ESCUELA POLITÉCNICA DEL EJÉRCITO

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

PROYECTO DE GRADO PARA LA OBTENCIÓN DEL TÍTULO DE INGENIERÍA

"*DISEÑO E IMPLEMENTACIÓN DE UN PROTOTIPO DE SISTEMA DE SUPERVISIÓN DE ACCESO, UTILIZANDO LA IDENTIFICACIÓN DE RADIOFRECUENCIA Y LA TECNOLOGÍA BLUETOOTH PARA LA TRANSMISIÓN DE DATOS*"

OSCAR FABIAN HERRÁN RENGIFO

SANGOLQUÍ - ECUADOR 2009

CERTIFICACIÓN

Certificamos que el presente proyecto de grado con título "Diseño e implementación de un prototipo de sistema de supervisión de acceso, utilizando la identificación de radiofrecuencia y la tecnología bluetooth para la transmisión de datos", fue desarrollado en su totalidad por el señor Oscar Fabian Herrán Rengifo con C.I. 171216551-1 bajo nuestra dirección como requerimiento para la obtención del título en INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES.

_____	_____
Sr. Ing. Darwin Aguilar	Sr. Ing. Carlos Romero
DIRECTOR	CODIRECTOR

Quito, 2009

DEDICATORIA

Para mi familia quien me apoyo en todo momento, a mi padre Luis Gonzalo Rengifo quien me enseño a luchar en la vida a que jamás me deje vencer y la que cada día se puede ser mejor a mis tres madres: Ruthcita quien con su amor y comprensión me enseño que una madre puede ser también una buena amiga, Teresita quien me demostró que no hay edad para aprender y que con ganas de salir adelante si se puede a Marianita de quien aprendí que hay que ser constante en la vida y que por amor y sentirse bien uno trabaja mejor a mi Hermanita Adriana Pitufo quien con su forma de ser me demostró que no existe imposibles que cada uno se pone sus límites y que lo que se quiere hay que luchar para conseguirlo y a mi Hermano Pableins a quien admiro porque es mi amigo de él aprendí que no hay que dejarse que las personas nos humillen y para mi es la mejor guía para nosotros tus hermanos.

Dedico a mis mejor amigos casi hermanos: Jorge Polo, José Arauz y Juan Pico ya que gracias a ellos esto sueño se pudo hacer realidad y que cuando los necesite siempre estuvieron ahí.

AGRADECIMIENTOS

A Dios y a la Virgencita por darme la fuerza necesaria para salir adelante y cubrirme de una bendición Divina

A mi familia con quien luchamos para que desde este momento llegue a cumplir una meta más en mi vida

A los mejores amigos casi hermanos y no compañeritos Jorge Polo, José Arauz y Juan Pico ya que hoy puedo constatar que las amistades pueden durar para siempre y que los mejores consejos vienen de las personas que mejor te conocen

A las personitas tan bellas mis amigas cuasi hermanas Lydy Aguirre y Karina Saquicela ya que ellas cambiaron mi vida y alteraron mi destino demostrándome que los hombres y las mujeres pueden llegar a ser los mejores amigos y que una buena amistad hay que saber conservarla gracias por llegar a mi vida

A mis amigos de la universidad: Cesar Bastidas, Mauricio Sarzosa, German Culqui, David Viteri, Mauricio Moreno, Jhaji ludeña y Yoco, por apoyarme en esos momentos cuando no salían las cosas además por demostrarme que los amigos en la universidad si existen y si se puede llevar fuera de la universidad y pueden ser tu mejor apoyo

PROLOGO

En este proyecto se ha desarrollado un dispositivo con el cual se podrá administrar el ingreso y salida de un laboratorio. El objetivo de este proyecto es de proporcionar una herramienta tecnológica que ayude a sistematiza y controlar el uso, además de almacenar los movimientos de las horas y de las personas que lo utilizan.

El dispositivo permite diferenciar o identificar personas mediante la utilización de tarjetas de identificación. Para esto, el dispositivo permite grabar y almacenar los datos personales y asociar a una etiqueta RFID. Posteriormente al acercar la etiqueta al dispositivo registrara que el tag que tiene el usuario esté previamente activada para permitirle el ingreso del caso contrario se lo negara. Este dispositivo tiene capacidad para registrar hasta 65 536 tarjetas de identificación relacionados a usuarios cada uno con sus propia información personal.

El dispositivo fue diseñado en base a un lector de tecnología RFID (identificación por radio frecuencia), un microcontrolador, un dispositivo Bluetooth y el desarrollo de un programa. Este último se usó para el control de todo el sistema. En el diseño se tuvieron en cuenta consideraciones de fácil manejo y capacidad de almacenamiento.

En este proyecto se realizaron pruebas con el objetivo de determinar la característica de funcionamiento y desempeño del dispositivo.

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

CAPITULO 1

TECNOLOGÍA RFID

RFID (Radio Frequency IDentification, en español Identificación por radiofrecuencia) es un sistema de almacenamiento y recuperación de datos remoto que usa dispositivos denominados etiquetas, transpondedores o tags RFID. El propósito fundamental de la tecnología RFID es transmitir la identidad de un objeto (similar a un número de serie único) mediante ondas de radio sin necesidad de contacto, ni siquiera visual. Las tecnologías RFID se agrupan dentro de las denominadas Auto ID (Automatic Identification, o Identificación Automática).

Una etiqueta RFID es un dispositivo pequeño, que consiste en un microchip que va adjunto a una antena de radio y que sirve para identificar unívocamente al elemento portador de la etiqueta.

Los microchips en las etiquetas RFID pueden ser o bien de lectura o bien regrabables, teniendo éstos más posibilidades ya que puede variarse su información o aumentarse la misma, lo cual es muy útil para realizar seguimiento de los objetos que portan la etiqueta como estudios biométricos en animales, movimientos en las cadenas de fabricación y montaje, etc. [5]

1.1. HISTORIA

El origen de RFID está relacionado con la guerra, concretamente con la II Guerra Mundial, en la que el uso del radar permitía la detección de aviones a kilómetros de distancia, pero no su identificación. El ejército alemán descubrió que si los pilotos balanceaban sus aviones al volver a la base, cambiaría la señal de radio reflejada de vuelta. Este método hacía así distinguir a los aviones alemanes de los aliados y se convirtió en el primer dispositivo de RFID pasivo.

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 IRÉ, pp. 1196-1204, octubre de 1948).

Los sistemas de radar y de comunicaciones por radiofrecuencia avanzaron en las décadas de los 50 y los 60. Las compañías pronto comenzaron a trabajar con sistemas antirrobo que usando ondas de radio y determinaban si un objeto había sido pagado o no a la salida de las tiendas. Se utilizaba una etiqueta en la que un único bit decida si se ha pagado o no por el objeto en cuestión. La etiqueta pasaba a través de sensores colocados a la salida y se sonaba una alarma si el objeto no se había pagado.

Las primeras patentes para dispositivos RFID fueron solicitadas en Estados Unidos, concretamente en enero de 1973 cuando Mario W. Cardullo se presentó con una etiqueta RFID activa que portaba una memoria re escribible. El mismo año, Charles Walton recibió la patente para un sistema RFID pasivo que abría las puertas sin necesidad de llaves. Una tarjeta con un *transponedor* comunicaba una señal al lector de la puerta que cuando validaba la tarjeta desbloqueaba la cerradura.

El gobierno americano también trabajaba sobre esta tecnología en los años 70 y montó sistemas parecidos para el manejo de puertas en las centrales nucleares, cuyas puertas se abrían al paso de los camiones que portaban materiales para las mismas que iban equipados con un transponedor. También se desarrolló un sistema para el control del ganado que había sido vacunado insertando bajo la piel de los animales una etiqueta RFID pasiva con la que se identificaba los animales que habían sido vacunados y los que no. Después se han producido mejoras en la capacidad de emisión y recepción, así

como en la distancia, lo cual ha llevado a extender su uso en ámbitos tanto domésticos como de seguridad nacional, como sucede con el pasaporte expedido en la actualidad en los EEUU que lleva asociadas etiquetas RFID. [5]

1.2. FUNCIONAMIENTO

Un sistema típico de RFID está constituido por tres componentes principales: tags, lectores y antenas, ver figura 1.1. Un tag RFID está compuesto por un microchip y una antena flexible instalada sobre una superficie plástica. El lector es utilizado para leer y escribir información en el tag, (actualmente, el formato más común para tags es una etiqueta adhesiva de identificación).

A continuación se detalla en forma general el funcionamiento de un sistema típico de RFID.

- El interrogador o lector genera un campo de radiofrecuencia, normalmente conmutando una bobina a alta frecuencia. Las frecuencias usuales van desde 125 Khz hasta la banda ISM de 2.4 Ghz, incluso más.
- El campo de radiofrecuencia genera una comente eléctrica sobre la bobina de recepción del tag. Esta señal es rectificada y de esta manera se alimenta el circuito.
- Cuando la alimentación llega a ser suficiente el circuito transmite sus datos.
- El interrogador detecta los datos transmitidos por el tag como una perturbación del propio nivel de la señal.
- Los datos recibidos por el lector pueden ser enviados a un ordenador para su respectivo procesamiento.
- El ordenador instruye al lector.
- El lector puede transmitir datos al tag.

La distancia dentro de la cual un lector puede comunicarse con una etiqueta se llama *rango de lectura*. Las comunicaciones entre lectores y etiquetas están gobernadas por protocolos y estándares emergentes, ver subtema 1.4.2.

Figura 1.1 Comunicación entre Tag y Lector

Podemos encontrar además dos tipos de interrogadores diferentes:

- Sistemas con bobina simple, la misma bobina sirve para transmitir la energía y los datos. Son más simples y más baratos, pero tienen menos alcance.

- Sistemas interrogadores con dos bobinas, una para transmitir energía y otra para transmitir datos. Son más caros, pero consiguen unas prestaciones mayores. [8]

1.2.1. FRECUENCIA DE OPERACION

Es la frecuencia electromagnética que utiliza el tag y el lector para comunicarse y obtener energía. El espectro electromagnético para RFID opera normalmente en baja frecuencia (LF -- Low Frecuency), alta frecuencia (HF -- High Frecuency), ultra alta frecuencia (UHF - Ultra High Frecuency) o microondas, ver tabla 1.1. Los dispositivos RFID están regulados como un dispositivo radio porque emite ondas electromagnéticas (Broadcast).

Nombre (Rango de Frecuencias)	Frecuencias ISM
LF (30 – 300KHz)	< 135KHz
HF (330 MHz)	6,78MHz, 13,56MHz, 27,125 MHz, 40,68 MHz
UHF (300 MHz – 3GHz)	433,9MHz, 869MHz, 915 MHz
Microondas (>3GHz)	2,45GHz, 5,8 GHz, 24,125GHz

Tabla. 1.1 Frecuencias de Operación de RFID

Actualmente, en la práctica, las frecuencias disponibles para dispositivos RFID están limitadas a bandas ISM (Industrial Scientific Medical) ver subtema 1.4.1. Las frecuencias menores a 135 kHz no forman parte de esta banda libre pero se puede utilizar en sistemas RFID porque utilizan el campo magnético para operar en cortos rangos de lectura, que no interfiere a ningún otro dispositivo.

Los organismos reguladores de las distintas partes del mundo han escogido diferentes rangos UHF. En Europa, Sud América y algunos sitios de Asia, se opera en la frecuencia 868 MHz (865,6 – 867,6 MHz). En Norte América en 915 MHz (902-928 MHz), en cambio en la India han adoptado recientemente la banda comprendida entre 865-867 MHz. China aún no ha especificado la banda frecuencia que regulará para el uso de RFID pero soportará los estándares globales. [9]

Existen actualmente diversos sistemas de RFID operando en distintas frecuencias, y cada uno de ellos presenta ventajas y desventajas en relación a los otros, por lo que resulta necesario analizar la aplicación, para determinar cuál de ellos se adapta mejor a las condiciones y exigencias que se planteen, algunas de estas ventajas se presentan a continuación:

Frecuencia Baja (9 - 135 kHz), su principal ventaja es su aceptación en todo el mundo al estar ampliamente difundida. Es el sistema menos susceptible a los líquidos y metales, su velocidad de comunicación es baja, lo que lo hace deficiente para operar en entornos donde haya más de un tag presente en el campo de la antena. Su rango máximo

de lectura no supera los 150cms y su utilización más frecuente está asociada a controles de accesos e identificación de animales, barriles de cerveza, auto key and lock o bibliotecas, etc.

Frecuencia Alta (13,56 MHz), esta frecuencia también está muy difundida, pero a diferencia de la frecuencia baja, la alta no funciona cerca de los metales. Su respuesta en presencia de líquidos es buena, la velocidad de comunicación es aceptable para sistemas estáticos o de baja velocidad, su rango máximo de lectura es alrededor de un metro, sus principales aplicaciones se encuentran en librerías, identificación de contenedores, tarjetas inteligentes, trazabilidad de los productos, movimientos de equipajes de avión o acceso a edificios.

Frecuencia Ultra-alta (433 MHz y 860-960 MHz), sus principales inconvenientes se encuentran en la interferencia provocada por metales y líquidos. Otro punto negativo es la imposibilidad de estandarizar la frecuencia, dado que cada país legisla esta banda con distintas limitaciones. Entre sus puntos positivos está el rango de lectura (que alcanza hasta 9 metros), su velocidad de lectura (1200 Tags/seg.) y el bajo costo de los tags (se espera llegar a los 5 centavos por unidad). Sus principales aplicaciones se encuentran en la cadena de abastecimientos, tele-peajes e identificación de bultos pallets y equipajes.

Frecuencia de microondas en la banda UHF (2,45 GHz y 5,8 GHz), estas frecuencias son las más habituales para los tags activos, y no tienen el problema de la falta de regulaciones globales. Si bien su velocidad de transmisión es buena, su rango de lectura no es mayor a 2 metros. Este tipo de sistemas no se encuentran muy difundidos y su aplicación principal se encuentra en sistemas de tele-peaje. Los tags activos que operan en el rango de las microondas son muy usados para seguimiento y trazabilidad de personas u objetos.

1.2.2. MODO DE COMUNICACIÓN

Entre las varias maneras de clasificar a los tags es por el tipo de comunicación, entre el tag y el lector. Al igual que las comunicaciones por cables, las inalámbricas pueden ser Full-duplex (FDX), en que el lector y el tag pueden hablar simultáneamente

o Half-Duplex (HDX) en que es necesario turnos. En la mayoría de ocasiones, para los tags pasivos, es necesario que el lector proporcione la energía para que el tag inicie la comunicación, pero hay una variación en la comunicación HDX, gracias a capacitadores o propiedades físicas que permiten al tag almacenar energía y responder mientras el lector no emite señal, ver figura 1.2. [12]

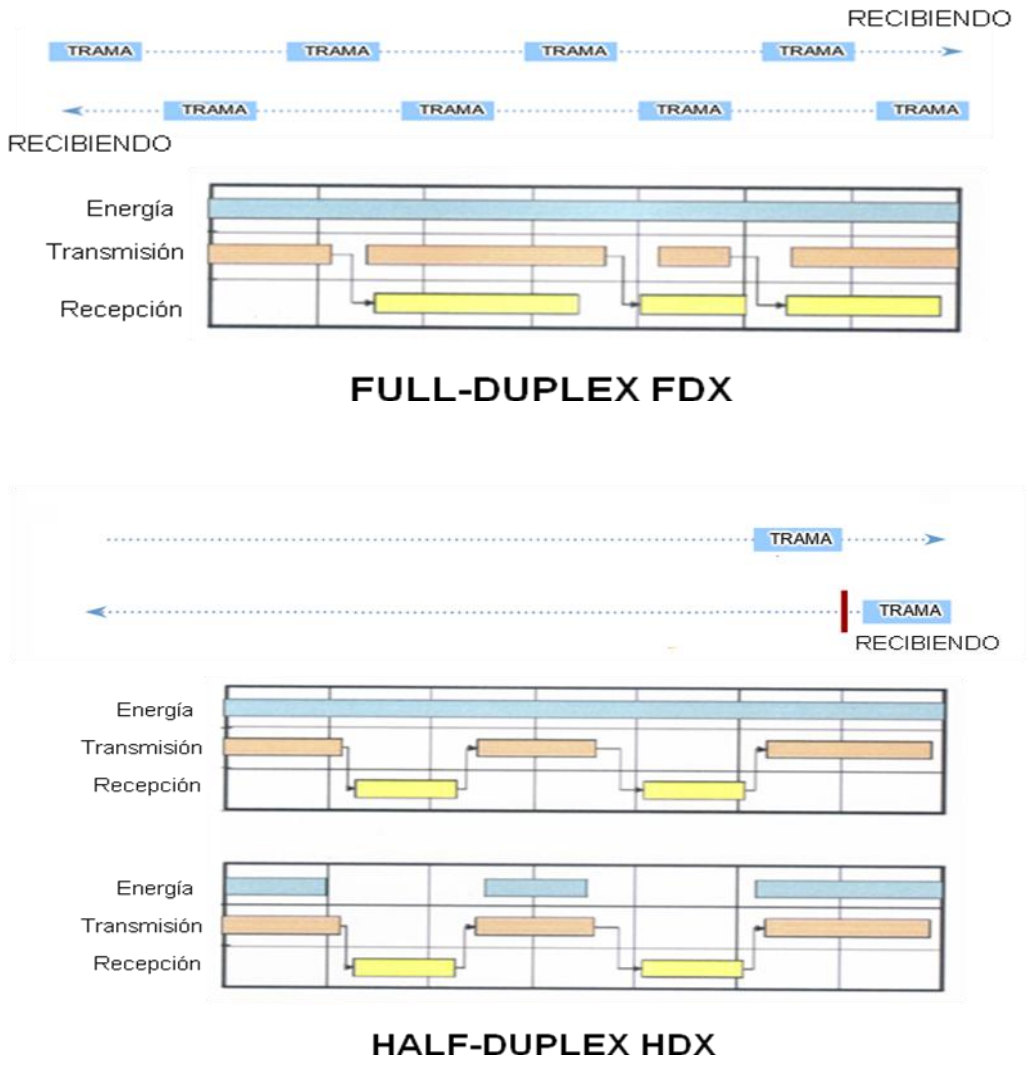


Figura 1.2 Modos de Comunicación

1.2.3. ACOPLAMIENTO

El mecanismo de acoplamiento del tag determina como los circuitos del tag y el lector se influencian y reciben la información o energía. El tipo de acopiamiento que el tag utiliza afecta directamente al rango de lectura entre los dos dispositivos (tag y lector). Podemos agrupar los diferentes rangos de lectura en diferentes sistemas: el

rango de lectura es cerrado en distancias menores a un centímetro, remotas entre 1 cm. y 1 m. o de largo alcance (rango de distancia) para más de 1 metro. El acoplamiento remoto es más conocido como "*vicinity coupling*". En el acoplamiento capacitivo (no muy utilizado) o magnético son ejemplos de acoplamiento cerrado, para el acoplamiento remoto se utiliza acoplamiento inductivo, y el acoplamiento "*backscatter*" es de largo alcance.

A lo largo de estos rangos, las diferentes opciones de acoplamiento se ven afectadas fuertemente por la frecuencia que el tag utiliza en su comunicación. El acoplamiento inductivo trabaja en las mejores condiciones en el rango de frecuencias de 100 kHz y 30 MHz, que comprenden las bandas LF y HF para RFID.

1.2.3.1. Acople por Dispersión Electromagnética (Backscatter coupling):

Los sistemas RFID con una distancia mayor a un metro entre el lector y el tag se denominan *long-range systems* (sistemas de largo alcance). Este tipo de acoplamiento es el utilizado en los sistemas RFID en UHF. Su nombre, *backscatter* (Scatter significa dispersar) describe el camino de las ondas de radiofrecuencia transmitidas por el lector y que son devueltas por el tag mediante dispersión. El término backscatter es usado actualmente para describir que los tags reflectan la señal con la misma frecuencia emitida por el lector pero cambiando la información contenida en ella. El acoplamiento consiste en reflejar la señal para enviarla al origen.

Como el lector y el tag usan la misma frecuencia para comunicarse, utilizan turnos para transmitir datos. Así el tipo de comunicación, tal y como se ha descrito anteriormente, es Half-Duplex (HDX). Pero el lector continúa proporcionando energía al tag mientras espera recibir la respuesta del tag.

A continuación se analiza el funcionamiento de este tipo de acople en términos técnicos, primero, la potencia Pl es emitida por la antena del lector, una pequeña proporción Pl' (teniendo en cuenta la atenuación espacial) alcanza la antena del tag. La potencia Pl' es suministrada a la antena como un voltaje de alta frecuencia y este puede ser usado para alimentar el circuito, ver figura 1.3

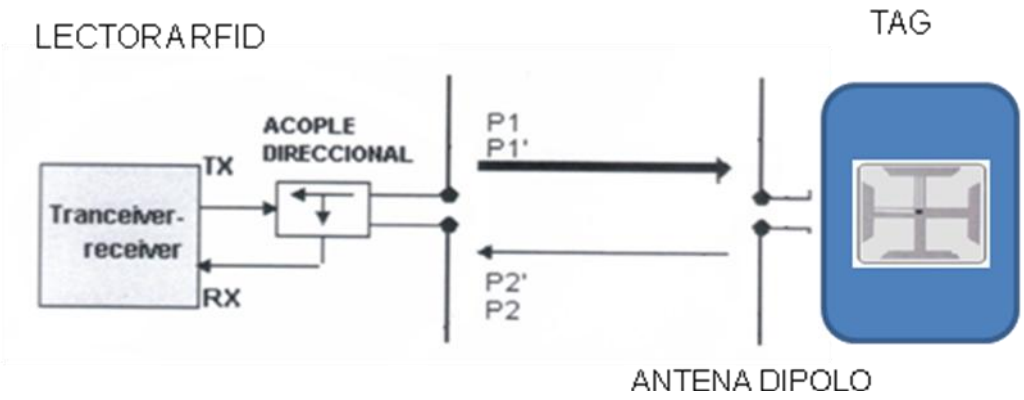


Figura 1.3 Dispersión Electromagnética

Una proporción de la potencia entrante P1’ es reflejada por la antena y devuelta como potencia P2, teniendo en cuenta, que las características de reflexión de la antena pueden estar influenciadas por el cambio de la carga conectada a ella. Para transmitir datos del tag al lector, así la amplitud de la potencia P2 reflejada del tag es modulada.

La potencia P2 reflejada del tag es irradiada, una pequeña proporción de esta P2' (debido a la atenuación espacial) es recibida por la antena del lector, la señal reflejada viaja hacia la antena del lector en "contrafase" y puede ser desacoplada utilizando un acoplador direccional y transferida a la entrada de receptor del lector.

1.2.3.2. Acoplamiento Inductivo (inductive couplmg):

Es el más común para tipos de acoplamiento remoto. Un ejemplo serían los tags que soportan o se rigen por el estándar ISO 15693. El lector proporciona energía por acoplamiento inductivo a los tags mediante antenas en forma de bobina para generar campo magnético.

Los tag inductivamente acoplados casi siempre son manejados pasivamente. Esto quiere decir que toda la energía necesaria para la operación del microchip tiene que ser proporcionada externamente por el lector. Por esta razón, el embobinado de antena del lector genera un campo electromagnético fuerte, de alta frecuencia, que penetra el área de corte transversal del embobinado y el área alrededor de éste. Como la longitud de onda de la frecuencia usada (<135 kHz: 2400 m, 13,56 MHz: 22,1 m) es varias veces

mayor que la distancia entre la antena del lector y el tag, el campo electromagnético puede ser tratado como un campo magnético AC teniendo en cuenta la distancia entre el tag y la antena. Esto es válido cuando la distancia entre los embobinados no excede 0.16λ, λ es longitud de onda, de modo que el tag sea localizado en el campo cercano de la antena de transmisor.

Por inducción, se genera un voltaje Vi en el embobinado de la antena del tag. Este voltaje es rectificado y sirve como la fuente de energía para los datos que llevan el dispositivo (microchip). Un condensador Cl es conectado en paralelo con el embobinado de antena del lector, la capacitancia es seleccionada de tal forma que, con la inductancia de embobinado de antena, forme un circuito paralelo resonante, con una frecuencia de resonancia que corresponde con la frecuencia de transmisión del lector, ver figura 1.4.

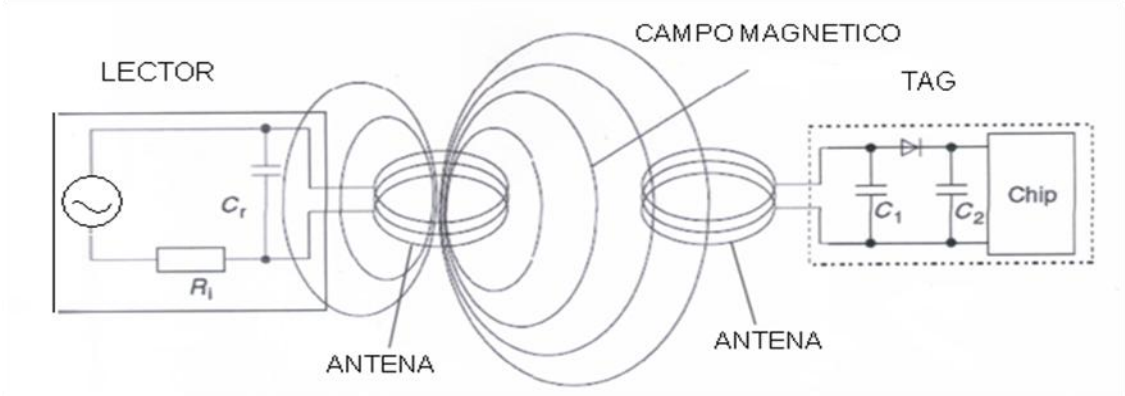


Figura. 1.4. Acople inductivo

La conmutación de una resistencia de carga en la antena del tag efectuará cambios de voltaje en la antena del lector y así tiene el efecto de una modulación en amplitud del voltaje de antena por el tag remoto. Si la conmutación de la resistencia de carga es controlada por los datos, entonces estos datos pueden ser transferidos del tag al lector. Este proceso se denomina modulación de carga.

Para adquirir los datos en el lector, el voltaje medido en la antena del lector es rectificado, esto representa la demodulación en amplitud de la señal.

1.2.3.3. Acoplamiento Magnético (magnetic coupling):

El acoplamiento electromagnético es similar al acoplamiento inductivo cuando nos referimos que el tag y el lector forman un par de transformadores mediante bobinas. La mayor diferencia se encuentra en la antena del lector que consiste en una bobina enrollada en una pieza de ferrita con los dos extremos al aire. El sistema esta diseñado para unos rangos de lectura entre 0,1 cm. y 1 cm. como máximo

1.3. LOS TAGS DE RFID

Un tag RFID es un elemento que puede almacenar y transmitir información hacía un elemento lector utilizando ondas de radio. El propósito de un tag RFID o etiqueta inteligente es poder adherir a un objeto información de este (ítem). Los tags pueden ser clasificados de diferentes formas según sus características, las cuales se tratan mas adelante en este capítulo. Un aspecto muy importante a tener en cuenta es que no todos los tags tienen microchip o fuente de alimentación interna, pero si es cierto que todos ellos contienen una bobina o antena, estas últimas pueden tener multiles formas. [15]

A pesar de que los chips que poseen los tags son pequeños, las antenas no lo son. Ellas necesitan ser lo suficientemente grandes para captar la señal emitida por el lector. El tamaño de la antena tiende a determinar el tamaño de una etiqueta RFID.

La figura 1.5 ilustra un diseño típico de un tag. El chip de baja potencia maneja la conversión de energía, el control lógico, el almacenamiento y recuperación de datos y la modulación requerida para devolver los datos al lector.

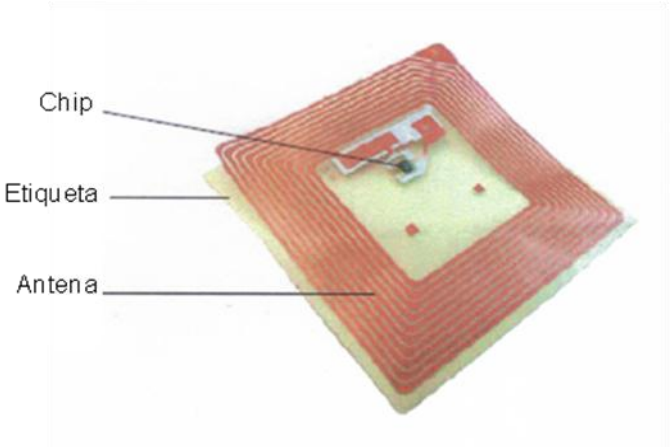


Figura. 1.5. Circuito inteligente

A continuación se muestra ejemplos de los diferentes diseños de antenas optimizadas para varias aplicaciones. Las antenas pueden ser fabricadas de aluminio, cobre u otros materiales, y son creadas por técnicas de disposición de materiales similares a la inyección de tinta sobre una hoja. Figura 1.6.

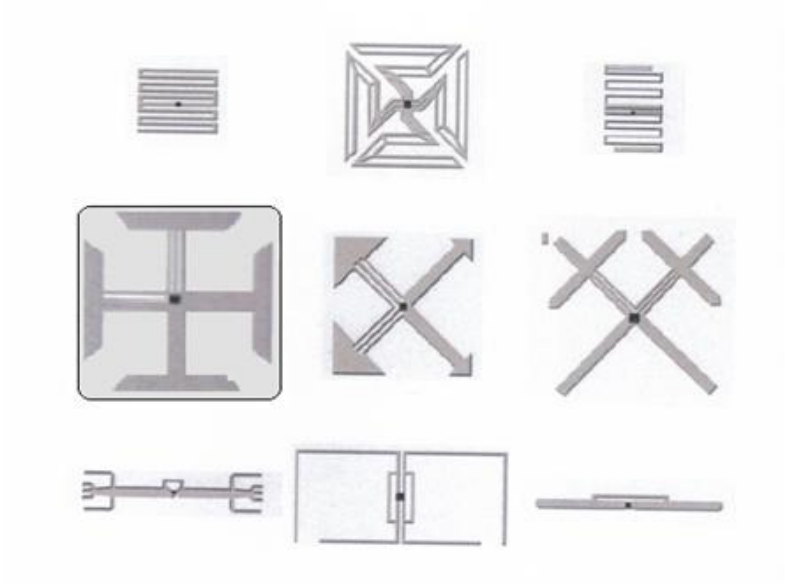


Figura 1.6. Diseños de Antenas

Las etiquetas están disponibles actualmente en cantidades industriales con varios formatos: como inlays puros, inlays con adhesivo de respaldo, insertados en etiquetas sin impresión, o como productos convertidos, donde la etiqueta está encapsulada dentro de plástico, caucho u otro material diseñado a medida, ya sea moldeado o laminado.

Las antenas de las etiquetas están diseñadas para soportar un amplio rango de condiciones. Las antenas de dos dipolos son menos sensibles a la orientación física de la fuente que las de un solo dipolo. Otras etiquetas están diseñadas para un rango de condiciones específicas, como la legibilidad cercana a metales. Las antenas de las etiquetas pueden ser optimizadas para ser leídas por un tipo específico de lector, o con una antena ubicada en una posición particular. [16]

Es necesario tomar en consideración los materiales en los que se ha de ubicar los tags, o los materiales cercanos en el momento de lectura y escritura en los tags, ya que las ondas de radio frecuencia tienen diferentes comportamientos dependiendo de los materiales con que interactúan. La tabla 1.2 muestra efectos en las ondas de radio frecuencia en algunos materiales.

COMPOSICIÓN DEL MATERIAL	EFECO EN LA ONDA RF
Inserción en la piel	Absorción, Reflexión
Líquidos Conductores	Absorción
Metales	Reflexión
Plásticos	Efecto Dieléctrico
Cartón Ondulado	Humedad Absorción

Tabla. 1. 2. Efectos en la Onda RF [19]

1.3.1. CARACTERÍSTICAS BÁSICAS

Los tags tienen características o capacidades muy diferentes, por lo que podemos realizar múltiples clasificaciones que nos ayuden a entender como afectan a su comportamiento o modo de trabajo. Podríamos clasificar tags según su tipología (activo, pasivo y semiactivo), por su tipo de memoria, capacidad de almacenamiento, origen de alimentación, frecuencias de trabajo, características físicas, protocolo de interfaz aérea (cómo se comunica con el equipo lector) y así sucesivamente con casi todas las características. Clasificar los tags según todas estas características, nos permite obtener

una guía para encontrar el mejor tipo de tag para cada una de las aplicaciones o proyectos. [15]

Hay muchas características básicas que pueden modificar el comportamiento de un tag RFID, algunas comunes a todos los tags (requerimientos mínimos que todos deben cumplir) y otras que sólo se encuentran según modelo o tag.

Adherir el tag: cualquier tipo de tag debe tener un mecanismo adhesivo o mecánico para adjuntarlo al objeto.

Lectura del tag: cualquier tag debe poder comunicar la información mediante radiofrecuencia.

Kill/Disable: algunos tags permiten al lector enviar un comando (orden) para que deje de funcionar permanentemente, siempre y cuando reciba el correcto "Kill code". Esto provoca que no responda nunca más.

Write many: algunos tags tienen la capacidad de poder escribir y reescribir tantas veces como se desee en el campo de datos del identificador (normalmente hay un límite de ciclos muy elevado, como por ejemplo 100.000 escrituras).

Anticolisión: Cuando hay muchos tags próximos a un lector, este puede tener la dificultad de hablar o comunicarse con ellos a la vez. La característica anticolisión permite a los tags conocer cuando debe transmitir para no entorpecer o molestar otras lecturas. Esta característica se realiza mediante protocolos que permiten controlar las comunicaciones entre tag y lector.

Seguridad y encriptación: algunos tags permiten encriptar la información en la comunicación, además hay la posibilidad en varios tipos de estos tags que permiten responder solo a lectores que les proporciona un password secreto.

1.3.2. ENCAPSULADOS DE LAS ETIQUETAS

Los tags RFID toman multitud de formas y tamaños según los diferentes entornos, donde deben utilizarse, esta característica de adaptación proporciona un elevado surtido de tags. Además estos pueden estar encapsulados en diferentes tipos de material. Se pueden encapsular en plástico (normalmente PVC), o botones para obtener mayor durabilidad, sobretodo en aplicaciones de ciclo cerrado donde se tiene que reutilizar o en ambientes hostiles. También pueden estar insertadas en tarjetas de plástico como las de crédito, este tipo se denominan "contactless smart cards", o láminas de papel (similar a los códigos de barra), que reciben el nombre de "smart labels".

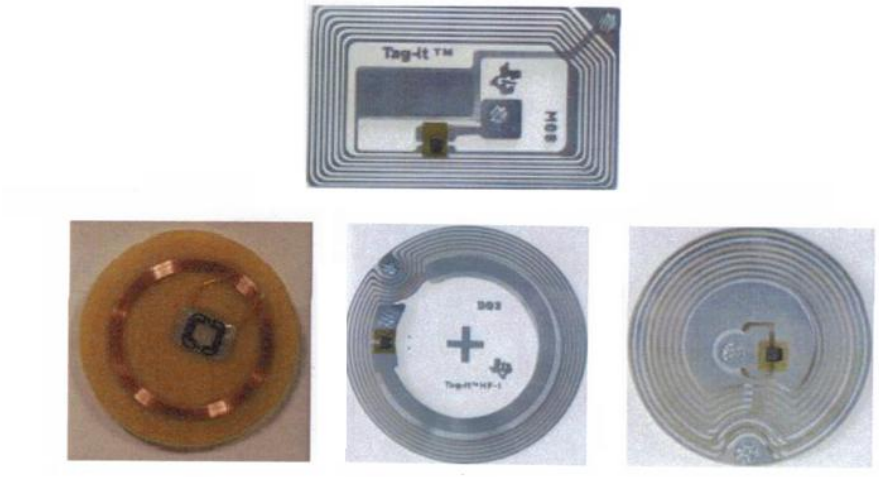


Figura 1.7 Tipo de Encapsulados

Cómo último destacamos los encapsulados de cerámica especialmente idóneos en entornos corrosivos, líquidos o para incrementar la protección, el embalaje o encapsulado del tag puede ser una de las características más visuales para clasificarlos, además es una característica que afecta directamente a cómo se adhiere. [18]

1.3.3. ORIGEN DE LA ALIMENTACIÓN O FUENTE DE ENERGÍA

Una de las clasificaciones más comunes es por el origen de la energía, batería o fuente de alimentación. Esta característica es uno de los principales factores que determina la durabilidad y el costo de los mismos. Pueden ser pasivas si no tienen

fuente de alimentación propia, semi-pasivas si utilizan una pequeña batería asociada y activas si tienen su propia fuente de alimentación. [5]

1.3.3.1. Tags Pasivos

Las etiquetas RFID pasivas no requieren batería ya que toda la energía que el circuito integrado necesita para poder transmitir una respuesta la recoge del campo electromagnético creado por el lector. Las etiquetas pasivas, en la práctica tienen distancias de lectura que varían entre unos 10 milímetros hasta 6 metros dependiendo del tamaño de la antena de la etiqueta, de la potencia y frecuencia en la que opera el lector. Estas etiquetas tienen la ventaja de poder ser mucho más pequeñas que las etiquetas activas. La forma de la etiqueta dependerá del uso que se vaya a hacer de las mismas. Como es de suponer son los más económicos y los de menor rango de comunicación, pero por su relación entre comportamiento y precio son los más utilizados. [20] [21] [22]

1.3.3.2. Tags Semi-pasivos

Las etiquetas RFID semi-pasivas incluyen una batería para activar la circuitería del chip pero la energía para generar la comunicación es la que recoge de las ondas radio del lector (como en los pasivos). Esto da lugar a que las antenas no requieran capturar la potencia de la señal entrante para devolver la señal saliente, sino que las antenas son mejoradas para la emisión de la respuesta. [20] [21] [22]

1.3.3.3. Tags Activos

Tiene una propia batería para el suministro de la energía. Dicha energía es utilizada para activar la circuitería del microchip y enviar la señal a la antena. Permiten una amplia cobertura de difusión, es decir, mayor alcance. Normalmente tienen una mayor capacidad de almacenar información. También pueden llevar sensores adicionales a la propia memoria como sensores de temperatura, de velocidad, de movimiento, etc. que permiten almacenar o controlar datos vitales en algunas aplicaciones. Actualmente, Su tamaño es mayor que los otros dos tipos de etiquetas, aunque las etiquetas activas más pequeñas tienen un tamaño aproximado de una

moneda. Muchas etiquetas activas tienen rangos prácticos de diez metros a cien metros, y una duración de batería de varios años. Se puede usar como un *transponedor*. [20] [21] [22]

1.3.4. CLASES DE TAGS

A continuación se dará las características de la capacidad de los Tags Cada clase tiene más capacidades que la anterior y es compatible con las anteriores. [23] [35]

- **Primera clase** seria un tag sencillo, pasivo, de solo lectura, con memoria no volátil programable solo en su fabricación
- **Segunda clase** seria un tag sencillo, pasivo, de solo lectura, con memoria no volátil programable.
- **Tercera clase** seria un tag pasivo, con memoria de lectura/escritura de hasta 65KB
- **Cuarta clase** seria un tag semi-pasivo, de solo lectura, con memoria no volátil programable, un batería adicional que aumentara su alcance
- **Quinta clase** seria un tag que utilice una batería para alimentar su circuitería, aumentando así las potencias transmitidas hacia un lector RFID
- **Sexta Clase** Sería un tag activo que puede comunicar con otro tag de clase cinco y/o otros dispositivos

1.4. NORMAS DE REGULACIÓN Y ESTANDARIZACIÓN

1.4.1. CONSIDERACIONES DE FRECUENCIA

Los sistemas RFID que generan e irradian ondas Electromagnéticas. La función de otros servicios de radio, en ningún caso debe ser interrumpida o perjudicada por la operación de los sistemas RFID. Es en particular importante asegurar que los sistemas RFID no interfieran con la radio cercana y con servicios de radio y televisión, móviles, servicios de radio marítimos y aeronáuticos.

La necesidad de ejercer el cuidado con respeto a otros servicios de radio restringe considerablemente la gama de frecuencias convenientes de operaciones disponibles a un sistema RFID. Por esta razón, usualmente solo es posible usar intervalos de frecuencia reservados específicamente para aplicaciones industriales, científicas o médicas o para dispositivos de corto alcance. Estas son frecuencias clasificadas mundialmente como ISM (Industrial-Scientifíc-Medical) o SRD (Short range devices).

1.4.2. Estándares

Como toda nueva tecnología, uno de los temas principales para su adopción a gran escala son la definición de estándares que garanticen la interoperabilidad y la disposición de soluciones no ligadas a un solo proveedor, que permite a la empresa obtener cierta libertad de decisión. Claro esta que cuando nos encontramos en aplicaciones que solo implican a una sola empresa no hay necesidad de existencia de estándares, pero si esta debe colaborar con otros agentes e intercambiar información, se hace imposible realizarlo sin un estándar que defina como comunicarse para que todo el mundo lo entienda. En este tipo de sistemas, normalmente, se ven involucrados en los estándares aspectos físicos del tag y la interfaz aérea. Los estándares principales en los sistemas RFID los podríamos desglosar en dos:

- estándares de EPCglobal, empresa que desarrolla estándares industriales para el código de producto electrónico EPC (Electronic Product Code).
- La Organización Internacional para la Estandarización o International Organization for Standardization (ISO). [24]

Entre las cosas que se estandarizan están las siguientes:

Tecnología: Estándares para tecnología aseguran interoperabilidad de componentes de sistemas comunes.

Conformidad: La tecnología debe estar conforme a las mejores prácticas y métodos del estándar aceptado.

Desenvolvimiento: Los lectores y tags deben ser evaluados de acuerdo a ciertos niveles del estándar.

ISO, es una ONG constituida por una red de institutos nacionales de estándares en 146 países, cuya aportación es igualitaria (1 miembro por país). El organismo tiene una central de coordinación en Genova (Suiza). En general, los estándares de los tag ISO (15693, 14443, 18000-6) usan el siguiente formato [26] [37]:

Dimensiones físicas: Define tamaños, niveles de luz ultravioleta, rayos X, temperaturas, campos eléctricos y magnéticos a los cuales el tag debe funcionar en forma adecuada.

Interfaz aérea e inicialización: Define valores de frecuencia y campo de operación, tipo de modulación, tipo de codificación, velocidad de transmisión y definición tramas de inicio y teminación.

Anticolisión y protocolo de comunicación: Define la organización de la memoria del tag, la organización de los datos en la memoria, el identificador único (UID), bloque de datos, describe el mecanismo para intercambiar instrucciones y datos entre el lector y el tag, el proceso de anticolisión, especificaciones de tiempo, define grupo de comandos.

Estándar EPCglobal permite una compatibilidad mundial de este protocolo en banda UHF. Su producción estándar permite leer 1500tag/s en Norteamérica, y 600 tags/s en Europa. La diferencia se debe principalmente a la diferencia de ancho de banda asignada en cada una de las regiones para el estándar. Tiene un control de privacidad y acceso integrado (no es muy potente, pero está presente). Existen funciones de des habilitación de tags (función Kill tag), y se puede proteger el acceso al tag mediante una contraseña. [36]

1.4.3. OTROS ESTÁNDARES

AIAG (Automotive Industry Action Group): Se trata de una asociación no lucrativa encargada de reducir costes y complejidad en el entorno de la automatización

de cadenas de producción. He aquí uno de los estándares bastante conocido en el mundo de los fabricantes/productores que trabajan con RFID:

AIAG B-ll. Estándar para ruedas utilizando RFID. La versión actual incluye un EPC de 96bits en el marco del protocolo EPCglobal.

ANSÍ (American National Standards Instituté): Se trata de un organismo privado con fines no lucrativos que administra y coordina el organismo de estándares americano. Su misión es asegurar tanto la competitividad como la calidad de los productos fabricados en USA promoviendo una serie de normas que lo garanticen. He aquí algunos estándares del ANSÍ relativos al RFID.

ANS INCITS 256-2001: Estándar que promueve la interoperabilidad de sistemas RFID en las bandas frecuenciales libres internacionales y desde el punto de vista de las potencias permitidas.

ANS INCITS 371. Información relativa a la localización en tiempo real. Posee 3 partes con los interfaces aire a 2.4GHz y a 433MHz, y además incluye normas acerca de la interfaz de programación de aplicaciones sobre los mismos.

ANS MH10.8.4. Estándar sobre contenedores plásticos reutilizables. Es compatible con la norma ISO 17364.

EAN (European Anide Number)/UCC: Es el encargado de estandarizar números de identificación, conjuntos de transacción EDI, esquemas en XML, y otras soluciones eficientes para aplicaciones en cadenas de producción. Es un organismo muy importante.

El Uniform Code Council (UCC) es una organización no comercial dedicada al desarrollo e implementación de soluciones basadas en estándares. El EPC pertenece a este último. Su misión es crear estándares abiertos y globales. GTAG (Global TAG) da información técnica así como guías de aplicación, facilita a cadenas productivas a escala mundial en el trabajo en las bandas 862-928 MHz (UHF).

ETSI (European Telecommunicaüons Standards Instituté): Es la organización europea no comercial que se dedica a estandarizar normas en el campo de las telecomunicaciones. Al igual que otros organismos internacionales, solo diremos que tiene una lista exhaustiva de sus propias normativas referentes al RFID. [27]

1.5. APLICACIONES DE LA TECNOLOGÍA RFID

La tabla 1.3 presenta diferentes aplicaciones de esta tecnología de acuerdo a las frecuencias de operación. [28]

TAG RFID BAJA FRECUENCIA	TAG RFID ALTA FRECUENCIA	TAG RFID UHF
Identificación de Animales	Bibliotecas	Seguimientos de Envases
Seguimiento de Barriles	Control en Equipaje Aéreo	Seguimientos de Camionetas
Antirrobo	Pacientes en Hospital	Seguimientos de envíos
Control de Acceso	Seguimientos de Libros	Control de Acceso de Vehículos
Pasaportes	Identificación Acreditaciones	
Carné de conducir	Control Acceso Edificios	

Tabla 1.3. Aplicaciones de acuerdo a la frecuencia de operación

1.6. VENTAJAS Y DESVENTAJAS

Actualmente el RFID presenta tanto ventajas como desventajas, que se resumen en la tabla 1.4.

En la tabla 1.4, se observa una relación estrecha con las tarjetas inteligentes. Sin embargo, el RFID enfrenta mejor todas las situaciones involucradas con el contacto que se manifiestan a través de los riesgos por sabotaje, sociedad, unidireccionalidad, entre otros. [29]

[1] El riesgo puede reducirse eligiendo los textos con un generador aleatorio, si el texto conocido con antelación.

[2] Sólo aplica a identificación de huella digital. En el caso de lectura de retina o de iris necesario o posible.

Parámetros del sistema	Código de barras	OCR	Reconocimiento de voz	Biometría	Magnética	RFID
Cantidad de bytes	1-100	1-100	-	-	16-64 k	16-64 k
Densidad de data	Baja	Baja	Alta	Alta	Muy alta	Muy alta
Lectura con máquinas	Buena	Buena	Cara	Cara	Buena	Buena
Capacidad de lectura humana	Limitada	Simple	Simple	Difícil	Imposible	Imposible
Influencia de suciedad / humedad	Muy alta	Muy alta	-	-	Posible (contacto)	No influye
Influencia de coberturas	Falla total	Falla total	-	Posible	-	No influye
Influencia de la dirección y posición	Baja	Baja	-	-	Unidíreccional	No influye
Degradación por uso	Limitada	Limitada	-	-	Por el contacto	No influye
Costo de dispositivo de lectura	Muy bajo	Medio	Muy alto	Muy alto	Bajo	Medio
Gastos de operación de lectura (por ejemplo, por desgaste, por reemplazos, por impresiones)	Bajo	Bajo	No hay	No hay	Medio	No hay
Copiado no autorizado/alteraciones Bajo condiciones normales de control	Simple	Simple	Posible[1] (cinta de audio)	Imposible	Imposible	Imposible
Velocidad de lectura, incluye la manipulación del portador de datos (el artículo), a registrar	Baja 4s	Baja 3s	Muy baja >3s	Muy baja >5-10s	Baja 4s	Muy rápida 0.5s
Máxima distancia entre la lectora y el portador de datos	0-50 cm	<1 cm Scanner	0-50 cm	Contacto directo[2]	Contacto directo	0-5 m, microondas

Tabla. 1. 4. Comparación de diferentes sistemas

1.6.1. VENTAJAS

En la tabla 1.5 se muestra ventajas del sistema RFID con respecto al código de barras.

Características	Código de barras	RFID
Capacidad	Espacio limitado	Almacena mayor cantidad de información sobre el producto
Identificación	Estandarizada	Unívoca por
Actualización	Sólo lectura	Lectura / escritura, la actualización de información de un ítem se hace en tiempo real
Flexibilidad	Requiere línea de visión para la lectura	No requiere línea de visión para lectura, identifica objetos en movimiento y es reutilizable
Lectura	Una lectura por vez	Lectura
Tipo de lectura	Lee sólo en superficie	Emite la información en toda dirección y lee a través de diversos materiales y
Precisión	Requiere intervención humana, la precisión de lectura es 95%	No requiere intervención humana, 100% automático con precisión de lectura de 99.9%
Durabilidad	Puede dañarse fácilmente en ambientes húmedos o a altas temperaturas	Tiene mayor vida útil, ya que soporta ambientes agresivos (intemperie, químicos, humedad, temperatura)
Rapidez	Requiere lecturas secuenciales	Permite leer múltiples etiquetas simultáneamente de forma automática

Tabla. 1.5. Tabla comparativa RFID versus Código de barras [30]

1.6.2. DESVENTAJAS

En la tabla 1.6 se especifican algunas desventajas de los sistemas RFID [31].

Características	RFID
Costos	Altos costos unitarios de los tags y alta inversión inicial en equipos y configuración de los puntos de control
Tamaño	El alcance de la señal y la superficie del tag están directamente relacionados
Distancia	Los tags pasivos tienen distancia de operación corta
Seguridad	Riesgo de adulteración o reprogramación de tags programables o actualizables

Tabla 1.6. Desventajas de los sistemas RFID

1.6.3. LIMITACIONES DE RFID

Las limitaciones más comunes de RFID se desarrollarán a continuación [32].

Pobre rendimiento con objetos absorbentes. Este es un comportamiento dependiente de la frecuencia de operación. La tecnología actual no opera bien con algunos materiales (metales, líquidos, etc.) y en algunos casos, puede fallar completamente.

Impactada por el entorno operativo. Las condiciones del entorno (por ejemplo, metal y líquidos) pueden impactar significativamente la exactitud de lectura de las etiquetas.

Limitación de lecturas múltiples. Existe un límite práctico en relación a cuántas etiquetas pueden ser leídas dentro de un espacio de tiempo especifico.

Impacto de la interferencia de hardware. Una solución RFID puede ser impactada negativamente si la instalación del equipamiento correspondiente (por ejemplo, el solapamiento debido a la posición y orientación de las antenas produce colisiones) no es realizada apropiadamente.

Poder limitado de la energía RFID. Aunque RFID no necesita una línea de visión, existe un límite de cuan profundo puede llegar la energía RF, incluso a través de objetos translúcidos para la radiofrecuencia. Estos límites se determinan por experimentación y regulaciones en cada país.

Tecnología Inmadura. Aunque la tecnología RFID esta avanzando rápidamente, esos cambios pueden generar inconvenientes para aquellas empresas que no estén preparadas.

TECNOLOGÍA BLUETOOTH

1.7. HISTORIA

Diente Azul es también como se lo conoce a la tecnología Bluetooth que no es precisamente la mejor traducción que se ha utilizado para denominar a esta tecnología. El vocablo Bluetooth viene de la historia de un Rey noruego en el 908 a.c. La tecnología fue bautizada por un ingeniero de Intel, al que le apasiona la historia y la geografía.

En 1.994, la compañía de telecomunicaciones ERICSSON, comenzó un estudio para investigar la viabilidad de una interfaz de radio de baja potencia y bajo costo para facilitar la comunicación entre dispositivos sin la utilización de cables, aprovechando la movilidad de los dispositivos inalámbricos, dio como resultado una tecnología cuyo nombre clave fue "Bluetooth".

El objetivo era eliminar los cables entre los teléfonos móviles y tarjetas de PCs, headsets, dispositivos desktop, etc. Todos hemos experimentado la incomodidad que surge cuando se empiezan a conectar periféricos a un computador, o cuando conectamos otros dispositivos electrónicos en el hogar, con una maraña de cables que se hace difícil de controlar. Entonces nos ponemos a pensar en lo fácil que sería si todas estas conexiones se hicieran utilizando otros medios distintos a los cables físicos, como pueden ser los infrarrojos, la radio o las microondas.

Pues bien, esta problemática ya se ha superado y los resultados están en el mercado; pero ahora surge otro problema y es que son muchos los estándares y las

tecnologías que existen, incompatibles entre sí. Es imprescindible entonces contar con un dispositivo universal, válido para la conexión de todo tipo de periféricos, y que funcione de manera transparente para el usuario. Eso es Bluetooth.

El estudio fue parte de otro gran proyecto de investigación que involucraba multi-comunicadores conectados a la red celular por medio de los teléfonos celulares. El ultimo enlace en dicha conexión debería ser un radio enlace de corto rango. A medida que el proyecto progresaba, se volvió claro que las aplicaciones que envuelven dicho enlace de corto rango serían ilimitadas. A comienzos de 1997, Ericsson se aproxima a otros fabricantes de dispositivos portátiles para incrementar el interés en esta tecnología.

El motivo era simple: para que el sistema fuera exitoso y verdaderamente utilizable, una cantidad crítica de dispositivos portátiles deberían utilizar la misma tecnología de radioenlaces de corto alcance. En Febrero de 1998, cinco compañías, Ericsson, Nokia, IBM, Toshiba e Intel, forman un Grupo de Interés Especial (SIG). Dicho grupo contiene la mezcla perfecta en lo que es el área de negocios, dos líderes del mercado en telefonía móvil, dos líderes del mercado en computadoras laptop y un líder del mercado en tecnología de procesamiento de señales digitales. La meta era establecer la creación de una especificación global para conectividad sin hilos de corto alcance. La razón del nombre es que en el siglo X el rey Harald II de Dinamarca, apodado "diente azul" (Bluetooth) a causa de una enfermedad que le daba esta coloración a su dentadura, reunificó bajo su reinado numerosos pequeños reinos que existían en Dinamarca y Noruega y que funcionaban con reglas distintas,… lo mismo que hace la tecnología Bluetooth, promovida por Ericsson (Suecia) y Nokia (Finlandia), dos países escandinavos. El 20 y el 21 de mayo de 1998, el consorcio de Bluetooth se anuncio al público general de Londres, Inglaterra, San José, California, y Tokio, Japón, lo que provocó la adopción de la tecnología por varias compañías. El propósito del consorcio era establecer un dispositivo estándar y un software que lo controle.

Actualmente ya pertenecen mas de 1.600 empresas al el SIG (Special Interest Group), que han adoptado esta tecnología para desarrollarla con sus propios productos, que empezaron a salir al mercado a finales del año 2000. Cada nueva compañía

miembro del SIG recibe de las otras una licencia para implantar la especificación 1.0, libre de royalties.

1.7.1. ANTECEDENTES

La complejidad para conectarse y configurarse, la baja transmisión de datos, la no disponibilidad de servicios globales y la falta de seguridad en transmisión de datos ha sido un obstáculo para una mayor penetración de la tecnología inalámbrica, sin embargo este escenario ha ido cambiado paulatinamente ya que por ejemplo, Intel ha estado trabajando en emigrar el mercado de las PCs móviles a las necesidades más específicas de los usuarios. La tecnología Bluetooth reemplazará los cables que conectan a un dispositivo con otro en un corto enlace de radio, esta tecnología Bluetooth está siendo desarrollada por las contribuciones de los miembros del SIG (Special Interest Group) fundado por Ericsson, IBM, Intel, Nokia y Toshiba.

El SIG de Bluetooth está tratando de hacer esta tecnología mundial, con productos como computadoras móviles, handsets, PDA's, puntos de acceso a red y muchos otros dispositivos. Adicionalmente Bluetooth está siendo desarrollada como especificación abierta, y la licencia para las compañías interesadas será libre de costos.

Bluetooth es una de varias especificaciones para la tecnología inalámbrica para comunicaciones de voz y datos, usando un rango corto de ondas de radio, lo cual permite una comunicación instantánea de hasta entre 8 dispositivos simultáneamente. Las frecuencias de radio utilizadas por el chip Bluetooth son del espectro de 2.4 Gigahertz (GHz), la cual no requiere licencia alguna para ser utilizada. Con una antena de OdBm, dos aparatos con esta tecnología pueden comunicarse a una distancia de 10 metros aproximadamente, la cual puede ser ampliada incrementando el tamaño de la antena; la potencia de transmisión salida que tenemos en Bluetooth es de 1mW, siendo tecnología flexible que permite ser reconfigurada para distintos ambientes inalámbricos, trabaja en la banda ISM (Industrial, Scientific and Medical) con licencia libre en el rango de frecuencias de 2.4 GHz a 2.483 GHz dividido en 79 canales espaciados por 1MHz. Además permite la conexión en una pequeña red ad hoc (piconets) en cualquier parte del mundo.

1.8. CARACTERÍSTICAS DE LA TECNOLOGÍA BLUETOOTH

Bluetooth es esencialmente un transmisor-receptor que opera en un modo de "spread-spectrum" (espectro disperso); cambia de frecuencia para cada paquete de datos unas 1.600 veces por segundo. Este salto de frecuencias, junto con el bajo consumo de energía que limita su alcance a pocos metros, es lo que permite a una conexión Bluetooth evitar la interferencia con otra. Bluetooth es, de hecho, tanto una especificación de hardware como un marco de software para la interoperación, con la implementación de ambas cosas en un solo chip de 9 mm x 9 mm.

El protocolo habilita el intercambio de información entre muchos dispositivos, incluyendo teléfonos móviles, PDAs, notebook PCs, handheld PCs, periféricos asociados, concentradores, que cuentan con RF. El radio opera en la banda libre de 2.45 GHz antes mencionada, además no requiere de línea de vista entre los dispositivos para la conexión, el protocolo en banda base de Bluetooth es una combinación de conmutación de circuitos y de paquetes, haciéndolo apropiado para voz y datos.

Bluetooth ha sido diseñado para operar en un ambiente multi - usuario, es decir hasta 8 usuarios o dispositivos pueden estar en piconet, y 10 piconets pueden coexistir en el mismo intervalo de cobertura. Ver Figura 1.8.

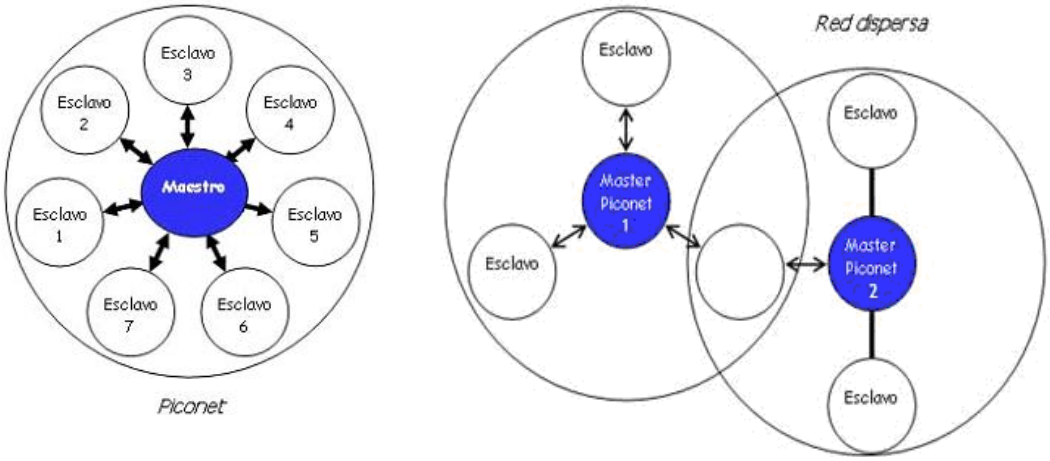


Figura. 1.8. Arquitectura de la red Bluetooth

Si un equipo se encuentra dentro del radio de cobertura de otro, éstos pueden establecer conexión entre ellos. En principio sólo son necesarias un par de unidades con las mismas características de hardware para establecer un enlace. Si dos o más unidades Bluetooth que comparten un mismo canal forman una piconet. Para regular el tráfico en el canal, una de las unidades participantes se convertirá en maestra, pero por definición, la unidad que establece la piconet asume éste papel y todos los demás serán esclavos como se indica en la Figura 1.8. Los participantes podrían intercambiar los papeles si una unidad esclava quisiera asumir el papel de maestra. Sin embargo sólo puede haber un maestro en la piconet al mismo tiempo.

Cada unidad de la piconet utiliza su identidad maestra y reloj nativo para seguir en el canal de salto. Cuando se establece la conexión, se añade un ajuste de reloj a la propia frecuencia de reloj nativa de la unidad esclava para poder sincronizarse con el reloj nativo del maestro y a su vez éste mantiene siempre constante su frecuencia, sin embargo los ajustes producidos por las unidades esclavas para sincronizarse con el maestro, sólo son válidos mientras dura la conexión.

Las unidades maestras controlan en tráfico del canal, por cuanto tienen la capacidad para reservar slots en los enlaces SCO (sincronización de conexión orientada), Para los enlaces ACL (asíncrono de baja conexión), se utiliza un esquema de sondeo. A un esclavo sólo se le permite enviar un slot a un maestro cuando ésta se ha dirigido por su dirección MAC (medio de control de acceso) en el procedimiento de slot maestro-esclavo. Éste tipo de slot implica un sondeo por parte del esclavo, por lo que, en un tráfico normal de paquetes, este es enviado a una urna del esclavo automáticamente. Si la información del esclavo no está disponible, el maestro puede utilizar un paquete para sondear al esclavo explícitamente. Los paquetes de sondeo consisten únicamente en uno de acceso y otro de cabecera. Éste esquema elimina las colisiones entre las transmisiones de los esclavos.

1.8.1. MÉTODO DE ACCESO

El sistema de radio Bluetooth deberá estar preparado para evitar múltiples interferencias que se pudieran producir, la misma que pueden ser evitadas utilizando un sistema que busque una parte no utilizada del espectro o un sistema de salto de

frecuencia. En los sistemas de radio Bluetooth se suele utilizar el método de salto de frecuencia debido a que ésta tecnología puede ser integrada en equipos de baja potencia y bajo coste. Éste sistema divide la banda de frecuencia en varios canales de salto, donde, los transceptores, durante la conexión van cambiando de uno a otro canal de salto de manera aleatoria. Con esto se consigue que el ancho de banda instantáneo sea muy pequeño y también una propagación efectiva sobre el total de ancho de banda. En conclusión, con el sistema FH (Salto de frecuencia), se pueden conseguir transceptores de banda estrecha con una gran inmunidad a las interferencias.

1.8.2. DEFINICIÓN DE CANAL

FH/TDD (salto de frecuencia/división de tiempo dúplex) es un sistema que utiliza Bluetooth para lo cual el canal queda dividido en intervalos de 625 µs, llamados slots, donde cada salto de frecuencia es ocupado por un slot. Esto da lugar a una frecuencia de salto de 1600 veces por segundo, en la que un paquete de datos ocupa un slot para la emisión y otro para la recepción y que pueden ser usados alternadamente dando lugar a un esquema de tipo TDD (Time División Dúplex); este esquema es flexible para la asignación de ancho de banda y usa la misma frecuencia para ambos enlaces.

En una *PICONET* dos o más unidades Bluetooth pueden compartir el mismo canal, donde una unidad actúa como maestra, controlando el tráfico de datos en la *PICONET* que se genera entre las demás unidades, donde estas actúan como esclavas, enviando y recibiendo señales hacia el maestro. El salto de frecuencia del canal está determinado por la secuencia de la señal, es decir, el orden en que llegan los saltos y por la fase de ésta secuencia

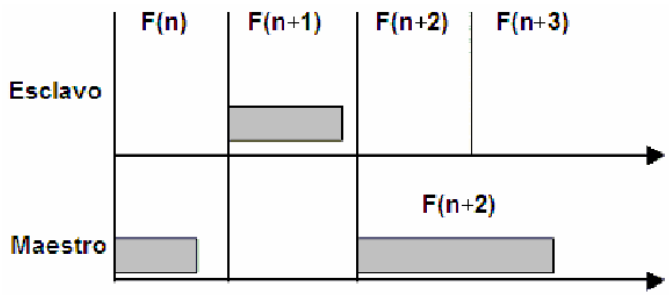


Figura. 1.9 Técnica TDD (*TIME DIVISION DUPLEX)*

En Bluetooth, la secuencia queda fijada por la identidad de la unidad maestra de la *PICONET* (un código único para cada equipo), y por su frecuencia de reloj. Por lo tanto, para que una unidad esclava pueda sincronizarse con una unidad maestra, ésta primera debe añadir un ajuste a su propio reloj nativo y así poder compartir la misma portadora de salto. En países donde la banda está abierta a 80 canales o más, espaciados todos ellos a 1 MHz, se han definido 79 saltos de portadora, y en aquellos donde la banda es más estrecha se han definido 23 saltos.

1.8.3. DEFINICIÓN DEL PAQUETE

La información que se intercambia entre dos unidades Bluetooth se realiza mediante un conjunto de slots que forman un paquete de datos. Cada paquete comienza con un código de acceso de 72 bits, que se deriva de la identidad maestra, seguido de un paquete de datos de cabecera de 54 bits, el cual contiene importante información de control, como tres bits de acceso de dirección, tipo de paquete, bits de control de flujo, bits para la retransmisión automática de la pregunta, y chequeo de errores de campos de cabeza. Finalmente, el paquete que contiene la información, que puede seguir al de cabeza, tiene una longitud de O a 2745 bits. En cualquier caso, cada paquete que se intercambia en el canal está precedido por el código de acceso.

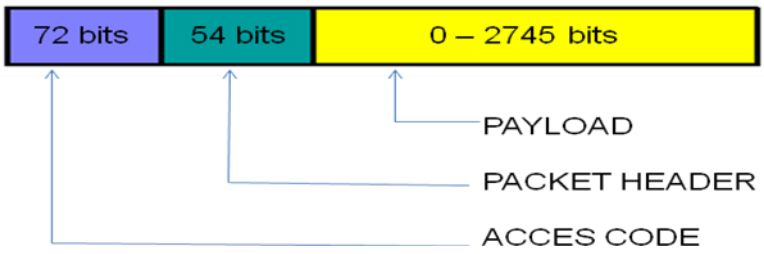


Figura 1.10 Estructura del paquete de datos

Los receptores de la *PICONET* comparan las señales que reciben con el código de acceso, si éstas no coinciden, el paquete recibido no es considerado como válido en el canal y el resto de su contenido es ignorado.

- **CÓDIGO DE ACCESO (72 BITS):** Es usado para sincronización, identificación y compensación. Todos los paquetes comunes que son enviados sobre el canal de la

piconet están precedidos del mismo código de acceso al canal. Existen tres tipos diferentes de código de acceso o access code:

- Channel Access Code o código de acceso al canal (CAC)**:** identifica una piconet. Se incluye en los paquetes intercambiados en el canal de una piconet

- *Device Access Code o Código de acceso de dispositivo (DAC)***:** utilizado para procesos de señalización especiales.

- *Inquiry Access Code o Código de Acceso de Búsqueda (IAC)***:** utilizado para procesos de búsqueda de dispositivos. Se llamará *IAC general* cuando se quiere descubrir a otras unidades *Bluetooth* dentro del rango, o *IAC dedicado* cuando se desea descubrir unidades de un tipo específico

- **CABECERA (54 BITS):** Contiene información del control de enlace con 6 campos:

  - *Dirección o AM_ADDR***:** Dirección temporal de 3 bits que se utiliza para distinguir los dispositivos activos en una piconet, siendo la dirección 000 la dirección broadcast.

  - *Tipo***:** Define qué tipo de paquete es enviado y cuántos slots va a ocupar.

  - *Flujo o Flow***:** El bit de control de flujo es usado para notificar al emisor cuándo el buffer del receptor está lleno y que debe de dejar de transmitir, en ese caso el bit tendrá el valor "0".

  - *ARQN***:** bit de reconocimiento de paquetes recibidos paquetes correcto o incorrecto (ultimo paquete recibido). Si es un "1" es un ACK, y con un "0" un NAK.

  - *SEQN***:** bit que se va invirtiendo para evitar retransmisiones en el receptor.

- *HEC*: Código de redundancia para comprobar errores en la transmisión.

- **CAMPO DE DATOS O CARGA ÚTIL (HASTA 2746 BITS):** Contiene el conjunto de datos que supone la información a transmitir.

1.8.4. DEFINICIÓN DEL ENLACE FÍSICO

En la especificación Bluetooth se han definido dos tipos de enlace que permitan soportar incluso aplicaciones multimedia:

- Enlace de sincronización de conexión orientada (SCO)
- Enlace asíncrono de baja conexión (ACL)

Los enlaces SCO soportan conexiones asimétricas, punto a punto, usadas normalmente en conexiones de voz, estos enlaces están definidos en el canal, reservándose dos slots consecutivos (envío y retorno) en intervalos fijos. Los enlaces ACL soportan conmutaciones punto a punto simétrico o asimétrico, típicamente usadas en la transmisión de datos.

Un conjunto de paquetes se han definido para cada tipo de enlace físico:

- Para los enlaces SCO, existen tres tipos de slot simple, cada uno con una portadora a una velocidad de 64 kbit/s. La transmisión de voz se realiza sin ningún mecanismo de protección, pero si el intervalo de las señales en el enlace SCO disminuye, se puede seleccionar una velocidad de corrección de envío de 1/3 o 2/3.

- Para los enlaces ACL, se han definido el slot-1, slot-3, slot-5. Cualquiera de los datos pueden ser enviados protegidos o sin proteger con una velocidad de corrección de 2/3. La máxima velocidad de envío es de 721 kbit/s en una dirección y 57.6 kbit/s en la otra.

1.8.5. INMUNIDAD A LAS INTERFERENCIAS

Como se mencionó anteriormente Bluetooth opera en una banda de frecuencia que está sujeta a considerables interferencias, por lo que el sistema ha sido optimizado para evitar éstas interferencias. En este caso la técnica de salto de frecuencia es aplicada a una alta velocidad y una corta longitud de los paquetes (1600 saltos/segundo, para slots-simples). Los paquetes de datos están protegidos por un esquema ARQ (repetición automática de consulta), en el cual los paquetes perdidos son automáticamente retransmitidos, aun así, con este sistema, si un paquete de datos no llegase a su destino, sólo una pequeña parte de la información se perdería. La voz no se retransmite nunca, sin embargo, se utiliza un esquema de codificación muy robusto. Éste esquema, que está basado en una modulación variable de declive delta (CSVD), que sigue la forma de la onda de audio y es muy resistente a los errores de bits. Estos errores son percibidos como ruido de fondo, que se intensifica si los errores aumentan.

1.9. FUNCIONAMIENTO DE LA RED BLUETOOTH

Se puede establecer que la secuencia de activación de cada una de las portadoras visitará cada salto una sola vez, con una longitud de la secuencia de 32 (16) saltos. En cada uno de los 2.048 (1.024) saltos, las unidades que se encuentran en modo standby (en espera) mueven sus saltos de portadora siguiendo la secuencia de las unidades activas. El reloj de la unidad activa siempre determina la secuencia de activación.

Durante la recepción de los intervalos, en los últimos 18 slots o 11,25 ms, las unidades escuchan una simple portadora de salto de activación y correlacionan las señales entrantes con el código de acceso derivado de su propia identidad. Si la mayoría de los bits recibidos coinciden con el código de acceso, la unidad se auto-activa e invoca un procedimiento de ajuste de conexión. Sin embargo si estas señales no coinciden, la unidad vuelve al estado de reposo hasta el siguiente evento activo.

Para establecer la *piconet*, la unidad maestra debe conocer la identidad del resto de unidades que están en modo *standby* en su radio de cobertura. El maestro o aquella unidad que inicia la piconet transmite el código de acceso continuamente en periodos de 10 ms, que son recibidas por el resto de unidades que se encuentran en standby. El tren

de 10 ms. de códigos de acceso de diferentes saltos de portadora, se transmite repetidamente hasta que el receptor responde o bien se excede el tiempo de respuesta.

Cuando una unidad emisora y una receptora seleccionan la misma portadora de salto, la receptora recibe el código de acceso y devuelve una confirmación de recibo de la señal, es entonces cuando la unidad emisora envía un paquete de datos que contiene su identidad y frecuencia de reloj actual.

Después de que el receptor acepta éste paquete, ajustará su reloj para seleccionar el canal de salto correcto determinado por emisor. De éste modo se establece una piconet en la que la unidad emisora actúa como maestra y la receptora como esclava. Posteriormente de haber recibido los paquetes de datos con los códigos de acceso, la unidad maestra debe esperar un procedimiento de requerimiento por parte de las esclavas, diferente al proceso de activación.

El número máximo de unidades que pueden participar activamente en una simple *piconet* es de 8, un maestro y siete esclavos, por lo que la dirección MAC del paquete de cabecera que se utiliza para distinguir a cada unidad dentro de la piconet, se limita a tres bits.

En un conjunto de varias *piconets*, cada una de ellas seleccionan diferentes saltos de frecuencia y controladas por diferentes maestros, por lo que si un mismo canal de salto es compartido temporalmente por *piconets* independientes, los paquetes de datos podrán ser distinguidos por el código de acceso que les precede, que es único en cada una.

La sincronización de varias de éstas no está permitida en la banda ISM, sin embargo, las unidades pueden participar en diferentes *piconets* en base a un sistema TDM (división de tiempo múltiplexada). En otras palabras, una unidad participa secuencialmente en diferentes piconets, a condición de que esté sólo activa en una al mismo tiempo. Una unidad al incorporarse a una nueva piconet debe modificar el offset (ajuste interno) de su reloj para minimizar la deriva entre su reloj nativo y el que le corresponde a él mismo, debido a éste sistema se puede participar en varias piconets

realizando cada vez los ajustes correspondientes una vez conocidos los diferentes parámetros de la piconet.

Cuando una unidad abandona una *piconet*, la esclava informa al maestro actual que ésta no estará disponible por un determinado periodo, que será en el que estará activa en otra *piconet* y durante su ausencia, el tráfico en la *piconet* entre el maestro y los esclavos continúa de la misma manera.

De igual forma que una esclava puede cambiar de una *piconet* a otra, una maestra también lo puede hacer, con la diferencia de que el tráfico de la *piconet* se suspende hasta la vuelta de la unidad maestra. La maestra que entra en una nueva *piconet*, en principio, lo hace como esclava, a no ser que posteriormente ésta solicite actuar como maestra.

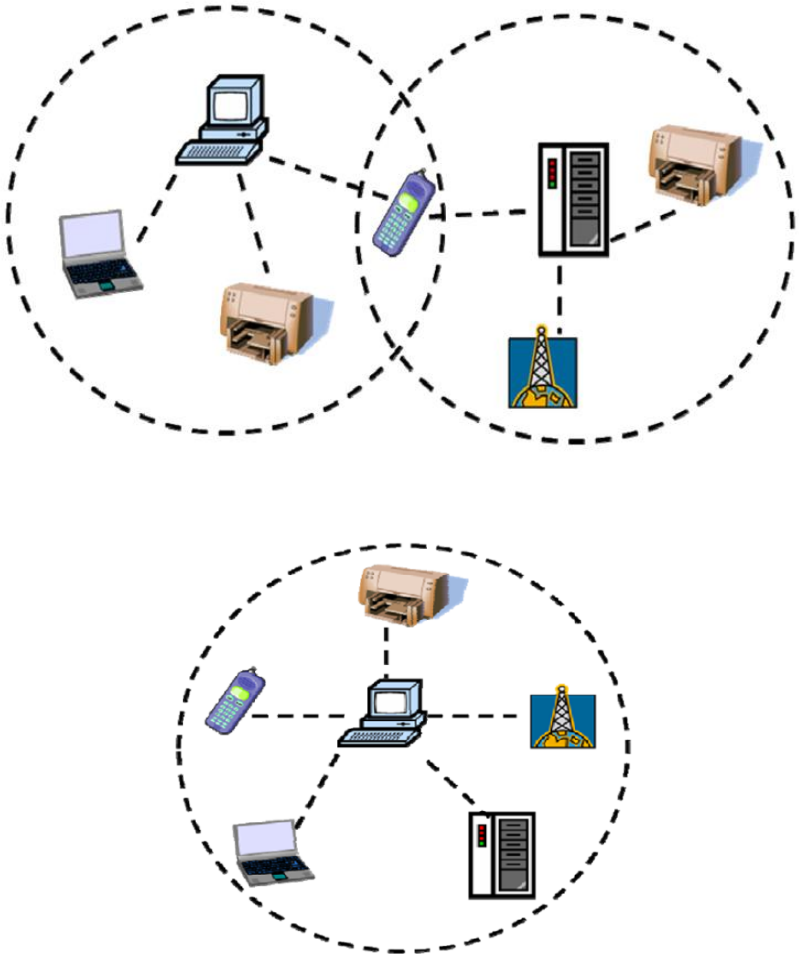


Figura 1.11 Tipos de Comunicaciones Inalámbricas de un Usuario

1.9.1. SINCRONIZACIÓN

El transceptor Bluetooth usa un método dúplex de división de tiempo (*Time-Division Dúplex*), lo que significa que transmite alternativamente y recibe de forma síncrona. El promedio de tiempo de la transmisión de paquetes por parte del maestro no debería ser mayor de 20 ppm. La *piconet* es sincronizada por el reloj del sistema del maestro. Para transmitir por el canal se necesitan tres piezas de información: *La secuencia hopping, la fase de la secuencia y el CAC para situarlo en los paquetes*.

La dirección del dispositivo Bluetooth (BD_ADDR) del maestro es utilizada para obtener su secuencia (*frecuency hopping*). El reloj del sistema del maestro determina la fase en la secuencia hopping. El código de acceso al canal se obtiene a través de la dirección del dispositivo Bluetooth del maestro (BD_ADDR). Los esclavos adaptan sus relojes nativos con una compensación de tiempo para coincidir con el reloj maestro. La compensación es cero para el maestro y su reloj nativo es el reloj maestro para la red. Se permite una ventana de 20us sobre el tiempo exacto recibido para que el receptor encuentre el código de acceso al canal correcto y se sincronice con el transmisor.

Cuando un esclavo vuelve del modo *hold*, puede trabajar con una ventana mayor hasta mientras no solapen las ranuras. Un esclavo en estado *park* se "despierta" periódicamente para escuchar los avisos del maestro y resincronizar la compensación de su reloj.

1.9.2. SEGURIDAD DE LA RED BLUETOOTH

Bluetooth tiene diferentes perfiles que condicionan la seguridad en su comunicación. El Acceso Genérico Bluetooth es un marco en el cual se centran todos los perfiles y define tres modos de seguridad:

- *No seguro*: no inicia ningún tipo de seguridad.
- *Seguridad impuesta a nivel de servicio*: inicia el procedimiento de seguridad después de que el canal haya sido establecido (capas altas de la pila de protocolos).

- *Seguridad impuesta a nivel de enlace*: inicia el procedimiento de seguridad antes de que el canal haya sido establecido (capas bajas de la pila de protocolos).

Existe la posibilidad de acceder a un servicio con diferentes accesos de dispositivo:

- *Dispositivo de confianza*: tienen acceso sin restricción a los servicios.
- *Dispositivos de no confianza*: tienen un acceso limitado

Estos dispositivos antes mencionados son catalogados a tres niveles de seguridad:

- *Servicios abiertos*: a los cuales puede acceder cualquier dispositivo.
- *Servicios que requieren sólo autenticación*: a los cuales puede acceder cualquier dispositivo que se haya autenticado, puesto que habrá demostrado que comparte una clave de enlace con el proveedor del servicio.
- *Servicios que requieren autenticación y autorización*: a los cuales sólo tendrán acceso aquellos dispositivos que sean de confianza (y así estarán marcados en la base de datos del servidor).

Para conseguir seguridad, tanto en el acceso a otros dispositivos Bluetooth como en la transmisión de la información entre ellos, es necesario un complejo entramado de seguridad que afiance estos dos aspectos.

En el nivel de enlace, la seguridad se mantiene mediante la autenticación de los usuarios y la encriptación de la información. Para esta seguridad básica se necesita una dirección pública que sea única para cada dispositivo (BD_ADDR), dos claves secretas (clave de autenticación y clave de encriptación) y un generador de números aleatorios. Primero, el dispositivo realiza la autenticación emitiendo un mensaje y el otro dispositivo tiene que enviar una respuesta a ese mensaje basado en el propio mensaje, su BD_ADDR y una clave de enlace compartida entre ellos. Después de la autenticación, la encriptación puede utilizarse para comunicar.

Esta encriptación se define en un nivel básico del mismo, el cual se incluye en el diseño de los chips de radio para proveer de seguridad en equipos que carezcan de capacidad de procesamiento, las principales medidas que se toman en consideración de seguridad son:

- Una rutina de pregunta-respuesta, para autentificación.
- Una corriente cifrada de datos, para encriptación.
- Generación de una clave de sesión (que puede ser cambiada durante la conexión).

Las entidades utilizadas en los algoritmos de seguridad son:

- La dirección de la unidad Bluetooth, que es una entidad pública.
- Una clave de usuario privada, como una entidad secreta.
- Un número aleatorio, que es diferente por cada nueva transacción.

En cuanto a la dirección Bluetooth ésta se puede obtener a través de un procedimiento de consulta. La clave privada se deriva durante la inicialización y no es revelada posteriormente. El número aleatorio se genera en un proceso de cada unidad Bluetooth.

1.9.3. FUNCIONES BANDA BASE Y CORRECCIÓN DE ERRORES

Usados en el protocolo banda base existen tres tipos de planificación para corregir errores

- *FEC de tasa 1/3*: donde cada bit es repetido tres veces para la redundancia
- *FEC de tasa 2/3*: un generador de polinomios es usado para codificar con códigos de 10 y 15 bit
- *Método ARQ*: en un paquete es retransmitido hasta que se recibe un acuse de recibo (o se excede un límite de tiempo).

Bluetooth utiliza acuses de recibos rápidos y no numerados en los que usa acuses de recibos positivos y negativos estableciendo valores ARQN apropiados. Si se excede el contador, Bluetooth marca el paquete y procede con el siguiente.

1.9.4. CONTROL DE FLUJO

El protocolo banda base recomienda usar colas FIFO en ACL y enlaces SCO para transmisión y recepción. El Link Manager rellena estas colas y el Link Controller las vacía automáticamente. Si estas colas RX FIFO están llenas, se utiliza el control de flujo para evitar la congestión y la pérdida de paquetes. Si no se pueden recibir los datos, se transmite una indicación de stop insertada por el Link Controller del receptor en la cabecera del paquete devuelto. Cuando el transmisor recibe la indicación de stop, congela sus colas FIFO. Si el receptor está preparado, envía un paquete *GO* que restablece el flujo.

1.9.5. EVOLUCIÓN

Una vez establecida la conexión en la red por las *piconets* se vio la necesidad de sobrepasar el obstáculo que presentaba el hecho de la comunicación para trasmitir en un ancho de banda de los 80 Mhz (como son los casos de Europa y USA en la cual Bluetooth trabaja en esa frecuencia exceptuando a España y Francia); en donde no puede ser utilizado eficazmente debido a que cada unidad ocupa una parte del mismo canal de salto de 1MHz. Para poder solucionar éste problema se adoptó una solución de la que nace el concepto de *scatternet.*

Dentro de este contexto los equipos que comparten un mismo canal sólo pueden utilizar una parte de su capacidad de este. Aunque los canales tienen un ancho de banda de un 1Mhz, cuantos más usuarios se incorporan a la *piconet*, disminuye la capacidad hasta unos 10 kbit/s más o menos. Teniendo en cuenta que el ancho de banda medio disponible es de unos 80 Mhz en los casos de Europa y USA (excepto en España y Francia), éste no puede ser utilizado eficazmente, cuando cada unidad ocupa una parte del mismo canal de salto de 1Mhz. Las unidades que se encuentran en el mismo radio de cobertura pueden establecer potencialmente comunicaciones entre ellas. Sin

embargo, sólo aquellas unidades que realmente quieran intercambiar información comparten un mismo canal creando la *piconet*.

Éste hecho permite que se creen varias *piconets* en áreas de cobertura superpuestas. De esta manera al grupo de *piconets* se le llama *scatternet*. El rendimiento, en conjunto e individualmente de los usuarios de una *scatternet* es mayor que el que tiene cada usuario cuando participa en un mismo canal de 1 Mhz. Además, estadísticamente se obtienen ganancias por multiplexión y rechazo de canales salto. Debido a que individualmente cada *piconet* tiene un salto de frecuencia diferente, diferentes *piconets* pueden usar simultáneamente diferentes canales de salto.

Se debe de tener en cuenta que cuantas más *piconets* se añaden a la *scatternet* el rendimiento del sistema FH (salto de frecuencia) disminuye poco a poco, habiendo una reducción por termino medio del 10%; sin embargo el rendimiento que finalmente se obtiene de múltiples *piconets* supera al de una simple *piconet*.

1.10. FUNCIONAMIENTO DEL CHIP BLUETOOH.

El controlador Bluetooth trabaja principalmente en dos estados: Standby y Connection. Existen también siete sub estados usados para añadir "esclavos" o crear conexiones en la *piconet*, los cuales son: *page, page sean, inquiry, inquiry sean, master response, slave response and inquiry response*.

1.10.1. STANDBY

El estado *Standby* es el estado por defecto con menor gasto de energía en la unidad Bluetooth. Sólo funciona el reloj interno y no hay interacciones con ningún otro dispositivo.

CONNECTION

En el estado *connection* el maestro y el esclavo pueden intercambiar paquetes usando el código de acceso al canal y el reloj maestro del Bluetooth. El esquema de salto usado es el esquema de canal de salto.

1.10.2. CONFIGURACIÓN DE LA CONEXIÓN (INQUIRY/PAGING)

Normalmente, una conexión entre dos dispositivos tiene lugar de la siguiente manera: Si no se conoce nada sobre el dispositivo remoto, deben seguirse los siguientes procedimientos:

- *Procedimiento Inquiry* este procedimiento permite a un dispositivo descubrir que dispositivos están en el rango y determinar las direcciones y relojes de los mismos

- *Procedimiento page* se puede establecer una conexión actual, el procedimiento paging sigue el procedimiento inquiry.

Si se conocen algunos detalles del dispositivo remoto, sólo será necesario el procedimiento *page*. El procedimiento inquiry implica a una unidad (fuente) enviando paquetes de salida (estado inquiry) y recibiendo entonces un paquete de respuesta.

La unidad que recibe los paquetes (el destino), estará en el estado *inquiry scan* para recibir los paquetes, entonces sólo se requiere la dirección del dispositivo Bluetooth para configurar una conexión. Los conocimientos sobre el reloj acelerarán el procedimiento de configuración. Una unidad que establezca una conexión llevará a cabo un procedimiento page y se convertirá automáticamente en el maestro de la conexión.

El destino entrará entonces en el estado inquiry response y enviará una respuesta inquiry a la fuente. Después de que se haya completado el procedimiento inquiry, se podrá establecer una conexión usando el procedimiento paging.

- Un dispositivo (la fuente) registra otro dispositivo (el destino). Estado Page
- El destino recibe paquete. Estado Page Sean
- El destino envía una respuesta a la fuente. Estado Slave Response
- La fuente envía un paquete FHS al destino. Estado Master Response
- El destino envía su segunda respuesta a la fuente. Estado Slave Response
- El destino y la fuente intercambian entonces los parámetros del canal fuente. Estado Master Response & Slave Response.

El estado Connection comienza con un paquete POLL enviado por el maestro para verificar que el esclavo ha cambiado al salto de frecuencia de canal y temporización del maestro. El esclavo puede responder con cualquier tipo de paquete.

1.10.3. MODOS DE CONEXIÓN

En el estado Connection puede encontrarse en cualquiera de los siguientes cuatro modos:

- *Modo Active*. La unidad Bluetooth participa activamente en el canal. El maestro planifica la transmisión basada en las demandas de tráfico hacia y desde los diferentes esclavos. Soporta transmisiones regulares de para mantener a los esclavos sincronizados al canal. Los esclavos activos escuchan el canal para esperar un paquete. Si un esclavo activo no es direccionado, podría dormir hasta la próxima transmisión del nuevo maestro.

- *Modo Hola*. Los dispositivos sincronizados a una *piconet* pueden entrar en los modos power-saving en los que la actividad de los dispositivos es menor. La unidad maestro puede poner unidades esclavos en modo *HOLD*, donde únicamente sólo está funcionando un contador interno. Las unidades esclavo también pueden demandar ser puestas en modo *HOLD*. La transferencia de datos vuelve a comenzar de forma instantánea cuando las unidades abandonan el modo *HOLD*. Tiene un ciclo de trabajo intermedio de los tres modos de ahorro de energía (sniff, hold y park).

- *Modo Park*. un dispositivo se encuentra aún sincronizado a la *piconet* pero no participa en el tráfico. Los dispositivos en el estado *park* han abandonado sus direcciones MAC y ocasionalmente escuchan el tráfico del maestro para volverse a sincronizar y comprobar los mensajes broadcast. Tiene el ciclo de trabajo más corto de los tres modos de ahorro de energía (sniff, hold y park).

- *Modo Sniff.* Los dispositivos sincronizados a una *piconet* pueden entrar en los modos de ahorro de energía en los cuales la actividad del dispositivo es menor. En el modo SNIFF, un dispositivo esclavo escucha a la piconet a una tasa reducida, lo que reduce su ciclo de trabajo. El intervalo SNIFF es programable y depende de la aplicación. Tiene el mayor ciclo de vida de los tres modos de ahorro de energía (sniff, hold y park).

1.11. VENTAJAS Y CARACTERÍSTICAS DE LA TECNOLOGÍA BLUETOOTH

1.11.1. PRINCIPALES VENTAJAS

Entre las principales ventajas tenemos las siguientes:

- Opera en la banda de frecuencia de 2.4 GHz, libre para ISM
- Es más robusto que la mayoría de otros sistemas porque salta más rápido y usa paquetes más pequeños
- Emplea una corrección de error hacia delante (FEC, Forward Correction Error) que reduce el efecto del ruido aleatorio en enlaces de larga distancia.
- Utiliza un esquema de división en el tiempo para la transmisión en full-dúplex.
- El protocolo de banda base de Bluetooth es una combinación de conmutación de paquetes y de circuitos.
- Bajo Costo.
- Hasta 10 metros cliente-cliente en aire abierto, hasta 5 metros dentro de edificios.
- Baja potencia.
- Alta velocidad -1 Mbps sin línea de vista. Rango de una PAN:
- Hasta 100 metros cliente a punto de acceso en aire abierto, hasta 30 metros dentro de edificios.

- Soporte de voz y datos.
- Alta seguridad -encriptación & autenticación.
- Alta aceptación en la industria.
- Bluetooth utiliza un esquema de reconocimiento rápido y saltos de frecuencia para garantizar la robustez del enlace.
- Cada paquete se transmite en un salto de frecuencia distinto.
- Bluetooth puede soportar un canal de datos asíncrono.

1.11.2. CARACTERÍSTICAS DE LA TECNOLOGÍA BLUETOOTH

En la tabla 1.7 se especifican algunas características de Bluetooth.

PARAMETROS	BENEFICIOS BLUETOOTH
Banda de frecuencias	2.4 GHz (banda ISM sin licencia)
Potencia transmitida	1 miliwatt (O dBm)
Tecnología	Espectro disperso
Híbrido	Secuencia directa y salto en frecuencia
Máximo canales de voz	3 por piconet
Máximo canales de datos	7 por piconet
Velocidad de datos	721 Kbps por piconet
Rango esperado del sistema	10 metros
Número de dispositivos soportados	8 por piconet, 10 por piconet en el área de cobertura
Seguridad	En la capa de enlace
Requerimiento de potencia	2.7 volts
Consumo de potencia	30 uA dormido, 60 uA parado, 300 uA standby, 8-30 mA transmitiendo
Tamaño del modulo	0,5 pulgadas cuadradas
Interferencia	Bluetooth minimiza la interferencia de potencia empleando rápidos saltos en frecuencia -1600 veces por segundo

Tabla 1.7 Beneficios de la Tecnología Bluetooth

CAPITULO 2

DISEÑO DEL PROTOTIPO DE CONTROL

Actualmente la tecnología Bluetooth es muy utilizada en comunicaciones inalámbricas los productos mas conocidos son los utilizados en celulares con los cuales se pueden desarrollar pequeñas redes para la compartición de archivos, conjuntamente la tecnología RFID tiene una gran aceptación en los campos de control de accesos, detección de productos por estas razones se ha tomado estos parámetros para el desarrollo del siguiente prototipo.

Para el diseño del sistema de supervisión de acceso se dividió el diseño en tres tipos de conexiones las cuales son:

- Lectoras RFID y Microcontrolador
- Microcontrolador y Bluetooth
- Bluetooth y el destino una PC

2.1. INTERCONEXIÓN ENTRE LAS LECTORAS RFID Y EL MICROCONTROLADOR

Para el diseño del sistema de acceso se deben tomar en cuenta aspectos como la confiabilidad del dispositivo, que se logra con la utilización de elementos electrónicos de precisión y alta calidad. Para obtener resultados óptimos, se realiza un análisis de los elementos a adquirir del mercado, haciendo que se cumplan los requerimientos específicos del diseño, para el correcto funcionamiento del sistema.

En la figura 2.1 se ilustra un diagrama de bloques que conforman el dispositivo del sistema de acceso.

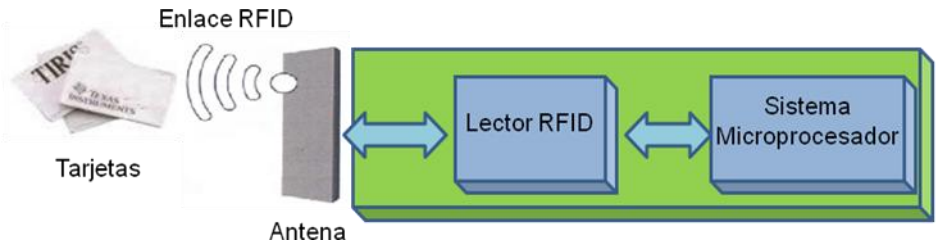


Figura 2.1 Diagrama de Bloque entre RFID y el Microcontrolador

2.1.1. RECEPCIÓN DE DATOS EN LA TECNOLOGÍA RFID

Para la captura de datos con la tecnología RFID, se ha elegido los lectores de marca EntryPass modelo EP.05, entre las principales prestaciones, se encuentra la frecuencia de operación es de 125KHz, el rango de cobertura del lector es de 4 cm.

En la tecnología RFID cuando una Tag entra en el alcance de la antena receptora genera un código numérico el cual se basa mediante el Protocolo de Comunicaciones Wiegand el cual fue desarrollado por la sociedad “Sensor Engineering Company”, se lo utiliza para la transmisión de datos a los controladores desde las lectoras RFID, según convención industrial aceptada.

Este protocolo se compone de tres líneas, las cuales utilizan voltajes TTL: Data 0, Data 1, y la línea de referencia de ambas. Si no se transmite ningún bit las líneas Data 0 y Data 1 se encuentran en alto, en un nivel de reposo.

Cuando se envía un 0 lógico, el nivel de la línea Data 0 cambia a un nivel bajo durante 50 µseg y regresa al reposo; mientras que si se transmite un 1 lógico, el nivel de la línea Data 1 cambia a un nivel bajo durante 50 µseg y regresa al reposo, en la figura 2.1 se muestra la transmisión de 4 bits.

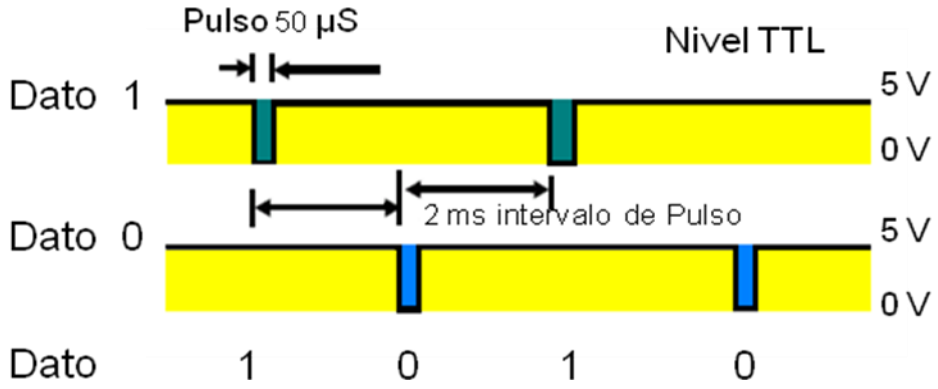


Figura 2.2 Transmisión con Protocolo Wiegand

Existen formatos propietarios de fabricantes, propietarios de usuarios finales y formatos estándar. El estándar Wiegand 26 es el mas conocido y utilizado, transmite 26 bits entre las dos líneas. En la figura 2.2 se muestra el formato de la trama Wiegand 26 estándar.

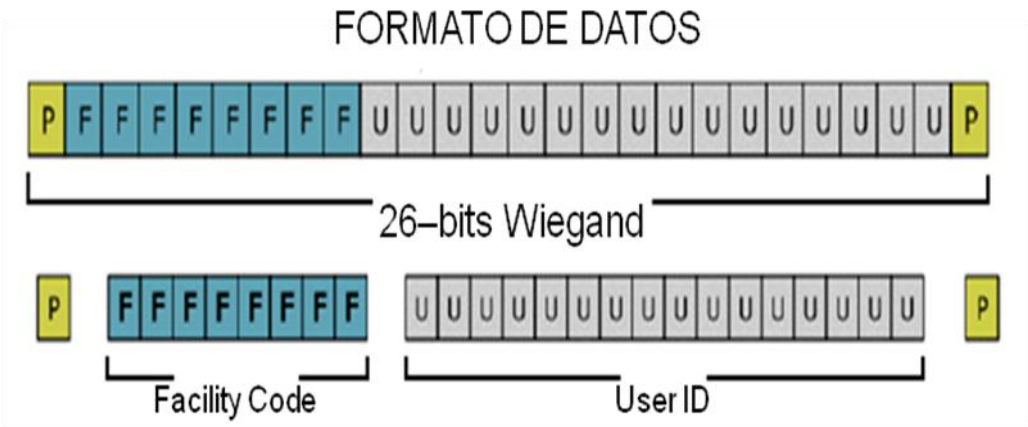


Figura 2.3 Formato de la trama Wiegand 26

El primer bit, es la paridad Par de los primeros 12 bits transmitidos, los 8 siguientes son un Byte, denominado Código de Facilidad (Facility Code), los 16 siguientes son dos Bytes, al que se le llama Código de Usuario (User Code), y el último bit es la paridad Impar de los últimos 16 bits

El código de facilidad permite tener 256 combinaciones diferentes con 65 536 códigos de usuario cada una. En este formato estándar de 26 bits, pueden ocurrir

duplicaciones de números, pero la probabilidad de que ocurra es muy baja; para mayor seguridad de que no existan duplicaciones, se tienen formatos como Wiegand 32 y Wiegand 44.

2.1.2. RECEPCIÓN DE DATOS EN EL MICROCONTROLADOR

EL Microcontrolador en el sistema de control de acceso es una parte indispensable debido a que es el encargado de receptar, transmitir y administrar los diferentes datos de los dos sistemas tanto como los de RFID como los del Bluetooth para organizar los datos recibidos por la parte RFID se realizo lo siguiente:

- Conexión y activación de los contactos por la interfaz del dispositivo.
- Reinicializar la tarjeta.
- Respuesta al restablecimiento por la tarjeta.
- Intercambio subsiguiente de información entre la tarjeta y el dispositivo de interfaz.
- Desactivación de los contactos por la interfaz del dispositivo.
- Recibe y almacenar en un registro los pulsos correspondientes a la señal Wiegand 26 enviados por la lectora RFID.
- Los datos son enviados en una conexión punto a punto.
- Estos son distribuidos en tres registros de donde los bits luego son enviados mediante el sistema Bluetooth.

La de cada uno de los puertos del microcontrolador se muestra en la figura 2.4

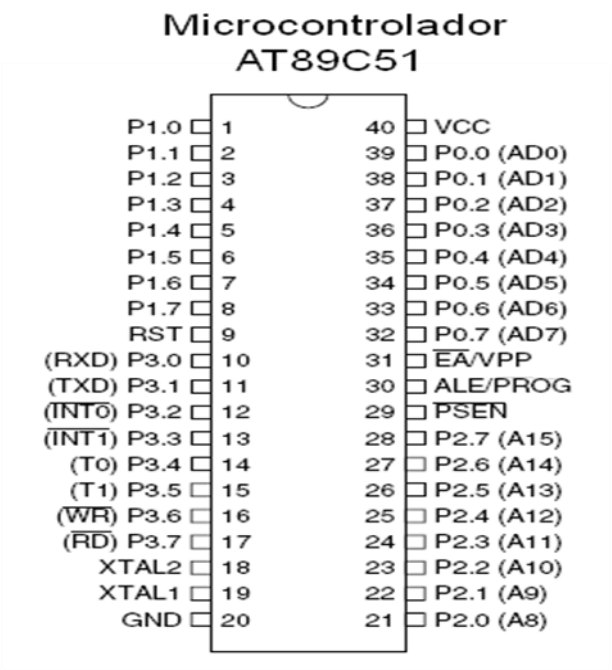


Figura 2.4 Disposición Física AT89c51

AT89C51 es un microcontrolador desarrollado por la empresa ATMEL, físicamente se compone de 40 pines, con cuatro puertos de 8 bits cada uno, estos pueden funcionar como entrada, o salida de datos, las cuales utilizan niveles de voltaje TTL de 5 Voltios, tiene también 8 pines de control como VCC, tierra y dispositivos de Oscilación entre las características más importantes son:

- CPU de 8 bits, optimizado para aplicaciones de control.
- Procesador Booleano (operación sobre bits).
- Espacio de memoria de programas de 64 KBytes.
- Espacio de memoria de datos de 64 KBytes.
- 4 Kbytes de memoria interna de programa.
- 128 bytes de memoria RAM interna.
- 32 líneas de entrada salida, direccionables bit a bit.
- 2 temporizadores/contadores de 16 bits.

- Comunicación asíncrona full dúplex.
- 5 fuentes de interrupción.
- Oscilador interno.
- 4 puertos

Los Microcontroladores prestan funciones que permiten realizar interrupciones, manejo del puerto serial, modos de operación en los cuales se programa números de bits de transmisión y recepción, la paridad y velocidad de transmisión.

Para el desarrollo del prototipo de utilizo los puertos P1.0 y P1.1 los cuales tienen las conexiones de los datos Dato 0 y Dato 1 respectivamente teniendo en cuenta que tendremos que estar monitoreando los dos puertos e ir organizando los datos que vamos recibiendo de los Tag.

Para la recepción de los datos en el microcontrolador AT89c51 es necesario como utilizar los marcos estándar que son usados para el intercambio de datos y esta compuesto por los siguientes bits que se muestra en la figura 2.5:

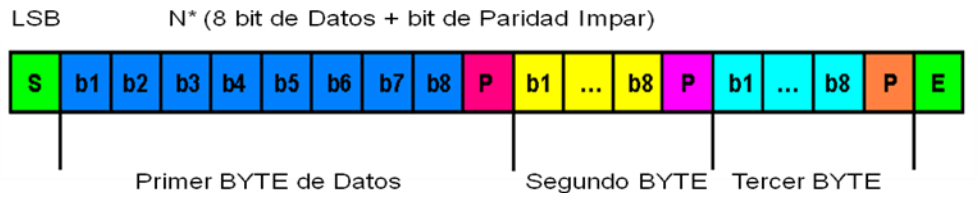


Figura 2.5. Marco Estándar

- **S** Primer bit Transmitido
- **LSB** Bit menos significativo
- **P** Bit de paridad
- **E** Fin de Transmisión
- **(S)** Inicio de comunicación

- **N*(8 bits de datos + bit de paridad impar)** con n ≥ 1. El bit menos significativo de cada byte es transmitido primero. Cada byte de datos es seguido por un bit de paridad impar.
- **(E)** Fin de la comunicación

Estados de la tarjeta de proximidad especificada para el protocolo de detección de colisiones se muestra en la figura 2.6.

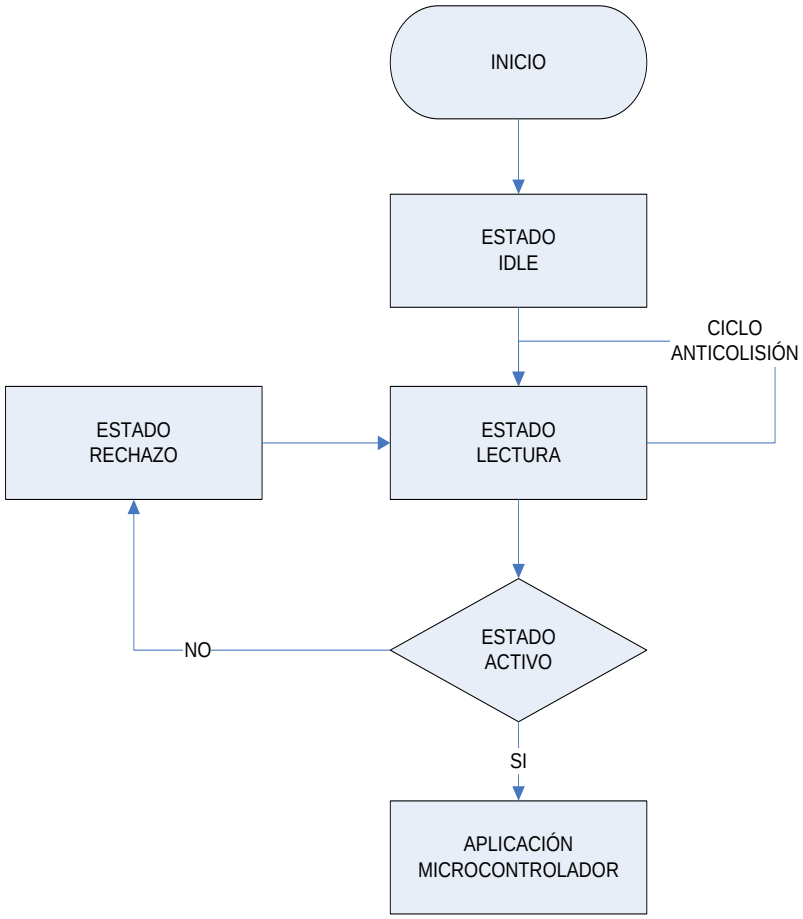


Figura 2.6 Diagrama de estado

- En el Primer Estado (INICIO) la tarjeta de proximidad no esta energizada debido a la falta de energía en el carrier y no se debe emitir subcarrier.

- Después de que el campo ha sido activado por un retraso máximo, la tarjeta de proximidad debe entrar a su estado inactivo (IDLE), en este estado, la tarjeta de proximidad es encendida, y es capaz de re modular y reconocer comandos validos del dispositivo de acoplamiento.

- Una vez ingresado es recibido se entra en el estado listo (LECTURA) y se sale cuando la tarjeta de proximidad es seleccionada con la identificación única (UID). En este estado se puede aplicar el marco de bit anticolisión o cualquier otro método anticolisión opcional.

- Una vez seleccionada la tarjeta de proximidad con su identificación única completa se entra en el estado activo (ACTIVO).

- Se entra en el estado de parada (RECHAZO) bien sea que no sea activada o no ingresada o se ingrese un comando específico de la aplicación como la de DESACTIVACIÓN. En este estado la tarjeta de proximidad debe responder únicamente al comando de nuestra aplicación, que conduce a la tarjeta de proximidad a su estado listo (LECTURA)

- Para finalizar la tarjeta de proximidad ingresa al Estado (APLICACIÓN) la cual dependiendo del programa de administración de acceso guardara sus datos en una base de datos.

2.2. INTERCONEXIÓN ENTRE MICROCONTROLADOR Y BLUETOOTH

Obteniendo un resultado favorable del bloque entre la tecnología RFID y el micro controlador tendremos que tomar en cuenta el acoplamiento del micro controlador AT89c51 y el dispositivo Bluetooth KC – 21 para ello tendremos realizar un análisis de los dos elementos para que la parte de interconexión tenga un correcto funcionamiento.

En la figura 2.7 se ilustra un diagrama de bloques que conforman el bloque de conexión.

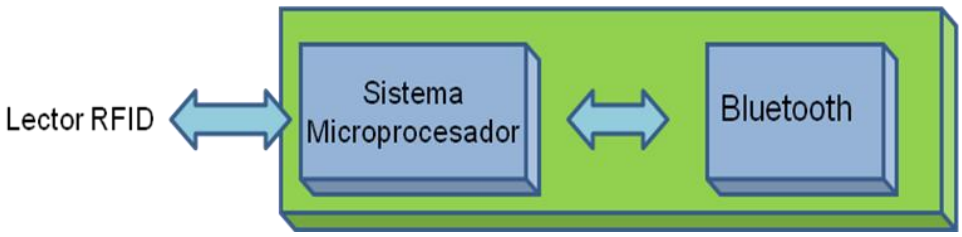


Figura 2.7 Diagrama de Bloque entre Microcontrolador y Bluetooth

2.2.1. TRANSMISIÓN DE DATOS CON EL MICROCONTROLADOR

Como ya se explico en el ítem **2.1.2** las características, descripción, almacenamiento y recepción del micro controlador AT89c51 ahora describiremos la interconexión con el dispositivo Bluetooth tanto para transmitir los datos capturados como para receptar los datos que provienen de nuestra unidad de administración del sistema en este caso un PC.

El microcontrolador está listo para recibir datos de los lectores que captaron de los tags ya que en todo momento esta monitoreando las entradas de ingreso, estos son procesados por el microcontrolador y enviados de manera serial a través del módulo Bluetooth KC – 21.

El microcontrolador sigue su funcionamiento normal sin interrupciones pero hay que tener en cuenta que siempre está pendiente de la bandera de interrupción serial que proporciona el modulo Bluetooth KC – 21, aun si se encuentra atendiendo a una bandera de recepción de datos por el pórtico serial y por esta razón es en el cual este momento se produce la interrupción, hasta realizar el proceso respectivo.

El proceso de transmitir es una conexión sencilla punto a punto lo cual hace que los datos sean transmitidos en una conexión la cual tiene un uso compartido de los recursos e identifica procesos o servicios que se comunican dentro de los dispositivos finales.

Para ahorrar recursos en el momento de enviar los datos con el dispositivo Bluetooth, restringimos datos que le pertenecen a los tag como son los del código de facilidad (Facility Code) mostrados en la figura 2.3, debido a que todos los tag

contienen la misma serie por ende para transmitir no se lo realiza el envió de los 26 bits que son registrados de las lectoras si no solamente de 18 bits, haciendo mas óptimo y menorando el trafico en la red inalámbrica.

El micro controlador AT89c51 enviará la secuencia de datos que son los correspondientes al código de usuario (USER ID) mostrado en la figura 2.3, debido a que cada tag tiene un código diferente poseyendo un promedio de 65536 posibles números de tarjetas diferentes o lo que es igual a 2^{16}.

2.2.2. TRANSMISIÓN DE LOS DATOS EN LA TECNOLOGÍA BLUETOOTH

Para realizar comunicación de los dos dispositivos el microcontrolador y el dispositivo Bluetooth se realizo una conexión serial, mientras que para los dos dispositivos que conforman la red inalámbrica se que se realiza a corta distancia ya que gracias a los servicios o perfiles que el estándar suministra permite tener una factible comunicación a los diferentes tipos de aplicaciones.

La técnica de saltos de frecuencia en la banda ISM de 2.4 GHz garantiza que los datos lleguen a su destino de manera segura, evitando frecuencias que puedan interferir con el correcto funcionamiento del enlace.

A continuación en la figura 2.8 se muestra la imagen real el dispositivo Bluetooth KC – 21

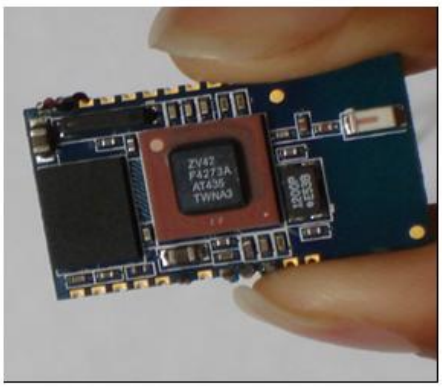


Figura 2.8 Dispositivo Bluetooth KC – 21

En el mercado existen varios módulos Bluetooth para diferentes aplicaciones, los servicios o perfiles, es la característica principal por lo que se eligió el módulo Bluetooth KC-21, a mas de esto, también brinda la facilidad de velocidad de transmisión alta, alcanzando los 921 Kbps en modo asincrónico, en cada una de sus 14 entradas. Este módulo también ofrece otras prestaciones, como: memoria flash, perfil SPP y configuración mediante comandos AT.

La figura 2.9 muestra el módulo Bluetooth KC-21, así como la distribución de los pines.

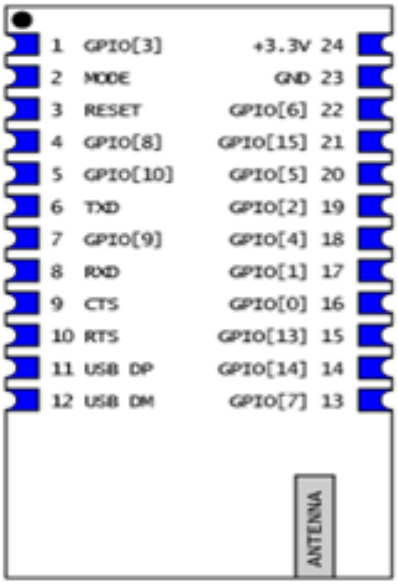


Figura 2.9 Módulo Bluetooth KC – 21 y su distribución de pines

Las Principales prestaciones del módulo KC – 21, son:

- Aprobado por el FCC y el consorcio Bluetooth
- RF totalmente resuelto
- Serial Port Profile (SPP) totalmente embebido
- Radio Clase 2
- Bluetooth v1.2
- Comunicación inalámbrica de datos
- Procesador ARM7 hasta 48MHZ

- Memoria Flash de 8Mb
- Tasa de trasmisión de datos de 921K baudios
- Antena Chip integrada
- Seguridad con encriptación de 128-bit
- Alcance de hasta 20m LOS
- Interface SPI de hasta 24Mhz
- 14 I/O de propósitos generales
- Set de Comandos AT
- Capacidad Multipoint

Los perfiles o servicios prestados por el módulo KC-21, hace que en el proyecto sea utilizado como un *transceiver* inalámbrico conectado al sistema de captura de datos de las etiquetas RFID controlado por el microcontrolador AT89C51.

El módulo Bluetooth KC-21, se lo configura a través de los Comandos de Atención (AT Command), los cuales tienen instrucciones codificadas específicas para cada uno de los propósitos como: velocidad, bit de paridad, bit de datos, entre otros. A través de la PC se configura los módulos, para lo cual, se utiliza un circuito conversor de voltajes de niveles RS-232 a TTL mediante el canal de comunicaciones serial, teniendo en cuenta que la interfaz utilizada para la configuración del módulo es el Hyperterminal

El circuito por medio del cual se realiza la conexión para la configuración de las especificaciones de transmisión mencionadas en el párrafo anterior se muestra en la figura 2.10.

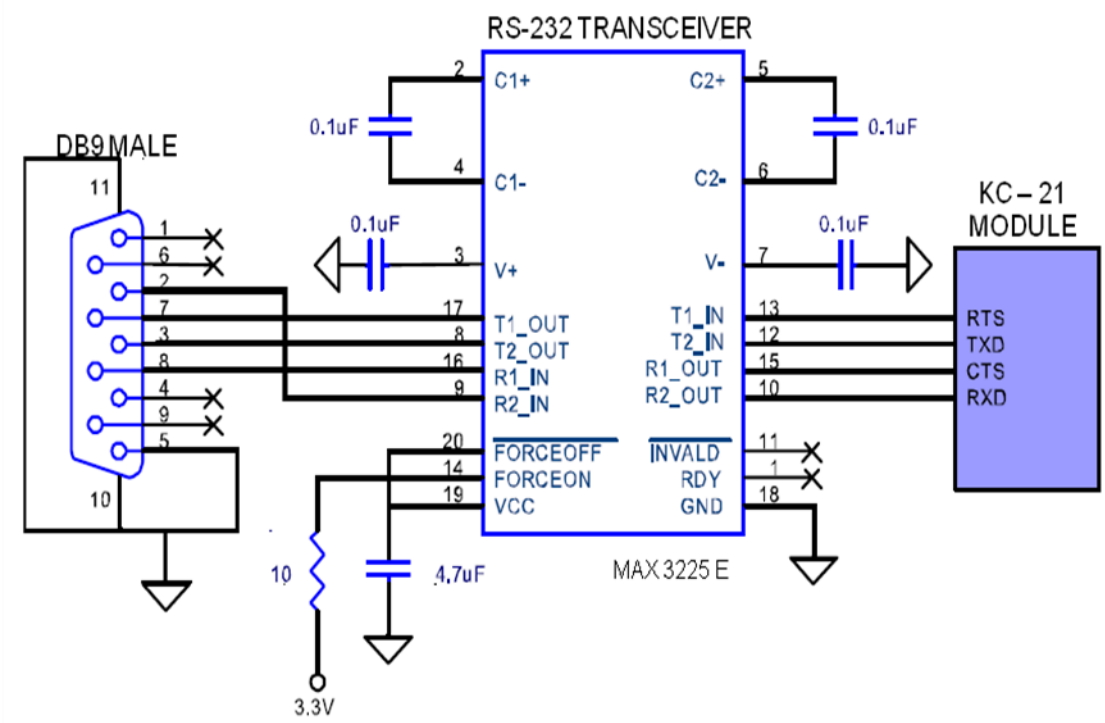


Figura 2.10 Circuito para configuración del módulo Bluetooth KC -21

2.3. CARACTERÍSTICA DE COMUNICACIÓN BLUETOOTH HACIA EL PC

Obteniendo un resultado favorable del bloque entre el microcontrolador y la tecnología Bluetooth tendremos que tomar en cuenta el acoplamiento del dispositivo KC – 21 y el puerto al cual le vamos a conectar al PC en este caso será un puerto USB para ello tendremos realizar un análisis de los dos elementos para que la parte de interconexión tenga un correcto funcionamiento.

En la figura 2.11 se ilustra un diagrama de bloques que conforman el bloque de conexión.

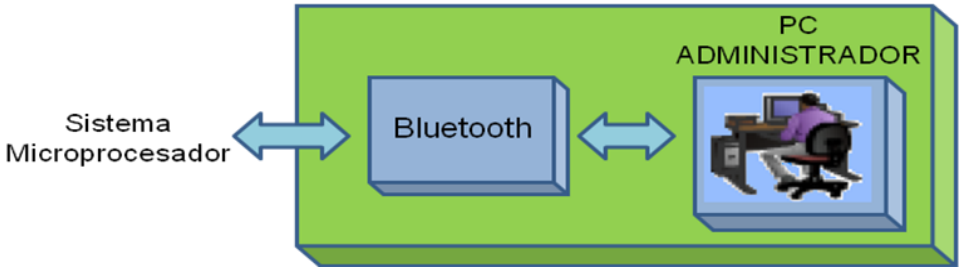


Figura 2.11 Diagrama de Bloque entre el Bluetooth y la PC

2.3.1. TRANSMISIÓN DE LOS DATOS EN LA TECNOLOGÍA BLUETOOTH

Como ya se explico en el ítem **2.2.2** las características, banda de frecuencia y configuración del dispositivo KC – 21, a continuación describiremos la interconexión con el dispositivo Bluetooth y nuestra unidad de administración del sistema en este caso con el puerto serial del PC.

Para establecer el enlace entre la PC y el dispositivo, se realizan un conjunto de pasos descritos a continuación:

- En la PC, se enciende el dispositivo Bluetooth externo, como se muestra en la figura 2.12

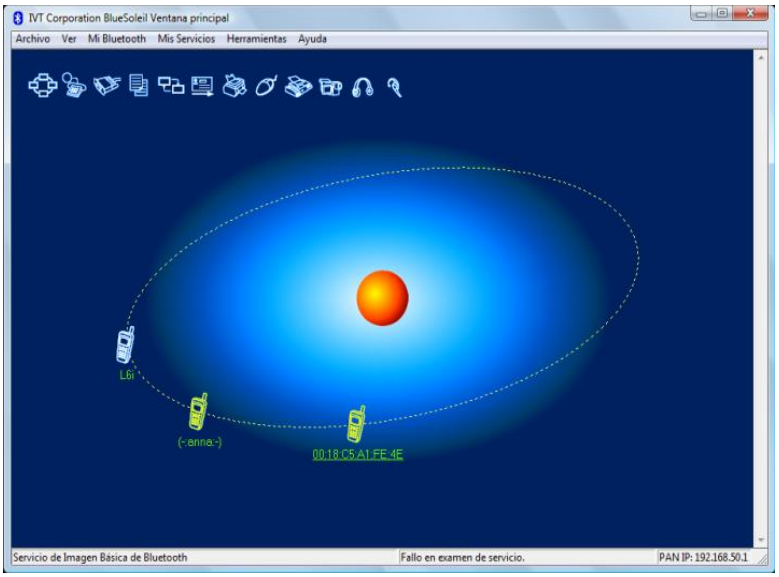


Figura 2.12 Encendido del adaptador Bluetooth en la PC

- El dispositivo Bluetooth externo de la PC trata de establecer un enlace con otros módulos Bluetooth no conocidos, mediante la negociación de la dirección del dispositivo (MAC Address).

- Una vez establecido el enlace, la PC inicia una comunicación con un solo módulo a la vez (conexión punto-punto), a través de un puerto serial de comunicaciones VIRTUAL (perfil puerto serial).

- La PC, a través de una aplicación, espera la información enviada desde la etiqueta RFID a través del microcontrolador.

- El microcontrolador, autentifica la secuencia de caracteres y envía la información solicitada al modulo Bluetooth (KC-21) conectado al puerto serial del mismo.

- El módulo Bluetooth KC-21, envía la información de las etiquetas hacia la PC, a través del canal inalámbrico establecido.

- Luego la PC, almacena dicha información en una base de datos, la cual es manipulada en un programa que sirve como interfaz grafica para el administrador del sistema, luego de esto se envía información de control hacia el microcontrolador, dicha información servirá para censar el acceso de los diferentes usuarios.

- La PC corta la comunicación con el módulo Bluetooth KC-21.

- El microcontrolador sigue censando el canal, esperando una nueva comunicación.

- Después de haber encontrado un nuevo inicio de comunicación del dispositivo con la PC, el procedimiento se repite.

2.3.2. TERMINAL DE EMISIÓN Y RECEPCIÓN DE DATOS (ADAPTADOR USB-BLUETOOTH).

Debido al tipo de comunicación que se realiza en el proyecto, es necesario e imprescindible que este elemento Bluetooth utilizado proporcione el "Servicio de Puerto Serie de Bluetooth" mediante el cual se puede emular una comunicación serial virtual, el cual permite el envío y recepción de datos desde y hacia los dispositivo finales de nuestro sistema de supervisión.

2.3.3. ADAPTADOR USB-BLUETOOTH

El adaptador USB-Bluetooth es utilizado comúnmente para la trasferencia de archivos entre el PC y otros dispositivos con tecnología Bluetooth, como celulares, Palms, PDA, Notebooks, impresoras y todos los dispositivos que presten esta tecnología inalámbrica. Este dispositivo presenta características que permiten realizar conexiones de hasta 100 metros. Además el adaptador USB-Bluetooth, provee el servicio de un puerto serial de envío y recepción de datos, el cual es configurado con los mismos parámetros de configuración del módulo Bluetooth KC–21.

En la figura 2.13 se tiene una imagen del adaptador USB-Bluetooth con su respectivo software.

Figura 2.13 Adaptador Bluetooth con su respectivo software

2.3.4. CARACTERÍSTICAS DEL ADAPTADOR USB-BLUETOOTH

Para poder realizar la conexión inalámbrica entre dispositivos que presenten la tecnología Bluetooth, es necesario que se cumplan características técnicas, para conseguir los objetivos de facilitar las comunicaciones entre equipos móviles y fijos y tener la posibilidad de realizar pequeñas redes inalámbricas; estas especificaciones son las que se presentan a continuación:

- Bluetooth V2.0 compatible
- Compatabilida: USB UHCI / OHCI spec 2.0 (USB 1.1 compatible)
- Interface USB
- Rango de operacion:0-100M(Bluetooth class l)
- LED indicador de estado
- Banda de frecuencia: 2.4GHZ ISM banda abierta
- Single chip Bluetooth sistema con tecnología de CMOS
- Tarifa máxima de la fecha: 1MB
- Sensibilidad:-89dBM 0.1%BER
- Peso: 43g
- Medidas: 5.3×2×1cm

Para que el adaptador USB – Bluetooth funcione correctamente, se necesita el soporte del sistema, los cuales pueden ser:

- Windows 98/98SE/ME
- Windows 2000
- Windows XP/VISTA

2.4. DIAGRAMA DE BLOQUES DEL SISTEMA DE ACCESO COMPLETO

A continuación en la figura 2.14 mostraremos el diagrama de Bloque completo del sistema de supervisión

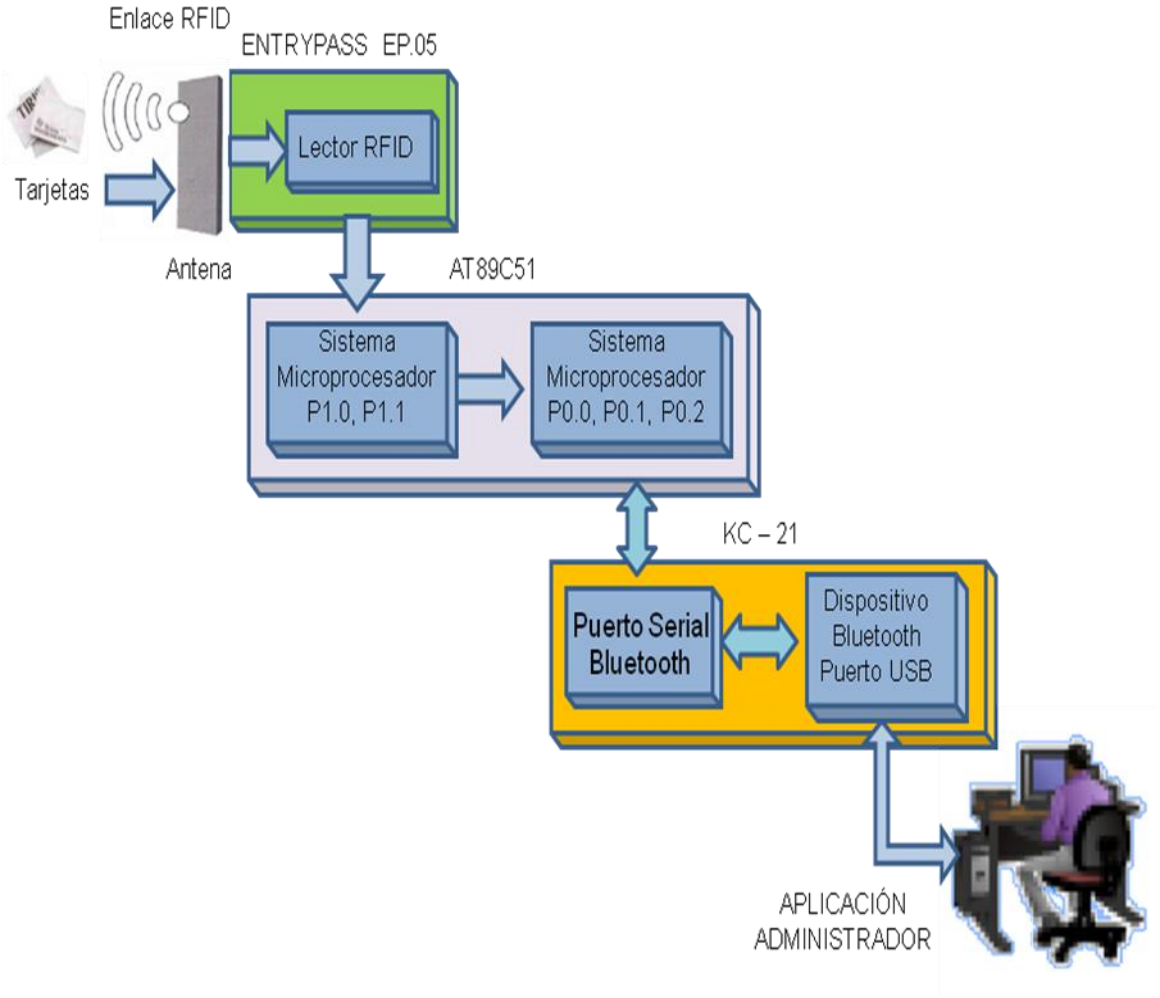


Figura 2.14 Diagrama Completo del Sistema

2.5. DIAGRAMA DE FLUJO COMPLETO DEL FUNCIONAMIENTO DEL HARDWARE DEL SISTEMA

A continuación se muestra un diagrama de Flujo del hardware del sistema de supervisión

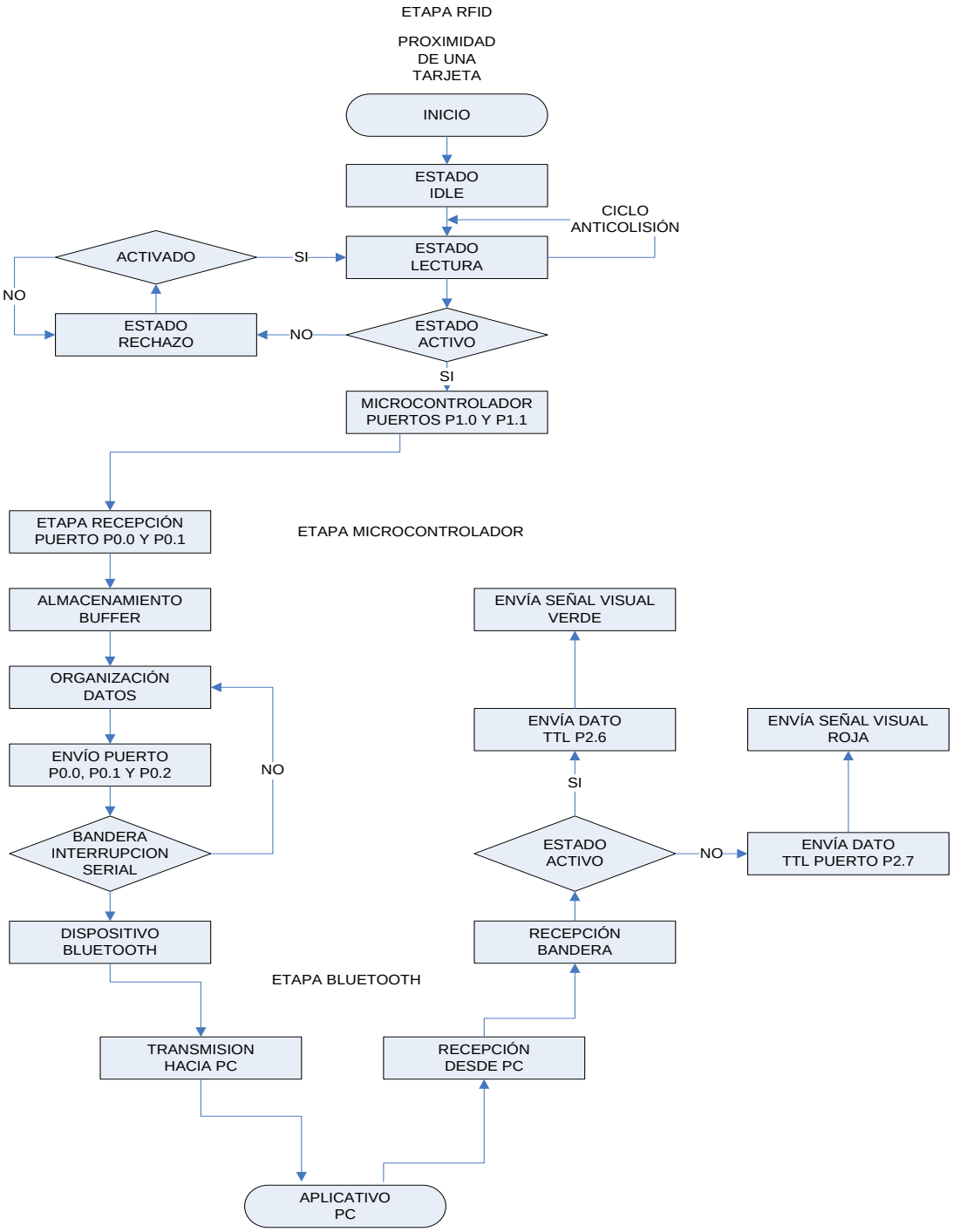


Figura 2.15 Diagrama de Flujo de Hardware del Prototipo

2.6. DIAGRAMA DEL CIRCUITO REALIZADO EN ORCAD

Realización de diagrama del circuito en ORCAD

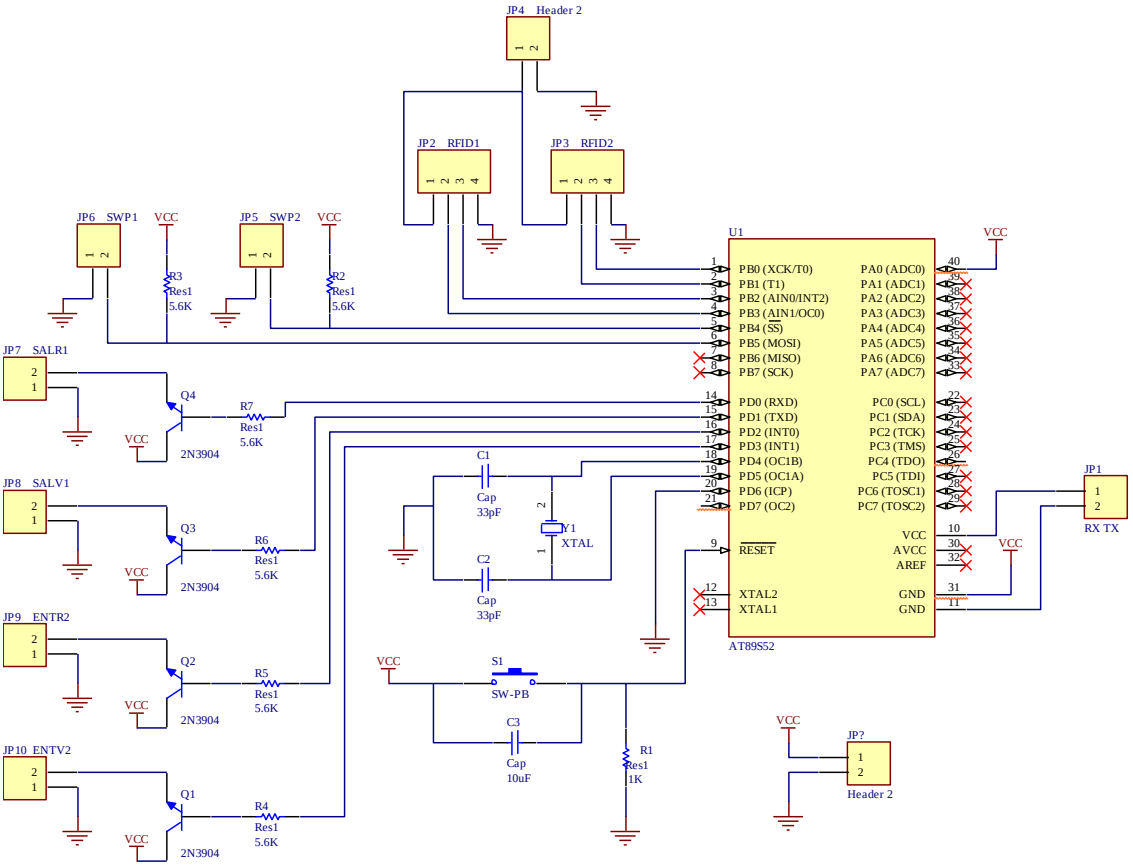


Figura 2.16 Diagrama del Circuito Implementado

CAPITULO 3

DISEÑO DE LA INTERFAZ DE USUARIO

En este capitulo nos referiremos a la parte del Software desarrollado para la implementación del prototipo, se ha visto la necesidad de realizar la creación de una base de datos y una interfaz hombre maquina, lo cual facilitará la utilización del sistema de supervisión, dándole un aspecto amigable de manejo tanto con el almacenamiento, búsqueda, modificaciones de los datos y la fase de transferencia de información con el Bluetooth, haciendo más sencillo la distribución de cada bloque.

Mediante la Base de Datos desarrollada podemos tener un reporte de los usuarios que ingresan y salen en cada día, los datos personales como: nombre, apellido, cedula de identidad y teléfono, además el control de los tags tanto para la activación y la desactivación de los mismos

Para el diseño del sistema de supervisión de acceso la parte del software de lo ha divido en dos partes que son las siguientes:

- Interfaz Hombre Maquina
- Base de Datos

La combinación de Microsoft Access y Microsoft Visual Basic nos proporciona una excelente herramienta para la creación de bases de datos (Access) y su acceso (Visual Basic) que nos permite administrar el sistema de supervisión de acceso permitiendo construir una base datos que se amolden a nuestras necesidades particulares.

3.1. DESCRIPCIÓN DEL PROGRAMA DE ALMACENAMIENTO

A continuación describiremos el lenguaje de programación que se utilizó para realizar la Base de Datos de nuestro sistema de supervisión la cual fue desarrollada en Microsoft Access 2007.

Para el desarrollo de la Base de Datos primero se tuvo que diseñar previamente las tablas con el contenido de los datos que se iban a manejar en cada una de ellas, tanto para los usuarios como para los diferentes Tags, con toda la información distribuida tenemos que relacionar las tablas para tener un mejor desenvolvimiento.

Para el diseño de la tabla que se utilizará, indicare los pasos de cómo fue desarrollada:

- Crear una carpeta que será **exclusiva** para el proyecto de tesis la cual la llamare: "**Proyecto_tesis**" para guardar todos los componentes del proyecto.
- Iniciar una sesión del programa Microsoft Office Access en este caso 2007 ya que nos da ventaja y facilita para el desarrollo.
- A continuación se eligió Nueva Base de Datos en Blanco le ponemos un nombre y clic en Crear.

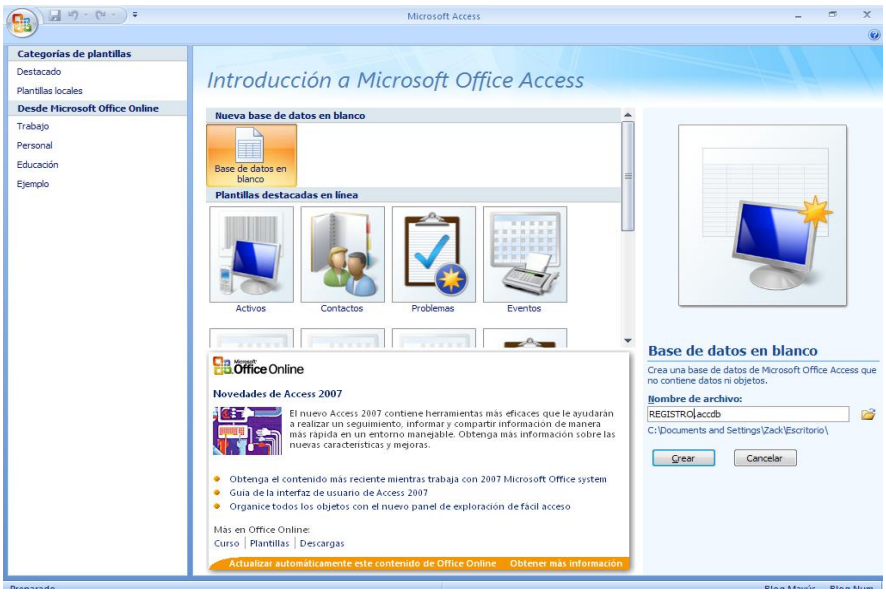


Figura 3.1 Inicio de Base de Datos

- Haz clic en **Crear**, **Diseño de Tabla.**

- Y se abrirá el **Administrador datos**, en la cual se añadirá los datos que necesitemos controlar, teniendo en cuenta que cada **Nombre del Campo** tiene que tener el tipo de dato ya sea: Texto, Número, Fecha/Hora, etc.
- A continuación escribe el nombre del primer campo de la tabla que estamos creando, para agregar campos en la tabla, haz clic en **Agregar campo,** en la tabla Usuario del Proyecto se agregó siete campos,: IDEN_USUA, CI, NOMBRES, APELLIDOS, NUM_TEL, FECHA_ENTREGA y TARJETA.

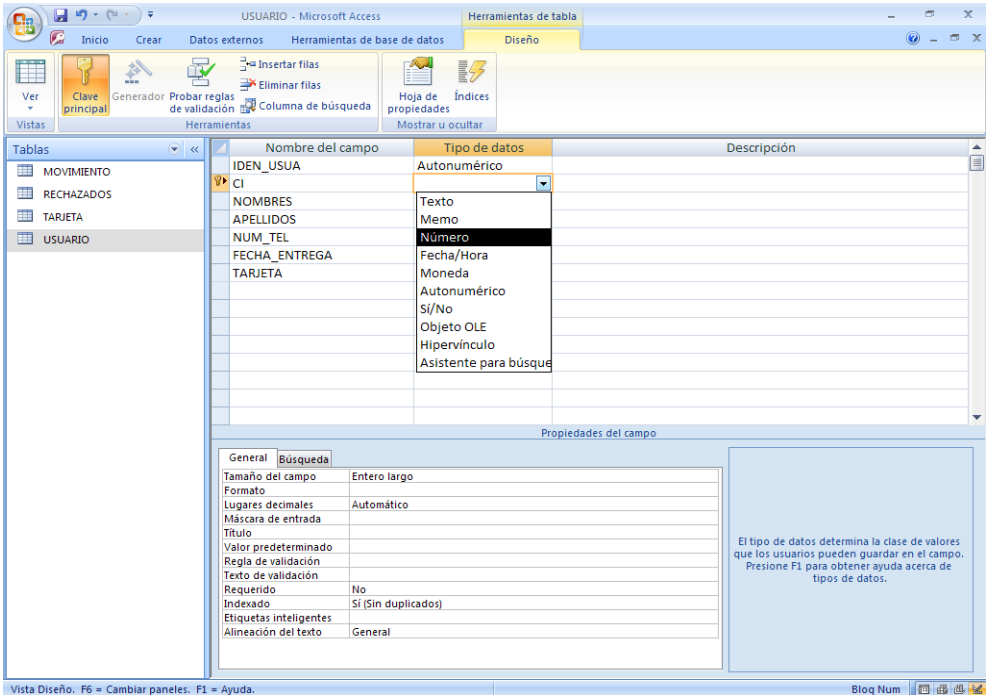


Figura 3.2 Creación de Tablas

- En **Tipo**: selecciona el tipo de datos que contendrá el campo, en nuestro caso serán:
  - Campo: NOMBRES, tipo de datos: texto, tamaño: 50
  - Campo: APELLIDOS, tipo de datos: Texto, tamaño: 50
  - Campo: NUM_TEL, tipo de datos: Número, tamaño: Entero Largo
  - Campo: CÉDULA: tipo de datos: Número, tamaño: Entero Largo
  - Campo: TARJETA: tipo de datos: Número, tamaño: Entero Largo

- Campo: IDEN_USUA: tipo de datos: Auto numérico, tamaño: Entero Largo
- Campo: FECHA_ENTREGA: tipo de datos: Fecha/Hora, tamaño: Fecha Corta

- En **Tamaño**: selecciona la cantidad de caracteres (incluyendo espacios) que tendrá el campo (ver arriba) y haz clic en **Aceptar**.
- Para agregar otra tabla dar un clic en **Crear, Tabla,** repite los pasos anteriormente mencionados
- Al crear una tabla y campos, y recuerda que cada tabla tendrá Nombre, Tipo y Tamaño, para cada campo que tendrá la tabla.
- Se desarrollo cuatro tablas diferentes las cuales son: USUARIO, TARJETA, RECHAZADOS Y MOVIMIENTO, la cuales tendrán los siguientes datos
  - TARJETA, la encargada de almacenar los datos con respecto a los números de cada Tag y los campos y tamaños son los siguientes:
    - Campo: TARJETA: tipo de datos: Número, tamaño: Doble
    - Campo: ESTADO: tipo de datos: Sí/No, tamaño: Doble
    - Campo: Id: tipo de datos: Autonúmerico, tamaño: Doble

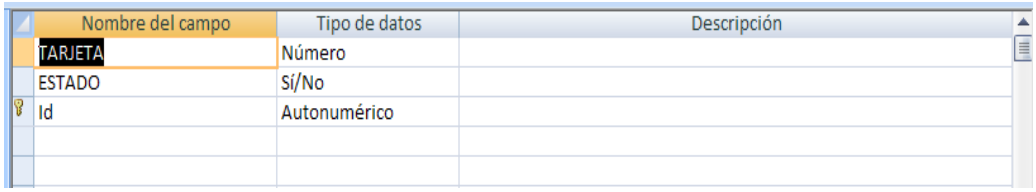


Figura 3.3 Diseño Tabla Tarjeta

  - RECHAZADOS, la encargada de cada Tag que no se encuentran almacenadas, los campos y tamaños son los siguientes:
    - Campo: TARJETA: tipo de datos: Texto, tamaño: 50
    - Campo: FECHA: tipo de datos: Fecha/Hora, tamaño: Fecha Corta

- Campo: HORA: tipo de datos: Fecha/Hora, tamaño: Fecha Corta
- Campo: Id: tipo de datos: Autonumérico, tamaño: Entero Largo

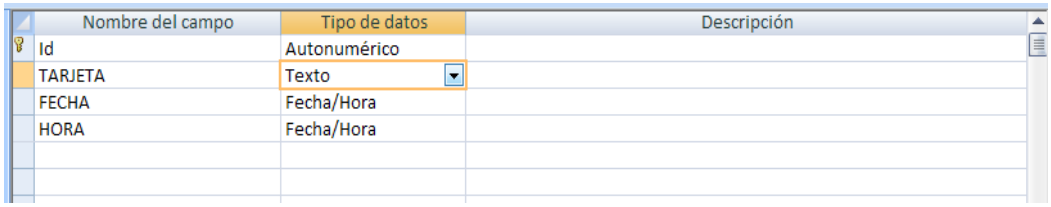
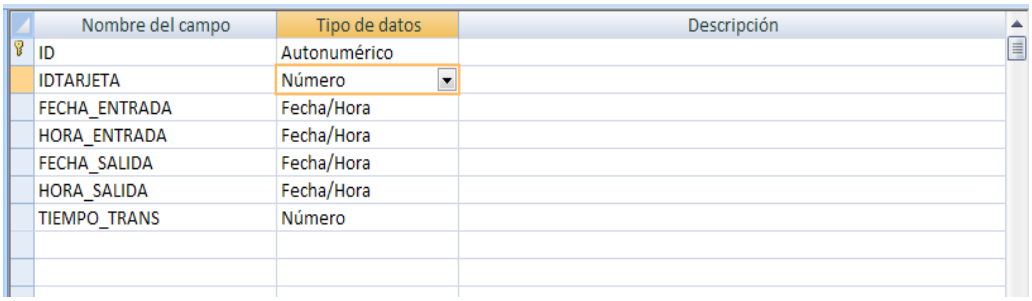


Figura 3.4 Diseño Tabla Rechazados

- MOVIMIENTO, la encargada de almacenar la entrada, salida, hora y fecha a la que ingresa cada Tag, los campos y tamaños son los siguientes:
  - Campo: IDTARJETA: tipo de datos: Número, tamaño: Doble
  - Campo: FECHA_ENTRADA: tipo de datos: Fecha/Hora, tamaño: Fecha Corta
  - Campo: HORA_ENTRADA: tipo de datos: Fecha/Hora, tamaño: Fecha Corta
  - Campo: FECHA_SALIDA: tipo de datos: Fecha/Hora, tamaño: Fecha Corta
  - Campo: Id: tipo de datos: Autonumérico, tamaño: Entero Largo
  - Campo: TIEMPO_TRANS: tipo de datos: Número, tamaño: Entero Largo



Nombre del campo	Tipo de datos	Descripción
ID	Autonumérico	
IDTARJETA	Número	
FECHA_ENTRADA	Fecha/Hora	
HORA_ENTRADA	Fecha/Hora	
FECHA_SALIDA	Fecha/Hora	
HORA_SALIDA	Fecha/Hora	
TIEMPO_TRANS	Número	

Figura 3.5 Diseño Tabla Movimiento

Una vez terminada la creación de las diferentes tablas tenemos que hacer una relación entre algunas de ellas, asumiendo que para las tablas que tendrán relación una con la otra debe tener una **Clave Principal**, la cual es un a variable que no debe repetirse en las otras tablas creadas previamente, siendo una variable única que le pertenecerá a dicha tabla como se muestra en la figura 3.6.

Asumiendo lo antes mencionado la distribución de las tablas quedaron de la siguiente manera:

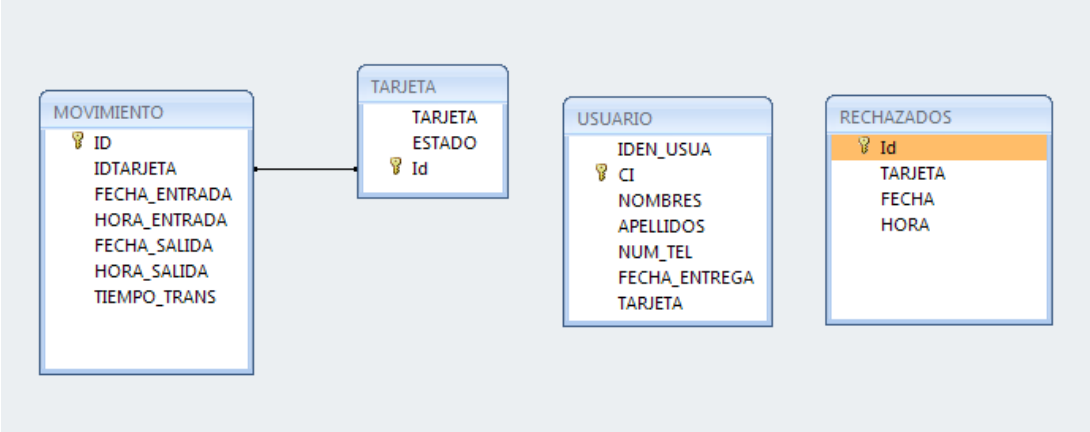


Figura 3.6 Relación Entre Tablas Creadas

Como podemos observar en la figura 3.6 la tabla MOVIMIENTO y TARJETA están relacionadas con la Clave Principal Id para TARJETA e IDTARJETA para MOVIMIENTO, con esto podemos tener las dos tablas interconectadas con variables que cada tabla la manipula, la razón de esta conexión es la de identificar cada Tag con el movimiento de la misma, decir su hora de entrada y salida, y así tener una identificación entre su movimiento con la tarjeta y su estado.

3.2. DESCRIPCIÓN DEL PROGRAMA COMO INTERFAZ PARA EL USUARIO

En este punto describiremos la aplicación que se utilizó para el sistema de control de acceso la cual fue desarrollada en el lenguaje de programación Visual Basic 6.0.

3.2.1. PREPARANDO LOS FORMULARIOS

En un formulario de Visual Basic se creo las **etiquetas** necesarias que correspondan –modificando su propiedad Caption- con los nombres de los campos de la tabla **Usuario**, a saber, IDEN_USUA, CI, NOMBRES, APELLIDOS, NUM_TEL, FECHA_ENTREGA y TARJETA, lo mismo se puede hacer con la otros formularios.

Crea las **cajas de texto** –dejando en blanco su propiedad **Text**- necesarias para mostrar el contenido de los campos y un control **Adodc1**, repite los pasos para cada tabla que tengas en tu base de datos.

Haz clic en el menú **Proyecto**, **Componentes**, selecciona el componente **Microsoft FlexGrid Control 6.0** y haz clic en **Aceptar**. Ahora el objeto se halla en la **Caja de herramientas**, dibújalo en el formulario para que se vea más o menos como se ve abajo.

Figura 3.7 Implementación Adodc1

3.2.2. CREANDO LA CONEXIÓN CON LA BASE DE DATOS Y LA TABLA

- Conectando el control Adodc1:

Selecciona el control **Adodc** y modifica sus propiedades como sigue:

- **DatabaseName**: localiza la carpeta del proyecto y selecciona **la base de datos** (REGISTRO) en donde se halla la tabla.
- **RecordSource**: selecciona **el nombre de la tabla** (USUARIOS) cuyos campos se mostrarán en el formulario.

- Conectando las cajas de texto

Selecciona el control **Adodc** y verifica su conexión con la base de datos pero antes revisa sus propiedades como se explica a continuación:

- Si no se pueden ver los registros en alguna de las conexiones, significa que no se conectaron correctamente el control **Adodc1** y las **cajas de texto**, simplemente revisa las conexiones una por una como a continuación le mostrare:

  - De un clic derecho en un conector **Adodc1** y elija la opción **ADODC Properties**

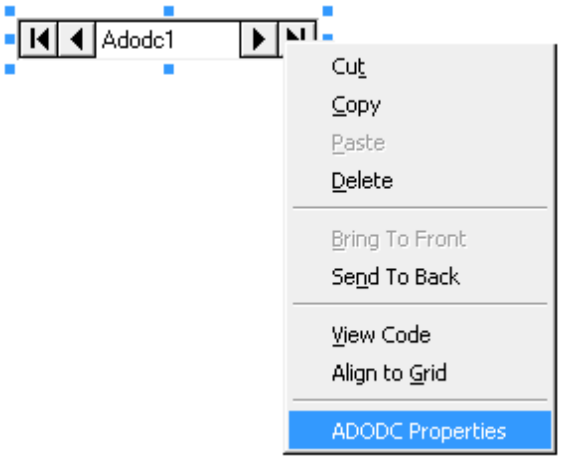


Figura 3.8 Propiedades ADODC 72

  - A continuación damos un clic en Build

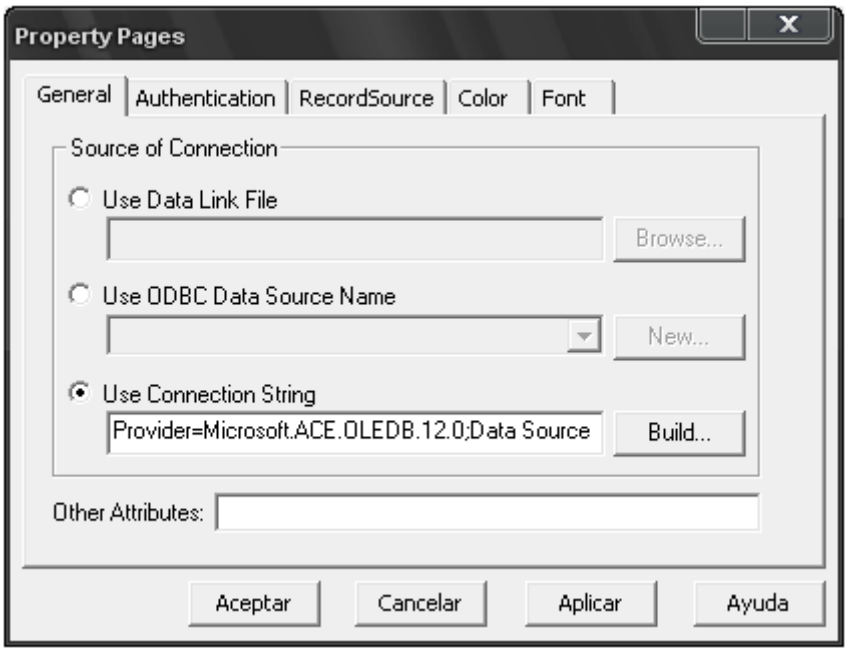


Figura 3.9 Property Pages

- Seguida dar un clic en el botón **Proba Conexión** y ver si te obtiene un resultado satisfactorio como se muestra a continuación en la figura 3.10

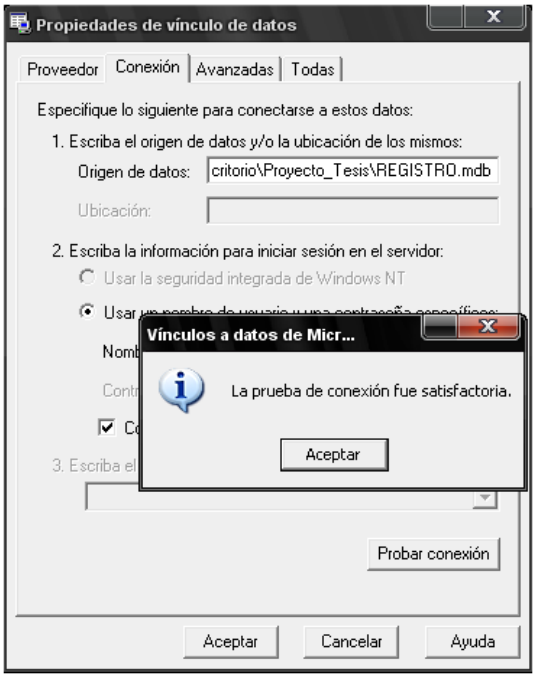


Figura 3.10 Verificación de Conexión

- Si no se obtiene un resultado satisfactorio revise que en el punto 1 el **Origen de Datos** este bien direccionada la ruta de la base de datos que generamos (REGISTRO) como se muestra en la figura 3.10.

3.2.3. CREANDO LOS DIFERENTES MENÚS

Para el Sistema de Acceso se diseño un formulario de ingreso, con una etiqueta y dos botones, como se muestra en la figura 3.11 a continuación.

Figura 3.11 Formulario de Ingreso

- El código del botón **ENTRAR AL PROGRAMA** es:

```
Private Sub Command1_Click()
        val_contraseña = Text_Contraseña.Text
If val_contraseña = Espe200& Then
        Form_Contraseña.Visible = False
        Form_Administrador.Visible = True
```

```
Else
        MsgBox "!!!  LA CLAVE ESTA INCORRECTA
End If
End Sub
```

Cuya función es la de ocultar el formulario de **BIENVENIDA** y mostrar el formulario de **ADMINISTRADOR**.

El código del botón **SALIR DEL SISTEMA** es:

```
        Private Sub Command2_Click()
        Unload Me
        End
        End Sub
```

Cuya función es la de cerrar el programa

Se creo un nuevo formulario llamada **ADMINISTRADOR**, para crear una caja de diálogo nueva realizamos los siguiente: **Project**, **Add Form**, **Form**, haz clic en **Abrir**.

El formulario ADMINISTRADOR contiene cuatro pestañas las cuales se detallaran a continuación:

- Pestaña INICIO

Figura 3.12 Forma Inicio

En esta pestaña se mostrara un preámbulo del Sistema de Acceso y tiene dos botones los cuales son: SALIR DEL PROGRAMA y ABOUT

- SALIR DEL PROGRAMA: Este botón nos servirá como dice el botón salir del sistema y el código ya lo mostramos en los pasos de arriba.

- ABOUT: Este botón servirá para dar información del sistema elaborado.

- Pestaña REPORTES:

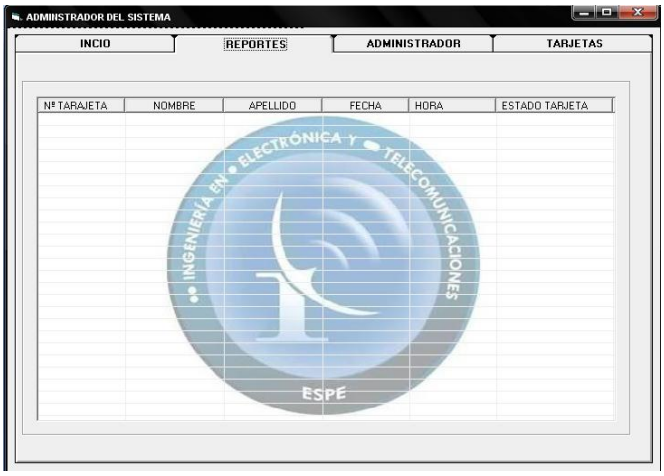


Figura 3.13 Forma Reportes

En el formulario REPORTES nos servirá para mostrar un reporte de las tarjetas que ingresan al Sistema de Acceso.

Para realizar que se muestren los datos necesarios se insertaron cuatro cuadros de texto T1, T2, T3 y T3, los cuales llevaran los datos almacenados como son: TARJETA, FECHA_INGRESO, HORA y ESTADO, respectivamente mostrando en la pestaña REPORTES.

- El código para el ListView1es el siguiente:

  Set Nuevo2 =.ListItems.Add(, , T1.Text)

  Nuevo2.SubItems(1) = T2.Text

  Nuevo2.SubItems(2) = T3.Text

  Nuevo2.SubItems(3) = T4.Text

- Pestaña ADMINISTRADOR Y TARJETAS

Se eligieron estas dos pestañas ya que se podrían tener un desenvolvimiento casi similar ya que las dos pestañas tienen botones como: GUARDAR, ELIMINAR, SALIR, a continuación se mostrara las pantallas de las mismas.

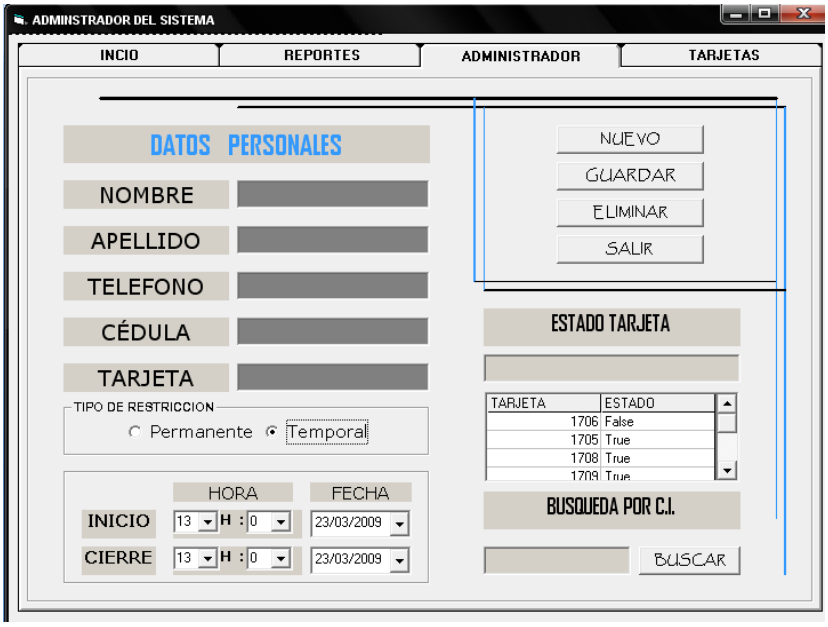


Figura 3.14 Forma Administrador

La forma Administrador es una de las mas importantes ya que aquí podremos almacenar los datos personales de los usuarios también podemos eliminarlos buscar una tarjeta que este libre para añadirle a un usuario y para terminar una opción de buscar un usuario si se encuentra en la base.

Figura 3.15 Forma Tarjetas

En la Forma Tarjetas nosotros podremos almacenar los números de los diferentes Tags, también borrarlos de la Base de Datos y salir del programa.

A continuación se mostrara el código que se empleo para realizareste Sistema para eso abre el menú y haz clic en cada una de las opciones del menú:

- Opción **GUARDAR**, el cual servirá para **crear un nuevo registro** en la tabla, el código es el siguiente:

  Private Sub nuevo_Click ()

  Data1.Recordset.AddNew

  End Sub

  P.D. Esta opción debe presionarse antes de dar de alta un nuevo registro en la base de datos.

- Opción **GUARDAR**, el cual servirá para **guardar un nuevo registro** en la tabla, el código es el siguiente:

```
Private Sub guardar_Click()
Consulta = "SELECT * FROM USUARIO"
        Adodc1.RecordSource = consulta
        Adodc1.Refresh
        Adodc1.Recordset ("VARIBLE BASE").Value = Dato.Text
        Adodc1.Recordset.Update
MsgBox ("EL USUARIO FUE ALMACENADO EN LA BASE")
End Sub
```

P.D. Esta opción debe presionarse una vez que se haya completado la información del registro.

- Opción **Buscar**, el cual servirá para **buscar un registro** en la tabla, el código es el siguiente:

```
Private Sub buscar_Click()
Dim Dato As Long
Dato = Val(InputBox("Introduce la Matrícula que Buscas"))
Adodc1.Recordset.FindFirst "USUARIO=" & Dato
If Data1.Recordset.NoMatch Then
MsgBox " NO EXISTE EL USUARIO QUE ENVIO A BUSCAR"
End If
End Sub
```

Nota: aquí declaramos una variable (**Dato**) que representará el número del registro (CÉDULA) que estemos buscando. Es de vital importancia que en la línea subrayada la palabra “USUARIO” esté escrita exactamente como llamaste el campo “USUARIO” al crear la tabla.

- Opción **Eliminar**, el cual servirá para **eliminar un registro** de la tabla, el código es el siguiente:

```
Private Sub Eliminar_Click()
If MsgBox("¿ESTA SEGURO QUE QUIERE ELIMINAR: " &
TextCI & "?", 16 + 4) = 6 Then
Data1.Recordset.Delete
Data1.Refresh
MsgBox "Se Eliminó la Matrícula
Else
MsgBox " NO SE ELIMINO EL USUARIO "
End If
End Sub
```

Ahora corre tu programa con la tecla **F5** dirígete al formulario y ahora podrás agregar, guardar, buscar y eliminar registros de las tablas: USUARIOS, TARJETA, RECHAZADOS y MOVIMIENTO de la base de datos de Access mediante Visual Basic.

CAPITULO 4

PRUEBAS DEL PROTOTIPO

Este capítulo describe pruebas técnicas y de nivel de satisfacción realizadas con el prototipo implementado.

4.1. PRUEBAS NIVEL DE SATISFACCIÓN

Con esta prueba se pretende evaluar el servicio que el dispositivo pudiera brindar a las personas que utilizan los laboratorios. La prueba del prototipo fue realizada con el montaje de mismo en una maqueta simulando el ingreso de los estudiantes, para lo cual se siguieron los siguientes pasos:

- **Primero.** Se procedió a explicar las diferentes etapas que tiene el prototipo y el modo en el que fueron acoplados para armar el sistema de control de acceso.

- **Segundo.** Se explicó y demostró el funcionamiento del dispositivo, con una capacitación previa del software desarrollado.

- **Tercero.** Se les facilito los *tags* y el dispositivo para que realizarán las distintas operaciones con los diferentes campos que tienen el software.

El dispositivo ha mostrado características que se adapta al medio en donde este puede ser implementado teniendo en cuenta que tiene la opción de que se puede modificar a las necesidades de los diferentes laboratorios, el sistema de acceso es útil y de fácil operación. Por otra parte, se requiere que el dispositivo tenga una base de datos de mayor capacidad, disponer de la mayor cantidad de tags y mayor alcance de lectura. Entre las

posibles aplicaciones se destacan la activación de los equipos que se encuentran dentro del laboratorio utilizando la misma tarjeta de identificación además de un sistema de vigilancia que acompañe a este dispositivo.

4.2. PRUEBAS TÉCNICAS

Con estas pruebas se pretende obtener especificaciones reales del dispositivo que ayudarán a establecer de mejor manera limitaciones en su funcionamiento. Al dispositivo se le hicieron las siguientes pruebas:

- **Prueba de energía** para conocer el número de lecturas que puede sostener la alimentación instalada y si existe problemas al transmitir los datos.

- **Pruebas de alcance** tanto para las lectoras *RFID* como para el modulo *BLUETOOTH*, para conocer la distancia máxima de lectura para diferentes tipos de etiquetas como para la transmisión de los distintos datos en la red inalámbrica.

- **Pruebas de software** para tener una idea del funcionamiento simulando un ambiente real y conocer las ventajas y desventajas que tiene el programa desarrollado.

4.2.1. PRUEBA DE ENERGÍA

Esta prueba consistió en realizar de manera consecutivas lecturas con el dispositivo usando una fuente de alimentación de: 5 V para el microcontrolador con una capacidad de 5 A, 12 V para las lectoras RFID con una capacidad de 18 A y 3.3 V para el modulo BLUETOOTH con una capacidad de 5A. Se obtuvo un sistema estable tanto al momento de realizar las diferentes lecturas con las lectoras RFID como al momento del envió y recepción de datos con el modulo BLUETOOTH en un tiempo aproximado de 5 horas

En estado de reposo, encendido y sin utilizar, el dispositivo consume 8 mA debido al consumo realizado por las lectoras por el motivo de que siempre tienen que estar

censando la presencia a alguna tag. El dispositivo no cuenta con una fuente de baterías extras.

4.2.2. PRUEBAS DE ALCANCE

Esta prueba consiste en saber las distancias máximas en que el dispositivo puede leer diferentes tipos de etiquetas de manera exitosa como también el alcance máximo y optimo para la transmisión de los datos con el modulo BLUETOOTH.

- **LECTORAS RFID.** Para esta prueba se usó una fuente externa de 12 V. Se empezó colocando la etiqueta a una distancia en la que se obtuvo una lectura exitosa, luego, se incrementaba la distancia hasta que ya no se obtuvo una lectura exitosa. Los resultados de esta prueba se encuentran en la tabla 4.1

Etiqueta RFID	DISTANCIA
Rectangular 7.5 cm. x 4.5 cm.	4
Rectangular 3.9 cm. x 2.3 cm.	3.5
Lámina circular 2.5 cm. de diámetro	3
Circulo pequeño 1.9 cm. de diámetro	0.7

Tabla. 4.1 Distancias máximas de lectura de etiquetas RFID

- **MODULO BLUETOOTH.** Para realizar las pruebas se utilizo una fuente constante de 3.3 V. colocando el transmisor y receptor a la distancia máxima que especifica este modulo en este caso es de 10 metros, dando como resultado perdidas de señal y retardos en la transmisión, para solucionar este inconveniente se redujo la distancia de la red inalámbrica llegando a la conclusión que la distancia máxima mas optima fue de 7 metros obteniendo así resultados favorables para el todo el sistema.

4.2.2.1. PRUEBAS DE SOFTWARE

Esta prueba consiste en saber la eficiencia del programa desarrollado para adaptarse a las necesidades de exigencia de un laboratorio real, conociendo el accionar y las facilidades que es para el administrador del dispositivo el manejo del mismo, dando como resultado que

el sistema es de fácil uso y que se adapta a las exigencias básicas de un laboratorio real pero teniendo en cuenta que el sistema se tiene que ir evaluando por lo menos semestralmente dando un mantenimiento de depurado la base de datos.

4.3. ANÁLISIS COMPLETO DE COSTO DEL SISTEMA DE ACCESO

Para el desarrollo del análisis de costos lo he dividido en dos grupos lo cuales son lo siguientes:

- **Análisis de costos SOFTWARE.** En esta parte se analizara el una relación tanto con el tiempo empleado y el valor económico que representa tanto para el programa desarrollado en Visual Basic 6.0 como la base de datos realizada en Microsoft Access 2007

- **Análisis de costos HARDWARE.** Se detallara todo lo referente a materiales que se utilizaron para la implementación del sistema, obteniendo la suma del gasto total y del valor de cada elemento.

4.3.1. ANÁLISIS DE COSTOS SOFTWARE

En la tabla 4.2 detallaremos un costo estimado del sistema determinado por la representación de las horas hombre.

CANTIDAD HORAS	DESCRIPCIÓN	VALOR TIEMPO HOMBRE(HORA)	VALOR TOTAL
30 h	Base Datos Microsoft Access	15 dólares	450
140 h	Programa desarrollado en Visual Basic 6,0	15 dólares	2100
10 h	Programa Microcontrolador	15 dólares	150
20 h	Programa Bluetooth	15 dólares	300
72 h	Mano de Obra	20 dólares	1440
		Valor Total	**4440**

Tabla. 4.2 Análisis Costo del Software

4.3.2. ANÁLISIS DE COSTOS HARDWARE

En la tabla 4.3 detallaremos el valor real de los materiales utilizados en el sistema de acceso.

CANTIDAD	DESCRIPCIÓN	VALOR UNITARIO	VALOR TOTAL
1	Potenciómetro de precisión 5 k	0,15	0,15
1	Pulsador (S7B)	0,20	0,20
2	1N4007	0,08	0,16
2	resistencia 220K	0,10	0,20
1	0,1 uF	0,10	0,10
7	10 uF	0,10	0,70
1	2N3904	0,10	0,10
2	S36C	0,50	1,00
2	led (Verde)	0,55	1,10
2	led (Rojo)	0,55	1,10
1	Placa Impresa	10,00	10,00
1	Microcontrolador AT89C51	6,00	6,00
1	Dispositivo Bluetooth KC – 21	60,00	60,00
1	Transceiver	15,00	15,00
2	Lectoras RFID	80,00	160,00
10	Tags	0,20	2,00
		Valor Total	**257,71**

Tabla. 4.3 Análisis Costo del Hardware

4.3.3. ANÁLISIS DE COSTOS DEL SISTEMA DE ACCESO

En la tabla 4.4 se mostrará el costo total del sistema de acceso

CANTIDAD	DESCRIPCIÓN	VALOR TOTAL
1	Costo Software	**4440**
1	Costo Hardware	**257,71**
	Valor total	**4697,71**

Tabla. 4.4 Análisis Costo Total del Sistema de Acceso

CAPITULO 5

CONCLUSIONES Y RECOMENDACIONES

Este capítulo describe pruebas realizadas con el prototipo implementado, conclusiones y recomendaciones

5.1. CONCLUSIONES

- Se logró diseñar e implementar un prototipo basado en la tecnología RFID y BLUETOOTH para identificar y sistematizar el ingreso permitido a un laboratorio.

- Como podernos darnos cuenta el sistema fue desarrollado para las exigencias de un laboratorio específico con la opción de que se puede ampliar su utilidad como es la de añadirle una red de cámaras de seguridad y así tener un sistema más robusto.

- El sistema de supervisión de acceso se divide básicamente en dos bloques: hardware que es la parte electrónica y tiene una sola tarea que es la de leer las tarjetas y la parte del software que es una parte que administra el dispositivo y este se pude cambiar para adaptarle para sistematizar otros elementos como son los equipos, libros, entrada y salida de vehículos, etc.

- Para obtener una red inalámbrica de mayor alcance existe la posibilidad de dos maneras, la primera es la de adquirir un transceiver y un modulo Bluetooth de un alcance de 100 metro lo cual antes de ponerlo a funcionar se deberá hacer las

pruebas respectivas para ver su distancia mas optima y la segunda será la de configurar una red *scatternet* la cual se basa en la unió de varias piconets.

- Este sistema seria beneficioso viéndolo por el lado de costo beneficio debido a que tendremos a comparación de otros sistemas el almacenamiento en una base de datos la cual nos permitirá guardar el movimiento de los diferentes tags pero esto es solo uno de las virtudes que tiene el dispositivo ya que mediante el programa desarrollado se puede restringir el acceso, activación, desactivación de los tags.

- Debido a que Bluetooth trabaja en la banda libre de 2.4GHz el modulo y transceiver Bluetooth se tuvo que configurar en un modo point to point serial, con el cual nos brinda la característica de que no tenga interferencias con otros equipos que tengan esta tecnología.

- Debido a cantidad de datos que contiene una tarjeta Wiegand 26 se tuvo que restringir los datos comunes de los tags en este caso fueron los cuatro ceros con las cuales empezaba el número de las tarjetas, teniendo en cuenta que se podrá tener una capacidad máxima de 65 536 posibles usuarios.

5.2. RECOMENDACIONES

- El sistema puede ser mejorado adaptándolo una fuente de baterías en el caso de que faltare la luz eléctrica

- Para que el sistema funcione adecuadamente se deberá dar una capacitación al personal que va administrar el sistema, teniendo en cuenta que se deberá dar un mantenimiento tanto a la parte del Hardware como la parte del Software en este caso será la de depurar la base de datos.

- Para que el dispositivo pueda almacenar un mayor número de etiquetas se podrá utilizar una base da datos de mayor capacidad

- De acuerdo a las pruebas y nivel de satisfacción, se recomienda que el dispositivo posea un mayor alcance en cuanto a la red inalámbrica y en cuanto al Software que contenga una interfaz más grafica y posea un diseño atractivo.

- La parte electrónica como son las lectoras, microcontrolador y Módulo bluetooth no debe tener contacto con el agua causada por cualquier motivo como puede ser lluvia, etc., ya que esto haría que el sistema deje de funcionar.

GLOSARIOS DE TÉRMINOS

En esta sección encontrará palabras usadas en la presente tesis y sus respectivos significados.

TECNOLOGÍA RFID

Biometría: La biometría es la ciencia que se dedica a la identificación de individuos a partir de una característica anatómica o un rasgo de su comportamiento, como pueden ser la identificación por huellas dactilares, el iris de los ojos, los rasgos faciales, el patrón de la voz, el reconocimiento por ADN entre otros. [13]

Etiqueta activa: Clase de etiqueta RFID que tiene una fuente de energía, por ejemplo una batería, que suministra energía al sistema de circuitos del microchip. Las etiquetas activas transmiten al lector una señal que puede ser leída desde una distancia de 100 pies (35 metros) o más. [12]

Etiqueta inteligente: Rótulo que contiene una etiqueta RFID que puede almacenar información como ser un número seriado singular y comunicarse con un lector.

Etiqueta pasiva: Etiqueta RFID que no contiene una fuente de energía. La etiqueta genera un campo magnético cuando las ondas radioeléctricas de un lector llegan a la antena. Este campo magnético energiza la etiqueta y le permite enviar la información almacenada en el chip. [12]

Etiqueta RFID: Microchip adherido a una antena que envía datos a un lector RFID. La etiqueta RFID contiene un número seriado único, y también pude contener datos adicionales. Las etiquetas RFID pueden ser activas, pasivas, o semi pasivas. [12]

Identificación por radio frecuencia: Tecnología portadora de datos que transmite información mediante señales en la porción de radio frecuencia del espectro

electromagnético. Un sistema de Identificación por Radio Frecuencia consiste de una antena y un transmisor-receptor, que lee la radio frecuencia y transmite la información a un dispositivo de procesamiento, y un transportador, o etiqueta, que es un circuito integrado que contiene los circuitos de radio frecuencia y la información que será transmitida. [12]

Identificación y captura de datos automática: Tecnología asociada con la creación y adquisición de datos legibles por una máquina. Las tecnologías primarias son códigos de barras y la Identificación por Radio Frecuencia (RFID). [12]

Interfaz aérea: Conexión de radio frecuencia entre un lector y etiquetas RFID. [12]

Lector RFID: Un lector RFID se comunica mediante ondas radioeléctricas con las etiquetas RFID y entrega información en formato digital a un sistema informático. También se lo conoce como Interrogador o lector. [12]

Lectura: Proceso de traducción de ondas radioeléctricas de una etiqueta RFID en bits de información que pueden ser utilizados por una computadora. [12]

Longitud de onda: Medida de la distancia entre el comienzo y el final, dos puntos correspondientes, o el ciclo completo de una onda. Para verificadores o escáneres, esta es la unidad, medida en nanómetros, de la energía lumínica emitida por el dispositivo. Esta es una de las dos condiciones que afectan los cálculos de los parámetros necesarios para crear un grado de símbolo ISO 15416 formal. [12]

Nivel de energía: Cantidad de energía de radio frecuencia irradiada de un lector RFID o una etiqueta activa. Cuanto mayor es el nivel de energía, más amplio es el rango de lectura. La mayoría de los gobiernos regula los niveles de energía para evitar interferencias con otros dispositivos. [12]

OCR: (Optical Character Recognition) es la tecnología que se utiliza para escanear y reconocer los caracteres impresos en cualquier tipo de documentos en segundos.

Radio frecuencia: Cualquier frecuencia dentro del espectro electromagnético asociada con la propagación de ondas radioeléctricas. Cuando se proporciona una corriente de radio frecuencia a una antena, se genera un campo electromagnético que entonces tiene capacidad para propagarse a través del espacio. Muchas tecnologías inalámbricas se basan en propagación del campo de radio frecuencia. [12]

Rango de escritura: Distancia entre un lector y una etiqueta RFID a la cual las operaciones de escritura de datos pueden realizarse en forma confiable. [12]

Rango de lectura: Distancia máxima a la cual un lector puede enviar o recibir datos de una etiqueta RFID. Las etiquetas activas ofrecen un rango mayor que las etiquetas pasivas como resultado de la batería que utilizan para transmitir señales al lector. El rango de lectura de una etiqueta pasiva puede ser afectado por la frecuencia, diseño de la antena, método de energización, y otros factores. [12]

Tag: Transmisor-receptor de radio que es activado por una señal predeterminada. A veces se hace referencia a las etiquetas RFID como transpondedores. [12]

Transponedor: Canal de recepción y transmisión amplificada de señales electromagnéticas en un satélite.

TECNOLOGÍA BLUETOOTH

Bluetooth. Es una nueva tecnología inalámbrica que permite las conexiones de datos entre dispositivos electrónicos tales como ordenadores, teléfonos móviles, agendas electrónicas e impresoras en un rango de 2.4 GHz (gigahercios). En estos dispositivos, Bluetooth reemplazaría las conexiones por cable o infrarrojo. Por favor, recuerda que actualmente el juego online de PlayStation 2 no soporta esta tecnología. Si quieres saber más *acerca* de Jos diferentes íjpos de estándares de servicios inalámbricos, consulta nuestra sección de FAQs sobre sistemas inalámbricos en artículos relacionados.

Infraestructura: Un tipo de configuración de red inalámbrica. Para establecer una configuración en infraestructura necesitas tener una estación base con la que se comunicarán todos tus dispositivos inalámbricos para transmitir los datos de uno a otro.

IrDA: Es un estándar para transmisión por infrarrojos sin cables entre ordenadores y entre teléfonos móviles. IrDA necesita estar enfocado directamente entre los dispositivos que van a comunicarse

Mac. Dirección de 3 bits para distinguir a los miembros de la piconet.

OBEX Capa de protocolo usado por la tecnología Bluetooth

Parked Una unidad en una piconet se encuentra en este modo cuando está sincronizada pero no tiene una dirección MAC.

Piconet. Colección de dispositivos (de 2 a 8) conectados por medio de la tecnología Bluetooth. Todos los dispositivos tienen la misma implementación. Sin embargo, al crearse la red una unidad actuará como maestra y el resto como esclavas mientras dure la conexión.

Scatternet Varias piconets independientes y no sincronizadas forman una scatternet.

Sniff y Hold Modos de ahorro de energía para los dispositivos de una piconet

WLAN (Wireless Local Área Network, red de área local inalámbrica): Acrónimo para un tipo de LAN que en lugar de cables, utiliza ondas de radio de alta frecuencia para transmitir información

802.11 Es el estándar del Institute of Electrical and Electronics Engineers para interoperabilidad de redes de área local inalámbricas. Hay muchos tipos distintos de este estándar y todos ellos están explicados en la sección FAQs sobre sistemas inalámbricos. Ver artículos relacionados.

ANEXOS

Modulo Bluetooth KC-21

KC Wirefree

KC-21

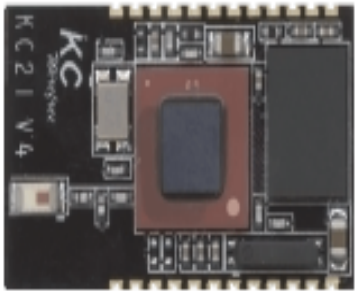
Bluetooth OEM Module Datasheet

Firmware Features

- Wireless Data Communications Subsystem
- Embedded Bluetooth Serial Port Profile (SPP)
- Easy to Use AT Command Interface Using UART
- OEM Programmable Configuration
- Remote Command And Control
- Multipoint / Piconet Capable
- 128-Bit Encryption Security
- Custom Firmware Available

Hardware Features

- Bluetooth v1.2
- 2.4 GHz Class 2 Radio
- Range Typically Exceeds 20m
- High Speed 921kbps Data Rate
- 14 Programmable I/O Pins
- Onboard Antenna
- 8Mbit Flash Memory



26.9mm x 15.3mm x 2.7mm

Bluetooth CE FC RoHS

Applications

- Data Cable Replacement
- Zero Installation Data Link
- Wireless Data Acquisition Upload/Download
- Remote Sensing
- Machine Data Uploads/Downloads
- Monitoring And Control
- Secure Mobile Financial Transactions
- Mobile Device Communications

Description

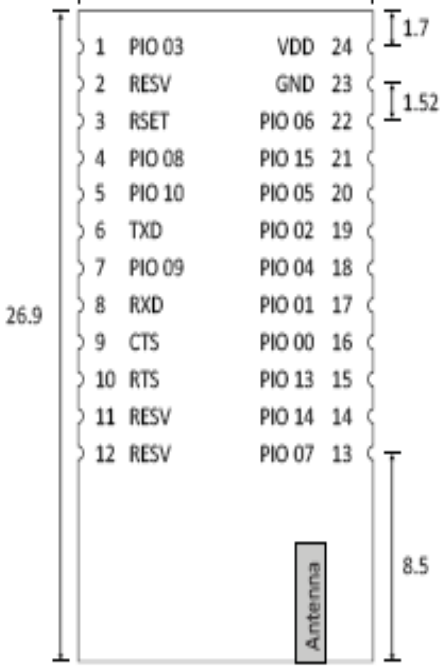
One of the most capable and full featured Bluetooth modules available, the KC-21 Bluetooth OEM Module is designed for maximum performance and easy deployment. The KC-21 module includes 14 programmable input/output lines, and offers high speed serial communications up to 921Kbaud.

The KC-21 is a pre-engineered and pre-licensed PCB module that provides fully embedded, ready to use Bluetooth wireless technology. Multi-surface pads provide both bottom pads for high volume reflow soldering and edge pads for low volume hand soldering. The reprogrammable flash memory contains embedded firmware for serial cable replacement deploying the Bluetooth Serial Port Profile (SPP). Other popular Bluetooth profiles are available.

Custom firmware can be pre-loaded into these highly tuned and tested modules so that they are ready to install without additional procedures.

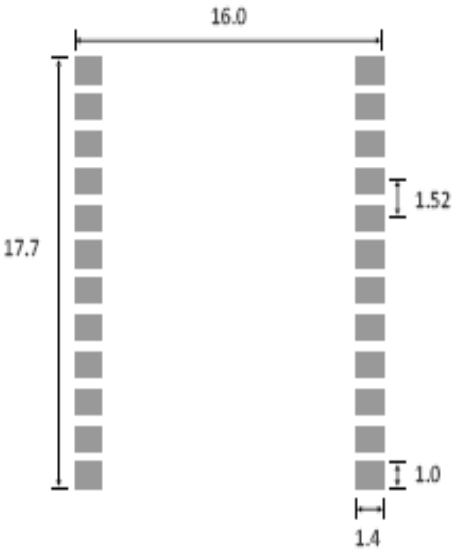
Physical Dimensions

KC-21.4 Top View
(dimensions in mm)



Max Thickness 2.7

KC-21.4 Landing Pattern
(dimensions in mm)



Pin Assignment

Pin	Function	Type	Description
1	PIO [3]	I/O	Programmable Input/Output
2	RESV	-	Reserved
3	RSET	Input	Hardware Reset - Low for 5 ms
4	PIO [8]	I/O	Programmable Input/Output
5	PIO [10]	I/O	Programmable Input/Output
6	TXD	Output	Transmit data
7	PIO [9]	I/O	Programmable Input/Output
8	RXD	Input	Receive data
9	CTS	Input	Flow Control - Clear to send
10	RTS	Output	Flow Control - Request to send
11	RESV	-	Reserved
12	RESV	-	Reserved
13	PIO [7]	I/O	Programmable Input/Output
14	PIO [14]	I/O	Programmable Input/Output
15	PIO [13]	I/O	Programmable Input/Output
16	PIO [0]	I/O	Programmable Input/Output
17	PIO [1]	I/O	Programmable Input/Output
18	PIO [4]	I/O	Programmable Input/Output
19	PIO [2]	I/O	Programmable Input/Output
20	PIO [5]	I/O	Programmable Input/Output
21	PIO [15]	I/O	Programmable Input/Output
22	PIO [6]	I/O	Programmable Input/Output
23	GND	-	Ground
24	VDD	Input	Voltage Supply

Electrical Characteristics

Absolute Maximum Ratings	Min	Max	Unit
Storage temperature range	-40	105	°C
Supply voltage VDD	-0.3	3.6	V
Input voltage for I/O Pin	-	6.0	V

Recommended Operating Conditions	Min	Max	Unit
Temperature Range	-25	85	°C
Supply Voltage VDD (recommend 3.3V)	2.7	3.6	V
Signal Pin Voltage	-	5.5	V

(Conditions VDD= 3.3V and 25 °C)

Programmable I/O Pins Operating Characteristics	Test Conditions	Min	Max	Unit
Input Voltage Low Logic		-	0.8	V
Input Voltage High Logic		2.0	5.5	V
Output Voltage Low Logic	2mA Current	-	0.4	V
Output Voltage High Logic	2mA Current	2.4	-	V
Output Current Low Logic	0.4V	-	2.2	mA
Output Current High Logic	2.4V	-	3.1	mA
Input Leakage Current		-1	1	µA
Low to High Schmitt Trigger Threshold		1.47	1.50	V
High to Low Schmitt Trigger Threshold		0.89	0.95	V
PIO [0-7] Internal Pull-Down Resistor		43	118	KΩ
PIO [8-15] Internal Pull-Up Resistor		53	113	KΩ
Input Capacitance			7.5	pF

Electrical Characteristics Cont.

(Conditions VDD= 3.3V and 25 °C)

Current Consumption	Avg	Unit
ACL data 115K Baud UART at max throughput (Master)	35	mA
ACL data 115K Baud UART at max throughput (Slave)	35	mA
Connection, no data traffic (Master)	18	mA
Connection, no data traffic (Slave)	29	mA
Peak current	90	mA

(Conditions VDD= 3.3V and 25 °C)

Selected RF Characteristics	Test Conditions	BT Spec	Typical	Unit
Antenna load			50	Ω
Sensitivity level	BER < .001 with DH5	≤ -70	-85	dBm
Maximum output power	50 Ω load	-6 to 4	1	dBm
Power control range		≥ 16	30	dB
Power control resolution		2 to 8	4	dB
Initial Carrier Frequency Tolerance		± 75	18	KHz
20 dB Bandwidth for modulated carrier		≤ 1000	930	KHz

Hardware Design

KC Wirefree modules provide UART and PIO hardware interfaces. This section illustrates a typical implementation. Contact our engineering department for application specific recommendations.

Application Notes

- RESET pin must be pulled high.
- RXD pin must be pulled high if not connected to a UART/RS-232 device.
- 10µF or larger capacitor filter for VDD input.
- All unused pins should be left not connected.
- Power supply should have less than 10mVrms noise between 0-10MHz.
- Regulator should have a fast response time < 20µs. It is essential that the power rail recover quickly.
- The area around the module should be free of any ground planes, power planes, trace routings, or metal. Minimum clearance is 5mm, but additional clearance allows improved range and throughput.
- Do not clean modules with Alcohol which can interact with no-clean solder flux residue.
- Do not use ultra sonic cleaning, which may cause interconnect damage.

UART Interface

The UART is compatible with the 16450 industry standard. Four signals are provided with the UART interface: the TXD and RXD pins are used for data, while the CTS and RTS pins are used for flow control. The UART pins operate at TTL voltage level and must be translated to higher RS-232 voltage levels for communicating with PC hosts. A Maxim 3225 series or similar translator is recommend. These terminals can sink 2mA, and are 5V input tolerant with 3V logic level output.

PIO Interface

All PIOs are capable of sinking and sourcing approximately 2mA of current. These terminals are 5V input tolerant, with 3V logic level output. PIO [0-7] are internally pulled down with 50KΩ nominal resistors, and PIO [8-15] are internally pulled up with 50KΩ nominal resistors when configured as inputs.

Example Hardware Interface Connections

Illustration of a KC-21 module to PC connection.

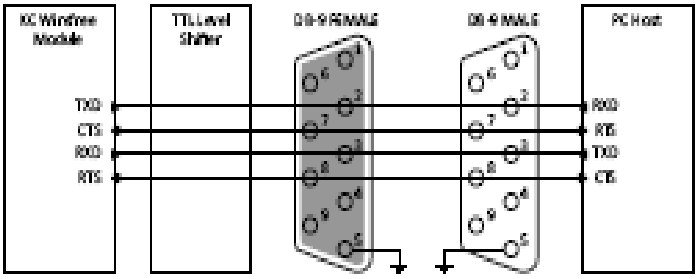
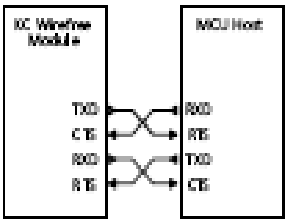
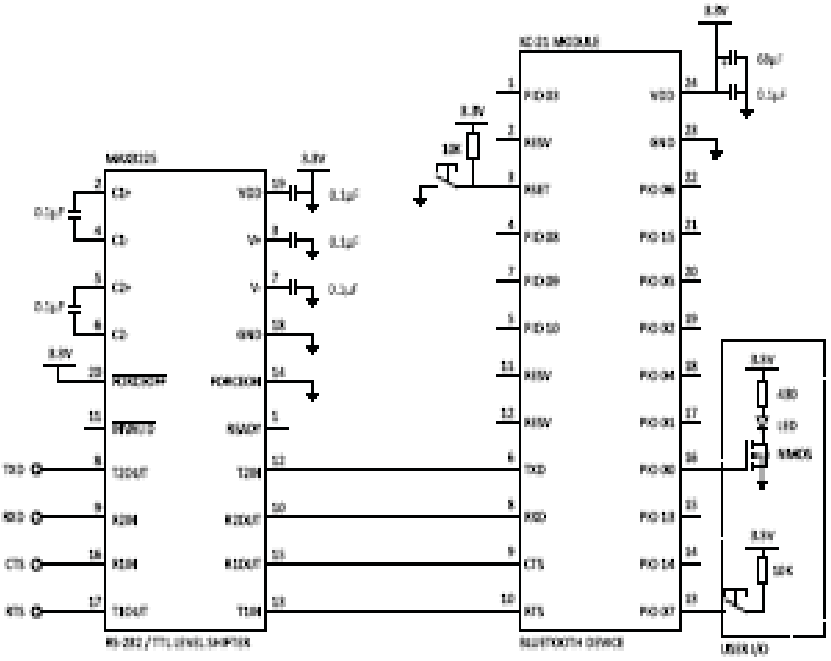


Illustration of a KC-21 module to MCU connection.



KC-21 sample circuit with TTL voltage level shifter ready to connect to a PC RS-232.



Firmware Interface

Our kcSerial firmware provides an easy to use AT command interface using the UART. The firmware interface allows persistent storage of configuration parameters such as device name, default baud rate, and security PIN. Additionally kcSerial provides operational commands such as connections, security, read/write commands for I/O pins, and our remote command mode offering this same programming interface on the linked remote device as well.

Please refer to our *kcSerial User Guide* for additional information.

kcSerial v2.2 AT Command List

Operation Commands	Configuration Commands
AT+KC Bond	AT+KC ChangeBaud
AT+KC Bypass	AT+KC ChangeDefaultBaud
AT+KC DisableBond	AT+KC DefaultLocalName
AT+KC Discovery	AT+KC DeleteSmartCable
AT+KC DUNConnect	AT+KC EraseBondTable
AT+KC DUNDisconnect	AT+KC GPIOConfig
AT+KC EnableBond	AT+KC HostEvent
AT+KC ExitPark	AT+KC LocalName
AT+KC ExitSniff	AT+KC Security
AT+KC GPIORead	AT+KC SmartCableSetup
AT+KC GPIOWrite	AT+KC StreamingSerial
AT+KC Hold	AT+KC UpdateInquiryScan
AT+KC Park	AT+KC UpdatePageScan
AT+KC RemoteCommand	AT+KC Version
AT+KC RemoteCmdDisconnect	
AT+KC Reset	
AT+KC Sniff	
AT+KC SPPConnect	
AT+KC SPPDisconnect	

KC-21

Bluetooth OEM Module Datasheet

Order Part Number	Description
KC-21.4	Bluetooth OEM Module, kcSerial
KC-21.4-FW	Bluetooth OEM Module, Custom kcSerial

Datasheet Version	October 3, 2008
Model	KC-21
Version	4.2
Manufactured	USA
Website	www.kcwirefree.com
Sales Support	info@kcwirefree.com
Technical Support	tech@kcwirefree.com
Phone	(602) 386-2640
Fax	(602) 386-2642
Office	KC Wirefree 2640 W Medtronic Way Tempe, Arizona 85281

Micro controlador

Features

- Compatible with MCS-51™ Products
- 4K Bytes of In-System Reprogrammable Flash Memory
  - Endurance: 1,000 Write/Erase Cycles
- Fully Static Operation: 0 Hz to 24 MHz
- Three-level Program Memory Lock
- 128 x 8-bit Internal RAM
- 32 Programmable I/O Lines
- Two 16-bit Timer/Counters
- Six Interrupt Sources
- Programmable Serial Channel
- Low-power Idle and Power-down Modes

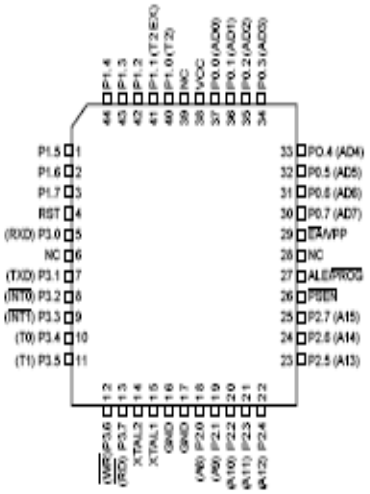
Description

The AT89C51 is a low-power, high-performance CMOS 8-bit microcomputer with 4K bytes of Flash programmable and erasable read only memory (PEROM). The device is manufactured using Atmel's high-density nonvolatile memory technology and is compatible with the industry-standard MCS-51 instruction set and pinout. The on-chip Flash allows the program memory to be reprogrammed in-system or by a conventional nonvolatile memory programmer. By combining a versatile 8-bit CPU with Flash on a monolithic chip, the Atmel AT89C51 is a powerful microcomputer which provides a highly-flexible and cost-effective solution to many embedded control applications.

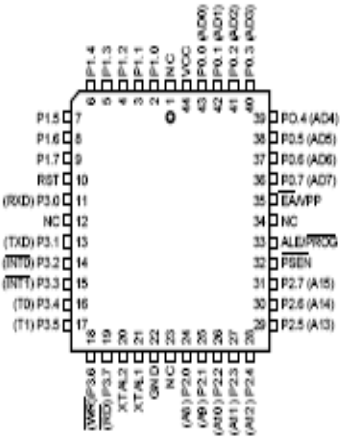
Pin Configurations

PDIP

PQFP/TQFP



PLCC



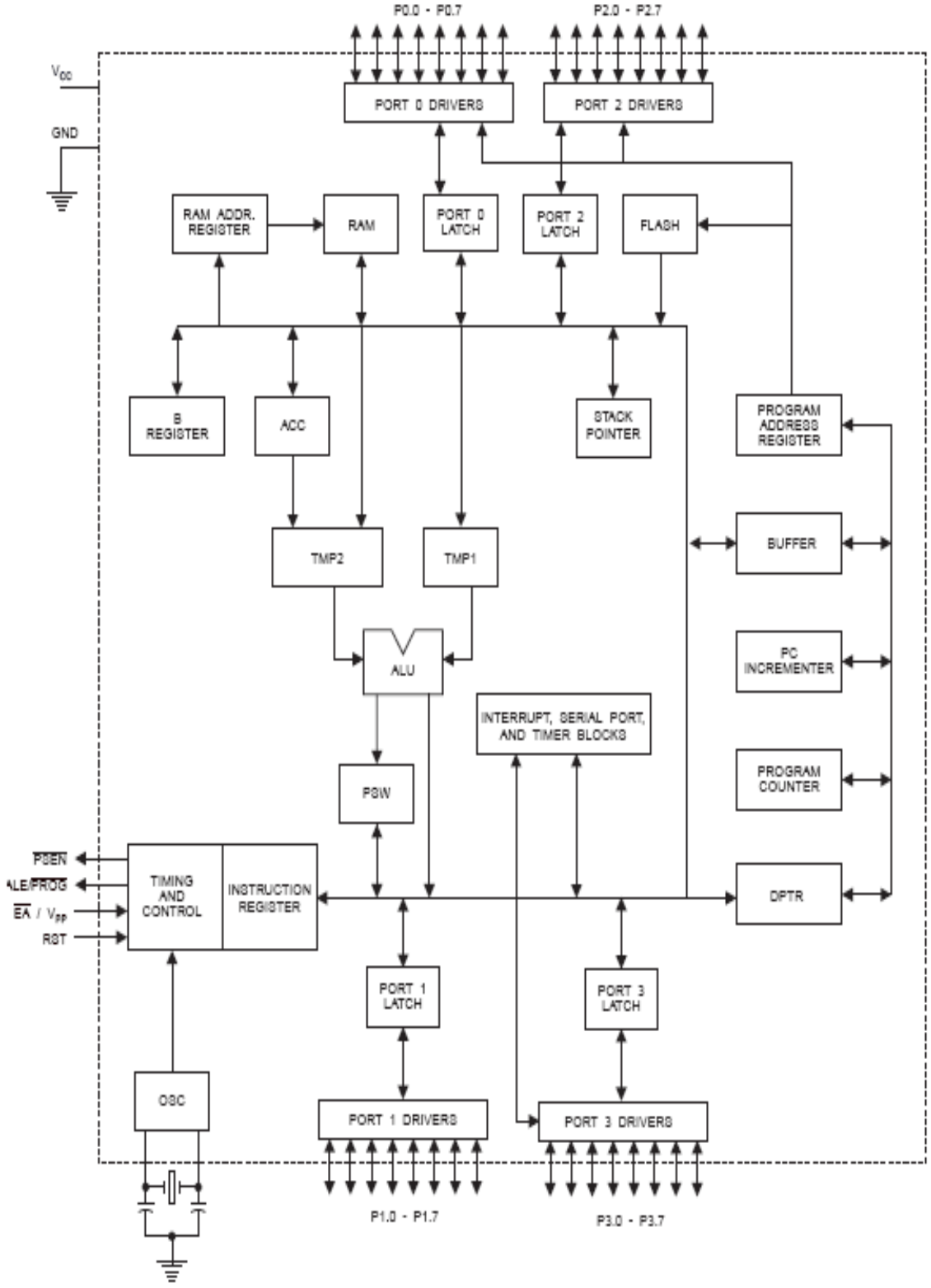
8-bit Microcontroller with 4K Bytes Flash

AT89C51

Not Recommended for New Designs. Use AT89S51.

Rev. 0265G–02/00

Block Diagram



The AT89C51 provides the following standard features: 4K bytes of Flash, 128 bytes of RAM, 32 I/O lines, two 16-bit timer/counters, a five vector two-level interrupt architecture, a full duplex serial port, on-chip oscillator and clock circuitry. In addition, the AT89C51 is designed with static logic for operation down to zero frequency and supports two software selectable power saving modes. The Idle Mode stops the CPU while allowing the RAM, timer/counters, serial port and interrupt system to continue functioning. The Power-down Mode saves the RAM contents but freezes the oscillator disabling all other chip functions until the next hardware reset.

Pin Description

VCC

Supply voltage.

GND

Ground.

Port 0

Port 0 is an 8-bit open-drain bi-directional I/O port. As an output port, each pin can sink eight TTL inputs. When 1s are written to port 0 pins, the pins can be used as high-impedance inputs.

Port 0 may also be configured to be the multiplexed low-order address/data bus during accesses to external program and data memory. In this mode P0 has internal pullups.

Port 0 also receives the code bytes during Flash programming, and outputs the code bytes during program verification. External pullups are required during program verification.

Port 1

Port 1 is an 8-bit bi-directional I/O port with internal pullups. The Port 1 output buffers can sink/source four TTL inputs. When 1s are written to Port 1 pins they are pulled high by the internal pullups and can be used as inputs. As inputs, Port 1 pins that are externally being pulled low will source current (I_{IL}) because of the internal pullups.

Port 1 also receives the low-order address bytes during Flash programming and verification.

Port 2

Port 2 is an 8-bit bi-directional I/O port with internal pullups. The Port 2 output buffers can sink/source four TTL inputs. When 1s are written to Port 2 pins they are pulled high by the internal pullups and can be used as inputs. As inputs, Port 2 pins that are externally being pulled low will source current (I_{IL}) because of the internal pullups.

Port 2 emits the high-order address byte during fetches from external program memory and during accesses to external data memory that use 16-bit addresses (MOVX @ DPTR). In this application, it uses strong internal pullups when emitting 1s. During accesses to external data memory that use 8-bit addresses (MOVX @ RI), Port 2 emits the contents of the P2 Special Function Register.

Port 2 also receives the high-order address bits and some control signals during Flash programming and verification.

Port 3

Port 3 is an 8-bit bi-directional I/O port with internal pullups. The Port 3 output buffers can sink/source four TTL inputs. When 1s are written to Port 3 pins they are pulled high by the internal pullups and can be used as inputs. As inputs, Port 3 pins that are externally being pulled low will source current (I_{IL}) because of the pullups.

Port 3 also serves the functions of various special features of the AT89C51 as listed below:

Port Pin	Alternate Functions
P3.0	RXD (serial input port)
P3.1	TXD (serial output port)
P3.2	$\overline{INT0}$ (external interrupt 0)
P3.3	$\overline{INT1}$ (external interrupt 1)
P3.4	T0 (timer 0 external input)
P3.5	T1 (timer 1 external input)
P3.6	$\overline{WR}$ (external data memory write strobe)
P3.7	$\overline{RD}$ (external data memory read strobe)

Port 3 also receives some control signals for Flash programming and verification.

RST

Reset input. A high on this pin for two machine cycles while the oscillator is running resets the device.

ALE/$\overline{PROG}$

Address Latch Enable output pulse for latching the low byte of the address during accesses to external memory. This pin is also the program pulse input ($\overline{PROG}$) during Flash programming.

In normal operation ALE is emitted at a constant rate of 1/6 the oscillator frequency, and may be used for external timing or clocking purposes. Note, however, that one ALE

pulse is skipped during each access to external Data Memory.

If desired, ALE operation can be disabled by setting bit 0 of SFR location 8EH. With the bit set, ALE is active only during a MOVX or MOVC instruction. Otherwise, the pin is weakly pulled high. Setting the ALE-disable bit has no effect if the microcontroller is in external execution mode.

$\overline{\text{PSEN}}$

Program Store Enable is the read strobe to external program memory.

When the AT89C51 is executing code from external program memory, $\overline{\text{PSEN}}$ is activated twice each machine cycle, except that two $\overline{\text{PSEN}}$ activations are skipped during each access to external data memory.

$\overline{\text{EA}}$/VPP

External Access Enable. $\overline{\text{EA}}$ must be strapped to GND in order to enable the device to fetch code from external program memory locations starting at 0000H up to FFFFH. Note, however, that if lock bit 1 is programmed, $\overline{\text{EA}}$ will be internally latched on reset.

$\overline{\text{EA}}$ should be strapped to V_{CC} for internal program executions.

This pin also receives the 12-volt programming enable voltage (V_{PP}) during Flash programming, for parts that require 12-volt V_{PP}.

XTAL1

Input to the inverting oscillator amplifier and input to the internal clock operating circuit.

XTAL2

Output from the inverting oscillator amplifier.

Oscillator Characteristics

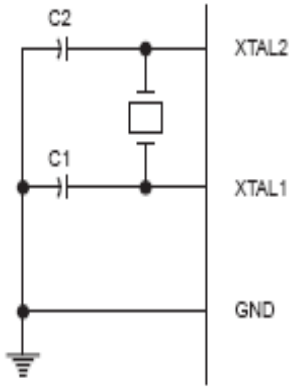
XTAL1 and XTAL2 are the input and output, respectively, of an inverting amplifier which can be configured for use as an on-chip oscillator, as shown in Figure 1. Either a quartz crystal or ceramic resonator may be used. To drive the device from an external clock source, XTAL2 should be left unconnected while XTAL1 is driven as shown in Figure 2. There are no requirements on the duty cycle of the external clock signal, since the input to the internal clocking circuitry is through a divide-by-two flip-flop, but minimum and maximum voltage high and low time specifications must be observed.

Idle Mode

In idle mode, the CPU puts itself to sleep while all the on-chip peripherals remain active. The mode is invoked by software. The content of the on-chip RAM and all the special functions registers remain unchanged during this mode. The idle mode can be terminated by any enabled interrupt or by a hardware reset.

It should be noted that when idle is terminated by a hard ware reset, the device normally resumes program execution, from where it left off, up to two machine cycles before the internal reset algorithm takes control. On-chip hardware inhibits access to internal RAM in this event, but access to the port pins is not inhibited. To eliminate the possibility of an unexpected write to a port pin when Idle is terminated by reset, the instruction following the one that invokes Idle should not be one that writes to a port pin or to external memory.

Figure 1. Oscillator Connections

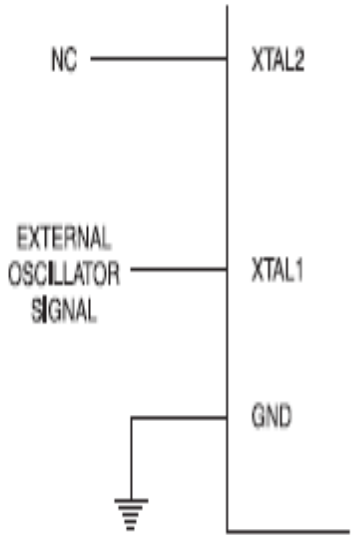


Note: C1, C2 = 30 pF ± 10 pF for Crystals
= 40 pF ± 10 pF for Ceramic Resonators

Status of External Pins During Idle and Power-down Modes

Mode	Program Memory	ALE	$\overline{\text{PSEN}}$	PORT0	PORT1	PORT2	PORT3
Idle	Internal	1	1	Data	Data	Data	Data
Idle	External	1	1	Float	Data	Address	Data
Power-down	Internal	0	0	Data	Data	Data	Data
Power-down	External	0	0	Float	Data	Data	Data

Figure 2. External Clock Drive Configuration



Power-down Mode

In the power-down mode, the oscillator is stopped, and the instruction that invokes power-down is the last instruction executed. The on-chip RAM and Special Function Registers retain their values until the power-down mode is terminated. The only exit from power-down is a hardware reset. Reset redefines the SFRs but does not change the on-chip RAM. The reset should not be activated before V_{CC} is restored to its normal operating level and must be held active long enough to allow the oscillator to restart and stabilize.

Program Memory Lock Bits

On the chip are three lock bits which can be left unprogrammed (U) or can be programmed (P) to obtain the additional features listed in the table below.

When lock bit 1 is programmed, the logic level at the $\overline{EA}$ pin is sampled and latched during reset. If the device is powered up without a reset, the latch initializes to a random value, and holds that value until reset is activated. It is necessary that the latched value of $\overline{EA}$ be in agreement with the current logic level at that pin in order for the device to function properly.

Lock Bit Protection Modes

Program Lock Bits				
	LB1	LB2	LB3	Protection Type
1	U	U	U	No program lock features
2	P	U	U	MOVC instructions executed from external program memory are disabled from fetching code bytes from internal memory, $\overline{EA}$ is sampled and latched on reset, and further programming of the Flash is disabled
3	P	P	U	Same as mode 2, also verify is disabled
4	P	P	P	Same as mode 3, also external execution is disabled

Programming the Flash

The AT89C51 is normally shipped with the on-chip Flash memory array in the erased state (that is, contents = FFH) and ready to be programmed. The programming interface accepts either a high-voltage (12-volt) or a low-voltage (V_{CC}) program enable signal. The low-voltage programming mode provides a convenient way to program the AT89C51 inside the user's system, while the high-voltage programming mode is compatible with conventional third-party Flash or EPROM programmers.

The AT89C51 is shipped with either the high-voltage or low-voltage programming mode enabled. The respective top-side marking and device signature codes are listed in the following table.

	V_{pp} = 12V	V_{pp} = 5V
Top-side Mark	AT89C51 xxxx yyww	AT89C51 xxxx-5 yyww
Signature	(030H) = 1EH (031H) = 51H (032H) =F FH	(030H) = 1EH (031H) = 51H (032H) = 05H

The AT89C51 code memory array is programmed byte-by-byte in either programming mode. *To program any non-blank byte in the on-chip Flash Memory, the entire memory must be erased using the Chip Erase Mode.*

Programming Algorithm: Before programming the AT89C51, the address, data and control signals should be set up according to the Flash programming mode table and Figure 3 and Figure 4. To program the AT89C51, take the following steps.

1. Input the desired memory location on the address lines.
2. Input the appropriate data byte on the data lines.
3. Activate the correct combination of control signals.
4. Raise $\overline{EA}/V_{PP}$ to 12V for the high-voltage programming mode.
5. Pulse ALE/$\overline{PROG}$ once to program a byte in the Flash array or the lock bits. The byte-write cycle is self-timed and typically takes no more than 1.5 ms. Repeat steps 1 through 5, changing the address and data for the entire array or until the end of the object file is reached.

$\overline{Data}$ Polling: The AT89C51 features $\overline{Data}$ Polling to indicate the end of a write cycle. During a write cycle, an attempted read of the last byte written will result in the complement of the written datum on PO.7. Once the write cycle has been completed, true data are valid on all outputs, and the next cycle may begin. $\overline{Data}$ Polling may begin any time after a write cycle has been initiated.

Ready/$\overline{Busy}$: The progress of byte programming can also be monitored by the RDY/$\overline{BSY}$ output signal. P3.4 is pulled low after ALE goes high during programming to indicate BUSY. P3.4 is pulled high again when programming is done to indicate READY.

Program Verify: If lock bits LB1 and LB2 have not been programmed, the programmed code data can be read back via the address and data lines for verification. The lock bits cannot be verified directly. Verification of the lock bits is achieved by observing that their features are enabled.

Chip Erase: The entire Flash array is erased electrically by using the proper combination of control signals and by holding ALE/$\overline{PROG}$ low for 10 ms. The code array is written with all "1"s. The chip erase operation must be executed before the code memory can be re-programmed.

Reading the Signature Bytes: The signature bytes are read by the same procedure as a normal verification of locations 030H, 031H, and 032H, except that P3.6 and P3.7 must be pulled to a logic low. The values returned are as follows.

(030H) = 1EH indicates manufactured by Atmel
(031H) = 51H indicates 89C51
(032H) = FFH indicates 12V programming
(032H) = 05H indicates 5V programming

Programming Interface

Every code byte in the Flash array can be written and the entire array can be erased by using the appropriate combination of control signals. The write operation cycle is self-timed and once initiated, will automatically time itself to completion.

All major programming vendors offer worldwide support for the Atmel microcontroller series. Please contact your local programming vendor for the appropriate software revision.

Flash Programming Modes

Mode		RST	$\overline{PSEN}$	ALE/$\overline{PROG}$	$\overline{EA}$/V_{PP}	P2.6	P2.7	P3.6	P3.7
Write Code Data		H	L		H/12V	L	H	H	H
Read Code Data		H	L	H	H	L	L	H	H
Write Lock	Bit - 1	H	L		H/12V	H	H	H	H
	Bit - 2	H	L		H/12V	H	H	L	L
	Bit - 3	H	L		H/12V	H	L	H	L
Chip Erase		H	L	(1)	H/12V	H	L	L	L
Read Signature Byte		H	L	H	H	L	L	L	L

Note: 1. Chip Erase requires a 10 ms $\overline{PROG}$ pulse.

Figure 3. Programming the Flash

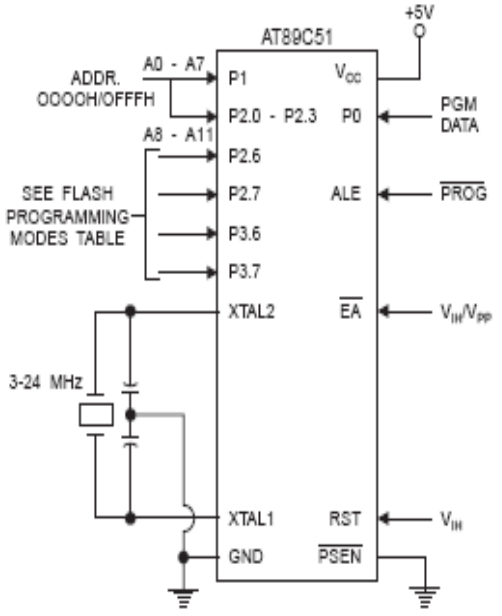
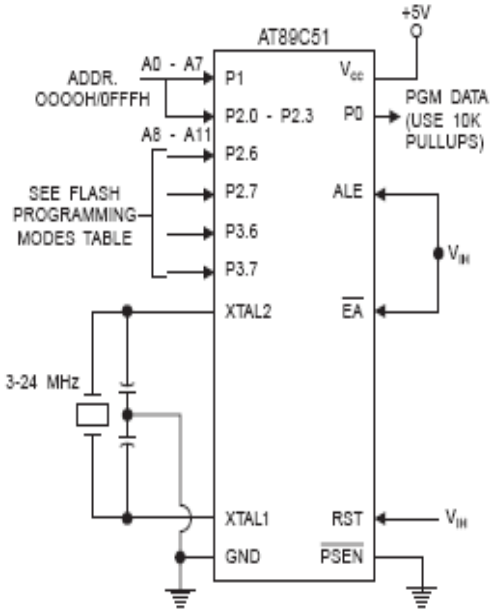
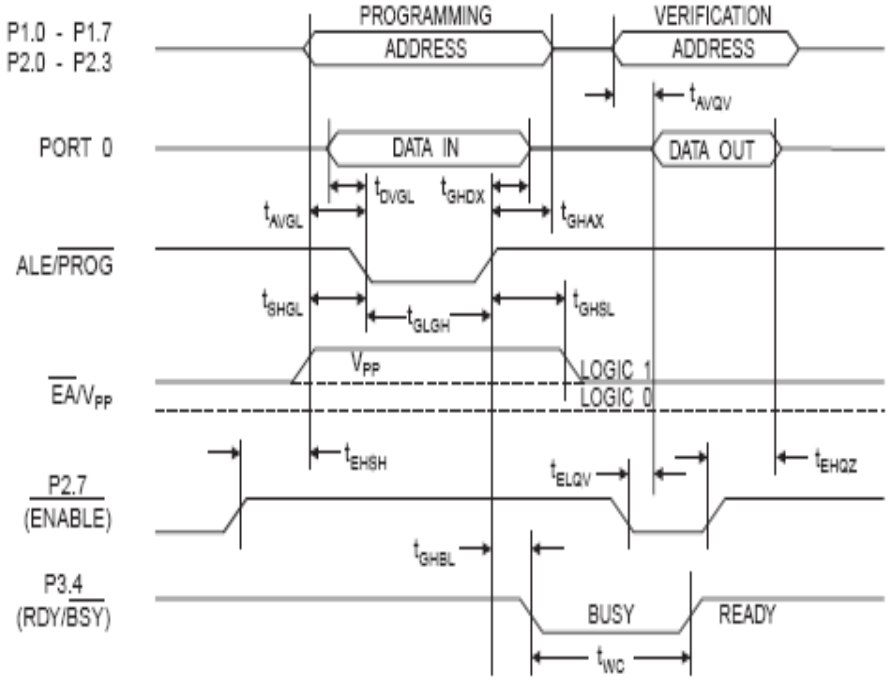


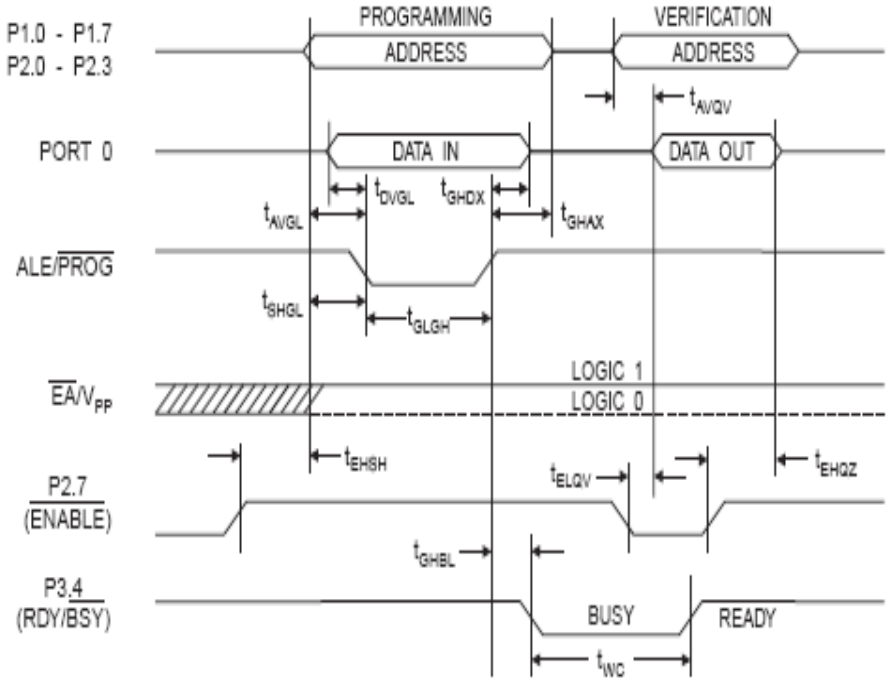
Figure 4. Verifying the Flash



Flash Programming and Verification Waveforms - High-voltage Mode (V_{PP} = 12V)



Flash Programming and Verification Waveforms - Low-voltage Mode (V_{PP} = 5V)



Flash Programming and Verification Characteristics

T_A = 0°C to 70°C, V_{CC} = 5.0 ± 10%

Symbol	Parameter	Min	Max	Units
V_{pp}[1]	Programming Enable Voltage	11.5	12.5	V
I_{pp}[1]	Programming Enable Current		1.0	mA
$1/t_{CLCL}$	Oscillator Frequency	3	24	MHz
t_{AVGL}	Address Setup to $\overline{PROG}$ Low	$48t_{CLCL}$		
t_{GHAX}	Address Hold after $\overline{PROG}$	$48t_{CLCL}$		
t_{DVGL}	Data Setup to $\overline{PROG}$ Low	$48t_{CLCL}$		
t_{GHDX}	Data Hold after $\overline{PROG}$	$48t_{CLCL}$		
t_{EHSH}	P2.7 ($\overline{ENABLE}$) High to V_{pp}	$48t_{CLCL}$		
t_{SHGL}	V_{pp} Setup to $\overline{PROG}$ Low	10		µs
t_{GHSL}[1]	V_{pp} Hold after $\overline{PROG}$	10		µs
t_{GLGH}	$\overline{PROG}$ Width	1	110	µs
t_{AVQV}	Address to Data Valid		$48t_{CLCL}$	
t_{ELQV}	$\overline{ENABLE}$ Low to Data Valid		$48t_{CLCL}$	
t_{EHQZ}	Data Float after $\overline{ENABLE}$	0	$48t_{CLCL}$	
t_{GHBL}	$\overline{PROG}$ High to $\overline{BUSY}$ Low		1.0	µs
t_{WC}	Byte Write Cycle Time		2.0	ms

Note: 1. Only used in 12-volt programming mode.

Atmel Headquarters

Corporate Headquarters
2325 Orchard Parkway
San Jose, CA 95131
TEL (408) 441-0311
FAX (408) 487-2600

Europe
Atmel U.K., Ltd.
Coliseum Business Centre
Riverside Way
Camberley, Surrey GU15 3YL
England
TEL (44) 1276-686-677
FAX (44) 1276-686-697

Asia
Atmel Asia, Ltd.
Room 1219
Chinachem Golden Plaza
77 Mody Road Tsimhatsui
East Kowloon
Hong Kong
TEL (852) 2721-9778
FAX (852) 2722-1369

Japan
Atmel Japan K.K.
9F, Tonetsu Shinkawa Bldg.
1-24-8 Shinkawa
Chuo-ku, Tokyo 104-0033
Japan
TEL (81) 3-3523-3551
FAX (81) 3-3523-7581

Atmel Operations

Atmel Colorado Springs
1150 E. Cheyenne Mtn. Blvd.
Colorado Springs, CO 80906
TEL (719) 576-3300
FAX (719) 540-1759

Atmel Rousset
Zone Industrielle
13106 Rousset Cedex
France
TEL (33) 4-4253-6000
FAX (33) 4-4253-6001

Fax-on-Demand
North America:
1-(800) 292-8635
International:
1-(408) 441-0732

e-mail
literature@atmel.com

Web Site
http://www.atmel.com

BBS
1-(408) 436-4309

REFERENCIAS BIBLIOGRÁFICAS

[1] Introducción al capítulo, historia de RFID, http://es.wikipedia.org/wiki/RFID, consultada el 7-06-2007

[2] Telectrónica, *Introducción a la identificación por radiofrecuencia,* Fundamentos de RFID

[3] Operación del circuito RFID, http://www.telectronica.com/rfid-detalle.asp?id_productos=297, consultada el 7-06-2007

[4] Como funciona, http://www.ecojoven.com/dos/Q3/RFID.html. consultada el 7-06-2007

[5] Frecuencia de operación, Guía Conozcamos el tag RFID, http://www.rfid-magazine.com, consultada el 7-16-2007

[6] Frecuencias de funcionamiento, http://www.kimaldi.com/kimaldi/area_de_conocimiento/rfid/frecuencias de funcionamiento

[7] Telectrónica, *Introducción a la identificación por radiofrecuencia,* Sistemas RFID

[8] Modo de comunicación, Guía: Conozcamos el tag RFID, http://www.rfid-magazine.com, consultada el 7-16-2007

[9] Acoplamiento, Guía Conozcamos el tag RFID, http://www.rfid-magazine.com, consultada el 7-16-2007

[10] Acebedo Víctor, García Alejandro, Sandino Juan, *Tesis Sistema De Registro Y Control De Salida De Elementos Mediante Dispositivos Rfid,* Pontificia Universidad Javeriana, Noviembre 2004

[11] Introducción, Guía Conozcamos el tag RFID, http://www.rfid-magazine.com, consultada el 7-16-2007

[12] Telectrónica, *Introducción a la identificación por radiofrecuencia,* Los Tags de RFID, Glosario

[13] Características básicas, Guía Conozcamos el tag RFID, http://www.rfid-magazine.com, consultada el 7-16-2007

[14] Características físicas, Guía Conozcamos el tag RFID, http://www.rfid-magazine.com, consultada el 7-16-2007

[15] Origen de la alimentación o fuente de energía, Guía Conozcamos el tag RFID, http://www.rfid-magazine.com, consultada el 7-16-2007

[16] Tipos de etiquetas RFID, http://es.wikipedia.org/wiki/RFID, consultada el 7-16-2007

[17] Estándares, Guía Conozcamos el tag RFID, http://www.rfid-magazine.com, consultada el 7-16-2007

[18] Standards, http://www.remoteidentity.com/standards/standards.php, consultada el 7-16-2007

[19] Uso actual, http://es.wikipedia.org/wiki/RFID, consultada el 7-16-2007

[20] RFID y ePC: Aplicaciones, Tabla comparativa, http://www.pucp.edu.pe/secc/industrial/docs/RFID%20y%20ePC%20aplicaciones.pdf

[21] Telectrónica, *Introducción a la identificación por radiofrecuencia*, Los Tags de RFID, RFID vs. el Código de Barras

[22] Bluetooth. Estándar para la conexión sin cables: TECNOLOGIA DE BLUETOOTH de MULLER NATHAN J.

[23] Bluetooth [http://Bluetooth.com/]: La página oficial de Bluetooth

[24]Visual Basic: vBCity/DevCity.NET Forums

http://vbcity.com/forums/forum.asp?fid=35

[25] - Bluetooth Technology Overview Version 1.0 http://www.forum.nokia.com

[26] Bluetooth Profiles Dean A. Gratton

[27]- Bluetooth, http://es.Bluetooth.org/wauinki/Bluetooth

FECHA DE ENTREGA

El presente Proyecto de Grado fue entregado en la fecha:

Sangolquí. _____de JUNIO del 2009

Oscar Fabian Herrán Rengifo

Autor

Sr. Ing. Gonzalo Olmedo

Coordinador de la Carrera de Ingeniería en

Electrónica y Telecomunicaciones