UNIVERSIDAD LASALLISTA BENAVENTE

Escuela de ingeniería en Computación

Con estudios incorporados a la Universidad Nacional Autónoma de México

CLAVE: 879316

"SIMULACIÓN CON VHDL DEL FUNCIONAMIENTO DE UNA TARJETA INTELIGENTE, BASADA EN RADIO FRECUENCIA PASIVA MCRF, PARA UN SISTEMA DE CONTROL DE ACCESO"

TESIS

Que para obtener el titulo de:

INGENIERO EN COMPUTACIÓN

Presenta:

C. HERIBERTO ARREGUÍN ARREGUÍN

Asesor: Ing. Carlos Alfonso Hernández Villanueva

Celaya, Gto., Enero de 2007

AGRADECIMIENTOS

A DIOS

Gracias por guiar mi camino, por estar conmigo en todo momento, por la fortaleza espiritual que me has brindado, por haberme dado a mis padres y por poner en mi camino y en mi vida a las mejores personas.

Gracias.

A MIS PADRES

Agradezco a mis padres por haberme dado la vida, por amarme con mis virtudes y defectos. Por haberme dejado ser y hacer de mi vida mi propio ideal.

A ellos mil gracias.

A MIS HERMANOS

Porque aunque estemos lejos siempre sabré que cuento con ustedes, y que estarán ahí en cualquier situación. Gracias por su apoyo, por su cariño y gran calidad humana. Ojalá nunca dejen de ser hombres emprendedores, que no pierdan pierdan la fe y la confianza en sí mismos.

A ellos mil gracias.

A LUCY

Gracias por tus cuidados, por tu cariño, por ese ángel que tú tienes, por la confianza que me tienes y la seguridad que me brindaste, para tener el impulso necesario para llegar a culminarme como un profesionista y lograr mi superación personal.

Te agradezco y te admiro.

A tí mil gracias.

A PACO

Gracias por guiarme de la mejor forma siempre buscando el buen camino para mí como a un hijo. Con mucho cariño te agradezco tus consejos que siempre me brindaste. Por tu constante empeño en mi y calor de padre. Por creer en mí.

Te admiro y te respeto.

A tí mil gracias.

A LAS FAMILIAS DE MIS HERMANOS Y HERMANA.

Con cariño y respeto, por brindarme su apoyo para ser mejor cada día.

Gracias.

A MIS COMPAÑEROS Y COMPADRES.

Gracias por las experiencias y convivencia que como familia se logró y por compartir conmigo un camino en la vida. Ojalá sigamos así compadres como siempre.

Gracias.

MAESTROS

Con respeto por transmitirme sus conocimientos y confianza para culminar mis estudios satisfactoriamente.

Gracias.

INDICE

CONCLUSION

BIBLIOGRAFIA

Introducción

El presente trabajo lo he elegido por la problemática que actualmente se ve tanto en la industria como en la sociedad, acerca de la seguridad que se tiene en el acceso de las personas sin un permiso a una área restringida o simplemente el acceso de personas ajenas a la propia industria o establecimiento.

Por lo cual yo propongo la implantación de un sistema de control de acceso, para manejar una seguridad más controlada ya sea en todo el lugar como podrían ser la industria, oficinas, escuelas y hasta la propia casa. Esto con el fin de monitorear el acceso de todas las personas a un determinado lugar.

Dicho sistema podría prestarse no solo para un control de acceso si no que también podrá ayudar en otros aspectos, como podrían ser:

Un control de pago de nómina, un sistema de prepago, identificación personal, ubicación de algún artículo o de alguna persona, etc. Estos son solo algunos ejemplos de las aplicaciones que se podrían pensar después de leer esta tesis, aunque claro, llevará una investigación de lo que se desee realizar.

Para llevar acabo el proyecto de control de acceso en el siguiente trabajo yo propongo el uso de las memorias EEPROM ya que son eléctricamente borrables y además se prestan para implantarlas en las tarjetas ya conocidas como tarjetas inteligentes, ya que con la nanotecnología las memorias prácticamente han quedado invisibles por lo cual una tarjeta inteligente en la actualidad es idéntica a lo que conocemos como una tarjeta de crédito donde no se percibe si cuenta con un integrado o no.

De acuerdo al objetivo general fijado, se ha establecido la hipótesis correspondiente:

En nuestra actualidad ya se escucha mucho sobre tarjetas inteligentes y un ejemplo muy común son los celulares con su chip o mas conocido como SIM el cual almacena la información del usuario como datos de sus contactos y tiempo aire disponible, pero también se ve en las casetas de cobro en carretera donde solo debes pasar por un carril establecido, en el cual no tienes que detenerte y automáticamente se te hace el descuento adecuado de tu tarjeta, esto quiere decir que todo se hace de forma inalámbrica, por lo cual es mas fácil el flujo de automóviles. De la misma manera yo propongo el control de acceso también de forma inalámbrica ya que sin tener que sacar tu credencial para identificarte solo la tienes que aproximar a un sensor que acciona un mecanismo que permitirá el acceso de acuerdo a la seguridad que se maneje.

En cada uno de los siguientes capítulos se describe la idea de lo que llevaría al finalizar este trabajo con éxito aunque es una simulación lo que se muestra es práctico. Cada uno de los capítulos tiene su gran importancia para el estudio que se hace en cuanto a el almacenamiento de información, conocimiento de las tarjetas inteligentes, estándares y operabilidad, enfoque en la radio frecuencia y simulación del dispositivo que se propone en el capítulo tres. Así que no se duda que este estudio será de gran ayuda para el lector interesado en darle una aplicación más real, cabe mencionar que el lector debe contar con los conocimientos tanto de electrónica como de sistemas de almacenamiento para una mejor comprensión del mismo.

CAPITULO I

LAS MEMORIAS ROM COMO DISPOSITIVOS PROGRAMABLES

1.1 Introducción y estructura general

Una de las partes más importantes de los sistemas digitales es el almacenamiento de la información que está tratando el sistema. Esta es la tarea de las memorias: Dispositivos que son capaces de proveer el medio físico para almacenar esta información.

Y aunque esta es su tarea fundamental (más del 90 % de las memorias se dedican a este fin) también se pueden utilizar para la implementación de circuitos combinacionales y pueden sustituir la mayor parte de la lógica de un sistema.

En la actualidad las ya conocidas tarjetas inteligentes también las utilizan para su programación interna, en ellas almacenan datos protegidos con diferentes niveles de seguridad.

1.2 Definición General de Memorias

Podemos considerar una memoria como un conjunto de M registros de N bits cada uno de ellos. Estos registros ocupan las posiciones desde el valor 0 hasta M-1. Para acceder a cada registro es necesario una lógica de selección. En general, para cada registro se pueden realizar procesos de lectura y de escritura. Para realizar todas estas operaciones son necesarios los siguientes buses:

- Bus de datos (de entrada y de salida).
- Bus de direcciones. son necesarios m, de tal forma de 2m=M
- Bus de control. Son los que permiten especificar si se desea realizar una operación de escritura o de lectura, seleccionar el dispositivo.
    1. /CS (Chip select): Es la terminal de selección de chip (habitualmente es activado con nivel bajo)

2. R/W (Read/Write): Selecciona el modo de operación (lectura o escritura) sobre la memoria. habitualmente con valor bajo se activa el modo de escritura y con valor alto el de lectura.

3. OE (Output Enable). Controla el estado de alta impedancia del bus de salida del dispositivo.

1.3 Clasificación de las memorias de semiconductores.

Acceso aleatorio	Volátiles	Estáticas (SRAM o RAM)	Bipolares MOS
		Dinámicas	MOS
		Pseudoestáticas	MOS
	No volátiles	ROM	Bipolares MOS
		PROM	Bipolares MOS
		EPROM	MOS
		EEPROM	MOS
		PLASH EPROM	MOS
		NVRAM	MOS
Acceso secuencial	Registro de desplazamiento	estáticos	
		Dinámicos	
	Cicuitos de acoplo de carga	CCD	MOS
	FIFO		Bipolares MOS
Asociativas (CAM)	TAGRAM		MOS

Tabla 1.1 Clasificación de memorias[1]

Memorias de acceso aleatorio: (Random Access Memory): Son memorias de acceso directo; esto es, cada uno de los registros puede ser leído o escrito de forma directa sin más que presentar en las terminales de dirección el código correspondiente de la posición que ocupa dentro de la memoria.

[1] www.howstuffworks.com

Memorias de acceso secuencial: En este tipo de memorias, el acceso a una posición se consigue por desplazamiento hacia la salida de todas las informaciones almacenadas en las posiciones anteriores a la deseada. Su modo de acceso es similar al de una cinta magnética. En este caso, el tiempo de acceso depende de la posición que ocupa cada dato.

Memorias CAM (Content addressable memory): Estas memorias son direccionables por su contenido. La operación de lectura no se realiza indicando una dirección y observando el contenido, sino que se suministra un dato y la memoria responde si dicho dato está almacenado o no. En caso afirmativo indica en qué posición se encuentra.

Otra posible clasificación la encontramos al saber si los datos almacenados se mantienen en ausencia de alimentación:

- Memorias no volátiles: ROM, PROM, EPROM, EEPROM y RAM alimentadas con baterías.
- Memorias volátiles: SRAM y DRAM[2]

[2] www.universidaddezaragosa.com en el departamento de ing. electrónica y comunicaciones

1.4 Breve historia de los sistemas de almacenamiento de datos informáticos

La base de todo sistema informático es el manejo de gran cantidad de información de una forma ordenada y rápida. Para realizar este cometido se precisan dispositivos que permitan guardar y manejar una gran cantidad de datos y funciones, de una forma rápida y controlada, este es el origen de los sistemas de almacenamiento de datos informáticos o memorias.

En la protohistoria de la informática (máquina sumadora de Babbage), se ejecutaban las aplicaciones (sumas, restas) en función de posiciones físicas de los componentes que formaban las máquinas.

La sección operativa del Ingeniero de Diferencias nº 1, ensamblada por Joseph Clement, ingeniero jefe de Charles Babbage, en 1832 es considerada la primera calculadora automática conocida. Babbage estaba convencido de que era posible superar las imprecisiones de las tablas matemáticas impresas a través de mecanismos mecánicos.

Con el nacimiento de las primeras computadoras en los años 40 los datos, las funciones y la sincronización de los procesos se ejecutaban introduciendo en las máquinas fichas perforadas, en las que se indicaban estos datos mediante perforaciones. Cada perforación indicaba un **0 ó un 1 lógico**.

Por estas fechas no existían ni lenguajes de programación ni sistemas operativos y este procedimiento exigía introducir una serie de fichas en un orden determinado con lo cual el lanzamiento de un programa se convertía en un proceso bastante largo y engorroso. Cabe recordar que la primer computadora electrónica (**ENIAC**) funcionaba basándose en un sistema decimal y en su caso las posiciones indicaban códigos de mensaje. En la actualidad las tarjetas perforadas se emplean para procesos de corrección automática de ejercicios tipo

test. En 1945 Von Neuman realizó dos propuestas que revolucionaron el mundo de la informática:

- Emplear código binario.
- El programa está residente en la memoria de la computadora.

Estas premisas son básicas en el desarrollo de equipos informáticos, con su aplicación se ha conseguido el gran desarrollo informático producido hasta nuestros días.

Para poder cumplir estas propuestas era preciso encontrar un sistema que permitiera hacer residentes los programas dentro de la computadora con la mayor fiabilidad posible, con este propósito surgen a principios de los años 50 las memorias de **núcleos de ferrita**. Estas memorias están formadas por una matriz de cables y un núcleo de ferrita de forma toroidal en cada nudo.

En función de la tensión que circule por los cables se magnetizan los núcleos de una forma u otra dando lugar, en función de la magnetización del núcleo, agrupaciones de ceros y unos lógicos que se podían mantener de forma permanente y ser variados con facilidad.

Para su época fue un paso adelante de gran importancia pero estos sistemas eran muy costosos, de gran tamaño, sensibles a las variaciones ambientales y difíciles de transportar.

Por estas fechas se llegó a la conclusión de que una computadora precisaba de al menos dos tipos de memorias para mejorar su trabajo:

- Una memoria de acceso rápido para la ejecución de los programas.

- Una memoria con un acceso más lento para el almacenamiento de programas y datos para su uso cargándolos en la memoria anteriormente indicada.

Al primer tipo de memoria se le conoce actualmente como memoria **RAM (Memoria de Acceso Aleatorio)**, el segundo tipo se conoce como **memoria secundaria**. El desarrollo de la tecnología para los distintos tipos de memorias indicados se ha hecho de una forma diferente.

Las memorias denominadas RAM son memorias de lectura y escritura están basadas en tecnología de biestables (bipolares), su proceso de funcionamiento es similar, salvando las distancias, al de los núcleos de ferrita. En vez de un núcleo de ferrita se sitúa un biestable, que es un componente electrónico construido a partir de transistores que en función de las condiciones de las entradas y salidas es capaz de almacenar un cero o un uno lógico. Este tipo de memorias pierden su contenido una vez que se ha apagado la alimentación eléctrica.

A modo de anécdota cabe decir que la denominación de RAM no coincide con la función de estas memorias, pues una memoria de acceso aleatorio puede ser cualquier tipo de memoria a la que se pueda acceder desde cualquier punto, no necesariamente una memoria de lectura y escritura.

A principios de los años 60 se inició su desarrollo gracias al empleo de **transistores bipolares**. A principio de los años 70 comenzó a desarrollarse la tecnología **VLSI** que consiste en la miniaturización de los componentes electrónicos con lo que, aparte de reducir su tamaño, se reducen los gastos, el consumo energético y se aumenta la velocidad de transferencia de datos. En un principio los transistores se fabricaban empleando tecnología **TTL** con esta tecnología el control de los transistores se realiza en función de la intensidad que

circula por la base del transistor. Los primeros transistores con esta tecnología tenían un consumo elevado en función de los parámetros actuales y provocaban problemas por la elevada temperatura que podían adquirir. Con el tiempo se ha reducido mucho sus consumos y elevado su velocidad de transferencia de datos.

Desde finales de los 70 se ha desarrollado la tecnología **CMOS** para la fabricación de transistores, con esta tecnología el control del transistor se hace con tensión en vez de con corriente con lo que se reducen muchísimo los problemas de consumo y temperatura, lo que permite una mayor miniaturización. En la actualidad es la tecnología dominante manteniendo la competencia con la tecnología TTL en algunos campos.

Entre otros tipos de memorias de esta gama caben citar los siguientes:

- **Memorias de sólo lectura (ROM)**: Son memorias que una vez grabadas no se pueden volver a regrabar, sólo pueden leerse. En estas memorias el biestable se sustituye por un microfusible de aluminio que se funde para grabar los ceros y unos lógicos.

- **Memorias EPROM:** Son memorias que una vez grabadas pueden ser borradas mediante luz ultravioleta y vueltas a regrabar.

- **Memorias EEPROM:** Son similares a las anteriores pero el borrado se realiza por medios eléctricos.

- **Memorias Flash:** Es un tipo de memorias similares a las EEPROM pero con una mayor velocidad.

Las memorias secundarias también son llamadas **memorias de**

almacenamiento masivo, su principal diferencia respecto a las memorias RAM es que la información almacenada no se pierde una vez desconectada la alimentación eléctrica. La tecnología básica que se emplea para su desarrollo es la basada en sustancias fácilmente magnetizables por medio de corrientes eléctricas que mantienen la orientación de los campos una vez eliminado el estímulo eléctrico. En este tipo de equipos se tiende en la actualidad a aumentar lo máximo posible la velocidad de transferencia de datos desde y hacia ellos para mejorar en lo posible las prestaciones de los equipos.

Los primeros elementos que se desarrollaron fueron las **cintas magnéticas** en los años 60. Su principio de funcionamiento es igual que el de las cintas de cassette, se trata de una cinta de material plástico impregnado de resina magnética que pasa por unas cabezas de grabación que varían la orientación magnética del material grabando ceros o unos lógicos. Para la lectura las cabezas detectan la variación del campo generando señales eléctricas que se transmiten a donde interese. Este tipo de dispositivo permite almacenar una enorme cantidad de información, pero no permite el acceso aleatorio a los datos y es lento. En la actualidad se emplean sobre todo para realizar copias de seguridad que contengan una gran cantidad de información.

A principios de los años 70 aparecieron las **unidades de almacenamiento en disco**, su principio de funcionamiento es el mismo que las cintas pero son mucho más rápidas y ocupan menos espacio. En este tipo de unidades la lectura y grabación de los datos se puede hacer por contacto físico entre la cabeza y los discos (**disquetes)** o sin contacto (**discos duros**), los elementos del primer tipo se emplean para los discos transportables y los del segundo forman la unidad principal de almacenamiento de datos de nuestras actuales computadoras.

A principios de los 90 aparecieron los **discos compactos**, que han supuesto una autentica revolución en este tipo de materiales. Su principio de

funcionamiento está basado en el empleo de luz láser para la lectura y grabación. Tienen una velocidad de transferencia muy alta, reducido costo, gran capacidad y son muy fáciles de transportar. En la actualidad están siendo sustituidas por los discos de tecnología **DVD** que, teniendo el mismo principio de funcionamiento, tienen unas prestaciones, sobre todo en capacidad, muy superiores.[3]

1.5 ¿Qué son las memorias ROM?

La memoria ROM (Read Only Memory – Memoria de solo lectura) es una memoria no volátil de solo lectura. Sin embargo, también existen dos características a enfatizar en esta definición. La memoria ROM es memoria no volátil: Los programas almacenados en ROM no se pierden aun cuando se interrumpe el suministro de energía y se vuelve a activar, sino que se mantiene la información binaria en los chips ROM durante toda su existencia, además la memoria ROM es, como su nombre indica, memoria de sólo lectura, es decir, los programas almacenados en los chips ROM no se pueden modificar. El usuario puede leer y ejecutar los programas de la memoria ROM, pero nunca puede escribir en la memoria ROM otros programas de los ya residentes en él. Las ROM vienen con fusibles electrónicos internos especiales que se pueden "programar" para generar una configuración específica.

Un diagrama a bloques de una memoria **ROM** se ilustra en la **figura 1.1**. Este consta de *K* entradas y *n* salidas. Las entradas proporcionan la dirección de la memoria y las salidas dan los bits de datos de la palabra almacenada que selecciona la dirección. El número de palabras de una ROM se determina a partir de que se necesitan *K* líneas de entrada de direcciones para especificar 2^k palabras. La ROM no tiene entrada de datos porque no tiene operación de escritura. Los chips ROM de circuitos integrados tienen una o mas entradas

[3] http://centros5.pntic.mec.es/cpr.de.aranjuez/foro/tecno/informatica.html

habilitadoras y vienen con salidas de tres estados para facilitar la construcción de arreglos grandes de memorias de sólo lectura.

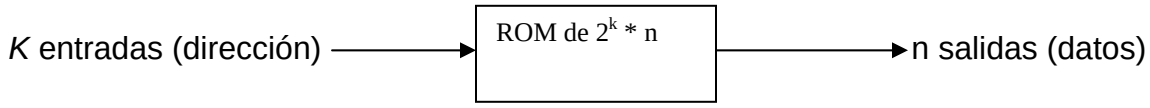


Figura 1.1, Diagrama a bloques de una memoria[4]

Para tener un mejor entendimiento de esto se muestra el siguiente ejemplo:

Considerar una ROM de 32 * 8. La unidad consta de 32 palabras de ocho bits cada una. Hay cinco líneas de entrada que forman los números binarios del 0 al 31 para la dirección. En la **figura 1.2** se presenta la construcción lógica interna de la ROM. Las cinco entradas se decodifican en 32 salidas distintas por medio de un decodificador de 5 * 32. Cada salida representa una dirección de la memoria. Las 32 salidas del decodificador se conectan a través de fusibles a cada una de las compuertas OR. El diagrama muestra la convención lógica de arreglos que se aplica en circuitos complejos. Cada compuerta OR debe considerarse como un dispositivo de 32 entradas. Cada salida del decodificador se conecta a través de un fusible a una de las entradas de cada compuerta OR. Como cada compuerta OR tiene 32 fusibles internos y hay ocho compuertas OR, la ROM contiene 32 * 8 = 256 enlaces de fusibles internos. En general, una ROM de 2^k * n tendrá un decodificador interno de K * 2^k y n compuertas OR. Cada compuerta OR tiene 2^k entradas que se conectan a través de fusibles a cada una de las salidas del decodificador.

[4]M. Morris Mano, Ingeniería Computacional Diseño del Hardware, Editorial PRENTICE HALL, 199l, p. 214

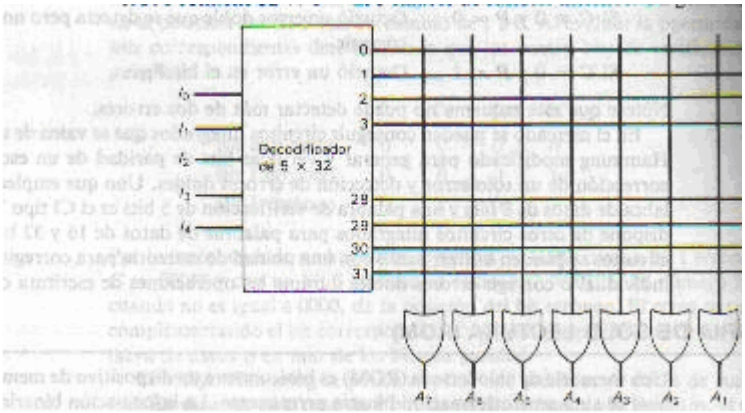


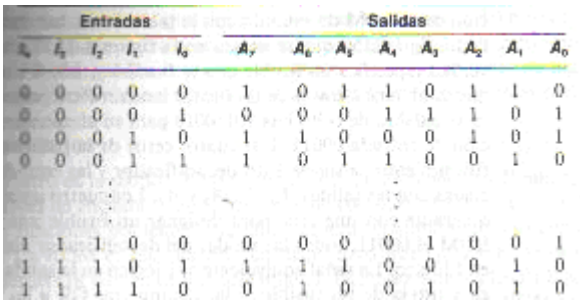
Figura 1.2, Lógica interna de una ROM de 32 x 8[5]

El almacenamiento binario interno de una ROM lo especifica una tabla de verdad que muestra el contenido de palabras en cada dirección. Por ejemplo, el contenido de una ROM de 32 * 8 se puede especificar con una tabla de verdad análoga a la que se presenta en la **tabla 1.2**. La tabla de verdad muestra las cinco entradas debajo de las cuales se citan las 32 direcciones. Cada entrada especifica la dirección de una palabra de ocho bits cuyo valor se especifica debajo de las columnas de salida. La **tabla 1.2** presenta solo las cuatro primeras y las cuatro ultimas palabras de la ROM. La tabla completa debe incluir una lista de las 32 palabras.

El procedimiento de *Hardware* que proporciona la ROM ocasiona que se fundan fusibles internos de acuerdo con una tabla de verdad dada. Por ejemplo, la programación de la ROM de acuerdo con la tabla de verdad dada por la **tabla 1.2** da origen a la configuración que se ilustra en la **figura 1.3**. Todo 0 presentado en la tabla de verdad especifica un fusible que se fundirá y todo 1 citado especifica una trayectoria que se obtiene a través de un fusible intacto.

[5] M. Morris Mano, OP.CIT, P. 613

Tabla 1.2 Tabla de verdad de ROM (parcial)[6]



Entradas					Salidas							
					A_7	A_6	A_5	A_4	A_3	A_2	A_1	A_0
0	0	0	0	0	1	0	1	1	0	1	1	0
0	0	0	0	1	0	0	0	1	1	1	0	1
0	0	0	1	0	1	1	0	0	0	1	0	1
0	0	0	1	1	1	0	1	1	0	0	1	0
.												
.												
.												
1	1	1	0	0	0	0	0	0	1	0	0	1
1	1	1	0	1	1	1	1	0	0	0	1	0
1	1	1	1	0	0	1	0	0	1	0	1	0

Para poner un ejemplo, la tabla especifica la palabra de ocho bits 10110010 para su alimentación permanente en la dirección de entrada 00011. Los cuatro ceros de la palabra se programan fundiendo los fusibles entre las salidas 3 del decodificador y las entradas de las compuertas OR asociadas con las salidas A_6, A_3,A_2 Y A_0. Los cuatro unos de la palabra se marcan en el diagrama con una cruz para designar un fusible intacto. Cuando la entrada de la ROM es 00011, todas las salidas del decodificador son 0 menos la salida 3 que está en 1 lógico.

La señal equivalente al 1 lógico en la salida 3 del decodificador se propaga a través de los fusibles y las compuertas OR a las salidas, A7, A5, A4 Y A1. Las otras cuatro salidas permanecen en 0. El resultado es que la palabra almacenada 10110010 se aplica a las ocho salidas de datos.

Las trayectorias que se requieren en una ROM se pueden programar en tres formas diferentes. La primera se denomina programación por mascara y la realiza la compañía de semiconductores durante el ultimo proceso de fabricación de la unidad.

El proceso para fabricar una ROM requiere que el comprador llene la tabla de verdad que desee que la ROM satisfaga. El fabricante crea la mascara correspondiente de las trayectorias a fin de producir los unos (1) y los ceros (0) que están en la tabla de verdad del comprador.[7]

[6] M. Morris Mano. Op cit. P.615
[7] M. Morris Mano. Op cit. P.213 – 216.

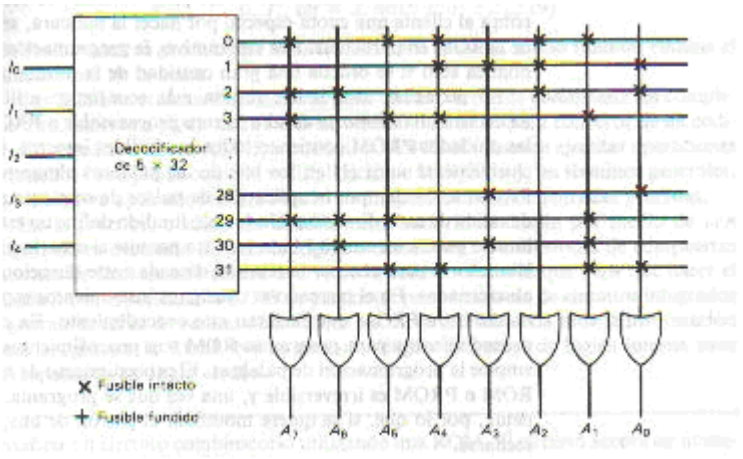


Figura 1.3 Programación de la ROM de acuerdo con la tabla 1.2[8]

1.6 Programación de la ROM de acuerdo con la tabla 1.1

Como ya sabemos las memorias **ROM** están compuestas por una matriz de fusibles así como un decodificador/es y compuertas OR que son los que se encargan de la programación interna del dispositivo. Esta matriz puede variar de acuerdo al tamaño de la ROM esto lo decide el fabricante una ves que decide realizar la memoria ROM ya que esta debe ser por pedido para su realización especial porque lleva una programación especial cada ROM. Una ves fabricada con cierto programa no se puede volver a reprogramar ya que se funden los fusibles y no hay forma de reconstruirla, esta es la característica de este estilo de memoria.

Y tiene sus desventajas ya que en ocasiones no es necesario toda su capacidad así que el resto puede ser desperdiciado ya que no podemos volver programar esta memoria.

En cuanto a la tecnología de fabricación se utiliza o bien tecnología bipolar (TTL o ECL) para aplicaciones que requieren una alta velocidad de trabajo, o bien en tecnología MOS (transistores de efecto de campo de canal N) para aplicaciones en las que es necesaria una alta densidad de integración y bajo consumo.

[8]Ib. Ident. 215

Desde el punto de vista de dispositivos programables una memoria consta de una matriz “and” fija y una matriz “or” programable; esto es, en la que se puede seleccionar mediante programación las interconexiones entre sus filas y columnas.

Parámetros de interés:

Tamaño. El fabricante indica el número de palabras, que dependen del tamaño del bus de direcciones y de la longitud de la palabra que depende del tamaño del bus de datos. Un dato que puede ser de bastante importancia es el *tiempo de acceso* a los datos; esto es, el tiempo desde que se requiere la solicitud del dato hasta que éste se encuentra en el bus de datos. Este parámetro depende de la tecnología de fabricación y se debe tener en cuenta.

Consumo. En la actualidad este parámetro no es significativo ya que la tecnología de fabricación dominante es MOS.

Encapsulado. Para la misma capacidad de memoria, el tipo de encapsulado y la distribución del patillaje(patas del integrado) puede ser importante a la hora de diseñar el circuito impreso.

- **Memorias de sólo lectura Bipolares.**

Las primeras memorias programables que aparecieron en el mercado fueron las memorias bipolares de fusibles (década de los setenta). Los fusibles eran el único medio disponible para asegurar un almacenamiento permanente de la información colocada en la memoria.

Como ya sabemos, este tipo de memoria consta de una matriz de hilos que se cruzan, en cuyas intersecciones se ha situado unos diodos en serie con los fusibles. Antes de ser programada todos los fusibles están intactos. Entonces, programar la memoria consiste en hacer saltar aquellos fusibles no deseados. Para ello se suele utilizar una tensión relativamente alta (típicamente12 voltios) para hacer saltar el fusible.

Debido a la alta disipación térmica estas memorias son obligatoriamente pequeñas (típicamente hasta 16Kx8) y en la actualidad se encuentran en desuso.

Como dato significativo encontramos unos tiempos de acceso del orden de 50 nseg. No creemos necesario más comentario acerca de las mismas.

- **Memorias de sólo lectura CMOS EPROM.**

Aunque pueda parecer increíble, los fabricantes de este tipo de memorias casi se han puesto de acuerdo para la denominación de las mismas. Así la referencia indica directamente su capacidad; por ejemplo el C.I. 2764 indica una memoria de 64Kbytes. Esto siempre es de agradecer ya que no multiplica innecesariamente las referencias para dispositivos que hacen lo mismo.

El modo de funcionamiento de un transistor MOS se ve con mucho más detalle en otras asignaturas. Aquí sólo vamos ha realizar los siguientes comentarios:

Teóricamente el proceso de grabado y borrado de una celda CMOS es reversible hasta el infinito. En la realidad las memorias EPROM empiezan a dar problemas a partir de los 1000 ciclos de programación y borrado. (Suficiente para las necesidades de la mayoría de los usuarios).

Sabemos que estas memorias son sensibles a los rayos UV (se borran mediante una exposición a una fuente de luz ultravioleta de 10 a 20 minutos). Debemos tener en cuenta que fuentes de luz habituales en nuestro entorno, como pueden ser fluorescentes o la luz solar, también emiten energía en longitudes de onda del UV, aunque en mucha menor medida. No obstante es aconsejable proteger la ventana de una EPROM con un adhesivo opaco, para evitar que este tipo de luz degrade el contenido de la misma.

En cuanto a la tensión de programación, es necesario saber con qué tipo de memoria se está trabajando. Las primeras memorias de este tipo necesitaban de tensiones de programación de 25 voltios. Versiones más modernas permiten unas tensiones de programación de 12,5 voltios.

Debido a su mayor capacidad de integración, el tamaño de las memorias puede ser mucho mayor. De hecho, basta mirar cualquier "databook" de fabricantes de memorias (por ejemplo AMD o Cypress) para ver la gran cantidad de dispositivos diferentes que ofrecen, cada uno pensado para aplicaciones concretas.

En cuanto a los tiempos de acceso, las primeras memorias de tipo MOS ofrecían unos tiempos de acceso del orden de 200 nseg. En la actualidad, los tiempos de acceso se han reducido considerablemente, y son comparables a las memorias bipolares, por lo que éstas han caído en desuso.[9]

1.7 Memorias de solo lectura programables (PROM)

En pequeñas cantidades, resulta más económico utilizar un segundo tipo de ROM llamadas *memoria de solo lectura programable* o PROM. Cuando se solicitan las unidades PROM todos los fusibles están intactos, lo que hace que haya exclusivamente unos (1) en los bits de las palabras almacenadas. Los fusibles de la PROM se funden por la aplicación de pulsos de corriente a través de las terminales de salida de cada dirección. Un fusible fundido define un estado 0 binario y el fusible intacto genera un estado 1 binario. Esto permite al usuario programar la PROM en su laboratorio para obtener la relación deseada entre direcciones de entrada y palabras almacenadas. En el mercado se consiguen instrumentos especiales llamados *programadores* de PROM que facilitan este procedimiento. En cualquier caso, todos los procedimientos para programar las ROM son procedimientos de *Hardware* aunque se emplee la programación de palabras. El procedimiento de *Hardware* para programar ROM o PROM es irreversible y, una vez que se programa, el patrón fijo es permanente, por lo que si se quiere modificar el patrón de bits, la unidad tiene que desecharse.

Los chips PROM cuentan con una parrilla de columnas y renglones igual que los chips ROM. La diferencia es que cada intersección de columnas y

[9] www.universidaddezaragosa.com en el departamento de ing. electrónica y comunicaciones

renglones cuenta con un fusible que los conecta. Inicialmente todos los chips PROM cuentan con sus fusibles intactos esto es que cuentan con valores de 1 lógico, y cambian de 1 a 0 lógico al utilizar un programador de PROM el cual funde los fusibles deseados de acuerdo a una tabla de verdad. Los funde enviando voltajes altos hacia donde se requiere fundir y es así como se programa esta memoria.

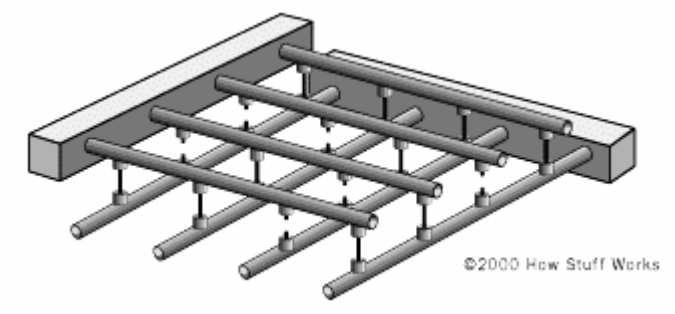


Figura 1.4. Memoria PROM.[10]

La PROM es esencial para hacer prototipos antes de usar las ROM ya que son de menor costo y una ves que ya se tenga un resultado deseable entonces si utilizar las ROM que son mucho mas costosas.

1.8 PROM Borrable

La **EPROM(Erraesable PROM)** se puede restaurar al valor inicial aun cuando sus fusibles se hayan fundido previamente. Cuando la EPROM se coloca bajo una luz ultravioleta especial por un espacio de tiempo dado, la radiación de onda corta descarga y regresa a su estado inicial y se puede reprogramar a un nuevo conjunto de palabras.

Sabiendo que existen esta nueva tecnología es pérdida de tiempo utilizar las memorias antes mencionadas (ROM Y PROM). Ya que aun que son mas

[10] www.howstuffworks.com

baratas que esta pero desechables, en cambio esta tecnología te permite reprogramar en caso de algún error cometido o en caso de adaptaciones. Estas son programadas por un programador de EPROM, el cual provee voltajes de niveles específicos ya que esto depende del tipo de EPROM que se utilice.

El transistor utilizado en una célula EPROM tiene dos puertas, una de ellas está conectada a la tensión de puerta Vg y la segunda es flotante. En esta segunda puerta se puede acumular carga por medio de un mecanismo denominado inyección por avalancha (avalanche injection o también hot electron injection). Este mecanismo se induce aplicando una tensión de programación (típicamente 20V) a la puerta de drenaje y seleccionando el transistor por medio de la tensión de puerta. El alto campo eléctrico generado entre ambas terminales arrastra a electrones, de forma que algunos tienen suficiente energía como para atravesar la barrera que existe entre el sustrato p y la puerta. Este tipo de transistores se denomina FAMOS: Floating gate Avalanche-injection MOS.

En operación normal un transistor FAMOS que tiene carga en su puerta flotante no conducirá en ningún caso, incluso si se selecciona la tensión de puerta es Vcc. En el caso en que el transistor no disponga de carga en su puerta flotante, éste se comportará como un transistor de tipo NMOS.

Es esta también tenemos una parrilla de columnas y renglones solo que en cada intersección hay dos transistores. Los transistores están separados uno del otro por una capa delgada de oxido.

1.9 OTP(Programable una vez)

Este modelo de memoria sólo se puede grabar una vez por parte del usuario. Utilizando el mismo procedimiento que con la memoria EPROM. Posteriormente no se puede borrar. Su bajo precio y la sencillez de grabación aconsejan este tipo de memoria para prototipos finales y series de producción cortas.

1.10 PROM Borrable Electrónicamente y FLASH MEMORY

Como ya sabemos las EPROM son un gran paso delante de las PROM, pero también tienen su desventaja y ya que en caso de que deseemos borrar solo parte de la PROM no se puede, ésta al entrarle una luz ultravioleta se borra toda sin excepción, en cambio la nueva tecnología **EEPROM** esta lista para ser manipulada con mucho más ventaja, ya que está si permite ser borrada por partes ya que toda la manipulación de está es electrónica.

La región de óxido es mucho más pequeña (espesores típicos de menos de 100 angstroms frente a los 200 angtroms del FAMOS).

Este tamaño permite acumular carga en la puerta flotante mediante un mecanismo denominado efecto túnel Fowler-Nordheim: Aparece una corriente de efecto túnel aplicando una tensión de programación a la puerta y manteniendo la tensión de drenaje a tierra que carga la puerta flotante. Este proceso es reversible invirtiendo los papeles de la puerta y el drenaje, de forma que una puerta flotante cargada se puede descargar por métodos eléctricos. Estos transistores se denominan FLOTOX: Floating Gate Tunnel Oxide Transistor.

Las Estructuras EEPROM necesitan de un transistor de selección debido a que, cuando la puerta flotante no tiene carga, la tensión umbral de un transistor FLOTOX es negativa. Entonces un transistor FLOTOX no programado podría conducir corriente entre la fuente y el drenaje si la tensión de puerta es cero.

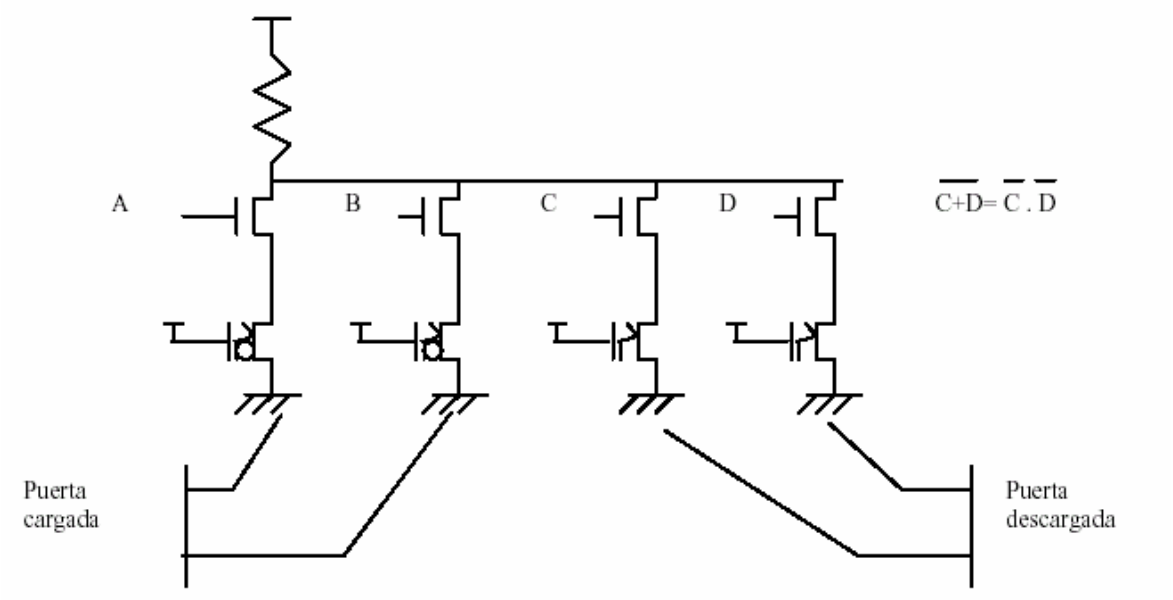


Figura 1.5, Interior de la EEPROM[11]

Características de las EEPROM:

- El chip no tiene que ser borrado completamente para rescribir en ella.
- No se debe borrar ni una porción para ser manipulado nuevamente e ingresar mas datos binarios.
- Cambiar el contexto no requiere equipo dedicado adicional.

En ves de utilizar luz ultra violeta, se utilizan los electrones en las células de las EEPROM para localizar los campos eléctricos, y así borrar las células requeridas de la EEPROM y entonces rescribir. Las EEPROM utilizan 1 octeto a la vez, que las hace versátiles pero se retardan. Al realizar el borrado e ingresar nuevos datos lo hace byte por byte y esto la hace versátil pero lento. Y por ello los fabricantes de estas memorias respondieron a esta limitación con memorias de destello (**FLASH MEMORY**).

1.11 Memorias FLASH.

[11] www.howstuffworks.com

Las **FLASH MEMORY** son un tipo de EEPROM que utiliza cableado dentro del circuito (in-circuit wiring) para que el borrado sea aplicado por campos donde se pueda borrar toda la memoria o en secciones de bytes llamados bloques **(blocks).** Trabaja mucho más rápido que las EEPROM, porque escribe en grandes cantidades de bytes en vez de byte por byte, escribe 512 bytes en tamaño.

Las memorias electrónicas tienen diferentes formas y propósitos, la FLASH MEMORY es fácil y rápido de usar para almacenar información. De hecho la memoria FLASH esta considerada como una memoria de estado sólido, que indica que sus partes no se mueven, en vez de ser movimiento mecánico todo es eléctrico. [12]

12 http://www.howstuffworks.com/rom1.htm

CAPITULO II

LAS TARJETAS INTELIGENTES

2.1 TARJETAS INTELIGENTES

2.1.1 Definición de tarjetas inteligentes.

Una tarjeta Inteligente es aquella que cuenta con un dispositivo de energía de proceso y/o memoria, y que es capaz de embonar con el formato definido por la Organización Internacional de Estándares. Para ser más precisos en términos de la ISO, ésta es más conocida como la ICC (Integrated Circuit Card).

Es muy similar en apariencia a una tarjeta de crédito, pero tiene una microcomputadora (chip) embonada la cual puede procesar tanto como una computadora personal; y se consideran como la siguiente generación de las computadoras portátiles. Este chip tiene la habilidad de almacenar y manipular datos y resolver problemas matemáticos. Este microchip embonado tiene hasta 60 veces más memoria que una tarjeta de cinta magnética convencional.

De acuerdo a la inteligencia de procesamiento, tamaño y almacenamiento que poseen estas tarjetas, pueden ofrecer mayor seguridad y muchas otras aplicaciones para varias áreas. Actualmente las tarjetas inteligentes existen para el pago de llamadas telefónicas, pago de estacionamiento, almacenamiento de un record medico, acceso a satélites de televisión así como muchas otras aplicaciones.

Otra definición para estos nuevos miembros de la familia de las tarjetas de plástico es:

“Una tarjeta de plástico, similar en tamaño y forma a una tarjeta de crédito, que contiene un microprocesador y/o memoria (el cual sirve para almacenar y procesar datos) y que cumple con el estándar ISO 7816”

En otros términos es una tarjeta con una pequeña computadora embonada.

2.1.2 Elementos de una tarjeta inteligente típica.

Una tarjeta inteligente tiene los mismos tres fundamentos de una computadora:

Energía de proceso, almacenamiento y el medio (entradas y salidas) de datos. La energía de proceso es proveída por un microprocesador chip (ejemplo; Intel 8051 o Motorota 6805) y almacenamiento de datos una memoria chip (EEPROM, FLASH, ROM, RAM). En algunos casos los tres elementos pueden ser combinados en un solo chip. El medio en el cual los datos son transferidos varia de tarjeta a tarjeta, en orden para que esta opere, cada tarjeta debe tener una fuente de poder, ya sea en un lector o igual embonada.

2.1.3 Breve historia de las tarjetas inteligentes.

Mucha gente considera que las tarjetas inteligentes son de reciente invención.

Pero nada es mejor que la verdad, en 1968, un inventor Aleman Jurgen Dethloff en compañía de Helmet Grotrupp archivaron la patente del embonado de microchips en plástico. En 1970, el inventor japones, Kunitake Arimura, aplicó para una patente similar. Y las tarjetas inteligentes fueron introducidas en el mismo año. En 1974, Frenchman Roland Moreno registró la patente de su tarjeta inteligente en Francia.

Dado a que la mayoría de la investigación de las tarjetas inteligentes inició en Europa, no es sorprendente que haya una cantidad de europeos utilizándolas. Actualmente Europa cuenta con aproximadamente el 80% del mercado en cuanto a tarjetas inteligentes se refiere. Francia y Alemania han sido los líderes del mundo en la introducción de varia aplicaciones para las tarjetas inteligentes. Las tarjetas inteligentes ya se están utilizando alrededor del mundo

para varios propósitos y en le futuro se espera que sean mucho más penetrantes.

Antes de continuar más a detalle con las tarjetas inteligentes, sería buena idea entender un poco acerca de su antecesor, la tarjeta de cinta magnética.

2.2 TARJETA DE CINTA MAGNETICA.

Esta aparece normalmente al reverso de una tarjeta de crédito, como ves es la cinta negra que se encuentra adherida en la propia tarjeta, aproximadamente tiene un ancho de media pulgada y va de extremo a extremo. Esta cinta negra, consiste de tres series de partículas magnetizadas y es el corazón de las tarjetas de la cinta magnética. Las tarjetas de cinta magnética fueron introducidas para:

- Almacenamiento de datos de forma que una maquina pueda leerlos.
- Minimizar la utilización de papel en transacciones financieras.
- Permitir la automatización.

Como ya fue explicado, la cinta magnética consiste de tres series, una serie esta dividida en pequeños dominios cada dominio cuenta o es de 1/75 th de pulgada de largo. Para almacenar datos en una tarjeta de cinta magnética, las partículas del dominio son magnetizadas en una forma particular (**Ver fig. 2.1**). Si dentro de cada dominio la polarización de las partículas no cambia, entonces no hay flujo de regreso y esto representa un 0 binario. Pero si la polarización cambia entonces hay flujo de regreso y esto representa un 1 binario.

Figura 2.1 Cinta magnética con dominios, (las flechas en los dominios representan la polarización de magnetización de partículas en el dominio)[1]

Cuando la tarjeta de cinta magnética es leída, el lector se basa en los flujos de regreso para obtener los datos almacenados en ella. En la figura 2.1 se representa una cinta magnética que al ser leída nos daría: 010010.

La longitud de una cinta magnética es de alrededor de 4 pulgadas y consiste de tres series cada serie esta hecha de dominios de 1/75 th de pulgada de largo. Cada dominio representa un bit. El total de datos que se pueden almacenar en una tarjeta de cinta magnética solo va de 900 a 1,000 bits.

El problema principal de una tarjeta de cinta magnética es que los datos pueden ser fácilmente leídos y alterados por cualquiera que tenga acceso a un equipo lector de cintas magnéticas. **CARD SKIMMING** es el nombre que se le da al proceso de leer datos válidos de una tarjeta y copiar bit por bit en otra. Los lectores de cinta magnética cuestan alrededor de 100 dólares mientras que un codificador (quemador) cuesta 1,000 dólares. Como resultados de estos costos estás tarjetas no pueden ser confiables para el almacenamiento de información confidencial.

2.3 CLASIFICACION DE TARJETAS INTELIGENTES

Estas tarjetas pueden ser clasificadas en base a varios parámetros, las clasificaremos en base a los componentes de cada tarjeta, la interfase de la tarjeta y el sistema operativo de la tarjeta. Esta clasificación se describe mejor en la **figura 2.2.**

[1] www.howstuffworks.com

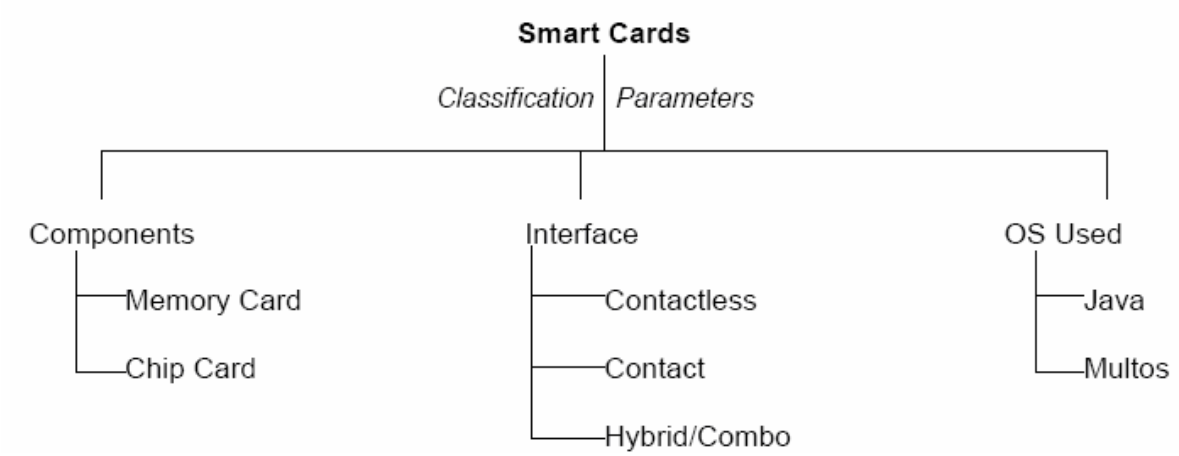


Figura 2.2 Clasificación de una tarjeta inteligente[2]

2.3.1 CLASIFICACION EN BASE A COMPONENTE.

Cuando clasificamos en base a los componentes que contiene, las tarjetas inteligentes pueden estar divididas en dos categorías. Aquellas con un procesador son llamadas tarjetas con chip o tarjetas con microprocesador y aquellas que no tienen chip son llamadas tarjetas con memoria.

TARJETAS CON MEMORIA (MEMORY CARDS):

Estas son más comunes y de un costo accesible, contienen:

- EEPROM: Electrically Erasable Programable Read Only Memory. Esto es como datos almacenados en un dispositivo donde todos los datos de la aplicación son escritos, típicamente la EEPROM cuenta con una capacidad desde 2 KB hasta 8 KB. La información o datos almacenados en una EEPROM puede ser bloqueada con un fin y usualmente varía con tiempo. Por ejemplo, las tarjetas de teléfono, en estas la EEPROM debe mantener el tiempo restante para hablar.

[2] www.howstuffworks.com

- ROM: Read Only Memory. Ésta almacena datos que no cambian durante el tiempo de vida de la tarjeta. Pueden ser números de tarjeta, nombres de tarjeta, etc.

La seguridad de las memorias se accesan mediante lógica de control por medio de esta se habilitan la lectura y escritura hacia la memoria, esto es que las regiones de las memorias se accesan solo después de ingresar un código secreto. Este código secreto es proveído por el lector de tarjetas inteligentes o por el usuario. Una simple arquitectura de una tarjeta con memoria se describe en la **figura 2.3**.

Una simple tecnología como es esta tarjeta puede ser construida por la cantidad de un dólar cuando se compra en cantidad. Estas tarjetas pueden almacenar información o datos desde 100 bytes hasta 8 KB. Estas tarjetas tienen mayor aceptación en las tarjetas de prepago como son las tarjetas de teléfono por su simplicidad. Otras áreas posibles donde también pueden ser utilizadas son las máquinas de refresco, el transporte público y estacionamientos públicos.

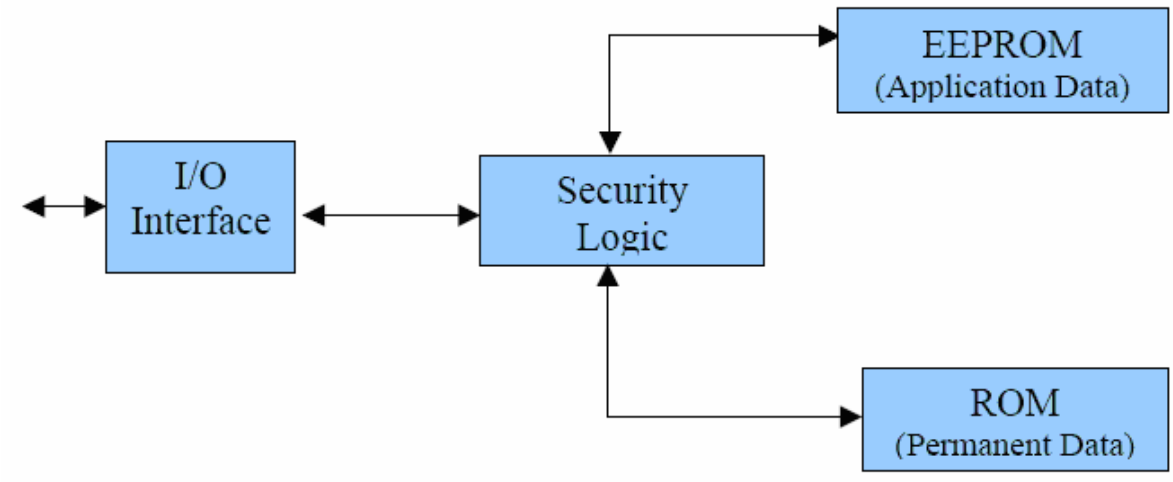


Figura 2.3 Arquitectura interna de una tarjeta con memoria.[3]

[3] www.howstuffhows.com

TARJETAS CON MICROPROCESADOR (CHIP CARDS):

Como el nombre lo dice estas son tarjetas que contienen un micro procesador, éstas son las que técnicamente se les podría llamar tarjetas inteligentes. Los componentes de una tarjeta son:

- ROM: Memorias de sólo lectura, la ROM en la tarjeta se encarga de mantener el sistema operativo y también es conocida como la máscara de la tarjeta. El tamaño de la ROM varía de acuerdo al sistema operativo desde algunos KB hasta 32 KB dependiendo en qué sistema operativo se esté usando en la tarjeta. Una vez que se grava la ROM no puede ser modificada.

- EEPROM: Ésta mantiene los programas de aplicación y los datos de los programas, estos datos no son permanentes y frecuentemente se borran y se rescriben. Las EEPROM típicas tienen un rango de 2 KB a 32 KB.

- RAM: Memoria de acceso aleatorio, ésta memoria es volátil y es utilizada por el procesador para almacenar funciones deseadas y los datos se borran cuando se le desconecta la fuente de poder, puede sonar sorprendente pero el típico tamaño de una RAM es de alrededor de 256 KB.

- CPU: Unidad central de procesamiento, éste es como el corazón de una tarjeta con chip, es un microprocesador basado en 8 bits con una velocidad de reloj de 5 Mhz. Esto parece lento comparado con uno de 32 bits, el CPU es el encargado de sacar varias instrucciones.

Las tarjetas de chip son más caras que las tarjetas de memoria, el rango del costo para estas tarjetas está entre 2 a 20 dólares dependiendo de las características disponibles. Estas tarjetas pueden almacenar múltiples aplicaciones y provee una seguridad robusta, estas tarjetas son utilizadas como control de acceso y tarjetas de crédito y otras tarjetas financieras entre otras aplicaciones que requieren de alta seguridad. En la figura 2.4 puede verse un ejemplo de su arquitectura interna.

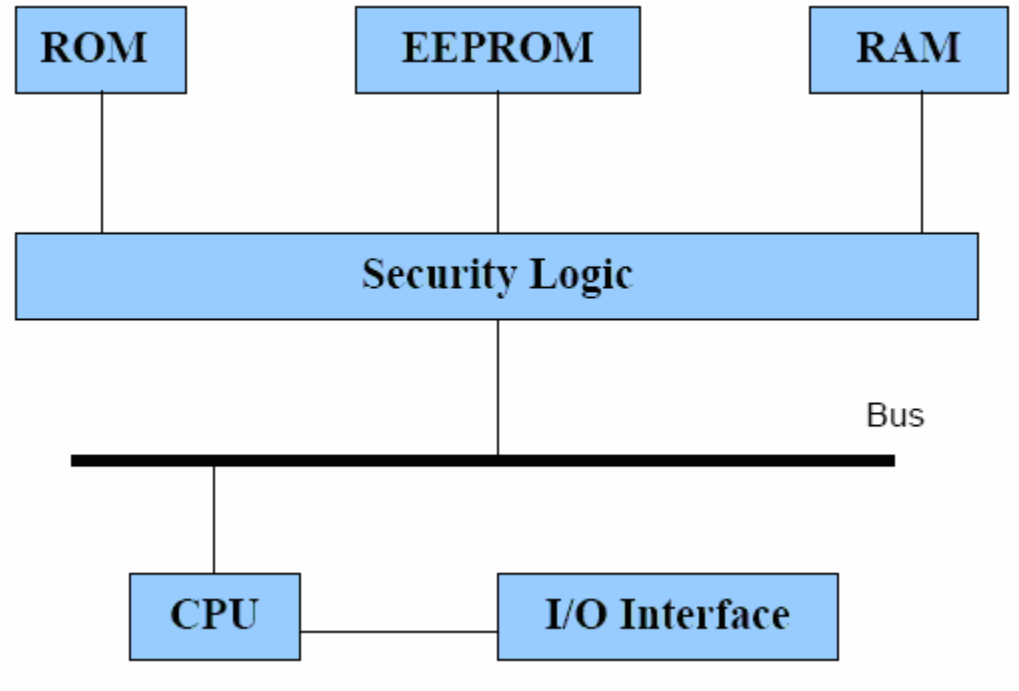


FIGURA 2.4 Arquitectura interna de una tarjeta con chip.[4]

2.3.2 CLASIFICACION EN BASE A INTERFACE

Las tarjetas inteligentes también se clasifican en base a su método de comunicación para la transferencia de datos con el dispositivo lector, en base a este criterio pues se clasifican como tarjetas de contacto, tarjetas sin contacto e híbridas (combinadas). Las tarjetas de contacto tienen que ser insertadas en un

[4] www.howstuffworks.com

dispositivo lector mientras que las tarjetas sin contacto son activadas mediante una señal de radio frecuencia y las tarjetas Híbridas o combinadas pueden ser insertadas en dispositivo lector o activadas por una señal de radio frecuencia.

TARJETAS DE CONTACTO:

Estas tarjetas requieren de ser insertadas para ser activadas, cada tarjeta contiene de 6-8 patillas marcadas usualmente en oro que establecen contacto con el dispositivo lector para la transferencia de datos. La tarjeta recibe alimentación a través del dispositivo lector vía las patillas ya mencionadas, y de acuerdo a la norma ISO 7816 ya está establecido el orden del patillaje en la tarjeta, como se muestra en la figura 2.5, aquí también vemos la designación de los contactos así como sus funciones que se explican en la tabla 2.1.

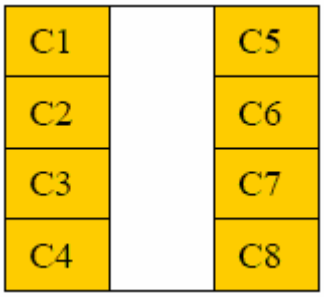


FIGURA 2.5 Contactos de una tarjeta de acuerdo al ISO-7816.[5]

[5] www.howstuffworks.com

TABLA 2.1 Nombres de los contactos de acuerdo con el ISO-7816.[6]

Contact No.	Contact Designation	Contact Function
C1	Vcc	Supply Voltage
C2	RST	Reset
C3	CLK	Clock
C4	RFU	Reserved for Future Use
C5	GND	Ground
C6	Vpp	Programming Voltage
C7	I/O	Input/Output
C8	RFU	Reserved for Future Use

Las tarjetas de contacto también tienen sus limitaciones, con el tiempo estos contactos se desgastan que llegan a un punto donde pueden no ser detectados por el lector, descargas electrostáticas pueden ser provocadas por no colocar adecuadamente la tarjeta y dañar los integrados, o en ocasiones por el mismo usuario que podría no dejar que el proceso de lectura termine correctamente y sacar la tarjeta antes de que la transacción termine o por último el uso rudo o tensiones de la misma pueden hacer que sufra daños físicos y no funcionar correctamente.

TARJETAS SIN CONTACTO:

Estas tarjetas no necesitan ser insertadas, basta con solo pasarlas cerca de una antena para que el lector realice la transacción de datos necesarios. La distancia de un lector varia desde unos pocos centímetros hasta 50 centímetros. Como en estas no existe contacto estas tarjetas cubren muchas de las limitaciones mencionadas en las tarjetas de contacto y además son muy rápidas en realizar sus transacciones por eso se utilizan en lugares donde se requiere que los datos sean descargados rápidamente por ejemplo: en casetas

[6] www.howstuffworks.com

automovilísticas, accesos electrónicos donde existe una gran masa de transito, etc.

Las tarjetas sin contacto obviamente tienen un costo mas elevado que las tarjetas de contacto aunque en cantidad no varia mucho, pero también tienen una gran ventaja en cuanto al tiempo de vida y son mas flexibles.

TARJETAS COMBINADAS O HIBRIDAS:

Las tarjetas combinadas son las que tienen ambas interfaces antes mencionadas tanto de contacto como sin contacto facilitando que sean utilizadas en cualquier aplicación requerida, cabe mencionar que tiene las limitaciones antes mencionadas y que existen este tipo de tarjetas para aplicaciones que necesitan de una seguridad avanzada pues utiliza el chip de contacto o de una gran velocidad de transferencia utiliza su antena y convertirse en sin contacto de inmediato.

2.3.3 CLASIFICACION EN BASE A SISTEMA OPERATIVO

Las tarjetas inteligentes también son clasificadas en base a su sistema operativo, esto quiere decir que también cuentan con un programa que tiene todas las funciones para realizar las transacciones necesarias. En el mercado podemos encontrar los siguientes sistemas operativos entre otros:

- MultOS
- JavaCard
- Ciberflex
- StrarCOS
- MFC

Los Sistemas Operativos para Tarjetas Inteligentes o SCOS como son conocidos, son grabados en la ROM y usualmente ocupan menos de 16 KB. Los SCOS tienen las siguientes propiedades:

- Manejo de archivos y su manipulación.
- Manejo de memoria.
- Protocolos de transmisión de datos.

2.4 VENTAJAS DE LAS TARJETAS INTELIGENTES

Comparadas con las tarjetas de cinta magnética las ventajas son muchas:

- La tarjeta inteligente puede almacenar hasta 32KB de datos mientras que las de cinta magnéticas solo pueden almacenar 1000 bits. Esto permite que la transacción de la tarjeta puede manejar mucha información adicional.

- Los datos en las tarjetas inteligentes pueden ser protegidos para que no sean vistos si no están autorizados, como resultado las contraseñas (PIN o PASSWORDS) son almacenados dentro de la tarjeta inteligente para el manejo de la información. Esto significa que los compradores no tienen que enlazarse mediante una línea para autorizar la transacción.

- Una tarjeta inteligente puede almacenar diferentes aplicaciones, esta puede ser tu licencia de conducir, el pasaporte, tarjeta de crédito, tarjetas de ID, etc..

- La vida de estas es larga.

- No es fácil crear una replica de una tarjeta inteligente y son mucho mas seguras que las tarjetas de cintas magnéticas.

Dadas estas ventajas, las tarjetas inteligentes han tomado el mercado de la telefonía publica, pero desafortunadamente no han sido tan exitosas como en el mercado financiero.

2.5 APLICACIONES DE LAS TARJETAS INTELIGENTES

Basado en números, las tarjetas telefónicas de prepago parecen ser las mas comunes en las aplicaciones del mercado, también existen aplicaciones donde la tarjeta es recargable, ya que el proveedor de estas tarjetas puede agregar un valor determinado de acuerdo a lo requerido por un usuario final, esto asegura que la tarjeta tenga un tiempo de uso alargado. Además de los teléfonos convencionales, los teléfonos celulares también utilizan tarjetas inteligentes, que es ya conocido chip o tarjeta SIM que se introduce al celular.

Otra ventaja es que ha permitido a los bancos financieros, remplazar sus tarjetas [ATM, tarjetas de debito, tarjetas de crédito, tarjetas de viajero y entretenimiento] por las nuevas tarjetas inteligentes y lo mejor es que pueden tener todas en una. También ya en algunos países las utilizan como monederos electrónicos, y ya algunos minoristas la utilizan como la tarjeta de confianza.

Las tarjetas inteligentes son utilizadas también para boletaje rápido (fast ticketing) para transporte público y estacionamiento en muchos países. Por

ejemplo en Corea del sur 1.5 millones de tarjetas para el transporte público son utilizadas por esto es uno de los países que mas utiliza las tarjetas inteligentes en transporte público, y le siguen Hong Kong e India en cuanto a esto respecta.

También muchas universidades y escuelas ya empiezan a utilizar estas tarjetas para identificación de los alumnos, ya que les dan un uso múltiple por mencionar algunos, la biblioteca, máquinas de dulces, pago en la cafetería, y algunos otros servicios con las que se cuenten dentro del campus universitario.

2.6 FUTURO DE LAS TARJETAS INTELIGENTES

Dadas las ventajas de la tarjeta inteligente contra las de una tarjeta de cinta magnética, ya se puede observar que se tienen muchas, y no hay duda de que el mercado de estas tarjetas es bastante amplio y ya podemos observar e imaginarnos muchas de las aplicaciones donde probablemente ya las veremos actuando en pocos años.

El mercado de estas tarjetas depende principalmente de las multi-aplicaciones que estemos manejando para poder adaptarlas y realizar una tarjeta inteligente que contenga todas estas aplicaciones en un solo pedazo de plástico y hacer mucho mas fácil la vida de los simples mortales.

CAPITULO III

FABRICANTES/OFERTA TECHNOLOGIA

3.1 INTEROPERABILIDAD

Así como todo artículo esta reglamentado o establecido por un estándar también las tarjetas inteligentes cuentan con su propio estándar, pero esto no quiere decir que deban estar bajo una sola tecnología ya que así como muchos artículos que realizan la misma función pueden ser de diferentes marcas, a esto se refiere la interoperabilidad que las tarjetas inteligentes tienen también la opción de trabajar bajo los diferentes fabricantes de tecnologías de tarjetas inteligentes, los cuales ya se verán posteriormente en este capitulo.

Las especificaciones de las tarjetas inteligentes son un conjunto de requisitos técnicos y de negocio que deben cumplir las compañías que participan en la emisión y aceptación de tarjetas inteligentes. Estas especificaciones se han desarrollado para garantizar que las tarjetas inteligentes puedan utilizarse globalmente.

La incompatibilidad de las aplicaciones, tarjetas y lectores ha sido uno de los motivos principales para la lenta adopción de tarjetas inteligentes fuera de Europa. La interoperabilidad entre los productos de los diferentes proveedores es un requisito necesario para habilitar la amplia aceptación de los consumidores de tarjetas inteligentes y para que las organizaciones distribuyan tarjetas inteligentes para su uso dentro de la empresa.

3.1.1 ESTANDARIZACIÓN

De contacto (ISO 7816, EMV y GSM)

Para promocionar la interoperabilidad entre las tarjetas inteligentes y los lectores, la Organización internacional de estándares (ISO) desarrolló los estándares ISO 7816 para las tarjetas de circuitos integrados con contactos. Estas especificaciones se centraron en la interoperabilidad física, eléctrica y de

protocolo de vinculación de datos. En 1996, Europay, MasterCard y VISA (EMV) definieron una especificación de tarjetas inteligentes propia del sector que adoptó los estándares ISO 7816 y definió algunos tipos de datos y reglas de codificación adicionales para su uso por la industria de servicios financieros. La industria de telecomunicaciones europea también adoptó los estándares ISO 7816 en su especificación de tarjetas inteligentes para el Sistema global para las comunicaciones móviles (GSM) con el fin de habilitar la identificación y autenticación de usuarios de teléfonos móviles.

Aunque todas estas especificaciones (ISO 7816, EMV y GSM) constituían un paso en la dirección correcta, cada una de ellas era de demasiado bajo nivel o demasiado específica de la aplicación como para ofrecer compatibilidad amplia con el sector. En ninguna de estas especificaciones se abordaban los problemas de interoperabilidad de las aplicaciones, como las API independientes del dispositivo, las herramientas para desarrolladores y el uso de recursos compartido.

ISO 7816 se encarga de definir las características de la tarjeta inteligente como son físicas, eléctricas y de protocolo de vinculación de datos.

3.1.2 Tarjeta Inteligente de Contacto

La serie de estándares **ISO/IEC 7816** e **ISO/IEC 7810** definen:

- la forma física
- la posición de las formas de los conectores eléctricos
- las características eléctricas
- los protocolos de comunicación
- el formato de los comandos enviados a la tarjeta y las respuestas retornadas por la misma
- robustez de la tarjeta
- funcionalidad

Las tarjetas no contienen baterías; la energía es suministrada por los lectores de tarjetas.

Los lectores de tarjetas inteligentes de contacto son utilizados como un medio de comunicación entre la tarjeta inteligente y un anfitrión, como por ejemplo una computadora.

Sin contacto (ISO 14443, 15693)

Son similares a las de contacto con respecto a lo que pueden hacer y a sus funciones pero utilizan diferentes protocolos de transmisión en capa lógica y física, no utiliza contacto galvanico sino de interfase inductiva, puede ser de media distancia sin necesidad de ser introducida en una terminal de lector inteligente. Una de las ventajas que ésta tarjeta tiene es que como no existen contactos externos con la tarjeta, esta es mas resistente a los elementos externos tales como la suciedad.

3.1.3 Tarjetas Inteligentes sin Contacto

El segundo tipo es la tarjeta inteligente sin contacto en el cual el chip se comunica con el lector de tarjetas mediante inducción a una tasa de transferencia de 106 a 848 Kb/s). El estándar de comunicación de tarjetas inteligentes sin contacto es el **ISO/IEC 14443** del 2001. Define dos tipos de tarjetas sin contacto ("A" y "B"), permitidos para distancias de comunicación de hasta 10 cm. Han habido propuestas para la ISO 14443 tipos C, D, E y F que todavía tienen que completar el proceso de estandarización. Un estándar alternativo de tarjetas inteligentes sin contacto es el **ISO 15693**, el cual permite la comunicación a distancias de hasta 50 cm.

Para ver más acerca de los estándares y sus actualizaciones con respecto a tarjetas inteligentes visite la página Web de la Organización Internacional de Estándares (ISO) www.iso.org. [1]

3.2 TECNOLOGIA MIFARE

La tarjeta inteligente de memoria MIFARE está basada en el chip MIFARE F1-S50 de Philips, tiene una distancia de lectura y escritura sin contacto de hasta 10 cm., la cual varía según el lector. Puede tener hasta 15 aplicaciones en su memoria. No requiere de baterías. Las soluciones principales Son:

- Control de Acceso
- Almacenamiento de patrones biométricos
- Monedero electrónico
- Tarjetas de lealtad
- Tarjetas de débito para universidades
- Transporte público

3.2.1 ESPECIFICACIONES FUNCIONALES:

3.2.1.1 Características…

Interfaz de radio frecuencia MIFARE (ISO/IEC 14443 A)

- Transmisión sin contacto de datos y fuente de energía (no necesita batería)

[1] www.iso.org

- Distancia de operación: hasta 100 mm (dependiendo en la geometría de la antena)
- Frecuencia de operación: 13.56 MHz
- Transferencia de datos rápida: 106 kbits/s
- Alta integridad de datos: 16 Bit CRC, parity, bit coding, bit counting
- Anti-collision verdadera
- Transacción típica de recibos: <100 ms (incluye el manejo de respaldos)

3.2.1.2 EEPROM

- 1Kbyte, organizada en 16 sectores con 4 bloques de 16 bytes cada uno (cada bloque consiste de 16 bytes)
- Acceso definido de usuario mediante condiciones para cada bloque de memoria.
- Detención de datos de 10 años.
- Resistencia de escritura hasta de 100,000 ciclos.

3.2.1.3 SEGURIDAD

- Autentificación del paso triple mutuo (ISO-IEC DIS9798-2)
- Encriptación de datos en el canal de radio frecuencia (RF-CHANNEL) con la protección de ataque.
- Compuesto individual de dos llaves por sector (por aplicación) para soportar multi-aplicación con llaves jerárquicas.
- Numero de serie único para cada dispositivo.
- Llave transportable para protección de acceso a la memoria (EEPROM) en el envió del integrado (Chip).

3.2.2 Descripción General

3.2.2.1Alimentación de energía sin contacto y transferencia de datos.

En el sistema de MIFARE, el MF1 IC S50 es conectado a una bobina con unas pocas vueltas y embonada en un plástico para formar una tarjeta inteligente pasiva. No necesita batería. En cuanto esta es posicionada cerca de la antena del dispositivo de lectura y escritura (RWD), la alta velocidad de comunicación en RF permite a la interfaz transmitir datos a 106 kBit/s.

3.2.2.2 Anti-collision

Tiene una función inteligente para la anti-collision que permite operar mas que otras tarjetas del mismo campo, simultáneamente. El algoritmo de anti-collision selecciona cada tarjeta individual y se asegura que la ejecución de la transacción con la tarjeta seleccionada sea procesada perfectamente sin corrupción de datos resultantes de otras tarjetas del mismo medio.

3.2.2.3 Conveniencia de usuario

El sistema MIFARE esta diseñado para un óptimo uso convencional. El alto porcentaje de transmisión de datos permite completar la transacción de un recibo en menos de 100 ms. Y de hecho permite al usuario mantenerla dentro de la cartera aun cuando esta tiene monedas, al momento de pasarla en un dispositivo de lectura/escritura (RWD)

3.2.2.4 Seguridad

Actualmente se ha puesto un énfasis especial en la seguridad por el fraude ya existente. Un reto mutuo y respuesta autentificada, el cifrado de datos y autentificación de mensajes son revisados para proteger el sistema de cualquier tipo de violación forzosa y que la haga atractiva para aplicaciones duplicadas. Los números de serie, tampoco pueden ser alterados, ya que es único para cada tarjeta.

3.2.2.5 De aplicación múltiple.

El sistema MIFARE ofrece una real multi-aplicación funcional que se compara con las características de una tarjeta de procesador. Utiliza dos llaves diferentes para cada sector que este sistema soporta, y estas son jerárquicas.

3.2.2.6 Opciones de envió.

- dado en la oblea (die on wafer)
- dado topado en la oblea (bumped die on wafer)
- modulo de tarjeta de chip (chip card module)

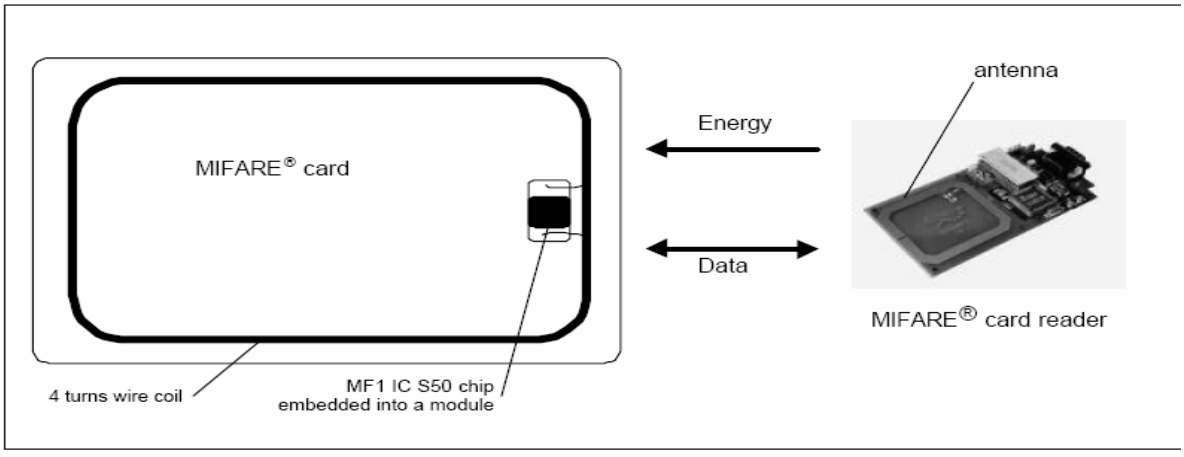


Figura. 3.1 Tarjeta MIFARE.[2]

[2] www.hid.com

3.3 Descripción Funcional

3.3.1 Descripción del bloque.

El integrado MF1 IC S50, consiste de 1kByte EEPROM, la interfase RF y la unidad de control digital. La energía y datos son transferidos vía antena, la cual consiste de una bobina con unas pocas vueltas directamente conectada al MF1 IC S50. Sin embargo son necesarios componentes externos.

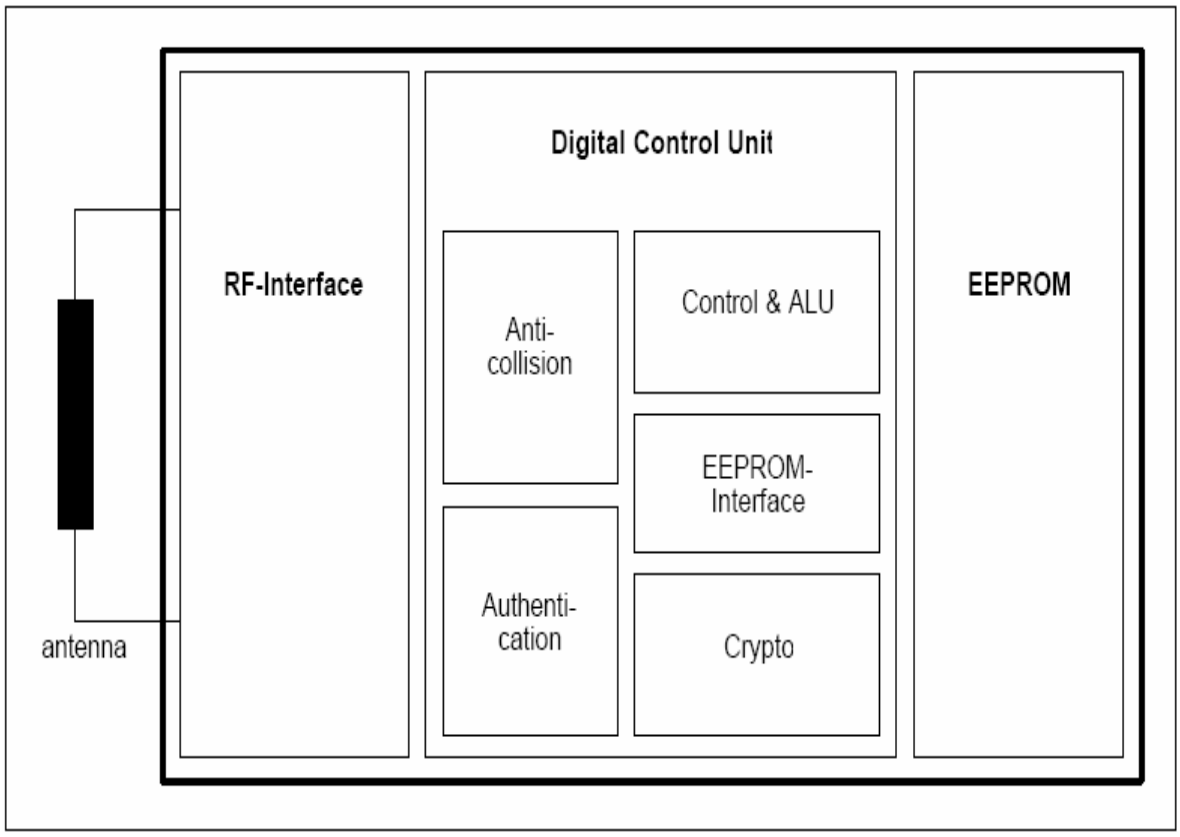


Figura. 3.2 Diagrama de bloques de una tarjeta Mifare.[3]

[3] www.hid.com

3.3.2 Principio de la comunicación

Los comandos son iniciados por el dispositivo de lectura y escritura (RWD) y controlado por la unidad de control digital (ALU) del integrado MF1 IC S50 de acuerdo con las condiciones de acceso validas al sector correspondiente.

3.3.3 Petición estándar/todos (REQUEST STANDARD/ALL)

Después del power on reset (POR) de una tarjeta, se hace la petición de un comando, enviado por el dispositivo de lectura/escritura (RWD) a todas las tarjetas dentro del campo magnético (antena), y se genera un código requerido por el RWD. (de acuerdo al ISO/IEC 14443).

3.3.4 Lazo de la anticolisión (ANTICOLLISION LOOP)

En el lazo de anticolisión el numero de serie de una tarjeta es leído, y dado a que todas las tarjetas tienen un numero de serie diferente el RWD (dispositivo de lectura/escritura) puede fácilmente identificar dicha tarjeta para transacciones posteriores, en caso de estar mas de una tarjeta las demás regresan a su estado standby y esperan a una nueva petición de comandos.

3.3.5 Tarjeta seleccionada (SELECT CARD)

Con el comando de la tarjeta seleccionada por medio del RWD, este selecciona una autentificación y operación relacionada con la memoria.

3.3.6 Autentificación paso triple (3 PASS AUTHENTICATION)

Ya que se selecciono la tarjeta mediante el RWD se especifica la ubicación de la memoria y usa la llave correspondiente para el procedimiento de la autentificación paso triple, y al obtener éxito en este procedimiento todas las operaciones son codificadas (encripted).

3.3.7 Operaciones de memorias (MEMORY OPERATIONS)

Después de la autentificación cualquiera de las operaciones siguientes pueden ser procesadas:

- Read block : leer bloque.
- Write block: escribir bloque.
- Decrement: Decremento del contenido del bloque y el resultado lo almacena dentro de un registro temporal interno.
- Increment: Incremento del contenido del bloque y el resultado lo almacena dentro del registro de datos.
- Restore: Mueve el contenido de un bloque al registro de datos.
- Transfer: Escribe el contenido del registro temporal interno a un valor del bloque.

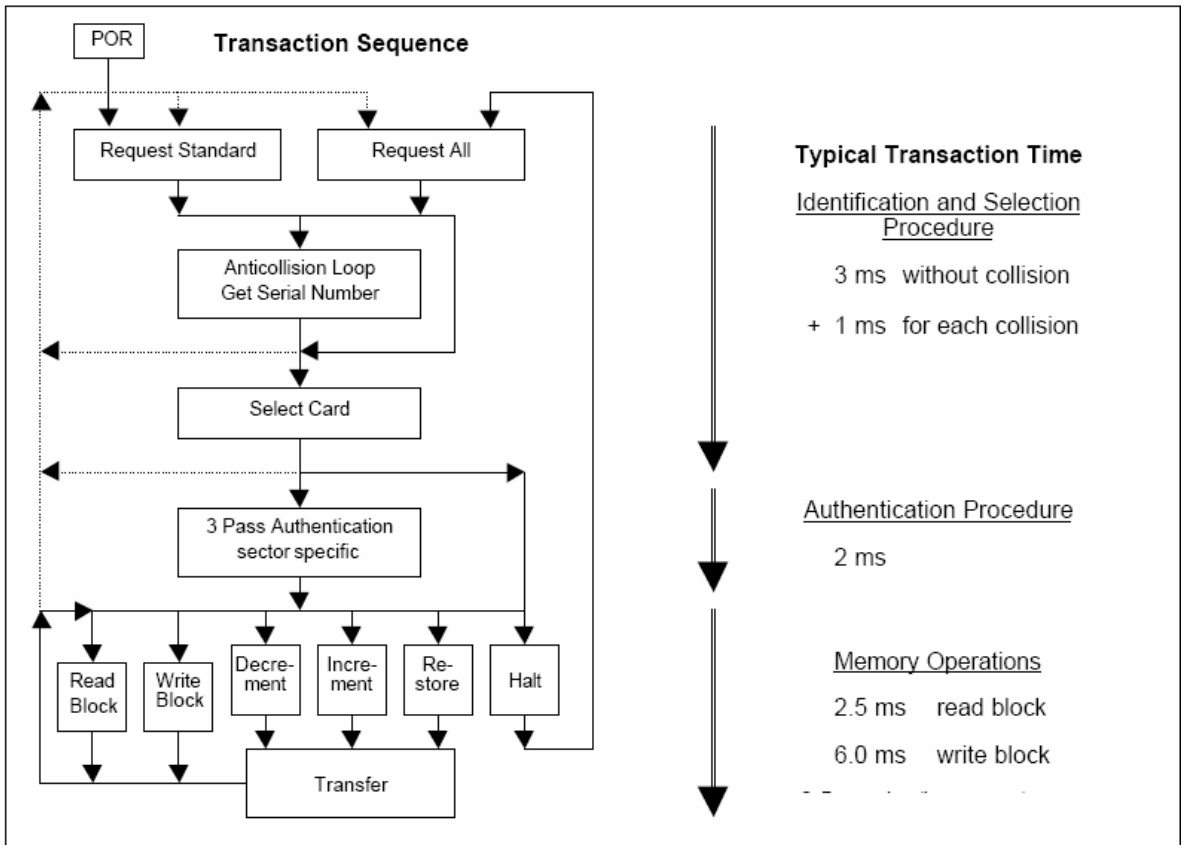


Figura. 3.3 Transacción de operaciones.[4]

3.4 Integridad de datos

Los siguientes mecanismos son implementados para la comunicación entre el RWD y la tarjeta para asegurar que sea confiable la transmisión de datos:

- 16 bits CRC (cyclic redundancy code) per block.
- Parity bits for each byte.
- Bit count checking.
- Bit coding to distinguish between “1”, “0”, and no information.
- Channel monitoring (protocol sequence and bit stream analysis)

[4] www.hid.com

3.5 Seguridad

Para proveer un alto nivel de seguridad se utiliza la autentificación paso triple de acuerdo al estándar ISO 9798-2.

3.5.1 Secuencia de autentificación paso triple (Three pass authentication sequence)

a) El RWD especifica el sector que será accesado y selecciona la llave A o B.

b) La tarjeta lee la llave secreta y permite el acceso con condiciones las condiciones del sector de la memoria. Después la tarjeta envía un número aleatorio como reto al RWD. (Paso uno)

c) El RWD calcula la respuesta usando la llave secreta y entradas adicionales. La respuesta, junto con el número aleatorio del RWD, se transmite nuevamente a la tarjeta. (Paso dos)

d) La tarjeta verifica la respuesta del RWD mediante una comparación su propio número aleatorio, entonces lo calcula y lo transmite. (Paso tres)

e) El RWD verifica que la respuesta de la tarjeta por medio de una comparación con el de el mismo.

Después de la transmisión del primer numero aleatorio la comunicación entre el RWD y la tarjeta se codifica (communication between card and RWD is encrypted).

3.6 Interfase de RF

La interfaz-RF es de acuerdo al estándar de la tarjeta sin contacto ISO/IEC 14443A. El campo de acarreo del RWD siempre esta presente porque es utilizado como fuente de energía para la tarjeta sin contacto. (Con pausas cortas en la transmisión)

3.7 Organización de la memoria

La memoria EEPROM de 1024 X 8 bit esta organizada en 16 sectores con 4 bloques cada uno. En el estado de borrado la celda de EEPROM son leídas con un “0” lógico y en el estado de escritura con un “1” lógico.

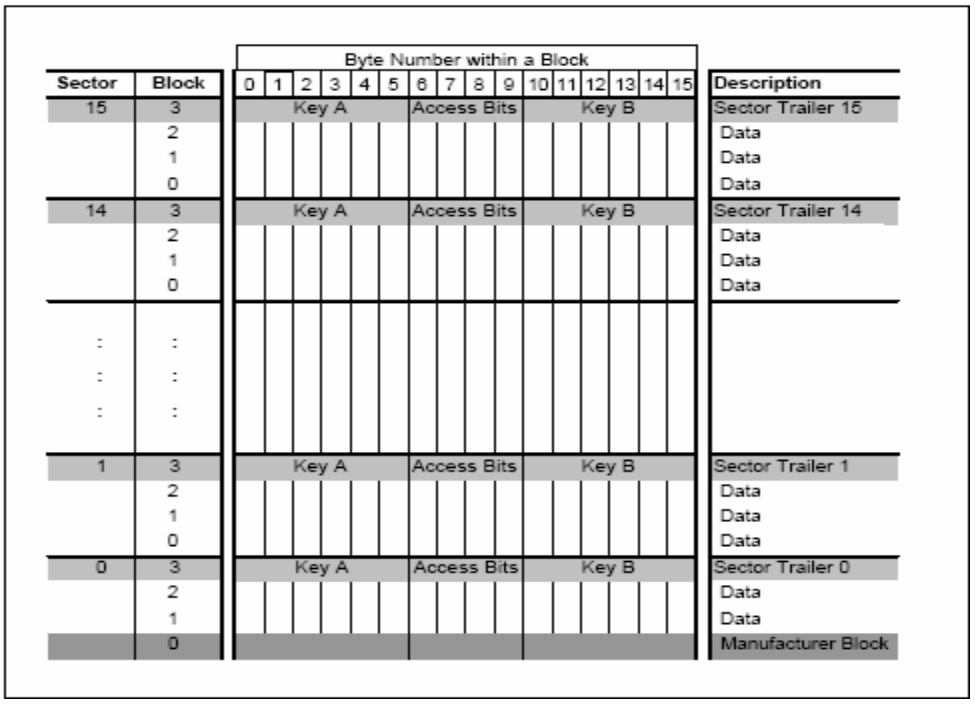


Figura. 3.4 Organización de la memoria.[5]

[5] www.hid.com

3.7.1 Manufactura del Bloque

Este es el primer dato del bloque (block 0) del primer sector (sector 0). Y contiene la manufactura de datos del integrado. Por cuestión de seguridad y requisitos del sistema este bloque esta protegido de escritura después de haber sido programado en su momento de manufactura en la producción.

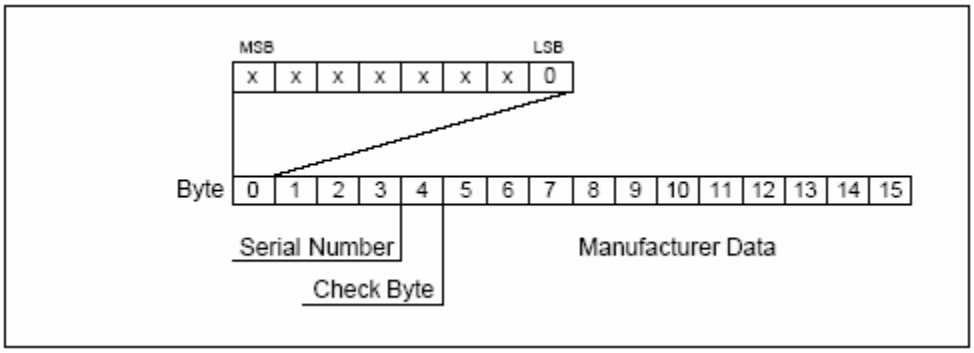


Figura. 3.5 Bloque de memoria[6]

3.7.2 Bloques de Datos

Todos los sectores contienen 3 bloques de 16 bytes para el almacenamiento de datos (el sector 0 contiene dos bloques solamente y el de lectura-solamente que es el bloque de fabricación).

Los bloques de datos pueden ser configurados por los bits de acceso como:

- Bloques de Lectura/Escritura por ejemplo, acceso controlado sin contacto.
- Bloques de valor por ejemplo, aplicaciones de monedero electrónico, donde comandos adicionales como incremento y

[6] www.hid.com

decremento para un control directo del almacenamiento de un valor proveído.

Un comando de autentificación tiene que ser acarreado antes de cualquier operación de la memoria para permitir comandos posteriormente.

3.7.2.1 Bloques de Valor

Los bloques de valor permiten realizar funciones de monedero electrónico (valid comands: read, write, increment, decremen, restore, transfer).

Los bloques de valor tienen un formato de datos compuesto que permite la detección de errores y un manejo de corrección y respaldo. Un valor solo puede ser generado mediante una operación de escritura en un formato del bloque de valor:

- Value: significa un valor asignado de 4-byte. El byte menos significativo es almacenado en el byte menos significativo de la dirección. Los valores negativos son almacenados con complemento a 2 como estándar. Por razones de integridad de datos y seguridad, un valor es almacenado 3 veces, dos no invertidas y una invertida.
- Adr: significa 1-byte para la dirección, la cual puede ser grabada y almacenar la dirección de un bloque, cuando se genera un respaldo de importancia. La dirección se almacena 4 veces, dos invertidas y dos no invertidas. Durante las operaciones de incremento, decremento, restablecimiento y transferencia, las direcciones se mantienen sin cambio. Solo pueden ser alteradas mediante el comando de escritura.

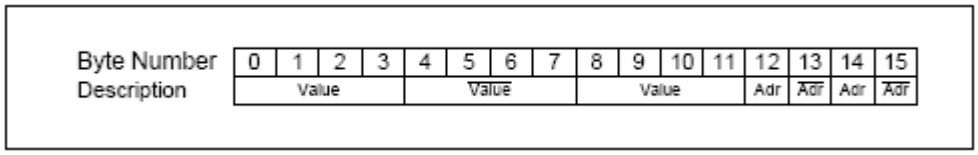


Figura. 3.6 Descripción del bloque de valor[7]

3.7.3 Sector Acoplado (SECTOR TRAILER)(Bloque 3)

Cada sector tiene un sector acoplado que contiene:

- Llave secreta A y B (opcional), la cual regresa un “0” lógico cuando se lee.
- Las condiciones de acceso para los 4 bloques del sector, los cuales están almacenados dentro de los 6-9 bytes. Los bits de acceso especifican (read/write or value) de los bloques de datos.

Si la llave B se necesita los últimos 6 bytes del bloque 3 pueden ser usados como bytes de datos.

El byte 9 del sector acoplado esta disponible para datos de usuario. Para este byte también aplican los mismos derechos que para los bytes 6,7 y 8.

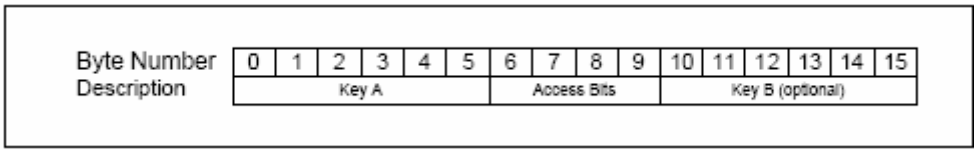


Figura. 3.7 Bloque 3

[7] www.hid.com

3.8 Acceso a memoria

Antes de que cualquier operación pueda ser acarreada, la tarjeta debe ser seleccionada y autentificada como se describe previamente. Las posibles operaciones de una memoria en un bloque de direcciones depende de tener acceso al almacenamiento del sector acoplado y de la llave utilizada.

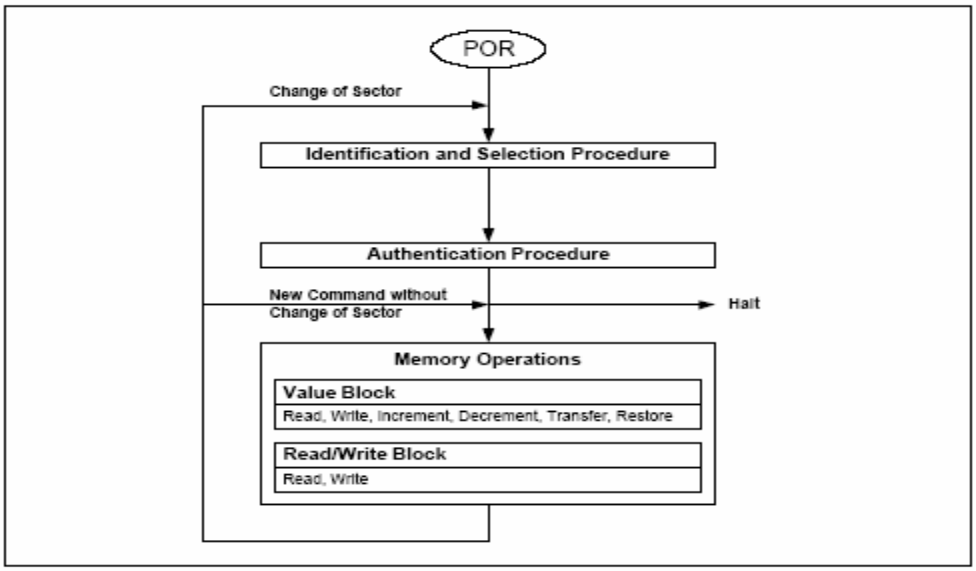


Figura. 3.9 Diagrama de flujo para el acceso a memoria.[8]

Tabla. 3.1 operaciones de la memoria.[9]

Memory Operations		
Operation	**Description**	**Valid for Block Type**
Read	reads one memory block	read/write, value and sector trailer
Write	writes one memory block	read/write, value and sector trailer
Increment	increments the contents of a block and stores the result in the internal data register	value
Decrement	decrements the contents of a block and stores the result in the internal data register	value
Transfer	writes the contents of the internal data register to a block	value
Restore	reads the contents of a block into the internal data register	value

[8] www.hid.com
[9] www.hid.com

3.8.1 Condiciones de acceso

Las condiciones de acceso para cada bloque de datos y sector acoplado están definidas por 3 bits, los cuales están almacenados como no-invertido e invertido en el sector de acoplamiento del sector especificado.

El acceso de bits controla los derechos de la memoria de acceso utilizando las llaves secretas A y B. Las condiciones de acceso pueden ser alteradas, mientras sepamos la llave relevante y el acceso en curso la condición permite la operación.

La lógica interna de el integrado MF1IC S50 asegura que los comandos son ejecutado solamente después de un procedimiento de autentificación o nunca.

Nota: en la próxima descripción de acceso de bits son mencionados solamente en modo de no-invertido.

Access Bits	Valid Commands		Block	Description
$C1_3\ C2_3\ C3_3$	read, write	→	3	sector trailer
$C1_2\ C2_2\ C3_2$	read, write, increment, decrement, transfer, restore	→	2	data block
$C1_1\ C2_1\ C3_1$	read, write, increment, decrement, transfer, restore	→	1	data block
$C1_0\ C2_0\ C3_0$	read, write, increment, decrement, transfer, restore	→	0	data block

Figura. 3.10 Acceso de bits en modo no invertido.[10]

[10] www.hid.com

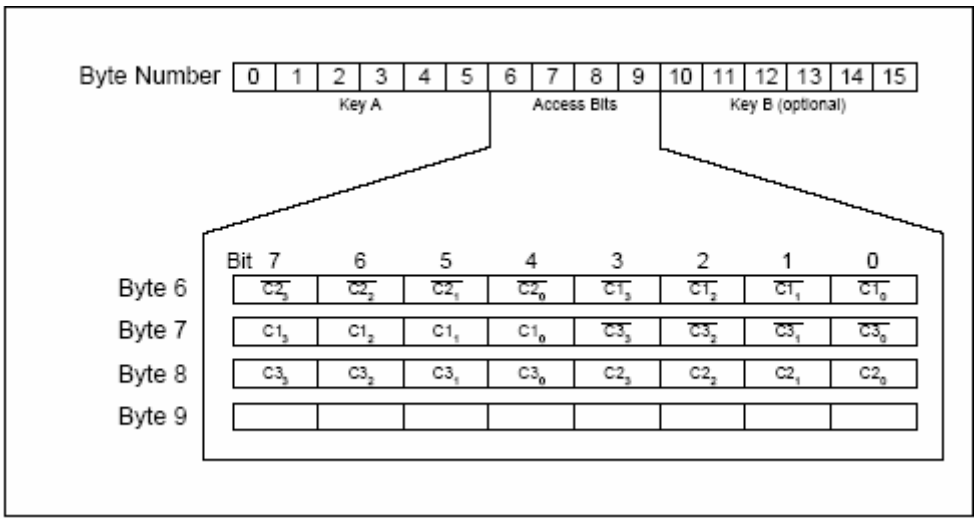


Figura. 3.11 Descripción de acceso de bits por byte.[11]

Nota: Con cada acceso de memoria la lógica interna verifica el formato de las condiciones de acceso. Y si detecta violación en el formato todo el sector puede generar un bloqueo irreversible.

3.8.2 Condiciones de acceso para el sector acoplado.

Dependiendo de el acceso de bits para el sector acoplado (bloque 3) la lectura/escritura de acceso a las llaves y al acceso de bits que se especifican como ‘NEVER’, ‘KEY A’, ‘KEY B’, o ‘KEY A|B’ (KEY A or KEY B)

En el envió del integrado las condiciones de acceso para el sector acoplado y la llave A (KEY A) son predefinidas como configuración de transporte. Dado que la llave B (KEYB) puede ser leída en la configuración de transporte, las tarjetas nuevas deben ser autentificadas con la llave A (KEY A).

Se deben tomar las precauciones especiales para la personalización de tarjetas ya que el acceso de bits puede ser bloqueado.

[11] www.hid.com

Access bits			Access condition for						Remark
			KEYA		Access bits		KEYB		
C1	C2	C3	read	write	read	write	read	write	
0	0	0	never	key A	key A	never	key A	key A	Key B may be read
0	1	0	never	never	key A	never	key A	never	Key B may be read
1	0	0	never	key B	key A|B	never	never	key B	
1	1	0	never	never	key A|B	never	never	never	
0	0	1	never	key A	key A	key A	key A	key A	Key B may be read, transport configuration
0	1	1	never	key B	key A|B	key B	never	key B	
1	0	1	never	never	key A|B	key B	never	never	
1	1	1	never	never	key A|B	never	never	never	

Figura. 3.12 Accesos para las llaves. [12]

Nota: las líneas marcadas en gris son condiciones de acceso de bits que indican que la llave B (KEY B) puede ser leída y utilizada para datos.

3.8.3 Condiciones de acceso para los bloques de datos.

Dependiendo de el acceso de bits los accesos a los bloques (blocks 0…2) de lectura/escritura son especificados como 'NEVER', KEYA', 'KEYB', o 'KEY A|B'. La configuración del acceso de bits relevante define la aplicación y los comandos correspondientes que aplican. Aquí se describen:

- Read/write block: las operaciones de lectura/escritura habilitada
- Value block: habilita las operaciones adicionales increment, decrement, restore, transfer. En el caso de ('001') solamente se permite leer y decrementar para tarjetas no recargables. En otro caso ('110') el recargado es posible al utilizar la llave B (KEY B).

[12] www.hid.com

- Manufacturer block: la condición de solo lectura no se afecta por la configuración del acceso de bits.
- Key management: En transport la llave A (KEY A) debe ser utilizada para la autentificación.*

Access bits			Access condition for				Application
C1	C2	C3	read	write	increment	decrement, transfer, restore	
0	0	0	key A|B[1]	key A|B[1]	key A|B[1]	key A|B[1]	transport configuration
0	1	0	key A|B[1]	never	never	never	read/write block
1	0	0	key A|B[1]	key B[1]	never	never	read/write block
1	1	0	key A|B[1]	key B[1]	key B[1]	key A|B[1]	value block
0	0	1	key A|B[1]	never	never	key A|B[1]	value block
0	1	1	key B[1]	key B[1]	never	never	read/write block
1	0	1	key B[1]	never	never	never	read/write block
1	1	1	never	never	never	never	read/write block

Figura. 3.13 Acceso a los bloques de datos.[13]

3.9 Aplicaciones para mejora de la vida

Estos productos no son diseñados para uso en aparatos, dispositivos, o sistemas donde se pueda ver un mal funcionamiento razonable y tener como resultado hasta una fractura personal.[14]

3.10 TECNOLOGIA ICLASS

HID Corporation, el líder mundial en tarjetas y lectores de proximidad y Wiegand, tiene el orgullo de presentar iCLASS, una nueva tecnología de tarjetas inteligentes sin contacto optimizada para control de acceso físico, autentificación segura en sistemas informáticos y otras aplicaciones.

[13] www.hid.com
[14] www.hid.com

Las Tarjetas y los lectores inteligentes iCLASS hacen el control de acceso más seguro, más versátil y, lo más importante, incrementan la seguridad por medio de encriptación y autentificación recíproca. Al mismo tiempo, iCLASS es de fácil uso, ofreciendo por un precio accesible, la conveniencia y la confiabilidad de la tecnología de proximidad por la cual HID es conocida en todo el mundo.

Imagine una solución con una sola tarjeta, que le permite no solamente leer información en forma rápida y segura, sino que además le permite grabar datos con absoluta seguridad, para un sinnúmero de aplicaciones.

Usted ha imaginado iCLASS, de HID.

3.10.1 iCLASS cumple con los Estándares de la Industria

El equipo de desarrollo de Identification Technology Group (ITG) de ASSA ABLOY ha utilizado una tecnología avanzada de semiconductor basada en la frecuencia de 13.56 MHZ para cumplir con varios estándares ISO. Los lectores iCLASS pueden leer datos de tarjetas que son compatibles con los siguientes estándares:

- 15693 – lectura / escritura; credenciales de 2Kbits (256Bytes) y 16Kbits (2KBytes) iCLASS
- 14443A – solamente lectura; MIFARE® (número de serie)
- 14443B2 – lectura / escritura; credenciales de 16Kbits (2KBytes) iCLASS

Es muy importante en materia de tarjetas inteligentes, cumplir con los estándares arriba citados, porque esto permite que muchos desarrolladores de equipos y aplicaciones, trabajen con esta tecnología para crear una mayor variedad de usos para la tarjeta.

3.10.2 iCLASS Ofrece Seguridad Avanzada:

Las tarjetas y los lectores iCLASS ofrecen varias características únicas que los colocan por encima de la tecnología tradicional de identificación por radiofrecuencia (RFID). Estas características incluyen:

- Almacenamiento de datos encriptados (codificados)
- Autentificación recíproca
- Lectura y escritura segura de datos
- Llaves de acceso definibles por el usuario

Toda transmisión de datos por radio frecuencia entre la tarjeta y el lector es encriptada (codificada), usando un algoritmo seguro. Utilizando técnicas estándares de encriptación de la industria, iCLASS reduce el riesgo de datos comprometidos o de tarjetas duplicadas. Y para mayor seguridad, los datos pueden ser también protegidos con

Encriptación (codificación) DES o Tripe DES.

3.10.3 Familia de Productos iCLASS™

Para satisfacer las necesidades de nuestros clientes, iCLASS consistirá en una familia de productos:

Lectores de Tarjetas Inteligentes Sin Contacto iCLASS:

La familia de lectores iCLASS presenta un vigorizante estilo arquitectónico con una elegante cubierta curveada. La barra de luz de alta intensidad con tres colores provee una retroalimentación visual nítida aun en contacto directo con la luz del sol.

Secuencias de distintos tonos seleccionables indican condiciones de estado. Usted puede instalar con confianza los lectores de tarjetas sin contacto iCLASS, sabiendo que su salida Wiegand fácilmente se comunica con la mayoría de los paneles de control de acceso con protocolo Wiegand.

La familia de lectores de tarjeta inteligente sin contacto iCLASS incluirá:

- Lectores de solamente lectura
- Lectores de lectura / escritura
- Teclado de lectura / escritura
- Terminal LCD de lectura / escritura
- Terminal biométrico

Credenciales Inteligentes Sin Contacto iCLASS:

La familia de credenciales iCLASS incluirá los más populares formatos de tarjetas, etiquetas y llaveros. HID también ofrecerá credenciales multi-tecnologías: iCLASS Prox e iCLASS Wiegand. Todas las credenciales iCLASS estarán disponibles en configuraciones de 2Kbits (256KBytes) o de 16Kbits (2KBytes).

La Etiqueta iCLASS y las credenciales multi-tecnologías iCLASS le ayudarán a soportar la actualización de sistemas de ferrito de bario, código de barra, banda magnética, sistemas Wiegand o de proximidad, a la tecnología iCLASS. Adhiriendo la Etiqueta iCLASS a una tarjeta o dispositivo existente (como un PDA o teléfono celular), tendrá instantáneamente la tecnología iCLASS.

Las credenciales multi-tecnologías permiten a los usuarios contar con una tarjeta con foto identificación, y experimentar la conveniencia de poder utilizarla en diferentes tipos de lectores.

3.10.4 Módulos OEM iCLASS:

Los módulos OEM iCLASS permitirán a fabricantes integrar fácilmente la tecnología iCLASS en sus propios productos. Los usuarios finales de la tecnología iCLASS pueden usar estos productos para ayudarles a administrar y controlar diversos ambientes. Los módulos OEM les permiten a aquellos que no están dentro del negocio tradicional de la seguridad física, a desarrollar nuevas aplicaciones para la tecnología iCLASS.

3.10.5 Administración de Llaves de iCLASS:

La Administración de llaves es hecha fácilmente! Todas las tarjetas son enviadas con llaves únicas diversificadas, y los lectores son enviados con una base de datos de llaves compatible, todo esto derivado de la llave de transporte estándar de HID. Mientras que las tarjetas y los lectores con claves Padrones son intercambiables, las llaves son altamente seguras y las tarjetas pueden volverse exclusivas, ordenándolas con formato Corporate 1000.

Tarjetas y lectoras con llaves personalizadas específicas del local también están opcionalmente disponibles en la fábrica, o el programador CP400 iCLASS puede ser usado para crear una base de datos clave específica del local y una tarjeta de configuración de lector, lo que permite al usuario crear una nueva clave para tarjetas y lectores en el sitio. La adaptación de claves provee el nivel más alto de seguridad, donde tarjetas y lectores son exclusivamente combinados con sitios individuales o clientes y no son intercambiables.

3.10.6 Aplicaciones iCLASS:

La familia de productos iCLASS fue proyectada para atender a las expectativas de nuestros clientes con relación a una verdadera solución de varias aplicaciones.

- Control de acceso

- Puntualidad y Asistencia
- Acceso autorizado a equipos del escritorio
- Dinero digital
- Autenticación Segura de TI
- Control y facturación de iluminación y HVAC
- Pases de tránsito
- Patrulla de vigilancia por turno
- Verificación de equipo y material
- Programas de fidelidad y asociación

3.10.7 ¿Por qué iCLASS?

Otras tecnologías, como MIFARE®, que son basadas en la frecuencia de operación 13.56 MHz, fueron inicialmente desarrolladas para al mercado de “transacción” (o sea, venta en tránsito y sin dinero). Se ha probado que este factor limita mucho el uso de la tecnología tanto en el mercado de control de acceso como en otras áreas de aplicaciones más modernas.

iCLASS fue especialmente idealizado para convertir el control de acceso más poderoso, más versátil y más seguro. Todo esto a un precio accesible. Contando aún con la capacidad de administrar efectivamente el costo de la creación de nuevas aplicaciones, esto resulta una solución inteligente sin contacto y segura.

Las de 2KBITS (256 BYTES) ICLASS

- Disponibles en dos áreas de configuración solamente.
- Provee el acceso estándar de HID para controlar el área de aplicación y otra área de aplicación para personalizar.

- Cuenta con el estándar ISO 15693 para comunicaciones de lectura/escritura sin contacto.
- Provee un costo efectivo para cubrir la seguridad y de acceso y control de instalación.

Las de 16KBITS (2KBYTES) ICLASS

- Offer sufficient read/write memory to store multiple biometric templates.
- Ofrece suficiente capacidad de memoria para la lectura/escritura de múltiples aplicaciones.
- Esta disponible en 2 o 16 aplicaciones para el área de configuración.
- Offer multiple, securely separated areas to enable numerous applications, including the HID standard access control application.
- Ofrece multiples áreas para seguridad separada y numerosas aplicaciones, incluyendo el estándar de HID para el control de acceso.
- Dispuesto a soportar futuras tecnologías/ de lectura/escritura.
- Cuenta con el estándar ISO 15693 Y 14443B2 para lectura/escritura para comunicaciones sin contacto.

3.10.8 Organización de la Memoria

Los siguientes recuadros describen las diferentes capacidades de memorias que esta tecnología utiliza para llevar acabo sus aplicaciones en este campo.

Tabla 3. 2 Descripción de la memoria 2 k/2[15]

- **2 kilobits (256 Bytes)**
- **2 Application Areas**
- **Read/Write Area is blocks 6 through 31, 208 bytes**
- **Barrier at block 18 can be moved**
- **ISO 15693 Mode only**
- **Keys cannot be updated once fuse is set**

Tabla 3.3 Descripción de la memoria 16K/2[16]

- 16 kilobits (2kBytes)
- 2 Application Areas
- Read/Write Area is blocks 6 through 255, 2000 bytes
- ISO 15693 & 14443 Mode
- Keys can be updated by HID / partner / customer

[15] www.hid.com
[16] www.hid.com

Tabla 3.4 Descripción de la memoria 16K/16[17]

- 16 kilobits (2kBytes)
- 16 Application Areas, separated into 8 pages
- Read/Write Area is blocks 6 through 31, 208 bytes per page
- Barrier at Block 18 can be moved
- ISO 15693 & 14443 Mode
- Keys can be updated

Configuraciones y llaves de acceso

8 Bytes per block								Block
Card			Serial			Num.		0
Config							Block	1
Stored			Value			Area		2
Key 1								3
Key 2								4
App.			Issuer			Area		5

Figura. 3.16 Configuración de llaves.[18]

[17] www.hid.com
[18] www.hid.com

Seguridad y manejo de llaves

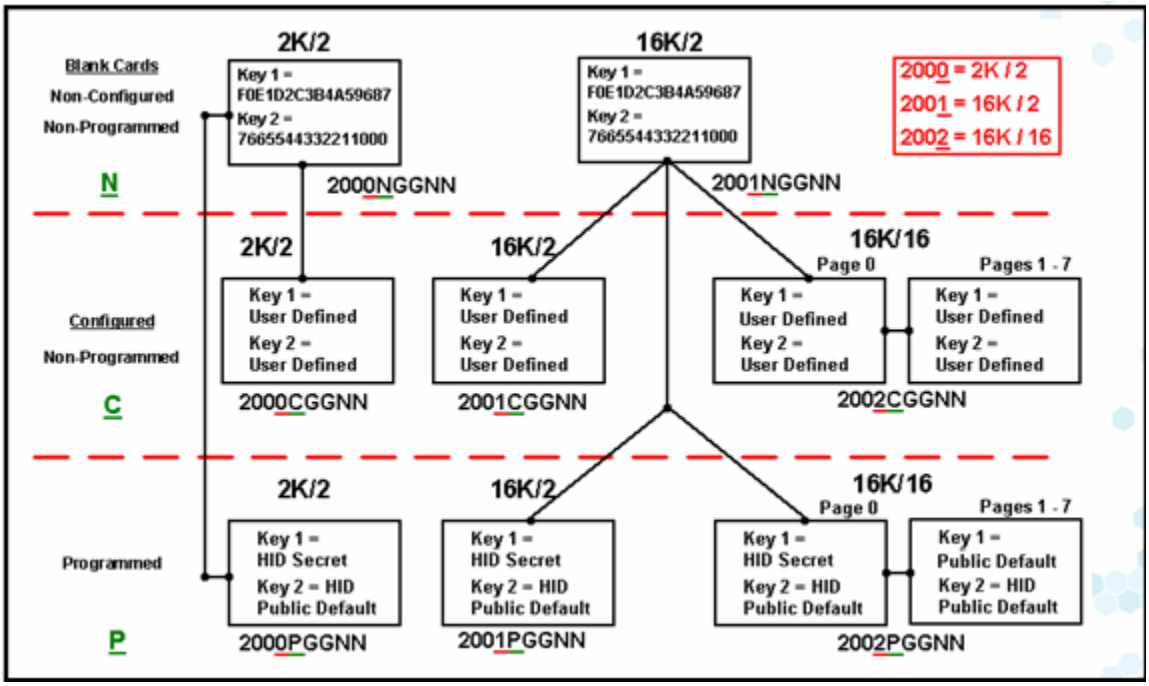


Figura. 3.17 Seguridad y manejo de llaves.[19]

La diferencia entre las tecnologías anteriores es que manejan diferentes estándares mifare 14443a e iclass 14443b, ya que el estándar 14443a establece que es de solo lectura (mifare) y 14443b2 es híbrida.

3.11 TECNOLOGIA NUEVA (OPCIONAL)[20]

La tecnología de opción siempre esta disponible para nuevos proyectos solo que es difícil competir contra las tecnologías ya existentes como son las ya mencionadas (MIFARE, ICLASS), pero para los lectores de esta tesis quiero comentar que existen otras opciones, los nuevos dispositivos con esta tecnología para el desarrollo de un proyecto enfocado con este fin están cada ves mas en el mercado, el cual apenas hace unos años se consideraba del

[19] www.hid.com
[20] www.microchips.com

futuro y que ahora esta siendo utilizado en el mercado internacional, aunque aun queda espacio para ser explotado.

Veremos un muy buen dispositivo que permitirá generar pequeños y grandes proyectos dependiendo de la aplicación que se desee realizar, el lector podrá realizar varios proyectos de interés. Ya que al igual que las tecnologías anteriores también permite que se adapte al estándar ISO 14443A/14443B aunque para lo que propongo aquí utilizaría el estándar ISO 14443B ya que el proyecto cumple con un dispositivo de solo lectura.

El dispositivo que se recomienda para el lector de este tesis es el MCRF 450, 451, 452, 455, que puede adaptarse bien al estándar que se requiere para estar dentro de la interoperabilidad que se maneja en este campo.

Las características de este dispositivo son:

- Lectura y escritura sin contacto con algoritmo de anticolisión.
- 1024 bits (32 blocks) de memoria total.
- 928 bits (29 blocks) de memoria para programar para usuario final.
- Único 32-bit tag ID (programado de fabrica).
- 32 bits para datos y 16 bits para el CRC por Bloque.
- Protección de escritura para el bloque.
- 70 kbit/s en lectura de datos (Manchester format).
- Bit especial (Fast Read) para una rápida identificación
- 1 de 16 PPM para codificar en datos de escritura.
- Interrogator-Talks-First (ITF) o Tag-Talks-First (TTF) operations.
- Alto rango de lectura y escritura.

- Algoritmo de anticolisión de alta velocidad para lectura y escritura.
- Estado de rápido y normal para la velocidad de escritura de datos.
- Transacciones de escritura segura.
- Operaciones asíncronas para consumo de baja energía y flexible para elegir frecuencias.
- Capacitor resonante interno (MCRF 451, 452, 455).
- Dos patillas para antena circuí tal externa (MCRF 452).
- Tres patillas para antena circuí tal externa (MCRF 450,451,450)
- Baja energía en el diseño de Cmos.
- Die in waffle pack, wafer, wafer on frame, bumped wafer, COB, PDIP or SOIC opciones de empaquetado.

Configuración típica para las aplicaciones.

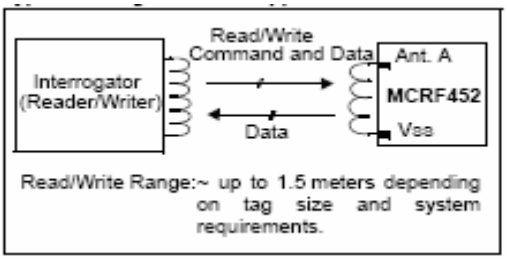


Figura. 3.18 Configuración típica de la aplicación.[21]

3.11.1Descripción de las características del dispositivo.

El integrado MCRF 45X, es un dispositivo diseñado para lectura/escritura RFID pasiva, que es optimo para la frecuencia de 13.56 MHz.

[21] www.microchips.com

Necesita un circuito LC resonante para la comunicación inalámbrica con el interrogador (lector de datos). Se energiza remotamente por la rectificación de la señal RF que es transmitida del interrogador que transmite o actualiza información dentro del contenido de la memoria mediante comandos transmitidos por el interrogador.

El dispositivo contiene 32 bloques de memoria EEPROM (B0-B31), cada bloque de memoria consiste de 32 bits, los primeros 3 bloques (B0-B2) están para la operación del propio dispositivo, mientras que los siguientes 29 bloques (B3-B31: 928 bits) están disponibles para los datos del usuario. El bloque 1 contiene una ID única como etiqueta de serie, esta ID es etiquetada en el momento de fabricación y esta protegida para escritura en modo inalámbrico, ya que se puede escribir en el siempre y cuando exista contacto directo.

Todos los bloques de datos son de acceso inalámbrico a excepción del bloque 0 que esta protegido contra escritura, sin embargo los bits 30 y 31 son de lectura y escritura para comandos de condición.

El dispositivo puede ser configurado como Tag-Talks-First (TTF) o Interrogator-Talks-First (ITF). En el modo TTF, el dispositivo transmite datos tan rápido como sea energizado y espera el siguiente comando. En modo ITF, el dispositivo espera un comando del interrogador antes de enviar datos. Los bits que tienen este control para TTF o ITF son los bits 30 y 31 del bloque 0.

Todos los comandos downlink del interrogador son codificados usando de 1 al 16 pulsos de posición por modulación y especialmente pulsos de bloque de tiempo (time gap pulses). Esta información codificada modula la amplitud de la señal RF del interrogador.

En la otra punta, el MCRF 450, 451, 452, 455, demodula la señal RF que recibe y envía los datos de la memoria a una velocidad de 70 kbit/s de nuevo al interrogador en formato Manchester.

La comunicación es asíncrona entre el dispositivo y el interrogador, por lo tanto para realzar que la detección de el dispositivo sea mas exacta, el interrogador envía una señal de referencia por tiempo al dispositivo (pulso de

tiempo calibrado) (TCP). El tiempo de la señal referencial es usado para calibrar el tiempo del decodificador interno.

Cuando un dispositivo de esta naturaleza (TAG), que en realidad es un dispositivo con un circuito resonante LC, es aproximado a un lector o interrogador de campo de Radio Frecuencia, este desarrolla un voltaje RF a través del circuito externo. El dispositivo rectifica el voltaje RF y desarrolla un voltaje (VDD). Entonces el dispositivo se mantiene activo mientras que el voltaje VDD esta en el nivel del voltaje.

El dispositivo entonces envía datos almacenado en la memoria al interrogador o lector de tarjeta, mediante el intercambio de apagado y encendido del transistor de modulación interno. Esta modulación interna del transistor esta localizada entre la antena B y VSS. La modulación del transistor tiene una pequeña resistencia de encendido entre el Drain (antena B) y la fuente (Vss) durante el tiempo de encendido.

Cuando la modulación del transistor es encendido, el componente del circuito resonante entre la antena B y Vss, el cual esta en paralelo con la modulación del transistor, esta es corta por la resistencia tan baja de encendido. Esto resulta en el cambio de valor del circuito LC. Como resultado de este circuito no por mucho tiempo se mantiene resonante ala frecuencia del interrogador. Por lo tanto el voltaje del circuito es minimizado, y a esto se le llama “Cloaking”.

Cuando el transistor de modulación es apagado el circuito resonante al momento de llevar la frecuencia al interrogador es cuando desarrolla su máximo voltaje esta condición se le llama “Uncloaking”. Por lo tanto, los datos que se envían del interrogador por medio del encendido (clocking) y apagado (Unclocking) al transistor de modulación.

El voltaje de la amplitud que se acarrea en una señal a través de un circuito resonante LC cambia dependiendo en la amplitud de modulación de los datos. A esto se le llama Señal de Amplitud Modulada. El canal que recibe en el

interrogador detecta esta señal de amplitud modulada y reconstruye la modulación de los datos para decodificarla.

El dispositivo incluye un único algoritmo de anticolisión para leer o escribir efectivamente en múltiples Tags del campo. Para minimizar la colisión de datos, el algoritmo utiliza un tiempo de división multiplexado de la respuesta del dispositivo. Cada dispositivo puede comunicarse con el interrogador en diferentes tiempos. Los dispositivos en el campo de radiofrecuencia del interrogador se mantienen en una condición de Non-Modulación sino se encuentran dentro de su tiempo de atención. Esto habilita al interrogador para comunicarse con múltiples dispositivos uno a la vez sin obtener coalición de datos.

Para permitir la integridad de datos en el momento de escritura, el dispositivo incluye una característica llamada anti-tearing. Esta característica permite la verificación de la integridad de los datos para los ciclos de escritos incompletos la cual es provocada en la falla de la comunicación entre el interrogador y el dispositivo durante una secuencia de escritura.

3.11.2 LA COMUNICACIÓN DE LOS DISPOSITIVOS CON EL INTERROGADOR

El dispositivo puede ser operado en dos diferentes modos ya sea Respuesta de Lectura Rápida (FRR) o Paso de lectura Rápido (FRB), dependiendo del estado del Bit 31 (FR: bit) del bloque 0. si el FR bit esta asignado, el dispositivo opera en el modo de FRR y FRB, y si el FR bit esta en blanco (cleared). El FR bit siempre es reprogramable y no esta protegido para escritura. El modo FRR es la configuración por de faul. La comunicación entre el interrogador y el Tag inicia con los comandos FRR o FRB.

En el modo de FRR el dispositivo envía la respuesta solo cuando recibe el comando FRR. Y Viceversa en el modo FRB, que envía respuesta cuando recibe el comando FRB.

Si el dispositivo esta en modo FRR y también en el modo TTF (TF bit = set), en este caso el dispositivo puede enviar la respuesta en cuanto es energizado.

Uno de los principales propósitos de utilizar dos diferentes modos (FRR y FRB) es para utilizar el dispositivo efectivamente en un nivel de aplicación supply-chain, donde una identificación rápida y efectiva de anticolisión es necesaria para el proceso de lectura/escritura. Esto puede realizarse mediante el chequeo del FR bit o mediante el chequeo de la respuesta del Tag hacia el comando. Por esta razón el FR bit es también llamado electronic Article Surveillance (EAS) bit.

3.11.3.1 EL TAG EN MODO DE OPERACIÓN FRR

Si el dispositivo esta en el modo FRR (FR bit= set), la comunicación entre el interrogador y el dispositivo puede iniciar de dos formas dependiendo del estado TF (bit 30 del bloque 0). Si el TF bit está en blanco (cleared), se le llama modo ITF. En este caso el Tag espera el comando FRR del interrogador y envía la respuesta de datos cuando ve el comando FRR. Si el TF bit =set, el dispositivo esta en modo TTF. En este caso el Tag envía la respuesta FRR en cuanto es energizada aun sin el comando FRR. El tag tiene un tiempo de espera corto (1ms) inmediatamente después de la respuesta FRR. El interrogador envía su próximo comando durante este tiempo de espera del Tag.

La respuesta FRR incluye 32 bits de la identificación del Tag y FRF (bloques 3-5). El interrogador identifica que Tags están en el campo de Frecuencia al obtener respuestas FRR.

Basándose en la respuesta FRR, el interrogador envía un matching code 1 (MC1) o un matching code 2 (MC2), durante el tiempo de espera del Tag. El interrogador envía el MC1 para poner al Tag en modo sleep. Los Tags en el

modo sleep nunca responden a ningún comando. La única forma de despertarlo es removiendo la energía de radiofrecuencia transmitida por el interrogador.

Si el Tag necesita prolongar el proceso de lectura o escritura el interrogador envía el MC2 seguido del comando de lectura/escritura. Una vez completada la escritura/lectura de un bloque de datos el interrogador envía un comando de fin (end command) para poner al Tag en modo sleep.

La lectura/escritura de un dispositivo FFR toma lugar en un modo de anticolisión. Por unos instantes si hay múltiples Tags en el campo de Radio Frecuencia, el interrogador selecciona solamente un Tag a la vez para el control de los time slot en la respuesta FRR. El interrogador repite esta frecuencia hasta que todos los Tags dentro del campo de RF son procesados.

PROCESO DE ESTA OPERACIÓN:

- Envía comando FRR
- Recibe respuesta FRR
- Envía MC1 o MC2
- En el modo de espera del Tag (Listening Window)
- Envía comando de lectura del bloque o envía de escritura del bloque y datos
- Verifica la respuesta de lectura/escritura
- Envía el comando de fin (end command)
- Verifica el comando de respuesta de fin
- Busca si existen más Tags con respuesta FRR

3.11.3.2 TAG EN MODO DE OPERACIÓN FRB

La comunicación con el dispositivo en el modo FRB se inicia con el comando FRB solamente. Si el dispositivo ve el comando FRB en el interrogador envía sus 32 bits de identificación y espera el MC2. Esto es seguido del comando de lectura/escritura, una vez que el dispositivo es leído o escrito el interrogador envía un comando de fin.

A diferencia del modo FRR, la lectura o escritura del Tag es procesada en un modo de no anticolisión.

CAPITULO IV

RADIO FRECUENCIA

4.1 ¿QUÉ ES RFID?

RFID es el acrónimo de **Radio Frequency Identification**, que viene a ser en la lengua de Cervantes, **Identificación por Radiofrecuencia**. Bueno, pues se trata de una tecnología basada en la utilización de un **pequeño chip** adherido a un producto, y a través del cual es posible mantener un rastreo de su localización. La distancia de rastreo varía mucho, dependiendo del tamaño, tipo y antena del chip, pero podría ser desde 2cm. a 13 metros en los sencillos, hasta incluso varios kilómetros en los más complejos. Son realmente pequeños y tal y como van los avances, en poco tiempo podrían ser considerados virtualmente invisibles.

A la combinación de chip y antena se la conoce como etiqueta RFID. Pues bien, la idea es que cada producto lleve una etiqueta que tendrá un número identificativo único (a diferencia del código de barras que es el mismo para todos los productos iguales), pudiendo asociarlo perfectamente al comprado. Vaya donde vaya esa persona, ese producto podrá identificarlo unívocamente. A primera vista pueden saltar a la mente cientos de aplicaciones comerciales e industriales, por ejemplo:

- Dentro de un almacén industrial, mediante tecnología RFID sería posible mantener un control exhaustivo del inventario de los productos, su localización, cantidad y demás variables que mejorarían los procesos industriales y de producción.
- En una tienda sería posible encontrar los productos que no están correctamente colocados o el zapato que ha perdido su otro par.

Pero también saltan a la vista aplicaciones que están dado que hablar mucho en USA y que han llevado a la creación de diversas plataformas en contra de la tecnología RFID o al menos pidiendo una legislación y unas normas de conducta para las empresas que actualmente no existe. La privacidad de los compradores está en entredicho. Por ejemplo:

- A largo plazo, cualquiera que tuviera un lector de chips RFID podría saber los aparatos electrodomésticos ó ropa, que tenemos en casa sin necesidad de entrar.
- Un chip RFID en nuestro móvil, reloj o cartera podría permitir saber si hemos estado en un determinado establecimiento.

Puede parecer algo exagerado, pero esta es la razón por la que distintas plataformas como StopRFID alertan sobre la inexistencia de una legislación que permita la implantación de esta tecnología de una manera segura.

4.2 HISTORIA

Se ha sugerido que el primer dispositivo conocido pudo haber sido una herramienta de espionaje inventada por Léon Theremin para el gobierno ruso en 1945. Éste no es el caso. El dispositivo de Theremin era un dispositivo de escucha secreto pasivo, no una etiqueta de identificación. La tecnología usada en RFID ha existido desde comienzos de los años 1920, según una fuente (aunque la misma fuente establece que los sistemas RFID han existido desde finales de los años 1960).

Una tecnología similar, el transpondedor de IFF, fue inventada por los británicos en 1939, y fue utilizada de forma rutinaria por los aliados en la Segunda Guerra Mundial para identificar los aeroplanos como amigos o enemigos. Otro trabajo temprano que trata el RFID es el artículo de 1948 de Harry Stockman, titulado "Comunicación por medio de la energía reflejada" (Actas del IRE, pp1196-1204, octubre de 1948). Stockman predijo que "... el trabajo considerable de investigación y de desarrollo tiene que ser realizado antes de que los problemas básicos restantes en la comunicación de la energía reflejada se solucionen, y antes de que el campo de aplicaciones útiles se explore." Hicieron falta treinta años de avances en multitud de campos diversos antes de que RFID se convirtiera en una realidad.

4.3 TIPOS DE ETIQUETAS DE RFID.

Las etiquetas RFID pueden ser activas, semi-pasivas (o semi-activas) o pasivas. Las etiquetas RFID pasivas no tienen fuente de alimentación propia. La mínima corriente eléctrica inducida en la antena por la señal de escaneo de radiofrecuencia proporciona suficiente energía al circuito integrado CMOS de la etiqueta para poder transmitir una respuesta. Debido a las preocupaciones por la energía y el coste, la respuesta de una etiqueta pasiva RFID es necesariamente breve, normalmente apenas un número de identificación (GUID). La falta de una fuente de alimentación propia hace que el dispositivo pueda ser bastante pequeño: existen productos disponibles de forma comercial que pueden ser insertados bajo la piel. Las etiquetas pasivas, en la práctica tienen distancias de lectura que varían entre unos 10 milímetros hasta cerca de 6 metros dependiendo del tamaño de la antena del Tag y de la potencia y frecuencia en la que opera el lector. Estando en 2005, el dispositivo disponible comercialmente más pequeño de este tipo medía 0.4 milímetros × 0.4 milímetros, y más fino que una hoja de papel; estos dispositivos son prácticamente invisibles.

Las etiquetas RFID semi-pasivas son muy similares a las pasivas, salvo que incorporan además una pequeña batería. Esta batería permite al circuito integrado de la etiqueta estar constantemente alimentado. Además, elimina la necesidad de diseñar una antena para recoger potencia de una señal entrante. Por ello, las antenas pueden ser optimizadas para la señal de backscattering. Las etiquetas RFID semi-pasivas responden más rápidamente, por lo que son más fuertes en el ratio de lectura comparadas con las etiquetas pasivas.

Las etiquetas RFID activas, por otra parte, deben tener una fuente de energía, y pueden tener rangos mayores y memorias más grandes que las etiquetas pasivas, así como la capacidad de poder almacenar información adicional enviada por el transmisor-receptor. Actualmente, las etiquetas activas más pequeñas tienen un tamaño aproximado de una moneda. Muchas etiquetas

activas tienen rangos prácticos de diez metros, y una duración de batería de hasta varios años.

Como las etiquetas pasivas son mucho más baratas de fabricar y no necesitan batería, la gran mayoría de las etiquetas RFID existentes son del tipo pasivo. En fecha de 2004, las etiquetas tienen un precio desde 0,40$, en grandes pedidos. El marcado de RFID universal de productos individuales será comercialmente viable con volúmenes muy grandes de 10.000 millones de unidades al año, llevando el coste de producción a menos de 0,05$ según un fabricante. La demanda actual de chips de circuitos integrados con RFID no está cerca de soportar ese costo. Los analistas de las compañías independientes de investigación como Gartner and Forrester Research convienen en que un nivel de precio de menos de $0.10 (con un volumen de producción de 1.000 millones de unidades) sólo se puede lograr en unos 6 u 8 años, lo que limita los planes a corto plazo para una adopción extensa de las etiquetas RFID pasivas. Otros analistas creen que esos precios serían alcanzables dentro de 10-15 años.

A pesar de las ventajas en cuanto al costo de las etiquetas pasivas con respecto a las activas son significativas, otros factores incluyendo exactitud, funcionamiento en ciertos ambientes como cerca del agua o metal, y confiabilidad hacen que el uso de etiquetas activas sea muy común hoy en día.

Hay cuatro clases distintas de etiquetas en uso. Son categorizadas según su radiofrecuencia: las etiquetas de frecuencia baja (entre 125 ó 134,2 kilohertz), las etiquetas de alta frecuencia (13,56 megahertz), las etiquetas UHF o frecuencia ultra elevada (868 a 956 megahertz), y las etiquetas de microondas (2,45 gigahertz). Las etiquetas UHF no pueden ser utilizadas de forma global porque no existen regulaciones globales para su uso.

Hay algunos dispositivos transpondedores y tarjetas de chip sin contacto que ofrecen una función similar.

4.4 EL SISTEMA RFID

Un sistema de RFID puede estar formado por varios componentes:

Etiquetas, lectores de etiquetas, estaciones de programación de etiquetas, lectores de circulación, equipamiento de ordenación, y wands de inventario de etiquetas. La seguridad se puede manejar de dos formas. Los puertos de seguridad pueden preguntar el ILS para determinar su estado de seguridad o la etiqueta puede contener un bit de seguridad que se pondría a nivel alto y bajo por circulación o por las estaciones de lector de auto-comprobación. El propósito de un sistema RFID es permitir que se puedan transmitir datos mediante un dispositivo portátil, llamado etiqueta, que es leída por un lector RFID y procesada según las necesidades de una aplicación determinada. Los datos transmitidos por la etiqueta pueden proporcionar información sobre la identificación o localización, o específicos sobre el producto marcado con la etiqueta, como por ejemplo precio, color, fecha de compra, etc. El uso de RFID para aplicaciones de acceso y de seguimiento, apareció por primera vez durante los años 1980. Pronto RFID destacó debido a su capacidad de seguir objetos móviles.

4.5 USO ACTUAL

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, seguimiento de artículos de ropa y ahora último en pacientes de centros hospitalarios para hacer un seguimiento de su historia clínica. Un uso extendido

de las etiquetas de alta frecuencia como identificación de acreditaciones, 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. Una etiqueta RFID empleada para la recaudación con peaje electrónico. 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, el telé peaje TAG en las autopistas urbanas en Santiago de Chile 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 cobrar el peaje en una cuenta periódica o descontarla de una cuenta prepago. El sistema ayuda a disminuir el tráfico causado por las cabinas de peaje. 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. Los internos tienen unos transmisores del tamaño de un reloj de muñeca que pueden 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.[1]

4.6 ASPECTOS FISICOS DE LA TECNOLOGIA RFID

Hoy en día la mayoría de la gente ha oído hablar de la tecnología RFID y el estándar EPC. Muchos de ellos no sólo han oído hablar sino que ya saben los principios básicos de la tecnología como por ejemplo como funciona y que elementos conforman un sistema RFID. Y por si fuera poco aún hay más gente que no conoce la tecnología pero ha escuchado que será el sustituto del código de barras o que será imprescindible en el mundo de las empresas.

Todo este rápido conocimiento y expansión de referencias es muy atractiva y bonito, pero como en toda tecnología hay que frenar y mirar la situación actual y no centrarse o solo hablar de lo que será idealmente en el 2015. La tecnología tiene un enorme potencial, pero como toda comunicación por radiofrecuencia (ondas electromagnéticas) tiene aspectos físicos detrás que hay que entender. Sólo así podremos saber porque los sistemas funcionan, cuando porque no, la razón por la cual no es adecuado o las modificaciones que podríamos hacer para mejorar el rendimiento.

[1] www.wikipedia.com

Como ya han podido comprobar las primeras empresas que han empezado a adoptar la tecnología RFID/EPC, no es tan fácil como comprar e instalar, sino que detrás de cualquier proyecto debe haber estudios detallados y correctos de varias condiciones, entre ellas, los aspectos que pueden interferir en nuestro sistema RF que solo entenderemos si somos capaces de entender porque suceden, y sólo hay un camino para eso, y es entender los aspectos físicos de RF.

4.7 CONCEPTOS PREVIOS

En la radiación electromagnética, la propagación de la energía se realiza en forma de onda.

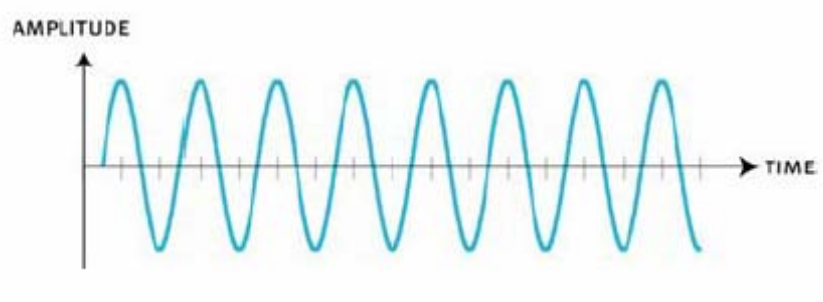


Figura 4.1, amplitud de onda.[2]

Su naturaleza puede ser alterada en frecuencia y amplitud.

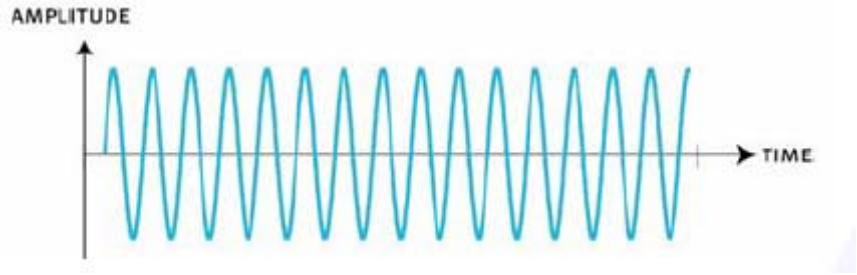


Figura 4.2. Frecuencia y amplitud.[3]

[2] www.ChipDesignMagazine.htm
[3] www.ChipDesignMagazine.htm

La potencia se calcula en Watts, pero hay diferentes maneras de medir y mostrar esta unidad de medida. La frecuencia, número de ciclos completos que hace la señal por segundo, se mide en Hertz o su longitud de onda (wavelength), distancia transcurrida en volver la señal a la misma posición (medido en metros).

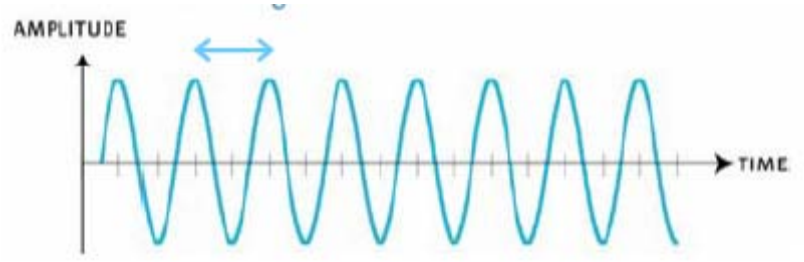
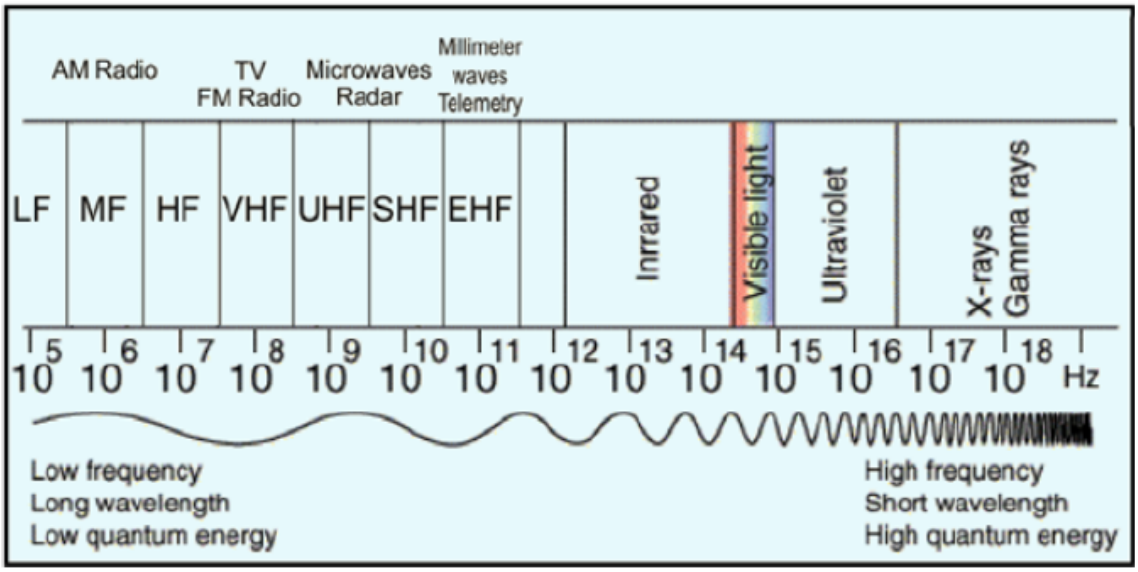


Figura 4.3. Longitud de onda[4]

Las frecuencias están agrupadas en bandas de frecuencias que contienen características similares. Además a medida que incrementados o disminuimos la frecuencia seguimos una relación respecto a la longitud de onda y la energía.

Tabla 4.1. Espectro de la frecuencia.[5]



[4] www.ChipDesignMagazine.htm
[5] www.ChipDesignMagazine.htm

A continuación se muestran los valores de frecuencia y longitudes de onda de las primeras bandas frecuenciales de la tabla 4.1, donde se encuentran las utilizadas por la tecnología RFID. La tabla 4.2, en la primera fila se especifica las siglas y su nombre, en la segunda las frecuencias que engloban la banda y como último el umbral de tamaños de la longitud de onda.

Tabla 4.2. Valores de frecuencia y longitud.[6]

LF low frequency	MF medium frequency	HF high frequency	VHF very high frequency	UHF ultra high frequency	SHF super high frequency
30–300kHz	300kHz–3MHz	3–30MHz	30–300MHz	300MHz–3GHz	3–30GHz
10–1km	1000–100m	100–10m	10m–1m	1m–0.1m	0.1–0.01m

La comunicación vía radiofrecuencia, la utilizada en RFID consiste entre un transmisor y un emisor. Tanto el transmisor como el receptor deben tener incorporada o conectada una antena.

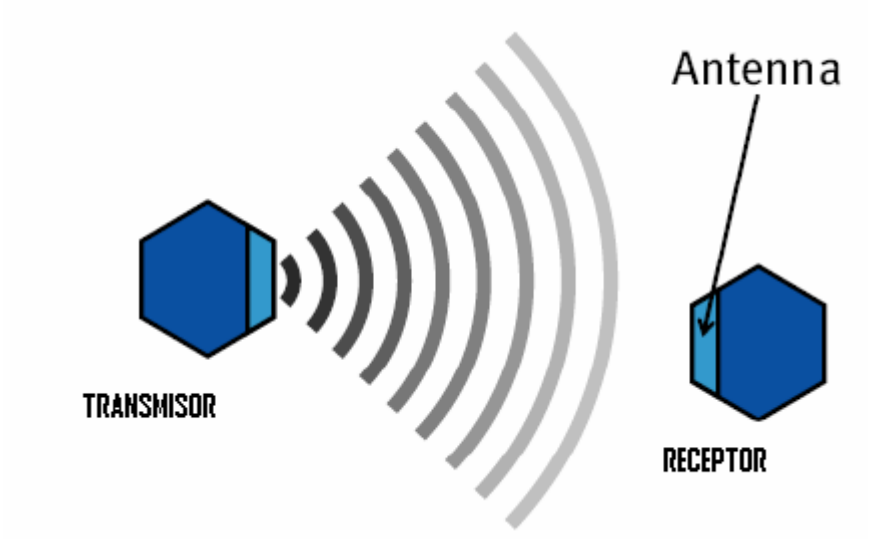


Figura 4.4t Transmisor y receptor RF[7]

[6] www.ChipDesignMagazine.htm
[7] www.ChipDesignMagazine.htm

En la comunicación vía radio se transmite información y energía. A veces hay repetidores entre los dos dispositivos con el objetivo de incrementar su cobertura. Para enviar datos mediante una comunicación radio se debe realizar mediante una modulación, que no es más que el método como se envían. Esta modulación depende la interfaz aérea, es decir, las normas y lenguajes que deben seguir tanto el lector como el receptor para hablarse y entenderse. Podríamos hacer el símil de los antiguos mensajes mediante luz que utilizaban para comunicarse los barcos, la luz o el tipo de luz sería la modulación, mientras que los intervalos de esa luz y su orden serían la interfaz aérea, todo con un único objetivo hablarse entre ellos. Hay dos tipos de mecanismos para las comunicaciones electromagnéticas (EM). Se tiene que pensar en electromagnéticas y en magnéticas, dependiendo de la distancia de la comunicación y de la frecuencia utilizada.

4.8 TIPOS DE COMUNICACIONES

Hay dos tipos de mecanismos para las comunicaciones electromagnéticas (EM), es decir vía radio. Se tiene que pensar en electromagnéticas y en magnéticas, dependiendo de la distancia de la comunicación y de la frecuencia utilizada.

.

- Far-Field (Campo lejano): esta basado en los campos electromagnéticos. En
  comunicaciones de largas distancias o altas frecuencias como el caso de la UHF. Es sensible al entorno como los elementos líquidos o metálicos.

- . Near-Field (Campo próximo): esta basado en los campos magnéticos. En comunicaciones de cortas distancias y bajas frecuencias como el caso de la HF.

4.9 FACTOR ANTENA

La antena del tag es crítica en las operaciones de las comunicaciones e igual de importante tanto en la recepción como en la emisión de las señales de información. Su forma y tamaño varia según estamos en campo lejano (UHF) o próximo (LF y HF), pero es en el lejano (farfield) donde el tamaño de la antena es importante, debido a la obligación de que su tamaño sea la mitad de la longitud de onda.

Por ejemplo, la frecuencia 915 MHz, tiene una longitud de onda de 33 cm. Obteniendo un tamaño de antena de 16-17 cm. En el caso de 868 MHz es de 34 cm. resultando una antena de 17 cm.

Para calcular la longitud de onda de la frecuencia determinada es:
Longitud de onda (λ)= velocidad de la luz (m/s) / frecuencia (Hz)

Figura 4.5. Longitud de antena.[8]

Las antenas tienen patrones de radiación, es decir, por donde y con que potencia envían la señal. Esta característica es muy importante para visualizar o calcular la cobertura que tenemos (zonas que podemos leer). Normalmente pueden ser antenas directivas, que envían y reciben la señal a una zona

[8] www.ChipDesignMagazine.htm

determinada, u omnidireccionales, que lo hacen de igual forma en todas las direcciones. Antena omnidireccional Antena directiva.

Hay una gran complejidad teórica para calcular estos patrones de radiación, pero los efectos prácticos que nos encontramos son zonas de vacío de señal y zonas de lectura.

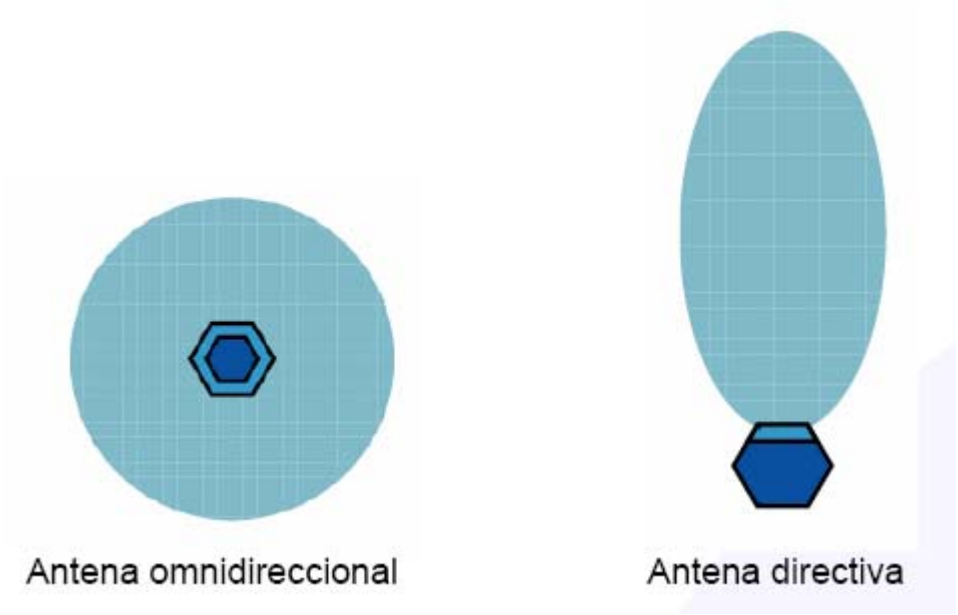


Figura 4.6, tipos de antenas.[9]

Hay una gran complejidad teórica para calcular estos patrones de radiación, pero los efectos prácticos que nos encontramos son zonas de vacío de señal y zonas de lectura.

En los dos casos vemos que obtenemos zonas oscuras (no cobertura), pero en el caso de disponer de más de una antena en comunicaciones de largas distancias solapamos sus coberturas individuales para incrementar nuestra capacidad.

Los lectores pueden tener conectadas más de una antena para incrementar la cobertura. En estos casos el lector debe tener un multiplexador para conmutar entre las distintas antenas, solo una puede ser utilizada al mismo tiempo.

[9] www.ChipDesignMagazine.htm

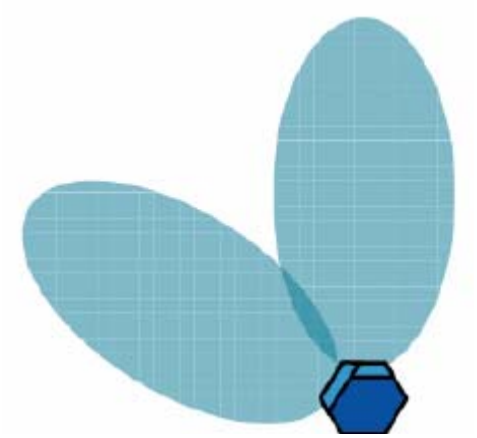


Figura 4.7. Ejemplo de incremento de la cobertura mediante un lector con dos antenas[10]

También pueden tener las antenas situadas frente a frente para incrementar la cobertura y eliminar posibles zonas oscuras que reducen la fiabilidad. Este caso necesita un alineamiento de las antenas muy afinado.

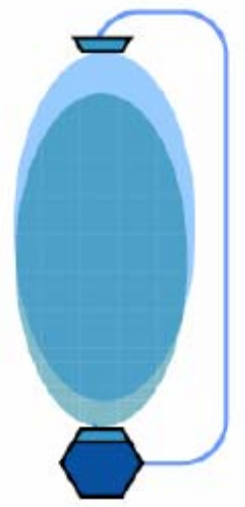


Figura 4.7, Antenas conectadas a un lector para incrementar la fiabilidad[11]

[10] www.ChipDesignMagazine.htm
[11] www.ChipDesignMagazine.htm

4.10 LA POLARIZACION

Hay dos tipos de polarización en antenas para campo lejano: la lineal o circular.

Figura 4.8. Polarización lineal y circular.[12]

La polarización lineal:

- La energía es radiada de forma fija en dirección lineal
- Se obtienen los mayores rangos
- Tendencia a genera un haz de señal delgada o muy estrecha
- Requiere de un preciso alineamiento entre las antenas de emisión y recepción (Depende de la orientación)
- Mejor comportamiento en entornos controlados

En la polarización circular:

- Alineamiento de las antenas menos crítico
- Mejor comportamiento en presencia de múltiples caminos de señal o muy dispersas
- Rango reducido
- Tendencia a generar haz de señal muy ancha
- La energía rota de manera circular
- Independencia de la orientación (buena para etiquetar sin tener una orientación definida en entornos no controlados)

[12] www.ChipDesignMagazine.htm

4.11 EFECTOS EN LA COMUNICACIÓN RFID

Hay que considerar diferentes parámetros que impactan en el comportamiento del tag y sus respuestas según la frecuencia utilizada. A continuación se muestran los cuatro efectos principales que ciertos materiales provocan sobre las señales de radio frecuencia, y por tanto, sobre el comportamiento del tag.

Absorción: algunos materiales absorben la energía de la propagación de ondas radio. Esta situación es también conocida como pérdidas (loss), en términos de RFID, provoca que haya menos potencia disponible para que el tag pueda devolver la señal.

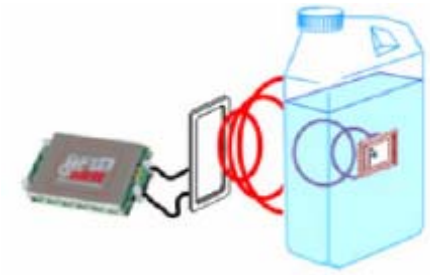


Figura 4.8. Comunicación RFID, (absorción)[13]

Reflexión o refracción: Idealmente, los tags reciben una onda directa desde el lector, pero la mayoría de veces, los materiales del entorno del tag pueden reflejar o refractar esta onda principal. Entonces la etiqueta o tag recibe la onda principal conjuntamente con las reflejadas o refractadas, que son totalmente diferentes a la onda original.

[13] www.ChipDesignMagazine.htm

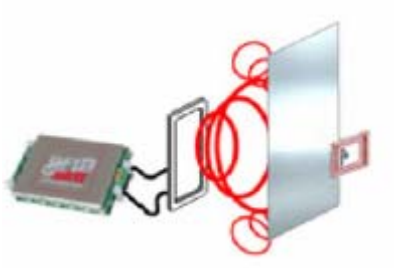


Figura 4.9. Onda de refracción.[14]

Efectos dieléctricos: cuando un material dieléctrico esta cerca de la etiqueta, la concentración de campo eléctrico se puede multiplicar, provocando un efecto de desintonización de la antena del tag.

Efectos de propagaciones complejas: estos efectos existen porqué dos fenómenos físicos suceden cuando trabajamos con sistemas RFID para interferir a la comunicación correcta.

Estos fenómenos son:

- Ondas estacionarias u ondas diferentes a la directa que quiere alcanzar la etiqueta o tag. Ondas rebotadas en la misma dirección y diferente sentido que provocan que las ondas se sumen y creen una onda con más energía o sin ella, según el punto de medición.
- Múltiples caminos que son causados por las ondas estacionarias y pueden cancelar la onda directa en conjunto (interferencia destructiva).

Los objetos pueden exhibir un amplio rango de comportamiento en relación a la radio frecuencia que depende de la composición de los materiales. Un objeto puede ser transparente, absorbente o reflejante a la radio frecuencia (RF). La mayoría de los objetos exhiben una combinación de los tres, debido a los materiales usados para su fabricación. Por ejemplo es normal que cualquier artículo que compremos hoy en día pueda tener una parte metálica, otra plástica

[14] www.ChipDesignMagazine.htm

y una líquida. A continuación examinamos el comportamiento de los dos materiales más comunes:

Metálico: los objetos metálicos provocan reflexión. El tag no puede absorber la suficiente energía, que proviene del lector, porqué el material metálico desintoniza la antena del tag, modificando su frecuencia de resonancia. Estos objetos son difíciles de etiquetar, pero existen etiquetas situadas directamente en el metal que pueden trabajar si tiene una muy buena y especial sintonización. Es posible utilizar objetos metálicos como limitadores de RF o como parte de la antena.

Líquido: los materiales líquidos como el agua, el jabón, soluciones salinas o medicamentos provocan absorción en RF. Estos absorben las ondas radio y reducen la energía que el tag necesita. El resultado es una reducción de la fuerza de la señal original debido a la absorción o disipación de la energía, que provocan que al tag no le llegue energía, o no la suficiente, para poder enviar la información que contiene al lector. Hay que tener en cuenta que el lector puede emitir mayor energía que el tag, por lo que a veces el lector si que alcanzará el tag pero este no podrá alcanzar el lector. El tag depende de la energía que absorba de la señal enviada por el lector. También dejar claro, que no todos los líquidos se comportan igual, por ejemplo el agua tiene un comportamiento muy distinto al del aceite.

4.12 LA PIRAMIDE RF

Como en la vida real la mayoría de productos son combinaciones de estos materiales se ha creado una pirámide RF que permite representar las propiedades de cada uno de ellos. Esta pirámide es muy útil para determinar como deberemos etiquetar los objetos, y seguramente donde. Por ejemplo, una caja con bolsas plásticas de aire la podríamos clasificar arriba de la pirámide,

donde es fácil etiquetar y leer. El pico de la pirámide representa un material 100 transparente que significa que es similar a leerlo al aire libre.

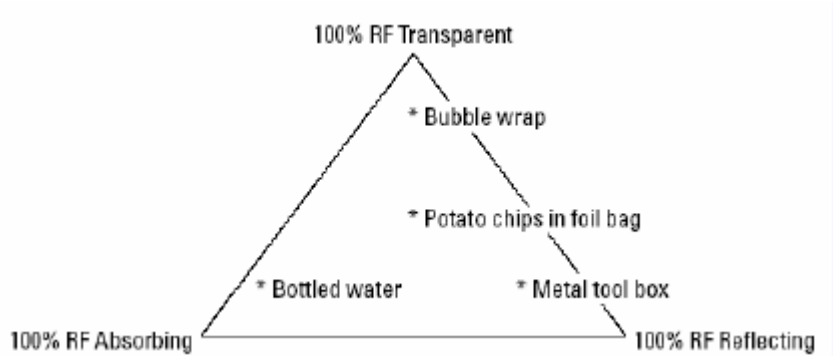


Figura 4.10, pirámide RF.[15]

La visualización de la pirámide ayuda a determinar la optima o posibles localizaciones del tag en las pruebas pilotos, aunque todo debe ser confirmado por un test.

4.13 TESTEAR LA SITUACION DE LOS TAGS.

Para superar estos efectos las antenas de los tags pueden ser diseñadas para trabajar en entornos especiales (metales, líquidos, etc.). Para determinar el mejor punto de test, hay que seguir los siguientes pasos:

Determinar si el embalaje es de material transparente para la RF: si este es cartón, no hay ningún problema, es transparente, pero si el embalaje contiene material metálico, este será opaco. Necesitaremos utilizar un embalaje lo más transparente posible para obtener mayor éxito de lecturas, o tendremos que utilizar tags especialmente diseñados para adherirse al metal (normalmente llevan entre la etiqueta y la superficie un material especial que crea una separación).

[15] www.ChipDesignMagazine.htm

Figura 4.11. Tag para metal de Schreiner LogiData[16]

Si el embalaje es transparente a RF, hay que observar e inspeccionar visualmente que contiene: nos podemos encontrar con una mezcla de materiales que provocan reflexión y absorben las ondas RF. Por ejemplo, si abrimos un desodorante la etiqueta esta pegada alrededor de la botella del spray, fabricado con material basado en óxido líquido de aluminio. El difusor es de plástico y normalmente tiene una tapa de protección también de plástico. Determinar donde se ajusta el contenido a la pirámide RF: en el ejemplo del desodorante, la zona actual de etiquetaje podría estar situada cerca de la punta derecha de la pirámide (100% reflexión), pero su contenido en líquido y aluminio la situaría en el medio inferior entre los dos picos de reflexión y absorción. Analizar y escoger diferentes zonas de posible etiquetaje: con el conocimiento de que materiales constituyen el objeto, y basándonos en la pirámide RF, deberemos escoger unas 8 o 10 zonas donde etiquetar, así podremos analizarlas en un test. Empezar a testear: La realización del test se hará primero con las zonas más amigables a la RF (transparentes) e iremos hacia las zonas de mayor dificultad. Así, por ejemplo, en el caso de los desodorantes, iniciaremos el test etiquetando el tapón de plástico.

[16] www.ChipDesignMagazine.htm

Conclusiones.

Las conclusiones son claras:

- Hay limitaciones prácticas serias e importantes en el rango de lectura de la tecnología RFID pasiva en UHF (interferencias) y HF (cortas distancias).
- Las señales UHF RFID pueden ser fácilmente interferidas por materiales muy comunes (aluminio, el propio cuerpo humano, las bebidas, etc.)
- Mejoras en el diseño de circuito integrado o chip (IC) ayudan mucho a nivel comercial, pero no a incrementar el rango de lectura.

Pero también hay que destacar que la tecnología esta avanzando mucho, aunque como todos sabemos lo que hablamos aquí son de limitaciones físicas que están sujetas a unas leyes, que por mucho que queramos no podemos cambiar. Esto abre el debate de si vamos a una frecuencia para todo o una frecuencia para cada caso o según aplicación. Todos los temas desarrollados en la guía no pretenden desanimar a las empresas a implementar RFID, sino son informar y dejar claro que su correcto funcionamiento requiere de especialistas y de un buen desarrollo del proyecto, tomando en consideración todos los puntos descritos.[17]

[17] www.ChipDesignMagazine.htm

4.14 SISTEMA DE RF GENERICO

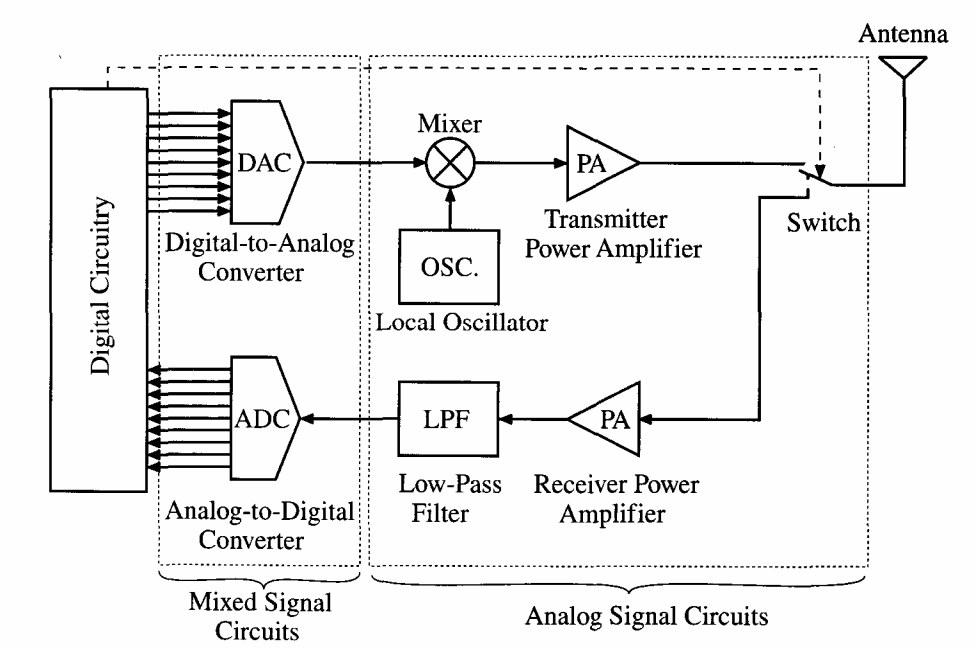


Figura 4.12. Sistema genérico de radio frecuencia.[18]

De la figura 4.12, se puede decir que es una típica configuración de un celular o una red inalámbrica, esta puede ser conocida como un receptor o transmisor dependiendo del switch en la entrada con la antena. Se tiene un amplificador de potencia para recobrar la señal que puede traer algunas perdidas en la entrada para esto la señal pasa por el amplificador PA y ahora se pasa por un filtro pasa bajas LPF pero ahora mejorada por el PA, se le hace la conversión a digital por medio de un circuito DAC (convertidor analógico/digital), para ser procesada por el circuito digital, y ahora para regresar ya sea un respuesta o bien enviar algún dato se hace lo contrario. Mediante el DAC la señal de baja frecuencia se convierte en analógica y se mezcla con una señal de alta frecuencia que provee el oscilador, y ahora la señal mezclada es amplificada nuevamente por otro PA, y direccionada a la antena que se encargara de radiar la información codificada como ondas magnéticas en el espacio.

[18] Reinhold Ludwig, Pavel Bretchko, RF Circuir Design Theory and Applications , Editorial PRENTICE HALL, 2000, p.p.3

Para esto se deben contemplar muchos parámetros en el diseño de todo el sistema de RF ya que dependiendo de la frecuencia, anchos de banda entre muchos otros. Esto con respecto a los amplificadores, filtros, tipo de antena y tiempo, ya que de esto dependerá si el circuito esta o no dentro del rango de la frecuencia que se quiere, así como los datos. [19]

[19] Reinhold Ludwig, Pavel Bretchko, RF Circuir Design Theory and Applications , Editorial PRENTICE HALL, 2000, p.p.3,4.

CAPITULO 5

SIMULACIÓN DE EL DISPOSITIVO MCRF 452 APLICADO EN LA TARJETA COMO EL RECEPTOR DE LA TARJETA EN VHDL

5.1 INTRODUCCION DE VHDL

Programación VHDL, primero que todo quiero dar una introducción de lo que es el lenguaje VHDL ya que esta tesis tiene el objetivo de simular la comunicación de una tarjeta con un receptor mediante el lenguaje VHDL utilizando Modelsim (herramienta de diseño), de hecho el programa propuesto para la simulación, puede ser el utilizado para programar algun fpga y utilizarlo como receptor, o incluso como el chip de la tarjeta. veamos.

Sus siglas están dadas por:

VHSINC: Very High Speed Integrated Circuits.
Hardware.
Descripción.
Lenguaje.

5.2 Primero que todo que son los HDL?

- Son una forma de notación para describir la estructura y el comportamiento de un circuito.
- HDL's: lenguaje de descripción del hardware, (Abel HDL, Verilog HDL, AHDL, entre otros),
- VHDL: es un estándar que no depende de ninguna compañía.

5.3 Porque usar VHDL?

- Es un estándar a nivel mundial.
- Puede describir el diseño con alto nivel de abstracción.
- La descripción no depende del tipo de la implementación.
- Capacidad de comprobación de tecnologías y diseños.

- Tiempo de desarrollo rápido y bajo costo.
- Migración a ASIC.[1]

Portabilidad.

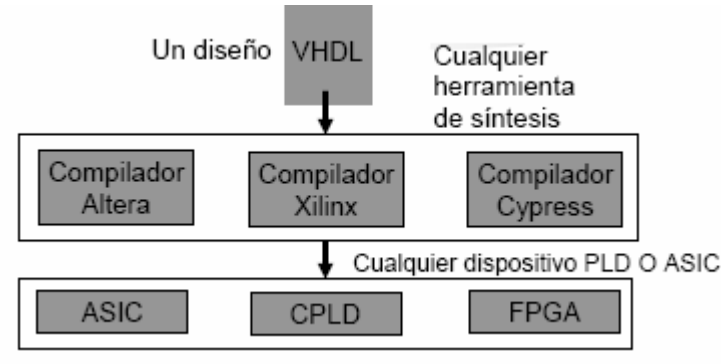


Figura 5.1. Descripción de la portabilidad.[2]

Aplicaciones y limitaciones:

- Cubre el ciclo de diseño electrónico:
    1. Especificación y modelado.
    2. Simulación.
    3. Implementación del hardware: ASIC, PLD, FPGA.
- No sirve para describir circuitos analógicos.
- No todo es código se puede sintetizar.
- Lenguaje extenso y complejo.

5.4 Historia VHDL

Solicitado por el departamento de la defensa de USA, para documentación de los diseños de 1980(para la ADA). Desarrollado por Intermetrics, IBM, TEXAS Instruments, (1983-1985) VHDL, ver. 7.2.

[1] Douglas J Smith, HDL Chip Design, Editorial Doone Publications, Madison, AL, USA, 1996, p.p.3
[2] Douglas J Smith, HDL Chip Design, Editorial Doone Publications, Madison, AL, USA, 1996.

En 1986, le trasfieren los derechos a la IEEE y se publica en 1987 como estándar , 1076-1987. Se revisa nuevamente en 1993 y se publica en 1994, como 1076-1993.

En 1984, Gateway design Automation, presenta Verilog HDL. Cadence Design Systems adquiere Gateway en 1988, y produce herramientas de síntesis basadas en Verilog.[3]

El departamento de la defensa de USA exige una descripción en VHDL, para cada ASIC. Una de las aplicaciones mas complejas fue el desarrollo del avión F22.

5.5 Encabezado y cuerpo de un diseño:

Library: archivo o directorio que guarda unidades de diseño previamente compiladas. Y la biblioteca de un proyecto por defecto se llama work.

Package: Unidad de un diseño que almacena declaraciones de tipo, constantes componentes, entre otros. Previamente compilados.

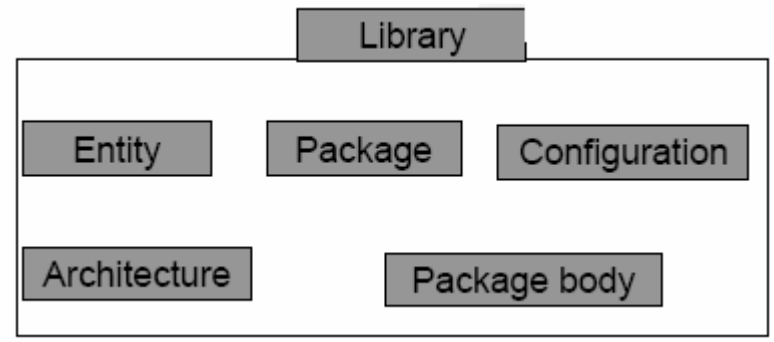


Figura 5.2. Descripción de una biblioteca.[4]

Entidad: La podemos ver como la envoltura o embonado de una arquitectura, esta contiene los puertos de entrada y salida de cierto componente, como se ve en la figura 5.3.

[3] Douglas J Smith, HDL Chip Design, Editorial Doone Publications, Madison, AL, USA, 1996, p.p.8
[4] Douglas J Smith, HDL Chip Design, Editorial Doone Publications, Madison, AL, USA, 1996.

```
ENTITY nombre_entidad IS
 PORT (   puerto_1 : modo tipo;
          puerto_2 : modo tipo;
          .....
          puerto_n : modo tipo
        );
END nombre_entidad;
```

Figura 5.3. Sintaxis de entidad en VHDL.

Arquitectura: es propiamente la descripción de lo que contendrá la entidad o componente, se puede usar cualquier nivel de abstracción o estilo para modelarla como son:

- Estructural.
- Flujo de datos (RTL).
- Funcional.

La figura 5.4 muestra la sintaxis de la arquitectura.

```
ARCHITECTURE nombre_arch OF nombre_entidad IS
   declaraciones de tipos
   declaraciones de señales
   declaraciones de constantes
   definición de funciones
   definición de procedimientos
   declaración de componentes
BEGIN
   declaraciones concurrentes
   ......
END nombre_arch;
```

Figura 5.4 Sintaxis de la Arquitectura en VHDL.[5]

[5] Douglas J Smith, HDL Chip Design, Editorial Doone Publications, Madison, AL, USA, 1996.

Prácticamente el código en VHDL, esta compuesto de estas tres partes. Aunque queda abierto a investigar mas acerca del lenguaje, por ahora cabe también mencionar que las herramientas de simulación mas utilizadas son:

- Altera: QuartusII.
- Xilings: ISE Foundation.
- Modeltech: Modelsim.

En estas compañías generalmente encuentras versiones de evaluación solo debemos registrarnos para que nos envíen una licencia, solo, que esta seria para la maquina de donde la estas solicitando ya que se genera para el numero de serie del disco duro o la tarjeta de red.

Estas evaluaciones las encuentras como: ISE WEBPACK, QUARTUSII y MODELSIM.

Para este proyecto se utilizo el simulador Modelsim, ya que es muy estable y te permite trabajar correctamente.

Primero que todo se explica como se establecieron las partes de este proyecto para hacer la simulación tanto de la tarjeta como del receptor que estará verificando que la tarjeta sea la adecuada para tal receptor (interrogador). En la figura 5.5, se pueden ver los diagramas de ambos componentes tanto de la tarjeta como del receptor. En algunas partes del código el receptor es conocido como interrogador ya que para las especificaciones del circuito (MCRF 452), definido en el capitulo 4 el interrogador es el receptor.

5.6 Descripción del proyecto

Iniciando con la descripción de la tarjeta, y como se ve en la figura 5.5. observamos que primero que todo debemos contar con una memoria la cual guarda los datos tanto de la propia tarjeta como es el numero de serie, así como los datos del usuario los cuales están dados en los primeros bloques de el

integrado MCRF 452, (0,1,2, bloques de información que se utilizaran para los datos personales e identificación de tarjeta), después de la memoria vemos un multiplexor el cual esta actuando como selector de una dirección (bloque) de memoria. Describiendo un poco un multiplexor es un componente al cual le llegan muchas entradas y de acuerdo a un selector deja pasar una de las entradas dejando salir la seleccionada. Y para esta selección en este proyecto se ha creado un componente que validara mediante una maquina de estados el o los datos que debe dejar pasar el multiplexor.

El componente que contiene la maquina de estados es prácticamente el control de esta tarjeta inteligente que en algunos casos también conocido como sistema operativo. De aquí el dato seleccionado por el control pasa a un registro de 32 bits (TR) ya que la memoria contiene direcciones o bloques de 32 bits, y este registro se encarga de transferir tal dato en serie hacia el receptor el cual lo recibe bit por bit para hacer su trabajo correspondiente, una ves que se cuentan con los tres bloques iniciales de la memoria de la tarjeta, en el receptor, el receptor acciona el bit MC1 de la tarjeta que permite que la tarjeta entre a un estado inactivo (sleep) el cual permite que el receptor haga su operación de comparación y verificación para tal tarjeta permite el acceso a la persona portadora de esta tarjeta,(chip).

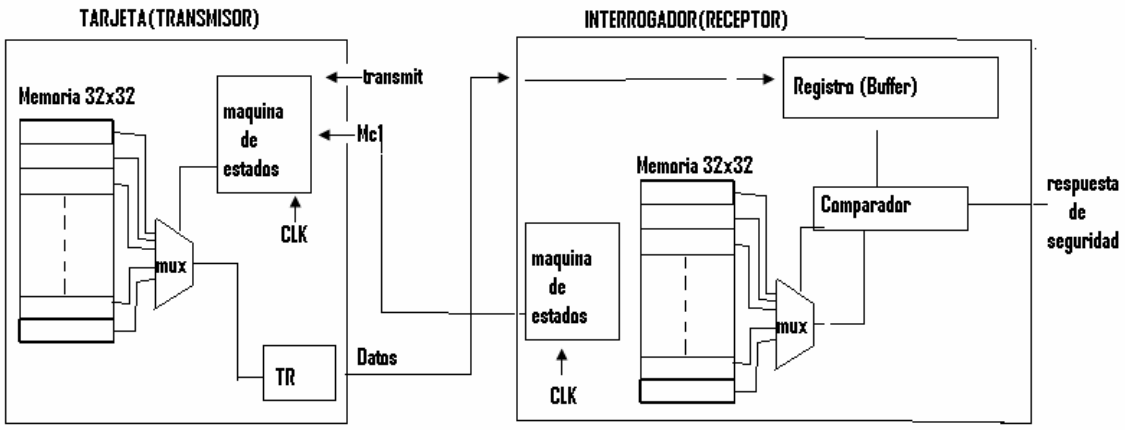


Figura 5.5. Diagrama de la tarjeta y el interrogador en operación.[6]

[6] Creado por el autor de esta tesis.

Inicialmente el receptor cuenta con un numero de dígitos almacenados, previamente grabados, que le indican los datos de los usuarios así como el numero único de serie para cada integrado, estos están dentro de su sistema de almacenamiento en este caso se ve como una memoria de 16 x 32. lo cual nos dice que podrá almacenar hasta 5 personas para esta capacidad de memoria por lo cual es bueno tener una gran cantidad de memoria pero para la cuestión de la simulación de este trabajo es suficiente. Dentro del receptor tenemos también un componente que lleva un control y que también por cuestión practica permite observar que pasa dentro del componente, esta es una maquina de estados donde también para ambos lados se cuenta con un reloj que permite realizar los movimientos y simulaciones de forma sincrona, así como también se pueden observar las formas de onda que ocurren.

Antes de continuar comentare en forma general que es una máquina de estados, prácticamente es un arreglo de código que dado a cierta estructura, este código sigue o no su paso hasta concluir con lo establecido mediante evaluaciones. En VHDL una forma conveniente de modelar maquinas de estados es utilizando dos procesos (funciones, o procedimientos), uno calcula es estado siguiente al que pasara el sistema y el otro para determinar las salidas. Existen dos tipos de maquinas de estados, las MEALY y las MOORE. Las MEALY son las mas generales y se caracterizan porque su salida de pende del estado en que se encuentran y su entrada. Las maquinas de MOORE son un caso particular de las anteriores y se caracterizan porque su salida solo depende del estado en que se encuentra el sistema. Y en VHDL se pueden modelar maquinas de estado tanto de MEALY como de MOORE.

Una vez descrito esto queda la tarea de continuar investigando mas acerca de este tema, por ahora continuamos en la descripción del interrogador. Una ves que la tarjeta inicia su transferencia de datos, estos llegan a un registro de 32 bits el cual por ahora esta formado como una memoria de 32 pero que solo se utilizan los primeros 3 bloques o direcciones de el, en donde se almacena temporalmente el dato de la memoria de la tarjeta, una ves que se

tiene dentro del registro el componente de la maquina de estados se encarga de enviar un bit por el puerto MC1 hacia la tarjeta para ponerla en el estado sleep, y así poder continuar con su trabajo de comparación de acuerdo con lo que existe almacenado en el sistema de almacenamiento del receptor, esto se hace en un registro de verificación mediante un conteo de direcciones en ambas memorias donde para la primera solo se hace un conteo hasta el 2 binario ya que como esto es un acceso solo verifica un numero de serie que esta en la primer dirección de la tarjeta y datos del usuario que toman las siguientes dos direcciones, esto es que va de la dirección 0 a la 2, mientras que para la memoria de almacenamiento del sistema dentro del receptor si se toman en cuenta todas las direcciones. Lo que hace para esto es que toma en cuenta los datos de estas 3 direcciones y mediante un barrido en la memoria del sistema de 3 en 3 y seleccionando mediante un multiplexor va comparando y si encuentra tres direcciones en forma sincrona iguales a las que contiene el registro buffer entonces es una tarjeta con permiso de acceso, y en lo real este pin de salida de respuesta de seguridad en el receptor seria el que accione algún interruptor para permitir el acceso a esta tarjeta. En este caso como solo es simulado veremos a la salida de la respuesta de seguridad un uno lógico.

Antes de presentar el código de la tarjeta, comentare de forma general lo que se hace para hacer la prueba de que este circuito esta funcionando correctamente. Para esta simulación en particular se realizaron dos componentes uno de ellos es la tarjeta con las características del integrado MCRF 452, el otro es el receptor para el mismo dispositivo, ya que se realizan ambos componentes en VHDL, existe una forma de probar que ambos dispositivos están trabajando correctamente, pero para este proyecto no se realiza porque se realiza la simulación por separado y de esta forma se comprobó su funcionamiento. Y a esto se le conoce como bancos de prueba (Test Bench). Un banco de prueba es la definición de un conjunto de patrones de prueba que se usan para verificar un circuito o modelo en VHDL. También VHDL permite modelar el banco de pruebas independientemente de la

herramienta de simulación, con la ventaja de ser usado en cualquier fase de proceso en diseño. El banco de pruebas se modela como una entidad sin puertos con su arquitectura de tipo estructural en la que las señales internas son las entradas y salidas del circuito, y la estructura es con las instancias de las entidades a probar en caso de ser varias. Esto también es parte de la tarea del lector interesado para realizar su búsqueda en cualquier referencia de su alcance referente a VHDL.

Dejando esto como información general pasamos a analizar el código de la tarjeta o bien del dispositivo interno. Como se comentaba la estructura que se lleva en un código VHDL, es la siguiente:

- BIBLIOTECA
- ENTIDAD
- ARQUITECTURA

Nota: Se encontrara dentro del código el parámetro “- -“, esto quiere decir que es un comentario dentro del código fuente.

5.7 Código de la tarjeta.

- Y así iniciamos con una Biblioteca. Donde se describe un archivo o directorio que guarda unidades de diseño previamente compiladas.

```
library ieee;
  use ieee.std_logic_1164.all;
  use ieee.std_logic_unsigned.all;
  use ieee.std_logic_arith.all;
```

- Continuamos con la entidad, donde se define el embonado de una arquitectura, esta contiene los puertos de entrada y salida de cierto componente.

- Para este caso aquí se definen los puertos de entrada y salida de la tarjeta como se ve a continuación.

```
entity tj is
    port(
        trs      : in std_logic; -- pin de entrada, se activa para iniciar la transmisión.
        Mc1      : in std_logic;-- pin de entrada, activa el estado sleep.
        transmit : out std_logic; -- pin que avisa al receptor de una transmisión.
        data     : out std_logic; -- pin de salida de datos. Bit por bit.
        wr_en    : in std_logic; -- pin que permite la escritura en la memoria.
        clk      : in std_logic;-- pin de entrada del reloj.
        dato_in  : in std_logic_vector(0 to 31); -- pin de datos en forma de vector.
        address  : in std_logic_vector(0 to 4));-- pin de direccion de memoria.
end entity tj;
```

- Arquitectura de el componente o entidad, aquí es propiamente la descripción de lo que contendrá la entidad o componente

```
architecture tj_bhv of tj is
```

- Ya vimos que para la entidad se definen sus entradas y salidas asignándoles un tipo de entrada y salida de igual forma dentro de una arquitectura se hacen declaraciones de señales que no son mas que pequeños cables dentro del integrado que permitirán la conexión entre dispositivos, pero puede verse la figura 5.4 para que esto quede mas claro.

```
    --maquina de estados----------------------------
    type states is (sleep, trx); -- declaración de estados.
    signal curr_st : states:=sleep; -- declaración de estado actual inicializado en
sleep.
    signal next_st : states:=sleep;-- declaración de estado siguiente inicializado en
sleep.


    --memoria de 32 x 32----------------------------
```

```
    subtype bloque is std_logic_vector(0 to 31);-- declaración de subtipo para una
dirección de memoria.
    type mem is array (natural range <>) of bloque;-- definición del tipo de arreglo.
    signal memory    : mem(0 to 31);-- declaración de memoria.
    --buff_mem,(registro) para asinar los bloques de la memoria-
    signal buff_mem  : std_logic_vector(0 to 31);

    --contadores inicializados en “0”----------------------------------------
    signal cnt_bloque: std_logic_vector(0 to 4):="00000";
    signal cnt_bit   : std_logic_vector(0 to 4):="00000";
    --activador de conteo--------------------------
    signal tx_ini    : std_logic:='0';
    --control de encendido-------------------------
    signal trs_aux   : std_logic:='0';
```

- Igual que en otros lenguajes de programación después de la declaración de señales es necesario un begin.

```
begin
```

- El process un pequeño modulo dentro de la arquitectura que puede ser definido como una función o procedimiento el cual es concurrente. Esto es que mientras halla un cambio de reloj el actúa no importa si existen tantos process como sean posibles ellos actuaran en paralelo, con el resto del código.
- Para este caso este process es realizado para el cambio de estado en la maquina de estados. Y lo que esta dentro de los paréntesis es la señal o pin de entrada a lo que puede ser sensible el process.

```
cmb:process(clk)
begin
    if (clk'event and clk='1') then - - evalua si hubo cambio en el reloj.
```

```
        curr_st <= next_st;- - paso a siguiente estado.
    end if; -- termina la evaluacion.
end process cmb; -- termina el process de cambio de estados.

--process que lleva el control de los estados dentro de la maquina de estados.
-- y determina las salidas. También es sensible a un reloj y a un bit que permite --el inicio de la transmisión,(trs).
stm:process(trs, clk)
-- esta es la estructura para las maquinas de estados van dentron de un case ---- como sigue.
begin
    case curr_st is
    when sleep =>--transmite los datos al mismo tiempo pasa al estado trx
        if (trs_aux='1')then  - -utiliza una señal inicializada en “0”
            next_st  <= trx; -- para al estado de transmisión.
            transmit <= '1'; -- activa el bit de transmit para que el receptor este listo.
            tx_ini   <= '1'; -- activa los contadores cuando se inicia la transmisión.
        else--mientras no este dormida puede enviar los datos.
            if (mc1 = '0' and trs = '1') then – valida si envia datos.
                trs_aux <= '1'; -- se queda en este estado.
            end if;
        end if;
    when trx => -- una ves enviado el dato se pone estado sleep.
        if (mc1 ='1')then - - valida si esta en modo sleep.
            next_st  <= sleep; - -  pasa al estado sleep.
            tx_ini   <= '0'; - - el contador se detiene.
            transmit <= '0';- - deja de transmitir.
            trs_aux  <= '0'; -- termina la transmisión.
        end if;
    end case; --
end process stm; -- fin del proceso de la maquina de estados.
```

- Proceso para el conteo sensible al reloj y a una señal de transmisión, tx_ini., como solo nos interesan los tres primeros se ve que se hace una evaluación con un if dentro del estado del reloj, donde solo se cuenta hasta 3 para la dirección aunque para los bits dentro de los bloques el conteo va hasta 32 ya que son bloques (Direcciones) de 32 bits.

```
cnt_trx:process(clk, tx_ini)
begin-- solo nos interesan los primeros 3 bloques.
   if(clk'event and clk='1') then - -  se evalua el estado del reloj.
      if (tx_ini = '1') then
        -- si se cumple el siguiente if, se reinician los contadores.
         if (cnt_bloque = "00010" and cnt_bit = "11111") then
            cnt_bloque <= "00000";
            cnt_bit    <= "00000";
         else
        -- si no se sigue contando, y llenado las direcciones hasta llegar a la
        --direction  2(00010)
            if (cnt_bit = "11111") then
               cnt_bloque <= cnt_bloque + 1;
            end if;
            cnt_bit <= cnt_bit + 1; -- sigue llenando la direccion especificada por
                                          -- el cnt_bloque.
         end if;
      end if;
```

- En el siguiente paso se llena el registro con lo que tiene la memoria en la direccion (cnt_bloque) haciendo una conversión a enteros para la direccion del registro (buff_mem) y una ves dentro de el este se encarga en hacer otra ves la conversión y enviarlos a data que es el bit de salida para la tarjeta y atraves de este se transmiten bit por bit al receptor.

```
      buff_mem <= memory (conv_integer (cnt_bloque));
      data <= buff_mem (conv_integer (cnt_bit));--bit por bit
```

```
--de auerdo al conteo de cnt_bit.
    end if;
end process cnt_trx;
```

- El siguiente process es para el llenado por primera vez de la tarjeta o reprogramación, en caso de ser necesario para otra aplicación.

```
llenadomemoria: process(wr_en, clk)
begin
  if(clk'event and clk='1') then
      if (wr_en = '1') then - - permite la escritura en la memoria.
-- asignación del dato a la dirección de memoria.
          memory(conv_integer(address)) <= dato_in;
          end if;
      end if;
end process llenadomemoria;

end tj_bhv; -- termino de la arquitectura de la tarjeta.
```

5.8 Simulación de la tarjeta

termina el código de la tarjeta aunque parece poco realmente se toma días de trabajo encontrarle la lógica que realmente se quiere como sugerencia puedo decir que esto solo con practica y persistencia se logra, mantener la calma y continuar sin llegar a la desesperación porque es lo que te puede sacar del camino.

Se inicia la simulación para 70kbit/s, que es la frecuencia a la que el dispositivo transmite los datos, sacamos la inversa de eso y nos da 14.28 us. Con los que estaremos trabajando en toda la simulación tanto en la tarjeta como en el receptor, por ahora en la tarjeta se ingresan los datos siguientes en el momento de la impresión.

(00000) .-10101010101010101010101010101010

(00001).- 01010101010101010101010101010101

(00010).- 00000000000000000000000000000000

Estos son datos que servirán de prueba para la tarjeta como se ve a continuación en los resultados de las simulaciones.

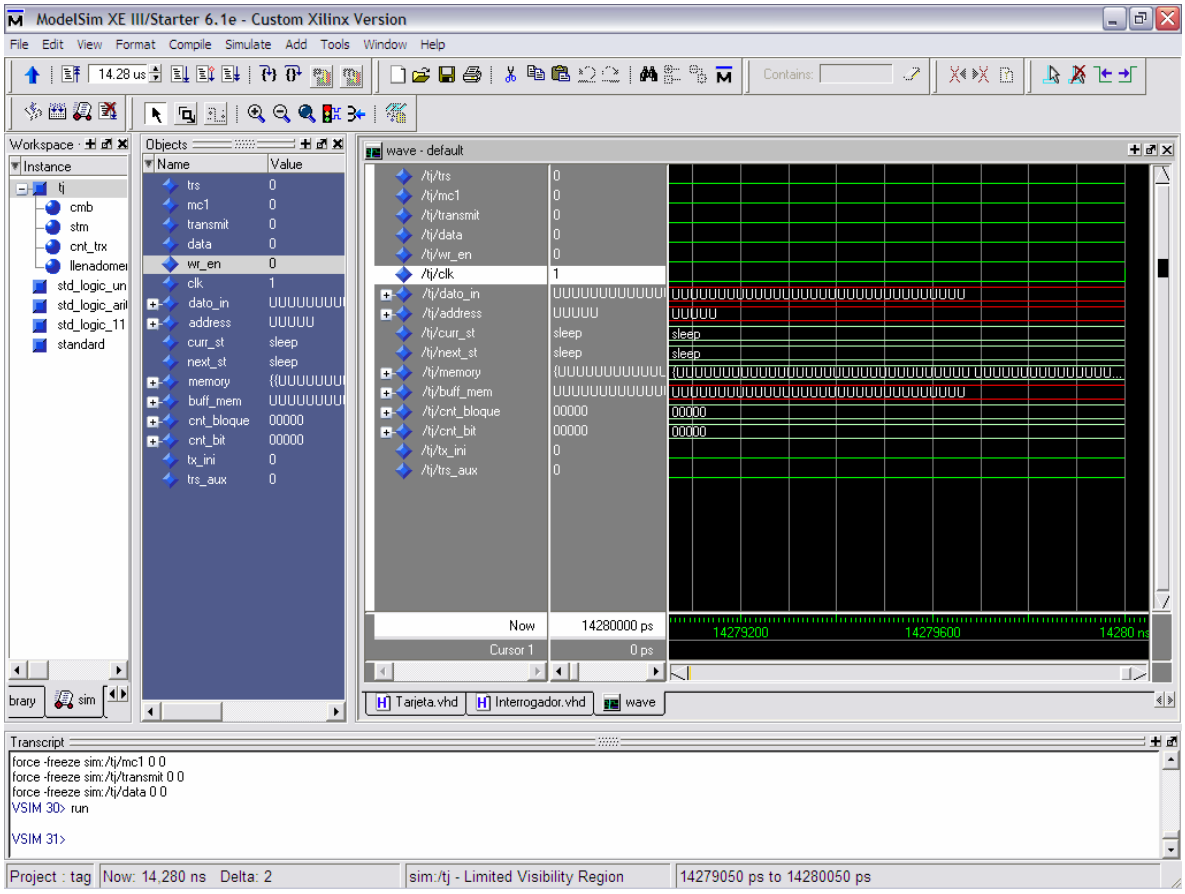


Figura 5.6. Todo en cero memoria vacía. Reloj a 14.28 us.[7]

Como se observa en la figura 5.6 el reloj esta activo en 14.28 us, y el we_en esta en ‘0’ y por ahora la memoria interna de la tarjeta esta vacía, así como también los otro pines (trs, mc1,transmit, data) y se encuentra en estado Sleep, este es el estado normal de la tarjeta a menos que se aproxime a una

[7] Creado por el autor de esta tesis.

estación de recepción donde por medio de radio frecuencia (ondas de radio) se activa e inicia una transmisión, ya que estas al ser inducidas en una bobina producen una corriente y alimenta al circuito interno de la tarjeta.

En la siguiente simulación agrego un dato para el numero de serie en la dirección 0 (00000) y simulo. Pero aun no he puesto el wr_en en uno así que solo estará listo para entrar.

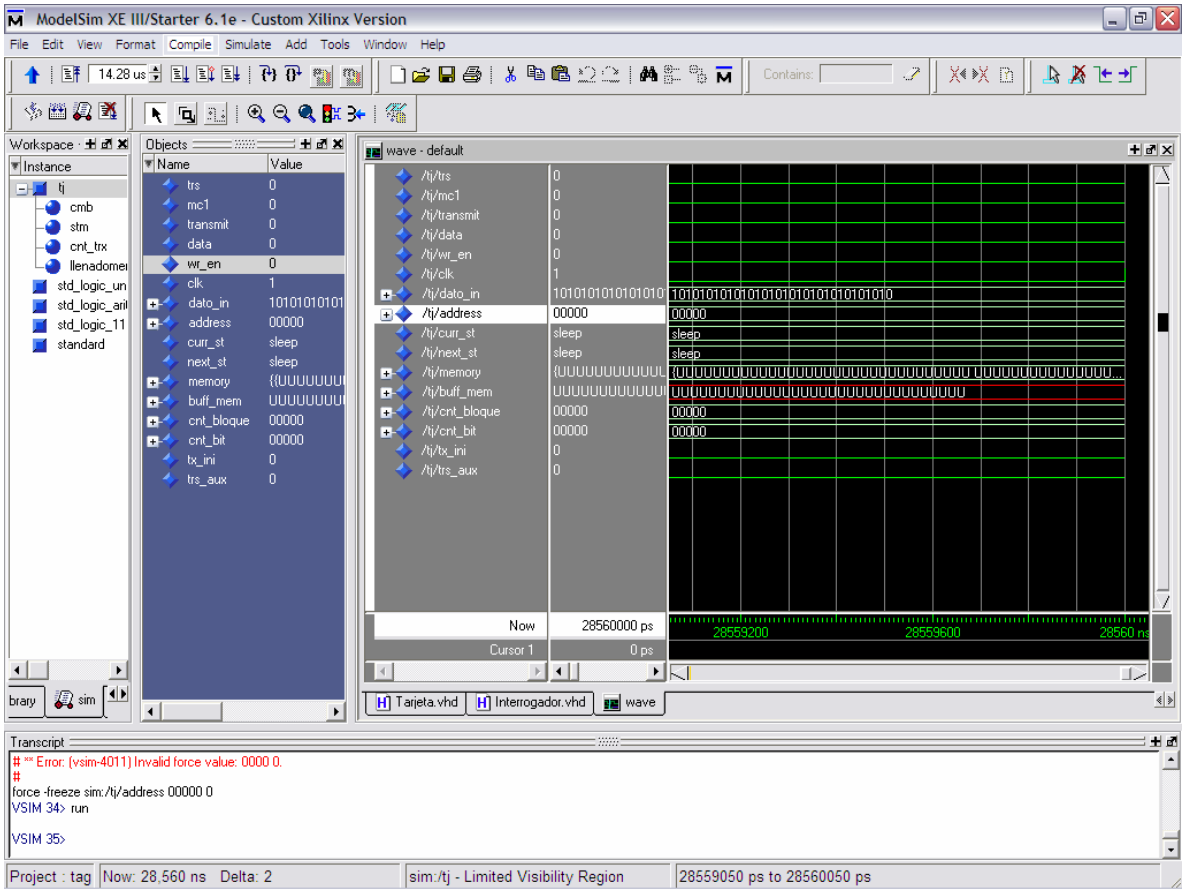


Figura 5.7. Datos puestos en la entrada y la direccion lista en '0'. [8]

Ya con lo anterior habilito el wr_en = '1', para cargar el dato en la memoria y en la dirección 0, como se ve en la figura 5.8.

[8] Creado por el autor de esta tesis.

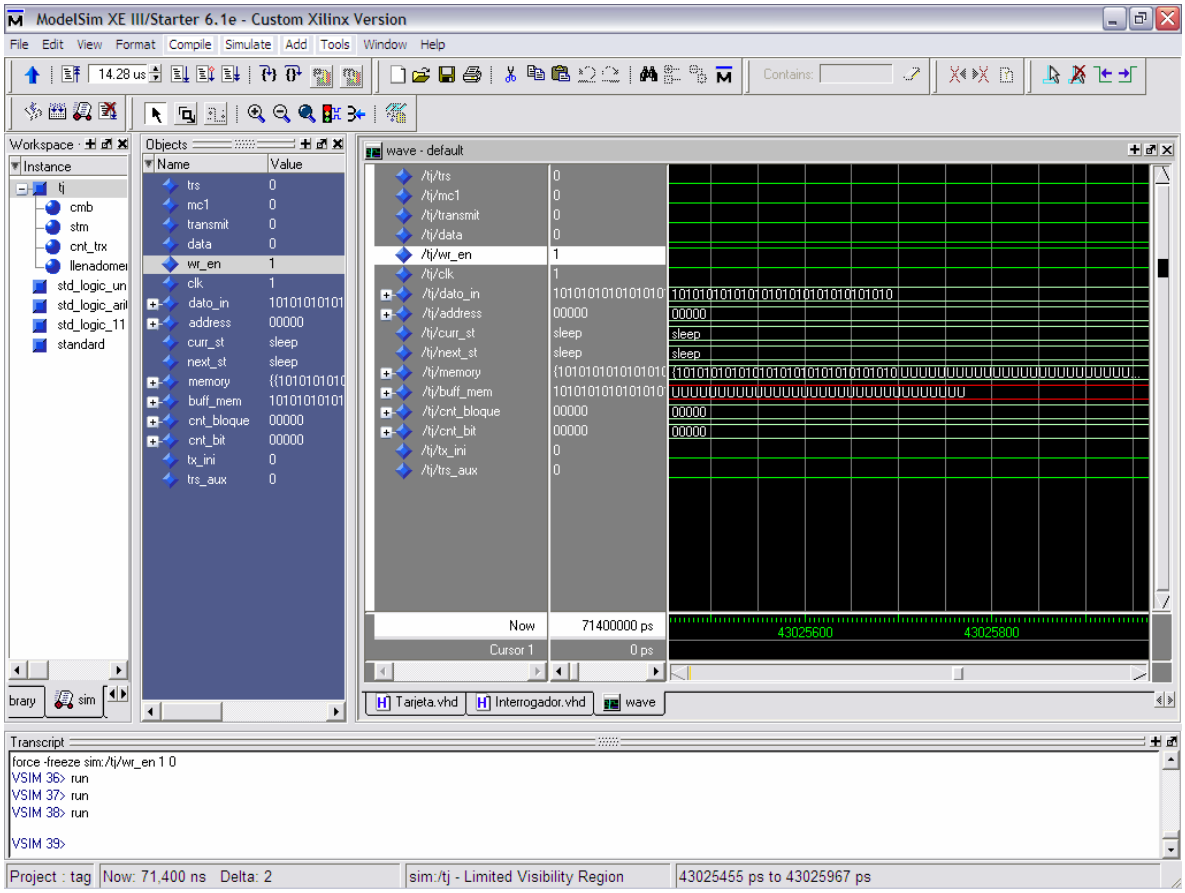


Figura 5.8. Wr_en = '1', primer dato cargado. En la direccion '0'. [9]

Ahora seleccionamos nada mas la memoria para ver que lo guardo correctamente en la dirección '0', se ve que ya esta cargada con el primer dato, que es el numero de serie siguiente: '10101010101010101010101010101010'.

[9] Creado por el autor de esta tesis.

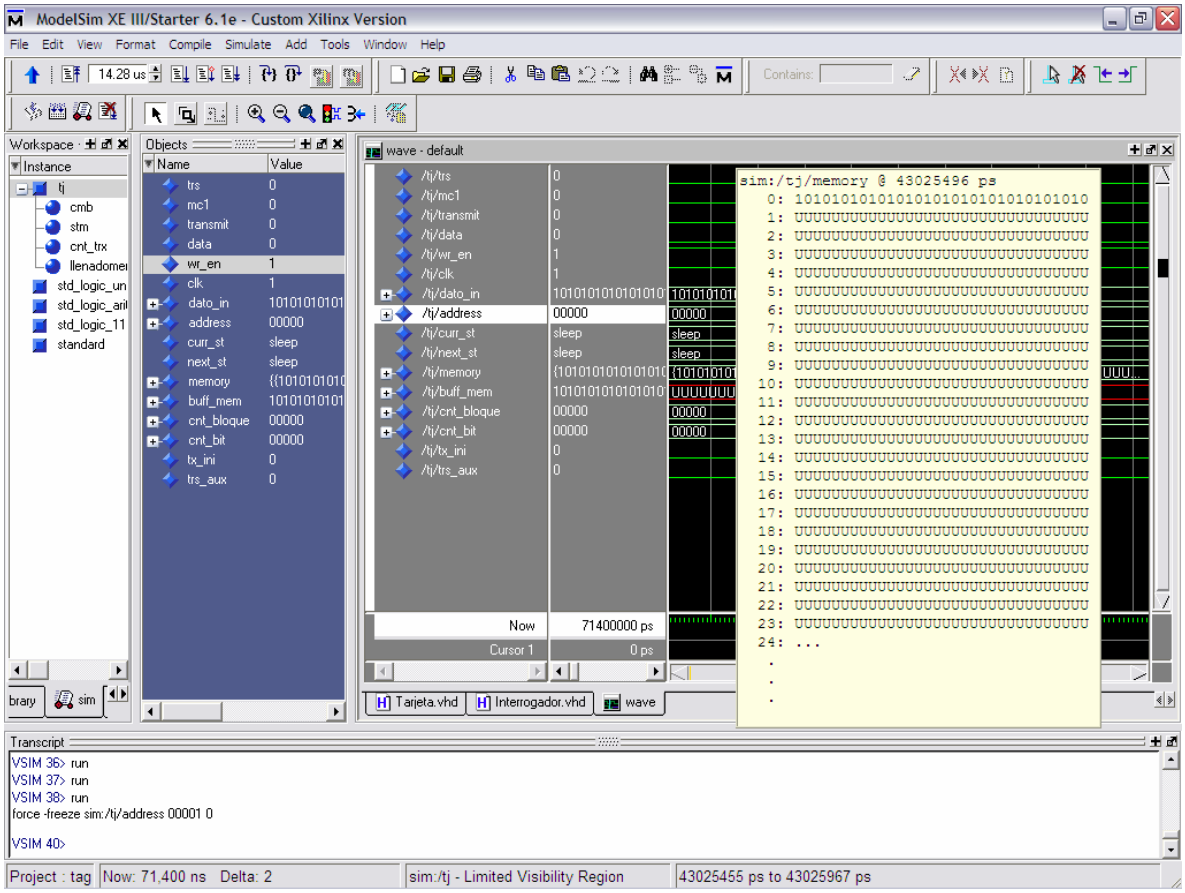


Figura 5.9. Muestra de la memoria con el primer dato cargado en memoria. [10]

Como el paso anterior ahora continuamos para los dos siguientes datos, que es el número del usuario y datos del mismo. Se puede verificar en las figuras 5.10 y 5.11. Para ver que están estos datos guardados.

[10] Creado por el autor de esta tesis.

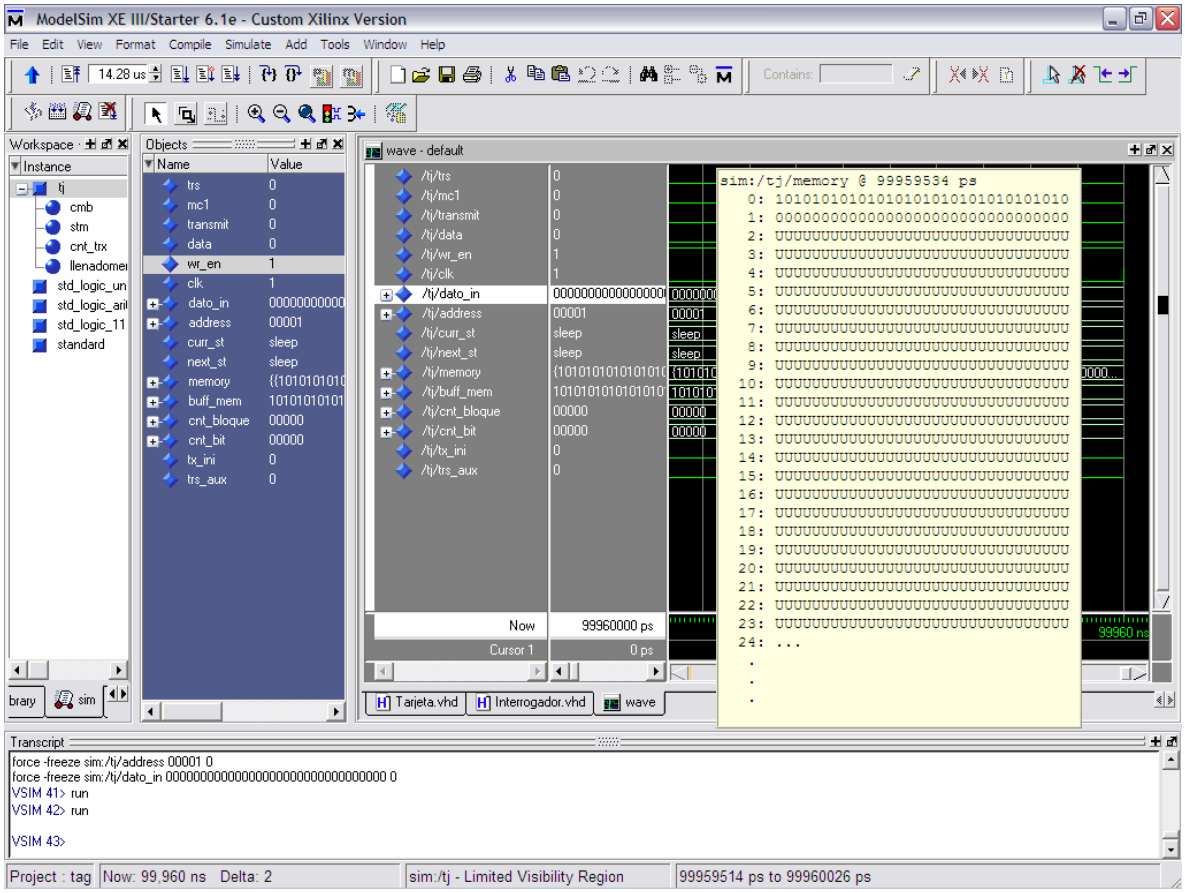


Figura 5.10. Dato dos cargado.[11]

[11] Creado por el autor de esta tesis.

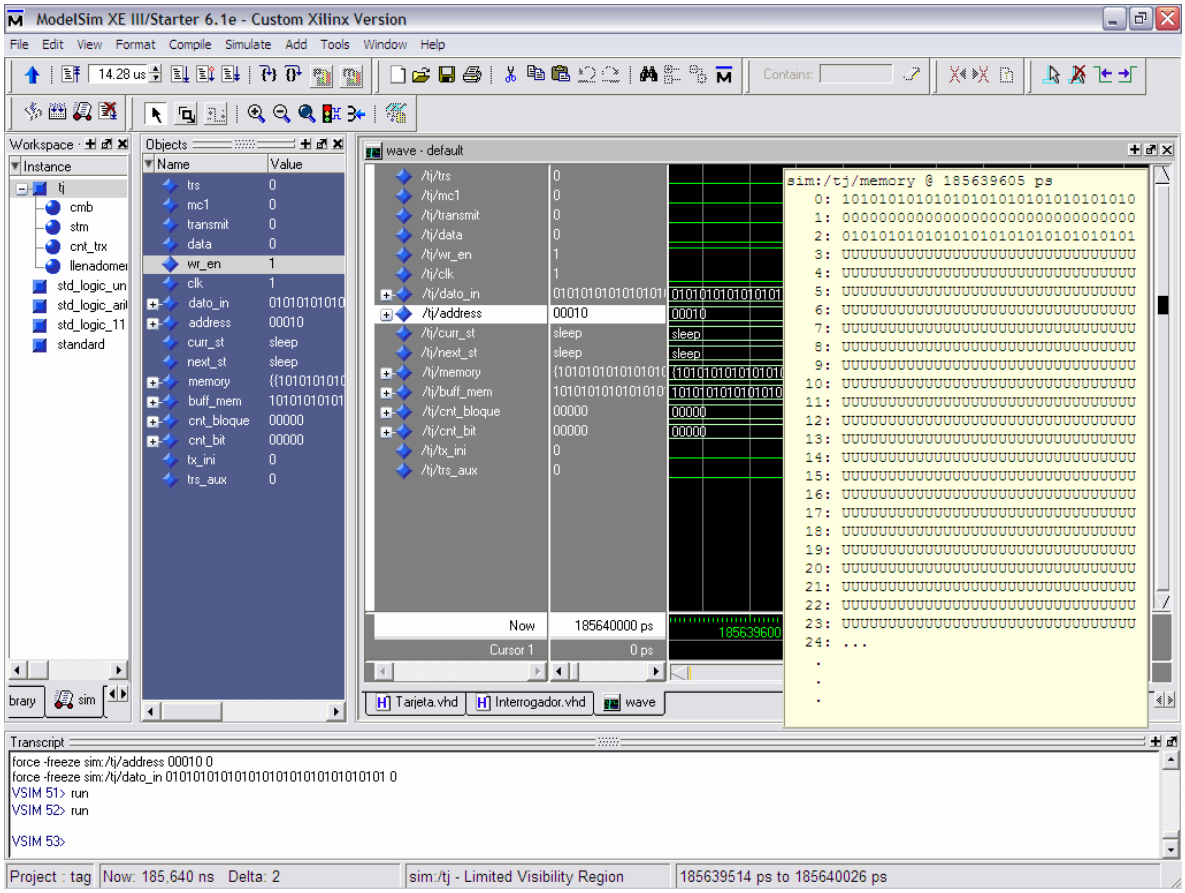


Figura 5.11. Dato tres cargado.[12]

Y así quedaron cargados los dígitos que me interesan para este proyecto, en la memoria entonces ya puedo deshabilitar el Wr_en, para no escribir mas ya que de ahora en adelante esta será de solo lectura, solo se programa por una ocasión para esta aplicación.

[12] Creado por el autor de esta tesis.

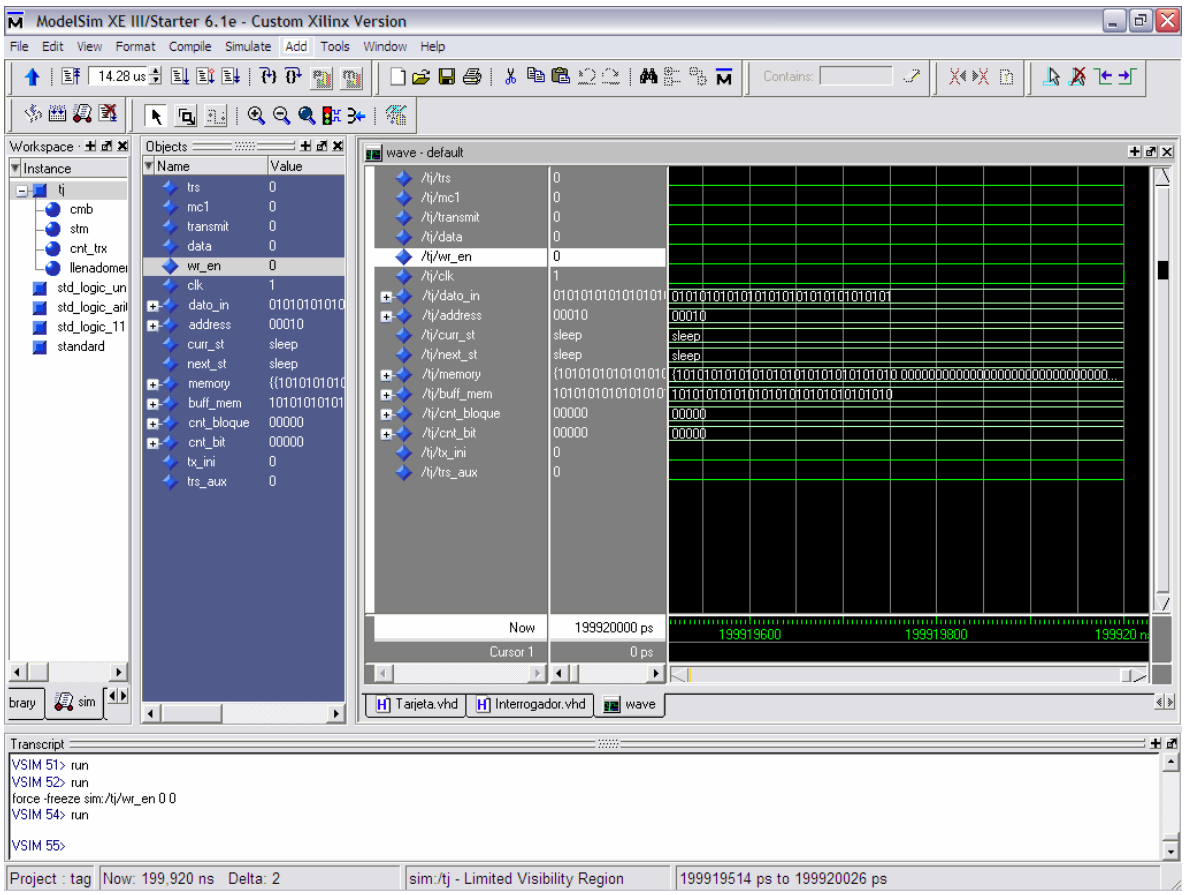


Figura 5.12. Estado normal de la tarjeta ya tiene los datos en memoria y esta en estado sleep. [13]

Ahora en la siguiente simulación haremos una transmisión de prueba para la tarjeta. Para esto es como si aproximáramos la tarjeta a un dispositivo de radio frecuencia (receptor) el cual por medio de ondas de radio activa el trs, que es el pin que habilita la transmisión y a su ves envía un pulso por medio del pin transmit que es que energiza al pin receive de el receptor el cual se pone activo para recibir los datos bit por bit. También el dato inicia su transmisión bit por bit, para esto también se sincroniza a una velocidad de 70kbits/s. O sea 14.28 us.

[13] Creado por el autor de esta tesis.

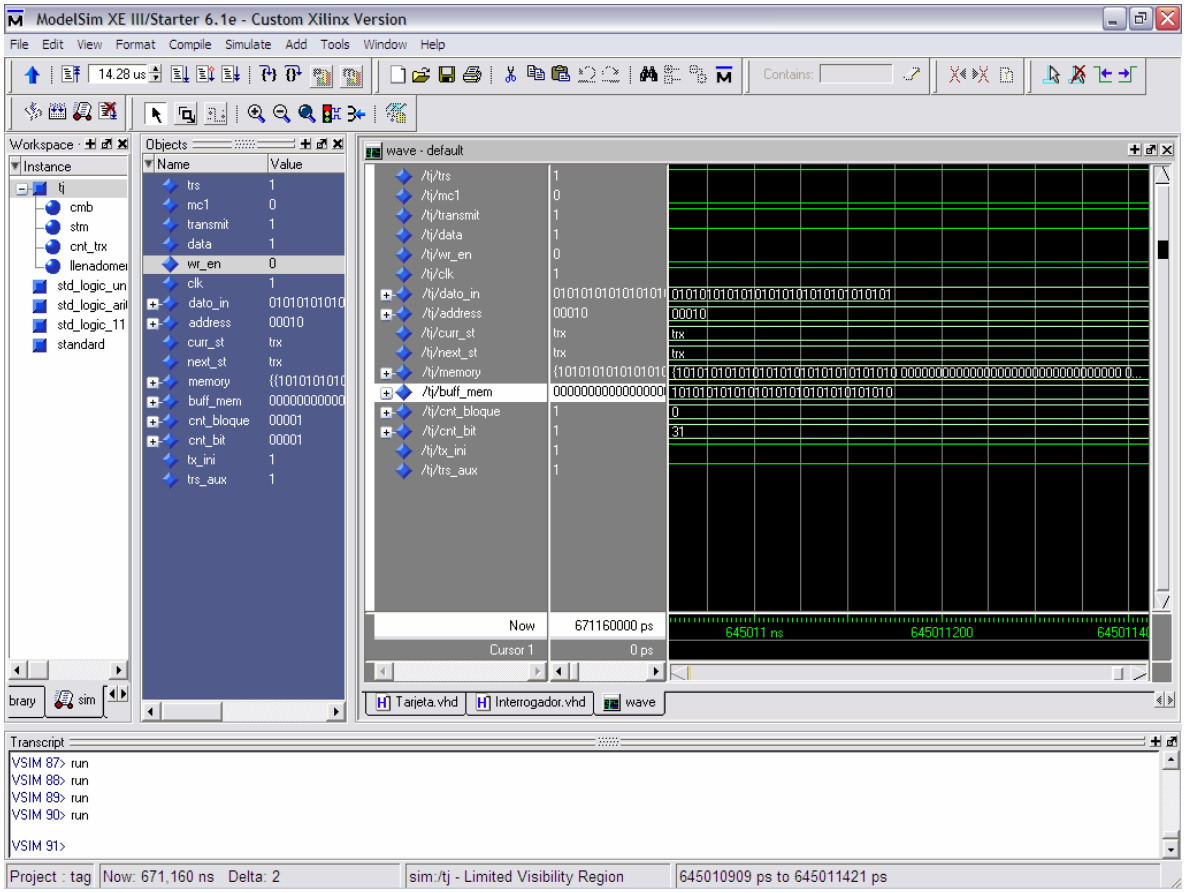


Figura 5.13. El dato lo paso a un buffer para enviarlo, y se encontraba en la dirección 0 ahora que termina de pasar ese digito, pasa al de la dirección 1 y así hasta llegar a la 2. Se encuentra en estado TRX(trasnmitir).[14]

[14] Creado por el autor de esta tesis.

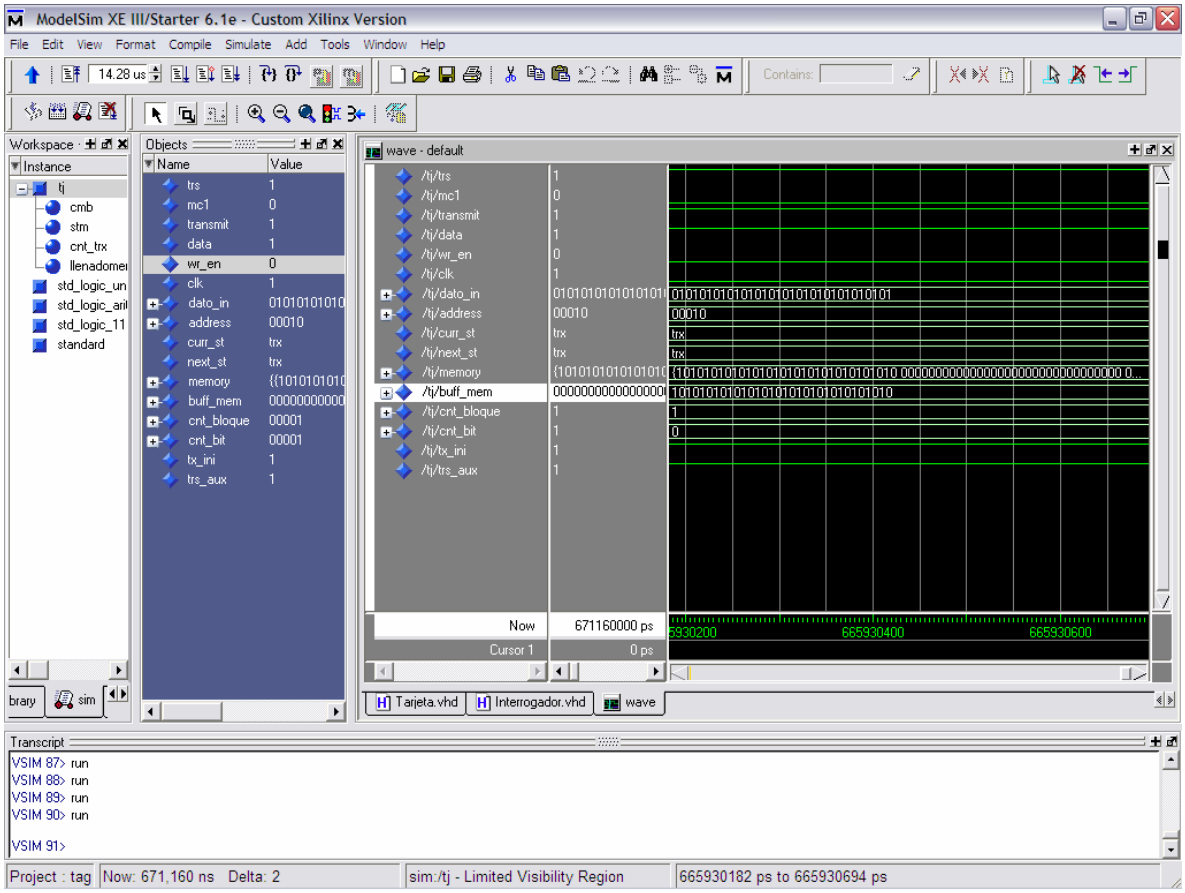
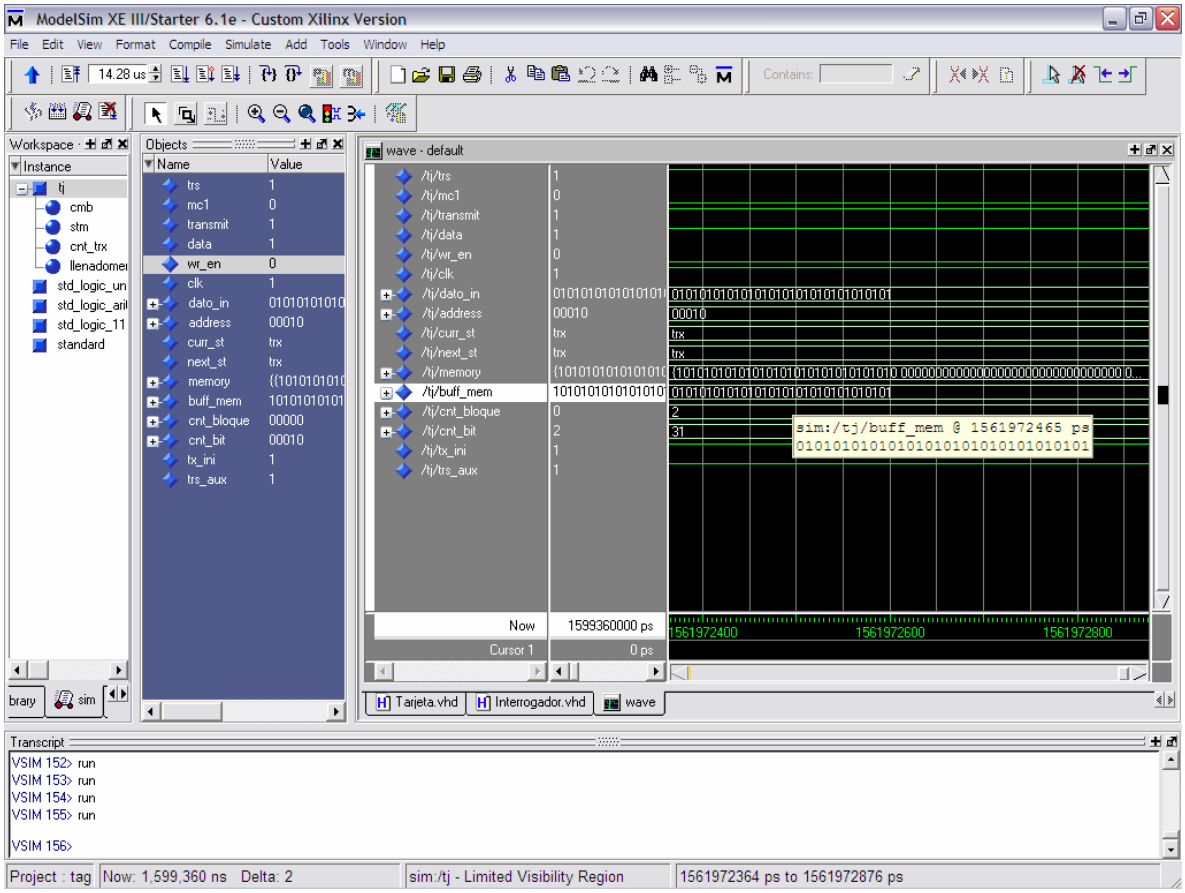


Figura 5.14. Transmitió todos los datos bit por bit y se pasa a la dirección 1, he indica que esta en el estado TRX(transmitir).[15]

[15] Creado por el autor de esta tesis.



Figura, 5.15. Aquí le ve que llega el contador de las direcciones (cnt_bloque) a 2 y el bit dentro de esta en 31(cnt_bit).[16]

Una ves que se transmiten los 3 bloques de datos se activa el mc1, ver figura 5.16, por medio del receptor y este avisa a la tarjeta que entre en estado sleep para así evitar colisión con otras tarjetas en caso de estar alguna otra presente, y ya con los datos el receptor entra en acción y compara los dígitos que están en su sistema de información con los que tiene de la tarjeta.

[16] Creado por el autor de esta tesis.

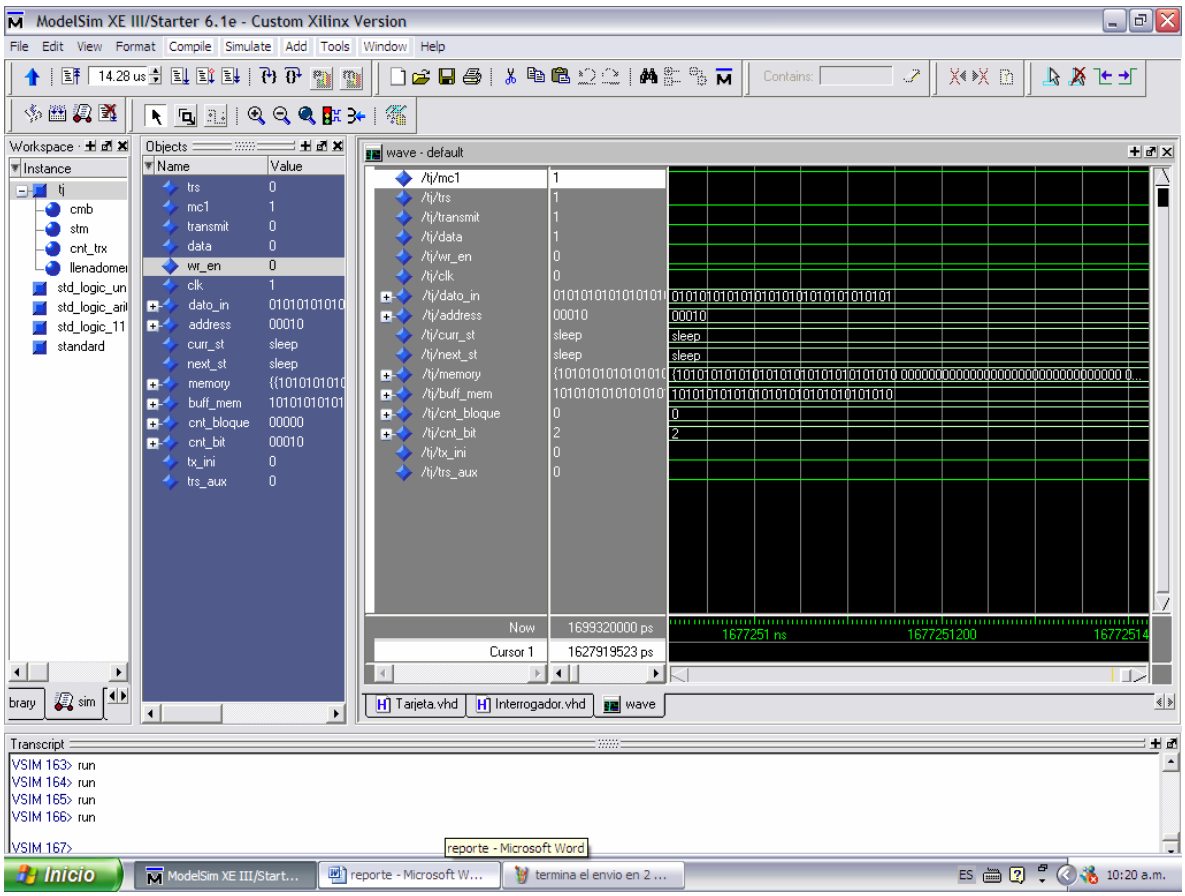


Figura 5.16. Se habilita la señal mc1 y el estado sleep. [17]

En la simulación anterior las señales de transmisión pasan a cero por la maquina de estados, y se sigue quedando en el estado sleep. Y de esta manera se describe la función de la tarjeta en simulación la cual de acuerdo a los resultados esta simulando correctamente.

Antes de pasar las simulaciones del receptor veamos como esta compuesto el código fuente. De igual forma que en el código de la tarjeta se verán "- -", que indican los comentarios dentro del código VHDL.

[17] Creado por el autor de esta tesis.

5.10 Código fuente del receptor.

- Declaración de la Biblioteca, de un archivo previamente compilado.

```
library ieee;
   use ieee.std_logic_1164.all;
   use ieee.std_logic_unsigned.all;
   use ieee.std_logic_arith.all;
```

- Continuamos con la entidad, donde se define el embonado de una arquitectura, esta contiene los puertos de entrada y salida de cierto componente.
- Para este caso aquí se definen los puertos de entrada y salida del receptor como se ve a continuación.

```
entity receptor is
   port(
      receive    : in std_logic; -- pin de entrada para la recepcion.
      data       : in std_logic; -- datos pin por pin.
      mc1resp    : out std_logic;-- respuesta para el estado sleep para la tarjeta.
      security   : out std_logic;-- activa interruptor o avisa que es segura la tarjeta.
      clk        : in std_logic;-- reloj interno
      wr_enint   : in std_logic;-- habilitador de escritura para memoria interna.
      dato_inint : in std_logic_vector(0 to 31);-- dato de 32 bit para la memoria
interna.
      addressint : in std_logic_vector(0 to 3));-- direcciones disponibles de la
memoria interna.
end entity receptor;
```

- Arquitectura de el componente o entidad, aquí es propiamente la descripción de lo que contendrá la entidad o componente

architecture interrogator_bhv of receptor is

- Ya vimos que para la entidad se definen sus entradas y salidas asignándoles un tipo de entrada y salida de igual forma dentro de una arquitectura se hacen declaraciones de señales que no son mas que pequeños cables dentro del integrado que permitirán la conexión entre dispositivos.

```
--maquina de estados---------------------------
type states is (recepting, idle, compare);
signal curr_st   : states:=idle;
signal next_st   : states:=idle;
--memoria de 32 x 32----------------------------
subtype bloque is std_logic_vector(0 to 31);
type mem is array (natural range <>) of bloque;
signal memory    : mem(0 to 31);
signal buff_mem  : std_logic_vector(0 to 31);

--memoria de 16 x 32----------------------------
signal memory16  : mem(0 to 16);

--contadores-----------------------------------
signal cnt_bloque: std_logic_vector(0 to 4):="00000";
signal cnt_bit   : std_logic_vector(0 to 4):="00000";
--activador de conteo---------------------------
signal rx_ini    : std_logic:= '0';
--auxiliar para comparador seguridad------------
signal sec_aux   : std_logic:='0';
--auxiliar para término de recepcion------------
signal mc1_aux   : std_logic:='0';
--contadores auxiliares de comparacion----------
signal cnt_buff  : std_logic_vector(0 to 4):="00000";
signal cnt_mem16 : std_logic_vector (0 to 3):="0000";
```

```
    --comparador auxiliar-------------------------
    signal comp_aux  : std_logic:='0';
    --señal termina de comparar-------------------
    signal comp_end  : std_logic:='0';

begin
- -process para calcular el estado siguiente al que pasara en el sistema la - -- -- -
-maquina de estados.
 asigned_st:process(clk)
begin
    if (clk'event and clk='1') then
        curr_st <= next_st;
    end if;
end process asigned_st;

- -process para determinar las salidas de la maquina de estados.
stm:process(receive, clk)
begin
    case curr_st is
    when idle =>-- esta ala espectativa de alguna tarjeta.
        if (receive='1')then – evalua el pin receive
            next_st  <= recepting; -- pasa al estado recepcion.
            rx_ini   <= '1'; -- activa la señal rx_ini
        end if; -- termina de evaluar en el estado idle
    when recepting => --recibe la transferencia de datos en serie
        if (mc1_aux ='1')then – evalua la señal mc1_aux
            next_st  <= compare; -- pasa al estado comparar
            comp_aux <= '1'; -- habilita la señal comp_aux
            rx_ini   <= '0'; -- desactiva la señal rx_ini.
        end if; -- termina de evaluar el estado de recepcion.
    when compare => --compara el dato recibido con su bd
```

```
        if (comp_end = '1')then – evalua la señal comp_end.
            next_st  <= idle; -- pasa al estado idle.
            comp_aux <= '0'; -- desactiva el comp_aux.
        end if;  - - termina de evaluar.
    end case;    -- termina de evaluar las salidas de  los estados.
end process stm; -- termina el proceso de maquina de estados.
```

-- asignación de que la salida mc1resp es igual a lo que este en la señal mc1_aux, esto se --hace así por que una salida no puede ser evaluada y en caso de necesitar eso se asigna --a una señal, lo mismo pasa para la siguiente asignación de security como es salida se -- -le asigna una señal, security = sec_aux.

```
mc1resp  <= mc1_aux;
security <= sec_aux;
```

-- recordando un poco todo esto que esta dentro del código es concurrente así que todo ---sucede en un mismo tiempo. Tanto lo que esta dentro de los procesos como lo que esta --afuera. Por eso se debe tener cuidado al momento de programar porque se pueden --------generar algunos cortos.

```
cnt_trx:process(clk, rx_ini) – esto indica que es sensible a clk y rx_ini.
begin-- solo nos interesan los primeros 3 bloques.
    if(clk'event and clk='1') then – esto pasara con un flanco de subida del reloj.
        if (rx_ini = '1') then—evalúa la señal rx_ini que indica una transmisión de
```

datos.

-- inicia el conteo tanto de la memoria temporal para recibir los datos de las tres ----------primeras direcciones y de los bits de estas direcciónes hasta 31, para después hacer la ---comparación. Y envia activa el mc1_aux para poner en estado sleep a la tarjeta.

```
            if (cnt_bloque = "00010" and cnt_bit = "11111") then
                cnt_bloque <= "00000";
                cnt_bit    <= "00000";
                mc1_aux    <= '1';
```

```
            else
--en caso de no tener haber llegado el conteo hasta 3 en la dirección evalúa que
el ----------contador del bit llegue a 31 y así pasar a la siguiente dirección hasta
llegar a la ------------direccion 3, y posteriormente hacer su comparación.
                if (cnt_bit = "11111") then
                    cnt_bloque <= cnt_bloque + 1;
                end if;
                cnt_bit <= cnt_bit + 1;
            end if;
--aquí asigna lo que esta en data que son los datos de entrada a un buffer donde
lo ---------convierte en entero para ponerlo en la casilla correspondiente de la
dirección, y este a ---su ves lo asigna a la memoria que será la que se tomara en
cuenta para la comparación --con la memoria del sistema (receptor).
            memory(conv_integer(cnt_bloque))<= buff_mem;
            buff_mem(conv_integer(cnt_bit)) <= data;
        end if;
    end if;
end process cnt_trx; -- termina el proceso de conteo para la transmisión.

-- proceso de comparación donde se toman en cuenta ambas memorias tanto la
temporal --como la del sistema de almacenamiento. Nuevamente como
recordatorio existe un ------reloj el cual dentro de todos los procesos es sincrono,
y recordando que esto es ------------concurrente todo pasa en un mismo pulso.
(Recuerda).
comparator:process(clk)
begin
    -- aquí verifica que los datos ya estén dentro de la memoria temporal por
medio de la --señal comp_aux la cual le indica si compara o reinicia los
contadores en cero de los -----contadores internos de la memoria del sistema.
    if (clk'event and clk='1')then
        if (comp_aux ='1')then
```

```
            if (cnt_mem16 = "1110") then
                cnt_buff  <= "00000";
                cnt_mem16 <= "0000";
                comp_end  <= '1';
-- en caso de que la señal sea comp_aux sea ‘0’ va hacer la comparación de las
3 ----------direcciones guardadas en la memoria temporal con las de la memoria
interna y esto lo --hace de 3 en 3. y si esto se cumple entonces también se
activa la señal de sec_aux que --a su ves acciona la salida security del
interrogador.
            else
                comp_end <= '0';
                if(memory16(conv_integer(cnt_mem16))= memory(0)and
                     memory16(conv_integer(cnt_mem16)+1)= memory(1)and
                     memory16(conv_integer(cnt_mem16)+2)= memory(2))then
                       sec_aux <= '1';
                end if;
-- y esto indica que mientras estemos en el estado de comparacion la memoria
del ---------sistema se va estar incrementando de 3 en 3
                if (curr_st=compare) then
                    cnt_mem16 <= cnt_mem16 + 3;
                end if;
            end if;
        end if;


    end if;
end process comparator;
-- este process permite guardar datos en la memoria del sistema habilitando el
wr_en. ------También con un cambio de reloj, en alto.
-- corrimiento de memoria.
llenadomemoria: process(wr_enint, clk)
begin
```

```
  if(clk'event and clk='1') then
      if (wr_enint = '1') then
          memory16(conv_integer(addressint)) <= dato_inint;
      end if;
  end if;

end process llenadomemoria;
end interrogator_bhv;-- termina el codigo del interrogador(receptor).
```

5.11 simulación de el receptor.

De igual forma para el receptor se simulo para una velocidad del integrado de 70kbits/s, o bien 14.28 us una ves que se obtiene la inversa, y también al igual que para la memoria se le cargan los datos iniciales para cuestión de prueba utilizamos los siguientes datos para tener información dentro del sistema de almacenamiento del receptor.

Datos utilizados:

(0000).- 10101010101010101010101010101010

(0001).- 10101010101010101010101010101010

(0010).- 10101010101010101010101010101010

En la figura 5.17 se ve lo que esta almacenado en la memoria del receptor, que por ahora solo es una memoria de prueba de 16*32, y que para efecto de simulación solo tiene las direcciones de ‘0’ a ‘2’ llenas, que son las que utilizara para la comparación con las de la tarjeta que de igual forma forzaremos que el buffer o memoria temporal tenga el mismo dato para poder hacer la comparación y ver como se activa la señal de security, la cual para este proyecto seria la que activaría el interruptor y dar acceso a la tarjeta.

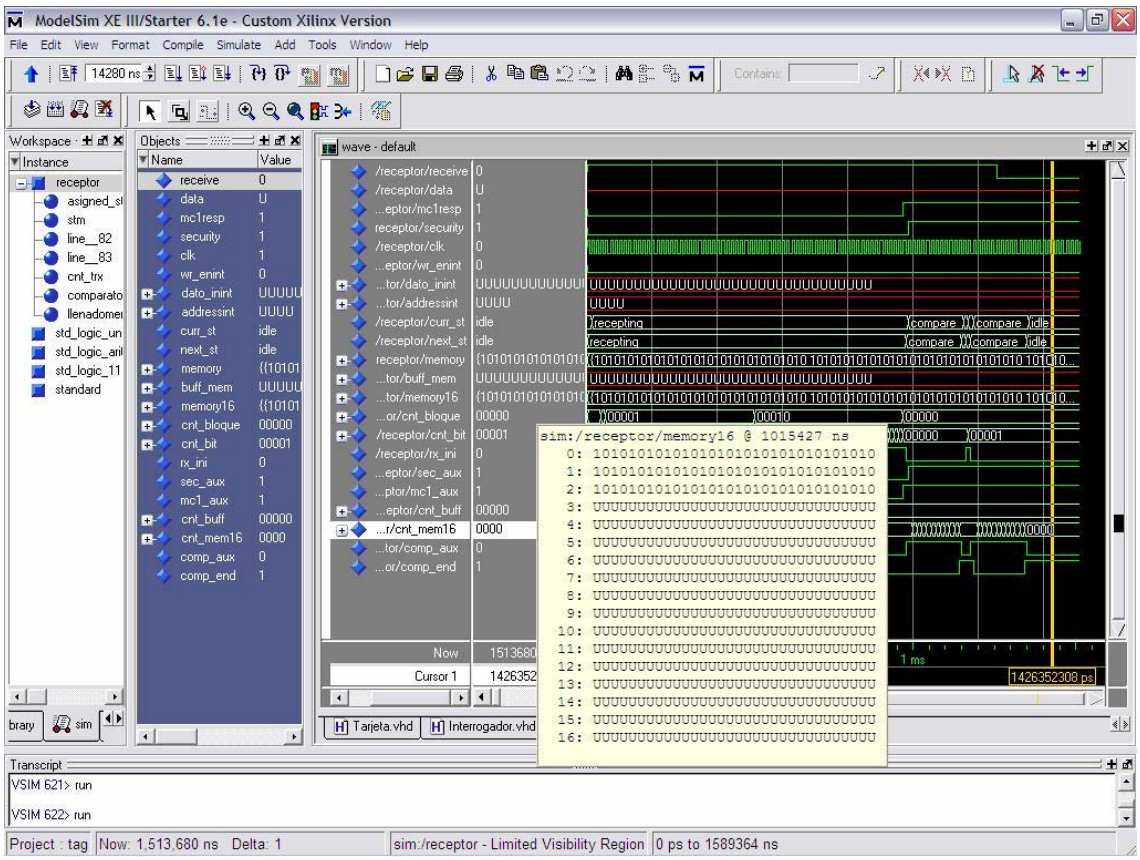


Figura 5.17. Memoria interna del receptor. [18]

[18] Creado por el autor de esta tesis.

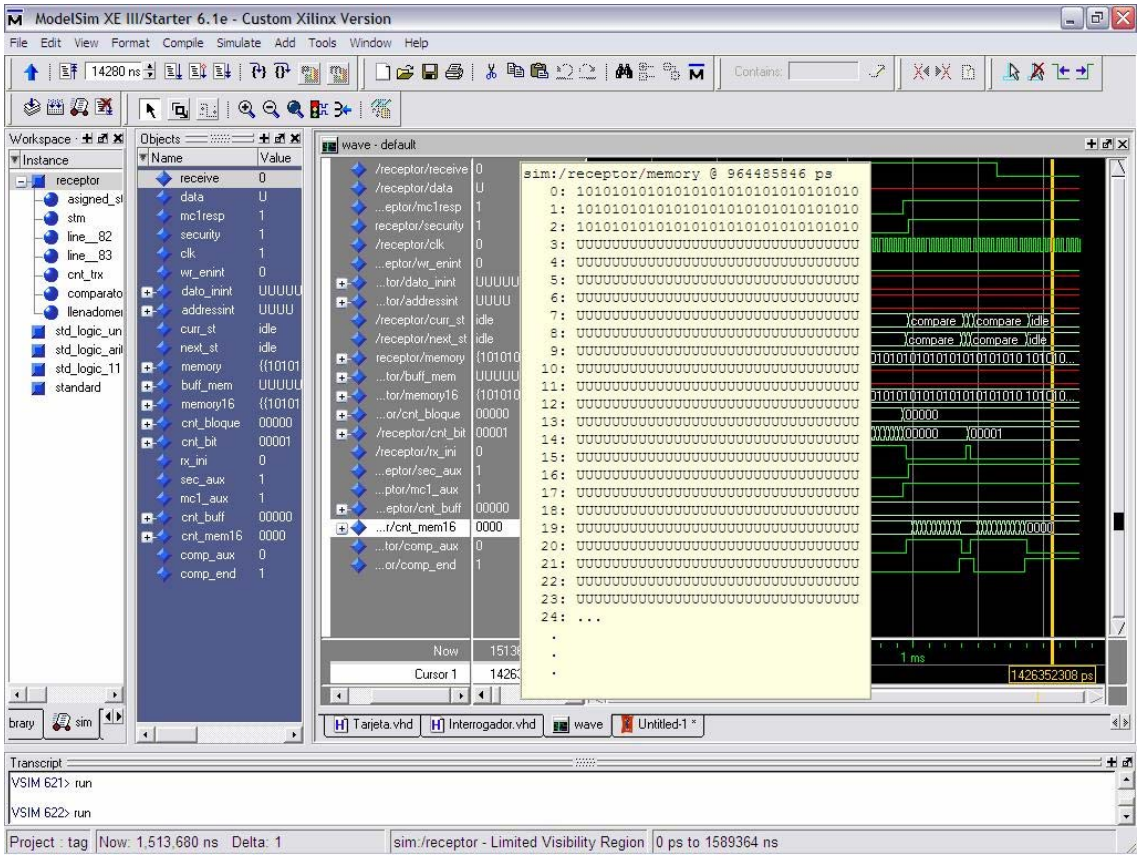


Figura 5.18. Muestra la memoria temporal (buffer), con los datos obtenidos de la memoria.[19]

Se puede observar en la figura 5.18 que el buffer de entrada tiene los mismos datos que el receptor lo cual nos dice que para el comparador esta será una tarea fácil, y activar la señal de security. La cual nos dice que además de abrir el interruptor también es una tarjeta de confianza ya que cuenta con datos verdaderos y que corresponden al receptor en función.

[19] Creado por el autor de esta tesis.

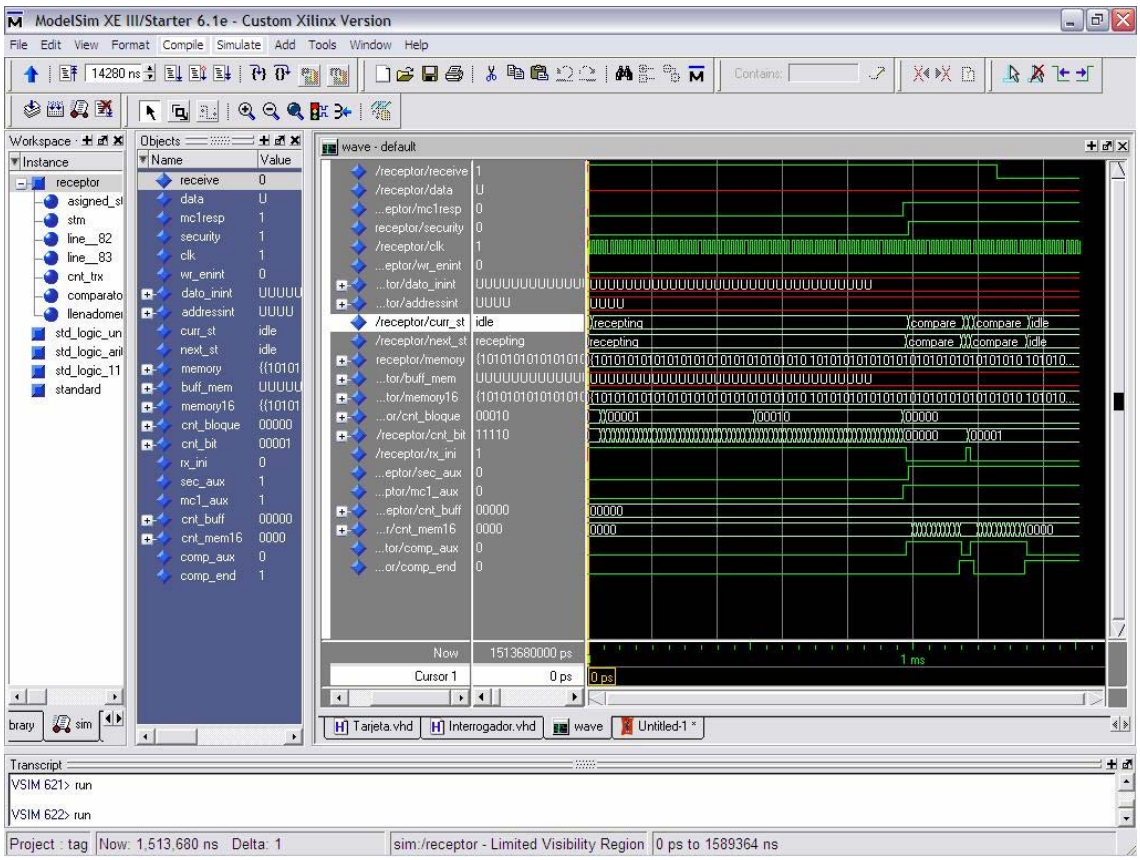


Figura 5.19. Operaciones del receptor exepto la carga inicial de datos en la memoria del receptor.[20]

En la figura 5.19, nos permite observar todas la señales dentro de el así como su cambio de estados (recepting, compare, idle), primero que todo cuando este esta sin operación esta en estado idle, una ves que detecta una tarjeta presente inicia su recepción de datos que almacena en la memoria temporal de 32*32, o buffer de entrada, una ves que tiene este dato como se vio en la figura 5.18, este envía una señal de salida (mc1) (ver figura 5.20), para poner en estado de sleep a la memoria y así poder hacer su comparación de datos con los que tiene en la memoria del sistema y así activar o no la señal de salida security. En la figura 5.20. Se puede ver más a fondo de lo que pasa en la simulación completa.

[20] Creado por el autor de esta tesis.

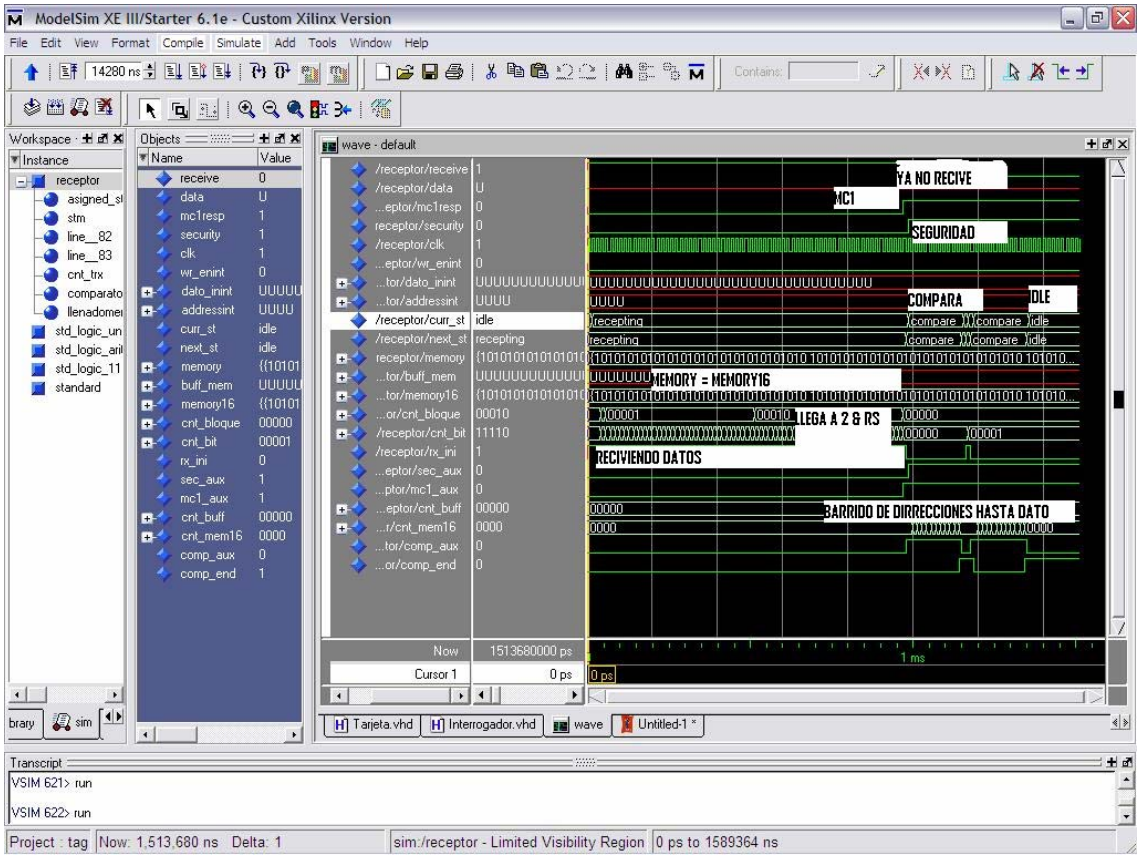


Figura 5.20. Descripción del receptor completo. [21]

[21] Creado por el autor de esta tesis.

Conclusión

Del análisis de la tecnología que se maneja en este trabajo se puede concluir que aunque aquí doy fin a este proyecto que de hecho está en pleno auge puede decirse que es sólo el inicio de una nueva tecnología más para el mundo.

Del objetivo propuesto en la introducción, el cual fue la implantación de un sistema de control de acceso, para tener una seguridad más controlada, se concluye que mediante la respuesta de la simulación en VHDL tanto de la tarjeta utilizando el dispositivo MCRF de microchips como del receptor para el mismo dispositivo, mediante el software Modelsim XE III 6.1e, se logra observar que ambos están correctamente sincronizados para una aplicación real que permitiría monitorear el acceso de todas las personas a un determinado lugar y de hecho el código presentado aquí puede ser utilizado para sintetizar el dispositivo y ver la opción de realizar el resto del trabajo que seria la parte real o analógica que se acoplaría a lo que se tiene para llevar a cabo el proyecto.

También como se propuso el uso de las memorias EEPROM ya que son eléctricamente borrables y además se prestan para implantarlas en las tarjetas ya conocidas como tarjetas inteligentes, ya que con la nanotecnología las memorias prácticamente han quedado invisibles por lo cual una tarjeta inteligente en la actualidad es idéntica a lo que conocemos como una tarjeta de crédito donde no se percibe si cuenta con un integrado o no, y por lo cual también se concluye que en este trabajo son totalmente indispensables para el manejo de la información que se propone en esta aplicación.

Aunque la tecnología de almacenamiento y radio frecuencia ya existen en muchas aplicaciones todavía siguen surgiendo nuevas necesidades en toda la industria y la sociedad.

El éxito obtenido en este trabajo mediante la simulación del control de acceso por una tarjeta inalámbrica que en cada uno de los capítulos se describe una parte de lo que la compone como son el almacenamiento de información, conocimiento de las tarjetas inteligentes, estándares y operabilidad, enfoque en lo inalámbrico y simulación en VHDL de el dispositivo propuesto, deja una satisfacción al saber que esto se puede realizar en la vida real.

En cada uno de los capítulos anteriores se describió de lo que consta esta nueva tecnología, a lo que prácticamente invito a los lectores a explorar las diferentes ramas que se tienen en la actualidad sobre los sistemas de almacenamiento y radio frecuencia ya que la tendencia de la tecnología actual va hacia los dispositivos de almacenamiento masivo e inalámbrico.

Con esto concluyo que mi trabajo expuesto en este libro está compuesto de la base para un dispositivo que permite realizar aplicaciones del presente y del futuro, ya que basta con ingresar las palabras: radio frecuencia o chip inteligente, en un sistema de búsqueda en Internet y te encontrarás con n-número de aplicaciones relacionado con la tecnología de de radio frecuencia y chips de almacenamiento extenso, para los cuales este dispositivo puede ser el ideal a considerar para dicha aplicación.

BIBLIOGRAFIA

M. Morris Mano, Ingeniería Computacional Diseño del Hardware, Editorial PRENTICE HALL, 199l, 301

Reinhold Ludwig, Pavel Bretchko, RF Circuir Design Theory and Applications , Editorial PRENTICE HALL, 2000, 410

Douglas J Smith, HDL Chip Design, Editorial Doone Publications, Madison, AL, USA, 1996, 448

OTRAS FUENTES

www.howstuffworks.com

http://www.howstuffworks.com/rom1.htm

www.universidaddezaragosa.com en el departamento de ing. electrónica y comunicaciones

http://centros5.pntic.mec.es/cpr.de.aranjuez/foro/tecno/informatica.html

www.iso.org

www.hid.com

www.microchips.com

www.wikipedia.com

www.ChipDesignMagazine.htm