ESCUELA POLITÉCNICA DEL EJÉRCITO

SEDE LATACUNGA

CARRERA DE INGENIERÍA EN ELECTRÓNICA E INSTRUMENTACIÓN

DISEÑO Y ELABORACIÓN DE UN SISTEMA DE SEGURIDAD VEHICULAR CON TECNOLOGÍA RFID, CON INTERFAZ USB 2.O Y CONTROLES DE ACCESO CODIFICADOS

PROYECTO PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERO EN ELECTRÓNICA E INSTRUMENTACIÓN

CAPT. DE MG. CAPELO BADILLO ALDO GRIVALDY
CRUZ GUANOLUISA JOSÉ LUIS

Latacunga, Octubre 2009

ESCUELA POLITÉCNICA DEL EJÉRCITO

CARRERA DE INGENIERIA ELECTRÓNICA E INSTRUMENTACIÓN

DECLARACIÓN DE RESPONSABILIDAD

Nosotros, CAPELO BADILLO ALDO GRIVALDY
CRUZ GUANOLUISA JOSÉ LUIS

DECLARAMOS QUE:

El proyecto de grado denominado "DISEÑO E IMPLEMENTACIÓN DEL PROTOTIPO DE UN SISTEMA DE SEGURIDAD VEHICULAR CON TECNOLOGÍA RFID, CON INTERFACE USB 2.0 Y CONTROLES DE ACCESO CODIFICADOS " ha sido desarrollado con base a una investigación exhaustiva, respetando derechos intelectuales de terceros, conforme las citas que constan al pie de las páginas correspondientes, cuyas fuentes se incorporan en la bibliografía.

Consecuentemente este trabajo es de nuestra autoría.

En virtud de esta declaración, nos responsabilizamos del contenido, veracidad y alcance científico del proyecto de grado en mención.

Latacunga, 19 de Octubre del 2009.

---------- ----------

CAPELO BADILLO ALDO GRIVALDY
Cl. No.- 060204553-6

CRUZ GUANOLUISA JOSÉ LUIS
Cl. No.- 050262818-3

ESCUELA POLITÉCNICA DEL EJÉRCITO

CARRERA DE INGENIERIA ELECTRÓNICA E INSTRUMENTACIÓN

AUTORIZACIÓN

Nosotros, CAPELO BADILLO ALDO GRIVALDY
CRUZ GUANOLUISA JOSÉ LUIS

Autorizamos a la Escuela Politécnica del Ejército la publicación, en la biblioteca virtual de la Institución del trabajo "DISEÑO E IMPLEMENTACIÓN DEL PROTOTIPO DE UN SISTEMA DE SEGURIDAD VEHICULAR CON TECNOLOGÍA RFID, CON INTERFACE USB 2.0 Y CONTROLES DE ACCESO CODIFICADOS" cuyo contenido, ideas y criterios son de nuestra exclusiva responsabilidad y autoría.

Latacunga, 19 de Octubre del 2009.

---	---
CAPELO BADILLO ALDO GRIVALDY	CRUZ GUANOLUISA JOSÉ LUIS
Cl. No.- 060204553-6	Cl. No.- 050262818-3

ESCUELA POLITÉCNICA DEL EJÉRCITO

CARRERA DE INGENIERIA ELECTRÓNICA E INSTRUMENTACIÓN

CERTIFICADO

ING. CÉSAR NARANJO HIDALGO (DIRECTOR)

ING. AMPARO MEYTHALER NARANJO (CODIRECTOR)

CERTIFICAN:

Que el trabajo titulado "DISEÑO E IMPLEMENTACIÓN DEL PROTOTIPO DE UN SISTEMA DE SEGURIDAD VEHICULAR CON TECNOLOGÍA RFID, CON INTERFACE USB 2.0 Y CONTROLES DE ACCESO CODIFICADOS" realizado por los señores: CAPELO BADILLO ALDO GRIVALDY Y CRUZ GUANOLUISA JOSÉ LUIS ha sido guiado y revisado periódicamente y cumple normas estatutarias establecidas por la ESPE, en el Reglamento de Estudiantes de la Escuela Politécnica del Ejército.

Debido a que constituye un trabajo de excelente contenido científico que coadyuvará a la aplicación de conocimientos y al desarrollo profesional, **SI** recomiendan su publicación.

El mencionado trabajo consta de UN empastado y UN disco compacto el cual contiene los archivos en formato portátil de Acrobat. Autorizan a los señores: CAPELO BADILLO ALDO GRIVALDY Y CRUZ GUANOLUISA JOSÉ LUIS que lo entregue al ING. ARMANDO ÁLAVREZ SALAZAR, en su calidad de Coordinador de Carrera.

Latacunga, 19 de Octubre del 2009.

---	---
Ing. César Naranjo Hidalgo	Ing. Amparo Meythaler Naranjo
DIRECTOR	**CODIRECTOR**

AGRADECIMIENTO

Al terminar una faceta más de mi vida, quisiera agradecer primeramente a Dios y al Divino niño por haberme dado salud y vida para cumplir un sueño en el que siempre creí.

A mi esposa, por estar incondicionalmente siempre apoyándome a lo largo de toda mi carrera profesional.

A mis hijos, por soportar muchas vicisitudes e injusticias que a veces los niños no entienden pero que son propias de la carrera universitaria.

A mis padres porque a pesar de la distancia, me apoyaron y siempre confiaron en mi capacidad.

Un agradecimiento especial a mis suegros por su voluntad, lealtad y ayuda, convirtiéndose en un ejemplo a seguir como familia.

A la Fuerza Terrestre por permitirme incrementar mis conocimientos.

Finalmente mi gratitud a todos quienes contribuyeron de una u otra manera al logro de un sueño ahora hecho realidad.

Capt. Aldo G. Capelo B.

Dedicatoria

A mis padres:

Que con su paciencia, esfuerzo y dedicación, me han inspirado a realizar y culminar con éxito este proyecto de investigación.

José L. Cruz G.

"Para el logro del triunfo siempre ha sido indispensable pasar por la senda de los sacrificios." Simón Bolívar.

Agradecimiento

A Dios por brindarme día a día, fortaleza, vida, salud y sabiduría para cumplir una a una, con las metas que me he propuesto hasta la actualidad.

A mis padres Luis y Alicia, por brindarme su apoyo incondicional durante mi formación como ser humano y profesional; por todo la confianza que depositaron en mí durante toda mi carrera universitaria.

A mis hermanos Edwin, Bismarck y Elías, por darme ánimos en aquellos momentos difíciles.

A la facultad de Eléctrica y Electrónica por haberme brindado la oportunidad de realizar este proyecto.

Y a todas aquellas personas que directa o indirectamente me brindaron su apoyo para la realización y culminación de este proyecto.

José L. Cruz G.

INTRODUCCIÓN

El presente trabajo tiene como objetivo principal el diseño de un sistema de seguridad vehicular con tecnología RFID, con interfaz USB 2.0 y controles de acceso codificados, el mismo que funciona de la siguiente manera:

Posee un dispositivo inicial (PRIMERA SEGURIDAD) que permite el ingreso al vehículo será una tarjeta magnética que dispone de un código de ingreso único para las personas que hayan sido codificadas para el uso del automóvil (padre, madre, hijos o a su vez empresarios y choferes).

Este dispositivo puede estar ubicado en cualquier parte del auto y no necesariamente actúa con un pulso de un control, sino que el propietario del automóvil acerca su dispositivo a una distancia sincronizada previamente y en el lugar seleccionado para su colocación. Al accionarse, permite que las seguridades se levanten y puedan ingresar las personas codificadas.

Las claves de acceso al automóvil pueden ser reprogramadas mediante el teclado portátil para que estas no sean las mismas siempre. El dispositivo puede ser reprogramado cada cierto tiempo para que las codificaciones anteriores sean cambiadas y el nivel de seguridad del automóvil sea mayor.

Una vez en el interior del vehículo y al momento de colocar en contacto el switch de encendido, se cierran las seguridades de las puertas, se activa un LCD que en conjunto con un teclado dará la bienvenida al automóvil y al mismo tiempo le pedirá la clave de encendido (SEGUNDA SEGURIDAD). Si no sabe la clave, que puede ser de 3, 4, 5, 6, 7 u 8 dígitos, automáticamente el automóvil se bloquea en forma total. En caso de que se haya perdido la tarjeta del vehículo, se podría acceder al mismo con la llave, pero el momento que accede su clave por teclado,

le va a pedir una segunda clave de confirmación, debido a que el sistema detectó que en primera instancia el ingreso al auto fue realizado con la llave. En el caso que la persona que ingresó no fue el propietario y digitó la clave incorrecta, automáticamente se cierran los seguros de las puertas y el auto se bloquea totalmente.

El momento que se apaga el vehículo inmediatamente se rearma el sistema por completo, es decir esperará reconocer un TAG adecuado para pedir que ingrese nuevamente su clave de acceso al encendido, o a su vez permitir que se desbloqueen las puertas con una nueva clave. Esta opción hace que en caso de que sea víctima de un asalto o robo, es suficiente el cerrar el switch para que el automóvil se bloquee totalmente y no sea robado.

El riesgo de la pérdida o robo de la tarjeta de acceso al vehículo, no es mayor problema, porque quien desee utilizarla, no conoce donde se colocó el dispositivo en el automóvil, y a su vez tampoco conoce la clave de acceso al encendido de los sistemas del vehículo. Por medio de la interfaz USB 2.0 y el programa de servicio técnico, se puede reprogramar y codificar una nueva tarjeta de proximidad (Touch Memory); de esta manera el sistema sigue confiable y seguro para su uso.

En forma general, el sistema de comunicación que se maneja, está compuesto por un transmisor de radio frecuencia incorporado en cada dispositivo, él cual tiene un receptor que recibe el código único transmitido por su Touch Memory. La base de datos creada es la que registra el código de cada persona que va a hacer uso del vehículo asignado, los datos del vehículo y de su propietario o funcionario.

Para plasmar lo antes expuesto el presente documento se divide en cuatro capítulos.

El primero posee los fundamentos teóricos que sustentan el diseño que se desarrollo en el segundo capítulo.

En el tercer capítulo se presentan los resultados y pruebas experimentales realizadas al prototipo, para concluir con el capítulo cuatro que incluye las conclusiones obtenidas a lo largo del desarrollo del proyecto, así como también las recomendaciones que se desprenden de las mismas.

Los Autores

ÍNDICE

CAPÍTULO I: FUNDAMENTOS TEÓRICOS

CAPÍTULO I

FUNDAMENTOS TEÓRICOS

1.1 DESCRIPCIÓN DEL PROBLEMA

Uno de los sistemas de los vehículos que es vulnerado, es el sistema de seguridad interno, a pesar de que los automóviles modernos disponen cada vez de elementos más sofisticados.

Los automóviles que disponen de este tipo de sistemas son más costosos, por lo que no todas las personas lo disponen en sus autos. Además; así los tuvieran, un alto porcentaje de estos dispositivos electrónicos son vulnerables de más de una forma, por lo que se pretende diseñar un sistema que minimice este riesgo.

Hoy en día las alarmas de los autos convencionales son tan vulnerables porque sólo se limitan a la apertura de sus seguridades por medio de los dos controles que vienen de fábrica, sin opción de modificación alguna.

Todo esto hace que se tengan los siguientes problemas y vulnerabilidades en los automóviles que disponen de ese tipo de sistemas de seguridad:

a) Cuando se averíe por cualquier eventualidad el control del sistema de seguridad, el conductor será el que realice manualmente la apertura y el cierre de la puerta, sin tener la opción de poder acceder a un nuevo control para la activación de su sistema, quedando de este modo obsoleto.

b) El sistema convencional se activa o desactiva sin tomar en cuenta si es la persona correcta que va a conducir el vehículo, tendría totalmente el control y acceso al auto sin problema.

c) Por el hecho de haber ingresado al interior del vehículo, cualquier individuo sin ningún problema puede encender el auto y conducir.

d) Una vez vulnerado el sistema de seguridad, no se tiene la opción de modificarlo, por lo que debería desecharse.

e) Los sistemas de seguridad convencionales, en muchas de las ocasiones tienen controles genéricos, que hacen que se activen o desactiven sin ningún problema.

Basados en algunos sistemas de seguridad del mercado y tomando como referente la tecnología empleada en los vehículos utilitarios FORD, se pone a consideración un sistema de seguridad altamente confiable y casi imposible de duplicar por la complejidad del mismo.

1.2EL MICROCONTROLADOR PIC18F4550

1.2.1 Introducción

En la actualidad los microcontroladores PIC de la Microchip son muy aceptados gracias a que ofrecen una gran variedad de familias que permiten adaptar el microcontrolador a las necesidades de cada aplicación, tienen herramientas comunes para el desarrollo de aplicaciones, gran variedad de funciones embebidas (temporizadores, USART, I2C, Convertidores A/D, receptores/transmisores RF, Ethernet, USB, etc., además de precios competitivos y buen soporte (hojas de información técnicas, libros, notas de aplicación, mucha información disponible en Internet).

Algunos de los microcontroladores de la Microchip son los siguientes:

- **PIC10:** Microcontroladores de 8 bits, de bajo costo, 6 pines y bajas prestaciones.
- **PIC12:** Microcontroladores de 8 bits, de bajo costo, 8 pines y bajas prestaciones.
- **PIC16:** Microcontroladores de 8 bits, con gran variedad de número de pines y prestaciones medias.
- **PIC18:** Microcontroladores de 8 bits, con gran variedad de número de pines y prestaciones medias/altas.
- **PIC24:** Microcontroladores de 16 bits, con gran variedad de número de pines y prestaciones altas.
- **dsPIC's:** Altas prestaciones para el procesamiento de señales e imágenes.

La fábrica Microchip distribuye de forma general dos tipos de microcontroladores, dependiendo del voltaje de alimentación:

- Clase F: Voltaje típico (4.2 V a 5.5V)
- Clase LF: Bajo voltaje (2.0 V a 5.5V)

Los dos tipos son exactamente iguales, la diferencia se encuentra en que los del tipo LF pueden ser usados con la nueva alimentación de 3.3V que actualmente y poco a poco se está imponiendo a los típicos 5V.

1.2.2 Características

Las características principales de microcontrolador PIC18F4550 son las que se indican en la tabla 1.1.

Tabla 1.1: Características principales del Microcontrolador PIC18F4550

Memoria de programa – Flash:	32768 bytes
Juego de instrucciones:	75 modo normal 83 modo extendido
Máximo número de instrucciones simples:	16384
Memoria de datos – SRAM:	2048 bytes
Memoria de datos – EEPROM:	256 bytes
Puertos de Entrada/Salida	A, B, C, D, E
Entradas / Salidas:	35
Fuentes de interrupción:	20
Número de entradas A/D:	13
Número de módulos CCP:	1
Número de módulos ECCP:	1
Soporta SPP:	Si
Soporta SPI:	Si
Soporta Master I2C:	Si
Número de EAUSART:	1
Número de comparadores:	2
Número de temporizadores de 8 bits:	1
Número de temporizadores de 16 bits:	3
Frecuencia de operación:	Hasta 48MHz
Universal Serial Bus (USB) Module:	Si
Velocidades de comunicación USB :	Baja Velocidad (1.5Mb/s) Alta Velocidad (12Mb/s)

Se destaca en este microcontrolador la capacidad de comunicación USB a alta y baja velocidad, por lo que es muy útil al momento de diseñar periféricos USB. Además, de su capacidad de comunicación SPI con lo cual puede comunicarse fácilmente con otros dispositivos como conversores A/D y D/A, memorias EEPROM, RAM, transmisores/receptores de RF, etc.

La configuración de pines del microcontrolador PIC18F4550 se presenta en la figura 1.1.

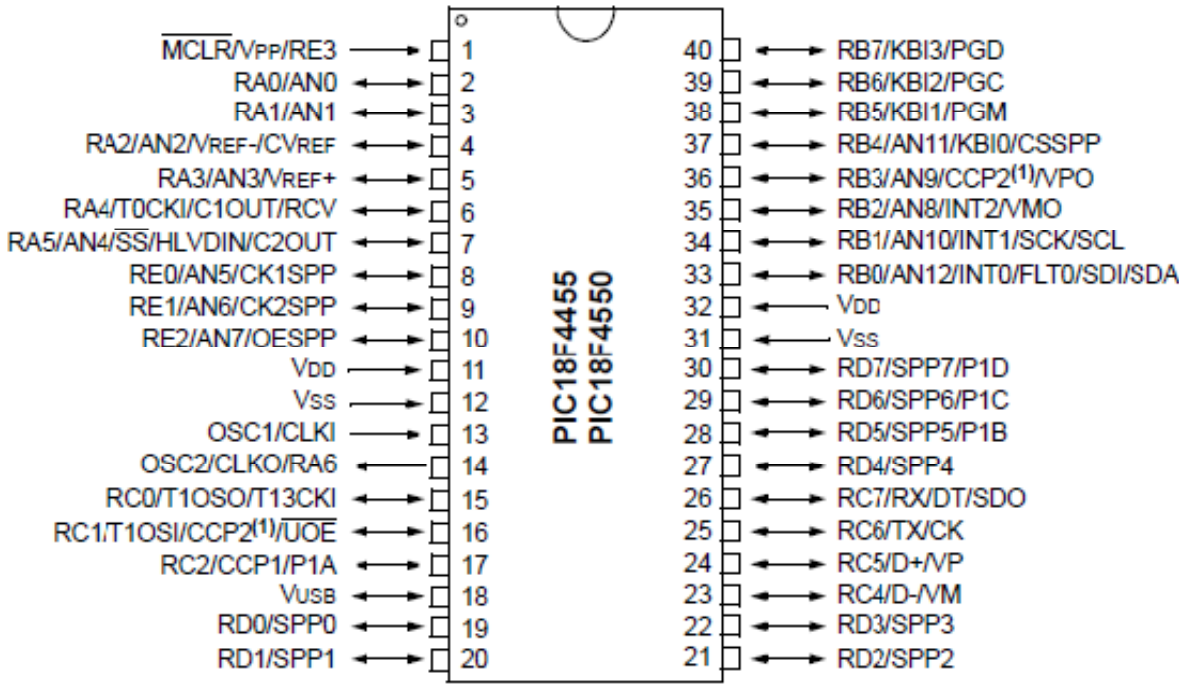


Fig. 1.1: Distribución de pines del microcontrolador PIC18F4550

El diagrama de bloques del microcontrolador PIC18F4550 se presenta en la figura 1.2.

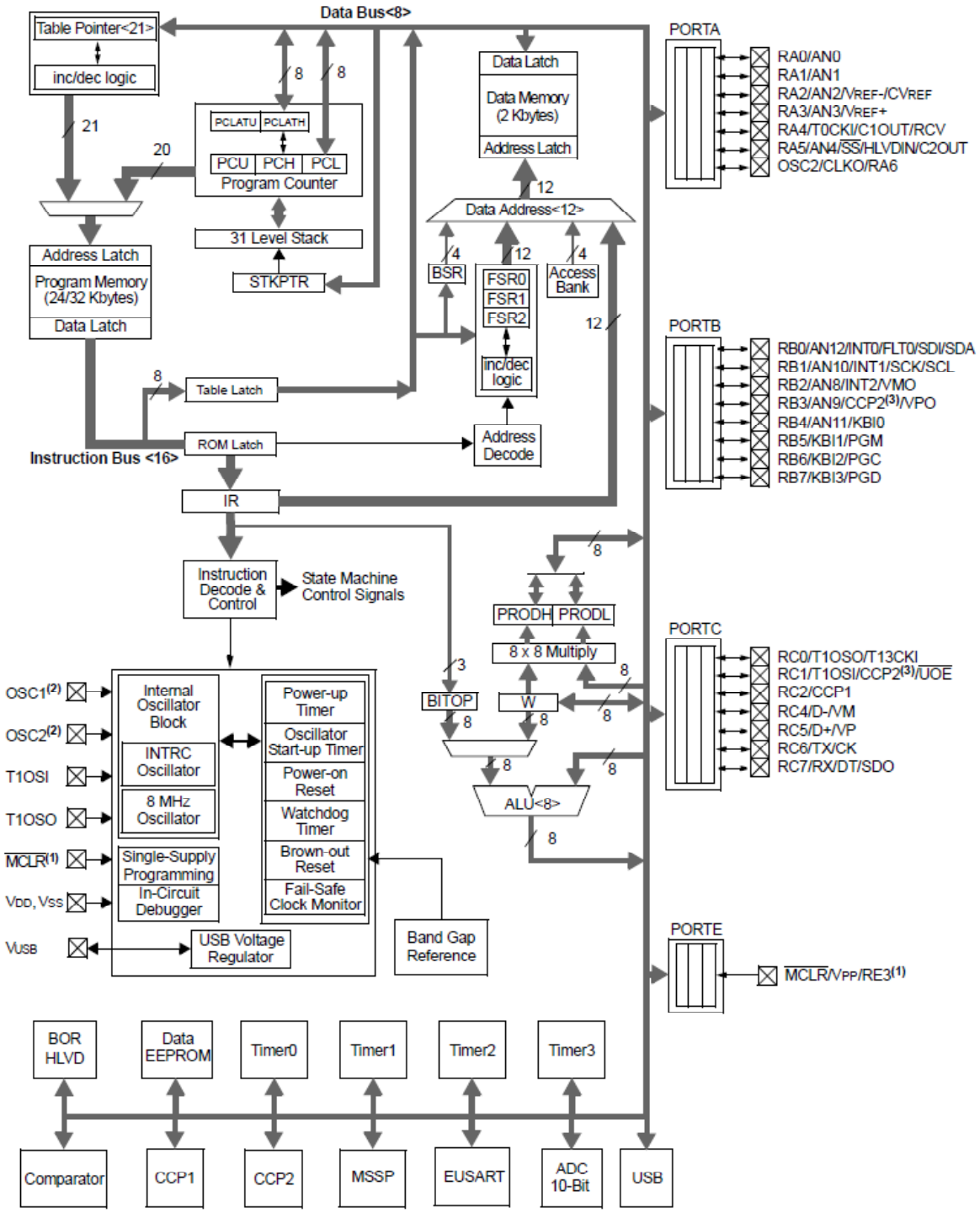


Fig. 1.2: Diagrama de bloques del microcontrolador PIC18F4550

1.2.3 Interrupciones

Las interrupciones son tareas programas, que el microcontrolador realiza cuando un evento asincrónico se produce. En el microcontrolador PIC18F4550 puede ser provocada una interrupción por alguna de las 20 fuentes que posee; con lo que el microcontrolador deja el programa principal y accede a una parte reservada de la memoria que se llama subrutina de interrupción. Una vez finalizada ésta subrutina continúa el programa principal donde lo había dejado antes de ir a este subprograma.

Las interrupciones en el PIC18F4550 pueden darse por los siguientes eventos:

- Interrupciones externas.
- Interrupciones por desbordamiento del contador.
- Interrupciones de EUSART.
- Interrupciones USB.
- Interrupciones del CAD.
- Interrupciones por periféricos externos.

El microcontrolador puede tener varias interrupciones programadas a la vez, pero hay que tener en cuenta que una vez que el microcontrolador ingresa en una subrutina de interrupción, este no puede acceder a otra interrupción hasta que la anterior que se está ejecutando finalice.

En el caso de que se produzcan a la vez 2 o más interrupciones, el microcontrolador accederá aleatoriamente a una de ellas, es por ello que suele darse prioridad a las interrupciones si tenemos alguna interrupción más importante que otra mediante, bits GIEL y GIEH, así como también con consultas de las banderas.

1.2.4 Temporizadores

Los temporizadores son contadores que al activarlos empiezan una cuenta y cuando ésta finaliza se activa una interrupción por el temporizador, entrando el microcontrolador en la subrutina de interrupción del temporizador, siempre y cuando se encuentre activada la correspondiente interrupción.

El PIC18F4550 tiene 4 temporizadores, de los cuales 1 de ellos es de 8 bits y el resto de una precisión de 16 bits. En la figura 1.3 se presenta el temporizador 0 que es de 8 bits.

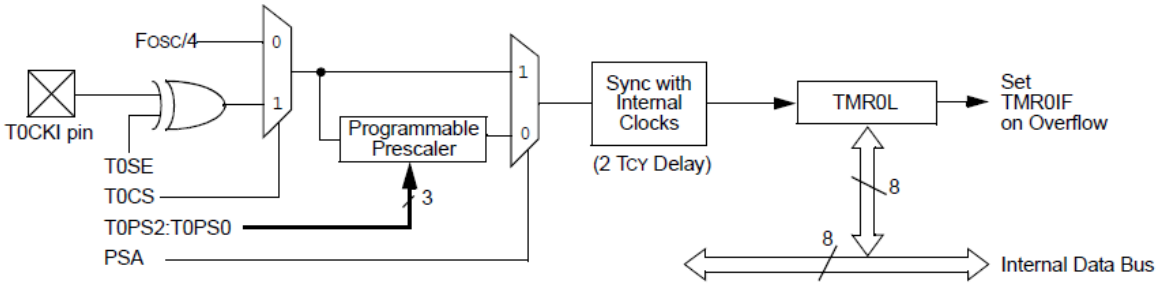


Fig. 1.3: Diagrama de bloques del Timer 0 de 8 bits

Existe la posibilidad de activar un predivisor de frecuencia en los temporizadores de forma que se pueda “alargar” la duración del conteo, dependiendo del temporizador puede ser de 2, 4, 8 e incluso 16. En la figura 1.4 se indica el temporizador 1 con la opción del predivisor (prescaler)

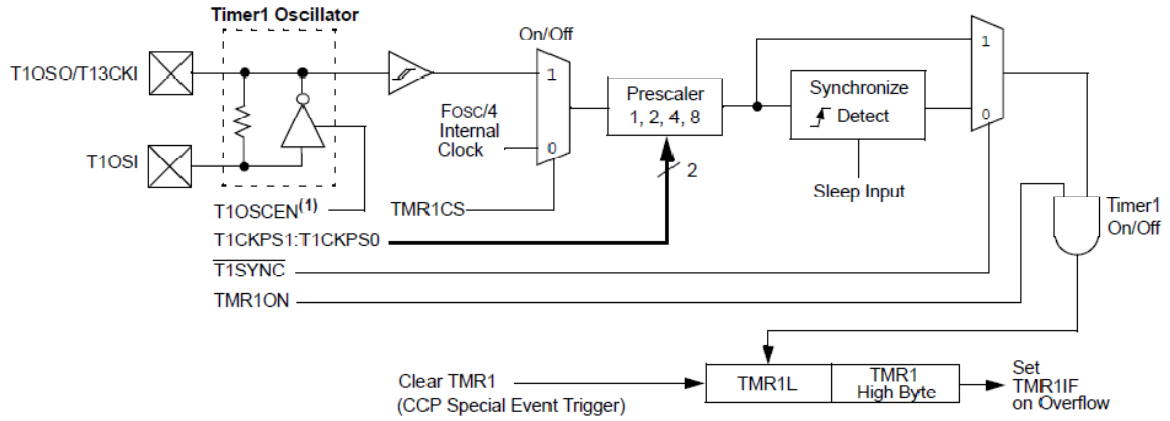


Fig. 1.4: Diagrama de bloques Timer 1

Resolución de los temporizadores:

- Timer0: Temporizador configurable de 8 ó 16 bits.
- Timer1: Temporizador de 16 bits.
- Timer2: Temporizador de 8 bits.
- Timer3: Temporizador de 16 bits.

1.3CONVERSOR ANÁLOGO – DIGITAL

El PIC18F4550 contiene 13 entradas hacia el convertidor analógico digital, las cuales pueden ser seleccionadas en modos de resolución de 8 ó 10 bits, para ello antes habrá que configurar las entradas en modo CAD[1] (entradas/salidas analógicas), pues ya que estas están por defecto como entradas/salidas digitales. En la figura 1.5 se presenta el diagrama de bloques del conversor análogo – digital.

[1] CAD o ADC: Conversor Análogo Digital en el microcontrolador.

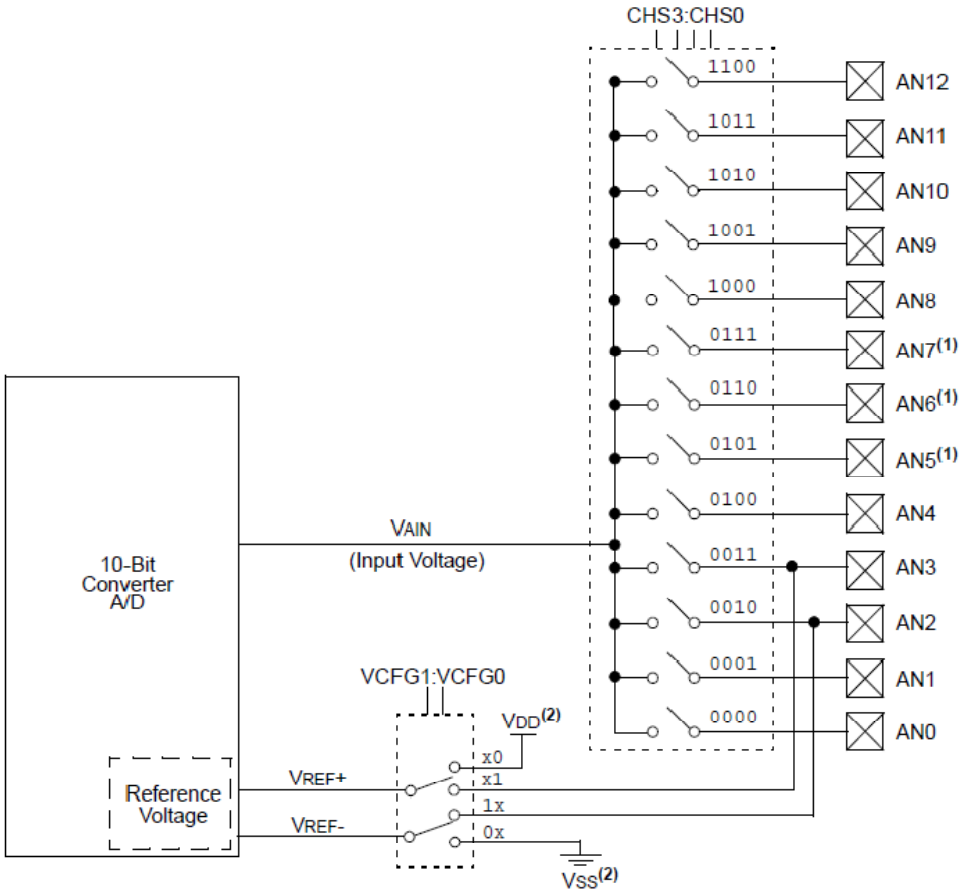


Fig. 1.5: Diagrama de bloques del conversor A/D

Una de las características del conversor es que tiene dos pines de referencia donde puede ingresarse la tensión de referencia para todas o algunas de las entradas del CAD.

Otra opción es configurar el tiempo de adquisición de datos, pues tiene un registro habilitado especialmente pare ello ya que en algunas ocasiones hay que esperar al interruptor de muestreo que se cierre y que el condensador (Chold) se descargue para poder hacer otra adquisición. En la figura 1.6 se indica el modelo de una entrada analógica.

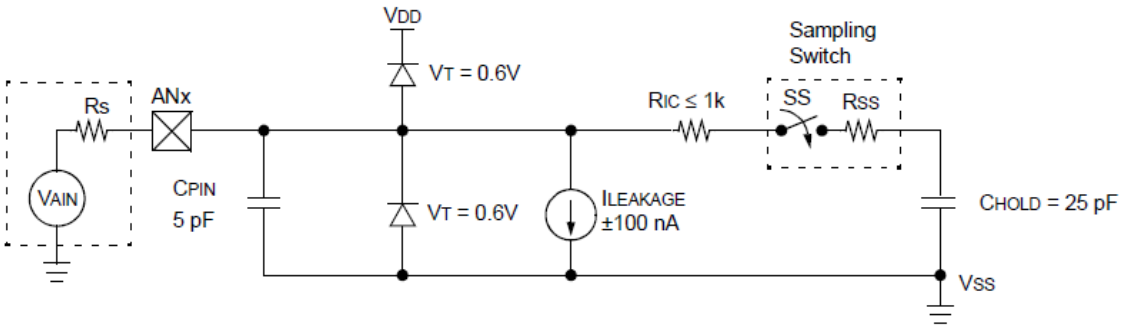


Fig. 1.6: Modelo de entrada analógica

Es recomendable que la máxima resistencia de entrada (Rs) sea de 2.5K, para que la conversión sea fiable, caso contrario debe hacerse una adaptación de impedancias entre la entrada y la señal a convertir.

1.4INTERFAZ USB (Universal Serial Bus)

1.4.1 Introducción

USB es una interfaz para transmisión de datos y distribución de energía desarrollada en el año de 1995 por siete empresas líderes en los sectores de telecomunicaciones y ordenadores como son Compaq (en la actualidad parte de HP), DEC, IBM, Intel, Microsoft, NEC y Northern Telecom y fue introducida en el mercado de computadores y periféricos para mejorar las lentas interfaces serie (RS-232) y paralelo.

En forma general la interfaz consta de 4 hilos (un par para enviar alimentación y el otro para enviar la información) que transmiten la información a una velocidad de 12 Mbps, permite que la conexión de hasta 127 periféricos (plug and play) a una única puerta de un PC, con detección y configuración automáticas, siendo esto posible sin tener que instalar ningún hardware ni software adicionales y lo más importante sin tener que reiniciar el ordenador.

1.4.2 Funcionamiento

Las señales del USB se transmiten en un cable de par trenzado con impedancia de 90 Ω ± 15%, cuyos hilos se denominan D+ y D-[2]. Estos, colectivamente, utilizan señalización diferencial en half duplex para combatir los efectos del ruido electromagnético en enlaces largos, D+ y D- suelen operar en conjunto y no son conexiones simples. Los niveles de transmisión de la señal en las versiones 1.0 y 1.1 varían de 0V a 0.3V para niveles bajos (ceros) y de 2.8V a 3.6V para niveles altos (unos), y en ±400mV en alta velocidad (USB 2.0).

En las primeras versiones, los alambres de los cables no se encontraban conectados a masa, pero en el modo de alta velocidad se tiene una terminación de 45 Ω a tierra o un diferencial de 90 Ω para acoplar la impedancia del cable. Este puerto sólo admite la conexión de dispositivos de bajo consumo; es decir, que tengan un consumo máximo de 100mA por cada puerto aunque con el desarrollo del estándar USB 3.0 se podrán conectar dispositivos que consuman hasta 900mA; sin embargo, en caso de que estuviese conectado un dispositivo que permite 4 puertos por cada salida USB (extensiones de máximo 4 puertos), entonces la energía del USB se asignará en unidades de 100mA hasta un máximo de 500mA por puerto. En la tabla 1.2 se presenta la descripción de pines de la interfaz USB.

Tabla 1.2: Descripción de pines de la interfaz USB

Pin	Nombre	Color de Cable	Descripción
1	VCC	Rojo	5V
2	D-	Blanco	Dato Negativo
3	D+	Verde	Dato Positivo
4	GND	Negro	Tierra

[2] D+ y D-: Denominación que se da al par de hilos por donde viajan los datos en comunicación USB.

El estándar permite que los dispositivos se encadenen mediante el uso de una topología en bus o en estrella como se puede verificar en la figura 1.7; por lo tanto, los dispositivos pueden conectarse entre ellos tanto en forma de cadena como en forma ramificada, ésta se realiza mediante el uso de cajas llamadas "**concentradores**" que constan de una sola entrada y varias salidas. Algunos son activos (es decir, suministran energía) y otros pasivos (la energía es suministrada por el ordenador).

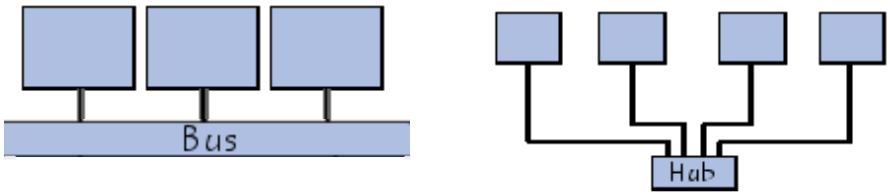


Fig. 1.7: Topologías soportadas por la interfaz USB

La comunicación entre el host (equipo) y los dispositivos se lleva a cabo por medio de un protocolo basado en el principio de red en anillo, lo que significa que el ancho de banda se comparte temporalmente entre todos los dispositivos conectados. El host emite una señal para comenzar la secuencia cada un milisegundo, el intervalo de tiempo durante el cual le ofrecerá simultáneamente a cada dispositivo la oportunidad de "hablar". Cuando el host desea comunicarse con un dispositivo, transmite un paquete de datos que contiene la dirección del dispositivo cifrada en 7 bits que se designa a un dispositivo, de tal manera que es el host el que decide "hablar" con los dispositivos.

Si el dispositivo reconoce su dirección en la red, envía un paquete de datos (entre 8 y 255 bytes) como respuesta, de lo contrario, le pasa el paquete a los otros dispositivos conectados. Los datos que se intercambian de esta manera están cifrados conforme a la codificación NRZI.

Como la dirección está cifrada en 7 bits, 127 (2^7 - 1) dispositivos pueden estar conectados simultáneamente a un puerto, en realidad, es recomendable reducir

esta cantidad a 127 porque la dirección 0 es una dirección reservada. Debido a la longitud máxima de 5 metros del cable entre los dos dispositivos y a la cantidad máxima de 5 concentradores (a los que se les suministra energía), es posible crear una cadena de 25 metros de longitud.

1.4.3 Componentes

El sistema USB consta de tres componentes:

- Un controlador
- Hubs o concentradores
- Periféricos

1.4.3.1 El Controlador

Reside dentro del host y es responsable de las comunicaciones y del control de flujo de datos entre el periférico y el host, también es responsable de la admisión de los periféricos dentro del bus, por lo que detecta tanto una conexión como una desconexión. Para cada periférico añadido, el controlador determina su tipo y le asigna una dirección lógica para utilizarla siempre en las comunicaciones con el mismo. Si se producen errores durante la conexión, el controlador lo comunica al host, la cual se lo transmite al usuario. Una vez se ha producido la conexión correctamente, el controlador asigna al periférico los recursos del sistema que éste precise para su funcionamiento.

1.4.3.2 Hubs o Concentradores

Son distribuidores inteligentes de los datos así como de la alimentación y hacen posible la conexión a un único puerto USB de 127 dispositivos. De una forma selectiva reparten datos y alimentación hacia sus puertas descendentes y permiten la comunicación hacia su puerta de retorno (ascendente).

Un hub de 4 puertos, por ejemplo, acepta datos del host para un periférico por su puerta de retorno y los distribuye a las 4 puertas descendentes si fuera necesario. Los concentradores también permiten las comunicaciones desde el periférico hacia el host, aceptando datos en las 4 puertas descendentes y enviándolos hacia el host por la puerta de retorno.

Algunos host como los computadores poseen un concentrador raíz. Este es el primer concentrador de toda la cadena que permite a los datos y a la energía pasar a uno ó dos conectores USB del host y de allí a los 127 periféricos que, como máximo, puede soportar el sistema. Esto es posible añadiendo concentradores adicionales.

Por ejemplo, si el host tiene una única puerta USB y a ella le conectamos un hub o concentrador de 4 puertas, el PC se queda sin más puertas disponibles; sin embargo, el hub de 4 puertas permite realizar 4 conexiones descendentes. Conectando otro hub de 4 puertas a una de las 4 puertas del primero, se ha creado un total de 7 puertas a partir de una puerta del host. De esta forma; es decir añadiendo concentradores, un host puede soportar hasta 127 periféricos USB.

La mayoría de los concentradores se encontrarán incorporados en los periféricos. Por ejemplo, un monitor USB puede contener un concentrador de 7 puertas incluido dentro de su chasis. El monitor utilizará una de ellas para sus datos y control y le quedarán 6 para conectar allí otros periféricos. En la figura 1.8 se muestra el esquema de un concentrador típico.

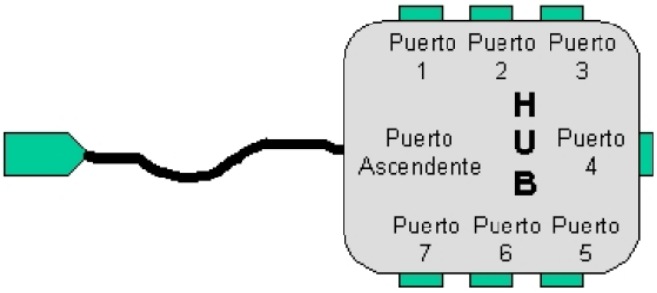


Fig. 1.8: Esquema de un concentrador típico

1.4.3.3 Periféricos

La interfaz soporta periféricos de baja y media velocidad, utilizando dos velocidades para la transmisión de datos de 1.5 y 12 Mbps se consigue una utilización más eficiente de sus recursos. Los periféricos de baja velocidad tales como teclados, ratones, joysticks y otros periféricos para juegos, no requieren 12 Mbps, empleando para ellos 1.5 Mbps, se puede dedicar más recursos del sistema a periféricos tales como monitores, impresoras, modems, scanners, equipos de audio, etc., que precisan de velocidades más altas para transmitir mayor volumen de datos o datos cuya dependencia temporal es más estricta. En la figura 1.9 se muestra un esquema típico de conexión de un bus USB.

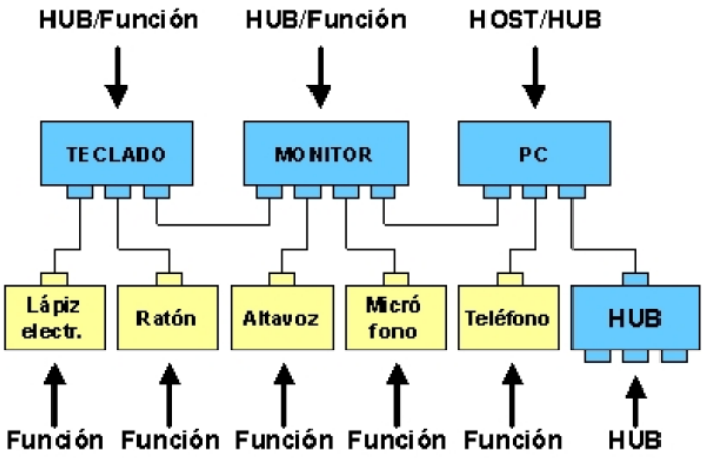


Fig. 1.9: Esquema típico de conexión de un bus USB

1.4.4 Forma de Comunicación

En la figura 1.10 se muestran las capas bajo las cuales se maneja la información entre un nivel real y un nivel lógico.

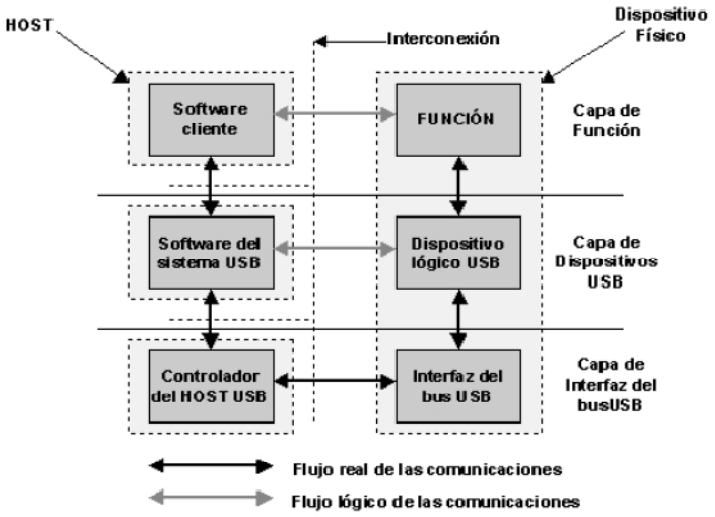


Fig. 1.10: Conexión entre el controlador host y un dispositivo periférico

El software del sistema USB es el que soporta esta comunicación en un determinado sistema operativo, éste se suministra con el sistema operativo independientemente de los dispositivos USB o del software cliente. El controlador anfitrión USB está constituido por el hardware y el software que permite a los dispositivos USB ser conectados al anfitrión.

Ahora, la conexión entre un host y un dispositivo requiere la interacción entre las capas, la capa de interfaz de bus USB proporciona la conexión física entre el host y el dispositivo, la capa de dispositivo USB es la que permite que el software del sistema USB realice operaciones genéricas USB con el dispositivo.

La capa de función proporciona capacidades adicionales al host vía una adecuada capa de software cliente. Las capas de función y dispositivos USB tienen cada una de ellas una visión de la comunicación lógica dentro de su nivel, aunque la comunicación entre ellas se hace realmente por la capa de interfaz de bus USB.

1.4.5 Cables y Conectores

La interface transfiere señales y energía a los periféricos utilizando un cable de 4 hilos, apantallado para transmisiones a 12 Mbps y no apantallado para transmisiones a 1.5 Mbps, debiendo los dos cables destinados para llevar la información ser trenzados o no según la velocidad de transmisión.

El calibre de los conductores destinados a alimentación de los periféricos varía desde 20 a 26 AWG, mientras que el de los conductores de señal es de 28 AWG. La longitud máxima de los cables es de 5 metros.

Por lo que respecta a los conectores son de dos tipos: serie A y serie B. Los primeros presentan las cuatro patillas correspondientes a los cuatro conductores alineadas en un plano, el color recomendado es blanco sucio y los receptáculos se presentan en cuatro variantes: vertical, en ángulo recto, panel y apilado en ángulo recto así como para montaje pasa muro (paredes). Se emplean en aquellos dispositivos en los que el cable externo, está permanentemente unido a los mismos, tales como teclados, ratones y hubs o concentradores.

Los conectores de la serie B presentan los contactos distribuidos en dos planos paralelos, dos en cada plano y se emplean en los dispositivos que deban tener un receptáculo al que se puede conectar un cable USB, por ejemplo impresoras, scanner y módems. En las figuras 1.11 y 1.12 se revisan la distribución de pines y los distintos tipos de conectores USB respectivamente.

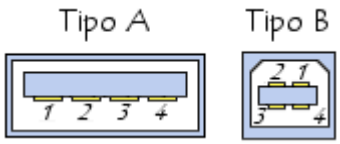


Fig. 1.11: Distribución de pines para los conectores tipo A y B

Fig. 1.12: Distintos tipos de Conectores USB

1.4.6 Clasificación

Existen diferentes variantes de este estándar, de entre las cuales el estándar USB 2.0 es el más usado en la actualidad, este posee una tasa de transferencia de hasta 480Mbps (teóricos) y permite la conexión de prácticamente todo tipo de dispositivos.

Actualmente se habla de “Super Speed USB 3.0” que se encuentra en fase experimental, proponiendo una tasa de transferencia de información de hasta 4.8Gbps (600 MB/s). La alta velocidad de este estándar se consigue gracias a que trabaja con 5 conectores y para hacerla compatible con los estándares anteriores se mantiene la forma de los conectores y la distribución de los 4 pines del estándar USB 2.0. A continuación se muestra las características más relevantes de cada estándar.

USB 1.0

- Contactos o pines: 4 (PW 5v / D- / D+ / GRN)
- Intensidad de corriente: 100mA
- Tasa de transferencia: Hasta 1.5Mbps (192 KB/s)

USB 1.1

- Contactos o pines: 4 (PW 5v / D- / D+ / GRN)
- Intensidad de corriente: 100mA
- Tasa de transferencia: Hasta 12Mbps (1.5 MB/s)

USB 2.0 High Speed

- Contactos o pines: 4 (PW 5v / D- / D+ / GRN)
- Intensidad de corriente: 100mA
- Tasa de transferencia: Hasta 480Mbs (60 MB/s)

USB 3.0 Super Speed

- Contactos o pines: 5
- Intensidad de corriente: 900mA
- Tasa de transferencia: Hasta 4.8Gbs (600 MB/s)

1.5TECNOLOGÍA RFID (Radio Frequency Identification Devices)

1.5.1 Introducción

La tecnología de auto identificación por radiofrecuencia o Radio Frequency Identification Devices (RFID), es un método para identificar objetos, productos, animales o personas que utilicen ondas de radio y etiquetas con microchips. Esta técnica inalámbrica está soportada en el almacenamiento y la recuperación de

datos usando dispositivos llamados etiquetas RFID o transreceptores. Una etiqueta RFID es un objeto que puede ser aplicado o incorporado a cualquier objeto con el fin de identificarlo usando las ondas de radio (ver Fig. 1.13). Algunas etiquetas se pueden leer desde varios metros de distancia.

Estas etiquetas se pueden incorporar a todos los productos y hacen posible identificarlos a distancia, por ejemplo para controlarlos a lo largo de toda una cadena de distribución, desde el fabricante hasta el comprador. Además, permiten almacenar múltiples informaciones referentes al artículo portador de las mismas.

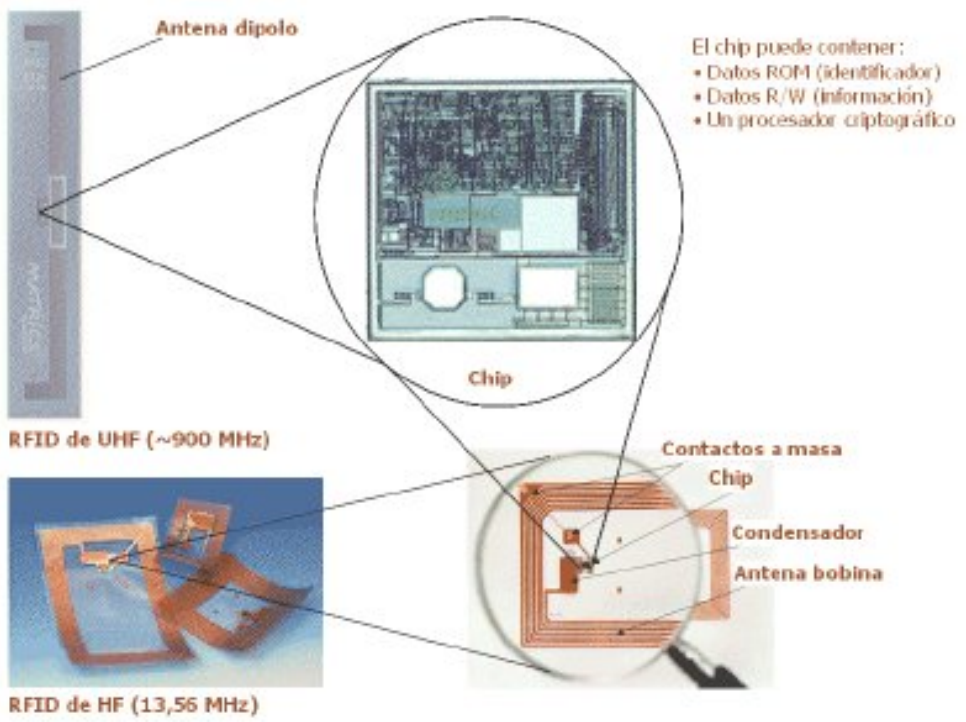


Fig. 1.13: Chip y etiquetas RFID.

La mayoría de las etiquetas RFID contienen por lo menos dos partes. La primera es un chip para almacenar y procesar la información, modulando y demodulando la señal (RF) y otras funciones especializadas, la segunda es la antena para recibir y transmitir la señal. Al no utilizar chips, la tecnología RFID permite la discreta identificación de etiquetas sin un circuito integrado, imprimiendo etiquetas directamente sobre objetos.

1.5.2 Funcionamiento

Para el funcionamiento de la tecnología RFID son necesarios tres elementos básicos: una etiqueta electrónica o tag, un lector de tags y una base de datos. Las etiquetas electrónicas llevan un microchip incorporado que almacena el código único identificativo del producto al que están adheridas. El lector envía una serie de ondas de radiofrecuencia al tag, el cual capta a través de una pequeña antena, estas ondas activan el microchip, que mediante la micro antena y la radiofrecuencia, transmite al lector cuál es el código único del artículo. En definitiva, un equipo lector envía una señal de interrogación a un conjunto de productos y estos responden enviando cada uno su número único de identificación, por este motivo, se dice que la tecnología RFID es una tecnología de auto-identificación (ver Fig. 1.14).

En Resumen:

a) El lector manda una señal de interrogación al RFID.
b) El RFID usa la energía de esta señal para funcionar y su frecuencia como reloj.
c) El RFID lee los datos que manda el lector, en caso de que existan.
d) El RFID contesta con su propia información.
e) Un protocolo anticolisión permite gestionar la respuesta simultánea de múltiples RFID.
f) La información recibida se integra con el resto de Sistemas de Información.

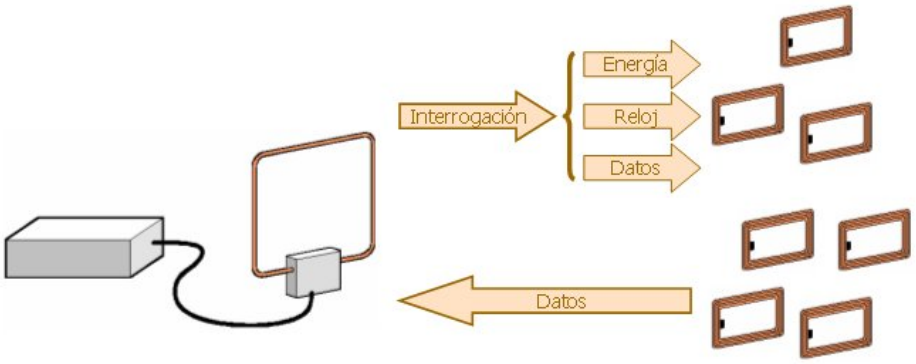


Fig. 1.14: Funcionamiento de la tecnología RFID

1.5.3 Tags

Las etiquetas o tags RFID contienen un chip capaz de almacenar datos (desde un simple identificador a datos más complejos sobre las procedencia del producto, sus características, fecha de envasado y caducidad, etc.). Estos pueden ser activos, semipasivos (también conocidos como semiactivos o asistidos por batería) o pasivos.

La gran mayoría de los tags son pasivos, porque son mucho más baratos de fabricar y no necesitan batería. En el año 2004, estas etiquetas tenían un precio desde $0,40 para grandes pedidos, hasta $0,95 para tags rígidos (encapsulados) usados frecuentemente en el sector textil, precios que se mantienen hasta la actualidad.

Pese a la ventaja en cuanto al costo de las etiquetas RFID pasivas con respecto a las activas, otros factores como la exactitud, el funcionamiento en ciertos ambientes como cerca del agua o metal y la confiabilidad, hacen que el uso de etiquetas activas aumente día a día.

Para comunicarse los tags responden a peticiones o preguntas generando señales que a su vez no deben interferir con las transmisiones del lector, ya que las señales que llegan de los tags pueden ser muy débiles y deben poder

distinguirse. Además, debe poder manipularse el campo magnético del lector por medio de técnicas de modulación de carga en campo próximo y lejano.

1.5.3.1 Tags Pasivos

Los tags pasivos no poseen alimentación eléctrica, la señal que les llega de los lectores induce una corriente eléctrica pequeña y suficiente para operar el circuito integrado CMOS del tag, de forma que puede generar y transmitir una respuesta. La mayoría de tags pasivos utiliza backscatter[3] sobre la portadora recibida; esto es, la antena ha de estar diseñada para obtener la energía necesaria para funcionar a la vez que para transmitir la respuesta por backscatter. Esta respuesta puede ser cualquier tipo de información, no sólo un código identificador. Un tag puede incluir memoria no volátil, posiblemente escribible (por ejemplo EEPROM).

Los tags pasivos suelen tener distancias de uso práctico comprendidas entre los 10 cm y llegando hasta unos pocos metros, según la frecuencia de funcionamiento, el diseño y tamaño de la antena. Por su sencillez conceptual, son obtenibles por medio de un proceso de impresión de las antenas y como precisan de alimentación energética, el dispositivo puede resultar muy pequeño: pueden incluirse en una pegatina o insertarse bajo la piel (tags de baja frecuencia).

En el año 2006, Hitachi desarrolló un dispositivo pasivo con un tamaño de 0,15×0,15 mm sin antena, más delgado que una hoja de papel (7,5 μm), se utiliza *SOI* (*Silicon-on-Insulator*) para lograr esta integración. Este chip puede transmitir un identificador único de 128 bits fijado a él en su fabricación, que no puede modificarse y confiere autenticidad al mismo, tiene un rango máximo de lectura de 30 cm. En febrero del 2007 Hitachi presentó un dispositivo aún menor de 0,05×0,05 mm y lo suficientemente delgado como para poder estar integrado en una hoja de papel. Estos chips tienen capacidad de almacenamiento y pueden funcionar en distancias de hasta unos pocos cientos de metros, su principal

[3] Reflexión de ondas partículas y señales de retorno en la dirección en la que vinieron.

inconveniente es que su antena debe ser como mínimo 80 veces más grande que el chip.

Existen tags fabricados con semiconductores basados en polímeros desarrollados por compañías de todo el mundo. En el año 2005 PolyIC y Philips presentaron tags sencillos en el rango de 13,56 MHz que utilizaban esta tecnología, si se introducen en el mercado con éxito, estos tags serían producibles en imprenta como una revista, con costos de producción mucho menores que los tags de silicio, sirviendo como alternativa totalmente impresa, como los actuales códigos de barras; sin embargo, para ello es necesario que superen aspectos técnicos y económicos, teniendo en cuenta que el silicio es una tecnología que lleva décadas disfrutando de inversiones de desarrollo multimillonarias que han resultado en un costo menor que el de la impresión convencional.

Debido a las preocupaciones por la energía y el costo, la respuesta de una etiqueta pasiva RFID es necesariamente breve, normalmente apenas un número de identificación. La falta de una fuente de alimentación propia hace que el dispositivo pueda ser bastante pequeño, en la práctica, las etiquetas pasivas tienen distancias de lectura que varían entre unos 10 milímetros hasta cerca de 6 metros, dependiendo del tamaño de la antena de la etiqueta y de la potencia y frecuencia en la que opera el lector. En el año 2007, el dispositivo disponible comercialmente más pequeño de este tipo medía 0.05 milímetros × 0.05 milímetros y es más fino que una hoja de papel, estos dispositivos son prácticamente invisibles.

1.5.3.2 Tags Activos

A diferencia de los tags pasivos, los activos poseen su propia fuente autónoma de energía, que utilizan para dar corriente a sus circuitos integrados y propagar su señal al lector. Estos tags son mucho más fiables (tienen menos errores) que los pasivos debido a su capacidad de establecer sesiones con el lector. Gracias a su fuente de energía son capaces de transmitir señales más potentes que las de los

tags pasivos, lo que les lleva a ser más eficientes en entornos dificultosos para la radiofrecuencia como el agua (incluyendo humanos y ganado, formados en su mayoría por agua), metal (contenedores, vehículos). También son efectivos a distancias mayores pudiendo generar respuestas claras a partir de recepciones débiles (lo contrario que los tags pasivos); pero encambio, suelen ser más grandes y caros y su vida útil es en general mucho más corta.

Muchos tags activos tienen rangos efectivos de cientos de metros y una vida útil de las baterías de hasta 10 años. Algunos de ellos integran sensores de registro de temperatura y otras variables que pueden usarse para monitorizar entornos de alimentación o productos farmacéuticos, otros sensores asociados con ARFID (Active RFID) incluyen humedad, vibración, luz, radiación, temperatura y componentes atmosféricos como el etileno. Los tags activos, además de mucho más rango (500 m), tienen capacidades de almacenamiento mayores y la habilidad de guardar información adicional enviada por el transceptor.

Actualmente, las etiquetas activas más pequeñas tienen un tamaño aproximado de una moneda. Muchas etiquetas activas tienen rangos prácticos de diez metros y una duración de batería de hasta varios años.

La principal ventaja de los tags RFID activos respecto a los pasivos es el elevado rango de lectura, el cual está en el orden de decenas de metros. Como desventajas, cabe destacar el precio, que es muy superior que los tags pasivos y la dependencia de alimentación por baterías. El tiempo de vida de las baterías depende de cada modelo de tag y también de la actividad de este, para facilitar la gestión de las baterías es habitual que los tags RFID activos envían al lector información del nivel de batería, lo que permite sustituir con antelación aquellas que están a punto de agotarse.

1.5.3.3 Tags Semipasivos

Los tags semipasivos se parecen a los activos en que poseen una fuente de alimentación propia, aunque en este caso se utiliza principalmente para alimentar el microchip y no para transmitir una señal, la energía contenida en la radiofrecuencia se refleja hacia el lector como en un tag pasivo. Un uso alternativo para la batería es almacenar información propagada desde el lector para emitir una respuesta en el futuro, típicamente usando backscatter. Los tags sin batería deben responder reflejando energía de la portadora del lector lo mas rápido posible.

La batería puede permitir al circuito integrado de la etiqueta estar constantemente alimentado y eliminar la necesidad de diseñar una antena para recoger potencia de una señal entrante, por ello, las antenas pueden ser optimizadas para utilizar métodos de backscattering. Las etiquetas RFID semipasivas responden más rápidamente, por lo que son más fuertes en el radio de lectura que las pasivas.

Este tipo de tags tienen una fiabilidad comparable a la de los tags activos a la vez que pueden mantener el rango operativo de un tag pasivo, también suelen durar más que los tags activos.

1.5.4 Baterías para Tags Activos

Son baterías de larga duración que proporcionan a los tags una alimentación en modo reposo en el cual la corriente consumida es muy pequeña (3uA generalmente) y en modo de funcionamiento, donde se consume 24mA, estas baterías pueden durar de 1 a 10 años lo, que los hace más robustos. Las más utilizadas son las de litio y dióxido de manganeso como la CR2032 y la CR2320, las características técnicas de estas baterías son:

- Sistema químico: Li /MnO2
- Voltaje nominal: 3 V

- Capacidad nominal: 235mAh
- Descarga de corriente estándar: 0,4mA
- Máxima corriente de descarga: 3,0mA
- Peso promedio: 2,8 g
- Rango de temperatura: de -30 a 70 °C
- Descarga pasiva a 23 ºC: < 1 %/al año

1.5.5 Tipos de Antenas

El tipo de antena utilizado en un tag depende de la aplicación para la que está diseñado y de la frecuencia de operación. Los tags de baja frecuencia (LF) normalmente se ayudan de la inducción electromagnética, como el voltaje inducido es proporcional a la frecuencia, se puede producir el necesario para alimentar un circuito integrado utilizando un número suficiente de espiras. Existen tags LF compactos (como los encapsulados en vidrio utilizados para identificación humana y animal) que utilizan una antena en varios niveles (tres de 100-150 espiras cada uno) alrededor de un núcleo de ferrita.

En alta frecuencia (HF, 13,56 MHz) se utiliza una espiral plana con 5-7 vueltas y un factor de forma parecido al de una tarjeta de crédito para lograr distancias de decenas de centímetros. Estas antenas son más baratas que las LF ya que pueden producirse por medio de litografía en lugar de espiración, aunque son necesarias dos superficies de metal y una aislante para realizar la conexión cruzada del nivel exterior al interior de la espiral, donde se encuentran el condensador de resonancia y el circuito integrado.

Los tags pasivos en frecuencias ultra alta (UHF) y de microondas suelen acoplarse por radio a la antena del lector y utilizar antenas clásicas de dipolo, sólo es necesaria una capa de metal, lo que reduce el costo. Las antenas de dipolo, no obstante, no se ajustan muy bien a las características de los circuitos integrados típicos (con alta impedancia de entrada, ligeramente capacitiva), se pueden utilizar dipolos plegados o bucles cortos como estructuras inductivas

complementarias para mejorar la alimentación. Los dipolos de media onda (16 cm a 900 MHz) son demasiado grandes para la mayoría de aplicaciones (por ejemplo los tags para uso en etiquetas no pueden medir más de 10 cm), por lo que hay que doblar las antenas para satisfacer las necesidades de tamaño. También pueden usarse estructuras de banda ancha, la ganancia de las antenas compactas suele ser menor que la de un dipolo (menos de 2 dBi) y pueden considerarse isótropas en el plano perpendicular a su eje.

Los dipolos experimentan acoplamiento con la radiación que se polariza en sus ejes, por lo que la visibilidad de un tag con una antena de dipolo simple depende de su orientación. Los tags con dos antenas ortogonales (tags de doble dipolo) dependen mucho menos de ella y de la polarización de la antena del lector, pero suelen ser más grandes y caras que sus contrapartidas simples.

Pueden usarse antenas de parche (patch) para dar servicio en las cercanías de superficies metálicas, aunque es necesario un grosor de 3 a 6 mm para lograr un buen ancho de banda, además de que es necesario tener una conexión a tierra que incrementa el costo comparado con estructuras de una capa más sencillas.

Las antenas HF y UHF suelen ser de cobre o aluminio, se han probado tintas conductoras en algunas antenas encontrando problemas con la adhesión al circuito integrado y la estabilidad del entorno.

1.5.6 Aplicaciones

Las aplicaciones más comunes de estos sistemas son en el control de accesos y en la inmovilización de vehículos. En el control de accesos se gana en comodidad, no es necesario el contacto físico de la tarjeta con el lector, siendo entonces más cómodo y más fácil de usar. Este es un sistema en el que el interrogador (el dispositivo que lee los datos) debe poder leer muchas tarjetas diferentes, tantas como usuarios hayan autorizados.

También se los emplea en chips identificadores de animales y mascotas, en identificación de equipaje en aeropuertos, para identificar envíos de cartas o paquetes en correos o agencias de transporte, identificación de productos en supermercados, otras aplicaciones posibles son: inventario automático, control de fabricación, identificación de mercancías, distribución automática de productos, logística, sistemas anti-secuestro, localización de documentos, seguimiento de activos de alto valor con sistemas de localización en tiempo real, comercio electrónico, cobranza electrónica del peaje, tarjetas de debito.

1.5.7 Ventajas

- Legible sin visibilidad directa.
- Permite leer múltiples etiquetas simultáneamente de forma automática.
- Tiene un código único, fijado en fábrica o escrito a distancia.
- Identifican cada producto de forma individual.
- Pueden contener información sobre el producto.
- Resistentes a la humedad y temperatura.

1.5.8 Desventajas

Una de las principales desventajas son los costos de implementación pese a que los tags son baratos, los lectores y escritores para RFID son costosos. También existe una gran preocupación sobre la seguridad y privacidad personal ya que el rastreo ilícito de los tags plantea un riesgo a la privacidad personal en términos de localización y de seguridad corporativa o militar.

Y quizás, una de las limitaciones más significativas es que no existe un estándar en cuanto a las frecuencias que deben manejar los tags, lo que implica una incompatibilidad entre dispositivos de distintos fabricantes.

1.6BASES DE DATOS

Una base de datos o banco de datos es un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso. En este sentido, una biblioteca puede considerarse una base de datos compuesta en su mayoría por documentos y textos impresos en papel e indexados para su consulta. En la actualidad, y debido al desarrollo tecnológico de campos como la informática y la electrónica, la mayoría de las bases de datos están en formato digital (electrónico), que ofrece un amplio rango de soluciones al problema de almacenar datos. Por medio de software SGBD (sistemas gestores de bases de datos), se puede almacenar y posteriormente acceder a los datos de forma rápida y estructurada.

1.6.1 Clasificación

Las bases de datos pueden clasificarse de varias maneras, de acuerdo al contexto que se este manejando o la utilidad de la misma. Por lo general se las clasifica según la variabilidad se los datos almacenados y según del contenido de la base de datos.

1.6.1.1 Según la Variabilidad de los Datos

- **Bases de datos estáticas:** Éstas son bases de datos de sólo lectura, utilizadas primordialmente para almacenar datos históricos que posteriormente se pueden utilizar para estudiar el comportamiento de un conjunto de datos a través del tiempo, realizar proyecciones y tomar decisiones.

- **Bases de datos dinámicas:** Éstas son bases de datos donde la información almacenada se modifica con el tiempo, permitiendo operaciones como actualización, borrado y adición de datos, además de las operaciones fundamentales de consulta. Un ejemplo de esto puede ser la base de datos

utilizada en un sistema de información de un banco, un colegio, una universidad.

1.6.1.2 Según el Contenido

- **Bases de datos bibliográficas:** Sólo contienen un representante de la fuente primaria, que permite localizarla. Un registro típico de una base de datos bibliográfica contiene información sobre el autor, fecha de publicación, editorial, título, edición, de una determinada publicación, etc. Puede contener un resumen o extracto de la publicación original, pero nunca el texto completo, porque sino estaríamos en presencia de una base de datos a texto completo. Como su nombre lo indica, el contenido son cifras o números, por ejemplo, una colección de resultados de análisis de laboratorio, entre otras.

- **Bases de datos de texto completo:** Almacenan las fuentes primarias, como por ejemplo, todo el contenido de todas las ediciones de una colección de revistas científicas.

- **Directorios:** Un ejemplo son las guías telefónicas en formato electrónico.

1.6.1.3 Según el Modelo de Administración de los Datos

- **Bases de datos jerárquicas:** Éstas son bases de datos que, como su nombre indica, almacenan su información en una estructura jerárquica. En este modelo los datos se organizan en una forma similar a un árbol (visto al revés), en donde un nodo padre de información puede tener varios hijos. El nodo que no tiene padres es llamado raíz y a los nodos que no tienen hijos se los conoce como hojas.

  Las bases de datos jerárquicas son especialmente útiles en el caso de aplicaciones que manejan un gran volumen de información y datos muy compartidos permitiendo crear estructuras estables y de gran rendimiento.

Una de las principales limitaciones de este modelo es su incapacidad de representar eficientemente la redundancia de datos.

- **Base de datos de red:** Éste es un modelo ligeramente distinto del jerárquico; su diferencia fundamental es la modificación del concepto de nodo: se permite que un mismo nodo tenga varios padres (posibilidad no permitida en el modelo jerárquico).

  Fue una gran mejora con respecto al modelo jerárquico, ya que ofrecía una solución eficiente al problema de redundancia de datos; pero, aún así, la dificultad que significa administrar la información en una base de datos de red ha significado que sea un modelo utilizado en su mayoría por programadores más que por usuarios finales.

- **Bases de datos transaccionales:** Son bases de datos cuyo único fin es el envió y recepción de datos a grandes velocidades, estas bases son muy poco comunes y están dirigidas por lo general al entorno de análisis de calidad, datos de producción e industrial, es importante entender que su fin único es recolectar y recuperar los datos a la mayor velocidad posible, por lo tanto la redundancia y duplicación de información no es un problema como con las demás bases de datos, por lo general para poderlas aprovechar al máximo permiten algún tipo de conectividad a bases de datos relacionales.

- **Base de datos relacionales:** Éste es el modelo utilizado en la actualidad para modelar problemas reales y administrar datos dinámicamente. En este modelo, el lugar y la forma en que se almacenen los datos no tienen relevancia (a diferencia de otros modelos como el jerárquico y el de red). Esto tiene la considerable ventaja de que es más fácil de entender y de utilizar para un usuario esporádico de la base de datos, la información puede ser recuperada o almacenada mediante "consultas" que ofrecen una amplia flexibilidad y poder para administrar la información.

El lenguaje más habitual para construir las consultas a bases de datos relacionales es SQL (Structured Query Language), un estándar implementado por los principales motores o sistemas de gestión de bases de datos relacionales. Durante su diseño, una base de datos relacional pasa por un proceso al que se le conoce como normalización de una base de datos.

- **Bases de datos multidimensionales:** Son bases de datos ideadas para desarrollar aplicaciones muy concretas, básicamente no se diferencian demasiado de las bases de datos relacionales (una tabla en una base de datos relacional podría serlo también en una base de datos multidimensional), la diferencia está más bien a nivel conceptual; en las bases de datos multidimensionales los campos o atributos de una tabla pueden ser de dos tipos, o bien representan dimensiones de la tabla, o bien representan métricas que se desean estudiar.

- **Base de datos deductivas:** Es un sistema de base de datos pero con la diferencia de que permite hacer deducciones a través de inferencias. Se basa principalmente en reglas y hechos que son almacenados en la base de datos. También las bases de datos deductivas son llamadas base de datos lógica, a raíz de que se basa en lógica matemática.

1.6.2 Sistemas de Gestión de Bases de Datos (SGBD)

Los SGBD no manipulan documentos, sino que manipulan registros, es un programa o aplicación capaz de gestionar adecuadamente las bases de datos, actualmente casi todos los SGBD implementan los conceptos descritos en la teoría relacional. Un SGBDR (sistema gestor de bases de datos relacional) almacena la información en tablas organizadas lógicamente que se enlazan definiendo relaciones y contienen datos. El lenguaje de consulta SQL (Structured Query Language), que ha sido estandarizado por la ISO, proporciona la recuperación y gestión de estos datos.

Generalmente las bases de datos manejan transacciones que deben cumplir una serie de propiedades, a las que, comúnmente, se les suele denominar como propiedades ACID (Atomicity, Consistency, Isolation, Durability):

- **Atomicidad**: Garantiza que, o se ejecutan todas las acciones o no lo hace ninguna.
- **Consistencia**: Garantiza que, aunque hayan muchos usuarios accediendo a la base de datos de manera concurrente, se mantenga la integridad de la información.
- **Aislamiento**: Garantiza que, las transacciones que se están realizando concurrentemente en el sistema no interfieran entre ellas.
- **Durabilidad**: Garantiza que, una transacción que finaliza correctamente queda adecuadamente reflejada. Además, el sistema será capaz de recordar todas las transacciones que han sido realizadas.

Los sistemas de gestión de bases de datos que más se utilizan en la actualidad son los que se pueden integrar en la red, entre los que destacan:

- **MySQL:** Se trata de la base de datos relacional de código abierto más popular en Internet.
- **mSQL** (*Mini SQL*): Se trata de un gestor de bases de datos ligero, diseñado para proporcionar acceso rápido a conjuntos relativamente pequeños de datos almacenados en sistemas con poca memoria.
- **PostgreSQL:** Es un gestor de bases de datos Relacional-Objetual, es uno de los sistemas de gestión de bases de datos relacional de código abierto más antiguos, pues la primera versión data de 1985. Está muy extendido en el mundo Unix/Linux ya que muchas distribuciones Linux, como Red Hat lo instalan por defecto, aunque existen versiones para plataformas Windows. Soporta casi todas las construcciones SQL, tiene una amplia conectividad y una gran diversidad de herramientas disponibles.
- **Microsoft SQL Server**: Aunque Microsoft cuenta con productos de escritorio para gestión de bases de datos como Access, este es el sistema de gestión

de bases de datos más potente. Se integra en la nueva plataforma .NET y funciona sobre Windows NT/2000.

- **Sybase Adaptative Server**: Proporciona una plataforma diseñada para soportar aplicaciones que utilizan transacciones de manera intensiva.
- **Oracle:** Existen un gran número de sistemas desarrollados por la empresa Oracle, una de las compañías que desarrollan bases de datos que tienen una mayor presencia en la Web. Se trata de sistemas muy potentes, configurables, escalables y confiables y que proporcionan bastantes funcionalidades, muchas de ellas no soportadas por los sistemas de gestión de bases de datos de código libre. Sin embargo, no son gratuitos y debido a las grandes posibilidades de configuración que ofrecen sólo pueden ser utilizados por expertos.

1.7SISTEMAS DE SEGURIDAD PARA AUTOMÓVILES

En Ecuador, como en el resto de países del mundo, los robos de automóviles son una constante amenaza, siendo cada vez más violentos y provocando cuantiosas pérdidas a los propietarios.

En la actualidad, existen muchos sistemas de seguridad que ayudan a combatir este mal que crece a diario, entre los cuales se encuentran:

- Una alarma sencilla y básica como la sirena. Se pueden encontrar desde aquellas con un tono estándar a las más modernas con varias tonalidades.
- Otro tipo de alarma es la vía móvil, en donde el aviso va desde la central a un teléfono móvil mediante llamada o mensaje.
- Existen las que utilizan la vía GPS/GSM, estos sistemas se basan en la localización vía satélite del vehículo e indica el punto exacto en el que se puede encontrar el automóvil.

El sistema más seguro para proteger el vehículo de los ladrones es un inmovilizador electrónico, que garantiza un porcentaje de seguridad superior al

80%, pero cabe recalcar que los robos más comunes se ejecutan con ladrones menos experimentados por lo que este porcentaje de seguridad se vería reducido si son personas más experimentadas y agresivas. A continuación se brinda una breve explicación del funcionamiento de algunos sistemas de seguridad de tipo electrónico existentes.

1.7.1 Antirrobo con GSM[4] y SMS[5]

Este sistema puede conectarse a la salida de un sistema de alarma ya existente. Por otra parte, se trata de un dispositivo "personal", en el sentido de que la señal de alarma se envía directamente al teléfono móvil del propietario del vehículo, claro que para ello ha de disponer de teléfono móvil GSM y debe estar siempre conectado. Los mensajes de alarma, enviados en forma de SMS (Short Messages System), contienen las coordenadas geográficas que definen la posición del vehículo robado, ya que el sistema incorpora un receptor GPS (Geografic Position System) de gran precisión. Estos mensajes se transmiten automáticamente si el sistema antirrobo entra en funcionamiento y, además, el equipo puede ser "interrogado" desde el teléfono móvil del propietario en cualquier momento para conocer la posición exacta del vehículo. A la recepción del mensaje de alarma el propietario puede intervenir personalmente (si el vehículo se encuentra en las inmediaciones) o alertando a la fuerza Policial o en el mejor de los casos al Ejercito.

El sistema puede activar (desde la unidad remota) dos salidas relé con las que pueden controlarse otras funciones. Por ejemplo: una salida podría cortar la corriente eléctrica al encendido y la otra podrá activar el claxon y las luces de emergencia. La supresión del encendido implica la detención inmediata del vehículo, pero hay que tener cuidado porque, si se desencadena esta situación en una autopista o carretera a alta velocidad puede crearse un peligro adicional,

[4] GSM: Sistema Global para Comunicaciones Móviles ("*Global System for Mobile communications*"). Protocolo de comunicaciones usado en telefonía móvil.
[5] SMS: Servicio de Mensajes Cortos ("*Short Message Service*"), sistema de mensajes de texto para teléfonos móviles.

quizás muy elevado, para los otros usuarios de la ruta. Esta solución se usa sólo cuando se tiene la certeza de que el vehículo está parado, por ejemplo, después de recibir dos o más veces consecutivas la misma posición geográfica. En la figura 1.15 se muestra un módulo GSM/SMS usado en este sistema.

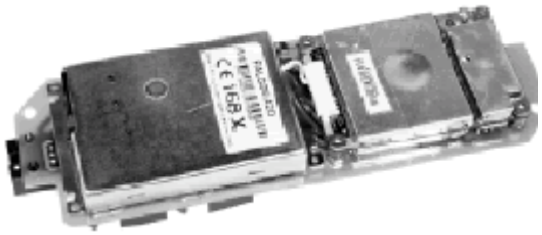


Fig. 1.15: Módulo GSM/SMS usado en este tipo de sistema

1.7.2 Antirrobo por Paro del Motor

En este sistema, el vehículo funciona normalmente por unos segundo, luego un circuito provocará el paro del motor del automóvil (simulando una avería en el encendido), haciendo desistir al posible intento de robo. Este ciclo se repite sucesivamente en tanto que el intruso persevere en su acción. Un interruptor oculto activa y desactiva este sistema, el consumo de corriente es casi nulo debido al uso sólo de elementos pasivos, por lo que podría dejar el dispositivo de alarma conectado sin problema, incluso en largos períodos en que el automóvil se encuentre estacionado.

1.7.3 Antirrobo GPS

Este sistema trabaja en conjunto con una alarma existe en el vehículo, se usa únicamente para recuperación del automóvil robado ya que no ofrece alguna característica de bloqueo hacia algún elemento del vehículo, brindando únicamente información de la localización exacta del mismo. Una vez que se obtienen las coordenadas se puede optar por ir personalmente por el vehículo o avisar a las autoridades, este sistema es tan estricto como los de uso militar (en el

peor de los casos, el error puede oscilar entre los 4 y 5 metros), lo ofertan algunas empresas como Chevrolet y su principal ventaja es que no tiene límite de distancia mientras se encuentre en una región de cobertura GSM y se pueden aplicar a cualquier tipo de vehículo de vía terrestre o marítima.

1.7.4 Antirrobo de Última Generación

En la actualidad se intenta combinar las ventajas de cada uno de los sistemas indicados anteriormente, obteniendo así dispositivos que permiten monitorear la actividad del vehículo por medio del internet, alerta de alarmas con lo cual, en caso de una situación de anormal, el usuario recibirá un mensaje de alerta de: presión de botón de pánico, apertura de puertas, sensor de golpes, etc. También hacen posible una interacción vía SMS con el teléfono del cliente permitiendo a través del celular poder localizar, abrir seguros, y bloquear/desbloquear el vehículo y finalmente permiten la localización del vehículo por medio del sistema GPS. La figura 1.16 muestra un esquema de un sistema vehicular de última generación.

Fig. 1.16: Esquema de un sistema de seguridad vehicular de última generación

1.7.5 Elementos Básicos de un Sistema de Seguridad Vehicular

Todo sistema de seguridad consta de varios bloques que hacen posible su funcionamiento, a continuación se muestra en la figura 1.17 un esquema básico de un sistema de seguridad estándar.

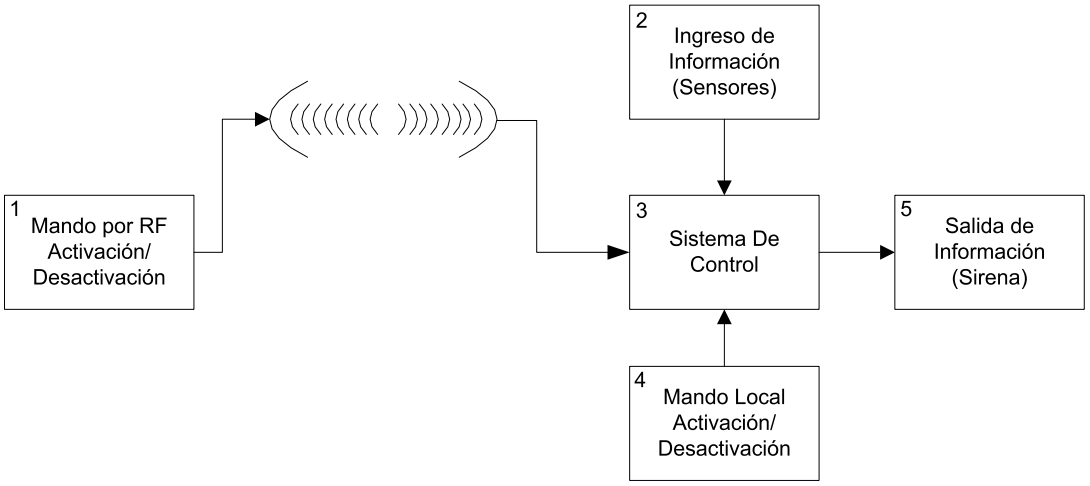


Fig. 1.17: Esquema de un sistema de seguridad básico

1. **Mando por RF (Radio Frecuencia):** De este modo, se consigue la activación/desactivación del sistema de una manera muy simple, únicamente con la pulsación de un botón.

2. **Ingreso de Información:** Se hace por medio de sensores, que en este caso son simples interruptores que indican un estado de encendido/apagado y están colocados en puertas o en el capot, también pueden existir sensores de impacto colocados en los parabrisas para indicar si se están ingresando al vehículo a través de ellos. La información de estos sensores es enviada al sistema de control para ser interpretada.

3. **Sistema de Control:** Aquí se procesa la información enviada por los sensores puede ser desde un simple juego de contacto para activación o desactivación,

hasta micro controladores que realicen una interpretación y procesamiento más complejo de la información.

4. **Mando Local:** El bloque para la activación del sistema puede ser también un interruptor de encendido/apagado. El propietario, antes de abandonar del vehículo, únicamente debe actuar sobre dicho interruptor para producir la activación/desactivación del sistema.

5. **Salida de Información:** Para informar al propietario que su vehículo está siendo robado o desmantelado, un sistema básico consta de una sirena que suena si están ingresando al interior, con lo cual el propietario, según sea el caso, actúe personalmente o informe a las autoridades.

CAPÍTULO II

DISEÑO DEL SISTEMA

2.1ESPECIFICACIONES

El prototipo del sistema de seguridad vehicular con tecnología RFID, interfase USB 2.0 y controles de acceso codificados posee las siguientes características:

- El sistema está diseñado para proveer un aislamiento total del automóvil a través del bloqueo de los inyectores del mismo, esto se consigue colocando una resistencia de bajo valor (47Ω) en relación a la resistencia que presenta el inyector que aproximadamente es de 16 Ω. Al colocar esta resistencia en cada uno de los inyectores se bloquea el paso de combustible hacia el motor, pero el computador del vehículo “piensa” que todos los sistemas se encuentran en funcionamiento sin presentar anomalías.

- Dejando el vehículo con esta conexión en los inyectores no se encenderá bajo ninguna circunstancia, ahora bien, para que se encienda se debe cortocircuitar cada una de las resistencias que se colocaron en los inyectores.

- El cortocircuito de las mencionadas resistencias se lo hace a través de un relé de 12VDC – 14 pines, que está controlado por una de las salidas del PIC18F4550 junto a un circuito de aislamiento, el cual sirve para no afectar el funcionamiento del microcontrolador, cuando se acciona la bobina del relé.

- El relé se activará siempre y cuando se cumplan todas las condiciones programadas en los microcontroladores PIC18F2550 y PIC18F4550. Primeramente para activar el microcontrolador en donde se encuentran programados los códigos de acceso (PIC18F4550) se debe pasar el TAG[6] por el lector RFID[7].

El lector RFID enviará una trama de 12 bytes al PIC18F2550 vía comunicación RS232; en este microcontrolador se seleccionan 3 de los 12 bytes para el reconocimiento del TAG, estos 3 bytes se encuentran almacenados en la memoria EEPROM del microcontrolador. Este microcontrolador también posee comunicación USB 2.0 con el computador por medio de una interfaz diseñada en Visual Basic 6.0 que será utilizada por el propietario del sistema para brindar servicio técnico en caso de pérdida o cambio del TAG.

Realizado el reconocimiento del TAG el PIC18F2550 enviará una señal al PIC18F4550 para que éste salga del modo de espera y permita ingresar el código para encender el vehículo.

Este microcontrolador posee una interfaz gráfica por medio de un LCD alfanumérico y el ingreso de los códigos de acceso a través de un teclado 4x4. Una vez que el PIC18F4550 reciba la señal del PIC18F2550, abrirá los seguros del vehículo por un lapso de tiempo permitiendo el ingreso del conductor; una vez dentro el sistema le pedirá que abra el switch de encendido para poder ingresar la clave de desbloqueo. Ya ingresada la clave de desbloqueo se activa una salida del microcontrolador que hará que se active el relé que cortocircuita las resistencias colocadas en los inyectores, permitiendo que el vehículo se encienda.

Una vez que se apaga el vehículo el sistema abre los seguros durante un período de tiempo hasta que el conductor salga, pasado este tiempo los seguros se

[6] TAG: Etiqueta RFID. Sistema para identificar con tecnología RFID.
[7] RFID: Identificación por Radio Frecuencia.

activan y el sistema está listo para recibir la señal del TAG e iniciar nuevamente el proceso.

El propietario del vehículo tendrá tres oportunidades para ingresar el código de desbloqueo, si no lo ingresó correctamente el sistema le pedirá un código extra para desbloquear por completo todo el sistema. Todos los códigos de acceso se encuentran almacenados en la memoria EEPROM del microcontrolador por lo que si se va la energía no se perderán los códigos. Si el propietario del vehículo se olvida las claves de acceso, el sistema tiene una entrada que sólo la conocen los diseñadores, con la cual se borran por completo las códigos guardados.

2.2DIAGRAMA DE BLOQUES EL SISTEMA

El sistema consta de dos bloques, el primero (ver fig. 2.1) recibe la trama del lector RFID y la compara con la trama guardada en la memoria EEPROM del microcontrolador; si las tramas son iguales se envía una señal al otro bloque para que comience a funcionar. Si no lo son espera a que el lector envíe la trama correcta; todo esto lo hace si el switch de conexión USB está desactivado, si se lo activa hay comunicación entre el microcontrolador y la interfaz realizada en el computador con lo que se da servicio técnico al sistema.

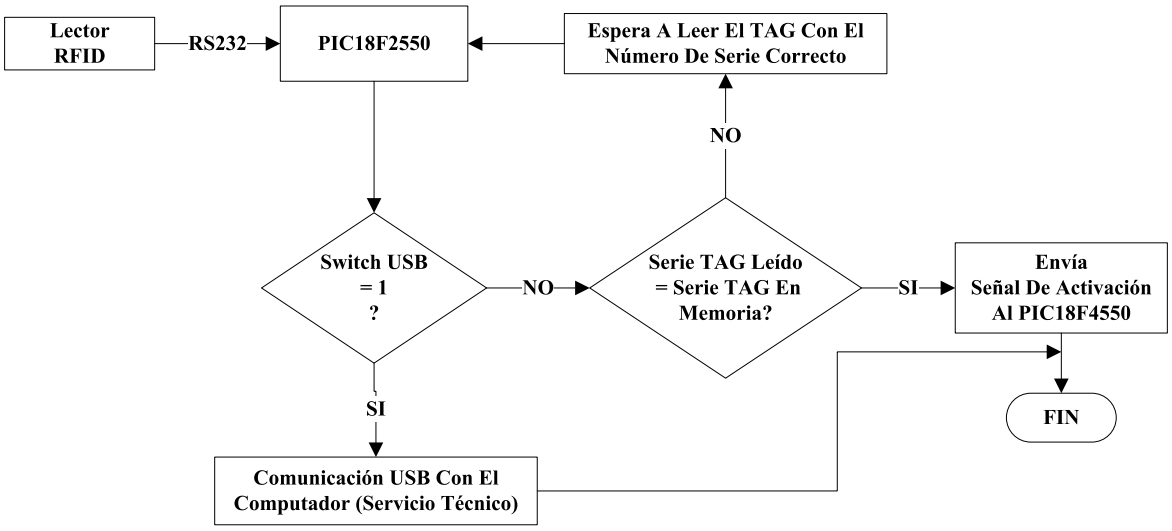


Fig. 2.1: Primer bloque de funcionamiento del sistema.

El segundo bloque (ver fig. 2.2) recibe la señal del primero para salir del modo de espera, con lo cual se desactiva por unos segundos los seguros para luego comprobar si el switch de ignición se encuentra en posición de encendido; si así lo es procede a pedir el código de desbloqueo pero si éste se ingresa incorrectamente por tres veces pasará a pedir otro código de desbloqueo general del sistema.

Luego de ingresar correctamente el código se envía una señal que activa el relé para cortocircuitar las resistencias colocadas en los inyectores, permitiendo encender el vehículo. Una vez que se apague el vehículo el sistema retorna a sus condiciones iníciales esperando leer el TAG correcto para iniciar nuevamente el proceso.

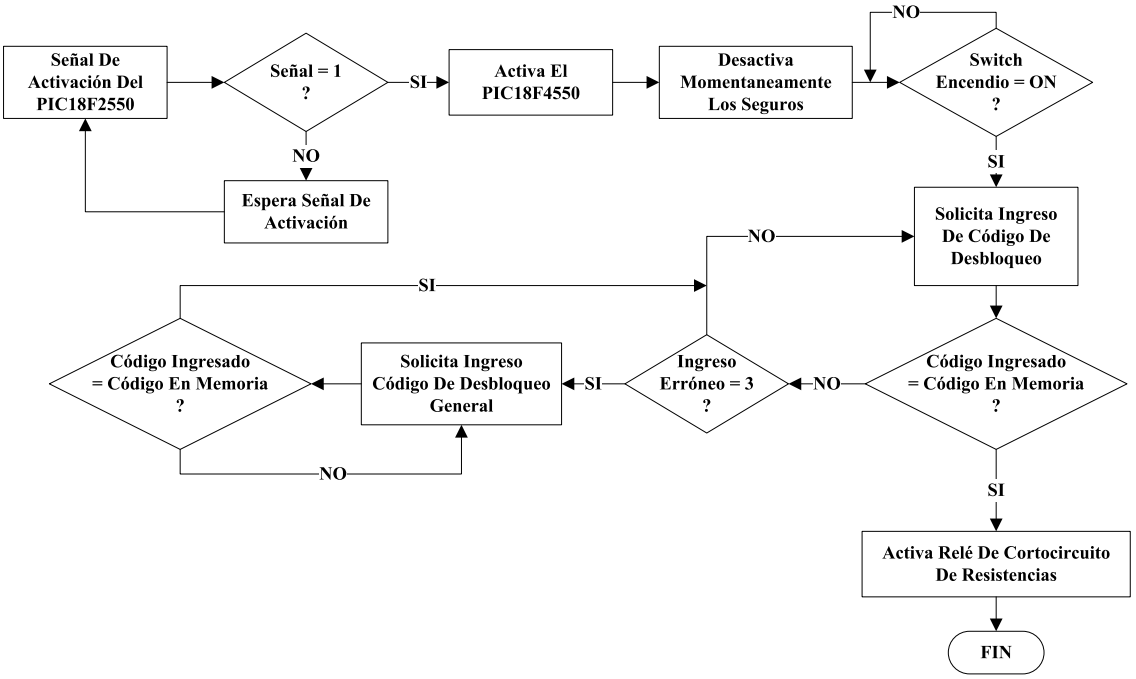


Fig. 2.2: Segundo bloque de funcionamiento del sistema.

2.3CONFIGURACIÓN DEL TECLADO ANALÓGICO

Para optimizar los pines de los puertos del PIC18F4550 se optó por una configuración del teclado matricial muy poco conocida. Se utiliza la configuración que se muestra en la figura 2.3; cuando se pulsa una tecla se genera un valor de voltaje que ingresa al ADC[8] del microcontrolador y será digitalizado dando un valor diferente para cada tecla.

[8] ADC: Conversor Analógico Digital

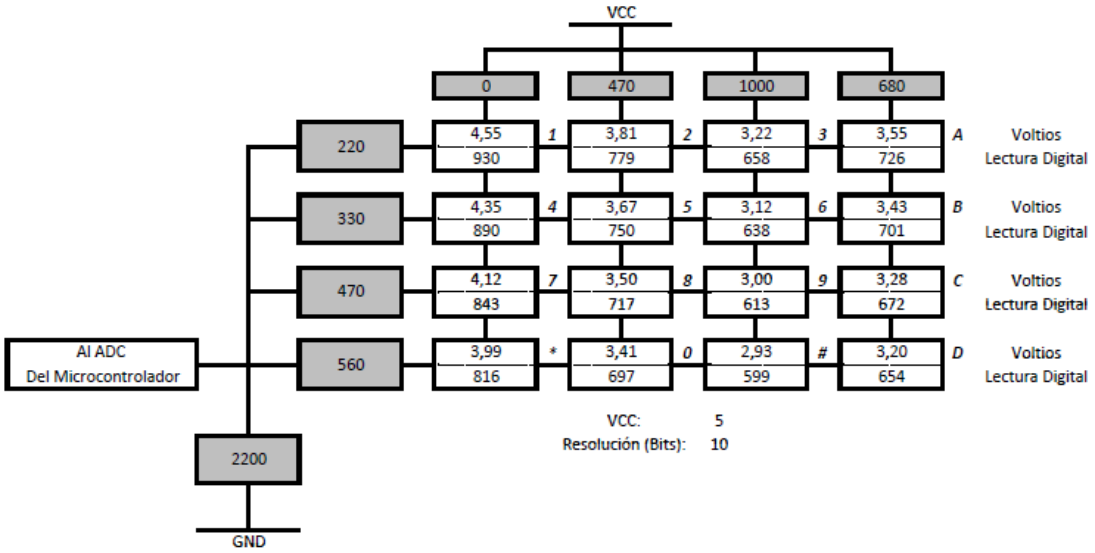


Fig. 2.3: Configuración del teclado analógico con sus respectivos valores de resistencia y lecturas para una resolución del ADC de 10 bits.

Para realizar de una manera más rápida y para tener una plantilla en caso de cambiar los valores de las resistencias se puede implementar esta configuración en una hoja de cálculo en Excel en donde se ingresan las fórmulas para el cálculo de los valores analógicos y digitales para cada tecla; además del voltaje que se usa y la resolución del ADC del microcontrolador. Las fórmulas necesarias son las ecuaciones 2.1 y 2.2.

$$Valor\ Analógico = \frac{Vcc * R.De\ GND}{R.Columna + R.Fila + R.De\ GND} \qquad \text{(EC. 2.1)}$$

Donde:

- VCC: Tensión con la cual se encuentra alimentado el teclado.
- R. De GND: Resistencia que se conecta a tierra.
- R. Columna: Resistencia que se encuentra en la columna de la tecla.
- R. Fila: Resistencia que se encuentran en la fila de la tecla.

$$Valor\ Digital_{10} = \left(\frac{Valor\ Analógico}{Vcc}\right) * 2\text{^}Resolución \qquad \text{(EC. 2.2)}$$

Por ejemplo los valores analógico y digital pertenecientes a la tecla 7 serían 4,12V y 843_{10} respectivamente.

Luego de obtener los valores analógico y digital de cada tecla se debe configurar el ADC del microcontrolador, para esto se empleó el MikroBasic, sin olvidar que pese a ser un lenguaje de alto nivel necesita que se configuren los registros de control para que funcione correctamente, en este caso se debe configurar el registro ADCON1[9].

En este registro se configuran los canales del ADC que van a ser analógicos o digitales además del voltaje de referencia que debe utilizar el microcontrolador para la conversión. Para esta aplicación sólo se necesita un canal analógico por lo cual se configuró al canal 0 del conversor como analógico y al resto como digitales, por lo tanto el valor hexadecimal que colocamos en el registro ADCON1 es 0E.

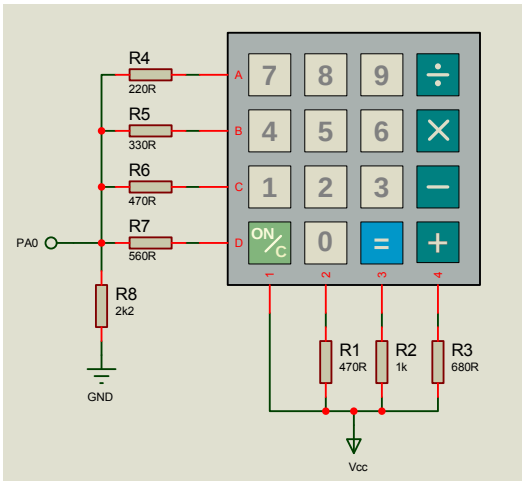


Fig. 2.4: Conexión del teclado analógico 4x4.

[9] PIC18F2550/4550 Microchip Datasheet. Página 262.

Del microcontrolador PIC18F4550 se utilizó por completo el puerto B para el manejo del LCD por lo que debe deshabilitar los canales analógicos de este puerto; con la configuración realizada en el ADCON1 se pensaría que es suficiente, pero muchas veces no lo es por lo que, en la palabra de configuración del microcontrolador también deben deshabilitarse estos canales. Ya que MikroBasic permite hacer esto es recomendable hacerlo al crear un nuevo proyecto. La conexión del teclado realizado se verifica en la figura 2.4, mientras que en la figura 2.5 se presenta la pantalla, en MikroBasic, de la configuración del microcontrolador.

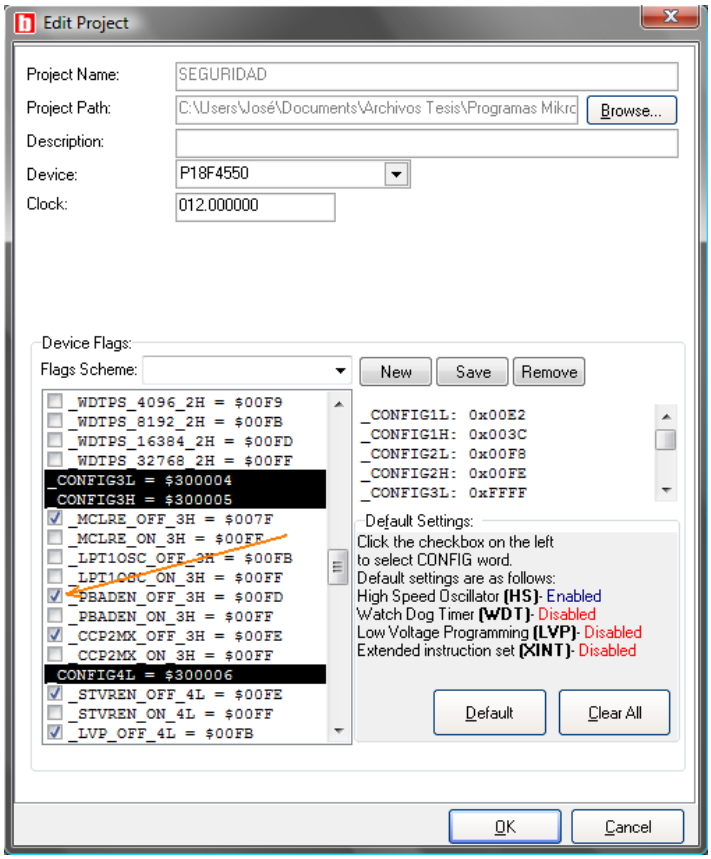


Fig. 2.5: Deshabilitación de los canales analógicos de puerto B desde MikroBasic.

Una vez realizada esta configuración se debe usar la función ADC_READ[10], que lee los 10 bits del conversor y entrega el valor de la lectura en hexadecimal. En el

[10]Librería ADC que utiliza MikroBasic para la lectura del módulo ADC del microcontrolador.

programa se debe utilizar un lazo infinito que lea el valor del ADC durante ciertos intervalos de tiempo, como se muestra en el siguiente fragmento de código.

```
WHILE TRUE

 DELAY_MS[11](100)     'Espera 100ms antes de realizar la siguiente lectura
TMP = Adc_Read(0)    'Lee el canal 0 del ADC y guarda ese valor en la variable TMP

WEND
```

Los valores que se ponen en el programa para reconocer qué tecla se ha presionado son los valores digitales que se calcularon para cada una de ellas, se puede trabajar con valores decimales o hexadecimales, en este caso se utilizan valores hexadecimales. Ahora, como las resistencias poseen tolerancia se debe incluir también a ese valor digital una tolerancia que dependerá del programador, para el diseño se utilizó una tolerancia de ±4 y ±5 al valor digital dependiendo de la tecla y la tolerancia de la resistencia. Por ejemplo para la tecla "1" el valor digital decimal es 930 y hexadecimal es 3A2 con una tolerancia de ±4 se debe entonces hacer la comparación entre 3A6 y 39E para la lectura de esa tecla. En el siguiente fragmento de código se aprecia cómo se realizaría la lectura de algunas teclas.

```
WHILE TRUE
DELAY_MS(100)
TMP = Adc_Read(0)
IF (TMP AND (TMP <> TECLA)) THEN

    IF ((TMP > $32C) AND (TMP < $334)) THEN
      'Lee la tecla "*"
    END IF
```

[11] Librería Delays que utiliza MikroBasic para realizar los retardos de tiempo.

```
    IF ((TMP > $2CE) AND (TMP < $2DC)) THEN
      'Lee la tecla "A"
    END IF

    IF ((TMP > $250) AND (TMP < $25E)) THEN
      'Lee la tecla "#"
    END IF
END IF
TECLA = TMP   'Guarda el valor de la variable TMP en la variable Tecla
              'para poder realizar la siguiente lectura

WEND
```

En el programa diseñado cada que se presiona una tecla se guarda el valor de ésta en un acumulador para luego poder realizar operaciones que permitan hacer el ingreso o cambio de los códigos de acceso. En el siguiente fragmento de código se muestra cómo se guarda el valor de la tecla "3" en un acumulador, además de utilizar la tecla "*" para llamar a una subrutina después de 30ms de presionada la tecla.

```
IF ((TMP > $28A) AND (TMP < $299)) THEN 'Tecla 3
   ACUM = 3
END IF

IF ((TMP > $250) AND (TMP < $25E)) THEN 'ENTER
     DELAY_MS(30)
     GOSUB[12] COMPROBACION
END IF
```

[12] Usada en Mikrobasic para realizar saltos incondicionales a subrutinas.

2.4CONFIGURACIÓN DEL LCD ALFANUMÉRICO

Al igual que en otros lenguajes de programación en alto nivel para microcontroladores como MicroCode[13], en MikroBasic existen librerías para el uso de LCD's alfanuméricos en interfases de 4 y 8 bits. La interfase de 4 bits es la más usada ya que no utiliza muchas líneas para la comunicación entre en LCD y el microcontrolador. Las funciones más importantes de la librería LCD (4-bit interface)[14] son:

- **LCD_CONFIG(dim byref** data_port **as byte**,**dim** db3, db2, db1, db0 **as byte**,**dim byref** ctrl_port **as byte**,**dim** rs, ctrl_rw, enable **as byte)**: Se utiliza esta función si el puerto de control y el puerto de datos del LCD no van a estar en un único puerto en el microcontrolador. Por ejemplo si los datos salen por el puerto D y el control del LCD lo vamos a realizar por el puerto B, la función sería LCD_Config(PORTD,3,2,1,0,PORTB,2,3,4).

- **LCD_INIT(dim byref** port **as byte):** El envío de datos y el control del LCD se lo realiza únicamente por un puerto con la siguiente configuración D7 - port.7, D6 - port.6, D5 - port.5, D4 - port.4, E - port.3, RS - port.2, RW → port.0. Por ejemplo si el LCD va estar conectado al puerto D la función quedaría LCD_Init(PORTD).

- **LCD_OUT(dim** row, col **as byte**, **dim byref** text **as char**[255]**):** Imprime texto en el LCD en la fila y columna especificadas en la función. Por ejemplo si deseamos imprimir Electrónica en la fila 2, columna 1, la función sería LCD_Out(2, 1, "Electrónica").

- **LCD_OUTCP(dim byref** text **as char**[255]**):** Imprime texto en el LCD desde la posición en la que se imprimió el último caracter.

[13] Mecanique MicroCode Studio software para programación de microcontroladores en alto nivel.
[14] Librería usada en MikroBasic para configurar LCD'S a una interface de datos de 4 bits.

- **LCD_CMD(dim** command **as byte):** Envía un comando al LCD que puede ser para borrar la pantalla, encender el cursor, mover a una fila o columna específica. Por ejemplo para limpiar la pantalla y para apagar el cursor los comandos serían LCD_CMD(LCD_CLEAR) y LCD_CMD(LCD_Cursor_Off) respectivamente.

Las configuraciones que se usaron son las que se muestran en el siguiente fragmento de código.

```
TRISB  = $00
PORTB  = $00

LCD_INIT(PORTB)
LCD_CMD(LCD_CLEAR)
LCD_CMD(LCD_Cursor_Off)
DELAY_MS(90)
LCD_OUT(1, 4, "BIENVENIDO")
LCD_OUT(2, 3, "SEGUCAR v1.0")
```

En el siguiente fragmento de código se puede observar cómo se va mostrando en el LCD el número que presiona con el teclado sin necesidad de incrementar la fila o la columna.

```
IF ((TMP > $39A) AND (TMP < $3A8)) THEN   'Tecla 1
LCD_Out_Cp("1")
ACUM = 1
END IF

IF ((TMP > $303) AND (TMP < $312)) THEN   'Tecla 2
LCD_Out_Cp("2")
ACUM = 2
END IF
```

En la figura 2.6 se verifica la conexión entre el PIC18f4550 y el LCD alfanumérico.

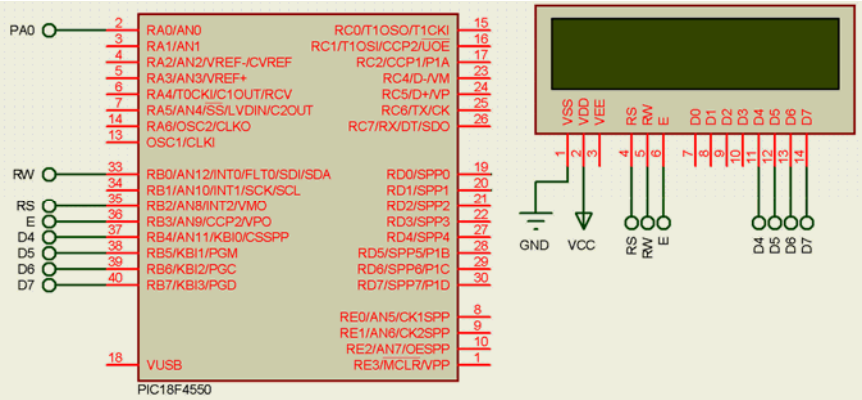


Fig. 2.6: Conexión del LCD al microcontrolador.

2.5LECTURA / ESCRITURA DE LA MEMORIA EEPROM

El microcontrolador PIC18F4550 posee una memoria EEPROM de 256 bytes lo que es más que suficiente para esta aplicación. Esta memoria trabaja con los registros EECON1, EECON2, EEDATA, EEADR[15], los dos primeros son de control de la memoria, el tercero recibe el dato después de la lectura de alguna dirección de la memoria y el último contiene de la dirección a leer/escribir de la memoria.

El hecho de trabajar en alto nivel no quiere decir que debemos olvidarnos de la configuración de los registros en bajo nivel, pese a que en MikroBasic no se usan ya que se encuentran implícitos en las funciones de lectura/escritura de la librería EEPROM, pero aún así en algún momento pueden empleárselos directamente.

Gracias a la librería EEPROM que posee MikroBasic el manejo de las memorias EEPROM de cualquier microcontrolador se hace muy fácil ya que sólo se necesita

[15] PIC18F4550, Microchip Datasheet. DATA EEPROM MEMORY. Página 91.

la dirección de la cual se va a leer o escribir un dato. Las funciones usadas para la lectura y escritura son las siguientes.

- **EEPROM_WRITE(dim** Address **as word):** Lee el dato de una dirección específica de la memoria.

- **EEPROM_READ(dim** Address **as word**, **dim** Data **as byte):** Escribe un dato en una dirección específica de la memoria.

En el siguiente fragmento de código se muestra un ejemplo de lectura y otro de escritura de un grupo de localidades de la memoria EEPROM y realizando la sumatoria de esas localidades en una variable, ayudados de un lazo FOR.

```
FOR EE = 51 TO 100
    ACUM = EEPROM_READ(EE)
    LEER = LEER + ACUM
NEXT EE

FOR j = 51 TO 100
     EEPROM_Write(j,255)
NEXT j
```

Como una recomendación se debe asegurar que, entre funciones de lectura y escritura exista por lo menos un retardo mínimo de 20ms para que en el microcontrolador se escriban o lean correctamente los datos, un ejemplo se muestra en el siguiente fragmento de código.

```
EEPROM_Write($01,38)
Delay_ms(20)
EEPROM_Read($67,255)
Delay_ms(20)
EEPROM_Write(56,$0A)
```

2.6 CONFIGURACIÓN DE LA INTERFAZ USB 2.0 ENTRE EL PC Y EL SISTEMA DE SEGURIDAD

La configuración de la interfaz USB 2.0, se realiza con el PIC18F2550 el mismo que permite este tipo de comunicación debido a que su estructura es muy semejante al PIC18F4550 que es el usado para la programación y control del sistema, estos micros permiten comunicación vía USB y lo más importante es que la respuesta que proporcionan lo hacen en tiempo real.

En la figura 2.7 se muestra la configuración de pines del PIC18F2550.

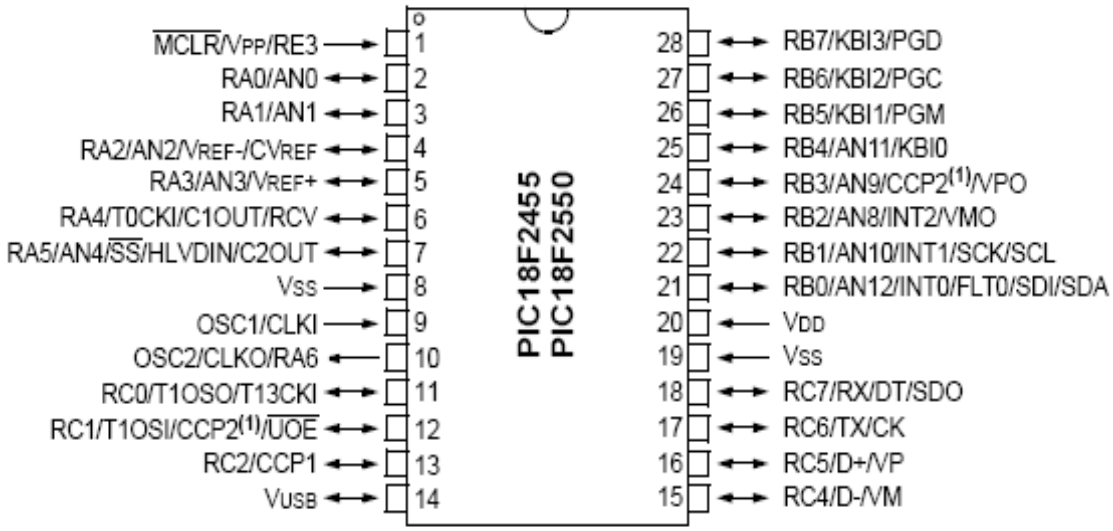


Fig. 2.7: Esquema de pines del PIC18F2550.

La comunicación vía USB 2.0 hacia el PC se puede también configurar y programar con el software MikroBasic 7.2, el mismo que tiene una librería que hace más sencilla su implementación de una forma rápida y fácil.

Para conseguir la comunicación con el PC por medio de este microcontrolador se necesita realizar la conexión del circuito que se presenta en la figura 2.8.

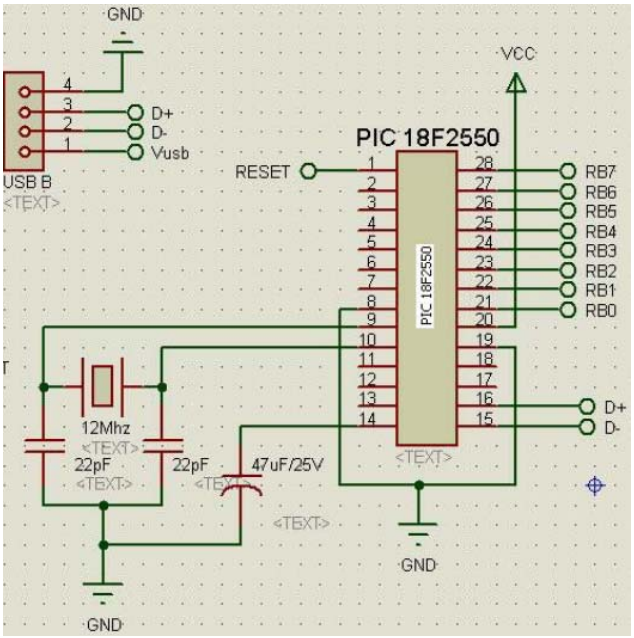


Fig. 2.8: Conexión del PIC18F2550 para comunicación con el PC.

2.6.1 Configuración del Oscilador

Como parte esencial para que el microcontrolador funcione correctamente y se comunique con el PC, debe escogerse con cuidado la configuración del oscilador en el software en MikroBasic 7.2 en base a la configuración de los bits de la palabra de configuración.

El sistema implementado es complejo debido a la inmensa versatilidad y posibilidades que ofrece. En OSC1 y OSC2 se puede conectar un cristal de: 4 MHz, 8 MHz, 12 MHz, 16 MHz, 20 MHz, 24 MHz, 40 MHz ó 48 MHz.

Hay que tener en cuenta que este cristal puede ser el mismo para generar la frecuencia de 48 MHz necesaria para el USB 2.0 y para el reloj del

microcontrolador, o no, según la configuración que al final se adopte, esto quiere decir que se puede tener el USB a 48 MHz y el programa en el microcontrolador funcionando a 12 MHz.

Detrás del Smicht Trigger del oscilador primario salen tres líneas en paralelo que van a módulos distintos con distintas posibilidades.

La opción de inyectar directamente la frecuencia del cristal es obviamente solo posible si usamos un Cristal de 48 MHz que es lo que necesitamos para el USB. Cualquier otro cristal debe ser tratado para conseguir los 48 MHz necesarios.

Esta Opción de inyectar directamente la frecuencia del cristal es sólo posible si se usa un Cristal de 48 MHz que es lo que se necesita para el USB. Cualquier otro cristal debe ser tratado para conseguir los 48 MHz necesarios.

El módulo USB Clock Source tiene a su entrada un PLL Prescaler, o sea un divisor de frecuencia. En cada una de sus salidas se posee FOSC dividida por 1, 2, 3, 4, 5, 6, 10 ó 12, y mediante PLLDIV que no es más que un Multiplexor, se puede seleccionar la que se desea emplear.

Así si el cristal es de 12 MHz y en PLLDIV se coloca un 010 se divide por 3 el valor de FOSC con lo que se tiene 4 MHz a la salida del MUX. Si por el contrario el cristal es de 20 MHz y en PLLDIV se coloca un 100 entonces se divide por 5 FOSC con lo que se obtendrá también 4 MHz a la salida del MUX.

Esta salida del MUX es lo que se utiliza para inyectársela al PLL de 96 MHz. Si se pone 4 MHz él genera 96 MHz, es ésta capacidad de pasar de 4 MHz a 96 MHz la que da la posibilidad de usar una variedad de cristales.

Pero 96 MHz es el doble de lo que hace falta para el USB que son 48 MHz. Así que inmediatamente se debe utilizar un divisor por 2 que es el segundo camino

por el que se llega a USBDIV y en este caso se le pone 1 para usar la señal proveniente del PLL.

Tomar en cuenta que además de inyectar la señal oscilante en USBDIV también se conecta la señal del PLL a 96 MHz en un Postscaler, otro divisor, en este caso por 2, 3, 4 ó 6 y cuyas señales van al CPUDIV. Por lo que se puede generar una señal de reloj para el microcontrolador, no para el USB sino para la velocidad de ejecución del programa tomando esta señal del PLL y que puede ser de 16 MHz, 24 MHz, 32 MHz ó 48 MHz.

Pero, además la señal original ingresa en paralelo al Oscilator Postcaler, otro divisor más, que de forma directa, sin pasar por el módulo PLL divide la frecuencia original del cristal por 1, 2, 3 ó 4 y que también va a parar al CPUDIV pero desde otro origen. Con este módulo se puede obtener otra gama de frecuencias distintas para ejecutar el programa.

El CPUDIV a utilizar se lo selecciona con el switch FOSC3:FOSC0 que es de donde se obtiene la definitiva frecuencia de ejecución de programas. Por último, también se dispone de una entrada proveniente del Primary Clock y que dividida por 4 llega también a FSEN y que puede utilizársele en lugar de la que le llega desde el canal directo/PLL.

El resto de flags, para el programa en Mikrobasic 7.2, se configuran en base a lo que se necesite para la programación respectiva, como por ejemplo el master clear, el watch dog y otros.

Como se puede ver es muy amplio este tema de los osciladores, sobre todo con lo que respecta a las inmensas capacidades que tiene para hacer correr el microcontrolador a decenas de velocidades distintas siendo capaz, al mismo tiempo, de tener disponibles los 48 MHz imprescindibles para el USB 2.0.

A continuación, en la figura 2.9, se observa la manera de configurar los flags en Mikrobasic 7.2, la misma que se la debe realizar antes de empezar a desarrollar el programa que permita la comunicación entre el PIC y el PC.

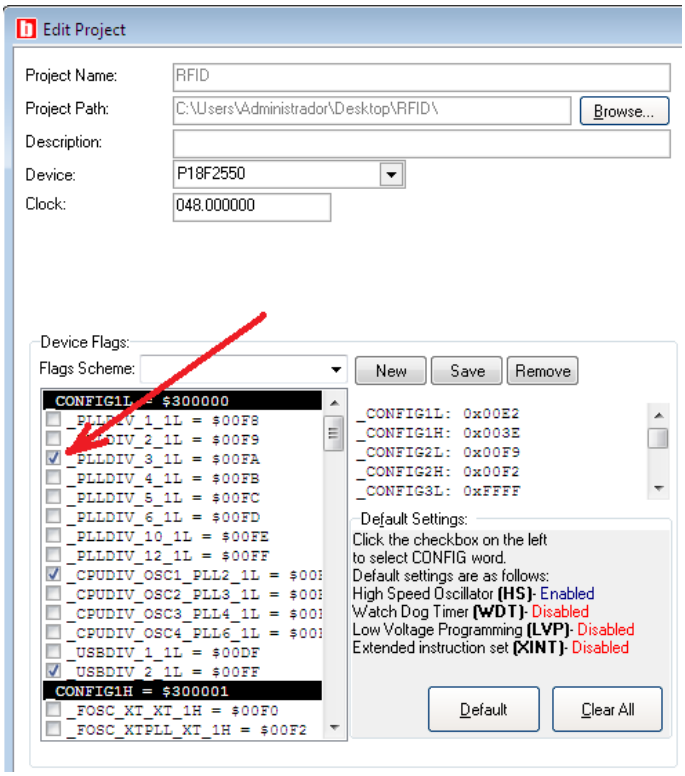


Fig. 2.9: Configuración del Oscilador para el PIC18F2550.

2.7 COMUNICACIÓN PIC – PC

La comunicación entre el microcontrolador y el PC se da por medio de la transmisión de datos en formato TTL, los mismos que inicialmente llegan al PIC18F2550 desde el dispositivo RFID HYE-01, para luego ser enviados al PC.

2.7.1 Lector HYE-01

Por medio de este lector de marca Huayuan, se logra leer el número serial de un TAG. Su salida da formato de las interfases RS232/RS485 y Wiegand. Este es un

lector de frecuencias bajas de 125 KHz y actualmente es usado en sistemas de acceso, en la figura 2.10 se puede observar al lector HYE-01.

Fig. 2.10: Lector HYE-01

Características del Lector HYE-01

Frecuencia de Operación: 125KHz
Transponders[16] Soportados: EM4100/EM4102; GK4001
Antena: Interna Integrada
Codificación: Manchester 64 bits – 82.
Rango de Lectura: Hasta 8cm
Interfase Opcional de Datos: RS485, Wiegand26[17], RS232
Velocidad de Transferencia: 9600bps, N, 8, 1
Indicador de Lectura: LED and buzzer
Niveles de Voltaje de Salida: RS232

Descripción de cables en el HYE – 01

Rojo 12V.
Negro GND.

[16] Transponder o tipos de TAG soportados por un lector de radio frecuencia.
[17] Wiegand26: protocolo de comunicación que transmite datos en forma digital en este caso 26 bits, sobre tres canales denominados D0, D1 y GND.

Verde WD0.
Blanco WD1.
Amarillo BUZ.
Azul LED.
Gris TXD.
Café GND.

En este caso, se usan los cables, rojo, negro, café y gris, los mismos que son de polarización y de transmisión de datos.

2.7.2 Funcionamiento del módulo RFID[18]

El módulo RFID emite una señal de radio frecuencia de baja potencia para crear un campo electromagnético. El campo electromagnético es emitido por el transceptor a través de una antena transmisora, típicamente en forma de bobina. Este campo electromagnético funciona como una señal "portadora" de potencia del lector hacia el transponder. Un transponder contiene una antena, también en forma de bobina y un circuito integrado, el circuito integrado requiere de una pequeña cantidad de energía eléctrica para poder funcionar. La antena contenida en el transponder funciona como un medio para tomar la energía presente en el campo magnético producido por el módulo de RFID y la convierte en energía eléctrica para ser usada por el circuito integrado.

Cuando un transponder se introduce en el campo electromagnético producido por módulo de RFID, la energía captada permite que el circuito integrado del transponder funcione, los datos contenidos en su memoria son transmitidos. En la figura 2.11 se puede observar la comunicación entre un transponder y el lector RFID.

[18] V. Daniel Hunt, Albert Puglia, *RFID A guide to radio frequency identification*. Ed. Wiley 2007

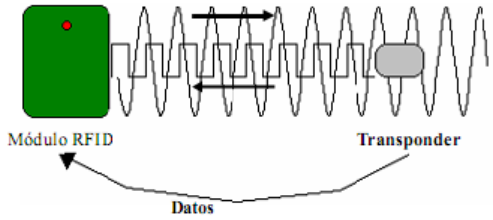


Fig. 2.11: Transmisión de los datos desde el lector RFID hacia el transponder.

La señal electromagnética que proviene del transponder es recuperada por la antena receptora del módulo RFID y convertida a una señal eléctrica. El transceptor tiene un sistema de recepción que está diseñado para detectar y procesar esta "débil" señal proveniente del transponder, demodulando los datos originales almacenados en la memoria del circuito integrado contenido dentro del transponder. Una vez que los datos del transponder han sido demodulados, el módulo digital comprueba que los datos recibidos son correctos.

El lector utiliza información redundante contenida en el código transmitido por el transponder para ejecutar el proceso de validación (BCC). Una vez que el lector verifica que no hay errores y valida la información recibida, los datos son decodificados y reestructurados para su transmisión como información en el formato requerido por el sistema al cual esté conectado el lector.

El rango de lectura, es decir la distancia a la que un lector puede leer un transponder, depende por lo general del tamaño de la antena del lector y del transponder utilizado.La etiqueta RFID, que contiene los datos de identificación del objeto al que se encuentra adherido, genera una señal de radiofrecuencia con dichos datos. Esta señal puede ser captada por un lector RFID, el cual se encarga de leer la información y pasársela, en formato digital, a la aplicación específica que utiliza RFID.

Para el monitoreo de los datos que se reciben desde el lector HYE-01, se usa un snifer (rastreador) que dispone MikroBasic 7.2 con la herramienta USART terminal, la misma que da la opción de saber si son datos hexadecimales,

decimales o ASCII. Debe tomarse en cuenta que antes de su uso se debe configurar su puerto de comunicación y también su velocidad de transmisión, lógicamente que esto se hace mediante un cable convertidor de RS232 – USB. En la figura 2.12 se puede observar la pantalla del USART terminal con el cual se realizo el monitoreo de los datos que envía el lector HYE-01.

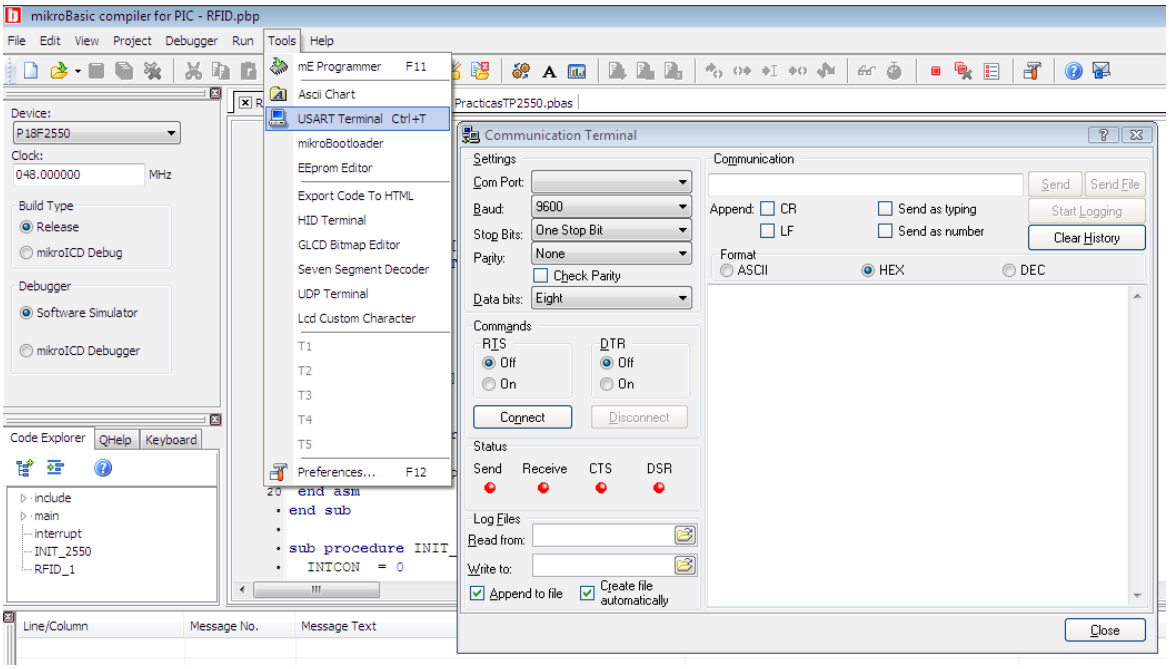


Fig. 2.12: Monitoreo de datos que envía el RFID.

Luego del envió de la trama de datos que viene de el dispositivo RFID (RS-232), esta es recibida y transformada a niveles TTL por medio de un MAX 232 y enviada al PIC18F25250.

2.7.3 MAX-232

Este integrado adapta los niveles RS232 a TTL y viceversa, permitiendo conectar un PC con un microcontrolador. Para eso es necesario 4 condensadores

electrolíticos de 22 microcontrolador-faradios, así mismo este integrado contiene dos drivers (convierten de lógica TTL a voltajes RS232) y dos receptores (convierten de RS-232 a niveles de voltaje TTL). En la figura 2.13 se puede observar la configuración del MAX232.

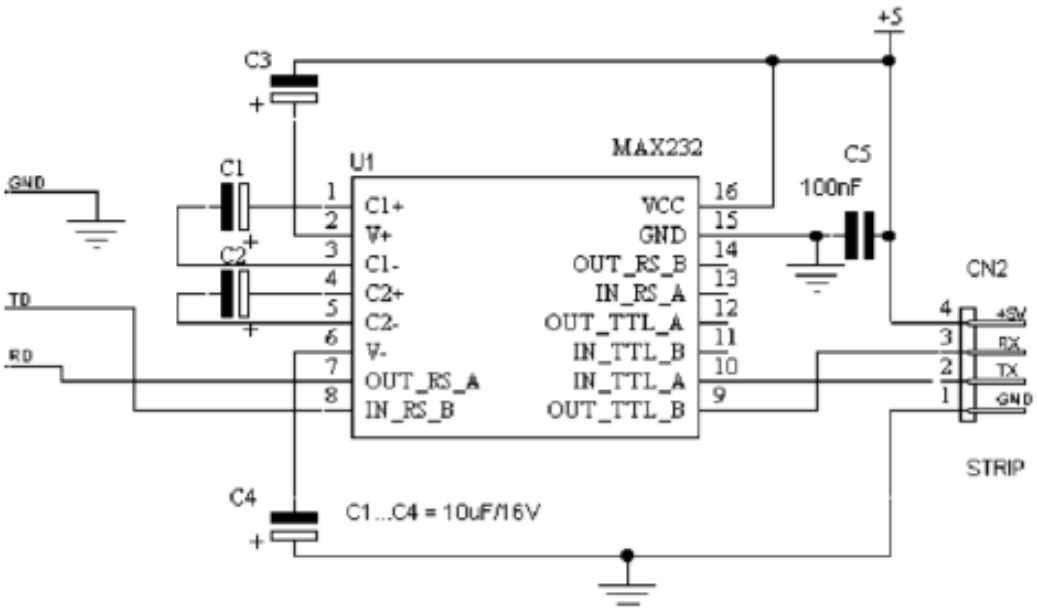


Fig. 2.13: Esquema de la conexión del MAX232.

Una vez que se transmiten los datos a través de los pines 11 y 12 del MAX 232 hacia el microcontrolador, estos son manipulados y tratados por medio del software de programación MikroBasic 7.2. En la figura 2.14 se puede observar una pantalla del software MikroBasic 7.2.

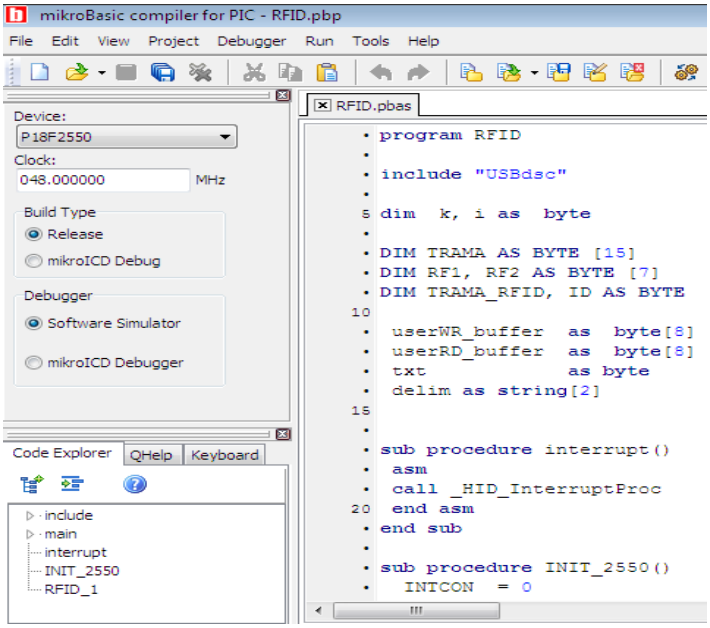


Fig. 2.14: Software de programación MikroBasic 7.2.

Al llegar a este punto, luego de que en el microcontrolador se han recibido los datos de las tramas enviadas por el dispositivo RFID, se procede a configurarle haciendo uso de la librería USB HID Library que se encuentra inmersa en el paquete de MikroBasic 7.2 y permite la comunicación desde y hacia el PC.

2.7.4 USB HID Library[19]

Universal Serial Bus (USB) mantiene un bus serial estándar conectado a una gran variedad de dispositivos, incluso las computadoras, teléfonos celulares, consolas de juegos, PDA, etc.

MikroBasic incluye una biblioteca para trabajar con dispositivos de interface humanos (HID) por medio de un Bus Serial Universal (USB). Un dispositivo de interfase humana, es un tipo de dispositivo que permite que la computadora actúe recíprocamente en forma directa con los humanos, como ejemplo se tiene, el teclado, el ratón, etc. Para hacer uso de esta librería se necesita crear un

[19] Library help, *USB HID Library*, *MIkrobasic 7.2*

descriptor file que es un archivo que se genera automáticamente luego que se configura la conexión con el PC.

2.7.4.1 Descriptor File

Para cada proyecto basado en el USB HID, la biblioteca debe incluir un archivo de fuente de descriptor que contiene el ID del vendedor y el ID del producto. Para crear un archivo del descriptor, se usa el USB HID integrado en el menú de MikroBasic (Herramientas › USB HID Terminal), el nombre predefinido para el archivo del descriptor es USBdsc.pbas, pero puede renombrarse.

El código en los trabajos se considera con 48MHz y las banderas (flags) no deben modificarse sin consultar primero el datasheet. En la figura 2.15 se muestra la ventana en la cual se configuran los parámetros del descriptor file.

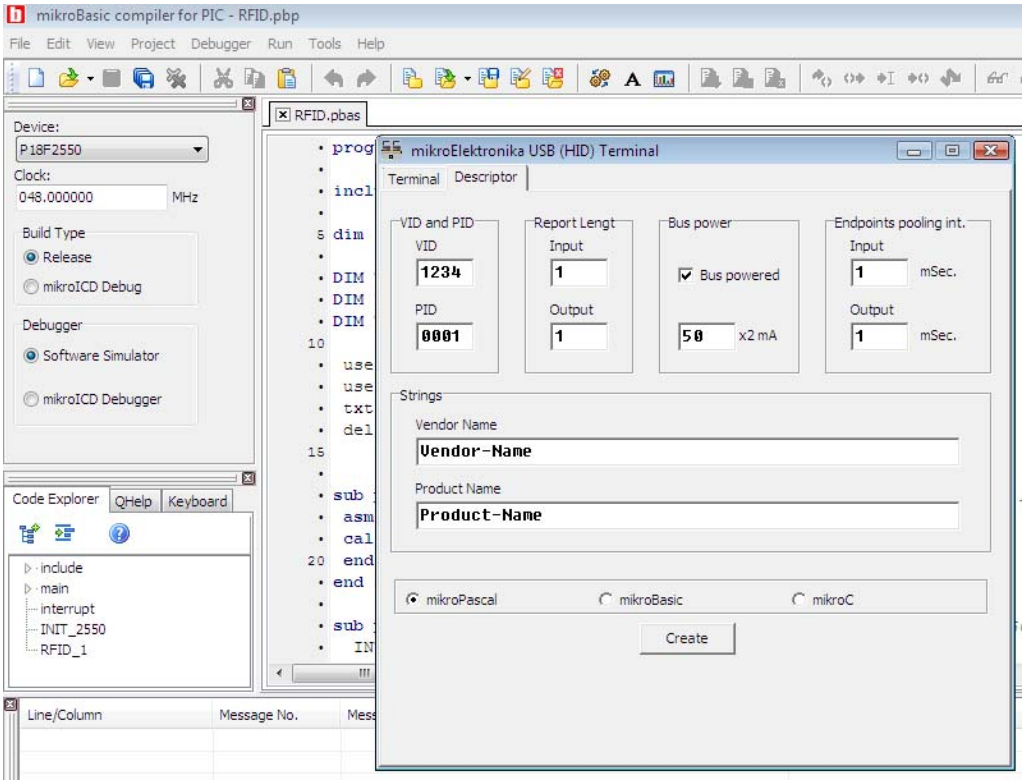


Fig. 2.15: Ventana para configurar el descriptor del microcontrolador.

En este caso, después de la creación del descriptor, el microcontrolador se presentó de la siguiente manera (ver Fig. 2.16).

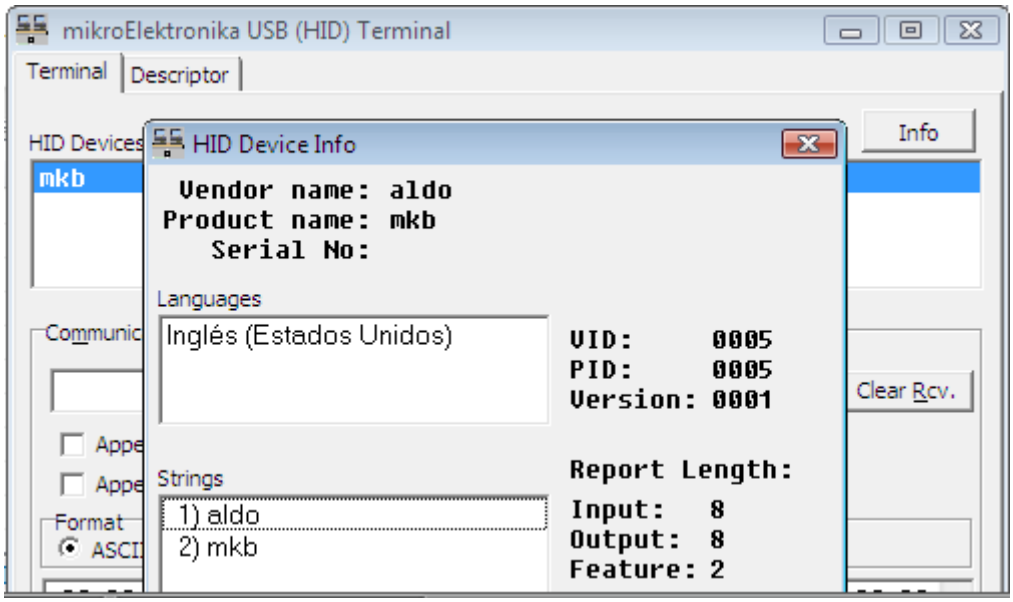


Fig. 2.16: Creación del descriptor file en MikroBasic 7.2.

Para que este descriptor file tenga efecto una vez que se ha programado y configurado el microcontrolador, lo único que se debe tomar en cuenta es que en el programa principal se encuentre como segunda línea de programación el código:

include "USBdsc"

Esto quiere decir que el file descriptor que se creó va a ejecutarse cada vez que se lo requiera en la comunicación USB hacia el PC. Para saber si se esta recibiendo datos desde el microcontrolador en el host del PC se utiliza un Snifer denominado USBTrace.

2.7.5 Rastreo USB (USBTrace) V1.3.1

El USBTrace es un programa para monitoreo de USB para Windows. USBTrace puede monitorear transacciones USB pasando en controladores, concentradores y dispositivos USB. USBTrace es un producto 100% software, especialmente diseñado para inspeccionar el lado del huésped del protocolo USB. USBTrace soporta sistemas operativos Windows 2000, Windows XP, Windows 2003 Server y Windows Vista.

Características del USBTrace[20]

- USBTrace soporta sistemas operativos Windows 2000, Windows XP, Windows 2003 Server y Windows Vista.
- Trabaja con controladores huéspedes, concentradores y dispositivos USB 1.x y 2.0.
- USBTrace puede capturar transacciones USB en controladores, concentradores y dispositivos USB.
- USBTrace puede capturar transacciones USB manejadas por cualquier dispositivo en la pila de dispositivos USB.
- USBTrace captura y despliega valiosa información para desarrolladores de controladores WDM y autores de firmware.
- USBTrace es un analizador de bus no invasivo. No usa ningún tipo de controladores de filtros para capturar transacciones USB.
- USBTrace puede capturar todas las transacciones USB durante la numeración de dispositivos.
- Captura automática para dispositivos conectados en caliente.
- Opciones de búsqueda y filtrado pueden ser realizadas sobre la información capturada.
- Exporta los requerimientos USB monitoreados a archivos de texto, HTML o XML.
- Soporta captura continua para análisis sin detención.

[20] http://www.USBTrace_35293_p/free.htm

En la figura 2.17 se muestra la pantalla principal del software USBTrace, utilizado para monitorear la información que envía el microcontrolador hacia el PC.

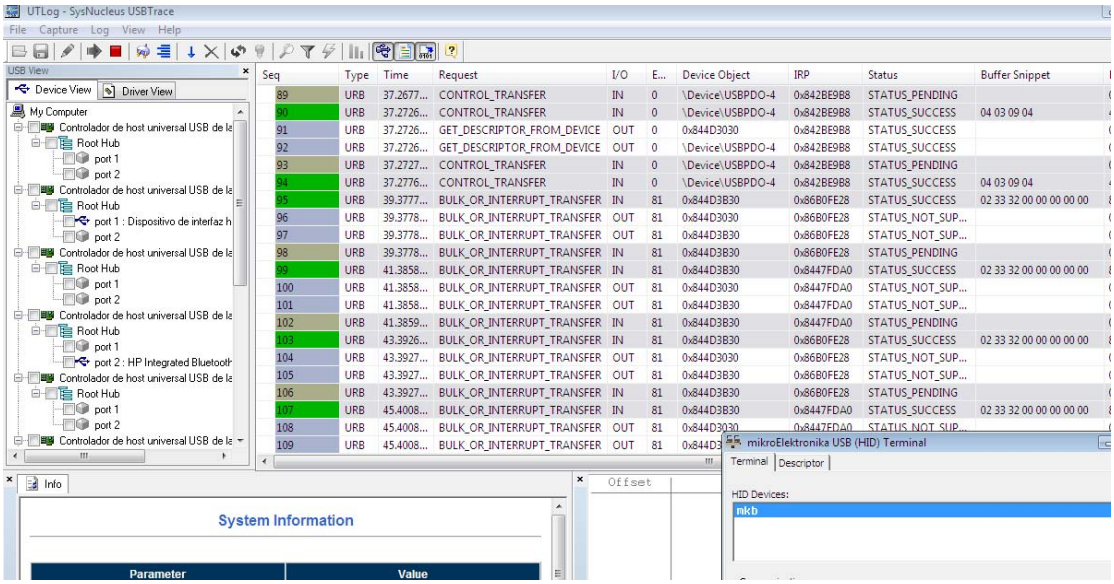


Fig. 2.17: Monitoreo de datos en el host del PC con el USBTrace.

Después de saber que el host en el PC está recibiendo los datos desde el microcontrolador PIC18F2550, se realiza una interfaz gráfica por medio de visual 6.0, (VB6), la misma que permite fácilmente manipular los datos desde y hacia un microcontrolador, gracias a su manejable programación en base a eventos.

2.8 INTERFAZ GRÁFICA CON VISUAL BASIC

Visual Basic es hoy el lenguaje de programación más popular del mundo. Es un producto con una interfaz gráfica de usuario para crear aplicaciones para Windows basado en el lenguaje Basic y en la programación orientada a objetos.

La palabra “Visual” hace referencia al método que se utiliza para crear la interfaz gráfica de usuario. En lugar de escribir numerosas líneas de código para

implementar una interfaz se utiliza el ratón para arrastrar y colocar los objetos prefabricados al lugar deseado dentro de un formulario.

La palabra “Basic” hace referencia al BASIC (Beginners All-Purpose Simbolic Instruction Code), un lenguaje utilizado por más programadores que ningún otro lenguaje en la historia de la informática. Visual Basic ha evolucionado a partir del lenguaje BASIC original y ahora contiene centenares de instrucciones, funciones y palabras clave, muchas de las cuales están directamente relacionadas con la interfaz gráfica de Windows.

Es importante saber también, que la inversión realizada en el aprendizaje de Visual Basic le ayudará a abarcar otras áreas, porque este lenguaje de programación no es exclusivo de la aplicación Visual Basic. Este lenguaje es utilizado también por Microsoft Excel, Microsoft Access y muchas otras aplicaciones Windows. El sistema de Visual Basic Sript para programar en Internet también es subconjunto del lenguaje Visual Basic.

Visual Basic constituye un IDE (entorno de desarrollo integrado o en inglés Integrated Development Enviroment) que ha sido empaquetado como un programa de aplicación, es decir, consiste en un editor de código (programa donde se escribe el código fuente), un depurador (programa que corrige errores en el código fuente para que pueda ser bien compilado), un compilador (programa que traduce el código fuente a lenguaje de máquina) y un constructor de interfaz gráfica o GUI (es una forma de programar en la que no es necesario escribir el código para la parte gráfica del programa, sino que se puede hacer de forma visual). En la figura 2.18 se muestra la pantalla inicial del Visual Basic 6.0.

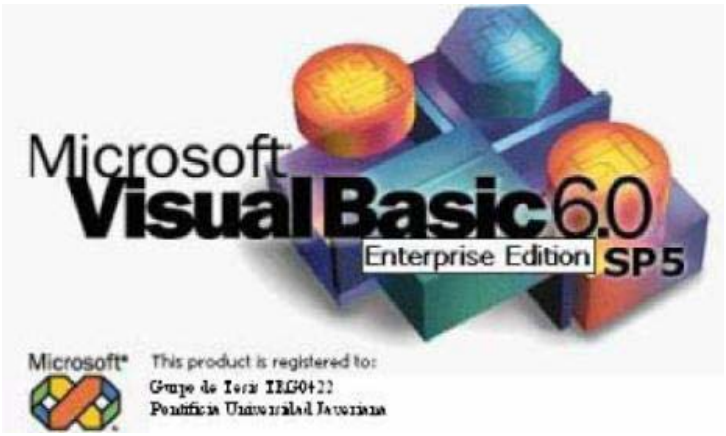


Fig. 2.18: Pantalla inicial del Software Microsoft Visual Basic 6.0.

2.8.1 Modo de Diseño y Modo de Ejecución de Visual Basic 6.0

La aplicación Visual Basic de Microsoft puede trabajar de dos modos distintos: en modo de diseño y en modo de ejecución. En modo de diseño el usuario construye interactivamente la aplicación, colocando controles en el formulario, definiendo sus propiedades y desarrollando funciones para gestionar los eventos.

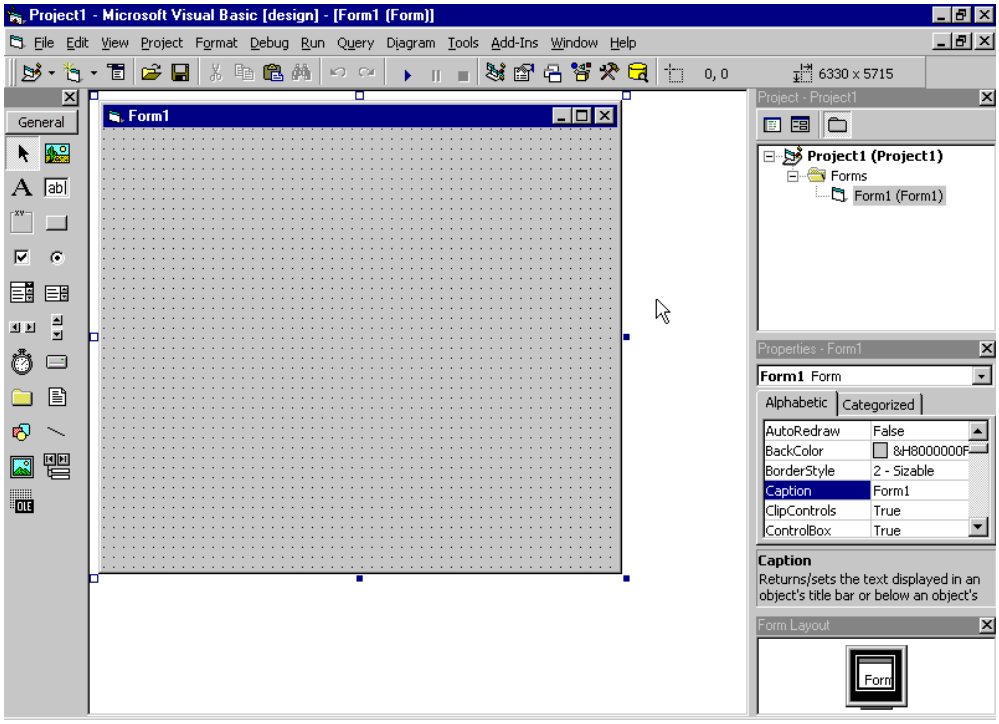


Fig. 2.19: Entorno de programación en Microsoft Visual Basic 6.0.

La aplicación se prueba en modo de ejecución. En ese caso el usuario actúa sobre el programa (introduce eventos) y prueba cómo responde el programa hay algunas propiedades de los controles que deben establecerse en modo de diseño, pero muchas otras pueden cambiarse en tiempo de ejecución desde el programa escrito en Visual Basic 6.0, también hay propiedades que sólo pueden establecerse en modo de ejecución y que no son visibles en modo de diseño. En la figura 2.19 se muestra el entorno de programación en Visual Basic 6.0.

Para la realización de esta interfaz, debemos tener muy claro qué es, en qué consiste y cómo se realiza la programación orientada a objetos (POO)

2.8.2 Programación Orientada a Objetos[21]

La programación orientada a objetos (POO) es una forma de programación que utiliza objetos, ligados mediante mensajes, para la solución de problemas. Puede

[21] Ing. Raymond Marquina

considerarse como una extensión natural de la programación estructurada en un intento de potenciar los conceptos de modularidad y reutilización de código.

2.8.3. Mecanismos Básicos de la POO

Los mecanismos básicos de la programación orientada a objetos (POO) son: Objetos, Mensajes, Métodos, Propiedades y Eventos.

- **Objetos**

Un programa tradicional se compone de procedimientos y de datos. Un programa orientado a objetos se compone solamente de objetos.

Un objeto es una encapsulación genérica de datos y de los procedimientos para manipularlos. Dicho de otra forma, un objeto es una entidad que tiene unos atributos particulares, las propiedades y unas formas de operar sobre ellas, los métodos. Por lo tanto, un objeto contiene, por una parte, operaciones que definen su comportamiento, y por otra, variables manipuladas por esas operaciones que definen su estado.

- **Mensajes**

Cuando se ejecuta un programa orientado a objetos, los objetos están recibiendo, interpretando y respondiendo a mensajes de otros objetos. Esto marca una clara diferencia con respecto a los elementos de datos pasivos de los sistemas tradicionales. Por ejemplo, en Visual Basic un mensaje está asociado con un procedimiento, de tal forma que cuando un objeto recibe un mensaje la respuesta a ese mensaje es ejecutar el procedimiento asociado. Este procedimiento recibe el nombre de método.

- **Métodos**

Un método se implementa en una clase de objetos y determina como tiene que actuar el objeto cuando recibe un mensaje. En adición, las propiedades permitirán almacenar información para dicho objeto. Un método puede también enviar mensajes a otros objetos solicitando una acción o información.

- **Propiedades**

Las propiedades de un objeto definen la manera en que dicho objeto se ve y se comporta.

- **Eventos**

Visual Basic es un lenguaje de programación controlado por eventos. Esto significa que el código se ejecutará en respuesta a algo que ocurre. Por ejemplo, si se hace clic en un botón durante la ejecución del programa, se generará un evento clic y se ejecutará automáticamente el código que le corresponde.

En la figura 2.20 se muestra la pantalla inicial diseñada para el manejo de datos del microcontrolador desde el computador por medio de Visual Basic 6.0.

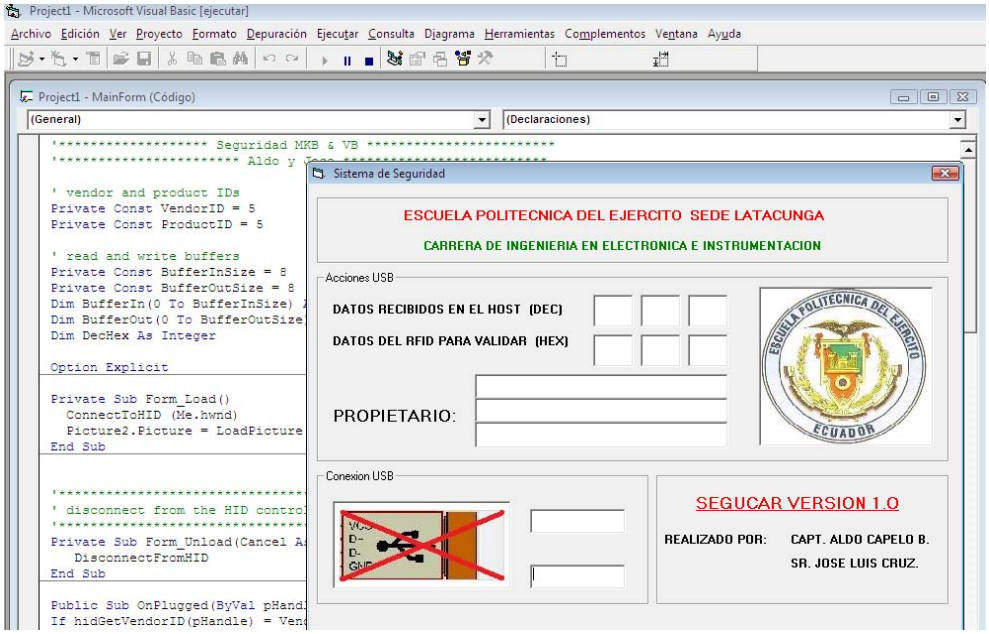


Fig. 2.20: Diseño de la interfaz (HMI) en VB6.

2.8.4 Comunicación de datos en Visual Basic

La comunicación de los datos que llegan desde el microcontrolador, se la configura en VB6, tomando en cuenta que el VID y el PID (ver figura 2.21) del descriptor de MikroBasic sea exactamente igual al que se programa en la parte visual.

Para la programación se considera que los datos que llegan desde el microcontrolador a través del USB deben leerse un índice arriba del dato original, ya que el VIP&PID, entre otras cosas son, enviados de manera automática y se leen en el buffer[0] del PIC o de VB6.

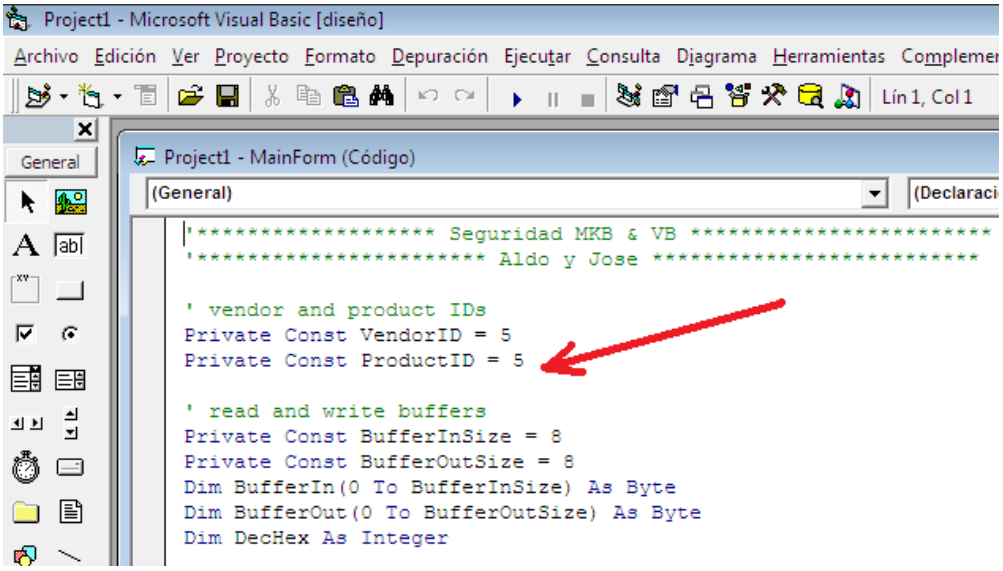


Fig. 2.21: Configuración de VB6 para la comunicación USB.

Una vez que se configura la recepción de los datos que vienen del microcontrolador, se realiza el formulario respectivo para el HMI, el mismo que permitirá leer los datos que llegan desde el dispositivo RFID y otras opciones más que se detallan a continuación:

- Datos recibidos en el host del PC: Son los datos que llegaron desde el microcontrolador, estos se encuentran en forma decimal, ya que VB6 los presenta en ese formato, estos datos no son conocidos debido a que toda la información que se maneja hasta el momento está en formato hexadecimal, para esto se realiza un algoritmo que permita leerlo en formato hexadecimal.

- Datos en hexadecimal: Son los datos que permiten una comparación con los datos que envía el dispositivo RFID, de tal manera que se pueda validar estos datos y verificar el usuario del vehículo.

- Propietario: Persona que está al momento validado para el uso del auto.

- Conexión o desconexión del dispositivo de seguridad vía USB.

En las figuras 2.22 y 2.23 se muestra la pantalla inicial diseñada para la comunicación USB entre el PIC18F2550, en estado de desconexión y conexión respectivamente.

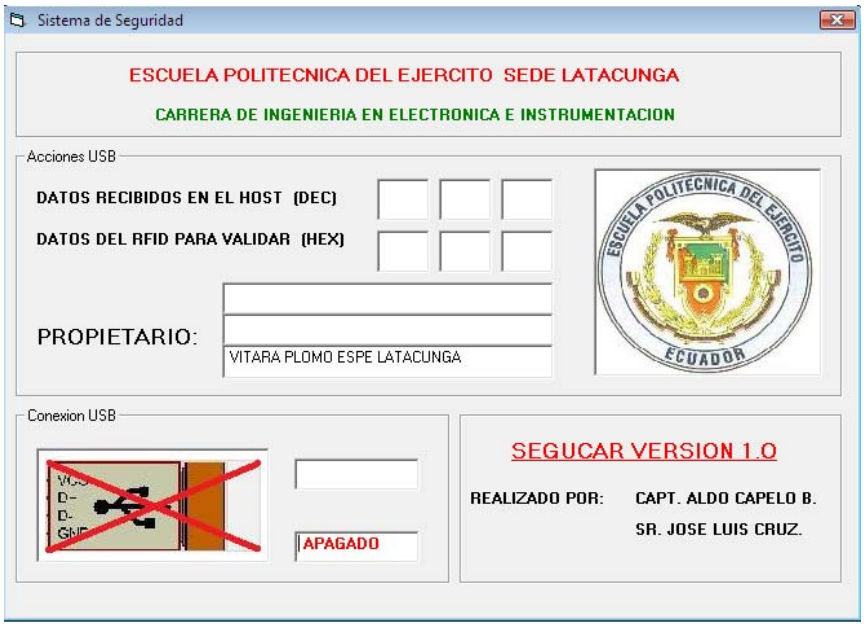


Fig. 2.22: Interfaz Gráfica Terminada (HMI) del sistema apagado.

Fig. 2.23: Interfaz Gráfica Terminada (HMI) del sistema encendido.

CAPÍTULO III

RESULTADOS Y PRUEBAS EXPERIMENTALES

3.1 DESCRIPCIÓN FÍSICA DEL SISTEMA

Al sistema de seguridad, una vez diseñado y montado en su totalidad en un protoboard, se procede a colocarlo en el vehículo (ver figura 3.1) para hacer las pruebas respectivas.

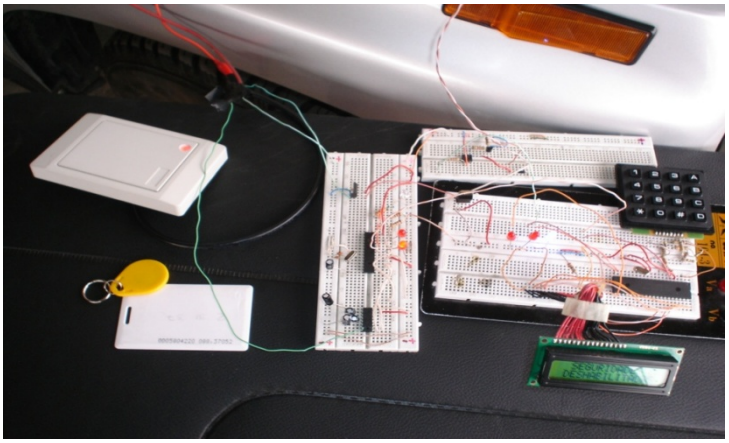


Fig. 3.1: Conexión del dispositivo antes del ingreso al sistema de inyección.

Luego de verificar voltajes y corrientes se acopla el sistema a uno de emulación[22] de inyección, el mismo que se realizó como se puede observar en la figura 3.2.

[22] Emular.- Simular una señal que no existe.

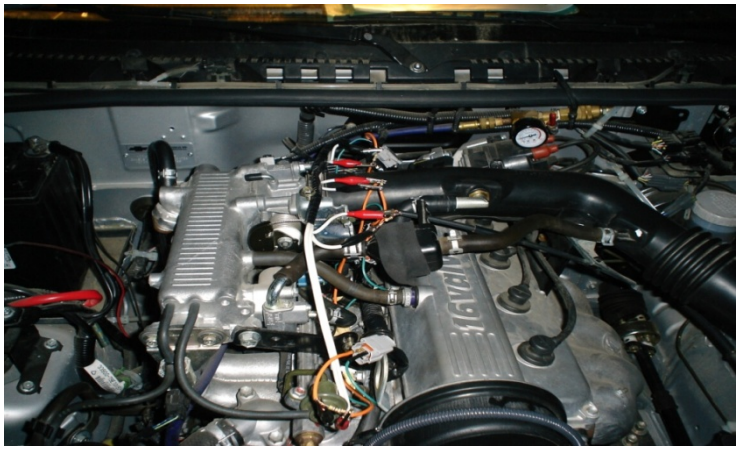


Fig. 3.2: Conexión del dispositivo con el sistema de inyección.

En forma general se puede indicar que al emular un inyector, lo que se consigue es hacer creer a la computadora del auto que existe señal de encendido, pero que en la realidad no es así, para esto lo único que se está haciendo es colocar una resistencia de 47 ohmios en serie con la entrada del inyector como se puede observar en la figura 3.3.

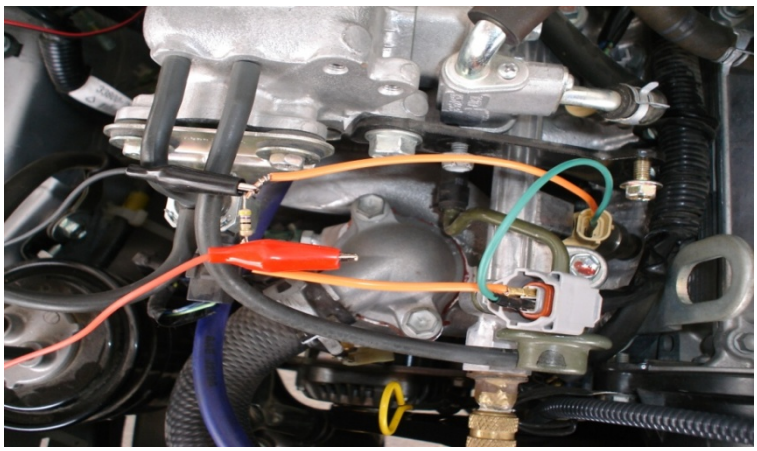


Fig. 3.3: Emulador instalado en el sistema de inyección.

Todo este sistema de emulación es controlado por un relay de varios contactos, el mismo que permite activarse o desactivarse con la señal enviada del sistema de seguridad en el caso que haya ingresado la clave correcta. La figura 3.4 muestra

el relay conectado entre el sistema de seguridad y el sistema de inyección del vehículo.

Fig. 3.4: Relay de control entre el sistema de seguridad y el sistema de inyección del auto.

Una vez probada la emulación y el bloqueo del sistema de seguridad de acuerdo a lo planificado, se instaló el sistema de seguridad en el interior del vehículo, haciendo uso de los voltajes propios del auto, en la figura 3.5 se observa que el sistema ya se encuentra activando las seguridades respectivas y los motores de la puertas sin ningún problema.

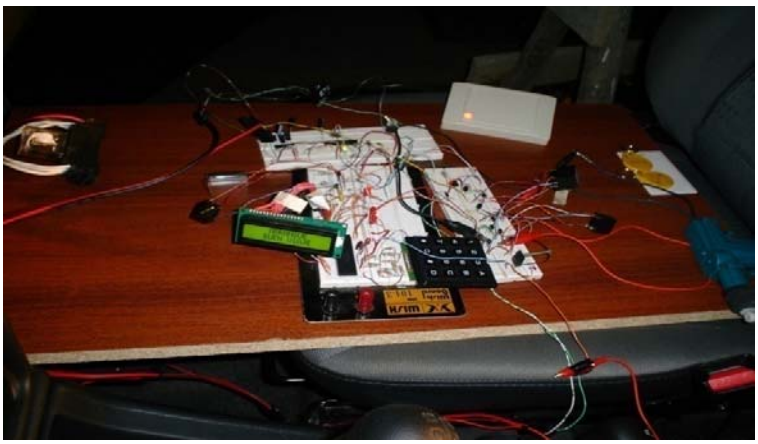


Fig. 3.5: Prueba de todo el sistema instalado en el interior del auto.

Finalizadas las pruebas en el protoboard, se realizó el diseño en una placa de baquelita, ésta se elaboró con la ayuda del software ALTIUM DESIGNER SUMMER 09, obteniendo como resultado el esquema que se muestra en las figuras 3.6 y 3.7.

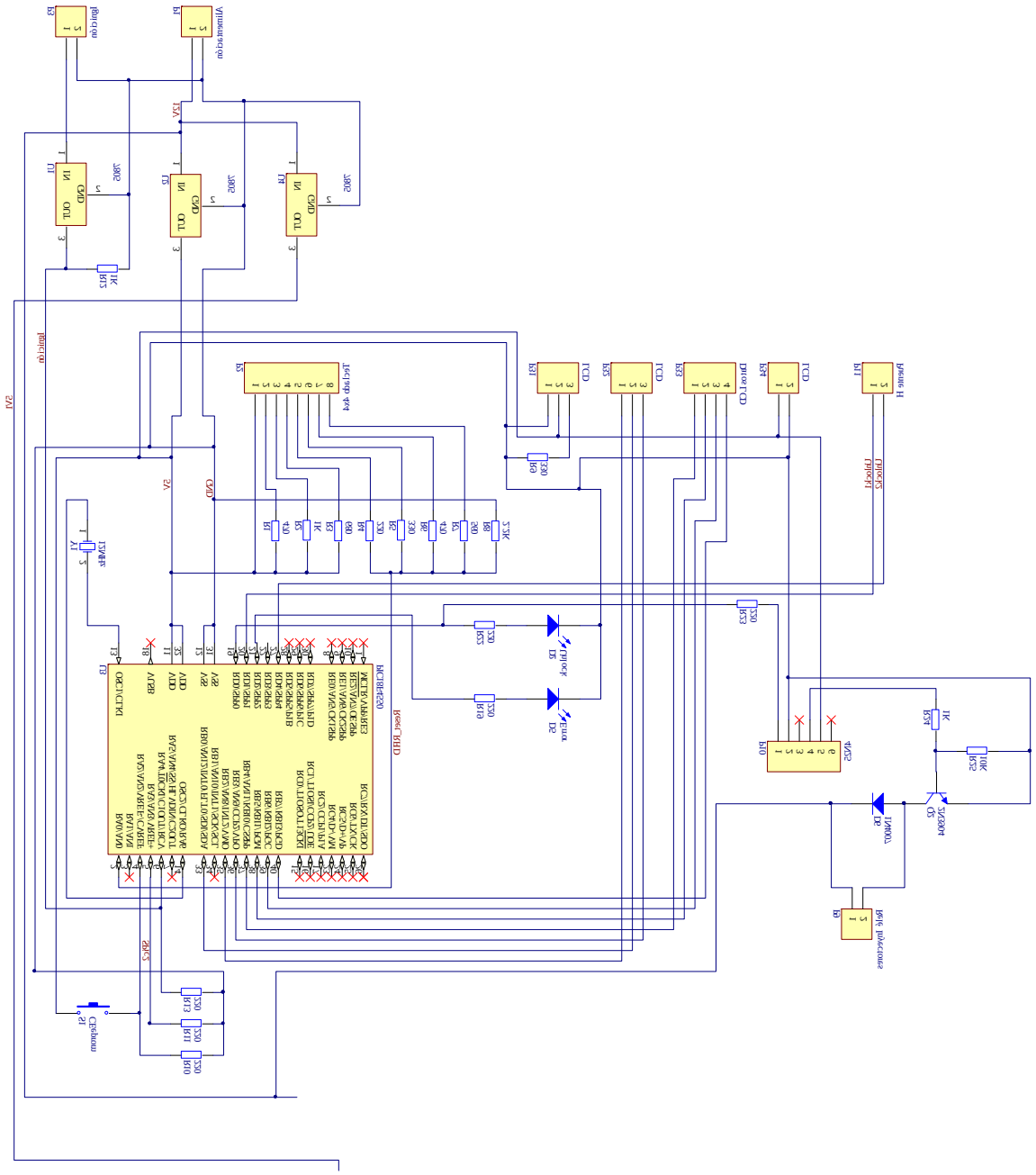


Fig. 3.6: Diseño de la primera parte del sistema realizado en ALTIUM DESIGNER SUMMER 09.

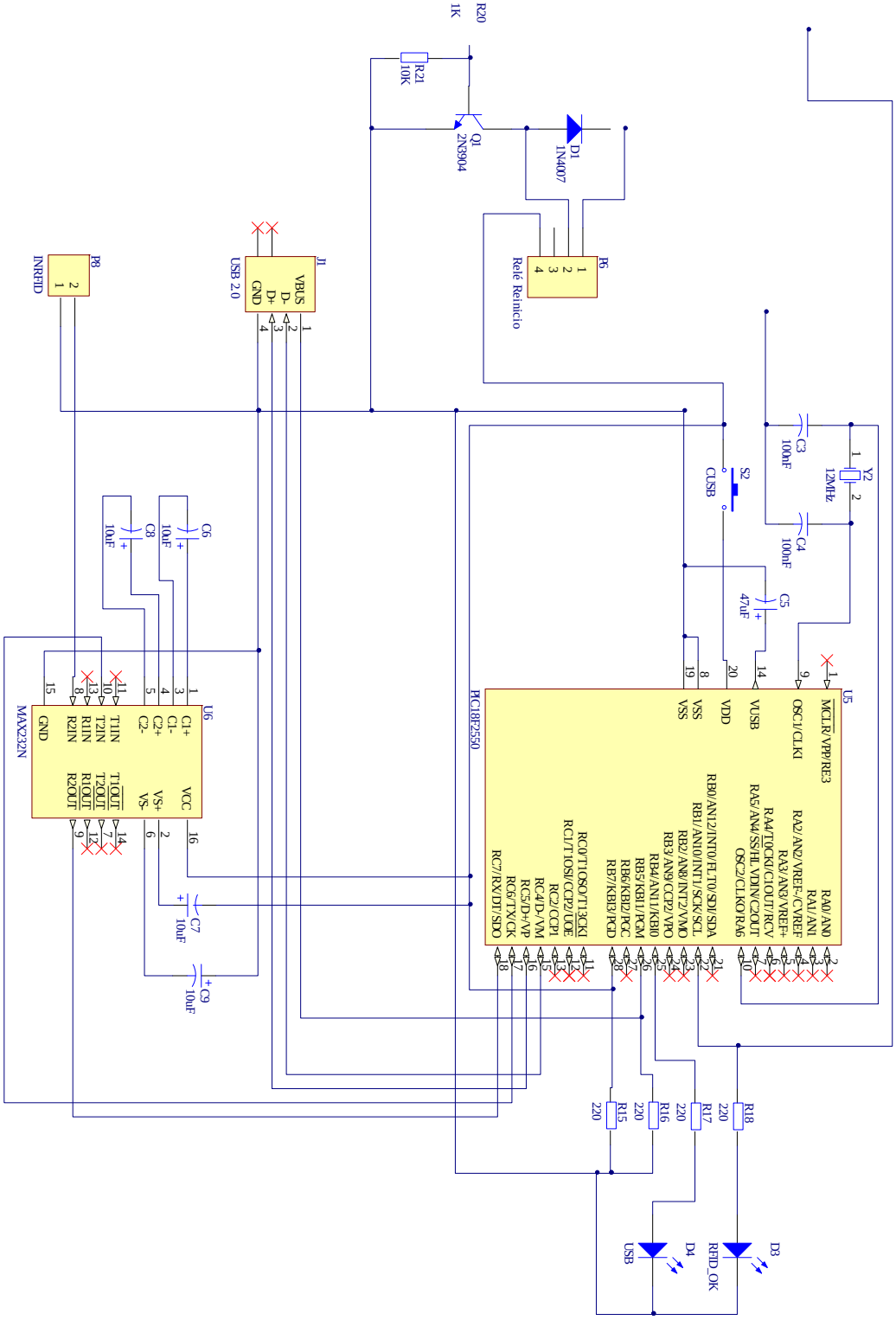


Fig. 3.7: Diseño de la segunda parte del sistema realizado en ALTIUM DESIGNER SUMMER 09.

Después de la compilación del diseño, se obtiene el archivo de la placa a realizarse, el mismo que se cargó en la máquina LPKF[23] ProtoMat S43. En las figuras 3.8 y 3.9 se muestran la placa, terminada y lista para ser enviada a la máquina LPKF y la segunda es una gráfica de la simulación 3D de la placa terminada cuando sale de la misma respectivamente.

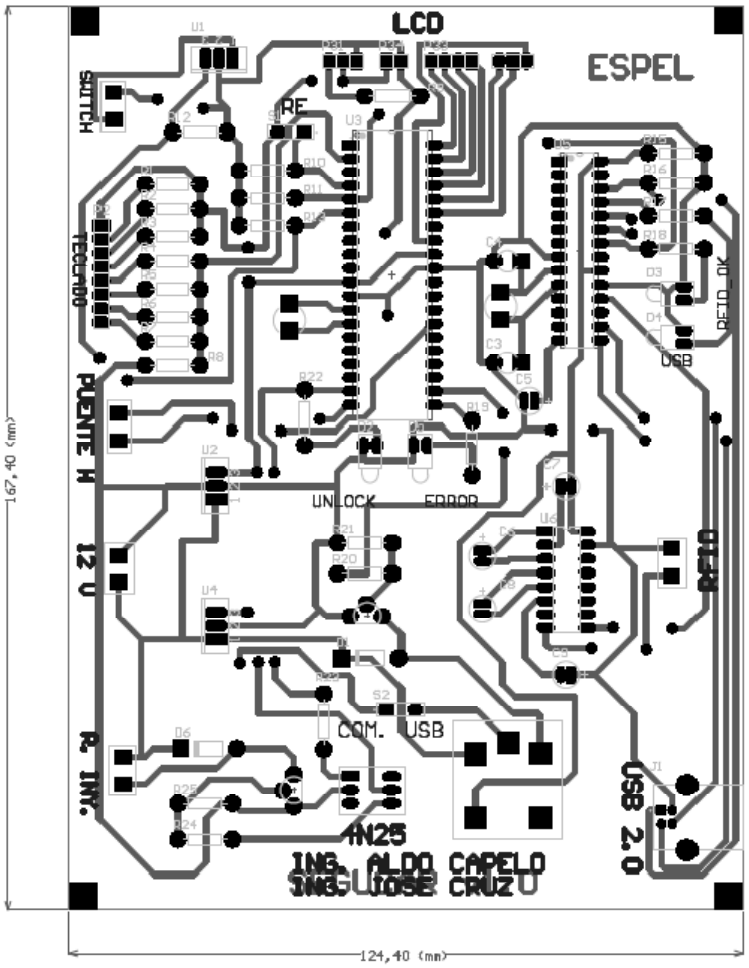


Fig. 3.8: Placa realizada en ALTIUM DESIGNER SUMMER 09.

[23] LPKF: Siglas de la empresa alemana que distribuye la máquina ProtoMat S43que significan "Leiterplatten Kopier Fräsen que traducidas al inglés significan "Circuit Board Copy Milling".

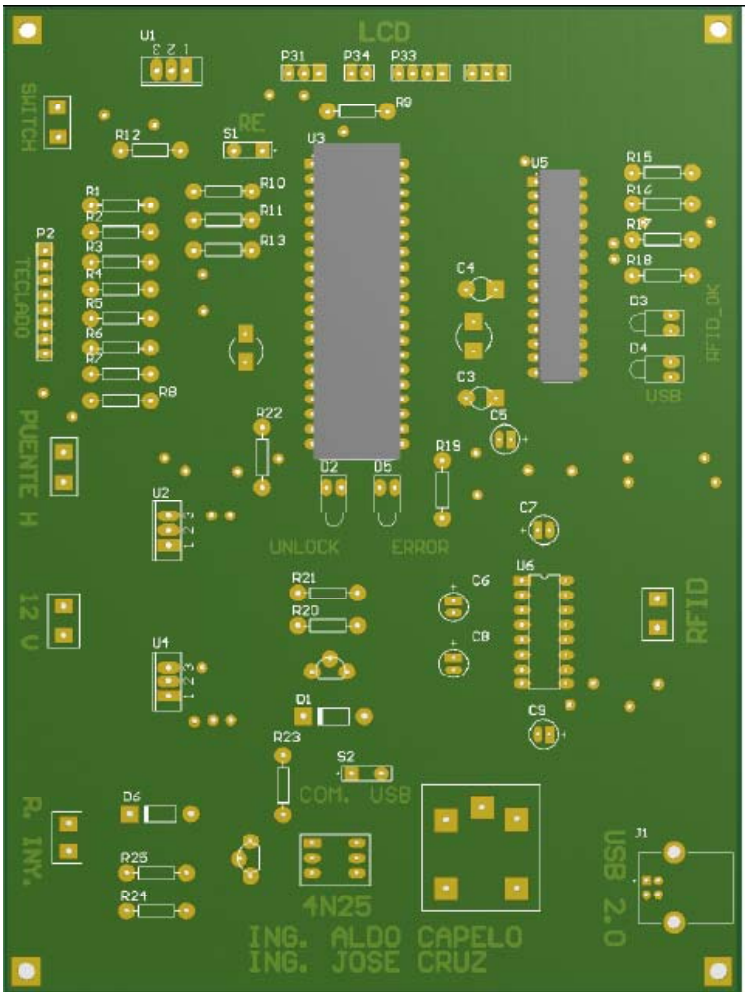


Fig. 3.9: Simulación 3D de la placa terminada.

Después de cargar el archivo en la máquina LPKF y luego de seguir el procedimiento establecido por el fabricante de la misma, se obtuvo un producto de excelentes características, esto se puede observar en las figuras 3.10 y 311 que muestran el reverso y anverso de la placa terminada respectivamente.

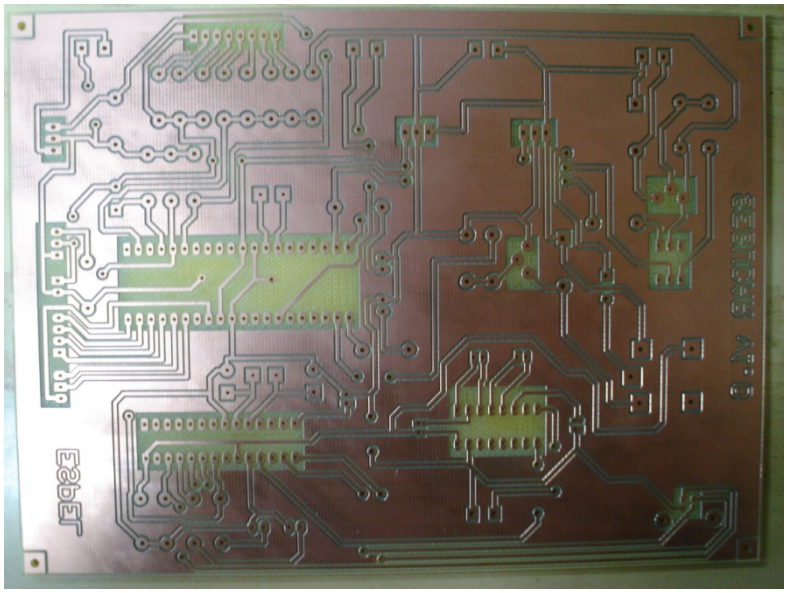


Fig. 3.10: Reverso de la placa realizada en la máquina LPKF.

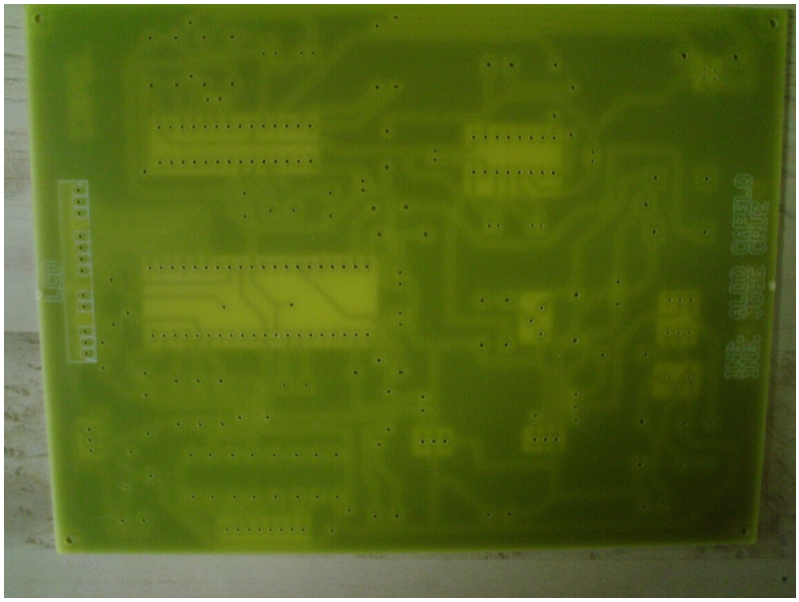


Fig. 3.11: Anverso de la placa realizada en la máquina LPKF.

Una vez terminada la placa, se procede al montaje del dispositivo de seguridad en el auto. Debe tomarse en cuenta que para la activación de los seguros de las puertas, se diseñó un puente H, debido a que el consumo de corriente se incrementa notablemente cuando se acciona el motor lo que provoca que el

sistema se resetee constantemente. El esquema del puente H se muestra en la figura 3.12.

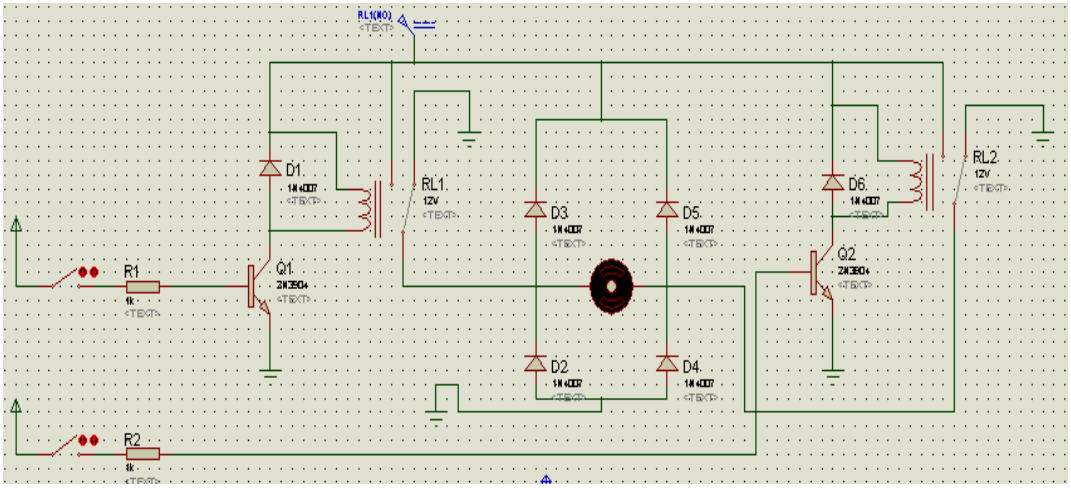


Fig. 3.12: Diagrama del puente H.

3.2 ANÁLISIS DE RESULTADOS Y PRUEBAS EXPERIMENTALES

En la tabla 3.1 se muestra en forma real, los consumos respectivos luego de que el sistema se lo dejo instalado y funcionando por varios días en el interior del auto, estos consumos se los ha medido periódicamente, considerando que este sistema dispone de tres reguladores de voltaje que todo el tiempo se encuentran polarizados y tienden a calentarse, razón por la que es necesario colocarles disipadores de temperatura en cada uno.

Tabla. 3.1: Cuadro de consumo de corriente y voltajes.

EVENTO Y/O DISPOSITIVO	CONSUMO DE CORRIENTE	CONSUMO DE VOLTAJE
RFID	Menor a 500 mA	12 Vcd
MOTOR DE PUERTA	3,6 A	+ 12 y -12 Vcd
OPERACIÓN NORMAL DEL SISTEMA	490 mA	12 Vcd

Se realizaron pruebas de funcionamiento, a temperaturas ambiente altas y bajas, obteniendo los mismos resultados en los dos casos. En la figura 3.13 se muestra una prueba realizada por la noche.

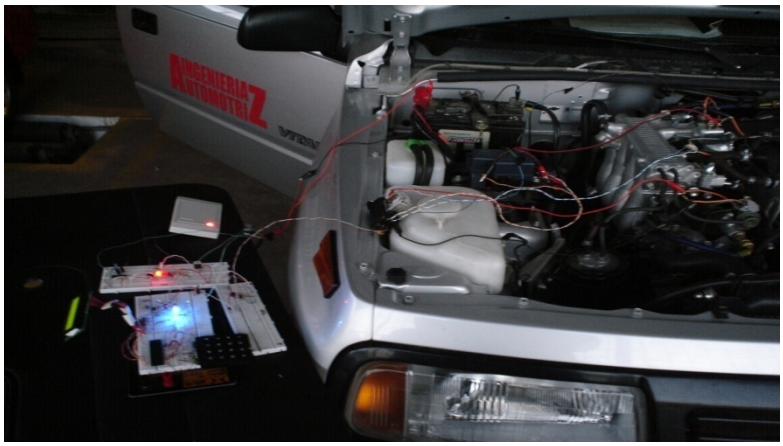


Fig. 3.13: Prueba nocturna del sistema.

Se monitoreo constantemente la comunicación de datos entre el PC y el sistema, fluían adecuadamente sin existir ningún problema al momento de la ejecución y

funcionamiento de la interfase entre la PC (HMI) y el sistema (micro). En la figura 3.14 se muestra la prueba de la interfase del PC con el sistema conectado al vehículo.

Fig. 3.14: Prueba de la interface (HMI) realizada VB6.

3.3 ANÁLISIS TÉCNICO ECONÓMICO

A continuación se listan los materiales y los costos de los mismos.

Tabla 3.2: Costo del sistema

ORD	CANTIDAD	DESCRIPCION	OPCION 1	OPCION 2
1	1	Sistema de fabrica listo para instalación Ej: Chevistar	0	1120
2	1	PIC18F2550	11	
3	1	PIC18F4550	13	
4	4	Relays	4	

5	1	MAX 232	2	
6	1	Placa Baquelita	8	
7	50	Resistencias	2	
8	1	Teclado	5	
9	1	LCD	12	
10	1	Rfid	80	
11	1	Relay industrial	4	
12	6	Borneras	5	
13	4	Socalos	8	
14	10	Mts de cable 18	8	
15	4	Type	4	
16	3	Tags	9	
17	2	Motor de 12Vcd	80	
18	15	Diodos	3	
19	25	Terminales	5	
20	10	Lagartos	4	
21	10	Trs. 2N3904	5	
22	1	Varios e instalación	200	
	TOTAL		472	1120

De acuerdo a los datos de la tabla 3.2 se puede afirmar que, es muy aceptable realizar la inversión en este sistema de seguridad, ya que es más económico que los existentes en el mercado de similares características.

3.4 ALCANCES Y LIMITACIONES

Alcances

- Se obtiene un mayor control, seguridad y fiabilidad de las personas que van hacer uso del vehículo.

- El dispositivo RFID es inviolable y único, brindando así una mayor seguridad al propietario, cuando este abandone su vehículo en lugares peligrosos.

- Permite llevar el registro en computadora de los diversos usuarios que tienen acceso al vehículo o que han sido ya descartados para su uso.

- Con toda la información, se puede crear una base de datos, guardar los datos y después de un determinado tiempo vaciarla.

- Se puede sacar reportes de cada usuario.

Limitaciones

- En el caso que se produzca un incendio o cortos en el sistema del auto, hay la posibilidad de que se queme el RFID o algún microcontrolador interno del sistema y de esta manera no tener el acceso al vehículo.

- Como es un sistema de última generación, posiblemente al inicio de su uso, el propietario va a tener unas pequeñas complicaciones hasta entender bien su correcto funcionamiento.

- Se debe tener mucho cuidado en el manejo y cambio de las claves por parte del propietario porque el momento que se olvide la clave de desbloqueo no podrá tener acceso de ninguna manera a su vehículo.

CAPÍTULO IV

CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

- Se diseñó, elaboró e instaló, un sistema de seguridad vehicular no convencional, basado en tecnología de última generación, mediante dispositivos de seguridad con un dispositivo de RFID y claves de acceso codificadas.

- Este sistema persigue una alternativa de solución en base al avance tecnológico y electrónico actual, para de esta manera satisfacer las necesidades que tienen los propietarios en relación a la seguridad de su vehículo.

- La principal ventaja del sistema radica en que si el relé que cortocircuita las resistencias de los inyectores no recibe la señal del microcontrolador, el vehículo no se encenderá, así que si alguna persona desea sustraerse el vehículo y desconecta el sistema no podrá efectuar el robo.

- El dispositivo RFID es inviolable y único, logrando así una mayor seguridad al propietario cuando éste abandone su vehículo en lugares peligrosos, o a su vez cuando se cambie de conductores constantemente.

- Los microcontroladores PIC18F2550 y PIC18F4550, elegidos para desarrollar este proyecto, cumplieron eficientemente su papel, ya que una de las virtudes

de estos es que otorgan respuesta en tiempo real en las aplicaciones en las que se los usa.

- Sólo el usuario conoce la secuencia y cómo codificar las claves de acceso para el encendido del auto.

- Se utilizó un sistema de seguridad aplicado al sistema de inyección del automóvil, basado en el principio de emular señales.

- El sistema desarrollado constituye una posible solución para resolver los varios inconvenientes que se tiene con las alarmas convencionales que hoy en día son tan vulnerables, de esta manera brindar mayor seguridad al parque automotor.

- Los dispositivos RFID tienen como desventaja su limitación de lectura en líquidos o metales.

- Hoy en día el uso de dispositivos RFID, ha crecido notablemente gracias a que se incrementa la eficiencia de sus operaciones en diversas aplicaciones y esto implica una reducción de costos.

- Mientras el transponder se encuentra en el proceso de carga no emite su código, y sólo empieza a emitirlo cuando desaparece el campo de la carga que se generó anteriormente.

- Existen actualmente diversos fabricantes de dispositivos RFID y se están comenzando a desarrollar aplicaciones empaquetadas a pedido o necesidad del cliente.

- Posiblemente en un corto plazo la identificación por radiofrecuencia se adopte de forma generalizada, lo que implicaría mejores precios y se facilitará la realización de otros proyectos universitarios.

- Actualmente el uso del RFID es una de las tecnologías más empleadas al hablar de almacenamiento y distribución de información porque ofrece grandes ventajas en comparación con la tecnología que actualmente se usa (código de barras).

- La tecnología RFID puede ser usada en diversos campos como la domótica en conjunto con microcontroladores, para adquirir la información y codificarla de acuerdo a los requerimientos de los clientes.

- Este sistema de acceso no requiere de contacto directo de los tags con el lector, ni tampoco es indispensable que haya línea de vista para la lectura, en nuestro caso los 125 KHz del dispositivo, permiten a los tags ser leídos a una distancia promedio de 8 cm atravesando varios obstáculos.

- El rango de lectura de la trama del lector, se la puede manipular con software para el mejor empleo o uso en las aplicaciones que así lo requieran.

- El software desarrollado, permite el control y cierto nivel de configuración de los accesos y dispositivos lectores utilizados por los propietarios.

- El software que se utilizó para el desarrollo del proyecto de investigación fue PROTEUS 7.4, MikroBasic 7.2, ALTIUM DESIGNER SUMMER 9.0, Visual Basic 6.0, MikroBasic Compiler, los cuales han sido de gran ayuda para el desarrollo de la aplicación.

- Este es un proyecto que podría ser el punto de inicio para otros que quisiera implementarse con este mismo tipo de tecnología ya que propone una alternativa de solución en base al avance tecnológico y electrónico para satisfacer las necesidades que tienen los propietarios en relación a la seguridad de su vehículo.

- Este proyecto puede ser parte complementaria de una empresa que disponga un parque automotor extenso y costoso. Cada vehículo podría estar registrado en una base de datos que contendrá la información básica de cada una de las personas que tienen el derecho de acceso al auto.

- El presente proyecto va dirigido a modernizar y actualizar los conocimientos de los alumnos de la Carrera de Ingeniería Automotriz, permitiendo mejorar el nivel de preparación los alumnos de la ESPEL, debiendo recalcar que un sistema de características similares en el país resultaría muy costoso.

4.2 RECOMENDACIONES

- Analizar el sistema de encendido que dispone el vehículo en la que se va a instalar el dispositivo, porque dependiendo el caso se debe tomar medidas compensatorias para realizar las conexiones en el interior y exterior del auto.

- Disponer de materiales de seguridad industrial a la mano, como extintores y otros, ya que al cortar cables, quitar cables, manejar corrientes altas, se pueden producir chispas que pueden generar algún riesgo de incendio.

- Manipular con cuidado el cableado que va hacia la placa principal, ya que con movimientos bruscos estos se pueden romper con facilidad.

- Elegir un lugar adecuado y fijo para la colocación del cerebro del sistema para evitar los problemas de desconexiones de cables o rupturas.
- Colocar unos disipadores en los reguladores de voltaje, para mantener a la placa a una temperatura adecuada y evitar cortos en los componentes.

- Ubicar en lugares estratégicos el sensor RFID y el cerebro del sistema, para de esta manera brindar protección y confort al conductor.

- Debemos colocar en el sistema una alimentación directa de la batería ya que al tener derivaciones dentro del sistema a otros componentes electrónicos del vehículo va a provocar fallos o mal funcionamiento del mismo.

- Se recomienda para el futuro, acondicionar las diferentes señales eléctricas ya que si no se pasa por este proceso, tanto los equipos RFID y la PC sufrirían daños, al no ser alimentadas con el voltaje requerido por estos elementos.

- Al colocar el sensor RFID tener mucha precaución al manipularlo y al conectarlo, no estar golpeándolo ya que se puede dañar con facilidad.

- Para un funcionamiento óptimo del sistema es recomendable que las puertas del vehículo permanezcan bien cerradas.

- Colocar al cerebro del sistema en un lugar libre de humedad ya que contiene elementos electrónicos y estos a la larga pueden ser averiados.

- La pantalla LCD es una guía en la cual se guía el proceso de encendido.

- RFID se debe colocar en un lugar estratégico que sólo el conductor conozca, así se elevará la seguridad del auto.

- Para iniciar con el funcionamiento del módulo, es necesario conectar el cable de datos, la fuente y por último la señal de ignición del auto.

- Para este tipo de aplicaciones el uso de microcontroladores de la Microchip es adecuado, ya que de ellos existe bastante información.

- Se recomienda el uso de herramientas de investigación que se encuentran en internet, foros, libros digitales y datasheets, ya que en ellos se puede encontrar información importante y confiable, de forma rápida y económica.

4.3 BIBLIOGRAFÍA Y ENLACES

- R. Weinstein, RFID: a technical overview and its application to the enterprise,& Professional,Volumen 7(3): 27-33, Junio 2005.

- SHIGLEY Joseph. GUALDA J.A., MARTINEZ S., MARTINEZ P.M., “Electrónica industrial: Técnicas de potencia”, Segunda edición, Editorial Marcombo, S.A., Barcelona, 1992.

- http://www.epc.org.mx/view.php?id=1

- http://www.maestrosdelweb.com/principiantes/%C2%BFque-son-las-bases-de-datos/

- GROOVER, Mikell. Robótica Industrial, Tecnología, programación y aplicaciones, México: McGRAW.HILL, 1994, p. 72 – 75.

- CEAC, Manual Del Automóvil, edición MMVI, editorial Cultural S.A., Madrid España.

- BARREIROS, Antonio. Fundamentos de Robótica, Madrid: Concepción Fernández Madrid, 1997, p. 26 -29, 37.

- www.emmicroelectronic.com

- Serrano, J., “Manual de Introducción a Microsoft Visual Basic 2005 Express Edition”, ANAYA MULTIMEDIA, Madrid, 2006.

- V. Daniel Hunt, Albert Puglia, RFID A guide to radio frequency identification. Ed. Wiley 2007

- Tom Miller, RFID Insider, January 05, 2006 - RFID Connections

- Tiznado, Best Seller, Visual Basic 6.0

- Hunt, Daniel, RFID guide to radio frequency identification: 23 - 34, Editorial Wiley.

- Weinstein, R., RFID: a . overview and its application to the enterprise: 27- 33.

- Bhuptani, Manish, RFID Field Guide: Deploying Radio: 45 - 63, Prentice Hall.

- Angulo, José, Microcontroladores PIC: 88 - 123, México: Edigrafos.

- REYES, Carlos, "Aprenda a Programar Microcontroladores PIC": 34 - 69, Ecuador.

- http://es.wikipedia.org/wiki/RFID

- http://www.ti.com/tiris/default.htm

- BATURONE, Anibal. Robótica, Manipuladores y robots móviles, Barcelona: Alfaomega, 2007, p. 5, 178.

- TORRES, F.; POMARES, J.; GIL, P.; PUENTE, S. T., y ARACIL, R. Robots y Sistemas Sensoriales, Madrid: Pearson Educación, 2002, p. 170 – 181.

- BARRIETOS, A.; PEÑIN, L.; BALAGUER, C.; ARACIL, R. España: McGRAWHILL, 2007, p. 151 – 156

- http://www.RFID-handbook.de/links/index.html

- http://www.Mikroelectronica.com.es/

- http://www.capta.com.mx/solucion/ems_rf_id_tags.htm
- http://www.semiconductors.philips.com/products/identification/index.html
- PROTEUS VSM. Ingeniería Eléctrica Electrónica, S.A.
- www.ieeproteus.com

ANEXOS

A. FRAGMENTO DE CÓDIGO: USO DEL ADC EN MIKROBASIC 7.2

```
program adc

DIM TECLA AS WORD

MAIN:

ADCON1 = $0E
TRISA = $03
TRISB = $00
PORTB = $00

WHILE TRUE

   DELAY_MS(100)
   ADC_READ(0) 'Lee del canal AN0 del ADC

   IF (ADRESL AND (ADRESL <> TECLA)) THEN
    'Si no pulsamos o mantenemos pulsado una tecla no hace nada

     IF ((ADRESL > $A0) AND (ADRESL < $A3)) THEN 'Tecla 1
     PORTB.0 = 1
     END IF

     IF ((ADRESL > $00) AND (ADRESL < $0C)) THEN 'Tecla 2
```

```
PORTB.1 = 1
END IF

IF ((ADRESL > $90) AND (ADRESL < $93)) THEN 'Tecla 3
PORTB.2 = 1
END IF

IF ((ADRESL > $78) AND (ADRESL < $7B)) THEN 'Tecla 4
PORTB.3 = 1
END IF

IF ((ADRESL > $EC) AND (ADRESL < $EF)) THEN 'Tecla 5
PORTB.4 = 1
END IF

IF ((ADRESL > $7C) AND (ADRESL < $7F)) THEN 'Tecla 6
PORTB.5 = 1
END IF

IF ((ADRESL > $40) AND (ADRESL < $4C)) THEN 'Tecla 7
PORTB.6 = 1
END IF

IF ((ADRESL > $CB) AND (ADRESL < $CE)) THEN 'Tecla 8
PORTB.7 = 1
END IF

IF ((ADRESL > $63) AND (ADRESL < $66)) THEN 'Tecla 9
PORTB.0 = 0
END IF

IF ((ADRESL > $B7) AND (ADRESL < $BA)) THEN 'Tecla 0
```

```
    PORTB.1 = 0
    END IF

    IF ((ADRESL > $D4) AND (ADRESL < $D7)) THEN 'Tecla A
    PORTB.2 = 0
    END IF

    IF ((ADRESL > $BB) AND (ADRESL < $BE)) THEN 'Tecla B
    PORTB.3 = 0
    END IF

    IF ((ADRESL > $9E) AND (ADRESL < $A1)) THEN 'Tecla C
    PORTB.4 = 0
    END IF

    IF ((ADRESL > $8C) AND (ADRESL < $8F)) THEN 'Tecla D
    PORTB.5 = 0
    END IF

    IF ((ADRESL > $2E) AND (ADRESL < $31)) THEN 'Tecla *
    PORTB.6 = 0
    END IF

    IF ((ADRESL > $55) AND (ADRESL < $58)) THEN 'Tecla #
    PORTB.7 = 0
    END IF

  END IF

TECLA = ADRESL
WEND
END.
```

B. FRAGMENTO DE CÓDIGO: USO DE LA COMUNICACIÓN USART EN MIKROBASIC 7.2

```
program TRAMA_RFID

DIM TRAMA_RFID, ID AS BYTE
DIM TRAMA AS BYTE [15]

main:

trisb = $00
trisc = %11000000
trisd = 0
portb = $00
portd = 0

LCD_INIT(PORTB)
LCD_CMD(LCD_CLEAR)
LCD_CMD(Lcd_Cursor_Off)
DELAY_MS(100)

USART_INIT(9600)

WHILE TRUE

   if ID > 3 then
      ID = 0
   end if

   IF Usart_Data_Ready = 1 THEN

      TRAMA_RFID = Usart_Read
```

```
      TRAMA[ID] = TRAMA_RFID

      ID = ID + 1

      IF ID = 3 THEN
        if (TRAMA[0] = $02) AND (TRAMA[1] = $33) AND (TRAMA[2] = $36) THEN
           portd.3 = 1
          ID = 0
        END IF

        if (TRAMA[0] = $02) AND (TRAMA[1] = $31) AND (TRAMA[2] = $37) THEN
          LCD_OUT(1,1,"OK")
          DELAY_MS(180)
          LCD_CMD(LCD_CLEAR)
          portd.3 = 1
          ID = 0
        END IF

      END IF

    END IF

WEND

END.
```

C. DATASHEET PIC18F4450/PIC18F2550

28/40/44-Pin, High-Performance, Enhanced Flash, USB Microcontrollers with nanoWatt Technology

Universal Serial Bus Features:

- USB V2.0 Compliant
- Low Speed (1.5 Mb/s) and Full Speed (12 Mb/s)
- Supports Control, Interrupt, Isochronous and Bulk Transfers
- Supports up to 32 Endpoints (16 bidirectional)
- 1-Kbyte Dual Access RAM for USB
- On-Chip USB Transceiver with On-Chip Voltage Regulator
- Interface for Off-Chip USB Transceiver
- Streaming Parallel Port (SPP) for USB streaming transfers (40/44-pin devices only)

Power-Managed Modes:

- Run: CPU on, peripherals on
- Idle: CPU off, peripherals on
- Sleep: CPU off, peripherals off
- Idle mode currents down to 5.8 µA typical
- Sleep mode currents down to 0.1 µA typical
- Timer1 Oscillator: 1.1 µA typical, 32 kHz, 2V
- Watchdog Timer: 2.1 µA typical
- Two-Speed Oscillator Start-up

Flexible Oscillator Structure:

- Four Crystal modes, including High Precision PLL for USB
- Two External Clock modes, up to 48 MHz
- Internal Oscillator Block:
  - 8 user-selectable frequencies, from 31 kHz to 8 MHz
  - User-tunable to compensate for frequency drift
- Secondary Oscillator using Timer1 @ 32 kHz
- Dual Oscillator options allow microcontroller and USB module to run at different clock speeds
- Fail-Safe Clock Monitor:
  - Allows for safe shutdown if any clock stops

Peripheral Highlights:

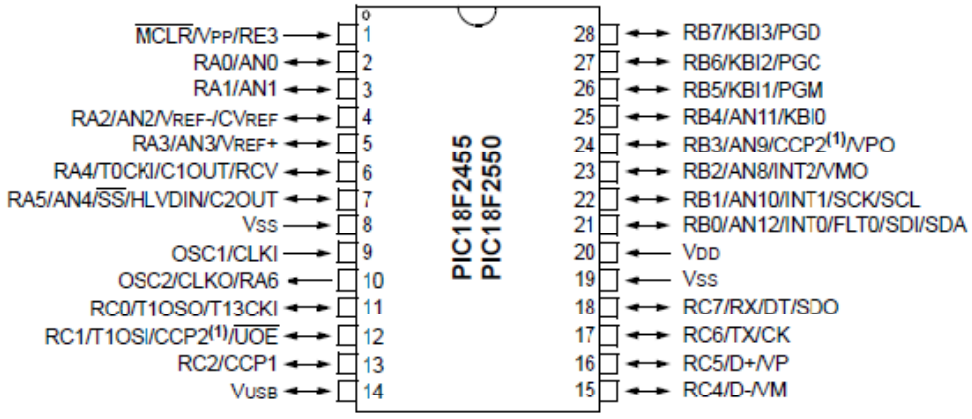
- High-Current Sink/Source: 25 mA/25 mA
- Three External Interrupts
- Four Timer modules (Timer0 to Timer3)
- Up to 2 Capture/Compare/PWM (CCP) modules:
  - Capture is 16-bit, max. resolution 5.2 ns (TCY/16)
  - Compare is 16-bit, max. resolution 83.3 ns (TCY)
  - PWM output: PWM resolution is 1 to 10-bit
- Enhanced Capture/Compare/PWM (ECCP) module:
  - Multiple output modes
  - Selectable polarity
  - Programmable dead time
  - Auto-shutdown and auto-restart
- Enhanced USART module:
  - LIN bus support
- Master Synchronous Serial Port (MSSP) module supporting 3-wire SPI (all 4 modes) and I^2C™ Master and Slave modes
- 10-bit, up to 13-channel Analog-to-Digital Converter module (A/D) with Programmable Acquisition Time
- Dual Analog Comparators with Input Multiplexing

Special Microcontroller Features:

- C Compiler Optimized Architecture with optional Extended Instruction Set
- 100,000 Erase/Write Cycle Enhanced Flash Program Memory typical
- 1,000,000 Erase/Write Cycle Data EEPROM Memory typical
- Flash/Data EEPROM Retention: > 40 years
- Self-Programmable under Software Control
- Priority Levels for Interrupts
- 8 x 8 Single-Cycle Hardware Multiplier
- Extended Watchdog Timer (WDT):
  - Programmable period from 41 ms to 131s
- Programmable Code Protection
- Single-Supply 5V In-Circuit Serial Programming™ (ICSP™) via two pins
- In-Circuit Debug (ICD) via two pins
- Optional dedicated ICD/ICSP port (44-pin devices only)
- Wide Operating Voltage Range (2.0V to 5.5V)

Device	Program Memory		Data Memory		I/O	10-Bit A/D (ch)	CCP/ECCP (PWM)	SPP	MSSP		EAUSART	Comparators	Timers 8/16-Bit
	Flash (bytes)	# Single-Word Instructions	SRAM (bytes)	EEPROM (bytes)					SPI	Master I^2C™			
PIC18F2455	24K	12288	2048	256	24	10	2/0	No	Y	Y	1	2	1/3
PIC18F2550	32K	16384	2048	256	24	10	2/0	No	Y	Y	1	2	1/3
PIC18F4455	24K	12288	2048	256	35	13	1/1	Yes	Y	Y	1	2	1/3
PIC18F4550	32K	16384	2048	256	35	13	1/1	Yes	Y	Y	1	2	1/3

28-Pin PDIP, SOIC



40-Pin PDIP