DISEÑO E IMPLEMENTACIÓN DE UNA HERRAMIENTA PARA EL REGISTRO Y CONTROL DE ACCESO UTILIZANDO TECNOLOGÍA *RFID* Y MÓDULOS BLUETOOTH

NELSON CAMILO HILLERA VEGA
SERGIO ANDRÉS MEZA AGUDELO

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERÍAS FISICOMECÁNICAS
ESCUELA DE INGENIERÍA ELÉCTRICA ELECTRÓNICA Y TELECOMUNICACIONES
BUCARAMANGA
2010

DISEÑO E IMPLEMENTACIÓN DE UNA HERRAMIENTA PARA EL REGISTRO Y CONTROL DE ACCESO UTILIZANDO TECNOLOGÍA *RFID* Y MÓDULOS BLUETOOTH

NELSON CAMILO HILLERA VEGA
SERGIO ANDRÉS MEZA AGUDELO

Trabajo de Grado presentado como requisito para optar el título de Ingeniero Electrónico

Director
Msc. JORGE HERNANDO RAMÓN SUÁREZ

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERÍAS FISICOMECÁNICAS
ESCUELA DE INGENIERÍA ELÉCTRICA ELECTRÓNICA Y TELECOMUNICACIONES
BUCARAMANGA
2010

DEDICATORIA

A Dios Todo Poderoso y misericordioso que siempre me dio fuerza y voluntad para seguir adelante.

A María Madre Santísima que me cubrió con su manto y no permitió que nada malo me sucediera.

A mi madre linda Amparo que siempre camino conmigo, me dio todo su amor, compresión y ánimo para seguir.

A mi padre Belisario quien con su ejemplo, humildad y serenidad me mostró el camino correcto y me enseñó que los sueños se logran con sacrificio esfuerzo y dedicación.

A mi hermano que siempre me dio su fuerza y me acompañó en los momentos más difíciles.
A mi abuela, mi segunda madre, por sus oraciones.
A toda mi familia, especialmente a mis primos Hernando y Leonardo que siempre me acompañaron y me dieron todo su apoyo.

A mis compañeros del Grupo ERA que siempre estuvieron presentes en mi formación como profesional.

A todas aquellas personas que de una u otra forma estuvieron a mi lado y con quienes compartí momentos que me ayudaron y me enseñaron a salir adelante.

Sergio Andrés

AGRADECIMIENTOS

Los autores expresan sus agradecimientos a

Todas las personas que contribuyeron en el desarrollo de este trabajo.

En especial al Director Jorge Hernando Ramón Suárez, Director del proyecto, por sus consejos y asesorías durante la ejecución y realización del proyecto.

Nuestras familias y amigos por el apoyo incondicional, por las palabras de ánimo, y por su comprensión en el desarrollo del proyecto.

Al Ingeniero León Valderrama por su orientación en el inicio del proyecto.

Al Grupo *ERA* y a todos sus miembros, especialmente a su coordinador Raúl Hernando Cadena por su apoyo y enseñanzas.

A la Escuela de Ingeniería Eléctrica Electrónica y Telecomunicaciones y la Universidad Industrial de Santander por acogernos durante este tiempo y darnos la oportunidad de formarnos Profesionalmente.

CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

LISTA DE ANEXOS

GLOSARIO

BLUETOOTH: nombre dado a la comunicación entre dos más dispositivos de manera inalámbrica según IEEE 802.15.1

CODIGO DE USUARIO: código de 16 Bits que hacen parte del código identificación dentro del Tag

ESCATTERNET: grupo de Piconets

NETBEANS: nombre del programa para desarrollar la aplicación de software.

PICONET: dos o más unidades Bluetooth que comparte el mismo canal

RADIO FRECUENCIA: principio en el cual se basa la tecnología RFID y medio por el cual realiza la identificación.

TAG: dispositivo usado como llave para acceder a determinado espacio. Está dotada con una antena y un microchip en el cual se almacena el código de identificación.

WIEGAND: protocolo de comunicación propio de los sistemas RFID

RESUMEN

TÍTULO: DISEÑO E IMPLEMENTACIÓN DE UNA HERRAMIENTA PARA EL REGISTRO Y CONTROL DE ACCESO USANDO TECNOLOGÍA *RFID* Y MÓDULOS BLUETOOTH.[*]

AUTORES: HILLERA VEGA, Nelson Camilo y MEZA AGUDELO, Sergio Andrés[**]

PALABRAS CLAVES: *RFID, TAG, BLUETOOTH, READER*

DESCRIPCIÓN

El siguiente documento presenta el diseño e implementación de una herramienta de hardware y software basada en tecnología *RFID* y módulos Bluetooth, que permite el control de acceso a un recinto. El diseño de esta herramienta está orientado a la seguridad y control de usuarios vinculados a un lugar determinado, registrando la entrada y salida en el sitio de instalación, evitando así que personas no autorizadas tenga acceso a él.

En materia de seguridad, los dispositivos funcionales bajo la tecnología *RFID* en aplicaciones de identificación y acceso, garantizan que el usuario portador del *Tag* (llave), sea identificado y se le conceda la petición de acceso. *RFID* es una tecnología que presenta la facilidad de tener *Tags* con diferentes números de identificación, los cuales no todos están vinculados y autorizados, lo que permite mantener un control salvaguardando sus intereses personales.

La implementación del hardware es necesaria para la funcionalidad de esta tecnología, ya que es la encargada de hacer la debida interpretación de la información de los Lectores *RFID,* permitiendo hacer un tratamiento con estos para la aplicación que se desee.

El diseño del software en esta herramienta es la parte complementaria y más importante ya que por medio de este se identifican, registran y se les concede el acceso a los usuarios habilitados previamente por el administrador del sistema. Todo este conjunto de aplicaciones forma una herramienta confiable para mantener segura un área de interés, teniendo un debido control de usuarios y restringiendo el acceso a personal no autorizando. Adicionalmente a esta herramienta se le implementa un sistema de comunicación inalámbrico usando tecnología Bluetooth que permite confiabilidad en la transmisión y facilidad de instalación.

---

[*] Proyecto de Grado

[**] Facultad de Ingenierías Fisicomecánicas, Escuela de Ingeniería Eléctrica Electrónica y Telecomunicaciones, Director Msc. Jorge Hernando Ramón Suárez

SUMMARY

TITLE: DESIGN AND IMPLEMENTATION OF A TOOL TO REGISTER AND ACCES CONTROL, USING RFIDTECHNOLOGY AND BLUETOOTH MODULES.[*]

AUTHORS: HILLERA VEGA, Nelson Camilo y MEZA AGUDELO, Sergio Andrés.[**]

KEYWORDS: *RFID, TAG, BLUETOOTH, READER*

DESCRIPTION

The following document presents the design and implementation of hardware and software tool based on RFID technology and Bluetooth a module that allows access control to precincts. The design of this tool aims at security and control of users linked to a particular site, recording to the entry and exit in the installation place, preventing unauthorized access users to it.

In terms of security, functional devices in applications under RFID technology in access and identification, ensuring that the user carrier the Tag (key), is identifies and guarantee the access request. RFID is a technology with the ease to have tags with different identification numbers which are not all linked and approved allowing it to maintain control and to safeguard him personal interests.

The hardware implementation is necessary for the functionality of this technology, because it is responsible for making the proper interpretation of information from RFID readers, allowing the treatment with these depending to the application that you want.

The software's design on this tool is the additional and more important part because through this are records, identified and given access to available users previously by the administrator. All of these applications is a reliable tool to keep secure an area of interest by having a proper control and restricting user access to unauthorized personnel. In addition to this tool is a wireless communication implements a system using Bluetooth technology that allows transmission reliability and ease of installation.

---

[*] Negree Project

[**] Engineer's Faculty Physical mechanics, High School Engineer Electric and Electronics and Telecommunications, Director Msc. Jorge Hernando Ramón Suárez

INTRODUCCIÓN

En la actualidad, alrededor de todo el mundo se desarrollan avances tecnológicos en materia de identificación, los cuales pueden ejercer sus funciones de manera fácil, rápida y confiable. *RFID* es una tecnología que presenta una solución para muchos de los problemas que sufren los usuarios, especialmente aquellos que necesitan mantener un registro y una identificación constante sobre algún tipo de unidades, lugares o personal.

Con el paso de los días, la evolución constante de la sociedad y los lugares donde residimos, generan nuevas necesidades que exigen atención y una solución que garantice la integridad de los usuarios, ofreciendo resultados seguros dentro de la aplicación sobre la cual se está ejecutando.

La identificación por radiofrecuencia se ha convertido en la solución preferida por los usuarios para dar solución a la mayoría de sus problemas. Existen múltiples aplicaciones en las cuales esta tecnología es utilizada, dando excelentes resultados y ratificándose como el futuro de la identificación.

El actual documento presenta la combinación de dos tecnologías para dar solución al problema de la identificación registro y control de personas a través de una puerta de acceso. La comunicación inalámbrica combinada con la acción de radiofrecuencia se presenta como una solución atractiva, ya que la adecuación y conexión de la herramienta conjunta se hace más sencilla brindando las mismas soluciones con más facilidad, evitando conexiones innecesarias y en algunos casos, no aptas para las aplicaciones y lugares.

Controlar y registrar el acceso de personas, cada día se ha vuelto más importante; ya que en los diferentes ámbitos y espacios laborales conocer el movimiento de

los miembros vinculados a un determinado lugar de residencia, es de vital importancia para tomar acciones, bien sean preventivas o correctivas, asegurando así el correcto funcionamiento de las actividades y la seguridad de las mismas.

1. GENERALIDADES DEL PROYECTO

1.1 DESCRIPCIÓN DEL PROYECTO

1.1.1 Objetivo General. Diseñar e implementar una herramienta que permita el registro y control el acceso de personas mediante una aplicación de software, empleando tecnología *RFID*[1] y módulos Bluetooth.

1.1.2 Objetivos Específicos

- Desarrollar una aplicación de hardware que obtenga los datos del lector *RFID* bajo el protocolo Wiegand y los transfiera al ordenador mediante un módulo Bluetooth.

- Desarrollar una aplicación de software de interfaz didáctica y amigable que proporcione información con características detalladas a cerca de la circulación de personas en determinados espacios.

1.2 PLANTEAMIENTO DEL PROBLEMA

¿Cómo ejercer control sobre el ingreso de empleados y visitantes de una empresa? Tener un control sobre todas las actividades que realizan empleados, empleadores y visitantes que integran una institución, es una tarea que por su complejidad, podría partirse en diferentes áreas. Cuando se tiene una empresa, en el ejercicio de las horas laborales, es necesario no solo restringir el acceso a determinados lugares tanto para empleados como para personas ajenas a la institución (visitantes), debido a que se necesita mantener la integridad y la seguridad de la empresa. Hoy en día, el uso de herramientas tecnológicas permite mejorar la eficiencia de procesos de cotidianidad y para este caso cumplir con las características de privacidad para la empresa; ofreciendo un servicio no solo

[1] RFID, Radio Frequency Identification

durante el horario de trabajo; sino también, restringiendo el ingreso a personal en horarios extra laborales sin haber realizado previamente la gestión correspondiente para tal fin.

Alterna a esta situación, también se presenta una preocupación por parte de los que dirigen la empresa, la cual trata sobre el tiempo laborado y cambio repentino en el horario de atención. Incentivar al empleado a documentar sus ausencias durante el horario laboral, facilita una mayor comunicación entre los actores de las diferentes jerarquías que componen la institución, mejorando las relaciones; esto también conlleva a que los empleadores tengan un control sobre la permanencia del personal en la institución.

RFID es una tecnología que en los últimos años ha tomado gran apogeo, incrementando así su implementación y abarcando con el tiempo cada vez más áreas. Como su nombre lo dice, la identificación es su principal aplicación; haciendo de ésta, una nueva forma más económica, fácil, completa y rápida. Esta propuesta ha venido tomando gran importancia a nivel mundial, aumentando su consumo, especialmente en los países desarrollados, en donde gran parte de la industria en general cuenta con esta herramienta para mejorar las diversas aplicaciones y de manera más confiable.

Acoplando esta tecnología, la cual va implementada sobre la puerta de acceso; ésta proporciona un flujo de datos cada vez que la puerta se accione y con ayuda de un software diseñado para interpretar los datos, poder registrar características como: la hora de apertura de la puerta, la persona que realiza la acción y su sentido (entra o sale); abriendo paso no solo a un control sobre el ingreso de personas a la empresa, si no también, que ofrezca una alternativa de información comprendida por las personas que atraviesan dicha puerta.

1.3 MARCO TEÓRICO

1.3.1 ¿Qué es *RFID*? El nombre proviene de sus siglas en inglés, *Radio Frequency IDentification* o Identificación por Radiofrecuencia.

El origen de la tecnología *RFID* se remonta a la segunda guerra mundial, nace por necesidad de reconocer aviones amigos y enemigos a ciertos kilómetros de distancia por parte del ejército Estadounidense. A este sistema se le conoció como Identificación amigo-o-enemigo (*IFF, Identification Friend-or-Foe*), y el proceso consiste en enviar una señal de *RF* hacia todos los aviones que se encuentran dentro del alcance del transmisor, los cuales reflejan una señal; para poder diferenciarlos, los aviones amigos balancean sus aviones, con lo que se obtiene la señal de radio reflejada diferente al resto. [1]

Para el año de 1969 Mario Cardullo registra en Estados Unidos la primera patente con tecnología *RFID* utilizada para identificar a locomotoras. En la siguiente década se aplica la tecnología *RFID* de modo restringido y controlado, una de esas aplicaciones es para la seguridad de las plantas nucleares. En la década de los 80`s se da en Europa la primera aplicación de la tecnología *RFID*, utilizándola para la identificación del ganado; además se desarrollan muchas aplicaciones comerciales en el sector de la industria automotriz. Para la década de los 90`s se tiende a la miniaturización del sistema *RFID*, *IBM*[2] integra la tecnología en un solo chip electrónico, con lo que se obtiene una mayor difusión de ésta. Para la década actual, la reducción de los costos de las etiquetas *RFID*, permite que se aplique al inventariado de objetos de una manera automática, al monitoreo de personas animales u objetos y la automatización de la industria. [1]

[2]International Business Machines

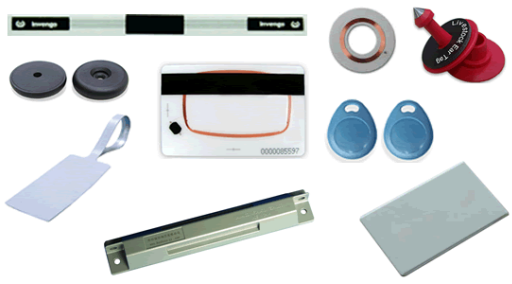
Figura 1. Imagen general de la tecnología

Fuente: http://antena420.blogspot.com

1.3.2 Descripción de la tecnología

- **Etiqueta.** Conocida también con el nombre de *Tag* o *transponder*; se adhiere al objeto que se desea identificar. Dependiendo la aplicación dada, esta etiqueta, puede contener información característica y propia del objeto como también comportarse simplemente como una llave de acceso. Está integrada por un microchip que permite almacenar información y una antena utilizada para la comunicación remota. [2]

Figura 2. Modelos diferentes *Tags RFID.*



Fuente: http://www.dipolerfid.es/productos/RFID_tag/Default.aspx

- **Lector.** Su función principal es brindar la energía necesaria para activar etiquetas de tipo pasivo y recibir la información de aquellos *Tags* que están dentro del rango[3]. Está compuesto por un transmisor, un receptor y una unidad de control. El lector, mediante la antena envía información digital codificada en ondas de radiofrecuencia para obtener la contenida en el *Tag*. [2]

Figura 3. Lector *RFID* de la empresa *HID*

Fuente: www.hidglobal.com

- **Antena.** Conectada al lector, sirve para establecer la comunicación con las etiquetas; ésta al ser el componente más sensible del sistema, es necesaria una ubicación en que tanto la recepción como la transmisión puedan realizarse de manera óptima y sin interferencia. Por su maniobrabilidad, puede ser de fácil traslado. [2]

Figura 4. Tipo de antena *RFID.*

Fuente: http://www.therfidshop.com

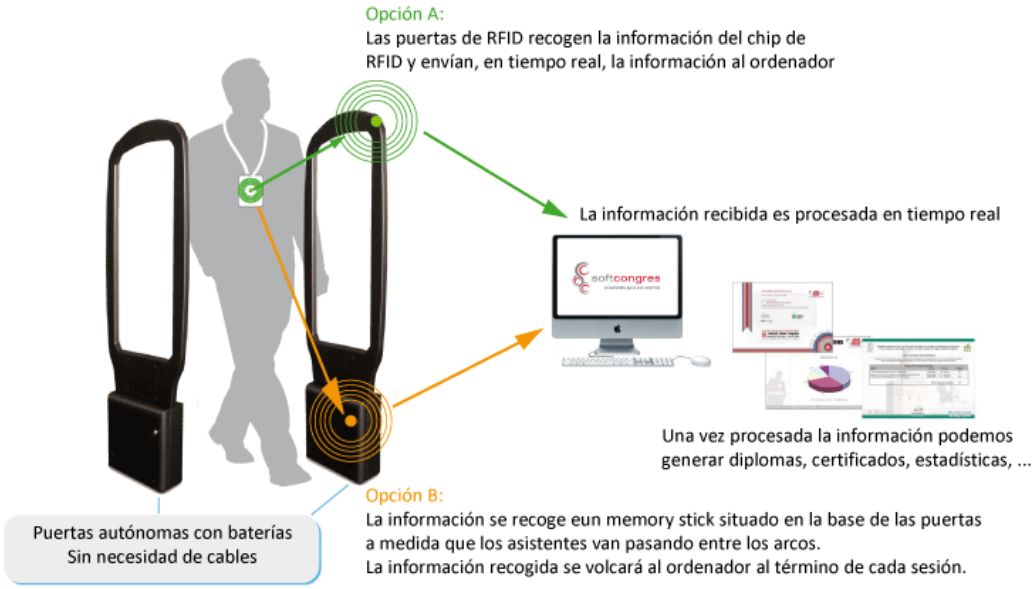
[3] Área en el que el lector está en capacidad de detectar la etiqueta

1.3.3 Principio de funcionamiento. Básicamente, el lector maneja un espacio determinado para detectar cualquier etiqueta que se encuentre dentro del rango. Tanto el lector como el *Tag*, deben estar sintonizados a la misma frecuencia para que exista la comunicación entre ellos, permitiendo la detección y la transmisión.

El lector envía una señal modulada a la frecuencia de funcionamiento, si el *Tag* es pasivo, la potencia de la señal debe ser mayor debido a que tendrá que alimentarlo; en caso contrario, simplemente la señal enviada corresponde a la necesaria para realizar la sincronización.

La transmisión entre el lector y la etiqueta se realiza por medio de radiofrecuencia; a medida que los datos son recibidos por la lectora, ésta gestiona por medio de protocolo *Wiegand*[4], la comunicación con el panel para realizar el tratamiento de los datos y ejecutar las acciones adecuadas.

Figura 5. Principio de funcionamiento de un sistema *RFID*



Fuente: www.softcongres.com

[4] Wiegand, Protocolo de comunicación, característico de la tecnología RFID

- **Frecuencias de operación**

LF: Trabaja en rangos de frecuencia inferiores a 125kHz. Su velocidad de comunicación es baja y su rango de lectura es de aproximadamente 0.5 m. [3]

HF: La frecuencia de trabajo para este sistema 13,56MHz. Por su velocidad de comunicación se aplica a sistemas estáticos y de baja velocidad, su rango máximo de lectura es aproximadamente 1m. [3]

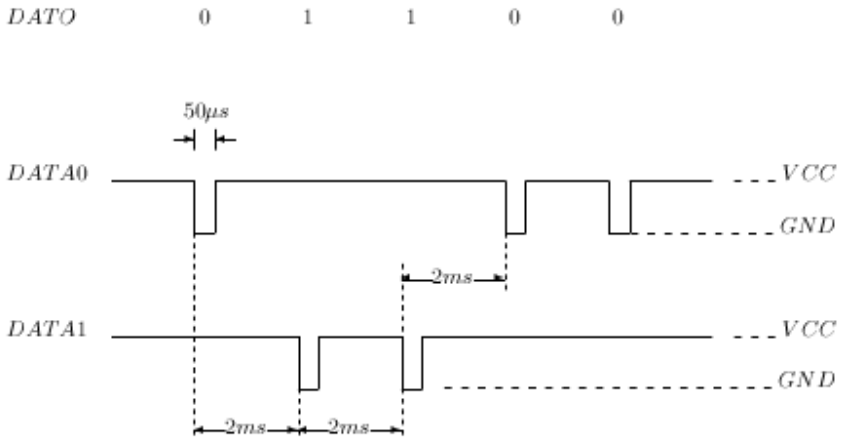
UHF: Comprende las frecuencias de funcionamiento: 868MHz y 928MHz. Su velocidad de comunicación es de 1200 *Tags* por segundo y rango máximo de lectura de 9m. [3]

- **Comunicación y Transmisión.** La transmisión de datos cuenta con dos líneas. Una línea para enviar los unos lógicos o *DATA1* y la línea para enviar los ceros lógicos o *DATA0*. Los niveles que usan son: bajo a nivel de *GND* y alto a nivel de *VCC*. En estado de reposo, es decir, en ausencia de transmisión, las líneas correspondientes a los 0 y 1 lógicos *DATA0* y *DAT A1* están en nivel 1 o VCC mientras que GND sigue siendo el nivel bajo.

Para transmitir un bit de valor 1, lo que se hace es enviar un pulso de bajo nivel normalmente de 50µs de duración por la línea *DATA1*; mientras *DATA0* permanece en alto. De manera contraria, si se desea enviar un bit 0, el pulso de nivel bajo de normalmente 50µs de duración, se envía por la línea *DATA0* permaneciendo en alto *DATA1*. Para evitar traslape y dar tiempo para que el sistema capte los datos, la separación entre pulsos es de 2ms. [6]

En la Figura 6, se puede apreciar de forma grafica el proceso de transmisión que realiza el protocolo de comunicación *Wiegand*

Figura 6. Transmisión de datos del protocolo de comunicación Wiegand.



Fuente: www.ucontrol.com modificada por los autores

1.3.4 Aplicaciones. Durante los últimos 10 años, la tecnología de identificación por radiofrecuencia *RFID*, ha venido creciendo exponencialmente en diferentes campos. En la industria, no solo se continúa implementando en los procesos que impulsaron el desarrollo de la tecnología; además, día a día aparecen nuevas herramientas para implementarse en procesos cotidianos, ofreciendo una mayor eficiencia y velocidad en los sistemas donde ésta se aplique.

Debido a la alta utilización de sistemas *RFID*, hoy en día pensar en adquirir un sistema de estas características no es imposible como se habría pensado una década atrás. Debido a la demanda y al fácil acople entre diferentes áreas, su uso es cada vez mayor, proponiendo un sistema económicamente asequible y llevando la tecnología a convertirse en casi un requisito para la industria del siglo *XXI*. [9]

A continuación, se destacan algunas aplicaciones para los sistemas *RFID*; manteniendo su objetivo principal el cual consiste en la identificación.

- Medicina
- Industria vehicular
- Dinero plástico
- Deportes
- Seguridad
- Inventarios
- Seguridad en Lokers
- Administración de Activos retornables
- Trazabilidad de medicamentos
- Parqueadero
- Joyería
- Administración de cargas
- Control de Peajes
- Seguimiento de contenedores
- Industria textil
- Minería
- Casinos
- Control de equipaje
- Bibliotecas y librerías

1.3.5 Tendencias. La tendencia de esta tecnología para el futuro es liderar en la industria y todos los campos de acción donde se necesite identificar, localizar y cuantificar algún producto o servicio. Esta tecnología como ya se había mencionado va ser el reemplazo del código de barras, encontrándose así en cualquier producto que lo requiera.

La utilización de *RFID* en la frecuencia de 13.56MHz es la tendencia actual y futura, brindando ésta ventajas adicionales en comparación a la trabajada a frecuencia menor de 125KHz, siendo esta última la más utilizada. La

implementación a 13.56MHz por su mayor capacidad permite tener una comunicación encriptada y la orientación a nuevas aplicaciones en el uso de: imagen, huella dactilar, etc.[5]. [11]

1.3.6 Estándares. Determinar la realización de estándares, depende básicamente de las necesidades del cliente. En algunos casos, la implementación de una solución, garantiza satisfactoriamente un buen resultado; mientras que en otros, obtener una solución avalada por expertos, es de preferencia por la confiabilidad dada. Sin embargo, la estandarización no se aleja del hecho de que lo que busca es controlar la oferta de servicio, evitando la obtención de soluciones que lleguen a afectar a los interesados convirtiendo su solución en un problema nuevo.

Actualmente, existen dos organismos que permiten mediante el desarrollo de estándares, regular la implementación de este servicio. La *ISO*[6] y la *EPC*Global[7], buscan la estandarización global para la industria y proponen estándares *RFID* en: el protocolo de interfaz área, es decir, aquello que comprende la comunicación entre el *Tag* y el lector *RFID*; contenido de los datos, básicamente definen el formato y la organización de los datos; conformidad, comprende la forma en que los productos cumplan las normas; y por último, de aplicación, que determina la implementación en las distintas áreas. [10]

El *ISO 11784*, define como los datos están estructurados en el *Tag*, mientras que el ISO *11785*, define los protocolos de interfaz área. Por otra parte, *ISO 14443* e *ISO 15693*, definen el uso de tarjetas inteligentes y de tarjetas de proximidad respectivamente. También está el estándar que prueba la conformidad de los *Tag* y lectores *RFID*, *ISO 18047*; y el *ISO 18046* que prueba el desempeño de la interacción *Tag* lector. [3]

[5]Protocolo de encriptación de la tarjeta de 64 Bits y capacidad de memoria entre 2Kby 32Kb
[6] ISO, International Organization for Standardization
[7] EPC, Electronic Product Code

Para *RFID*, la *ISO*, ha desarrollado una estandarización sobre la identificación automática y la gestión de objetos, conocida como la serie *ISO 18000*. Este estándar, tiene una cobertura sobre el protocolo de interfaz área y está compuesto de la siguiente manera:

– *ISO 18000-1*: Parámetros genéricos para las interfaces área sobre las frecuencias globalmente aceptadas.
– *ISO 18000-2*: Interfaz de aire a frecuencia 135KHz
– *ISO 18000-3*: Interfaz de aire de frecuencia 13.56MHz.
– *ISO 18000-4*: Interfaz de aire para frecuencias de 2.4GHz.
– *ISO 18000-5*: Interfaz de aire para frecuencias de 5.8GHz.
– *ISO 18000-6*: Interfaz de aire para frecuencias entre 860MHz y 930MHz.
– *ISO 18000-7*: Interfaz de aire para frecuencia 433.92MHz.[5]

1.3.7 Tecnología Bluetooth. Bluetooth es un estándar global que identifica un conjunto de protocolos que facilitan la comunicación inalámbrica entre diferentes tipos de dispositivos electrónicos. Su nombre viene del Rey vikingo, Harald Bluetooth (940 A.D – 981 A.D), famoso por su habilidad para la comunicación y para hacer que la gente hablara entre ella.

Bluetooth opera en la banda libre de radio ISM[8] a 2.4 GHz. Su máxima velocidad de transmisión de datos es de 1 Mbps. El rango de alcance Bluetooth depende de la potencia empleada en la transmisión. La mayor parte de los dispositivos que usan Bluetooth transmiten con una potencia nominal de salida de 0 dBm, lo que permite un alcance de unos 10 metros en un ambiente libre de obstáculos. [4]

1.3.8 Diagrama del Bluetooth. La información que se intercambia entre dos unidades Bluetooth se realiza mediante un conjunto de slots que forman un

[8] Banda Internacional Medico-Científica

paquete de datos. Cada paquete comienza con un código de acceso de 72 bits, que se deriva de la identidad maestra, seguido de un paquete de datos de cabecera de 54 bits. Éste contiene importante información de control, como tres bits de acceso de dirección, tipo de paquete, bits de control de flujo, bits para la retransmisión automática de la pregunta, y chequeo de errores de campos de cabecera.

La dirección del dispositivo es en forma hexadecimal. Finalmente, el paquete que contiene la información, que puede seguir al de cabecera, tiene una longitud de entre0 y 2745 bits.

Tabla 1. Estructura del paquete de datos del Bluetooth

Longitud en Bits	72 bits	54 bits	0 – 2745 bits
Campo	Cód. Acceso	Cabecera	Información

Fuente: Java 2.0 Micro Edition: Soporte para Bluetooth

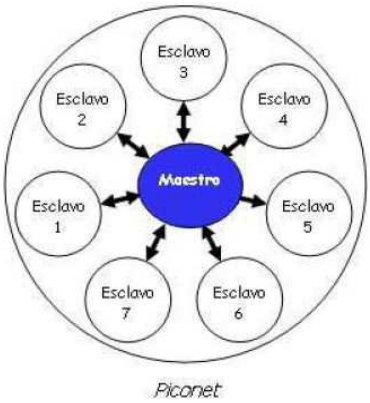
En cualquier caso, cada paquete que se intercambia en el canal está precedido por el código de acceso. Los receptores de la *Piconet*[9] como se muestra en al figura 7, comparan las señales que reciben con el código de acceso, si éstas no coinciden, el paquete recibido no es considerado como válido en el canal y el resto de su contenido es ignorado.

Como hemos citado anteriormente si un equipo se encuentra dentro del radio de cobertura de otro, éstos pueden establecer conexión entre ellos. Cada dispositivo tiene una dirección única de 48 bits, basada en el estándar IEEE 802.11 para WLAN. [4]

[9]Piconet, Dos o más unidades Bluetooth que comparten un mismo canal

En principio sólo son necesarias un par de unidades con las mismas características de hardware para establecer un enlace. Dos o más unidades Bluetooth que comparten un mismo canal forman una piconet.

Figura 7. Esquema de una Piconet



Fuente: Java 2.0 Micro Edition: Soporte para Bluetooth

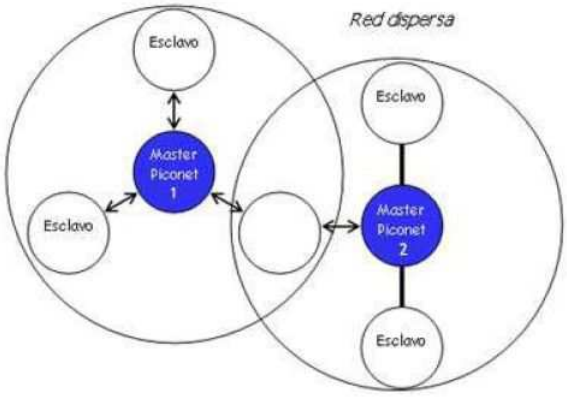
Para regular el tráfico en el canal, una de las unidades participantes se convertirá en maestra, pero por definición, la unidad que establece la Piconet asume éste papel y todos los demás serán esclavos. Los participantes podrían intercambiar los papeles si una unidad esclava quisiera asumir el papel de maestro. Sin embargo sólo puede haber un maestro en la Piconet al mismo tiempo. Hasta ocho usuarios o dispositivos pueden formar una Piconet y hasta diez Piconet pueden coexistir en una misma área de cobertura.

Medios y Velocidades

Además de los canales de datos, están habilitados tres canales de voz de 64 kbit/s por Piconet. Las conexiones son uno a uno con un rango máximo de diez metros, aunque utilizando amplificadores se puede llegar hasta los 100 metros, pero en este caso se introduce alguna distorsión.

Los datos se pueden intercambiar a velocidades de hasta 1 Mbit/s. A un grupo de Piconet se le llama scatternet[10]. El rendimiento, en conjunto e individualmente de los usuarios de una scatternet es mayor que el que tiene cada usuario cuando participa en un mismo canal de 1 Mbit. Además, estadísticamente se obtienen ganancias por multiplexación y rechazo de canales salto, debido a que individualmente cada Piconet tiene un salto de frecuencia diferente. Diferentes Piconet pueden usar simultáneamente diferentes canales de salto.

Figura 8. Imagen de una Scatternet



Fuente: Java 2.0 Micro Edition: Soporte para Bluetooth

Los equipos que comparten un mismo canal sólo pueden utilizar una parte de su capacidad.

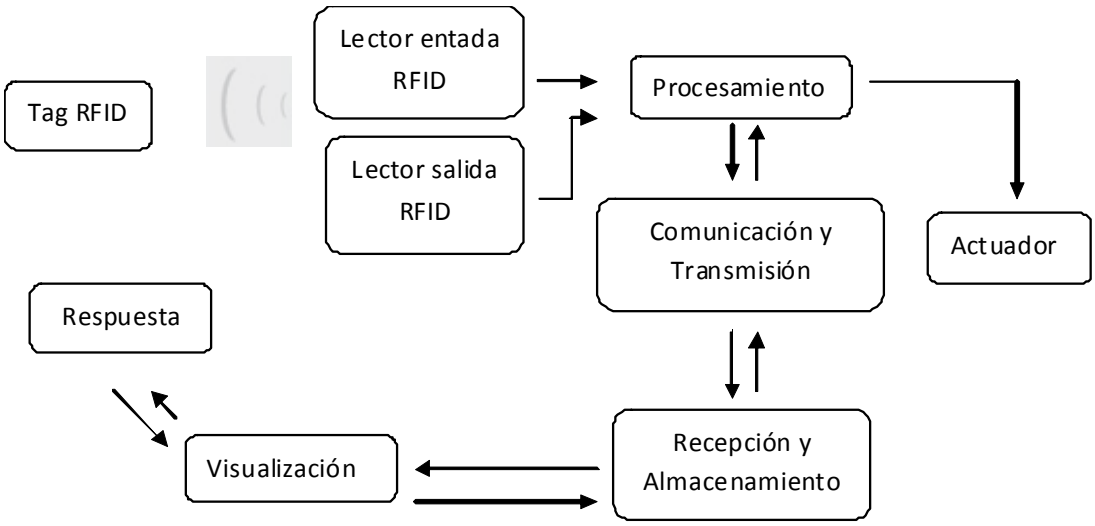
Aunque los canales tienen un ancho de banda de 1Mbit, cuanto más usuarios se incorporan a la Piconet, se disminuye su capacidad hasta unos 10kbit/s.

[10]Escarnet, Grupo de piconets

2. DISEÑO DEL SISTEMA

2.1 ESQUEMA GENERAL DE DISEÑO

Figura 9. Esquema General de Diseño



Fuente: Realizada por los Autores

El diseño del sistema se divide en tres secciones importantes que a su vez se dividen, en subsecciones definidas a continuación. Estas secciones son:

- Sistema y Comunicación *RFID*
- Transmisión de Datos
- Enlace Bluetooth y Software

2.2 SISTEMA Y COMUNICACIÓN *RFID*

2.2.1 Detección. La detección del sistema inicia en el momento en el que el lector, durante su emisión de ondas detecta el *Tag, el* cual al ser alcanzado y por medio de la antena incrustada, responde de manera autoinducida, alertando de manera

automática su presencia. Cabe resaltar que la detección se realiza dentro del rango de operación del lector.

2.2.2 Lectura. La lectura se lleva a cabo seguidamente de la detección de la tarjeta, en el momento en que esta responde, emite la información almacenada en su Chip integrado, equivalente a los códigos de identificación que caracterizan cada tarjeta.

2.3 TRANSMISIÓN DE LOS DATOS

La transmisión de los datos se realiza por medio de un protocolo de comunicación característico de esta tecnología llamado *Wiegand.* Luego de la detección y lectura de los datos el lector los transmite por sus puertos de salida para el propósito de la aplicación[11].

2.3.1 Adquisición y Tratamiento. La adquisición y el tratamiento de los datos están a cargo de una tarjeta de adquisición diseñada con esta finalidad. Esta tarjeta está dividida en bloques de funcionalidad encargados de cumplir a cabalidad los procesos necesarios y determinar un correcto funcionamiento del sistema.

2.3.2 Obtención y Procesamiento. Los datos de salida emitidos por el lector se obtienen con un esquema sencillo de adecuación de señal, diseñado para que no exista ninguna pérdida de información. Después de que estas señales han entrado a la unidad central de procesamiento, esta se encarga de sincronizar y obtener los datos por medio de la programación indicada, bajo los principios de operación de comunicación del lector.

[11] Ver comunicación y Transmisión en 0

2.3.3 Almacenamiento Temporal. El almacenamiento sucede luego de la interpretación y obtención de los códigos de las tarjetas. Estos códigos son guardados de manera temporal en vectores, seccionando y organizando la estructura de la lectura con la finalidad que a la hora de la Transmisión, no haya alguna perdida de información y así se garantice el correcto funcionamiento y visualización.

2.3.4 Comunicación y Transmisión. En la comunicación de los datos, un Microcontrolador se encarga por medio de los puertos de comunicación SCI[12], de enviar los datos hacia el dispositivo de transmisión encargado de establecer el enlace con una base central que complementará el proceso. La transmisión se ejecuta a través de un dispositivo Bluetooth de encargado recibir sincronizar y enviar ordenadamente los paquetes de datos.

2.4 ENLACE BLUETOOTH Y SOFTWARE

2.4.1 Recepción. La recepción se realiza al igual que en la transmisión, con un módulo Bluetooth conectado directamente a un computador encargado de recibir y ordenar los datos para ser procesados.

2.4.2 Software. El software es la central de todo el proceso, en él está la decisión de autorizar o denegar el acceso a determinada tarjeta. Otras de las funciones principales del software son analizar, registrar y almacenar la información, unida al acceso concedido.

[12] SCI, Puerto de comunicación serial de Microcontrolador

2.5 DESCRIPCIÓN Y FUNCIONAMIENTO DE LOS DISPOSITIVOS INTEGRADOS EN EL SISTEMA

En esta sección describiremos de manera detallada los dispositivos integrados en el funcionamiento del sistema.

2.5.1 Lector. En la búsqueda de los lectores, los criterios de selección se deben ajustar correctamente a la aplicación, brindando un adecuado funcionamiento de acuerdo a los requerimientos del sistema. Entre estos requerimientos cabe resaltar tamaño, frecuencia de operación, resolución, confiabilidad y garantía. La búsqueda del fabricante, corresponde a la necesidad de brindar un soporte y un producto que garantice su permanencia en el mercado. Los lectores resultantes, corresponden a la empresa HID[13] con referencia **ProxPoint Plus 6005.**

Este lector cuenta con diez puertos para su funcionamiento, donde es necesario identificar cuáles de estos son entradas, cuales salidas y sus pines de alimentación. Dentro de estos cabe resaltar dos puertos de alimentación y dos puertos encargados de transportar los datos de interés. Este lector puede ser alimentado desde una tensión DC de 5[V] a 16[V].

Figura 10. Lectoras a usar.

Fuente: www.hidglobal.com

[13] Human Interface Device

A continuación se detallarán algunas características de instalación de estas lectoras. Ver anexo B.

En la Tabla 2 se muestre el esquema de conexión de una lectora y sus respetivos hilos conductores marcados con un color diferente.

Tabla 2. Indicación de conexión de los Lectores

	VCC (5-16)		Cable Blindado		RETENCIÓN
	TIERRA		LED VERDE		Presencia Tarjeta
	DATOS 0		LED ROJO		
	DATOS 1		SEÑAL AUDIBLE		

Fuente: Hoja de datos del dispositivo.

- Dimensiones

3.135” x 1.720” x 0.660” (7.96 x 4.37 x 1.68 cm)

- Material

Policarbonato UL 94

- Temperatura de operación

-22 º a 150 º F (-30º a 65º C)

- Frecuencia de Operación

125kHz

- Requerimientos Máximos de Corriente.

Corriente (DC), Promedio 30mA, 75mA Pico

- Certificaciones

UL294/cUL (US), FCC Certification (US), IC (Canada), CE (EU),C-tick (Australia, New Zealand), SRRC (China), MIC (Korea), NCC (Taiwan), MIC (Japan), iDA (Singapore), RoHS.

2.5.2 ***Tags RFID.*** Las etiquetas o Tag RFID son piezas claves en la implementación del diseño, ya que estas son las que más expuestas están a posibles daños, siendo portadas por el usuario permanentemente y maniobradas de múltiples formas.

Para el desarrollo del trabajo se contemplaron en la elección de tarjetas: confiabilidad, duración, compatibilidad, rendimiento y robustez al momento de su manipulación; por ésta razón se escogieron tarjetas del mismo fabricante de los lectores, para garantizar una sincronización con el sistema sin ningún tipo de inconvenientes y obtener un valor agregado representado por la confiabilidad de la empresa HID.

Lo que hace única a la tarjeta, es la impresión de un número único de identificación en su espacio de memoria. Este código, está compuesto por el *UserCode* y *FaciltyCode*.

Es de vital importancia leer y adquirir correctamente este código de identificación, ya que de éste depende toda la información referente al usuario portador.

Figura 11. Tags a utilizar

Fuente: www.hidglobal.com

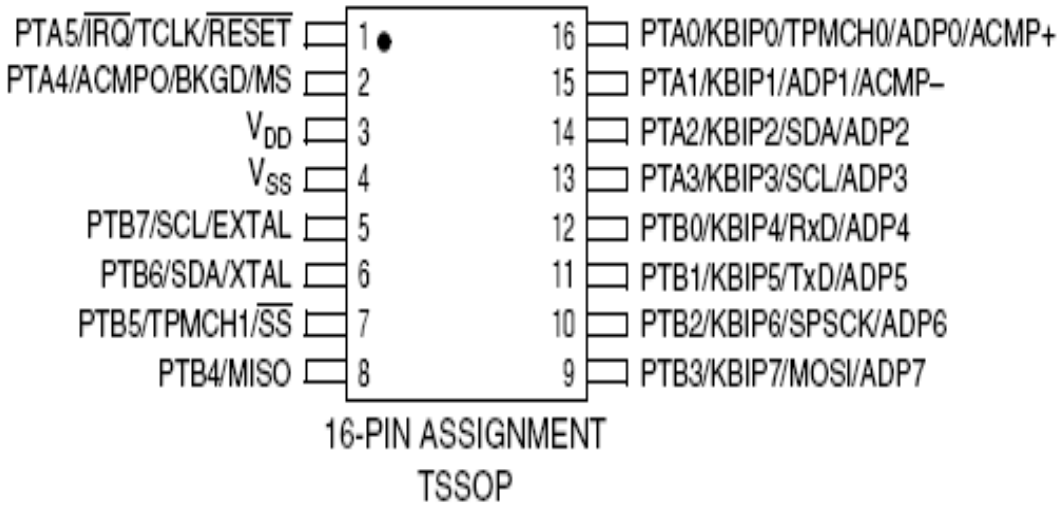
2.5.3 Unidad central de proceso. Como unidad de procesamiento se seleccionó un Microcontrolador de referencia MCS908QG8 de la empresa *Freescale*[14].

Las características del dispositivo en distribución de pines, puertos de propósito general, puertos de comunicación, velocidad de procesamiento, memoria, tamaño y baja alimentación; hacen de éste, atractivo para el trabajo a realizar, permitiendo un ajuste favorable para el funcionamiento de la herramienta.

El Microcontrolador estará encargado de adquirir, procesar y comunicar las señales provenientes de los lectores, recibiendo a su vez la autorización o rechazo de la identificación, permitiendo el acceso por medio de una señal que active el sistema de apertura de la puerta.

[14]Freescale, Empresa fabricante de semiconductores.

Figura 12. Imagen del Microcontrolador, distribución de pines y encapsulado



Fuente: Hoja de datos del dispositivo

Tabla 3. Periféricos del Microcontrolador

Módulo		**Número**
Comparador Analógico	(ACPM)	2
Conversor Análogo Digital	(ADC)	1
Unidad Central de Procesamiento	(CPU)	2
Módulo IIC	(IIC)	1
Fuente Interna de Reloj	(ICS)	1
Teclado de Interrupciones	(KBI)	2
Módulo Temporizador	(MTIM)	1
Interfaz de Comunicación Serial	(SCI)	3
Interfaz Periférica Serial	(SPI)	3
Temporizador PWM	(TPM)	2
Oscilador de Baja Potencia	(XOSC)	1
Módulo Debug	(DBG)	2

Fuente: Hoja de datos del dispositivo, Modificada por los Autores

A continuación se presentan las principales características del Microcontrolador.

- CPU 8 bits 20 MHz
- Memoria FLASH 8 Kbytes
- Memoria RAM 512 Bytes
- Comunicación Asíncrona Full Dúplex
- 12 puertos de propósito general I/O
- Salidas a 10 mA Max 60 mA pico
- Pullups por programación
- Alimentación 3.3 [V]

2.5.4 Módulo Bluetooth RN – 41

Figura 13. Módulo Bluetooth

Fuente: www.sparkfun.com, Distribuidor

La selección se basa en el cumplimiento de las especificaciones necesarias para llevar a cabo la transmisión rápida confiable y completa de acoplamiento dentro del sistema.

Este dispositivo cuenta generalmente con una serie de características que lo hacen muy atractivo para la aplicación, tales como gran distancia de transmisión (100m), bajo consumo de potencia, frecuencia de operación adecuada (2.4 GHz), comunicación serial y baja tensión de alimentación.

- Radio Clase 1 (17dbi-arriba de los 100 metros)
- Bluetooth
- Soporta V2.0 + EDR
- Soporta configuración por comandos AT
- Control de flujo RTS, CTS, DSR, DTR.
- Interface de conexiones de datos UART (SPP o HCI) y USB (HCI only).
- Tasa de transferencia con servicio SPP: 240Kbps en modo esclavo y 300Kbps como máster.
- Serial Port Profile (SPP) totalmente embebido
- Procesador ARM7 hasta 48MHz
- Memoria Flash de 8Mb
- Tasa de transmisión de datos de 921K baudios
- Antena Chip integrada
- Seguridad con encriptación de 128-bits
- Capacidad Multipunto
- Aprobado por el FCC y el consorcio Bluetooth

2.5.5 Adaptador USB Bluetooth. El adaptador Bluetooth – USB[15] es usado para la transmisión de datos entre un PC y cualquier dispositivo que contenga tecnología Bluetooth.

La principal característica de este módulo es la facilidad de adaptarse e instalarse en cualquier ordenador con el fin de realizar una comunicación.

[15] USB, Universal Serial Bus

Figura 14. Adaptador USB Bluetooth

Fuente: www.sparkfun.com, Distribuidor.

Este adaptador emula un puerto serial para el envío y recepción de los datos, donde las características y propiedades del puerto se ajustan a la comunicación con el otro dispositivo, en este caso, con el módulo Bluetooth *RN-41*.
A continuación se presentan las principales características de este dispositivo.

- Bluetooth V2.0 compatible
- Compatibilidad: USB UHCI[16] / OHCI[17]spec 2.0 (USB 1.1 Compatible)
- Interface USB
- LED indicador de Estado
- Banda de frecuencia: 2.4GHz ISM banda abierta
- Precio 20 USD

[16] UHCI, Universal Host Controller Interface
[17]OHCI Open Host Controller Interface.

3. DESARROLLO E IMPLEMENTACIÓN DEL SISTEMA

3.1 DESCRIPCIÓN DE LA TARJETA

Para el diseño y fabricación de la tarjeta se tuvieron en cuenta los ítems nombrados a continuación.

3.1.1 Alimentación y regulación. Primera y esencialmente se prueba el módulo de alimentación y regulación, ya que de este depende el buen funcionamiento de los elementos y el conjunto en general. La tarjeta cuenta con entrada de alimentación que es obtenida de la red eléctrica y seguidamente es pasada por tres regulaciones dentro del circuito.

Luego de la toma de alimentación eléctrica esta pasa por un circuito rectificador AC/DC, donde la tensión es regulada de 110V a 7.36V suficiente para trabajar todos los dispositivos de la tarjeta. Los lectores se alimentan a 5V, lo cual fue necesario regular esta tensión de entrada para poder proveer de manera continua y confiable, la tensión de los lectores.

Los dispositivos como el Microcontrolador y el módulo Bluetooth trabajan a una alimentación promedio de 3.3V, lo cual implica una nueva regulación de 5V/3.3V complementando la fase de regulación y alimentación del circuito.

3.1.2 Adecuación de señal. Dentro de la tarjeta se presentan dispositivos encargados de realizar adecuación de señales de entrada, tales como son las señales provenientes de los lectores que transportan la información pertinente de los *Tags* leídos.

Esta adecuación consta de la colocación de Pullups a las señales de Datos 0 y Datos 1, donde seguidamente pasarán a dos puertos de propósito general del Microcontrolador por cada lector, para ser procesado posteriormente.

3.1.3 Conexiones. La conexión de los lectores dentro del circuito se hace a través de un conector de 4 pines para cada lector. Los cuales corresponden a *VCC, GND, DATOS0, DATOS1,* donde cada una de estas conexiones continúa dentro del circuito.

Para la transmisión de datos, está el dispositivo Bluetooth que por medio de un conector de 4 pines que corresponden a VCC, GND, RX, TX, se une al Microcontrolador.

Seguidamente está la conexión de potencia para la apertura y cerrado de la puerta la cual va a estar implantada en el sistema y consta de un conector de 3 Pines que hacen referencia a alimentación, señal y tierra, que después de una pequeña etapa de potencia pasan a un relé que es el encardado de suministrar el pulso para la orden de apertura.

3.2 DISEÑO DE LA TARJETA DE ADQUISICIÓN

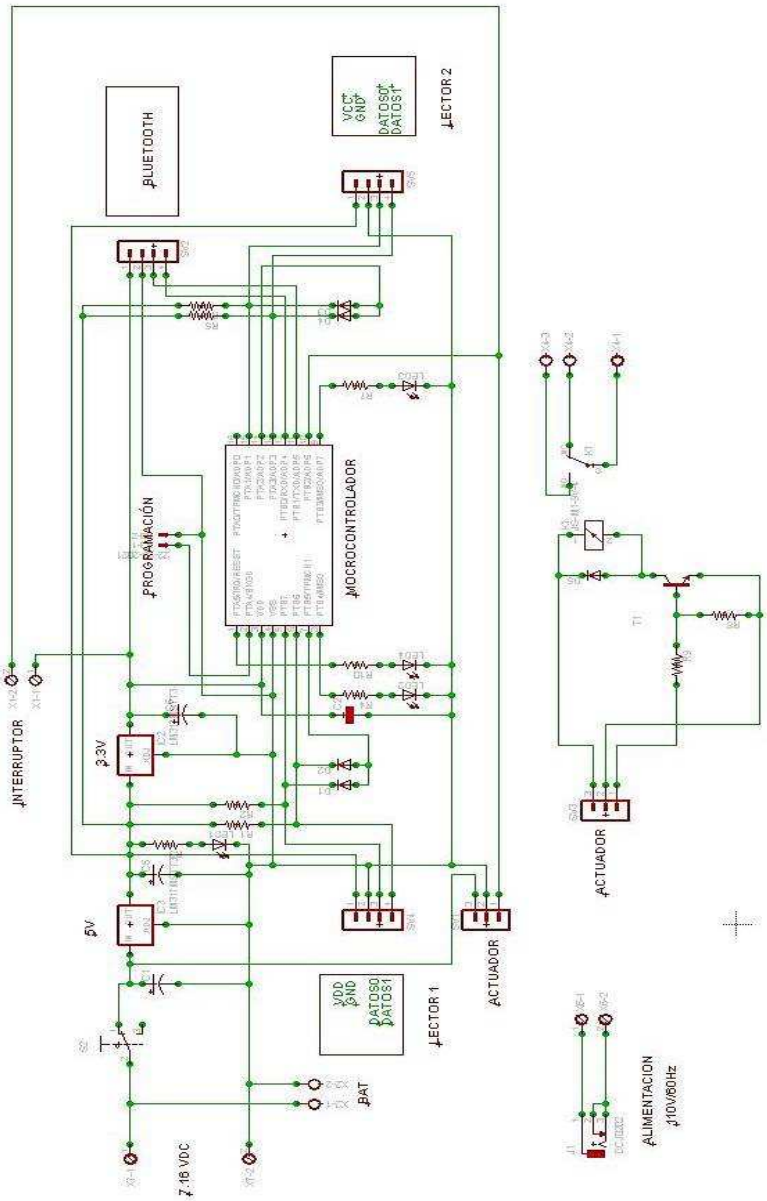
A continuación se muestra la distribución circuital de los dispositivos electrónicos de la tarjeta de adquisición y tratamiento de los datos, como una posible solución al problema planteado, siguiendo los criterios de diseño ya descritos.

Para la realización de la *PCB*[18], se utilizó un software especializado en el diseño de circuitos impresos; este software tiene por nombre *Eagle Layout Editor y* permite realizar esquemáticamente el diseño del circuito con posibilidad de hacer el enrutamiento de circuito.

[18] PCB, Print Circuit Board

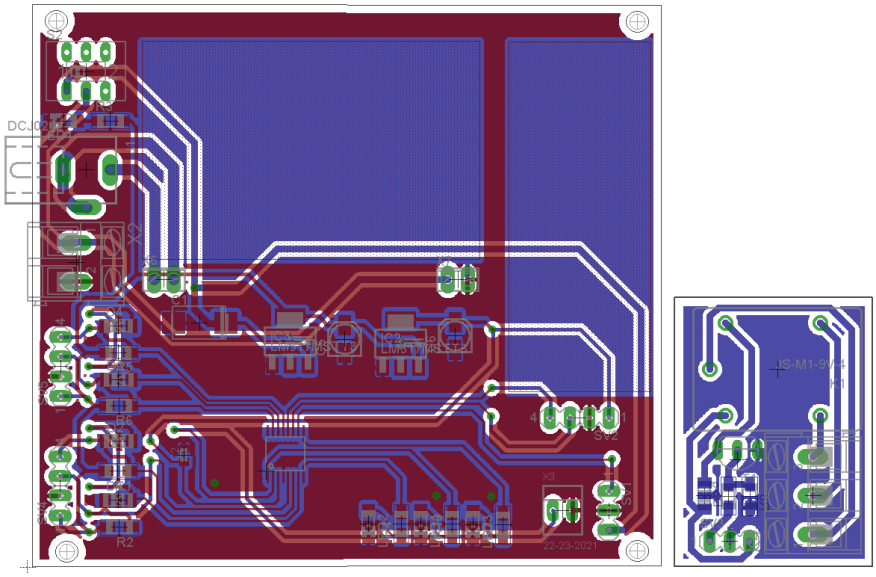
El diseño de la tarjeta se realizó teniendo en cuenta las normativa básica para la realización de *PCB*, en cuanto a ubicación de dispositivos, tipo de rutas y ancho de las vías.

Figura 15. Esquemático de la tarjeta



Fuente: Software de Diseño (Eagle)

Figura 16. Circuito Impreso de la tarjeta



Fuente: Software de Diseño

El diseño planteado anteriormente garantiza el cumplimiento de las operaciones predispuestas para la tarjeta, ofreciendo el servicio delegado y ejecutando las tareas de manera correcta y ordenada. La capacidad de recibir los datos de las lectoras y enviarlos mediante comunicación Bluetooth, y recibir respuesta por parte del PC; delega sobre la herramienta de software una complementación del proceso del sistema completo

3.3 DESCRIPCIÓN GENERAL

Inicialmente el sistema se encuentra en espera de la presencia o detección de alguna tarjeta, que le permita ponerse en funcionamiento. Una vez detectada, el código de identificación es transferido al lector que a su vez lo envía por sus puertos de comunicación de datos *DATA 0* y *DATA 1.*

Ya recibidos los datos, el Microcontrolador de acuerdo a su programación previa interpreta y organiza de manera correcta el código de identificación y lo transfiere por sus puertos de comunicación al dispositivo Bluetooth.

El dispositivo Bluetooth adquiere estos datos y los transfiere al PC donde por medio del software verifica si para este código está permitido el acceso. De esta manera si el acceso es concedido, envía una señal de confirmación a la tarjeta y permite la apertura de la puerta.

Análogamente si el código de la tarjeta es reconocido y se encuentra en la base de datos; el software registra características del acceso como hora de entrada, información del usuario y otras que serán descritas en una sección posterior.

3.3.1 Tratamiento de las señales Wiegand. Dentro de la programación del Microcontrolador, las señales *Wiegand* son tratadas y almacenadas en variables que me permiten un mejor procesamiento y transmisión de las señales.

Tabla 4. Variables Obtención código de Identificación

Variable	Tipo	Bits
UcerCode (UC)	Word (16 Bits)	0000000000000001
FacilityCode (FC)	Byte (8 Bits)	00100100
Wiegand	Long (24 Bits)	001001000000000000000001

Fuente: Hecha por los autores

Para el tratamiento y sincronización de las señales fue necesario generar una señal de reloj, a partir de las dos líneas de datos de entrada DATA1 y DATA0 por medio de una compuerta AND.

Esta compuerta AND se modeló con dos diodos, que de acuerdo a la señal enviada por el lector por medio de los hilos conductores, colocados en esta misma línea pueden generar una señal de reloj cada vez que pase el Tag por el lector.

3.4 DESCRIPCIÓN DEL PROGRAMA DE ADQUISICIÓN Y TRANSMISIÓN DE DATOS

Como primera medida, realizamos una función que permite la transmisión de datos seriales al Módulo Bluetooth, para posteriormente enviarlos al PC. Cabe resaltar que es necesario entregarle datos seriales al dispositivo Bluetooth ya que de esta manera se realiza una transmisión exitosa.

Esta función es llamada **cadena_tx;** la cual almacena en los registros del canal de comunicación serial del Microcontrolador los datos y les hace la respectiva transformación para poder enviar caracteres alfa numéricos. [Ver anexo A]

```
//funcion para transferencia de datos hacia el Dispositivo Bluetooth
voidcadena_tx (char *str)
{
for (TX=0;TX<strlen(str);TX++)
{
while(SCIS1_TC==0)
      {}…
```

3.4.1 Diagrama de Flujo del programa principal. El diagrama de flujo de programa principal se puede observar en el Anexo A.

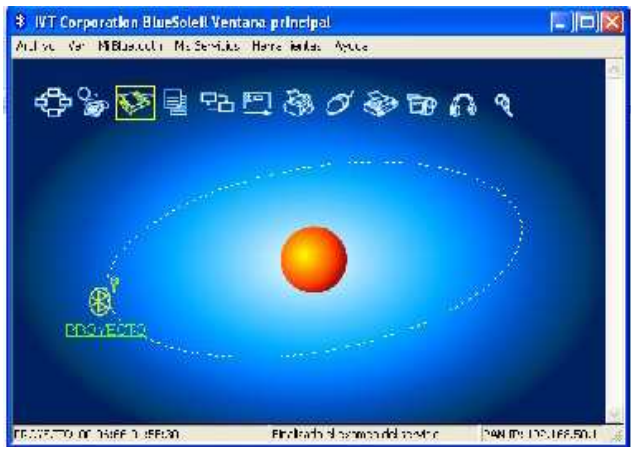
3.5 CONFIGURACIÓN DEL MÓDULO BLUETOOTH *RN-41*

La configuración del módulo Bluetooth, se realizó directamente con la tarjeta prediseñada para hacer las respectivas pruebas. La alimentación del este módulo fue tomada de la regulación de 3.3 V dentro de la tarjeta; esta tensión es necesaria para el funcionamiento del dispositivo.

Seguidamente de alimentarlo este nos indica por medio de un LED de color rojo parpadeante que esta listo para ser usado. Cuando el módulo es conectado este inmediatamente entra en modo para ser detectado y empezar una transmisión y recepción de datos. Para hacer la respectiva conexión es necesario otro módulo con el cual establecer la comunicación, para esta aplicación se usa un adaptador Bluetooth USB conectado.

El driver permite establecer la comunicación haciendo un rastreó de los dispositivos Bluetooth que se encuentran dentro de su área de cobertura, el cual cuenta con una interfaz que visualiza los dispositivos presentes.

Figura 17. Interfaz de módulo USB Bluetooth



Fuente: Interfaz del módulo USB Bluetooth

Luego de haber localizado el módulo RN-41 conectado a la tarjeta, es necesario establecer la conexión que se realiza por medio de una clave de acceso que trae el dispositivo por defecto.

Una vez establecida la comunicación el ordenador otorga un puerto de comunicación COM para el módulo, uno de transmisión y otro de recepción; se procede a la configuración del *RN-41.* Un LED de color verde ubicado en el módulo, alerta una conexión exitosa. Si el LED no se enciende, indica que el dispositivo aún no se ha conectado.

El módulo Bluetooth RN-41 por defecto transmite a una rata de baudios de 115200, que es necesario conocer para establecer comunicación. Este módulo puede ser configurado por medio del ordenador entrando en el modo de configuración.

Haciendo uso del Hyperterminal, se configuran los parámetros de recepción tales como la velocidad del puerto y por cual puerto se van a recibir los datos. Cabe aclarar que los dos dispositivos tienen que estar sincronizados a la misma velocidad y que el puerto asignado por el ordenador para el Bluetooth en la tarjeta debe ser configurado en el Hyperterminal.

Figura 18. Ventana de configuración del puerto de comunicación

Fuente: Interfaz de Hyperterminal

Para entrar en el modo de configuración se teclea de manera consecutiva 3 veces la tecla de signo $ sobre el espacio de trabajo de Hyperterminal.

$$$	***Comando***
CMD	***Respuesta***

Para desplegar todos los comandos que este tiene y lo que se puede configurar basta con teclear la letra H y automáticamente seran mostrados en pantalla.

Una vez estudiados los comandos de interés, procedemos a entrar en la configuración actual del dispositivo. Para hacer esto tecleamos la letra D.

Comando	***Respuesta***
D	*****Settings*****

BTA=000666015F30
BTName=PROYECTO
Baudrt=115200
Parity=None

Comando	*Respuesta*
D	**Mode=Slave**
Authen=0	
Encryp=0	
PinCod=1234	
Bonded=0	
Rem=NONE SET	

Para hacer un cambio en el nombre del dispositivo se debe teclear el siguiente comando

Comando	*Respuesta*
SN,“Nombre deseado”	**AOK**
SN, SID	**AOK**

Para la configuración de la velocidad de la transferencia de datos se usa el siguiente comando

Comando	*Respuesta*
SU, “velocidad deseada”	**AOK**
SU,96	**AOK**

Vale la pena resaltar que la velocidad esta estándarizada de acuerdo a los valores preestablecidos.

Después de haber realizado la configuración, para salir de este modo lo hacemos de la siguiente manera.

Comando	***Respuesta***
---	**END**

3.6 DISEÑO DE LA HERRAMIENTA DE SOFTWARE

Es quizás el elemento más importante del trabajo, ya que esta es la etapa que permitirá la comunicación entre el sistema y el usuario, convirtiéndose en base y guía para que el uso de toda la herramienta sea eficiente. Está basada en el lenguaje de programación JAVA y cuenta con características que facilitan la interacción y uso del usuario, para la administración y manejo tanto del acceso como de la información registrada. Para ésta, la plataforma Netbeans[19]con versión 6.9 fue la utilizada para llevar a cabo su diseño y posterior elaboración.

Aunque esta plataforma de desarrollo cuenta con un gran número de herramientas, es necesario adecuarla con la obtención de algunas librerías de acceso libre pero no contempladas dentro de la plataforma, para cumplir con el propósito.

3.6.1 Preparación de la plataforma. Como es de nuestro conocimiento, una de las ventajas que tiene *JAVA* y que lo diferencia drásticamente de otros lenguajes de programación, es que lo hace independiente del sistema operativo debido a que corre dentro de su propia máquina virtual, la cual ofrece lo necesario para que estas aplicaciones se puedan ejecutar sin ningún inconveniente. Esta máquina virtual se conoce como JVM, siglas en ingles *Java Virtual Machine*. Dentro de los requisitos principales de esta plataforma de desarrollo, está el JRE[20]y el JDK[21],

[19] Disponible en la página web oficial: http://www.netbeans.org
[20]Java RuntimeEnvironment. Disponible en la página Web: http://www.java.com/es/download

herramientas para la ejecución y desarrollo de aplicaciones *JAVA* respectivamente.

Hoy en día, con tanta facilidad para la adquisición e instalación de software desde la internet, hace redundante la tarea de entrar en detalle sobre éste proceso. Sin embargo, si se puntualizara en lo que comprende la post-instalación y la adecuación de la herramienta para que permita el trabajo sobre puertos de comunicación y que no están dentro de las librerías del *JDK* ni las de Netbeans.

A continuación se muestran los pasos realizados para la habilitación de Netbeans**.** Las herramientas provenientes de la red y utilizadas para la elaboración de esta fase, hacen parte del programa de software libre.

a. Obtener la plataforma de desarrollo Netbeans para aplicaciones *JAV A.* No es la única herramienta que presta el servicio para este tipo de desarrollo.

b. Realizar la instalación normal siguiendo las instrucciones de su guía. En caso de necesitar las herramientas *JRE* y el *JDK*, se pueden descargar desde sus casas de desarrollo.

c. Después de tener instalado y funcionando Netbeans, obtener los *APIs* para comunicaciones y manejo de puertos serial llamada *Comm.jar*[22]y *SerialPort.jar*[23] respectivamente.

d. Abrir **Netbeans** y crear un proyecto nuevo.

---

[21]Java Development Kit. Disponible en la página Web: http://www.oracle.com/technetwork/java/javase/downloads/jdk6-jsp-136632.html

[22] http://code.google.com/p/easyx10/downloads/detail?name=javacomm20-win32.zip&can=2&q=

[23]http://sourceforge.net/projects/serialport/

e. Debido a que el desarrollo para el manejo de puertos seriales se ha venido centrando para plataformas libres, hace que para la administración de puertos serie en Windows, sea necesario la descarga de unas librerías especiales para este propósito. Las librerías se llaman *libserialport.dll* y *libsoserialport.so*[24]y deben ser copiadas en la dirección donde se encuentra el proyecto (después de crear un proyecto nuevo).

f. Por último, queda el aprovechamiento de los conocimientos en este lenguaje.

3.6.2 Características. Para preparar la interfaz de usuario contemplando la funcionalidad que debía tener, es necesario como diseñador asumir un papel global acerca de las personas que van a rodear todo el sistema completo. Ser administrador, beneficiado e incluso como persona no habilitada para acceder a dicho recinto, hace parte de los roles que se deben contemplar y así, poder extraer características sociales y técnicas que debe tener la herramienta para su cómodo funcionamiento.

Básicamente la interfaz de usuario, tiene una ventana principal de acceso público con campos de texto en blanco que serán llenados al momento de reconocer una ID como permitida. La ventana se llama general y contiene la siguiente información: Apellidos, Nombres, Cargo, Oficina, Correo Electrónico, Teléfono, Último Ingreso, Última Salida y una fotografía digital en la parte superior derecha para un reconocimiento visual.

En esta misma ventana, en la parte inferior derecha, existe un botón con título Administrador, al ser presionado hace un bloqueo de la interfaz y solicitará el ingreso de la *Tag* identificado como administrador; al hacer la correspondiente verificación, de ser positivo, despliega opciones únicas para este usuario.

[24] http://code.google.com/p/giovynetserialport/downloads/detail?name=GiovynetDriver_1.1.zip&can=2&q=

Registro, donde se encuentran los datos del ingreso de todos los usuarios y al cual podrá acceder; y administración, donde podrá agregar nuevos usuarios, modificar la información personal o la asignación de un UC[25] y por último retirar los permisos de cualquier usuario.

A groso modo, este es en síntesis el funcionamiento de la herramienta. A continuación se describen las funciones contempladas para la elaboración y que servirán como guía para el ensamble de esta etapa.

3.6.3 Principales Funciones del Sistema

PuertosLibres

Verifica el hardware del computador y busca que puertos COM han sido asignados y están listos para ser usados.

PreparaPuertos

Crea un puerto virtual de comunicación con las características necesarias para la comunicación, como: Nombre del puerto y rata de baudios.

AsignaPuertos

Asigna la configuración hecha en *PreparaPuertos* a los puertos de comunicación de entrada y salida respectivamente. Estas son objetos de tipo Com.

EscuchaPuerto

Abre el puerto de comunicación de la entrada y queda en espera de empezar a recibir la información proveniente de la tarjeta de adquisición.

LeeID

Recibe y almacena la ID de la tarjeta inteligente *RFID*.

[25] UC, User Code del Tag

ComparaID

Compara dentro de la información interna de la interfaz, si la ID del *Tag* recibido, hace parte o no de las permitidas por el sistema.

TransResp

Envía hacia la tarjeta de adquisición un alto que describe el acceso permitido o un bajo como rechazo de la ID presentada como acceso denegado.

DatosFull

Descarga la información primaria del propietario de la tarjeta y con ella, completa los campos en la interfaz, haciendo una presentación del sujeto.

AdminLogin

Se activa cuando se quiere entrar con permisos de administrador. Verifica si el UC recibido corresponde al designado para la administración de la herramienta y de ser correcto, despliega las opciones individuales para este usuario: registro y administración.

Registro

Permite al usuario con todos los permisos, acceder al archivo de los beneficiados por el sistema de acceso. Aunque éste se encuentra habilitado para acceder a toda la información, los datos contenidos en esta región, no son medibles. El propósito es brindar contabilidad a la herramienta quitándole la posibilidad de alterar cierta información.

Administración

Permite Agregar más usuarios; asignando los *UC* por medio de las lectoras *RFID* y los datos personales en modo texto. La modificación de la información personal y de registro del *UC*, está contenida dentro de esta fase del diseño de la interfaz.

Por último el retiro de privilegios para cualquier usuario. También puede designar el roll de administrador para otros usuarios. Por seguridad, solo existirá un administrador; de tal forma que si se delega esta función a otro usuario, el primero pierde estos beneficios.

3.6.4 Diagrama de flujo. El diagrama de flujo se puede observar en el anexo A

4. PRUEBAS Y RESULTADOS

4.1 PRUEBAS DE FUNCIONAMIENTO DEL SISTEMA

Una vez configurados y programados los dispositivos de manera correcta se procede a hacer el acople y montaje de sistema para hacer las respectivas pruebas de funcionamiento.

En la Figura 19 se puede observar un montaje previo de la herramienta.

Figura 19. Montaje del Sistema

Fuente: Creada por los Autores

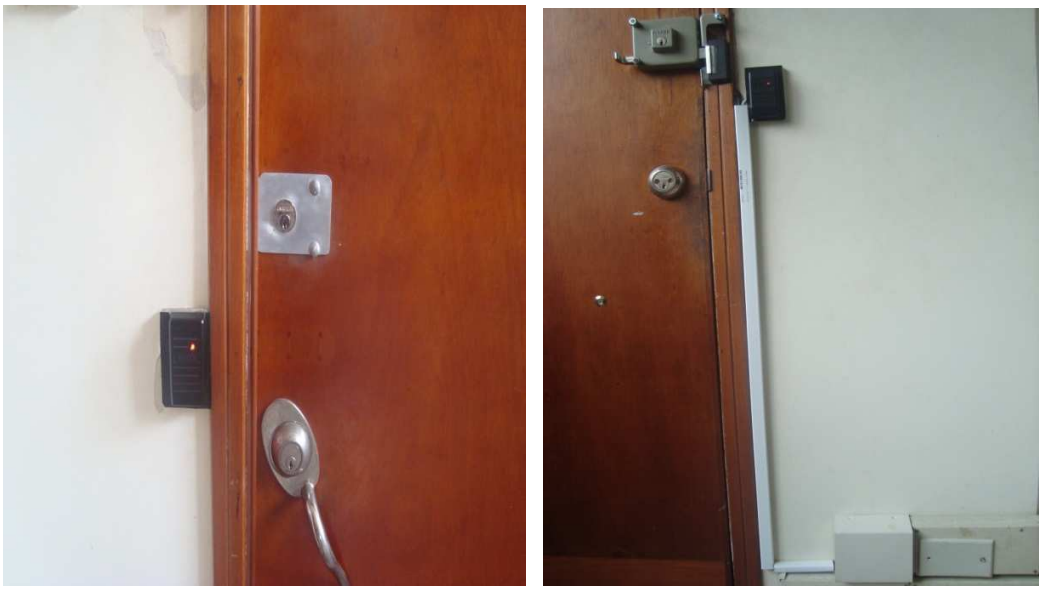
Para la realización de las pruebas, se necesitó de un ordenador con requerimientos suficientes para el buen funcionamiento del sistema. Este ordenador presenta las siguientes características.

- Procesador Intel Pentium: IV
- Velocidad del procesador:
- Memoria RAM: 512Mb

- Sistema Operativo: Windows XP

En la Figura 20 se observa el montaje final del sistema; este sistema se encuentra instalado en el salón 150 de laboratorios pesados donde realizan actividades los integrantes del grupo de investigación ERA.

Figura 20. Implementación Final del sistema



Fuente: Creada por los Autores

4.2 PRUEBAS DE CONECTIVIDAD

Inicialmente las pruebas de conectividad se realizaron con un programa sencillo generado a partir del Microcontrolador de envío de datos a través de módulo Bluetooth para verificar la conexión.

Esta prueba se realiza para verificar que los datos enviados estén llegando correctamente y no haya pérdida de información.

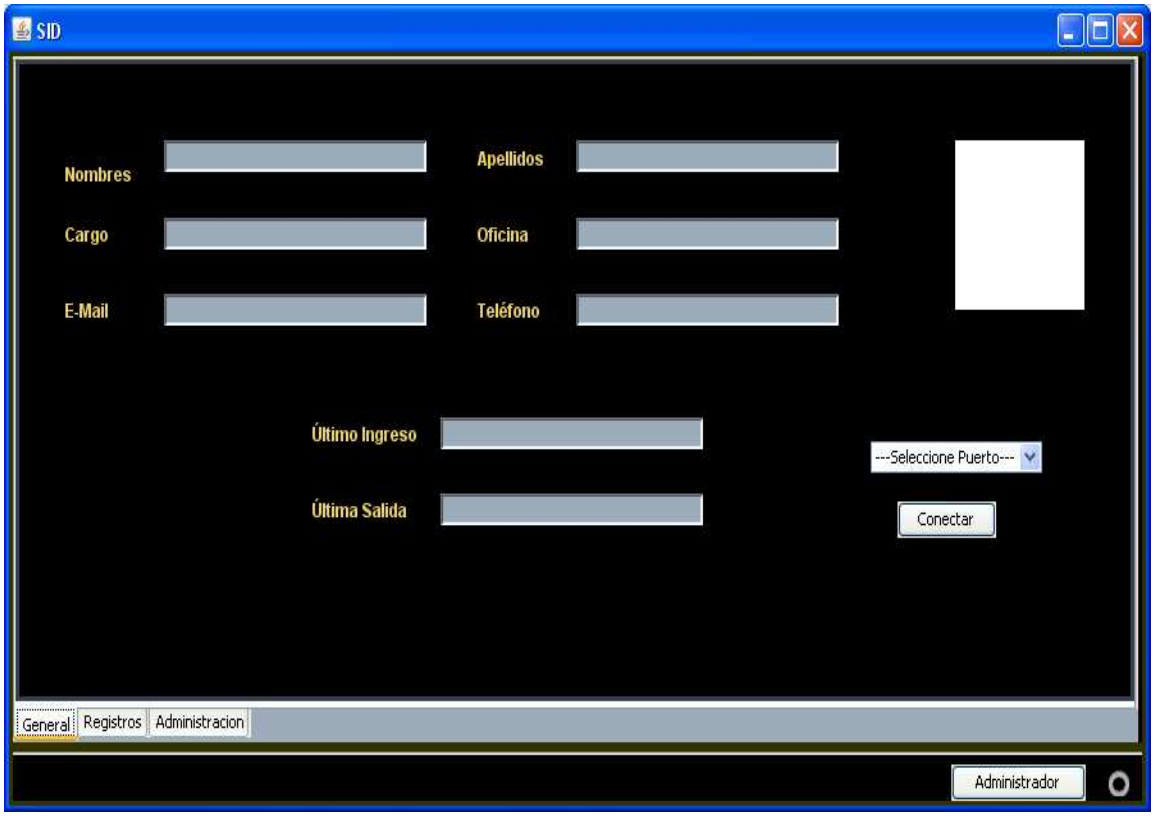
Para la realización de esta prueba se utilizó la herramienta de Hyperterminal del ordenador para visualizar los datos enviados por el módulo Bluetooth y de manera complementaria la comunicación bidireccional.

4.3 GENERALIDADES DE LA INTERFAZ

A continuación se observa la las principales características de la interfaz de usuario donde se detalla el funcionamiento y debido manejo.

4.3.1 Inicialización de la Interfaz. En la Figura 21 se muestra una imagen de la inicialización de la interfaz después de ejecutarse.

Figura 21. Inicialización de la Interfaz



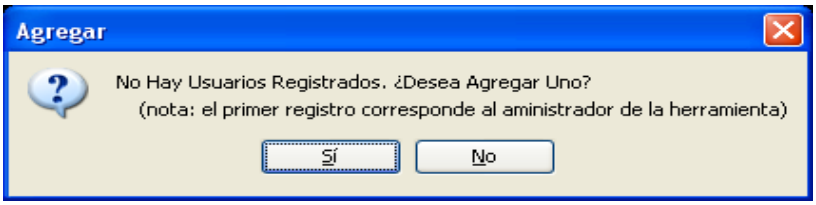
Fuente: Software de diseño de la interfaz, creada por los autores

En esta primera ejecución la herramienta posee una serie de casillas donde se muestran datos de registro del usuario que realiza una petición, previamente se debe establecer la conexión inalámbrica, escogiendo el puerto por el cual se desea comunicar y accionando conectar.

Una vez establecida la conexión, la opción de seleccionar puerto de comunicación desaparece.

Seguidamente aparece una cuadro de dialogo que se visualiza en la Figura 22 donde la interfaz realiza una aclaración a cerca del primer usuario registrado.

Figura 22. Registro del primer usuario.

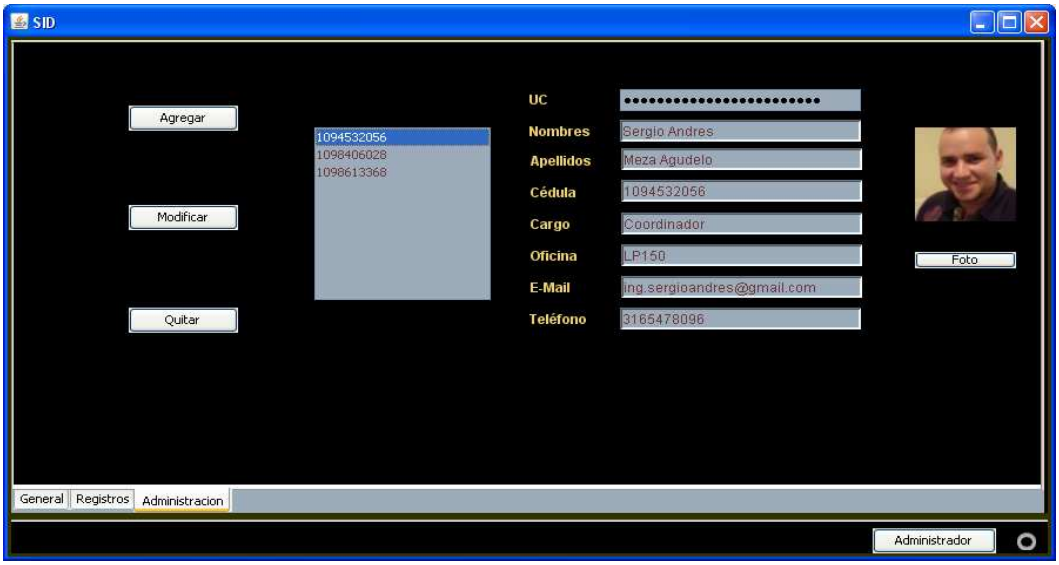


Fuente: Software de diseño, creada por los autores.

Como se pude visualizar, el primer usuario registrado es el administrador del sistema.

4.3.2 Adición de un usuario. Una vez inicializada la aplicación esta requiere el primer usuario que va a ejercer los papeles de administración. En la Figura 23 se muestra una imagen de esta sección de la aplicación.

Figura 23. Información del usuario a registrar



Fuente: Software de diseño

Para la adición de usuarios es necesario llenar toda la información correspondiente a los espacios visualizados en la interfaz. Una vez realizada esta operación la interfaz preguntara por la confirmación de los datos. En la Figura 24 se muestra una imagen de la confirmación de los datos.

Figura 24. Confirmación de los datos

Fuente: Software de diseño.

4.3.3 Funcionamiento general del sistema. Durante, el funcionamiento normal de la herramienta esta permanecerá en un modo de espera como se muestra en la Figura 25, en este modo la herramienta esta alerta a cualquier petición realizada por un usuario.

Figura 25. Acción de espera a petición de acceso.

Fuente: Software de diseño.

Una vez realizada una petición de acceso, la herramienta está en la capacidad de evaluar el código de donde proviene la solicitud y denegar o autorizar el acceso, como se muestra en la Figura 26.

Figura 26. Respuesta a una petición realizada

Fuente: Software de diseño.

Si la petición es favorable aparecerá una notificación de acceso concedido de lo contrario se notificara el acceso denegado.

Una vez concedido el acceso se visualizara la información del usuario asociado al ingreso, donde se registrara información tal como la fecha y hora de entrada.

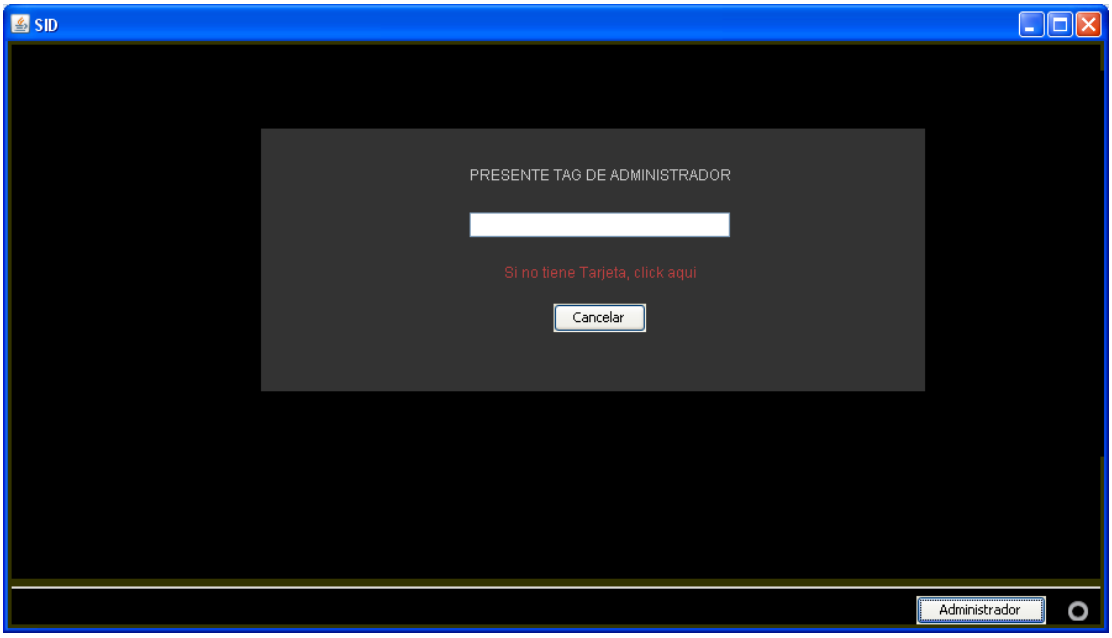
Figura 27. Identificación y acceso del usuario

Fuente: Software de diseño.

4.4 FUNCIONES ADMINISTRATIVAS

Como se mencionó anteriormente el primer usuario en registrar es el encargado de realizar las funciones administrativas de la herramienta. Para ingresar a la opción de administración basta con accionar el botón de administrador el cual lo remitirá un la ventana que se muestra en la Figura 28.

Figura 28. Acceso a administración



Fuente: Software de diseño

Para acceder a las funciones administrativas el usuario administrador debe presentar su *Tag* para habilitar estas opciones. Presentando el caso que el usuario administrador llegue a perder su *Tag* este puede ingresar por medio de un usuario y contraseña previamente registrada.

Las funciones administrativas se nombran a continuación.

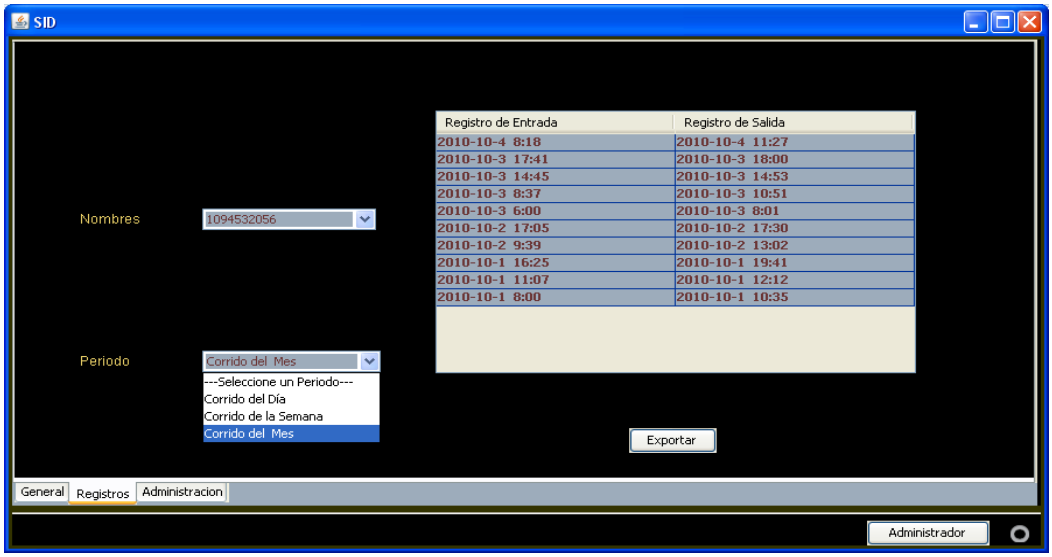
- Adición de usuarios
- Eliminación de usuarios
- Modificación de la información registrada de los usuarios
- Ingreso al registro de cada usuario.

4.5 REGISTRO DE USUARIOS

Cada vez que se realiza una petición de ingreso o salida, el usuario vinculado al sistema va almacenando un registro donde se detalla información de entrada y salida dentro determinados periodos de tiempo.

En la Figura 29 se muestra una imagen del registró de usuarios.

Figura 29. Registro de usuarios



Fuente: Software de Diseño.

El registro de la interfaz esta divido por periodos de tiempo las cuales son:

- Corrido del día
- Corrido de la semana
- Corrido del mes.

Para visualizar el registro de un usuario en general, se selecciona su número de identificación y el periodo de tiempo en el cual se desea conocer; una vez hecho

esto se muestra en pantalla el registro correspondiente a ese usuario. Adicionalmente este registro puede ser exportado a un documento compatible para aplicaciones deseadas.

CONCLUSIONES

Se diseñó e implementó una herramienta que permite controlar y registrar el acceso de personas vinculadas a un determinado sitio de trabajo.

La tarjeta de adquisición de datos diseñada e implementada está en plena capacidad de recibir, procesar, ordenar y transmitir los datos provenientes de los lectores RFID brindando un soporte confiable al sistema.

El software de diseño recibe, evalúa, contesta (acepto o rechazo) y registra los usuarios habilitados en tiempo real. Las funciones de adición, modificación, exclusión de usuarios, acceso y exportación del registro, corresponden a la administración de la herramienta, siendo éstas habilitadas con previa identificación.

Fue posible lograr la comunicación entre la tarjeta de adquisición y la interfaz de usuario bajo el sistema operativo Windows XP, después de la instalación de los controladores y configuración de puertos COM para los módulos Bluetooth. La herramienta completa se encuentra instalada en el salón LP 150 y la conexión Bluetooth se realiza a una distancia desde cualquier punto del salón.

Las pruebas realizadas de conectividad y transmisión de los datos por parte de la tarjeta de adquisición, muestran que son recibidos por el ordenador sin alteraciones en la información; garantizando una lectura confiable del *Tag* y una posterior confirmación de identidad.

Con la realización del proyecto, se presenta una solución de manera autónoma, didáctica y amigable en cuanto a la restricción de personal no autorizado para el acceso a un recinto, sitio o lugar de trabajo. La finalidad del este proyecto es

garantizar de manera confiable y segura el desempeño de todos los usuarios vinculados al sistema donde sea aplicada la herramienta.

RECOMENDACIONES

Al ejecutar una primera vez la interfaz de usuario, esta solicita la configuración del puerto designado por el sistema operativo y la adición de usuarios, quedando el primero de estos como el administrador de los servicios que ofrece el software.

Debido a que la herramienta cuenta con dos roles de acceso, permisos generales y administrativos, se recomienda al usuario administrador cerrar su sesión en cuanto termine de realizar los ajustes pertinentes dentro del sistema, para evitar cualquier tipo de manipulación por parte de personal no autorizado.

Durante el funcionamiento del sistema, es posible que el ordenador donde se ejecuta la interfaz de usuario, pierda el suministro de energía; para evitar que la herramienta quede bloqueando el acceso, la tarjeta de adquisición esta en la capacidad de identificar y evaluar la presencia de un Tag, concediendo o restringiendo el ingreso al usuario.

La comunicación inalámbrica del sistema por medio de los dispositivos Bluetooth es de suma importancia, por esta razón para que exista una conexión entre los módulos Bluetooth es necesario que estos se encuentren a la distancia correcta, ubicados dentro del rango de operación con la finalidad de que no exista una pérdida de información

BIBLIOGRAFÍA

[1] *Radio Frecuency IDentification (RF-ID)*
Smith, Roger. *RFID: A Brief Technology Analysis.* [En Línea] CTOnet.org. http://www.ctonet.org/documents/RFID_analysis.pdf [Consulta: 7 de Marzo]

[2] *RF-ID funcionamiento básico*
Llamazares, Juan Carlos. *¿Cómo funciona?: Tarjetas identificadoras sin contacto o sistemas RF-ID*.[En línea] http://www.ecojoven.com/dos/03/RFID.html [Consulta: 3 de Marzo 2006]

[3] MANZANARES ZÁRATE, Fabián. *Monitoreo de Personal mediante Tecnología GPS y control de horario*. Cartago 2006. Trabajo de Grado. Instituto Tecnológico de Costa Rica. Escuela de Ingeniería Electrónica.

[4] Java 2.0 Micro Edition, Soporte para Bluetooth

[5] RAMON ZARATE, Carolina: *Diseño e Implementación de Aplicaciones Bluetooth En Tiempo Real*. Bucaramanga. 2004. Trabajo de Grado. Universidad Industrial de Santander. Escuela de ingeniería Eléctrica, Electrónica y Telecomunicaciones.

[6] TRIGOS MARTINEZ, Miguel Angel: *Estado Del Arte Del Estándar Bluetooth en Aplicaciones de la automatización Industrial*. Bucaramanga. 2003. Trabajo de Grado. Universidad Industrial de Santander. Escuela de Ingeniería Eléctrica Electrónica y Telecomunicaciones.

[7] SANCHEZ G., Fernando Andrés, BUSTAMANTE M, Roberto, TELLEZ M., Juan Manuel *et al*. *Study of the Radio Channel in the ISM bands, UNII I/II, and the*

*interferences in the Hospital de la Samaritana***.** *rev.ing.* [online]. Jan./June 2006, no.23 [cited 06 November 2010], p.126-144. Available from World Wide Web: http://www.scielo.unal.edu.co/scielo.php?script=sci_arttext&pid=S0121 49932006000100016&lng=en&nrm=iso>. ISSN 0121-4993

[8] Modelo de referencia OSI: El modelo de referencia de inter conexión de sistemas abiertos (OSI, open system Interconnetion), creada por ISO, esto es un marco de referencia, para la definición de arquitecturas de interconexión de sistemas de comunicación.

[9] Página oficial
www.rfidpoint.com

[10] Página Estándares EPC global
http://www.epcglobalinc.og/standards

[11] Página Oficial de Información y Noticias
http://www.rfid-magazine.com/noticias

[12] Últimos avances
www.rfidjournal.com

[13] Fabricante Líder
www.hidglobal.com

ANEXOS

Anexo A. Diagrama de flujo programas principales

Diagrama de Flujo programa principal Tarjeta de adquisición

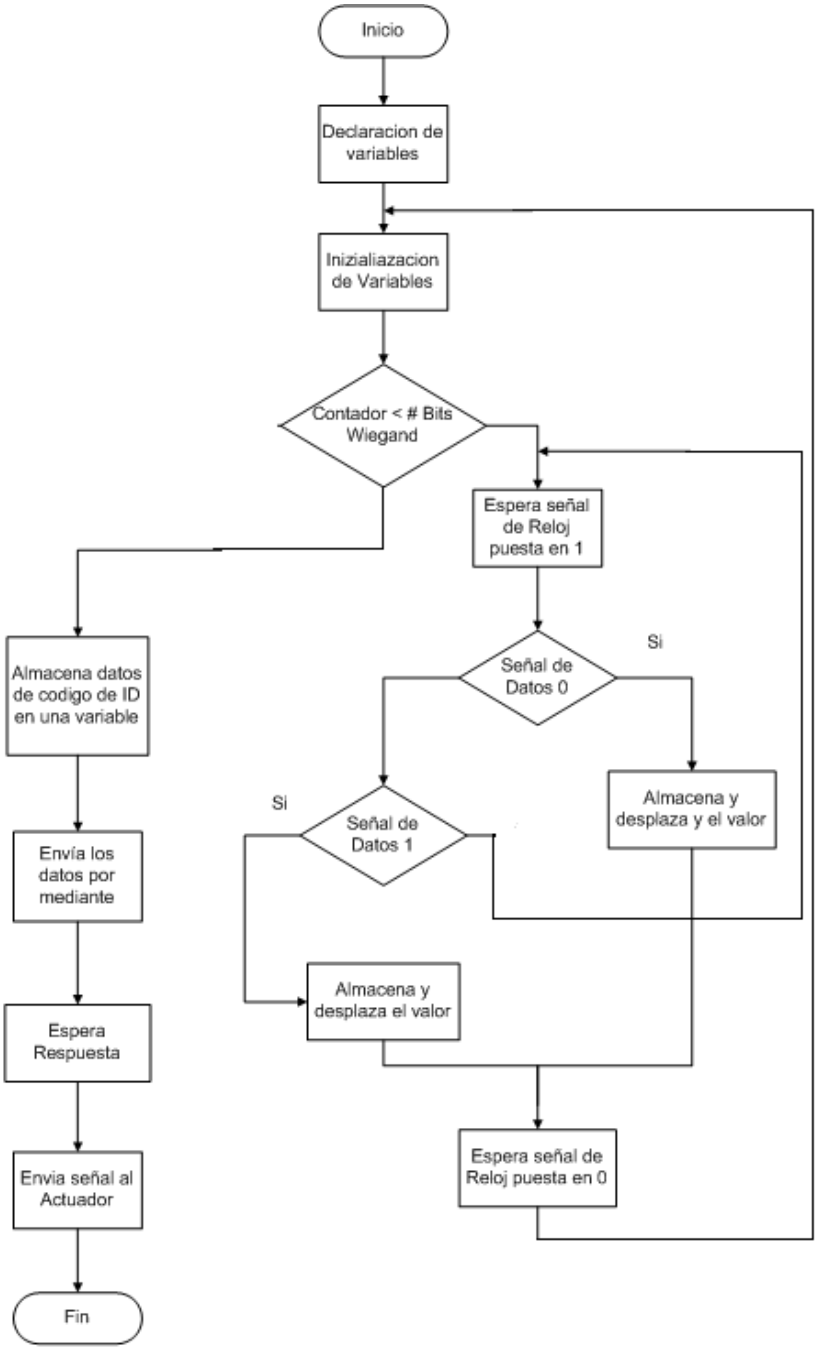
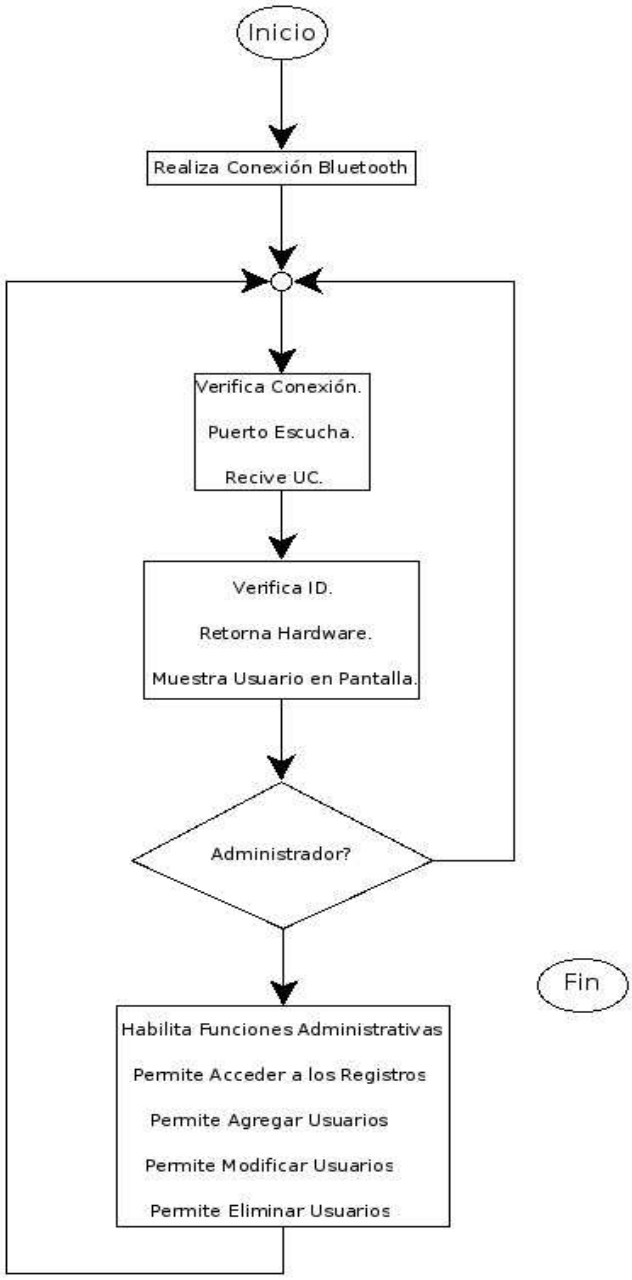


Diagrama de Flujo programa principal de la herramienta de software



Anexo B. Hoja de Datos Lector *RFID* HID

Application

HID's ProxPoint® Plus reader combines multiple configuration options with an attractive, inconspicuous design and economical price. Its secure potted electronics are ideal for both indoor and outdoor applications.

Features

- Features a beeper and multicolor LED which can be host and/or locally controlled.
- Enables various beeper and LED configurations, depending on individual site requirements.
- Can read HID cards with formats up to 85 bits.
- Designed for mounting directly onto metal with no change in read range performance.
- Available with either Wiegand or Clock-and-Data (magnetic stripe data) output.
- Compatible with all standard access control systems.
- Aesthetic design available in two cover designs and in four colors to match any decor.
- Includesmultilingualinstallation manual.

Features

Mounting Unobtrusive design can be mounted directly onto metal such as door mullions.

Audiovisual Indication Audiovisual indication: when a proximity card is presented to the reader, the red LED flashes green and the beeper sounds. The multicolor LED and beeper can also be controlled individually by the host system.

Diagnostics On reader power-up, an internal self-test routine checks and verifies the setup configuration, determines the internal or external control of the LED and beeper, and initializes reader operation. An additional external loop-back test allows for the reader outputs and inputs to be verified without the use of additional test equipment.

Indoor/outdoor Design Sealed in a rugged, weatherized polycarbonate enclosure designed to withstand harsh environments, providing reliable performance and a high degree of vandal resistance.

Easily Interfaced Wiegand output model interfaces with all existing Wiegand protocol access control systems. Clock-and-Data (magnetic stripe) model interfaces with most systems that accept magnetic stripe readers.

Security Recognizes card formats up to 85 bits, with over 137 billion unique codes.

Warranty Lifetime warranty against defects in materials and workmanship (see complete sales policy for details).

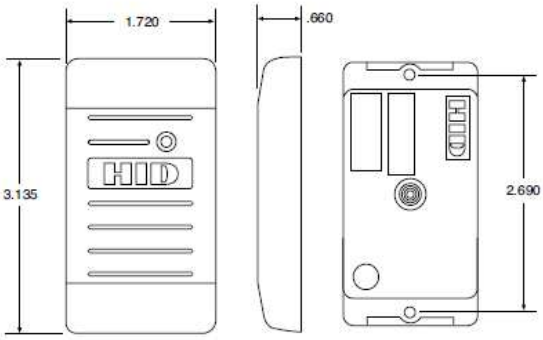
Part Numbers Base Part No.: 6005B Wiegand Interface
Base Part No.: 6008B Clock-and-Data Interface

Description Tri-State LED, Pigtail Connection

Options

- CLASSIC series cover in gray, beige, black or white (or)
- Designer series cover in grey, wave blue, black or white
- custom label
- custom embossing in housing

(Please see "How to Order Guide" for a description of options and associated part numbers).



Specifications

Typical Maximum* Read Range
ProxCard® II card - up to 3" (7.6 cm)
ISOProx® II card - up to 2.5" (6.35 cm)
DuoProx® II card – up to 2.5" (6.35 cm)
Smart ISOProx®/DuoProx® II cards – up to 2.5" (6.35 cm)
Proximity & MIFARE® card - up to 2.5" (6.35 cm)
ProxCard® Plus card - up to 1.0" (2.5 cm)
ProxKey® II keyfob - up to 1.5" (3.8 cm)
MicroProx® Tag - up to 2" (5.1 cm)
*Depending on local installation conditions.

Dimensions
3.135" x 1.720" x 0.660" (7.96 x 4.37 x 1.68 cm)

Material: Polycarbonate UL 94

Power Supply
5-16 VDC
Linear power supplies are recommended.

Maximum Current Requirements
Current (DC)
Average 30 mA, Peak 75 mA

Operating Temperature
-22° to 150° F (-30° to 65° C)

Operating Humidity
0-95% relative humidity noncondensing

Transmit Frequency: 125 kHz

Weight: 2.7 oz. (75 gm)

Environmental: IP55

Certifications
UL294/cUL (US), FCC Certification (US), IC (Canada), CE (EU), C-tick (Australia, New Zealand), SRRC (China), MIC (Korea), NCC (Taiwan), MIC (Japan), iDA (Singapore), RoHS

Cable Distance
Wiegand or Clock-and-Data interface:
500 feet (150 m)
Recommended cable is ALPHA 1295 (22 AWG) 5 conductor stranded with overall shield or equivalent.

© 2009 HID Global. All rights reserved. HID, and the HID logo are trademarks or registered trademarks of HID Global in the U.S. and/or other countries. All other trademarks, service marks, and product or service names are trademarks or registered trademarks of their respective owners. Rev. 05/2009

For best results, please print on recycled paper.

MKT-PROXPOINT_DS_EN

HID

ACCESS experience.

hidglobal.com

HID Global Offices:

Corporate North America
15370 Barranca Pkwy
Irvine, CA 92618

Asia Pacific
19/F 625 King's Road
North Point
Island East

Latin America
Circunvalacion Ote. #201 B
Despacho 2
Col. Jardines del Moral

Europe, Middle East & Africa
Haverhill Business Park
Phoenix Road
Haverhill

Anexo C. Redes Inalámbricas Radiopropagación e Interferencia

Tomado de: Trabajo de investigación. *Modelo de cobertura de redes inalámbricas de Interiores*. Universidad de Sevilla. España

Las redes inalámbricas ofrecen muchas ventajas, pero es inevitable considerar que también tienen algunos inconvenientes, como son:

Interferencias:

Por las características del medio usado, es inevitable darse cuenta que dispositivos que se encuentren en las cercanías de los nuestros, trabajando en esta banda, afectarán produciendo interferencias. Existe gran cantidad de dispositivos que trabajan en este segmento del espectro, hecho lógico, dado que éste es de uso libre. Las interferencias pueden provenir de otras redes inalámbricas próximas, efecto que se puede prevenir gestionando conjunta y adecuadamente las redes. Estas redes vecinas pueden estar usando cualquier otra tecnología que opere en el rango de los 2.4 GHz. Entre estos grupos está la tecnología Bluetooth, usada para interconectar equipos a corta distancia y baja capacidad.

Entre esta tecnología y las WLAN existen serios problemas de interferencias. A los sistemas de telecomunicaciones habría que añadir dispositivos que interfieren por trabajar en este rango de frecuencias tales como hornos microondas, algunos controles remotos de garajes, mandos a distancia y otros aparatos electrónicos. Cierto es que la mayoría de los fabricantes de estos productos tienen en cuenta este factor e intentan minimizar sus efectos. Así mismo, existen algunos radioenlaces que operan a la misma frecuencia que las redes inalámbricas y cuyo efecto, puede llegar a ser muy perjudicial, por lo que hay que tenerlos muy en cuenta a la hora de diseñar la red. Todas estas interferencias provocan que nuestra red inalámbrica no funcione a su más alto rendimiento.

- **Limitación en distancia:** El radio de acción de una red inalámbrica está limitado por la potencia máxima que se puede radiar según la legislación vigente. Para extender la zona de acción de la red sólo se puede añadir nuevos puntos de acceso o colocar repetidores.
- **Limitación en frecuencias:** Estamos confinados a un estrecho rango de frecuencias que son las de uso libre. Nuestro ancho de banda, a 2.4 GHz, está restringido a unos 100 MHz, que equivale a 3 canales. En la banda de 5 GHz, se tienen un total de 8 canales no solapados para Wi-Fi.
- **Seguridad:** Seguramente, este es el mayor inconveniente de las redes inalámbricas. Se debe diseñar nuestra red, con el nivel de seguridad más alto posible, para así evitar que usuarios no autorizados tengan acceso a nuestra red. Inicialmente, cuando se originaron los estándares de las redes inalámbricas no se prestó la suficiente atención a este concepto, quedando poco definido. En la actualidad, este es un tema prioritario, se trabaja en estándares que responden en exclusiva a la seguridad de las redes (como pueden ser el 802.11i ó el 802.1x).

El espectro electromagnético

El espectro electromagnético clasifica el conjunto de ondas existentes según su frecuencia y la magnitud de su longitud de onda. Se divide en diferentes zonas: las ondas de radiofrecuencia (con la mayor longitud de onda), las microondas, los rayos infrarrojos, la luz visible, los rayos ultravioleta y las ondas electromagnéticas con la menor longitud de onda: los rayos X y los rayos gamma.

Por otro lado, el espectro electromagnético se divide según la cantidad de radiación electromagnética que una determinada sustancia puede emitir o absorber, de forma que se puede usar para identificar una sustancia de forma similar a una huella dactilar. La magnitud de la longitud de onda de una sustancia es la inversa del valor de la frecuencia; por tanto, cuando la longitud de onda es mayor, la frecuencia será menor y viceversa. La relación entre ambas se expresa en la siguiente fórmula matemática:

Frecuencia(*KHz*) = 300.000(*km*/*s*)/*long*.*onda*(*m*)

La siguiente figura muestra la organización del espectro electromagnético, con la longitud de onda y los límites de frecuencia de cada zona. La longitud de onda se expresa en metros y la frecuencia en Hertzios (Hz).

Una vez que se ha estudiado el espectro electromagnético, la siguiente tabla muestra las bandas de frecuencia en las que operan las tecnologías inalámbricas, lo que ayudará en el siguiente apartado a conocer dónde se pueden producir las interferencias entre ellas.

Tabla 1. Relación de Bandas de Frecuencia

Tecnología inalámbrica	Bandas de frecuencias
NFC	13,56 MHz
IrDA	Espectro infrarrojo
Bluetooth	2,4 GHz
WiBree	2,4 GHz
ZigBee	2,4 GHz; 868 MHz en Europa y 915 MHz en EE.UU.
WiMedia UWB	3,1 a 10,6 GHz
Wireless USB	3,1 a 10,6 GHz
HomeRF	2,4 GHz
DECT	1,88 a 1,9 GHz en Europa y 1,92 a 1,93 GHz en EE.UU.
Wi-Fi	2,4 GHz
WiMAX	2 a 11 GHz (sin licencia) y 10 a 66 GHz (con licencia)
WiBro	2,3 GHz
GSM	900 MHz; 1,8 GHz y 1,9 GHz
GPRS	900 MHz; 1,8 GHz y 1,9 GHz
UMTS	2 GHz

Fuente: Trabajo de Investigación, Modelo de cobertura para redes inalámbricas de interiores

El principal problema reside en las denominadas bandas ISM *(Industrial, Scientific and Medical)*, como la de los 2,4 GHz, donde pueden estar operando hasta cinco tecnologías inalámbricas al mismo tiempo.

Además, otros dispositivos como los hornos microondas, los sistemas de vigilancia de bebés o los mandos de videojuegos inalámbricos también pueden utilizarla para funcionar.

Bandas ISM

Las bandas ISM son bandas reservadas internacionalmente para un uso no comercial. Éstas se corresponden con los rangos de frecuencias de 902-928 MHz, 2.400-2.483,5 MHz y 5.725-5.850 MHz y fueron definidas por la ITU en el artículo 5 de las Regulaciones de Radio, concretamente en los puntos 5.138 y 5.150. Su uso es abierto sin necesidad de licencia gubernamental, respetando las regulaciones que limitan los niveles de potencia transmitida. La tecnología Wi-Fi, Bluetooth, WiBree, ZigBee y HomeRF son ejemplos de tecnologías que usan estas bandas de licencia libre.

Otros dispositivos utilizan también estas bandas, como los hornos microondas, los abridores de puertas de garaje, los sistemas de vigilancia de bebés o los teléfonos inalámbricos en EE.UU. y América del Sur.

Espectro ensanchado

El espectro ensanchado es un método de transmisión de datos en el cual la información de interés se distribuye sobre un ancho de banda mucho mayor que el convencional, usando un nivel muy bajo de potencia y un alto nivel de protección de interferencias. Para ello, la información no se transmite usando una única frecuencia o canal, sino que usa toda la banda de frecuencias disponible, con lo que se minimizan las posibilidades de que la frecuencia de operación coincida con las de otros dispositivos que puedan estar activos en el mismo instante. Existen

dos variantes de este método: *Frequency Hopping Spread Spectrum* (FHSS) y *Direct Sequence Spread Spectrum* (DSSS).

Espectro ensanchado por salto de frecuencia

El FHSS fue el primer método de espectro ensanchado. Consiste en emitir una señal sobre una serie de frecuencias aleatorias, saltando de una frecuencia a otra de forma síncrona aproximadamente unas 1.600 veces por segundo. Por tanto, se utiliza toda la banda de frecuencias disponible y no una única frecuencia o canal (*Hopping Pattern)*. Esta transmisión ofrece ventajas de seguridad y minimiza la posibilidad de la generación de interferencias debido al cambio de canal. El estándar IEEE 802.11 es uno de los más importantes que usan este método, aunque la tecnología que sobresale es Bluetooth, que utiliza la banda de frecuencia libre de los 2,4 GHz, organizada en 23 frecuencias con un ancho de banda de 1 MHz cada una.

A continuación se presentan las tres principales ventajas del método FHSS:

1. Las señales son altamente resistentes al ruido y a las interferencias.
2. Las señales son difíciles de interceptar. Una transmisión de este tipo se percibe como un ruido de corta duración o como un incremento en el ruido para cada dispositivo que no esté usando la secuencia enviada por el emisor.
3. Este tipo de transmisiones pueden compartir una banda de frecuencias con muchos tipos de transmisiones inalámbricas simultáneas y una mínima interferencia.

Espectro ensanchado por secuencia directa

A diferencia de FHSS, DSSS es un método de transmisión de datos que no necesita enviar la información a través de varias frecuencias. Añade bits adicionales a los paquetes de información enviados al receptor, que es el único que conoce el algoritmo de estos bits y es capaz de descifrar los datos. Estos bits

adicionales permiten a DSSS transmitir información a una velocidad de 10 Mbps y a una distancia máxima entre dispositivos de 150 m. Una de las tecnologías que sobresalen usando este método es Wi-Fi (IEEE 802.11).

Salto de frecuencia adaptativo

Otro método para minimizar las interferencias entre dispositivos inalámbricos es el denominado Salto de Frecuencia Adaptativo (AFH) que, aunque no se engloba dentro de los métodos de espectro ensanchado, sigue en parte su misma filosofía. Utiliza la frecuencia disponible dentro del espectro detectando los dispositivos activos y descartando las frecuencias que están utilizando. Una vez localizada la porción del espectro que puede ser usada, su comportamiento es similar al de FHSS. Este salto adaptativo permite unas transmisiones más eficaces dentro del espectro, de forma que se mejora el funcionamiento del dispositivo, incluso si hay más de una tecnología inalámbrica funcionando a la vez.

Modelo de interferencias

La continua expansión de las tecnologías inalámbricas y la utilización del espectro de radiofrecuencia hace que se presente un problema unido al uso de estas tecnologías: las interferencias, que pueden producir efectos negativos sobre el rendimiento de las redes inalámbricas. En este apartado se demuestra la influencia entre las tecnologías inalámbricas más extendidas y los dispositivos inalámbricos cuando se encuentran funcionando en el mismo entorno, haciendo hincapié en los entornos de interiores, mostrando las variaciones producidas en su rendimiento.

Los resultados obtenidos en las pruebas experimentales permiten comprobar cómo con un horno microondas o con un sistema de vigilancia de bebés puede ponerse en peligro el rendimiento de la red corporativa de una organización o la red doméstica de cualquier hogar donde los dispositivos inalámbricos son ya muy abundantes.

Definición de interferencia

El término interferencia presenta diversas acepciones, dependiendo del contexto en el que se utilice:

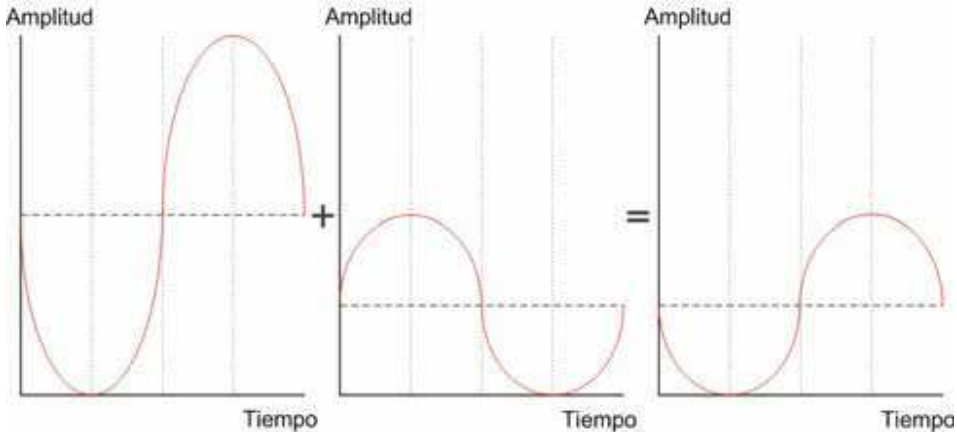
- En telecomunicaciones y aéreas afines, es cualquier proceso que altera, modifica o destruye una señal en el canal existente, entre el emisor y receptor.
- En mecánica ondulatoria, es el resultado de la superposición de dos o más ondas, de forma que se crea un nuevo patrón de ondas.

En electromagnetismo, es la perturbación sobre cualquier circuito eléctrico causada por la radiación electromagnética proveniente de una fuente externa. Se conoce también como *EMI (ElectroMagnetic Interference)* o *RFI (Radio Frequency Interference)*.

El Principio de Superposición de Ondas establece que la magnitud del desplazamiento ondulatorio en cualquier punto medio es igual a la suma de los desplazamientos de todas las ondas presentes en ese mismo punto. De este modo, si dos ondas se encuentran desfasadas, se interferirán destructivamente resultando una nueva onda de menor amplitud, como se puede observar en la Figura 6. En el contexto de las tecnologías inalámbricas, se pueden producir interferencias si utilizan las mismas frecuencias o la misma área del espectro electromagnético (canales).

Los materiales existentes en el entorno en el que se encuentran funcionando las tecnologías inalámbricas pueden influir sobre la comunicación.

Figura 1. Interferencia de dos ondas desfasadas.



Fuente: Trabajo de investigación, Modelo de cobertura para redes inalámbricas en interiores

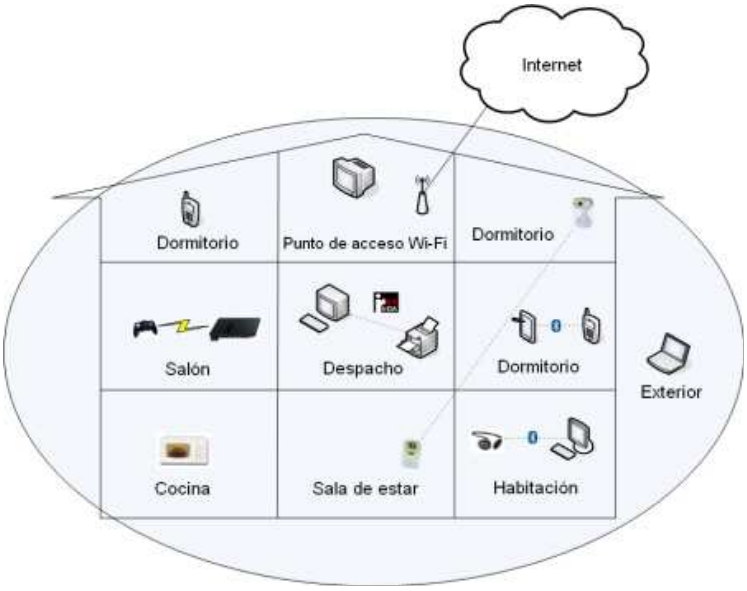
Estudio experimental de las interferencias

En este apartado se muestran los resultados obtenidos en un estudio de investigación desarrollado por miembros del Grupo de Investigación GITACA de la Universidad de Extremadura, a través del proyecto “Estudio analítico y evaluación de los efectos entre tecnologías de comunicaciones inalámbricas”.

El objetivo principal de esta investigación es obtener resultados fundamentados que permitan conocer el nivel de impacto existente entre las diferentes tecnologías de comunicaciones inalámbricas. Además, se pretende conocer qué tecnologías o dispositivos inalámbricos son más propensos a producir interferencias y disminuir el rendimiento de las redes. Para conseguirlo, se ha utilizado un software que calcula el aumento o caída de rendimiento de las redes inalámbricas cuando se producen interferencias causadas por otros dispositivos. También ha sido necesario realizar un estudio completo de las características de las tecnologías inalámbricas, como el alcance, el *throughput* (volumen de información que fluye en la red inalámbrica) y la frecuencia, así como un estudio del espectro electromagnético con sus diferentes regiones y las zonas en las que estas tecnologías operan.

En la siguiente figura se puede observar lo que puede ser un escenario general del ámbito en el que se han realizado las pruebas. En ella se observa una situación cotidiana que se puede dar hoy en día tanto en domicilios como en organizaciones: se trata de un domicilio de tres plantas con acceso a Internet y un punto de acceso Wi-Fi que proporciona cobertura tanto en el interior como en los exteriores más cercanos. De este modo, las personas que vivan en una casa como ésta pueden establecer simultáneamente una conexión Wi-Fi, enviar un archivo vía Bluetooth desde un teléfono móvil a un Pocket PC o escuchar música con los auriculares Bluetooth. Por otro lado, también pueden activar un sistema de vigilancia de bebés para tener lo controlado mientras duerme en el piso superior, jugar con la videoconsola usando un mando inalámbrico o utilizar el horno microondas.

Figura 2. Ejemplo de domicilio típico



Fuente: Trabajo de investigación, Modelo de cobertura para redes Inalámbricas de interiores.