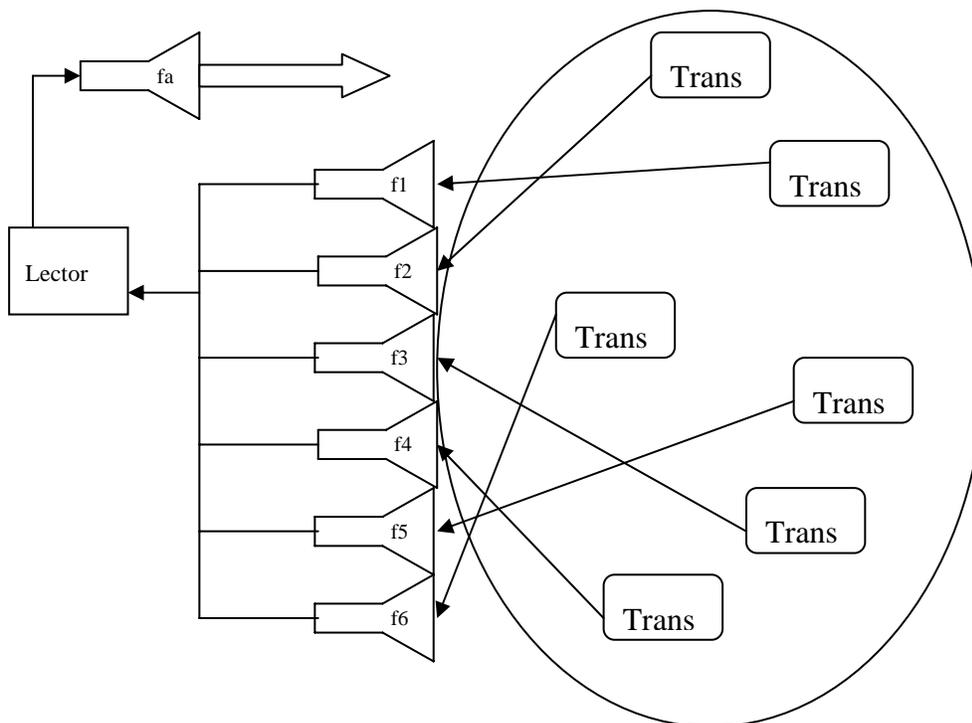
Una desventaja de la técnica SDMA es el relativamente alto costo de implementación del complicado sistema de antena. El uso de este tipo de procedimiento anticolidión se restringe entonces a sólo unas cuantas aplicaciones especializadas.

### 6.3.2.2 Acceso Múltiple en el Dominio de la Frecuencia (FDMA)

El término *acceso múltiple en el dominio de la frecuencia* tiene que ver con las técnicas en las cuales diferentes canales de transmisión en varias frecuencias portadoras están simultáneamente disponibles a los participantes de la comunicación.

En los sistemas RFID, esto se puede lograr usando transponders con una frecuencia de transmisión anarmónica ajustable. La fuente de energía al transponder y la transmisión de señales de control (broadcast) toman lugar a la frecuencia de lector  $f_a$  óptima. Los transponders responden a una de varias frecuencias de respuesta  $f_1-f_N$  (fig. 6.7). Por consiguiente, rangos de frecuencia completamente diferentes pueden ser usados para la transferencia de datos desde y hacia los transponders por ejemplo lector-transponder (downlink) a 135 kHz ó transponder-lector (uplink) diferentes canales en el rango de 433-435 MHz.

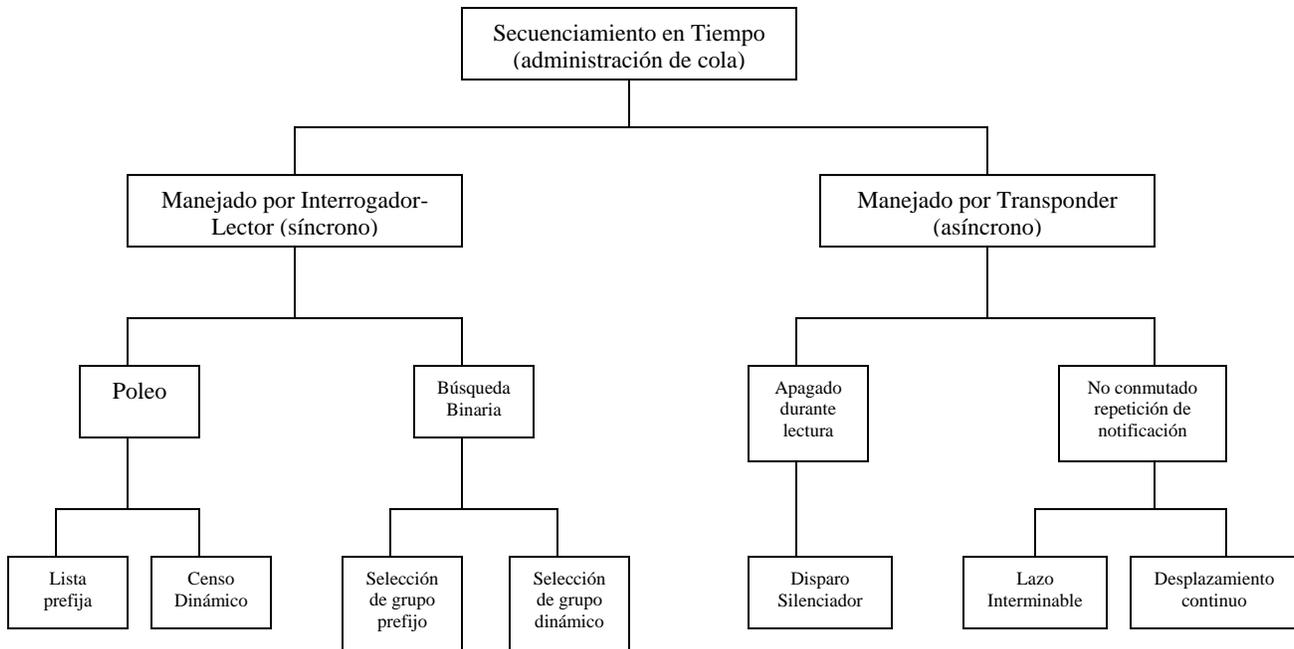
**Una opción para la modulación de carga en sistemas RFID es la de usar varias frecuencias subportadoras independientes para la transmisión de datos desde el transponder al lector. Una desventaja del procedimiento FDMA es el alto costo relativo de los lectores, debido a que un receptor dedicado debe proveerse para cada canal de recepción. Este procedimiento anticolidión, una vez más, permanece limitado a algunas cuantas aplicaciones especializadas.**



**Fig. 6.7**  
En un Procedimiento FDMA, varios canales de frecuencia están disponibles para la transferencia de datos de los transponders al lector

### 6.3.2.3 Acceso Múltiple en el Dominio del Tiempo (TDMA)

El término *acceso múltiple en el dominio del tiempo* se relaciona con las técnicas en las cuales toda la capacidad de canal disponible es dividida entre los participantes cronológicamente. Los procedimientos TDMA tienen amplio uso particularmente en el campo de los sistemas digitales de radio móviles. En los sistemas RFID, los procedimientos TDMA son por mucho el mayor grupo de procedimientos anticolidión. Diferenciaremos entre procedimientos *manejados por transponder* y los *manejados por lector* (ver fig. 6.8).



**Fig. 6.8 Clasificación de los procedimientos anticolidión en el dominio del tiempo para RFID**

Los procedimientos manejados por transponder funcionan de forma asíncrona, ya que el lector no controla la transferencia de datos. Este es el caso por ejemplo en el procedimiento ALOHA, el cual se describe un poco más en la siguiente sección (para más detalles ver Abramsom, Finkenzeller). Además diferenciamos entre procedimientos “apagado” y “no conmutado” dependiendo si un transponder se apaga debido a una señal desde el lector después de una exitosa transferencia de datos.

Los procedimientos manejados por transponder son por naturaleza muy lentos e inflexibles. Debido a esto muchas aplicaciones usan procedimientos que se controlan por el lector como maestro (manejados por interrogador). Estos procedimientos pueden ser considerados como síncronos, ya que todos los transponders se controlan y verifican por el lector simultáneamente. Un solo transponder se selecciona primeramente de un gran grupo de transponders en la zona de interrogación del lector usando un cierto algoritmo y después la comunicación toma lugar entre el transponder seleccionado y el lector. Desde ese momento sólo una comunicación se inicia en un cierto tiempo, pero los transponders se pueden

operar en sucesiones rápidas, los procedimientos manejados por interrogador son también conocidos como procedimientos *time duplex*. Los procedimientos manejados por interrogador se subdividen en procedimientos de *poleo* y *búsqueda binaria*. Todos estos procedimientos se basan en transponders que están identificados por un único número serial.

El procedimiento de poleo requiere una lista de todos los números seriales de transponder que puedan resultar en una aplicación. Todos los números seriales son interrogados por el lector uno después del otro, hasta que un transponder con un número serial idéntico responde. Este procedimiento puede, de cualquier manera, ser muy lento, dependiendo del número de posibles transponders y por lo tanto es recomendable solamente para aplicaciones con sólo algunos transponders conocidos en el campo de interrogación.

Los procedimientos de búsqueda binaria son los más flexibles, por lo tanto los más comunes. En un procedimiento de búsqueda binaria, un transponder se selecciona de un grupo intencionalmente, causando una colisión de datos en los números seriales de transponder transmitidos al lector siguiendo un comando *request* desde el lector. Si este procedimiento es exitoso sería crucial que el lector sea capaz de determinar la posición correcta de bit de una colisión usando un sistema de codificación de señal conveniente.

#### **6.3.2.4 Procedimientos anticolidión**

A continuación se explicarán superficialmente los procedimientos ALOHA para señales de datos, utilizados usualmente para transferencias de los mismos, para una descripción mas a detalle, ver Abramsom y Finkenzeller.

#### **ALOHA y ALOHA Ranurado**

La primera de las técnicas de contención o de acceso aleatorio para datos es ALOHA que se desarrolló para las redes de paquetes en radio, específicamente en los 70's para ALOHANET en Hawaii. En esta técnica tan pronto como se halla un paquete disponible, se envía desde el transponder al lector, por lo cual es un proceso estocástico TDMA manejado por transponder. De cualquier manera se le puede aplicar a cualquier medio de transmisión compartido. ALOHA o ALOHA puro como se le llama a veces esta verdaderamente disponible para todos (participantes) por igual. Insistiendo cuando sea que un transponder quiera enviar un paquete, simplemente lo hace y el lector entonces escucha en un tiempo considerado, de acuerdo a la técnica de acceso múltiple utilizada.

Haremos una analogía para ilustrar lo anterior con el caso del acceso al control de medio en ambientes LAN. Si una estación tiene alguna trama por enviar lo hace, la estación entonces escucha un tiempo igual a la máxima propagación posible para una topología en bus en viaje redondo (dos veces el tiempo que se toma el mandar una trama entre la dos estaciones más ampliamente separadas) más un pequeño incremento de tiempo, si la estación escucha una señal de respuesta (*acknowledgment*) durante ese tiempo, de otra manera reenvía la trama. Si la estación falla al recibir un *acknowledgment* después de repetidas transmisiones, se detiene. Una estación receptora determina si la trama que llega está libre de errores examinando la secuencia de su campo de verificación, como en HDLC. Si la trama es

válida y la dirección destino en la cabecera de la trama concuerda con la dirección de recepción, la estación inmediatamente envía un acknowledgment a la fuente. La trama puede ser invalidada debido a ruido en el canal o por que otra estación se encuentre transmitiendo una trama al mismo tiempo, para este último caso ambas tramas pueden interferirse en el receptor así que de todas formas no pasarían, esto es lo que se conoce como *colisión*. Si se determina que una trama recibida es inválida, la estación receptora simplemente ignora esa trama.

ALOHA es tan simple como se ve y paga un precio por ello. Debido a que el número de colisiones aumenta rápidamente cuando se incrementa la carga, la utilización máxima del canal es de tan solo cerca de 18%.

Para mejorar la eficiencia, se desarrolló una modificación de ALOHA llamada *ALOHA ranurada*. Para ilustrarlo retomaremos el ejemplo de red que se había tomado en cuenta. En este último esquema, el tiempo en el canal se organiza en ranuras de tiempo uniformes cuyo tamaño es igual al tiempo de transmisión de trama. Algún tipo de reloj central u otra técnica se utiliza para sincronizar a todas las estaciones (en el caso de sistemas RFID lo controla el lector). Sólo se permite que la transmisión inicie en un límite de ranuración, de esta forma, las tramas que se evita la transposición de tramas, lo que incrementa la utilización máxima del sistema a alrededor de 37%.

En los sistemas RFID, no necesariamente se tiene que dar el caso de una colisión de datos si varios paquetes se envían al mismo tiempo: si un transponder está más cerca del lector que los otros, éste transponder será capaz de arrollar los paquetes de datos de otros transponders como resultado de la mayor fuerza de señal en el lector, a esto se le conoce como el *efecto de captura*. El efecto de captura tiene un muy benéfico efecto sobre cualquier ambiente. Decisivo para lo anterior es el *umbral* magnético que indica la cantidad de fuerza de campo magnético con la cual un paquete debe contar para ser más fuerte que otros y ser detectado por el receptor sin ningún error, esta cantidad es característica de cada sistema.

#### **6.4 Seguridad de los Datos**

Los sistemas RFID cada vez son más usados en aplicaciones de alta seguridad, como sistemas de acceso y sistemas para hacer pagos, emisión de tickets o un conjunto de todo esto en un solo dispositivo 3G usado para transporte, compra de boletos o como tarjeta de crédito como lo hemos visto. De cualquier manera, el uso de sistemas RFID en estas aplicaciones necesita del uso de medidas de seguridad para protegerlos contra *intentos de ataque*, en los cuales la gente intenta violar el sistema RFID para obtener acceso no autorizado a edificios o permitirse a sí mismos algunos servicios sin pagar, desde un punto de vista tal vez inocente (sin mente criminal). Lo anterior no es nada nuevo, sólo debemos echar un vistazo a los mitos e historias de hadas para ver algunos ejemplos de intentos de burlar a los sistemas de seguridad. Como ejemplo tenemos a *Ali Baba* que fue capaz de tener acceso a la supuestamente segura guarida de los 40 ladrones cuando descubrió la contraseña secreta.

Los modernos *protocolos de autenticación* también trabajan de una forma parecida, verificando el conocimiento de un secreto (p.ej. una clave criptográfica). De cualquier manera, algoritmos convenientes pueden ser empleados para prevenir que la clave secreta sea descubierta. Los sistemas de alta seguridad RFID deben poseer una defensa contra los siguientes ataques individuales:

- Lectura no autorizada de un portador de datos (transponder) para duplicarlo y/o modificar datos.
- La colocación de un transponder extraño dentro de la zona de interrogación de un lector con la intención de ganar acceso no autorizado a un edificio o recibir servicios sin pagar.
- Inmiscuirse en las comunicaciones de radio y reproducir los datos en función de imitar a un portador de datos genuino.

Cuando seleccionamos un sistema RFID rentable, alguna consideración debe hacerse a las funciones criptológicas. Las aplicaciones que no requieren una función de seguridad (p.ej. automatización industrial, reconocimiento de herramienta) podrían ser innecesariamente caras con la incorporación de protocolos criptológicos. Por otro lado, en aplicaciones de alta seguridad (p.ej. boletaje, sistemas de pago) la omisión de procedimientos criptológicos puede significar un muy alto costo si la manipulación de transponders se usa para ganar acceso a servicios sin autorización.

#### **6.4.1 Autenticación Simétrica Mutua**

Una autenticación mutua entre lector y transponder se basa en el principio de autenticación mutua *three-pass* en concordancia con el estándar ISO 9798-2, en el cual ambos participantes en la comunicación verifican el conocimiento del secreto por parte de su contraparte (clave criptológica secreta).

En este procedimiento, todos los transponders y receptores que forman parte de una aplicación tienen posesión de la misma *clave criptológica* secreta  $K$  (procedimiento simétrico). Cuando un transponder entra primero a la zona de interrogación de un lector no se puede asumir que ambos participantes en la comunicación pertenezcan a la misma aplicación. Desde el punto de vista del lector, hay la necesidad de proteger la aplicación de la manipulación usando datos falsificados. De la misma forma, en la parte del transponder hay una necesidad de proteger los datos almacenados de lectura no-autorizada o sobre-escritura.

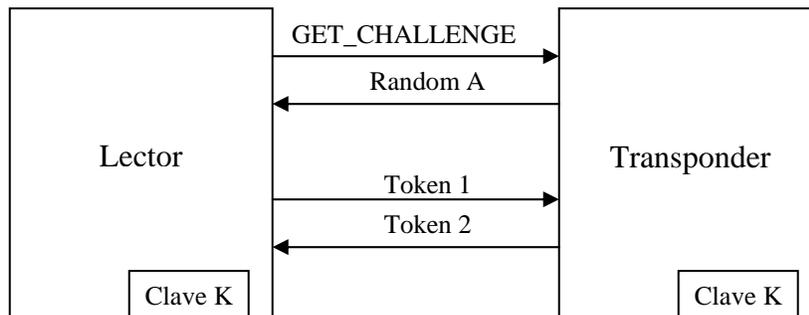
El procedimiento de autenticación mutuo empieza con el lector enviando un comando GET\_CHALLENGE al transponder. Un número aleatorio  $R_A$  es entonces generado dentro del transponder y enviado de vuelta al lector. El lector ahora genera un número aleatorio  $R_B$ . Usando la clave común secreta  $K$  y un algoritmo clave común  $e_K$ , el lector calcula un bloque de datos encriptado (token 1), el cual contiene tanto números aleatorios y datos de control adicionales y manda este bloque de datos al transponder:

$$Token1 = e_K(R_B \| R_A \| ID_A \| Text1)$$

El token 1 recibido es decodificado en el transponder y el número aleatorio  $R'_A$  contenido en el texto plano se compara con el previamente transmitido  $R_A$ . Si las dos figuras corresponden, entonces el transponder ha confirmado que las dos claves comunes corresponden. Otro número  $R_{A2}$  se genera en el transponder y este es usado para calcular un bloque de datos codificado (token 2), el cual además contiene a  $R_B$  y datos de control. Token 2 se envía desde el transponder al lector:

$$Token2 = e_K(R_{A2} \| R_B \| Text2)$$

El lector decodifica el token 2 y verifica si  $R_B$ , el cual se envió previamente, corresponde con  $R'_B$  el cual ha sido apenas recibido, si ambas figuras corresponden, entonces el lector está satisfecho con que la clave común ha sido comprobada. Tanto transponder como lector tienen la determinación ahora de que pertenecen al mismo sistema y una comunicación legitimizada entre ambas partes se puede establecer, permitiendo la transferencia de datos relevantes (fig 6.9).



**Fig. 6.9 Procedimiento de Autenticación Mutua entre Transponder y Lector**

En suma, el procedimiento de autenticación mutua tiene las siguientes ventajas:

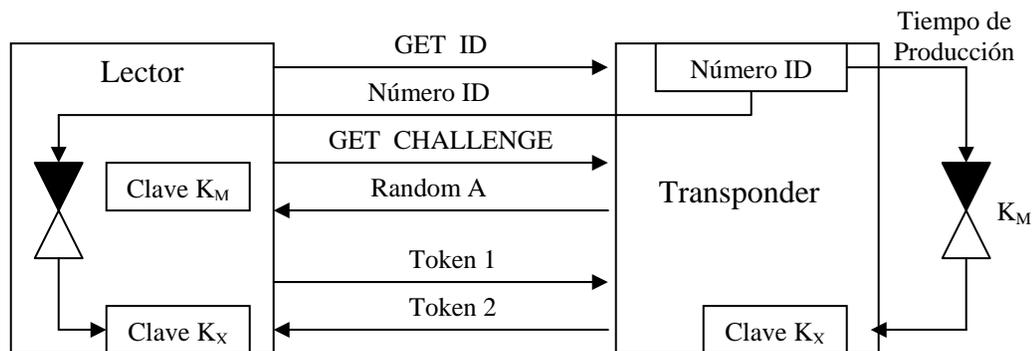
- Las claves secretas nunca se transmiten sobre las ondas aéreas, sólo los números aleatorios encriptados son transmitidos.
- Dos números aleatorios son siempre encriptados simultáneamente. Esto deja fuera la posibilidad de hacer una transformación inversa usando  $R_A$  para obtener el token 1, con la ayuda del cálculo de la clave secreta.
- El token se puede encriptar usando cualquier algoritmo.
- El uso estricto de números aleatorios desde dos fuentes independientes (transponder, reader) significa que grabar una secuencia de autenticación para reproducirla después fallaría.
- Una clave aleatoria (clave de sesión) se puede calcular de los números aleatorios generados, en función de criptológicamente asegurar la subsecuente transmisión de datos.

### 6.4.2 Autenticación por medio de Claves Derivadas

Una desventaja del método de autenticación anterior es que todos los transponders pertenecientes a una aplicación se aseguran usando una clave criptológica idéntica  $K$ . Para aplicaciones que envuelven una vasta cantidad de transponders (p.ej. sistemas de boletaje para la red de transporte público) esto representa una potencial fuente de riesgo. Debido a que tales transponders son accesibles a cualquiera en incontables números, la poca probabilidad de que la clave para un transponder sea descubierta debe ser tomada en cuenta, si eso ocurre, el procedimiento descrito anteriormente estaría totalmente abierto a la manipulación.

Una mejora significativa en el proceso de autenticación descrito se puede lograr asegurando cada transponder con una clave criptológica diferente. Para lograr esto, el número serial de cada transponder es leído durante su producción, entonces una clave  $K_X$  se calcula (se deriva) usando un algoritmo criptológico y una *clave maestra*  $K_M$ , de esta forma se inicializa el transponder. De esta forma cada transponder recibe una clave ligada a su propio número ID y la clave maestra  $K_M$ .

La autenticación mutua empieza cuando el lector pide el número ID del transponder (fig.6.10). En un modulo especial de seguridad en el lector, el SAM (módulo de autenticación segura), se calcula la clave de transponder específica usando la clave maestra  $K_M$ , de esta forma éste se puede utilizar para iniciar el proceso de autenticación. El SAM normalmente toma forma de una tarjeta inteligente de contacto incorporados en un cripto-procesador, lo cual significa que la clave maestra almacenada jamás podrá ser leída.



**Fig 6.10 Procedimiento de Autenticación por clave derivada**

### 6.4.3 Transferencia de Datos Encriptados

Existen algunos métodos para lidiar con la interferencia causada por efectos físicos durante la transmisión de datos (secc. 6.3), ahora extenderemos este modelo a un potencial atacante. Podemos diferenciar entre dos tipos básicos de ataque: el atacante 1 con comportamiento pasivo que intenta inmiscuirse en la transmisión para descubrir información confidencial con propósitos injustos; el atacante 2, por otro lado, permanece activo para manipular los datos transmitidos y alterarlos para su beneficio.

Los procedimientos criptológicos se utilizan para proteger a los sistemas contra ataques pasivos y activos. Para lograr esto, los datos transmitidos (texto plano) pueden ser alterados (encriptados) antes de una transmisión con la intención de que un atacante potencial no pueda ya sacar conclusiones acerca del contenido actual del mensaje (texto plano).

Una *transmisión de datos encriptados* siempre tiene lugar de acuerdo al mismo patrón. Los datos de transmisión (texto plano) se transforman en datos cifrados (texto cifrado), usando una clave secreta  $K$  y un algoritmo secreto. Sin conocer el algoritmo de encriptado y la clave secreta  $K$ , a un atacante potencial no le es posible interpretar los datos grabados. No es posible recrear los datos transmitidos a partir de los datos cifrados.

Los datos cifrados son transformados de vuelta a su forma original en el receptor usando la clave secreta  $K'$  y el algoritmo secreto (descifrado). Si las claves  $K$  para cifrado y  $K'$  para descifrado son idénticas ( $K=K'$ ) o tienen relación directa, el procedimiento es un *procedimiento de clave simétrica*. Si el conocimiento de la clave  $K$  es irrelevante para el proceso de descifrado, el procedimiento es un *procedimiento de clave asimétrica*. Los sistemas RFID han usado por un largo tiempo solamente procedimientos simétricos, por consiguiente a continuación se describirán sólo este tipo de procedimientos.

Si cada carácter es individualmente encriptado antes de la transmisión, el procedimiento se conoce como *cifrado secuencial* (ó cifrado continuo). Si, por otro lado, diferentes caracteres se incorporan en un bloque entonces hablamos de un cifrado en bloque. Debido a que los cifrados en bloque son generalmente muy exhaustivos en cálculos, éstos juegan un rol menos importante en los sistemas RFID, debido a esto el énfasis de las siguientes líneas se centra en el cifrado secuencial.

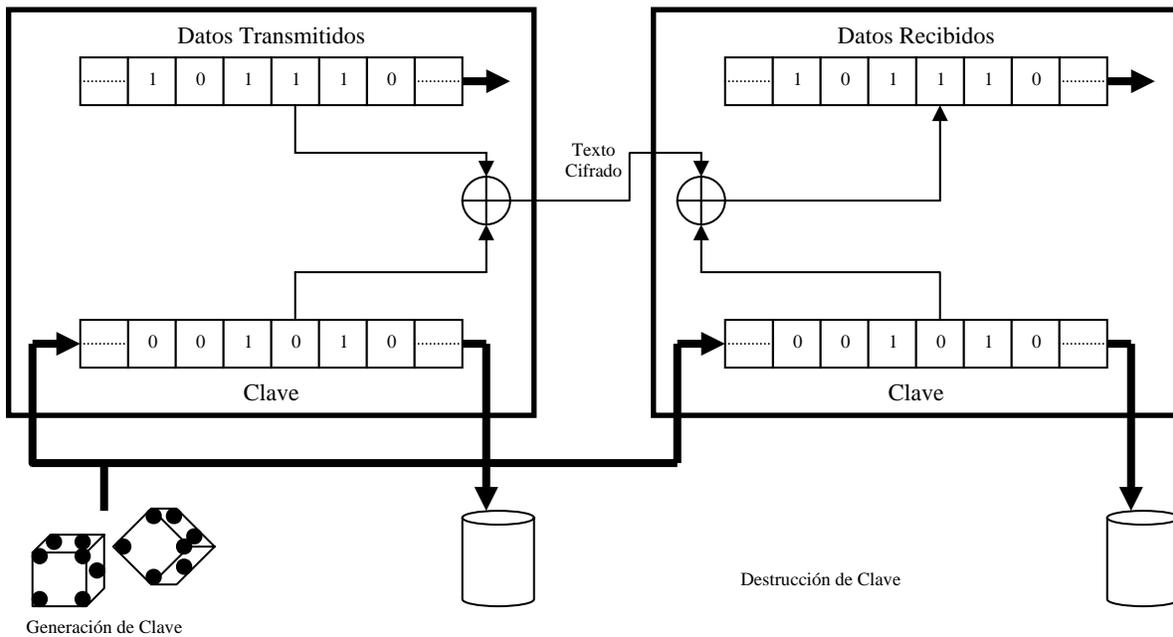
Un problema fundamental de todos los procedimientos criptológicos tiene que ver con la distribución segura de la clave secreta  $K$ , la cual debe ser conocida por los participantes de comunicación autorizados antes del inicio del proceso de transferencia de datos.

#### **6.4.3.1 Cifrado Continuo**

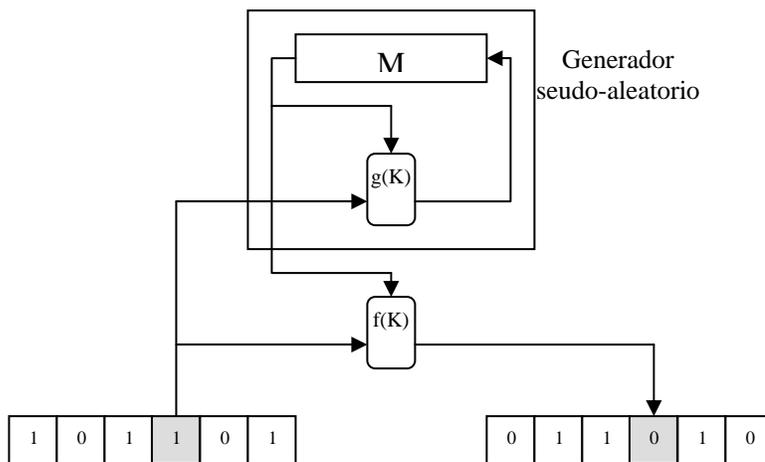
Los cifrados secuenciales o continuos son algoritmos de encriptado en los cuales la secuencia de caracteres texto plano se encriptan secuencialmente usando una función diferente en cada paso. La idealización de un cifrado continuo se puede ver en el cifrado one-time pad, también conocido como *cifrado Vernam* después de su descubrimiento.

En éste procedimiento una clave aleatoria(dados)  $K$  es generada antes de la transmisión de datos encriptados y ésta clave se hace disponible para ambas partes (fig. 6.11) La clave secuencial se liga con la secuencia de texto plano con la adición de caracteres o usando compuertas XOR. La secuencia aleatoria usada como una llave debe ser al menos tan extensa como el mensaje a ser encriptado, debido a que repeticiones periódicas de una clave típicamente corta en relación al texto plano permitiría el criptoanálisis y de esta forma un ataque en la transmisión. Además, la clave sólo se puede usar una vez, lo que significa que un extremadamente alto nivel de seguridad se requiere para la distribución secreta de claves. El cifrado continuo de esta forma es completamente impráctico para sistemas RFID.

Para tratar con el problema de la generación de clave y distribución, los sistemas han sido creados basándose en el principio del cifrado continuo one-time pad, que usa a su vez una *secuencia pseudo-aleatoria* en vez de una secuencia aleatoria como tal. Las secuencias pseudo-aleatorias se generan usando generadores pseudo-aleatorios.



**Fig. 6.11** En one-time pad las claves generadas de números aleatorios (dados) son usadas sólo una vez y destruidas (vaso). El problema aquí es la transmisión segura de la clave entre envío y recipiente.

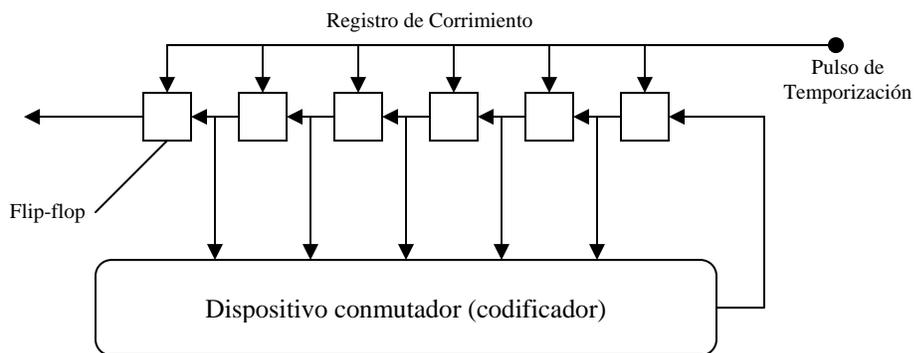


**Fig. 6.12** El principio de generación de una clave segura por un generador pseudo-aleatorio

La figura 6.12 muestra el principio fundamental de un cifrado secuencial usando un generador pseudo-aleatorio: debido a que la función de encriptado en un cifrado secuencial puede cambiar (aleatoriamente) con cada carácter, la función debe ser dependiente no sólo del carácter entrante en curso sino también de una característica adicional, el estado interno  $M$ . Este estado interno  $M$  es cambiado después de cada paso de encriptado por la función de transformación de estado  $g(K)$ . El generador pseudo-aleatorio está hecho de los componentes  $M$  y  $g(K)$ . La seguridad del cifrado depende principalmente del número de estados internos  $M$  y la complejidad de la función de transformación  $g(K)$ . El estudio de cifrados secuenciales está entonces principalmente ocupado del análisis de generadores pseudo-aleatorios.

La *función de encriptado*  $f(K)$  por sí misma, es generalmente muy simple y puede únicamente comprender la adición de una función lógica XOR. Desde el punto de vista de circuitería, los generadores pseudo-aleatorios se construyen de máquinas de estado, las cuales consisten de celdas de almacenamiento binario, también llamadas flip-flops. Si una máquina de estado tiene  $n$  celdas de almacenamiento entonces ésta puede tomar  $2^n$  diferentes estados internos  $M$ . La función de transformación de estado  $g(K)$  está representada por lógica combinatorial. La implementación y desarrollo de generadores pseudo-aleatorios se puede simplificar mucho si nos restringimos al uso de registros de corrimiento lineal realimentados (fig 6.13).

Un registro de desplazamiento se construye con la conexión serial de flip-flops (*salida<sub>n</sub>* conectada con *entrada<sub>n+1</sub>*) y la conexión paralela de todas las entradas de temporización. El contenido de la celda flip-flop es desplazado (corrido) hacia delante una posición por cada pulso de temporización. El contenido del último flip-flop es la salida.



**Fig. 6.13 Circuito básico de un generador pseudo-aleatorio que incorpora un registro de corrimiento lineal realimentado (LFSR)**

# ***CAPÍTULO 7***

## **ÁREAS ABIERTAS A DISCUSIÓN**

7.1 Introducción.....	183
7.2 Amenazas a la Privacidad y las Libertades Civiles.....	183
7.2.1 Marco de los derechos y responsabilidades RFID .....	184
7.2.2 Practicas RFID que deben estar prohibidas rotundamente .....	185
7.2.3 Usos aceptables del RFID .....	186
7.3 Limitaciones de la tecnología RFID: Mito y Realidad .....	187
7.4 Valoración de las soluciones propuestas en la industria .....	189
7.4.1 <i>Matar los tags en el punto de venta</i> .....	189
7.4.2 <i>Tags de bloqueo</i> .....	190
7.4.3 Sistema cerrado .....	192

## 7.1 Introducción.

La identificación por radiofrecuencia (RFID) es una tecnología de etiquetado de artículos con implicaciones sociales muy profundas. Usada inadecuadamente, esta tecnología implica un potencial riesgo para la privacidad del consumidor, reduciendo o eliminando el anonimato del comprador y amenazar las libertades civiles.

Tal como las organizaciones y los individuos, comprometidos con la protección de la privacidad y las libertades civiles, a continuación consideraremos los anterior en el despliegue del RFID en el ambiente del consumidor. En las siguientes páginas, veremos la tecnología y sus usos, definiremos los riesgos y discutiremos las aproximaciones potenciales en políticas públicas para mitigar los problemas que surgen al aplicar esta tecnología.

Debemos recordar que los tags RFID son pequeños chips conectados a antenas miniatura que se pueden fijar a objetos físicos. En las más comúnmente aclamadas aplicaciones RFID, el microchip contiene un *Código Electrónico de Producto (EPC)* con suficiente capacidad para proveer identificadores únicos para todos los artículos producidos a nivel mundial. Cuando un lector RFID emite una señal de radio, los tags en la vecindad responden emitiendo sus datos almacenados al lector. Con los tags RFID pasivos (sin batería), el rango de lectura puede variar desde unos cuantos centímetros hasta 6 ó 10 metros, mientras que los tags activos (auto-energizados) pueden tener un mucho más largo rango de lectura. Típicamente, los datos son enviados a un sistema de cómputo envuelto en el proceso (ver cap 4), quizá, de administración de la cadena de abastecimiento o control de inventario.

A continuación se detallarán las principales implicaciones sociales (*válidas o no*) en las que los oponentes a esta tecnología (RFID) se apoyan para fundamentar sus objeciones al despliegue de la misma en distintos sectores. En algunas objeciones se puede ver un cierto razonamiento lógico fundamentado, sin embargo los organismos internacionales que desarrollan la tecnología se están esforzando actualmente para solventar los impedimentos técnicos, principalmente los referidos al seguimiento, seguridad y encriptado.

## 7.2 Amenazas a la Privacidad y las Libertades Civiles

Las siguientes líneas son los principales argumentos de los opositores al RFID y sus consecuentes lineamientos de una *practica justa de información*, podremos o no estar de acuerdo en algunos puntos, pero sin duda deben estar sujetos a consideración.

Mientras existen usos muy benéficos del RFID, algunos atributos de la tecnología pueden ser desplegados en formas que amenacen la privacidad y las libertades civiles, entre ellas:

- *Colocación oculta de tags*: Los tags RFID se pueden adjuntar dentro o fuera de objetos y documentos sin el consentimiento del individuo que adquiere estos artículos. Ya que las ondas de radio viajan fácilmente y de manera silenciosa a

través de tejido, plástico y otros materiales, es posible la lectura de los tags cosidos a la ropa o fijados a objetos contenidos en bolsas, maletas, etc.

- *Identificadores únicos para todos los objetos a nivel mundial:* El código electrónico de producto permite potencialmente a cada objeto en la tierra, tener su propio y único identificador (ID). El uso de números ID únicos puede llevar a la creación de un sistema global de registro de artículo en el cual cada objeto físico sea identificado y ligado a su comprador o propietario en el punto de venta o transferencia.
- *Agregación masiva de datos:* Los despliegues RFID requieren la creación de bases de datos masivas conteniendo datos únicos de tag. Estos archivos se pueden ligar con datos de identificación personal, especialmente cuando la capacidad de memoria en las computadoras y las capacidades de procesamiento se van expandiendo.
- *Lectores ocultos:* Los tags pueden ser leídos desde una cierta distancia, no restringida a línea de vista, por lectores que se pueden incorporar de manera no visible en casi cualquier ambiente donde los humanos o los artículos se pudieran congregarse. Los lectores RFID ya han sido experimentalmente probados en los azulejos de piso, en los tejidos, alfombras, ocultos en puertas y al parecer también en los registros de retail y contadores, haciéndose virtualmente imposible para un consumidor el conocer cuando o si el o ella está siendo escaneado.
- *Rastreo individual y perfiles:* Si la identidad personal fuere ligada con números tag RFID únicos, los individuos podrían ser perfilados (gustos y tendencias) y rastreados sin su conocimiento o consentimiento. Por ejemplo un tag adjunto en un zapato podría servir como un identificador de ipso para la persona que lo porta. Incluso si la información a nivel artículo es genérica, los artículos de identificación que la gente porta o viste, pueden asociarse a ellos, por ejemplo, en eventos particulares como reuniones políticas.

### **7.2.1 Marco de los derechos y responsabilidades RFID**

Este marco respeta el interés del negocio en seguimiento de productos en la cadena de abastecimiento, pero enfatiza los derechos de los individuos a no ser rastreados en las tiendas y después de que los productos son comprados. Para mitigar las consecuencias potencialmente peligrosas del RFID para los individuos y la sociedad, se recomienda un marco tripartita: Primero, el RFID debe someterse a una valoración tecnológica formal y los tags RFID no deben ser fijados a productos de consumo individuales, hasta que dichas valoraciones se lleven a cabo satisfactoriamente. Segundo, la implementación RFID se debe guiar por los principios de una Práctica de Información Justa. Tercero, ciertos usos de RFID deben estar rotundamente prohibidos.

*Valoración Tecnológica:* El RFID debe estar sujeto a un proceso formal de valoración tecnológica, auspiciado por una entidad neutral, quizá similar al modelo establecido por el ahora desaparecido *Congressional Office of Technology Assesment*. El proceso debe ser multidisciplinario, envolviendo a todos los actores, incluyendo a los consumidores.

*Principios de una Práctica de Información Justa:* La tecnología RFID y su implementación deben ser guiadas por fuertes principios de información ó *fair information practices (FIP's)*. La octava parte de las *guías de privacidad* de la organización para la cooperación económica y desarrollo (OECD) proveen un valioso modelo. Se llega al acuerdo entonces, de que las siguientes líneas guía, basadas en parte de estos principios, se deben adherir mientras la gran valoración de las implicaciones sociales RFID toma lugar:

- *Apertura o Transparencia:* Los usuarios RFID deben hacer públicas sus políticas y prácticas que envuelven al uso y mantenimiento de los propios sistemas y no debe haber bases de datos secretas. Los individuos tienen el derecho a saber cuando los productos o artículos en el ambiente de venta, contienen tags RFID o lectores, además de tener derecho de saber las especificaciones técnicas de estos dispositivos. El etiquetado debe estar claramente visible y fácil de comprender. Cualquier lectura de tag que tome lugar en el punto de venta debe ser transparente para todas las partes, no debe haber lectura de tags en secreto.
- *Especificación de propósito:* Los usuarios RFID deben dar aviso de los propósitos por los que los tags y lectores son usados.
- *Limitación de información colectada:* La colecta de información se debe limitar a la que sea necesaria para el propósito en turno.
- *Responsabilidad:* Los usuarios RFID deben hacerse responsables de la implementación de esta tecnología y los datos asociados. Los usuarios RFID deben hacerse también legalmente responsables de cumplir con los principios. Un mecanismo de responsabilidades se debe establecer. Debe haber entidades tanto en la industria como en el gobierno con las cuales los individuos puedan hacer llegar sus quejas cuando estas previsiones sean violadas.
- *Resguardos en seguridad:* Debe haber seguridad e integridad en la transmisión, bases de datos y sistemas de acceso, todo esto se debe verificar desde el exterior, por una tercera parte y no ligada a publicidad para la auditoría.

### **7.2.2 Practicas RFID que deben estar prohibidas rotundamente**

A los mercaderes se les debe prohibir forzar a los clientes a aceptar consiente o inconscientemente a aceptar los tags RFID en los productos que compran.

No debe haber prohibición para los individuos de detectar los tags o lectores RFID y deshabilitarlos o removerlos de los artículos que adquieran.

El RFID no debe ser usado para rastrear individuos sin que estén informados o con el consentimiento escrito del asunto. El rastreo humano es inapropiado tanto directa como indirectamente a través de ropa, bins de consumo u otras.

El RFID nunca se debe emplear de forma que reduzca o elimine el anonimato. Por ninguna instancia se debe incorporar en la moneda.

### 7.2.3 Usos aceptables del RFID

Se han identificado varios ejemplos de usos “aceptables” del RFID en los cuales los ciudadanos consumidores no están sujetos a vivir con tags RFID y sus riesgos consecuentes.

- *Seguimiento de farmacéuticos:* Desde el punto de manufactura al punto de distribución. Los tags RFID pueden ayudar asegurando que estos bienes críticos no sean falsificados, que son manejados correctamente y que son distribuidos apropiadamente. Los tags RFID contenidos en los contenedores farmacéuticos deberían ser removidos físicamente o deshabilitados permanentemente antes de ser vendidos a los consumidores.
- *Seguimiento de bienes de manufactura:* Desde el punto de manufactura hasta la locación donde serán almacenados para su venta. Los tags RFID pueden ayudar a asegurar que los productos no se extravíen o sean robados cuando se mueven a través de la cadena de abastecimiento, también pueden asegurar que los bienes se manejan correctamente. A los tags se les debe confinar al exterior del paquete del producto (no incrustados dentro) y a ser destruidos permanentemente antes que los consumidores interactúen con ellos en las tiendas.
- *Detección de artículos con substancias peligrosas:* Cuando son entregados a los basureros, un tag RFID de corto alcance podría comunicar el contenido tóxico a un lector en el basurero. Es importante el subrayar que el uso en el caso anterior no requiere (y no debe implicar) identificadores únicos de artículos. El tag RFID puede, en su defecto, emitir un mensaje genérico (reciclable) o de desecho.

Como conclusión de todo lo anterior, se necesitan fabricantes y minoristas que concuerden en un etiquetado RFID voluntario y moratorio a nivel artículo para los artículos del consumidor hasta que una valoración formal que envuelva a los actores en este tema, incluidos los consumidores, pueda llevarse a cabo. Además, el desarrollo de esta tecnología se debe guiar por un fuerte conjunto de principios de práctica de información justa, asegurando que un significativo control de consumo sea construido en la implementación RFID. Finalmente, algunos usos de la tecnología RFID son inapropiados en una sociedad libre y deberán estar rotundamente prohibidos. Es deber de la sociedad no esperar por una crisis en cuanto a la tecnología sin que expresen sus puntos de vista también.

Aunque no se ha examinado, la gente que se opone también adjudica con las libertades civiles lo que respecta a la adopción gubernamental del RFID. En Estados Unidos el Departamento de Defensa ha promulgado un mandato a sus proveedores, que las escuelas y bibliotecas empiezen a implementar el RFID, también han considerado el uso del RFID en la moneda, también el gobierno Japonés y la fuerza jurídica británica ha considerado el uso como una herramienta de investigación. En México las fuerzas de seguridad han implantado el Verichip a unos 170 de sus oficiales de policía, para permitir el acceso a las bases de datos de la policía y para poder seguirlos en caso de ser secuestrados (ver secc 5.3). La oposición agrega que como una sociedad democrática, debemos adoptar una fuerte

marco político basado en los principios de práctica de información justa para guiar la implementación gubernamental del RFID.

Debemos recordar que “la oposición” a la tecnología muchas veces sólo conoce una cara de la misma y técnicamente no esta involucrada en los procesos y características propias de la radio frecuencia por lo que tienden a extremar las consecuencias, en la siguiente sección veremos los mitos que se han despejado a la fecha en cuanto al despliegue de la tecnología.

### **7.3 Limitaciones de la tecnología RFID: Mito y Realidad**

Las siguientes limitaciones técnicas han sido propuestas como razonamientos por los cuales los consumidores no se debieran preocupar por el despliegue del RFID en la actualidad. Vamos a dirigirnos a cada limitación percibida en turno y a explicar por que, como tales, estas limitaciones no debieran contar como una protección de consumo adecuada pero tampoco como un argumento suficientemente válido para los mencionados antes.

***Las distancias de Rango de lectura no son suficientes para permitir vigilancia de consumidor.***

Los tags RFID poseen diferentes rangos de lectura, dependiendo del tamaño de su antena, frecuencia de transmisión y de si son activos o pasivos. Algunos tags RFID pasivos tienen rangos de lectura de menos de 3 cm, otros tags se pueden leer a distancias de 6 metros o más. Los tags activos teóricamente tienen muy grandes rangos, actualmente los tags pretendidos para productos de consumo son pasivos con rangos de lectura de menos de 1.5 metros.

Contrario a algunas aserciones, los tags con bajos rangos de lectura no son necesariamente menos efectivos para seguimiento de seres humanos o artículos asociados con ello, de hecho, para algunos casos un rango de lectura corto puede ser más poderoso. Por ejemplo, si hubiese un interés en seguir individuos por medio de sus zapatos en cuanto se acerquen a un lector de piso dentro del rango, un rango de lectura de 5 cm sería preferible a un rango de 60 cm. Tal rango de lectura (corto) podría ayudar a minimizar la interferencia con otros tags en la vecindad y ayudar a asegurar la captura de solamente el tag pertinentemente posicionado hacia el lector.

***Los dispositivos de lectura no son lo suficientemente predominantes para permitir el rastreo humano desmedido.***

Los desarrolladores de la tecnología RFID prevén un mundo en donde los lectores RFID conformen una penetrante red global, no se necesita de una red ubicuota de lectores para rastrear objetos o la persona asociada a el. Por ejemplo, los automóviles que viajen por una carretera interestatal pueden ser rastreados sin colocar los lectores RFID a pocos metros de separación, sólo se les debe colocar en las casetas. De manera similar, para rastrear un individuo y sus locaciones en una ciudad determinada, no es necesario el colocar los

dispositivos lectores cada 3 metros en esa ciudad, ya que los lectores estarían presentes en locaciones estratégicas como las entradas a edificios.

### ***Información limitada contenida en los tags***

Algunos impulsores del RFID defienden la tecnología, apuntando que los tags asociados con la mayoría de los productos de consumo solo contendrán un número serial, como sea, el número actualmente puede ser utilizado como un número de referencia que corresponde a la información contenida en una o más bases de datos interconectadas. Esto significa que los datos asociados con ese número son teóricamente ilimitados y se puede aumentar con la nueva información colectada.

Por ejemplo, cuando un consumidor compra un producto con un tag EPC, la información acerca de la persona que compró puede agregarse a la base automáticamente. Información adicional se puede obtener del archivo mientras el consumidor se dirige a su negocio: “ingreso a la corte de Atlanta a las 12:32 p.m.”, “a la estación de gas Mobil a las 2:14 p.m.”, etc. Tales datos pueden ser accedidos por cualquiera con acceso a dicha base de datos, se autorice o no.

### ***Los tags pasivos no se pueden rastrear por satélite***

Los tags pasivos RFID previstos para la mayoría de los productos de consumo no generan su propia potencia, lo que significa que deben ser activados y sondeados por dispositivos lectores cercanos, por lo cual los dispositivos pasivos no tienen la habilidad para comunicarse vía satélite.

De cualquier manera la información contenida en los tags pasivos puede ser colectada por dispositivos lectores de ambiente, los cuales a su tiempo podrían transmitir su presencia y localización. Tal tecnología ha sido aplicada para el seguimiento de la locación en tiempo real de productos embarcados en vehículos en movimiento a través de la cadena norteamericana de abastecimiento.

En adición, tags activos con su propia fuente de energía se pueden habilitar con una capacidad de transmisión satelital. Por el momento dichos tags son demasiado caros para ser usados en la mayoría de los productos de consumo, sin embargo no es inconcebible debido al avance de la tecnología y los precios que caen.

### ***El alto costo de los tags los hacen no recomendables para un despliegue a gran escala***

Los desarrolladores RFID apuntan hacia el “alto costo” de los tags RFID como una manera de suavizar los miedos del consumidor acerca del potencial de dichos tags. Como sea, la tecnología mejora y los precios caen, se podría predecir que más y más productos de consumo portarán tags y estos tags se volverán más pequeños y más sofisticados, la tendencia seguirá hacia otros productos como computadoras y calculadoras, de hecho al hojear alguna revista de artículos para inventario y fabricantes de auto-partes se puede

notar los distintos productos para imprimir etiquetas RFID, con lo cual se muestra la rotunda contundencia de estas predicciones.

## **7.4 Valoración de las soluciones propuestas en la industria**

La industria RFID ha sugerido una variedad de soluciones para el problema de el etiquetado RFID de los productos de consumo. Entre estas soluciones esta el matar los tags en el punto de venta, el uso de “tags de bloqueo” y el “sistema cerrado”. Vamos a analizar cada estrategia en turno.

### **7.4.1 Matar los tags en el punto de venta**

Algunos han propuesto que el problema de etiquetado RFID se puede resolver mediante la inhabilitación de los tags en el punto de venta o “matándolos”. Existen diversas razones por las que la gente no cree que esta solución por sí sola y sin otras previsiones protegerá adecuadamente la privacidad del consumidor:

*Matar los tags después de la venta no soluciona el rastreo dentro de la tienda*

A la fecha, casi la mayoría de la invasión a la privacidad del consumidor asociada con el etiquetamiento RFID de los productos de consumo ha ocurrido dentro del ambiente al menudeo, hace tiempo los consumidores alcanzaban el verificador de salida donde los chips podían ser matados, algunos ejemplos:

- Se tomaban fotografías de acercamiento de los consumidores cuando recogían algún paquete etiquetado con RFID, para ser específicos de productos para afeitar Gillette, cuando eran recogidos de los estantes de la tienda equipados con lectores para tal propósito (tecnología “Auto-ID center” smart shelf).
- Una video cámara colocada en un estante de cosméticos para una tienda Wal-Mart en Oklahoma permitió a los ejecutivos (distantes del sitio) de *Procter and Gamble* observar a consumidores incautos cuando interactuaban con labiales etiquetados.
- Se han hecho planes para etiquetar libros y revistas con dispositivos RFID para permitir una observación detallada dentro de la tienda de gente que busca materiales de lectura. El potencial se demostró recientemente en la feria internacional de Tokio en el 2003, donde de acuerdo a un artículo japonés de la *Nikkei Electronic News*, “Colocando lectores de Tags en las estanterías de librerías, el sistema permite a las editoriales el obtener información tal como el rango de libros en los que el comprador ha dado un vistazo, cuantas veces un título en particular ha sido levantado e incluso el tiempo que se ha pasado hojeando cada libro.”

Se reconoce la necesidad de las tiendas de controlar el robo y de hacer valoraciones generales para ampliar operaciones. De cualquier manera, el monitoreo y grabación de los

comportamientos detallados del consumidor sin su pleno consentimiento, incluso si es sólo dentro de la tienda, viola los principios de una práctica de información justa.

*Los tags pueden aparentemente estar “muertos”, cuando en realidad están “dormidos” y pueden ser reactivados*

Algunos tags RFID poseen un estado “durmiente” o de “sueño”, que hace que parezca al consumidor promedio que el tag ha muerto. Es posible para los minoristas y otros el decir que los tags han sido desactivados permanentemente, cuando en realidad simplemente se han pasado de un estado activo a un estado de sueño.

*La opción de matar tags puede ser fácilmente cesada por una directiva gubernamental*

Tomaría muy poco para una amenaza en seguridad o cambio en políticas gubernamentales el quitar la opción de matar tags. Si a las etiquetas RFID se les permite la ubicuidad en los productos de consumo, al remover la opción de matarlas se permitiría instantáneamente la creación de una sociedad vigilada.

*Los minoristas podrían ofrecer incentivos o lo contrario a los consumidores para animarlos a dejar los tags activos.*

A los consumidores que deseen matar tags se les podría pedir hacer pasos adicionales a su compra o lidiar con cargas adicionales como esperar formado para un “killer kiosk” (dispositivo de escritura de tags) y tener que matar los tags por sí mismos. Los consumidores que elijan matar los tags podrían no disfrutar de los mismos beneficios y descuentos como los demás consumidores, o no les sería permitido la devolución en ciertos casos...etc. En muchas áreas de la ley de privacidad, este incentivo de las tiendas esta contemplado y existen prohibiciones legislativas contra la inducción del consumidor a renunciar a sus derechos de privacidad.

*La creación de dos tipos de consumidores*

Si matar tags requiere un esfuerzo consiente de parte de los consumidores, muchos no lo harán por miedo, ignorancia o falta de tiempo. Muchos elegirán no matar los tags si hacerlo les resulta inconveniente (la implementación actual para hacerlo, el “killer kiosk” requiere cargar un artículo a la vez, un proceso lento), esto podría crear dos clases de consumidores: aquellos que “cuiden bastante” la desactivación de los tags en sus productos y, por supuesto los que no lo hagan. El ser miembro de cualquier clase podría tener algunas ramificaciones negativas.

#### ***7.4.2 Tags de bloqueo***

Los tags de bloqueo son dispositivos electrónicos que teóricamente debieran irrumpir en la transmisión de toda o parte de la información contenida en los tags RFID, estos tags se deben adjuntar en una bolsa de mano o reloj u objeto que sea portado o vestido cerca de los tags con información que los consumidores deseen bloquear.

### *Los tags de bloqueo aún son teóricos*

De acuerdo a lo que se sabe, los tags de bloqueo aún no existen, hasta que uno sea construido y probado alguno no hay manera de saber que tan efectivos serán y si pueden ser técnicamente burlados.

### *Promueve el amplio despliegue de los tags RFID*

El tag de bloqueo podría promover la proliferación de dispositivos RFID dando a los consumidores un falso sentido de seguridad. Mientras que la invención propuesta es una idea ingeniosa, es también una idea que puede ser prohibida o no ser muy utilizada por los consumidores. También es posible que tal dispositivo electrónico fuere técnicamente burlado.

### *El tag de bloqueo podría ser prohibido por una directiva de gobierno o archivos policíacos.*

Los consumidores podrían perder su derecho a usar dispositivos de bloqueo si el gobierno juzga que el conocer lo que la gente viste o porta es necesario para la seguridad nacional. Podrían prohibir los dispositivos en su totalidad o promulgar espacios selectivos en aeropuertos o edificios públicos, por ejemplo.

Las tiendas podrían prohibir los tags de bloqueo si ellos creen que los tags se podrían usar para engañar a los dispositivos de seguridad o si creen que los detalles acerca de los consumidores son muy valiosos en sus esfuerzos de mercadeo.

Una vez que los tags y lectores sean ubicuitos en el ambiente, una completa o parcial prohibición al dispositivo para privacidad como por ejemplo el tag de bloqueo, podría dejar a los consumidores expuestos y vulnerables a la invasión de la privacidad.

### *Agrega una carga para los consumidores*

Un tag de bloqueo deja la carga de proteger la privacidad lejos de los fabricantes y minoristas y la coloca en los hombros de los consumidores. Además, los consumidores ocupados pueden olvidar el portar dispositivos de bloqueo, especialmente cuando pasos adicionales son requeridos para hacerlos efectivos.

### *Falla al proteger a los consumidores una vez que los productos son separados del tag de bloqueo*

Los tags de bloqueo teóricamente trabajan sólo cuando están cerca de los artículos para los que están diseñados para “ocultar” de los lectores RFID. Una vez que los artículos están fuera del rango del dispositivo de bloqueo, los consumidores podrían exponer y vulnerar su privacidad. Por ejemplo, un consumidor podría comprar un sweater y sentir que la información adjunta al tag no se expone debido a que ella carga una bolsa de mano impregnada con un dispositivo de bloqueo. De cualquier forma, una vez que ella quita ese

sweater de la bolsa y se lo prueba en el rango de un dispositivo lector, la información del tag puede ser vista.

#### *Creación de dos clases de consumidores*

Así como en la característica de matar tags, los tags de bloqueo también crearían dos clases de consumidores: los que bloquean los tags y los que no.

### **7.4.3 Sistema cerrado**

Los promotores industriales argumentan que cuando las aplicaciones RFID sean confinadas a sistemas cerrados, los datos sólo serán accesibles a aquellos dentro del sistema y a aquellos con una directiva de gobierno para tales fines. Entonces, argumentan, no se hará un perfilamiento de la ciudadanía ni un rastreo. Un ejemplo de una aplicación cerrada actual es el del RFID en bibliotecas, un libro de ingeniería en telecomunicaciones en la biblioteca X tendrá un código diferente que el del mismo libro en la biblioteca Y.

Teniendo en cuenta que las aplicaciones RFID de hoy se confinarán a sistemas cerrados, habrá entonces muchos incentivos para estandarizar el etiquetado a nivel producto. Las editoriales por ejemplo, podrían algún día embarcar los libros a las bibliotecas y librerías con tags de escritura, cada copia de un libro específico de ingeniería en telecomunicaciones contendrá una porción de su código EPC que será el mismo que el de cada una de las copias, la biblioteca podrá personalizar el resto del código convenientemente para sus propósitos de inventario o control.

Incluso si los sistemas permanecen cerrados, su ausencia de transparencia los hace problemáticos desde una perspectiva de privacidad, es decir debido a que los detalles acerca de los sistemas cerrados podrían no estar en disponibles y a la mano, los consumidores tendrían problemas al querer obtener la información necesaria para valorar los riesgos de privacidad y protegerse a sí mismos.

En conclusión, la gente que no apoya el RFID aprecia las propuestas que la industria propone y reconoce que están haciendo un esfuerzo en cuanto a la privacidad del consumidor y las libertades civiles asociadas a la tecnología RFID. De cualquier forma, mientras creen que las soluciones propuestas se ofrecen con buena intención, también proveen de una inadecuada protección. Hasta que soluciones apropiadas se desarrollen y se este de acuerdo con ellas, se podrá sujetar a los consumidores a los peligros de la tecnología a través del etiquetado de artículo de los productos de consumo.

## CONCLUSIONES.

Los sistemas RFID son ahora una realidad en muchos de los procesos de la vida cotidiana, tal como el pago electrónico, boletaje, control de accesos, industria farmacéutica, transporte internacional de contenedores, identificación de animales, sistemas de seguridad automotriz, procesos de producción industrial y hasta en los eventos deportivos. Es por lo anterior que no debemos ser ajenos a esta tecnología, que no es la única y que tampoco es de lo mas trascendental para discutir en cuanto a implementación ya que goza de una amplia aceptación en los sectores antes mencionados, en muchos de cuyos casos se ocupan incluso diferentes frecuencias y diferentes tipos de transponders como se ha visto a lo largo de este tratado, es decir esta tecnología se ha hecho de su propia área de estudio y es por ese motivo que recientemente se ha buscado en ésta como en muchas otras áreas de estudio la unificación o convergencia hacia sistemas mas interoperables con los servicios que actualmente se manejan en bancos, tiendas, empresas...etc, es el caso del NFC.

El NFC es una ramificación del RFID y se debe prestar atención a esta tecnología ya que con un principio tan simple como el de este protocolo se está logrando una mayor unificación de los servicios y todo con la interoperabilidad de este protocolo con la tercera generación de telefonía móvil, o con la inclusión de otro tipo de redes como la de los cajeros automáticos o la compra de boletos de avión, sólo por mencionar algunos ejemplos.

En el caso de la ciudad de México se tienen dos perfectos candidatos para empezar a implementar esta tecnología, nos referimos al caso del sistema de transporte colectivo metro y el metrobus en cuyos casos ya se cuenta actualmente con lectores RFID compatibles con el protocolo NFC en la banda de los 13.56 MHz. De hecho, basándose en los números de usuarios que actualmente ocupan las tarjetas inteligentes en el metro podemos ver que existe una clara tendencia al uso de las mismas por parte de los usuarios frecuentes del servicio, en el caso del metrobus la tarjeta es ocupada siempre que se desee viajar en este transporte, por lo que se convertiría en un elemento potencialmente exitoso.

Los dos casos descritos anteriormente son solamente algunas de las implementaciones al RFID actualmente existentes en la ciudad de México y que encuentran una amplia posibilidad de éxito en el NFC. Sin embargo, las demás aplicaciones antes mencionadas no pueden ser descartadas y es por esa razón que en este trabajo se han tratado en forma parcial cada una de estas.

Por último cabe destacar que no importa cual sea el tipo de sistema de comunicación que se desee ocupar, siempre existirá una tendencia hacia la convergencia que en un futuro estará marcando que tecnología permanecerá y cual está solo de paso ya que los usuarios de redes inalámbricas (cualquier red de comunicaciones) actualmente se deciden por una comunicación completa, confiable y por cualquier medio. El NFC aplicado a una red celular por ejemplo, no solo nos dará el beneficio de "toca y ve", sino que sobre esta interface se basarán muchos otros servicios que las redes inalámbricas actualmente ofrecen o que podrán ofrecer a sus abonados.

Los casos de éxito para NFC son muchos, hemos visto la evolución de esta tecnología y su impacto, las aplicaciones son inagotables y la interoperabilidad con otras tecnologías también así que todo lo demás se puede dejar a la imaginación y necesidades del mismo usuario.

# BIBLIOGRAFÍA.

RF AND MICROWAVE CIRCUIT AND COMPONENT DESIGN FOR WIRELESS SYSTEMS

Kai Chang-Inder Bahl-Vijay Nair  
Wiley Interscience

WIRELESS NETWORK EVOLUTION

Vijay K. Garg  
Prentice Hall Communications Engineering and Emerging Technologies

UMTS NETWORKS

Kaaranen Heikki, Ahtiainen Ari, Laitinen Lauri, Naghian Siamak, Niemi Valtteri  
Wiley

DATA AND COMPUTER COMMUNICATIONS

William Stallings  
Prentice Hall

RFID HANDBOOK

Klaus Finkenzeller  
Wiley

ELECTRÓNICA: TEORÍA DE CIRCUITOS

Bylestad, Nashelsky  
Pearson

MULTIPLE ACCESS IN WIRELESS DIGITAL NETWORKS

Norman Abramsom  
ALOHA Networks inc.  
<http://www.alohanet.com/sama/samatppr.html>

<http://www.nfc-forum.org>

<http://lanic.utexas.edu/la/Mexico/telecom/cap2.html>

<http://www.eveliux.com/fundatel/modulac.html>

<http://www.cucei.udg.mx/~siscom/modam.htm>

[http://scs1.netfirms.com/saavedra/sist\\_com/am.htm](http://scs1.netfirms.com/saavedra/sist_com/am.htm)

[http://scs1.netfirms.com/saavedra/sist\\_com/sist\\_rf.htm](http://scs1.netfirms.com/saavedra/sist_com/sist_rf.htm)

<http://www.profesores.frc.utn.edu.ar/electronica/electronicaaplicadaiiii/Aplicada/Cap03ModulacionAM1.pdf#search='tipos%20de%20modulacion'>

<http://www.rares.com.ar/PDF/1502.pdf#search='tipos%20de%20modulacion'>

[http://www.smartmobs.com/archive/2004/07/09/rfid\\_phones.html](http://www.smartmobs.com/archive/2004/07/09/rfid_phones.html)

<http://www.abiresearch.com>

<http://www.semiconductors.philips.com/markets/identification/products/nfc/>

<http://www.terra.com.mx/tecnologia/articulo/137609/>

<http://news.bbc.co.uk/2/hi/technology/3697940.stm>

<http://www.amal.net/rfid.html>

<http://www.bmezone.com/news/presenttense/20050330.html>

<http://www.newscientist.com/article.ns?id=dn7209>

<http://www.roadbeacon.com>

<http://www.oecd.org>

<http://www.tagblockers.com/>

<http://www.rfidjournal.com>

# I. GLOSARIO DE TERMINOS.

## I.A. TERMINOS GENERALES RFID

### **Tags Activos**

Transponders que usan baterías como una fuente de energía parcial o completa. Estos se diferencian además si se les divide en aquellos que contienen baterías reemplazables y aquellos que tienen las baterías dentro de una unidad sellada o que se les puede definir como unitizados.

### **Direccionabilidad**

Es la habilidad de direccionar bits, campos, archivos u otras porciones del almacenamiento en un tag.

### **Alineamiento**

Es la orientación del tag al lector.

### **Antena**

Las antenas son elementos conductores que irradian y/o reciben energía en el espectro de radiofrecuencia, hacia y desde el tag.

### **Bidireccional**

Capaz de operar en cualquiera de dos direcciones que son opuestas una de la otra.

### **Capacidad**

El número de bits o bytes que se pueden programar dentro de un tag. Esto puede representar los bits accesibles al usuario o el número total incluyendo aquellos exclusivos del fabricante.

### **Sistemas cerrados**

Sistema en el que datos relevantes relativos a los atributos del objeto se almacenan en una base de datos común, accesible vía enlace de datos en referencia al código individual ID. Se refiere usualmente a un sistema bajo el control de un solo propietario o autoridad.

### **Plato codificado**

Ver Tag.

### **Acople electromagnético**

A los sistemas que usan campos magnéticos para transferir datos o energía se les llama de acople electromagnético.

### **Etiqueta electrónica**

Ver Tag.

**Acople electrostático**

A los sistemas que usan la inducción de un voltaje en un transponder para transferir datos o energía se les llama de acople electrostático.

**Error**

Cualquier operación o datos que no están de acuerdo con el diseño o la entrada de un sistema.

**Código de corrección de error (ECC)**

Bits suplementarios en una transferencia de datos usados en conjunto con un algoritmo polinomial, a favor de computar el valor de bits de datos erróneos o perdidos.

**Modo de corrección de error**

Modo de comunicación de datos en el que los bits erróneos o perdidos son corregidos automáticamente.

**Protocolo de corrección de error**

Las reglas bajo las cuales el modo de corrección de error opera.

**Administración de error**

Técnicas usadas para asegurar que sólo información correcta es presentada al usuario del sistema.

**Tasa de error**

El número de errores por número de transacción.

**Excitador**

Los dispositivos electrónicos que manejan una antena se llaman excitadores o transmisores. En conjunto con la antena se les llama scanner.

**Puerto de expansión**

Un plug accediendo a una capacidad adicional 1/0 en una computadora o equipo periférico.

**Programación de fábrica**

La programación dentro de un tag que se lleva a cabo como parte del proceso de manufactura y que resulta en un tag de sólo lectura.

**Programación de campo**

La información de programación dentro del tag puede tomar lugar después de que los tags han sido embarcados del fabricante al usuario final. La programación de campo generalmente ocurre antes que el tag sea instalado en el objeto a ser identificado, esta aproximación permite la introducción de datos relevantes a las especificaciones propias de la aplicación en cualquier momento, de cualquier forma el tag típicamente tiene que ser quitado de su objeto, en algunos casos el cambio o duplicación de todos los datos en el tag es posible, en otros casos alguna porción se reserva para programación de fábrica, lo que podría ser un número serial único de tag.

**Protección de campo**

La habilidad de limitar las operaciones que se pueden efectuar en porciones o campos de los datos almacenados en un tag.

**Antena flat panel**

Antenas planas conductoras, hechas de metal o lámina.

**Acople inductivo**

Sistemas que aprovechan la inducción de una corriente en un devanado con la intención de transferir datos o energía.

**Programación en-uso**

Muchas aplicaciones requieren que nuevos datos o revisiones de los mismos en el tag se re-ingresen en el tag mientras permanece adjunto a un objeto. La habilidad de leer desde tag los datos y escribirlos en el tag mientras éste se encuentra adjunto al objeto se llama programación en-uso. Los tags y sistemas con estas características son llamados tags y sistemas de lectura/escritura.

**Interrogador**

Ver lector y programador.

**Vida**

Periodo razonable funcional en el que no se espera mantenimiento, ajuste o reparación.

**Tarjetas de memoria**

Un tag de lectura/escritura reprogramable en tamaño tarjeta de crédito.

**Módulos de memoria**

Un tag de lectura/escritura reprogramable.

**Multiplexor**

Dispositivo que soporta antenas múltiples o escáneres verificando cada uno de acuerdo con algún esquema convenido. Todo esto reduce la cantidad total de dispositivos en el sistema a expensas de tener a todos los escáneres “ciegos” en parte del tiempo. Se les llama también multicanalizadores o sólo controladores.

**Omnidireccional**

Capacidad de un tag para operar en cualquier dirección.

**Sistemas abiertos**

Aplicación en la cual la lectura/escritura no tiene acceso a ninguna base de datos común.

**Orientación**

Orientación del tag con respecto al escáner.

**Tags pasivos**

Los tags pasivos no contienen fuente de poder interna. Están externamente energizados y típicamente su poder deriva de la señal portadora radiada del escáner.

**Concentrador de puerto**

Dispositivo que acepta la salida de un número de interfaces de comunicación y las introduce a una red de comunicaciones.

**Niveles de potencia**

Niveles de potencia radiados desde un escáner o tag, usualmente medidos en volts/metro.

**Programación**

Grabación o alteración de un tag

**Programabilidad**

A favor de ser identificadores de un objeto en específico, los tags deben tener en algún punto su identificación y/o otros datos ingresados. Esta capacidad es llamada programabilidad.

**Programador**

Algunos tags pueden ver su propio contenido modificado por un juego de dispositivos proximidad cerrada o en contacto eléctrico con los mismos. Estos dispositivos y su empaque son llamados programadores.

**Rango**

Es la distancia en la que se puede obtener una exitosa lectura y/o escritura.

**Lectura**

Es la decodificación, extracción y presentación de datos, administración de los bits enviados desde tag (error y control).

**Legibilidad**

Habilidad para extraer datos bajo condiciones no muy óptimas.

**Tasa de lectura**

La máxima tasa desde la cual los datos pueden leerse de un tag, expresada en bits o bytes por segundo.

**Lector**

Es el dispositivo que contiene a su vez dispositivos electrónicos que extraen y separan la información contenida en un tag. Los dispositivos electrónicos internos son los que hacen toda la función de lectura, también pueden servir de interface a una pantalla y/o proveer comunicación paralela o serial con un host o controlador industrial.

**Reprogramable**

Muchas aplicaciones requieren que nuevos datos o revisiones de los mismos en el tag se reingresen en el tag mientras permanece adjunto a un objeto. La habilidad de leer desde tag los datos y escribirlos en el tag mientras éste se encuentra adjunto al objeto se llama programación en-uso. Los tags y sistemas con estas características son llamados tags y sistemas de lectura/escritura.

**SAW**

Onda acústica de superficie, una tecnología en la cual las señales de radiofrecuencia son convertidas a señales acústicas en un material piezoeléctrico cristalino. Las variaciones en desplazamientos de fase ionizan la señal reflejada que se puede utilizar para proveer una identidad única.

**Escáner**

El transmisor de la antena(excitador) y los dispositivos electrónicos del receptor integrados conforman un solo paquete llamado escáner. Pueden ser combinados con dispositivos digitales adicionales, incluyendo un microprocesador en lo que se llama un lector.

**Sensor**

Dispositivo que responde a un estímulo físico y produce una señal eléctrica, (ver escáner).

**Técnica de señalización**

Es la completa descripción de modulación, codificación, protocolo y secuencias requeridas para la comunicación entre dos sistemas.

**Tag**

El par transmisor/receptor o transceiver más el mecanismo de almacenamiento de información adjunto al objeto son referidos como tag, transponder, etiqueta electrónica, plato codificado...etc. Aunque transponder es el mas exacto técnicamente, el término más común y el preferido por los fabricantes es tag.

**Transponder**

Ver Tag.

**Escritura**

La transferencia de datos a un tag, la operación interna del tag de almacenamiento de datos que puede incluir la lectura de datos para verificación de la operación.

**Tasa de escritura**

La tasa a la cual la información es transmitida a un tag, escrita dentro de la memoria del tag y verificada, lo cual se cuantifica como el número de bits o bytes por segundo en los cuales una transacción promedio se completa.

## **I.B. TERMINOS ESPECÍFICOS NFCIP-1**

### **Modo de comunicación activo**

Modo NFCIP-1 en el que tanto el Iniciador como el Blanco usan su propio campo RF para permitir la comunicación.

### **BCD**

Codificación binaria decimal (binary coded decimal), es el sistema de numeración en el que cada uno de los números decimales del 0 al 9 tienen una representación en código binario de cuatro bits.

### **Colisión**

En términos del NFCIP-1, es la transmisión de datos por parte de dos o más Blancos o Iniciadores durante el mismo periodo de tiempo, de manera que el Iniciador/Blanco no distingue desde que Blanco/Iniciador se originaron los datos.

### **Trama**

Secuencia de bits de datos y bits de detección de errores opcionales con delimitadores de inicio y fin de trama.

### **Host**

Es el dispositivo u equipo (Teléfono, PDA, PC, Controles remoto inteligentes) en el cual reside un componente específico del ámbito de las comunicaciones NFCIP-1, en especial para los dispositivos que interactúan a nivel hardware. No se debe confundir con la connotación clásica de las redes de computadoras que también se mencionan en este tratado.

### **HThreshold**

Valor mínimo de un campo RF externo que un dispositivo NFCIP-1 detectaría a favor de no perturbar la comunicación saliente asegurándose de que su propio campo RF está inactivo.

### **Iniciador**

Generador del campo RF e iniciador de la comunicación NFCIP-1.

### **Modulación de carga**

Proceso de modulación en amplitud de un campo RF cuando se varían las propiedades de un circuito resonante colocado dentro del campo RF.

### **lsb first**

bit menos significativo primero, indica un sistema de transmisión de datos serial que envía lsb antes de todos los demás bits.

### **LSB first**

Byte menos significativo primero, indicando un sistema de transmisión de datos serial que envía el LSB antes de los demás bytes.

**msb first**

bit más significativo, indica un sistema de transmisión de datos serial que envía el msb antes que otros bits.

**MSB first**

Byte más significativo, indica un sistema de transmisión de datos que envía el MSB antes de los demás bytes.

**Dispositivo NFCIP-1**

Término general utilizado tanto para un Iniciador como para un Blanco comunicándose en el modo activo o pasivo.

**Identificador NFC (NFCID $n$ )**

Un número generado aleatoriamente usado por la secuencia RF Collision Avoidance and Single Device Detection tanto para el modo activo como para el pasivo.

**Modo de comunicación pasivo**

Cuando el Iniciador esta generando el campo RF y el Blanco responde a un comando Iniciador en un esquema de modulación de carga.

**RF Collision Avoidance (RFCA)**

Prevención de colisión RF, es el método para detectar la presencia de un campo RF basado en la frecuencia portadora, además de un método para detectar colisiones y resolverlas en un nivel de protocolo.

**Sensado**

Un dispositivo NFCIP-1 en el modo activo de comunicación esperando una respuesta a una petición que ha enviado en el campo RF para detectar el inicio de comunicación y recibir la petición.

**Single Device Detection (SDD)**

Detección de un sólo dispositivo, es un algoritmo usado por el Iniciador para detectar alguno de varios Blancos en su campo RF.

**Blanco**

Responde a un comando Iniciador usando tanto un esquema de modulación de carga (campo RF generado por el iniciador) o usando modulación o un campo RF auto generado.

**Periodo de Tiempo**

Define el número de slots (ranuras) usados para RF Collision avoidance.

**Transacción**

Incluye la inicialización y el intercambio de datos transparente entre el Iniciador y un Blanco tanto en el modo activo como en el pasivo.

## II. Acrónimos en NFCIP-1

**ALL\_REQ** Wake up ALL Request  
**ASK** Amplitude Shift Keying  
**ATR** Attribute Request and Attribute Response  
**ATR\_REQ** Attribute Request  
**ATR\_RES** Attribute Response  
**BCC NFCID1 CL<sub>n</sub>** check byte, calculated as exclusive-or over the 4 previous bytes  
**BCD** Binary Code Decimal  
**bd** Bit duration  
**BR<sub>i</sub>** Receiving bit duration supported by Initiator  
**BR<sub>t</sub>** Receiving bit duration supported by Target  
**BS<sub>i</sub>** Sending bit duration supported by Initiator  
**BS<sub>t</sub>** Sending bit duration supported by Target  
**CL<sub>n</sub>** Cascade Level  $n$ ,  $3 = n = 1$   
**CMD** Command  
**CRC** Cyclic Redundancy Check  
**CT** Cascade Tag  
**D** Divisor  
**DEP** Data Exchange Protocol Request and Data Exchange Protocol Response  
**DEP\_REQ** Data Exchange Protocol Request  
**DEP\_RES** Data Exchange Protocol Response  
**DID<sub>i</sub>** Initiator Device ID  
**DID<sub>t</sub>** Target Device ID  
**DR<sub>i</sub>** Data rate Received by initiator  
**DR<sub>t</sub>** Data rate Received by initiator  
**DS<sub>i</sub>** Data rate Send by initiator  
**DSL** Deselect Request and Deselect Response  
**DSL\_REQ** Deselect Request  
**DSL\_RES** Deselect Response  
**DSt** Data rate Send by Target  
**fc** Frequency of operating field (carrier frequency)  
**fd** Baseband frequency of Manchester coding  
**FRT** Frame Response Time  
**fs** Frequency of subcarrier ( $fc/16$ )  
**Gi** Optional information field for Initiator  
**Gt** Optional information field for Target  
**ID** Identification number  
**lsb** least significant bit  
**LSB** Least Significant Byte  
**MI** Multiple Information link for Data Exchange Protocol  
**msb** most significant bit  
**MSB** Most Significant Byte  
**NAD** Node Address  
**NFCID1** Random Identifier for single device detection in the Passive communication mode at 106 kbps  
**nfcid1<sub>n</sub>** Byte number  $n$  of NFCID1  
**NFCID2** Random ID for SDD in the Passive communication mode at 212 kbps and 424 kbps  
**nfcid2<sub>n</sub>** Byte number  $n$  of the Random Identifier NFCID2  
**NFCID3** Random ID for transport protocol activation  
**nfcid3<sub>n</sub>** Byte number  $n$  of the Random Identifier NFCID3  
**P** Odd parity bit  
**PA** Preamble

**pdu** protocol data unit  
**PFB** Control information for transaction  
**PNI** Packet Number Information  
**PPi** Protocol Parameters used by Initiator  
**PPt** Protocol Parameters used by Target  
**PSL** Parameter Selection Request and Parameter Selection Response  
**PSL\_REQ** Parameter Selection Request  
**PSL\_RES** Parameter Selection Response  
**RF** Radio Frequency  
**RFCA RF** Collision Avoidance  
**RFU** Reserved for Future Use  
**RLS** Release Request and Release Response  
**RLS\_REQ** Release Request  
**RLS\_RES** Release Response  
**RWT** Response Waiting Time  
**SB** Start byte for data exchange protocol at 106 kbps  
**SDD** Single Device Detection  
**SDD\_REQ** Single Device Detection Request command  
**SEL\_CMD** Select Command byte  
**SEL\_PAR** Select Parameter byte  
**SEL\_REQ** Select Request command  
**SENS\_REQ** Sense Request command  
**SENS\_RES** Sense Response command  
**SLP\_REQ** Sleep Request command  
**SYNC** Synchronous pattern  
**TO** Timeout value  
**WT** Waiting Time  
**WUP** Wakeup Request and Wakeup Response  
**WUP\_REQ** Wakeup Request  
**WUP\_RES** Wakeup Response