UNIVERSIDAD DE SONORA

DIVISIÓN DE INGENIERÍA
Departamento de Ingeniería Industrial

CONTROL DE ACCESO INTELIGENTE A LAS AULAS DEL DEPARTAMENTO DE INGENIERIA INDUSTRIAL

TESIS

Que para obtener el Título de:

INGENIERO EN MECATRÓNICA

PRESENTA:

FRANCISCO VÁZQUEZ GUERRERO

Hermosillo, Sonora. Diciembre 2015

Universidad de Sonora

Repositorio Institucional UNISON

Resumen

Control de acceso inteligente a las aulas de departamento de ingeniería industrial

Diciembre de 2015

Francisco Vázquez Guerrero

Existen varias soluciones en el mercado para sistemas de control de acceso, sin embargo estas soluciones son genéricas y por lo general la tecnología que se utiliza es propietaria. Lo anterior conlleva a gastos innecesarios en partes de la tecnología que no se usará, ligarse a un solo proveedor y pagar costos excesivos de mantenimiento. Estos son algunos de los problemas que se pueden solucionar implementando un sistema modular de control de acceso que tome en cuenta el ambiente en el cual se utilizará.

El presente trabajo muestra el desarrollo de un sistema inteligente de control de acceso diseñado para las aulas del Departamento de Ingeniería Industrial de la Universidad de Sonora. El sistema fue elaborado con componentes de hardware y software abiertos y fue probado utilizando los requerimientos de desempeño establecidos por la administración y se obtuvieron resultados satisfactorios. Dentro de las características que destacan al presente trabajo se encuentra el desarrollo de una guía de mantenimiento correctivo que puede ser empleada por personal sin experiencia con el manejo de tecnología.

Contenido

Capítulo 1

Planteamiento del problema

1.1 Antecedentes

El control de acceso es la habilidad de permitir o denegar el uso de un recurso en una entidad en particular. Los mecanismos para el control de acceso pueden ser usados para cuidar recursos físicos, como el acceso a las aulas, donde maestros y alumnos tienen permitido el ingreso al espacio; recursos lógicos, como una cuenta de banco, de donde solamente determinadas personas pueden extraer dinero; o recursos digitales, donde un archivo informático solo puede ser leído pero no modificado.

En la actualidad son muchos los sistemas de control de acceso electrónicos en el mercado, pudiéndose encontrar desde lectores de retina, tarjetas pre-programadas, hasta programas informáticos, pero realmente la diferencia está en el cumplimiento de las expectativas de los usuarios. Un sistema de control de acceso es fácil de conseguir, tan solo se requiere un teclado y una cerradura eléctrica y solamente accederán aquellas personas que conozcan la clave. Pero esto ya no es suficiente, puesto que al paso del tiempo la clave es conocida y lo que en un principio era un control de acceso termina convirtiéndose en un simple mecanismo para abrir puertas. Existen controles de acceso que usan sistemas de identificación por radio frecuencia (RFID por sus siglas en inglés), el cual es un sistema de almacenamiento y recuperación de datos remoto que utiliza dispositivos denominados tarjetas RFID [1]. El propósito fundamental

de la tecnología RFID es transmitir la identificación de un objeto (similar a un número de serie) mediante ondas de radio.

La aplicación de la tecnología RFID para el control de acceso ha sido muy versátil en nuestra década; sin embargo cuando se habla del acceso a un aula con bienes inmuebles y tecnología para educación, cambia la dinámica ya que se pueden emplear varias técnicas desde utilizar una cerradura eléctrica, utilizar una llave común, presionar un botón o lo más básico, que un encargado o auxiliar permita el acceso al área. Todas estas acciones toman tiempo, sin mencionar que en ocasiones los sistemas se dañan o deterioran [1].

Con el paso de los años, la tecnología ha evolucionado, de tal modo que ahora es posible interconectar prácticamente cualquier objeto de tecnología a la red y poder obtener datos de este así como poder controlarlo. Esta versatilidad, ha evolucionado en lo que se conoce como Internet de las Cosas (IoT por sus siglas en inglés), concepto que nace en MIT en 1999, donde se realizaban investigaciones en el campo de la identificación por radiofrecuencia en red (RFID) y tecnologías de sensores [2]. Esto es un precedente para impulsar el siguiente trabajo de tesis hacia la creación de un sistema inteligente para control de acceso a las aulas de departamento de Ingeniería Industrial de la Universidad de Sonora.

1.2 Problema actual

Los servicios de control de acceso en el estado de Sonora son manejados por pocas empresas, entre ellas Control Inteligente, seguritech integral security, grupo sertres, entre otras [3]. Sin embargo estas empresas no cuentan con el capital humano necesario para cubrir las necesidades en todo el estado y brindar un servicio de calidad, además de que no están dedicadas al 100% al control de acceso sino que además ofrecen servicios de seguridad, es decir, actúan cuando una persona no autorizada ha ingresado al lugar, en este sentido, no son especialistas en el área. Por otra parte, las empresas que trabajan más apegados al área de control de acceso, no ofrecen capacitación para el manejo de sus productos y/o su garantía es limitada.

En el Departamento de Ingeniería Industrial de la Universidad de Sonora, se cuenta con controles de acceso automatizados para las aulas. Dichos controles han comenzado a fallar y la empresa que ha instalado los equipos, argumenta que el sistema requiere una actualización más que un mantenimiento. Dicha actualización consiste en la instalación de un nuevo sistema de control de acceso del cual no se tienen garantías ni capacitaciones ni siquiera un manual de procedimientos para aplicar un mantenimiento correctivo. La tecnología que se utiliza en los controles de acceso actual es RFID, sin embargo es de baja frecuencia, lo que hace que el sistema no sea óptimo para el control de acceso. La figura 1.1 muestra el Controlador actual de las aulas del Departamento.

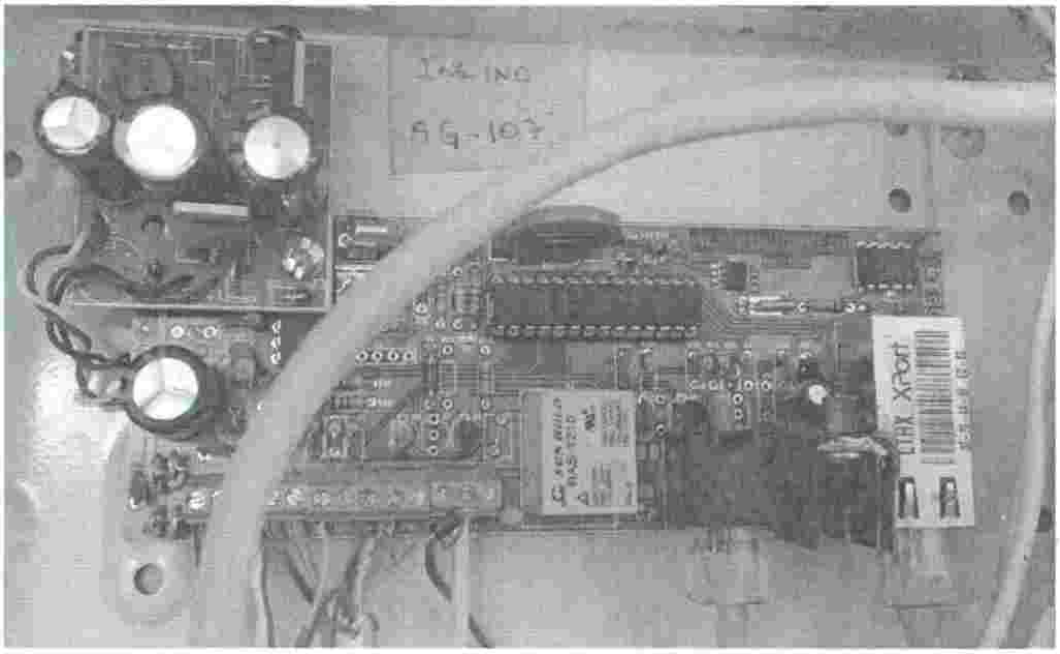

Figura 1.1. Controlador actual

Se realizó una evaluación en uno de los controles de acceso que habían dejado de funcionar, específicamente el control del aula 5G-201 del departamento de Ingeniería Industrial de la Universidad de Sonora. La razón aparente del mal funcionamiento fue sobrecalentamiento pues una de las resistencias del lector estaba quemada. Esto se puede deber a un sobre voltaje, corrientes parásitas o a que se calienta mucho en verano cuando la luz del sol llega directamente al lector. Por otra parte las instalaciones de esta aula tienen varios detalles, por ejemplo, el cable que instalaron para la lectora está ahogado en el concreto (sin tubería) como se muestra en la figura 1.2.

Figura 1.2. Cableado del lector de tarjetas hacia el controlador aula 5G-201

Esto afecta tanto la vida útil del cableado como la de los equipos instalados ya que normalmente induce corrientes parásitas o se crean falsos y/o corto-circuitos. Otra situación fue el suministro eléctrico, aquí tratamos de tomar la corriente del contacto pero de nuevo, los cables de corriente están ahogados en el concreto (hasta cierto punto llegan con canaletas y de allí se ahoga el cable en el concreto) como se puede apreciar en la figura 1.2.

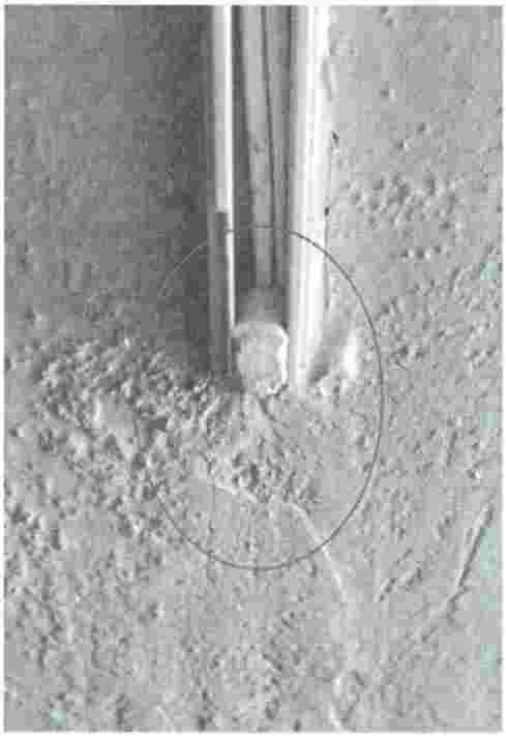

Figura 1.3. Cableado eléctrico en la pared del lado este del edificio 5G-201

1.3 Objetivo general

Para una correcta instalación y reemplazo de sistema de control de acceso, se requiere:

- Instalar tubería. Lo cual, aparte de ser lo correcto, ayudará a que el mantenimiento sea ágil, por ejemplo, si el cable de datos falla, se puede reemplazar sin tener que perforar o ranurar de nuevo la pared.
- Instalar el cableado adecuado. Muchos de los cables que se utilizan en el sistema original (de la empresa) no son del calibre adecuado, por ejemplo el cableado de corriente alterna es de calibre 18 cuando lo que se requiere es un calibre 14 (mas grueso).
- Cambiar los dispositivos lectores. Las tarjetas que se utilizan actualmente en el departamento son de tecnología anterior y muchos de los equipos nuevos no las leen, además el precio de las lectoras de tarjetas va desde los 3 hasta los 5 mil pesos. Una lectora de nueva generación como la instalada en el 5G-201 cuesta alrededor de 500 pesos.
- Cambiar la caja controladora. La caja actual es de buen material pero la fuente del controlador y sobre todo el módulo de comunicación con la red, se calientan y hay fluctuaciones de corriente.

1.4 Hipótesis

Es posible diseñar e implementar un sistema de control de acceso inteligente con comunicación centralizada cuyo mantenimiento sea sencillo, para las aulas del Departamento de Ingeniería Industrial de la Universidad de Sonora.

1.5 Delimitación

El presente trabajo se limita al diseño e implementación y pruebas de un controlador, además de la creación de un manual de mantenimiento para el sistema diseñado.

Capítulo 2

Estado del arte

2.1 Control de acceso biométrico

Un sistema de Control de Acceso Biométrico se define como aquel sistema encargado de restringir selectivamente el acceso de personas a recursos basándose en las posibilidades de las biometrías. Por ejemplo, supongamos que en una prisión estatal se desea controlar a los funcionarios que acceden al recinto para evitar riesgos de seguridad. Un sistema de control de acceso biométrico podría consistir en unas puertas de seguridad situadas a la entrada de la prisión (o de las zonas seguras dentro del recinto). Las puertas se abrirían cuando un funcionario autorizado presentara adecuadamente su iris. Una cámara capturaría una imagen del iris y determinaría si se trata de una persona con derechos de acceso, abriendo en este caso la puerta [4].

2.1.1 Control de acceso biométrico simple: una joyería más segura

Vamos a imaginar que la joyería LA GEMA SEGURA, propiedad de la familia Tévez, tiene una sala trasera donde se guardan las joyas de mayor valor. Actualmente la puerta se abre con llave, pero esto significa que la llave se puede copiar y que se puede utilizar en cualquier momento y por cualquier persona. No inspira confianza. Además no hay manera de conocer

cuándo un empleado ha abierto la puerta de la sala. Los Tévez quieren más seguridad, para lo cual podrían implementar un control de acceso biométrico que les permita lo siguiente:

- Para abrir la sala de seguridad es necesario estar registrado previamente como usuario del sistema, bien como empleado autorizado, bien como propietario. La puerta de seguridad de la sala se abre presentando la huella dactilar del usuario registrado.
- Los empleados autorizados únicamente pueden abrir la sala en horario comercial. Si se intenta abrir fuera del horario comercial saltará una alarma.
- Los propietarios pueden abrir la sala fuera del horario comercial. Pero en este caso, además de presentar su huella dactilar, tendrán que indicar un código secreto de seis cifras.
- El sistema registra todos los accesos a la sala, tanto exitosos como fallidos. Así los dueños pueden monitorizar cuándo y quién ha abierto la puerta.

2.1.2 Control de acceso biométrico complejo: planta de producción química

Imaginemos ahora la empresa química Chemistry 4 Security, centrada en componentes químicos utilizados para sistemas de seguridad del Ejército. Tiene una vasta planta productiva en la que trabajan múltiples equipos de personas. El acceso a la información y a los componentes químicos es muy sensible. La jerarquía de permisos a cada uno de ellos es compleja y se hace necesario un sistema de seguridad que controle adecuadamente el acceso a cada sala de producción dentro de la fábrica. Con un sistema de control de acceso biométrico centralizado se podrían orquestar óptimamente los accesos de los individuos. En función de la criticidad de cada componente químico, se podría requerir la presentación de un tipo de biometrías concreto. Por ejemplo, el acceso general a la planta podría gestionarse con tornos que se accionaran mediante la huella dactilar de los trabajadores. Para las salas de alta seguridad se podría exigir fusión biométrica de las biometrías de iris y vascular en las esclusas de acceso.

Además el sistema central tendría constancia en todo momento de la ubicación de cada trabajador mediante tarjetas RFID portadas por los empleados. Impediría acciones imposibles,

como puede ser el acceso a una sala de alta seguridad por parte de un empleado que no haya accedido a la planta ese día. O mandaría alertas ante situaciones anómalas como puede ser la congregación de muchas personas en una zona de paso.

2.1.3 Control de acceso biométrico: caso español en aeropuertos

Y seguimos con los ejemplos. En España tenemos una clara muestra de un control de accesos biométrico en funcionamiento. El ABC System, presente en los aeropuertos de El Prat y de Barajas, se encarga de controlar el tránsito de pasajeros. Concretamente, en cada puerta de acceso que conforma el sistema, se revisa la autenticidad del DNI electrónico o pasaporte electrónico y se verifica biométricamente que la persona en tránsito es el dueño de dicho documento. Para ello se comparan la imagen facial y la huella dactilar con muestras guardadas electrónicamente en el documento de identidad. Se restringe el paso de la persona en el caso de que la documentación esté falsificada, expirada o no sea propiedad del sujeto.

2.1.4 Suite de control de acceso biométrico

En Dolthink han desarrollado una Suite avanzada de Control de Accesos que permite adaptarse a cualquier necesidad del mercado. Integra biometrías, verificaciones documentales y un potente motor de reglas para que los gestores del sistema tengan el mayor grado de personalización posible. De esta manera la Suite es apta tanto para sistemas simples autónomos en pequeños negocios, como para complejos entornos distribuidos en los que se requiera una continua monitorización y unos requisitos de acceso cambiantes.

2.1.5 Control de acceso vehicular

Los sistemas de control de accesos vehicular se implementan para tener el control de los vehículos que circulan por un espacio público o privado, asegurando el paso a los vehículos

permitidos y restringiendo a aquellos que no estén autorizados. Al integrar un sistema de control de accesos vehicular, se puede tener el control total, tanto de los residentes como de los visitantes.

Se brindan soluciones en la automatización electromecánica para sistemas de parking y barreras de estacionamiento de medianas y grandes dimensiones. Soluciones potentes y versátiles que representa al máximo la fiabilidad y la tecnología de los mejores controles de acceso vehicular del mundo. Diseñan sistemas para las exigencias más complejas, tales como el uso intensivo, típico de las aplicaciones en las instalaciones comunitarias o industriales.

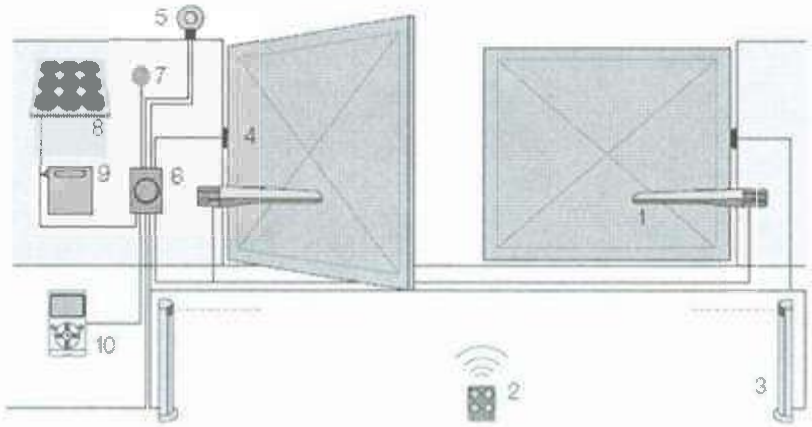

Figura 2.1 Diagrama de control de acceso vehicular

Se cuentan con todos los sistemas electromecánicos necesarios para integrar una solución completa y robusta, integrando todos los sistemas de control de accesos necesarios para satisfacer cualquier tipo de exigencia. Se integran sistemas biométricos de identificación, sistemas de visión artificial para reconocimiento de placas, sistemas de identificación por radio frecuencia para activar las puertas sin necesidad de abandonar los vehículos.

- Mayor control de entradas y salidas, horarios, grupos de acceso, zonas permitidas.
- Base de datos con toda la información necesaria.
- Ingreso de automóviles de forma controlada y organizada.
- Reconocimiento de placas para aplicaciones de avanzadas.
- Asociación de las placas con la identificación del conductor para mayor seguridad.

- Reconocimiento de TAGs RFID para aplicaciones manos libres.
- Alertas en caso de un intento de acceso sin autorización.
- Integración con todos los sistemas de seguridad para una gestión centralizada.

2.1.6 Control biométrico

En el sistema de control de acceso vehicular es posible utilizar lectores biométricos, tarjetas de control, claves y combinaciones. Estos sistemas biométricos pueden ser instalados estratégicamente teniendo en cuenta el fácil posicionamiento de cada vehículo y el diseño de la instalación. En efecto, se realiza el diseño del pedestal personalizado para cada instalación teniendo en cuenta factores de accesibilidad, exposición a la lluvia y al sol, protección del mismo dispositivo y facilidad en la autenticación de cada usuario. Cada sistema biométrico se comunica con el software de gestión para tener un control de accesos vehicular completo con todas las funcionalidades.

Figura 2.2 Ejemplos de control biométrico

Ventajas:

- Autenticación con huella dactilar, tarjetas de proximidad y/o clave
- Integración con todos los sistemas de seguridad del edificio

- Software intuitivo para administración del sistema
- Pedestales personalizados para cada solución
- Integración con los dispositivos electromecánicos

Aplicaciones:

- Entradas vehiculares a conjuntos residenciales, edificios y oficinas.

2.2 Aplicaciones automotrices

El sistema de reconocimiento de placas es una solución para un control de accesos vehicular. El reconocimiento de matriculas se hace de forma automática sin necesidad de un operario. El sistema tiene en cuenta los diferentes niveles de luminosidad que se puedan presentar a diferentes horas del día, los diferentes posicionamientos de los carros, condiciones de intemperie, deterioro de las placas, diferentes alturas y en general todas las variables que puede presentar el sistema. Las cámaras con visión artificial se complementan con a los sistemas electromecánicos para poder realizar un acceso vehicular seguro, personalizado y de acuerdo a las necesidades específicas del proyecto. Es posible asociar el sistema a un generador de tickets o un lector de huella dactilar del conductor para una mayor seguridad [5].

Figura 2.3 Sistema de reconocimiento de placas

Ventajas:

- Activación de puertas y barreras automáticamente
- Integración con tickets o huellas dactilares
- Notificación de placas no autorizadas
- Notificación intento de hurto
- Integración con todos los sistemas de seguridad
- Consulta y registro en base de datos

Aplicaciones:

- Centros comerciales
- Parking
- Edificios comerciales
- Edificios y conjuntos residenciales
- Edificios de oficinas

2.2.1 Acceso vehicular RFID identificación por radio frecuencia

La solución RFID realiza una identificación del vehículo por radiofrecuencia, esto quiere decir que no hay necesidad de bajarse del carro o sacar la mano por la ventana pará autenticarse o entregar dinero a una operadora. Una antena ubicada estratégicamente lee el TAG o Etiqueta que se encuentra en el vehículo. El sistema de control de accesos vehicular basado en RFID permite un acceso vehicular al mismo tiempo que acciona los sistemas electromecánicos, de esta forma el conductor no tiene que detenerse. Es un sistema muy eficiente para lugares en los cuales no es necesaria la identificación del conductor y la asociación del mismo con el carro. Sin embargo, si es posible identificar el carro y para soluciones en peajes se puede saber el saldo con el que cuenta el TAG para permitir el paso automático o negarlo.

Ventajas:

- El vehículo no se tiene que detener
- Agiliza el transito

- No hay necesidad de sacar la mano por la ventana
- Evita el manejo de dinero en efectivo en las casetas
- TAG con código de identificación único
- El TAG no necesita batería
- Rápida velocidad de lectura
- Interoperabilidad con otras zonas
- Integración con sistemas electromecánicos, por lo general se utilizan las barreras
- Integración con los semáforos de señalización

Aplicaciones:

- Peajes
- Entradas vehiculares plantas industriales
- Estacionamientos de buses y sistemas de transporte masivo
- Entradas y salidas obras civiles

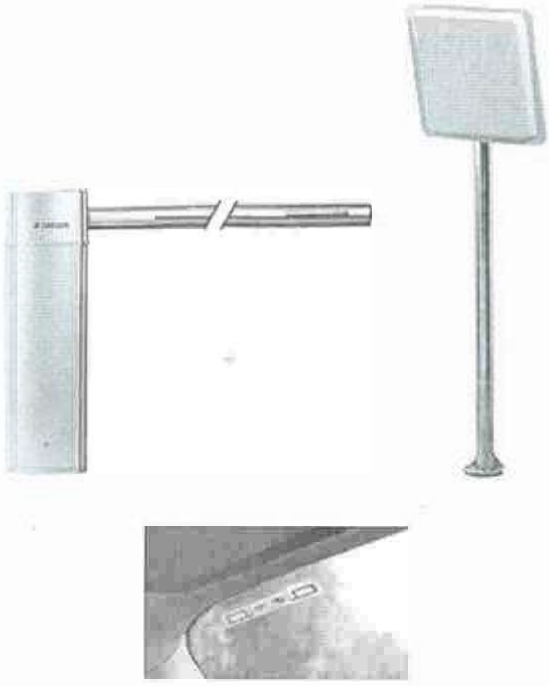

Figura 2.4 Control vehicular RFID

Los torniquetes, o tornos de acceso, son un sistema electromecánico que combinado a nuestros dispositivos y un software de gestión adecuado, se convierte en un excelente sistema de control de accesos, mejorando la seguridad, disminuyendo los costos ahorrando en personal extra para vigilancia, y generando una rápida y efectiva autenticación de cada persona.

2.2.2 Barreras vehiculares automáticas

Las barreras de estacionamiento se utilizan en integración con los controles de accesos vehicular para un correcto manejo del flujo vehicular en un determinado parqueadero. Su principal función se basa en permitir e impedir el paso a los vehículos, realizando la tarea de forma automática, eficiente, rápida y segura. Las barreras vehiculares cuentan con sistemas de anti-aplastamiento que impiden que un vehículo sea golpeado en caso de no avanzar rápidamente en la zona de accionamiento. Se cuentan con barreras de estacionamiento automáticas para distintas aplicaciones: barreras sencillas, barreras con bastidor articulado, barreras con cerca de protección, barreras de corto y largo alcance.

Ventajas:

- Accionamiento e integración con todos los dispositivos de control de accesos
- Trabajo continuo
- Sistema anti-aplastamiento y destrabe manual
- Tiempo de apertura rápido de 2 a 4 segundos dependiendo del modelo

Aplicaciones:

- Centros comerciales
- Edificios de oficinas y consultorios
- Parking
- Peajes
- Entradas vehiculares plantas industriales
- Estacionamientos de buses y sistemas de transporte masivo

- Entradas y salidas obras civiles

Figura 2.5 Barreras vehiculares

2.3 Control de acceso peatonal

Los sistemas de control de accesos peatonales se implementan para tener el control de todo el personal que transita en un espacio público o privado, asegurando el paso de personas que cuentan con un libre tránsito y restringiendo el paso de personas no autorizadas en áreas específicas. Las soluciones para control de accesos peatonales dependen de las aplicaciones y las necesidades de cada cliente, se pueden tener desde soluciones con un solo dispositivo que controla una puerta, hasta soluciones con múltiples dispositivos integrados a diferentes sistemas electromecánicos gestionados por medio de software centralizado [6].

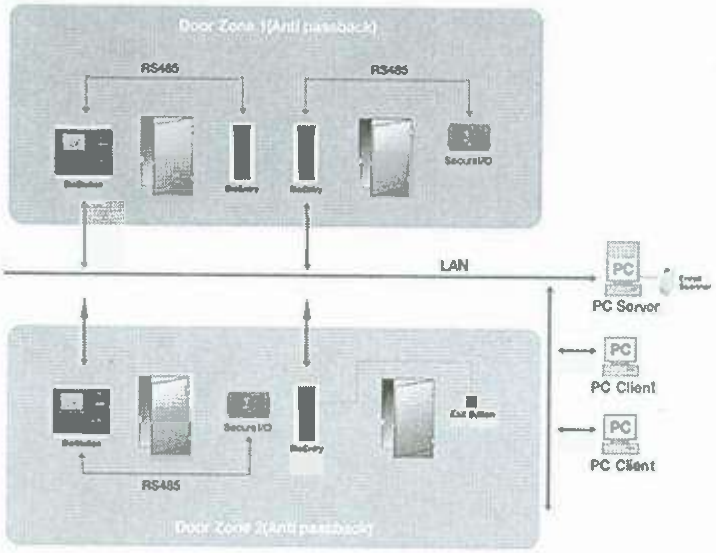

Figura 2.6 Arquitectura para control de acceso peatonal

Al implementar una solución para control de accesos peatonales podemos:

- Incrementar la seguridad del edificio, teniendo la certeza que únicamente ingresan personas autorizadas.
- Ahorrar en los costos y gastos fijos en personal especializado de vigilancia privada.
- Agilidad en los tiempos de entrada y salida.
- Mayor control y gestión de todo el personal, trabajadores y visitantes.

Características del Sistema

- Comunicación TCP/IP, Interfaces RS485 y Wiegand con las cuales se garantiza la compatibilidad con otros sistemas actuales o a futuro.
- Sistemas desde 500 hasta 40.000 usuarios
- 128 diferentes horarios
- 128 grupos de acceso
- 64 zonas
- Uso interior y exterior a prueba de agua y polvo
- Software intuitivo y sencillo para los usuarios y administradores del sistema
- Integración con todos los sistemas de seguridad del edificio

2.3.1 Lector de huellas digitales

Este es una forma de control biométrico utilizada muy a menudo como parte integral de un sistema de control de acceso. Los sistemas biométricos forman parte de una gran gama de alternativa usadas para la identificación de individuos. Esto se debe a que los sistemas biométricos hacen un análisis de cualidades personales únicos en cada individuo, como lo son las huellas dactilares, la retina, el iris y la geometría de la mano. El lector de huellas dactilares es la forma de control biométrico más popular y más eficiente en la verificación e identificación para control de accesos.

Figura 2.7 Lector de huellas digitales

Ventajas:

- Identificación rápida en el dispositivo (menos de 1seg)
- Identificación única por cada usuario
- No es necesario memorizar claves
- No es necesario cargar con tarjetas o controles
- La huella dactilar no es posible extraviarla
- No genera costo extra para cada usuario

Aplicaciones:

- Edificios de oficinas
- Edificios comerciales
- Conjuntos y edificios residenciales

2.3.2 Tarjeta de proximidad

Las tarjetas de control o proximidad son de gran aplicación en los sistemas de control de acceso, ya que estas nos permiten tener toda la información de cada usuario y además es posible personalizarlas con la imagen corporativa de la empresa y cualquier información impresa necesaria sobre la tarjeta. Tienen una gran aplicación en el control de asistencia y visitante. La mayor ventaja radica en la capacidad de darle autorización a puertas o zonas

específicas dentro de la edificación, generando seguridad y control sobre el acceso de las personas.

Figura 2.8 Tarjeta de proximidad

Ventajas:

- La transmisión de datos por radiofrecuencia entre la tarjeta y el lector es encriptada.
- Se visualiza como un carnet dentro del edificio o empresa.
- Costo de reemplazo bajo.
- Personalización de cada tarjeta tipo carnet.
- Las tarjetas no se deterioran.
- No les afectan los campos magnéticos..
- En caso de pérdida solo se desactivan en el software.

Aplicaciones:

- Edificios de oficinas
- Edificios comerciales
- Conjuntos y edificios residenciales, hoteles y hospitales

2.4 Combinación en controles de accesos

Según la aplicación es posible combinar diferentes tipos de autenticación en un solo dispositivo [4],[5] y [6]. Podemos realizar las siguientes combinaciones:

Figura 2.9 Combinaciones para Sistema de control de acceso

Ventajas:

- Huella dactilar+ clave
- Tarjeta de proximidad+ clave
- Huella dactilar+ tarjeta de proximidad
- Huella dactilar+ tarjera de proximidad+ clave

Se aplican en aquellos sitios donde se requiera aumentar la seguridad. Como siempre, es importante realizar un adecuado diseño para lograr la seguridad deseada sin comprometer el tiempo de autenticación:

- Bancos y Bodegas
- Depósitos
- Joyerías
- Locales comerciales

2.5 Torniquetes de acero

El Torniquete está indicado para control de los accesos peatonal en zonas de alto tránsito de personas. Es ideal como barrera de control para sitios donde se desee regular el flujo de

personas en las operaciones de entrada y salida. Es compatible e integrable con todos los dispositivos de control de accesos según sea la aplicación. Los torniquetes de acceso son mecanismos electromecánicos de alta confiabilidad, teniendo en cuenta que serán sometidos a duras condiciones de uso y desgaste. En su fabricación y diseño se tiene en cuenta las condiciones ergonómicas y elementos hidráulicos que facilitan el uso para personas de edad avanzada, mujeres en embarazo, niños y personas con discapacidad [6].

Figura 2.10 Torniquete de acero

Aplicaciones:

- Edificios con alto flujo de personas
- Estadios y áreas deportivas
- Estaciones ferroviarias, marítimas y subterráneas

Los torniquetes, o tornos de acceso, son un sistema electromecánico que combinado a nuestros dispositivos y un software de gestión adecuado, se convierte en un excelente sistema de control de accesos, mejorando la seguridad, disminuyendo los costos ahorrando en personal extra para vigilancia, y generando una rápida y efectiva autenticación de cada persona.

2.6 Puertas de seguridad

Las puertas de seguridad, o puertas corredizas, funcionan mediante diferentes sistemas electromecánicos: Sliders, electroimanes, cantoneras eléctricas, sensores y brazos para puertas

batientes. En general es posible automatizar la mayoría de puertas de control de accesos para obtener una mayor seguridad y ahorro. Se realizan diseños y soluciones para instalaciones nuevas y existentes [6]. También son completamente integrables a los dispositivos de control de acceso, para obtener un sistema completo.

Figura 2.11 Puertas de seguridad

Ventajas:

- Ajuste de la velocidad de apertura.
- Operación suave y silenciosa.
- Diseñadas para funcionamiento continuo.
- Apertura sin necesidad de tocar las puertas.
- Detección de presencia y movimiento.
- Soluciones para variedad de ambientes y dimensiones.
- Total cumplimiento con todos los estándares y normatividad de la construcción.

Aplicaciones:

- Centros comerciales
- Supermercados
- Edificios de oficinas
- Fachadas para conjuntos y edificios residenciales

2.7 Video portero

El video portero es una excelente solución cuando se quiere realizar una verificación antes de dar permiso de acceso al visitante. Se realiza la verificación de la persona, se establece la comunicación y una vez la persona es autorizada se realiza la apertura de la puerta remotamente [7].

Figura 2.12 Video portero

Ventajas:

- Video y audio para tener una mayor seguridad.
- Ahorro en pagos a vigilantes innecesarios.
- Placa exterior con tele cámara a color.
- Integración con el abre puertas eléctrico.
- Autoencendido y selección cámara principal / secundaria.
- Diseño estético y elegante.

Aplicaciones:

- Edificios residenciales
- Edificios de oficinas
- Oficinas
- Bodegas

2.8 Control de personal

Un adecuado sistema de control de personal es esencial para la buena administración en una empresa o un negocio, se trata de tener el control de entrada y salida de los empleados para mejorar la productividad, con seguimiento de horarios, grupos de acceso, zonas permitidas/restringidas y la certeza de un incremento en la productividad de la empresa. El módulo de control de asistencia del personal le proporciona la capacidad configurar y administrar el sistema desde cualquier navegador web estándar, desde la red corporativa o a través de Internet. La información se genera en tiempo real y sin ningún hardware adicional o instalaciones de software. Por otra parte, todos los datos de comunicación entre el sistema de control de personal y la red son encriptados para proporcionar seguridad adicional a los usuarios. La arquitectura del control de personal es mostrada en la imagen 2.13.

2.8.1 Sistema de control de personal beneficios y ventajas

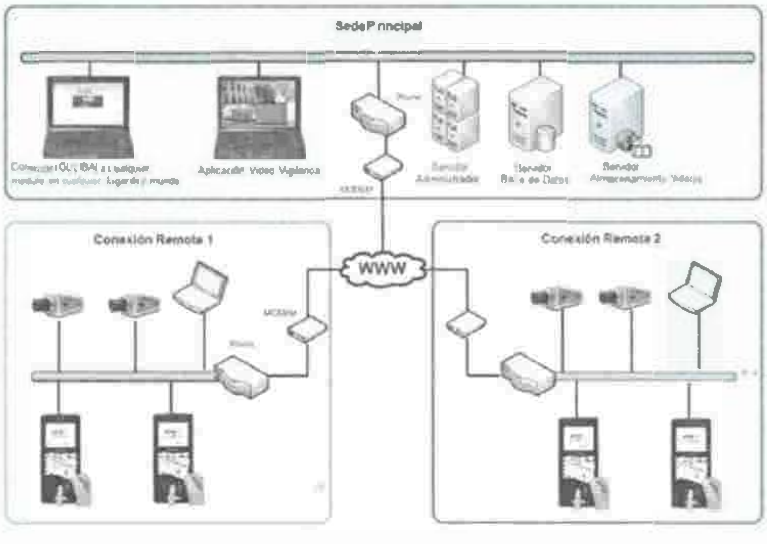

Figura 2.13 Arquitectura del control de personal

Según las necesidades y requerimientos de cada sistema de control de personal, se puede adaptar la configuración y calcular automáticamente las horas trabajadas por cada empleado durante todo el mes, o en el periodo en el cual se realiza el pago de nomina. Esto se traduce en un aumento en la puntualidad de los empleados y en una mayor productividad para la empresa.

- Mayor puntualidad y cumplimiento de todo el personal
- Disminución de horas improductivas
- Aumento en la seguridad de toda la empresa
- Integración con otros sistemas de gestión y control en la empresa
- Reportes personalizados
- Ahorro en personal extra que lleve los registros manualmente
- Indicadores de gestión para tomar decisiones

2.8.2 Módulo de registro de control de asistencia

El modulo principal de control de asistencia del personal tiene la capacidad de realizar la autenticación de cada empleado a través de un lector de huella dactilar, tarjeta de proximidad, clave o la combinación de cualquiera de los tres. Además cuenta con una cámara integrada para capturar una fotografía en el momento del registro y una cámara de video que se integra a un monitor externo, para ver el video en tiempo real del personal que está realizando el registro. El modulo principal es ubicado estratégicamente para realizar el registro diario. Este también puede estar controlando una puerta de entrada, permitiendo el paso únicamente al personal autorizado.

Figura 2.14 Control de asistencia

Ventajas:

- Cámara CMOS integrada para registrar la foto del usuario que se está registrando.
- Cámara de video integrable a un monitor externo o un sistema de video vigilancia.
- Módulos para 500 hasta 20.000 usuarios.
- Software embebido sin necesidad de instalaciones extras en PC's.
- Uso exterior con protección contra agua y polvo.
- Comunicación encriptada para protección de datos.

Aplicaciones:

- Fábricas
- Empresas
- Colegios
- Restaurantes
- Sector Público

2.9 Control de personal con lectores externos

Los lectores externos son módulos de control de asistencia del personal que se conectan al modulo principal. Según las aplicaciones y el tamaño del sistema de control de personal es posible integrar hasta 128 módulos adicionales para crear un completo control de personal. Al igual que los módulos principales, los módulos adicionales cuentan con direcciones IP propias para conectarse a cualquier red LAN, e incluso hacer la conexión a internet para integrar módulos ubicados en diferentes partes del mundo. Cuentan con múltiples tecnologías de comunicación para integrarse a cualquier control de accesos existente: HID proximity, HID iClass, Mifare, Sony felica, EM [4],[6].

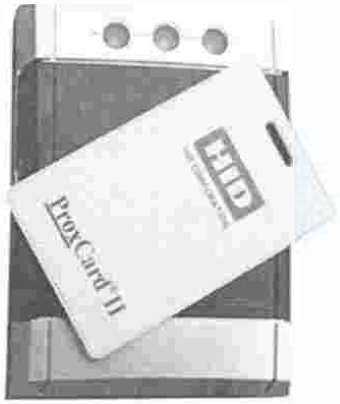

Figura 2.15 Lectores externos

Ventajas:

- Cuentan con direcciones IP propias
- Tamaño más pequeño que los módulos principales
- Leen múltiples tecnologías de tarjetas

Aplicaciones

- Fabricas
- Empresas
- Colegios
- Restaurantes
- Hospitales
- Sector Público

Capítulo 3

Marco referencial

3.1 Identificación por Radio Frecuencia (RFID)

La identificación por radiofrecuencia o RFID por sus siglas en inglés, es una tecnología que se utiliza para la identificación en todo, desde el etiquetado para el seguimiento de vehículos, hasta el control de acceso. RFID proporciona recopilación automática de datos para los que en la actualidad hay varias normas, y esto permite que la tecnología RFID sea ampliamente utilizada [1].

Todo sistema RFID se compone de un interrogador o sistema de base que lee y escribe datos en los dispositivos y un transmisor que responde al interrogador. El interrogador genera un campo de radiofrecuencia, normalmente conmutando una bobina a alta frecuencia. Las frecuencias usuales van desde 125 Khz hasta la banda ISM de 2.4 GHz. El campo de radiofrecuencia genera una corriente eléctrica sobre la bobina de recepción del dispositivo. Esta señal es rectificada y de esta manera se alimenta el circuito. Cuando la alimentación llega a ser suficiente el circuito transmite sus datos. El interrogador detecta los datos transmitidos por la tarjeta como una perturbación del propio nivel de la señal. La señal recibida por el interrogador desde la tarjeta está a un nivel de -60 db por debajo de la portadora de transmisión. El rango de lectura para la mayoría de los casos está entre los 30 y 60 centímetros de distancia entre interrogador y tarjeta.

Podemos encontrar además dos tipos de interrogadores diferentes:

- Sistemas con bobina simple, la misma bobina sirve para transmitir la energía y los datos. Son más simples y más baratos, pero tienen menos alcance.
- Sistemas interrogadores con dos bobinas, una para transmitir energía y otra para transmitir datos. Son más caros, pero consiguen unas prestaciones mayores.

3.1.1 RFID Activa y pasiva

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

A diferencia de las etiquetas pasivas, las activas poseen su propia fuente autónoma de energía, que utilizan para dar corriente a sus circuitos integrados y propagar su señal al lector. Estas son mucho más fiables (tienen menos errores) que las pasivas debido a su capacidad de establecer sesiones con el lector. Gracias a su fuente de energía son capaces de transmitir señales más potentes que las de las pasivas, lo que les lleva a ser más eficientes en entornos dificultosos para la radiofrecuencia como el agua (incluyendo humanos y ganado, formados en su mayoría por agua), metal (contenedores, vehículos). También son efectivas a distancias mayores pudiendo generar respuestas claras a partir de recepciones débiles (al contrario que las pasivas). Por el contrario, suelen ser mayores y más caras, y su vida útil es en general mucho más corta.

3.1.2 Protocolos y opciones de frecuencia

Normalmente el sistema de modulación usado es modulación de amplitud (AM) con codificación tipo Manchester NRZ. Para conseguir mayor alcance y más inmunidad al ruido eléctrico se utilizan sistemas más sofisticados. En algunos casos se divide la frecuencia del reloj de recepción. En algunos casos se llevan datos grabados de fábrica y en otros también hay datos que puede grabar el usuario. Algunos sistemas utilizan encriptación de clave pública para conseguir mayor seguridad ante posibles ataques maliciosos. Por otro lado podemos encontrar sistemas anticolisión que permiten leer varias tarjetas al mismo tiempo. En caso de que varias tarjetas estén en el rango de alcance del interrogador y dos o más quieran transmitir al mismo tiempo, se produce una colisión. El interrogador detecta la colisión y manda parar la transmisión de las tarjetas durante un tiempo. Después irán respondiendo cada una por separado por medio de algoritmos complejos.

Las etiquetas RFID de baja frecuencia (LF: 125 - 134 kHz y 140 - 148.5 kHz) y de alta frecuencia (HF: 13.56 MHz) se pueden utilizar de forma global sin necesidad de licencia. La frecuencia ultra-alta (UHF: 868 - 928 MHz) no puede ser utilizada de forma global, ya que no hay un único estándar global. En Norteamérica, la frecuencia ultra-elevada se puede utilizar sin licencia para frecuencias entre 908 - 928 MHz, pero hay restricciones en la energía de transmisión. En Europa la frecuencia ultra-elevada está bajo consideración para 865.6 - 867.6 MHz. Su uso es sin licencia sólo para el rango de 869.40 - 869.65 MHz, pero existen restricciones en la energía de transmisión. El estándar UHF norteamericano (908-928 MHz) no es aceptado en Francia e Italia ya que interfiere con sus bandas militares. En China y Japón no hay regulación para el uso de la frecuencia ultra-elevada. Cada aplicación de frecuencia ultra-elevada en estos países necesita de una licencia, que debe ser solicitada a las autoridades locales, y puede ser revocada. La tabla 2.1 muestra un concentrado de aplicaciones por frecuencia para la tecnología RFID.

Tabla 2.1. Aplicaciones típicas por fecuencia.

Rango de frecuencias	Aplicaciones típicas
125 a 134,2 kHz y 140 a 148,5 kHz (baja frecuencia)	A menudo se utiliza para la identificación del vehículo
13.553 - 13.567 MHz Alta frecuencia	Estas frecuencias RFID se utilizan normalmente para billetaje electrónico, pago sin contacto, control de acceso, seguimiento de ropa, etc.
26.957 - 27.283 MHz frecuencia media	Estas frecuencias RFID se utilizan con acoplamiento de retrodispersión, para aplicaciones tales como las llaves del coche a distancia en Europa.
858 - 930 MHz Ultra Alta Frecuencia	A menudo se utiliza para la gestión de activos, seguimiento de contenedores, seguimiento de equipaje, el trabajo en el seguimiento de los progresos, etc. y, a menudo en combinación con los sistemas Wi-Fi.

3.2 Arduino

Arduino es una Plataforma de Electrónica abierta para la creación de Prototipos basada en Software y Hardware flexibles y fáciles de usar. Se creó para artistas, diseñadores, aficionados y cualquiera interesado en crear entornos u objetos interactivos [8].

Arduino puede tomar información del entorno a través de sus pines de entrada de toda una gama de sensores y puede afectar aquello que le rodea controlando luces, motores y otros actuadores. El Microcontrolador en la placa se programa mediante el Lenguaje de Programación Arduino (basado en Wiring) y el entorno de desarrollo (basado en Processing). Los Proyectos hechos con Arduino pueden ejecutarse sin necesidad de conectar a una Computadora, si bien tienen la posibilidad de hacerlo y comunicar con diferentes tipos de Software. Las placas pueden ser hechas a mano o compradas montadas de fábrica; el Software puede ser descargado de forma gratuita.

Es una Plataforma de desarrollo de computación física de Código abierto, basada en una placa con un sencillo microcontrolador y un entorno de desarrollo para crear Software embebido.

Los Proyectos de Arduino pueden ser autónomos o comunicarse con un software que se ejecute en la Computadora.

3.2.1 Ventajas de Arduino respecto a otros Sistemas

Las Placas son más accesibles comparadas con otras Plataformas de Microcontroladores. La versión más costosa de un Módulo de Arduino puede ser montada a mano, e incluso ya montada cuesta bastante menos. El Software funciona en los Sistemas Operativos Windows, Macintosh OSX y Linux. La mayoría de los entornos para Microcontroladores están limitados a Windows.

El entorno de programación es fácil de usar para principiantes y lo suficientemente flexible para los usuarios avanzados. Pensando en los Profesores, Arduino está basado en el entorno de Programación de Processing con lo que el estudiante que aprenda a programar en este entorno se sentirá familiarizado con el entorno de desarrollo Arduino. El Software está publicado bajo una licencia libre y está preparado para ser ampliado por programadores experimentados. El Lenguaje puede ampliarse a través de Librerías de C++.

Arduino está basado en los Microcontroladores ATmega168, ATmega328 y ATmega1280. Los diseños de los Módulos están publicados Licencia Creative Commons, por lo que diseñadores de Circuitos con experiencia pueden hacer su propia versión del Módulo, ampliándolo u optimizándolo. Incluso usuarios relativamente inexpertos pueden construir la versión para placa de desarrollo para entender cómo funciona y ahorrar algo de dinero.

3.2.2 Características de arduino UNO

Arduino UNO (como se muestra en la Figura 3.1) es una Placa Electrónica basada en el Microcontrolador ATmega328. Cuenta con 14 entradas digitales/Pines de salida (de los cuales seis pueden ser utilizados como salidas PWM), seis entradas Analógicas, un Oscilador de

Cristal de 16 MHz, una conexión USB, un Conector de Alimentación, una Cabecera de ICSP (In Circuit Serial Programming, método de programación directamente AVR), y un botón de Reset. Contiene todos los Periféricos necesarios para hacer funcionar el Microcontrolador, sólo tiene que conectarlo a una Computadora con un Cable USB o con un Adaptador AC-DC o la Batería para empezar.

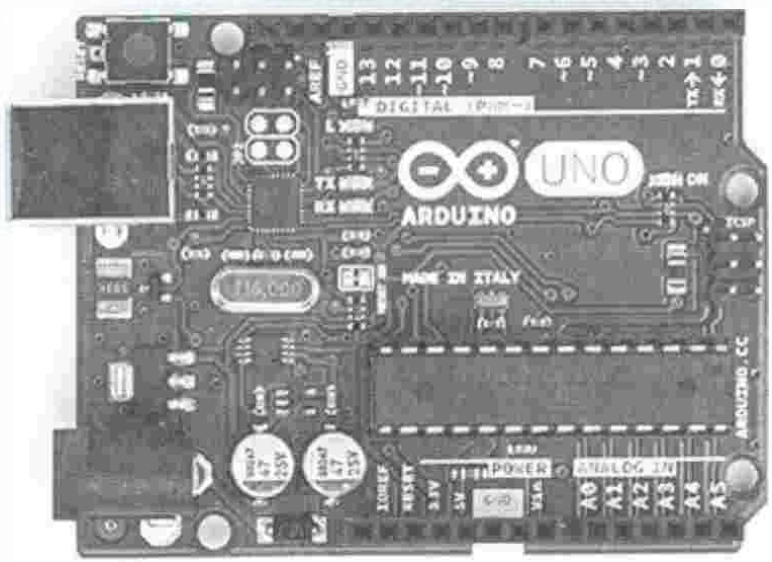

Figura 3.1 Placa de Arduino UNO

Características Técnicas de Arduino UNO

- Microcontrolador ATmega 328.
- Voltaje de Operación 5V.
- Voltaje de Entrada (recomendado) 7-12 V.
- Voltaje de Entrada (límites) 6-20 V.
- Canales de E/S (de los cuales seis proporcionan una salida PWM)
- Pines de Entrada Analógica 6.
- Corriente de E/S de CC Pin 40 mA.
- De Corriente Continua de 3.3 V Pin 50 mA.

Memoria Flash de 32 MB (ATmega328) de los cuales 0.5 KB utilizado por gestor de arranque.

- SRAM 2 KB (ATmega328).
- EEPROM 1 KB (ATmega328).
- Velocidad del Reloj de 16 MHz.

Puede ser alimentado a través de la conexión USB o con una fuente de alimentación externa. La fuente de alimentación se selecciona automáticamente. Externo (no USB), la fuente de alimentación puede venir de un adaptador de CA a CC o con una Batería. Los cables de la Batería se pueden insertar en los Pines GND y VIN del conector de alimentación. La Fuente puede operar en un suministro externo de 6 a 20 Voltios. Si se suministran con menos de 7V, sin embargo, el Adaptador puede suministrar menos de 7 Voltios y la Placa puede ser inestable. Si se utiliza más de 12V, el Regulador de Voltaje se puede sobrecalentar y dañar la Placa. El rango recomendado es de 7 a 12 Voltios.

Los Pines de alimentación se describen a continuación:

VIN: El Voltaje de Entrada a la Placa Arduino cuando se utiliza una Fuente de alimentación externa (a diferencia de 5 Voltios de de la conexión USB o de otra Fuente de Alimentación regulada). Se puede suministrar Tensión a través de este PIN.

5V: Este PIN genera unos 5V regulados por el Regulador de la Tarjeta. La Tarjeta puede ser alimentada ya sea desde la entrada de alimentación (7-12 V), el Conector USB (5V), o el Pin de VIN de la Placa (7-12V). El suministro de Tensión a través de los Pines de 5V o 3.3V no pasa por el Regulador, y puede dañar la Placa. NO ACONSEJABLE.

3.3V: Un suministro de 3.3 Voltios generada por el Regulador. El consumo de Corriente máxima es de 50 mA.

GND: Pin de Tierra. Arduino UNO en su tercera revisión, cuenta con tres pines reservados para referencia a tierra.

Memoria: El ATmega328 tiene 32 MB (con 0.5 KB utilizados para el Gestor de Arranque). También dispone de 2 KB de SRAM y 1 KB de Memoria EEPROM (que puede ser leído y escrito con la Librería EEPROM).

Entrada y Salida: Cada uno de los 14 Pines digitales en el Arduino UNO se puede utilizar como Entrada o Salida, usando las funciones pinMode (), digitalWrite (), y las Funciones digitalRead (). Ellos operan a 5 Voltios. Cada Pin puede proporcionar o recibir un máximo de 40 mA y tiene un arreglo interno de resistencia pull-up (desconectado por defecto) de 20 a 50 kΩ. Además, algunos Pines tiene funciones especializadas:

Puerto serial: Serie 0 (RX) y 1 (TX).- Se utiliza para recibir (RX) y Transmitir (TX) datos Serie TTL. Estos se encuentran conectados a los Pines correspondientes de la ATmega8U2 USB a Chip de Serie TTL.

PWM: Las salidas 3, 5, 6, 9, 10 y 11 proporcionan 8-Bits de salida PWM con una Función analogWrite ().

LED 13: Hay un Led conectado al Pin digital 13, el cual funciona como un indicador de propósito general. Cuando el Pin es de alto valor, el Led está encendido, cuando el pasador es bajo, está apagado.

El Arduino UNO tiene seis entradas analógicas, etiquetadas A0 a A5, cada una de las cuales proporcionan 10 Bits de resolución (es decir 1024 valores diferentes). Por defecto miden desde 0 a 5 Voltios, aunque es posible cambiar el extremo superior de su rango con el Pin y el AREF y la función analogReferencce ().

3.2.3 Comunicación

Arduino tiene una serie de facilidades para comunicarse con una Computadora, otro Arduino, u otros Microcontroladores. El ATmega328 ofrece una UART TTL (5V) de comunicación en

serie, que está disponible en los Pines digitales 0 (RX) y 1 (TX). Un ATmegal 6U2 en los canales de comunicación a través de USB y aparece como un Puerto COM virtual con el Software en la Computadora. El firmware 16U2 utiliza el estándar de los Controladores USB, COM y no es necesario ningún Controlador externo. Sin embargo, en Windows; un Archivo "inf" es requerido. El Software de Arduino requiere un Monitor de Datos (Data Monitor) que permite el monitoreo de Datos que se envía desde y hacia la Placa. Los LEDs RX y TX en la Tarjeta parpadean cuando se están transmitiendo Datos a través del Puerto USB a serie y la conexión USB a la Computadora (pero no para comunicación de serie en los Pines 0 y 1).

La Biblioteca SoftwareSerial permite la comunicación de serie en cualquiera de los Pines digitales de Arduino UNO.

El ATmega328 también soporta comunicación 12C (bus de comunicaciones en serie) y SPI. El Software incluye una Librería Wire para simplificar el uso del Bus 12C. Para la comunicación SPI, utilizar la Biblioteca de SPI.

3.2.4 Programación

La Placa puede ser programada bajo el entorno de Programación Arduino. El ATmega328 viene pre-quemado con un Gestor de Arranque que le permite cargar nuevo Código a la Placa sin el uso de un Programador de Hardware externo.

También puede pasar por alto el Gestor de Arranque y el Programa del Microcontrolador a través de la ICSP (Programación In-Circuit Serial). El ATmegal6U2 (o 8U2 en los REVl y REV2) el Código Fuente está disponible en el Firmware.

3.2.5 Reset

En lugar de requerir presionar el Botón de Reset antes de una carga, el Arduino está diseñado de una manera que le permite ser restaurado mediante el Software que se ejecuta en una Computadora conectada. Una de las Líneas de Control de Flujo de Hardware (DTR) de la ATmega8U2/l6U2 está conectado a la Línea de reposición del ATmega328 a través de un

Condensador de 100 Nanofaradios. Cuando ésta toma un valor bajo, el Voltaje suministrado de la Línea de Reset cae lo suficiente como para restablecer el Chip. El Software de Arduino utiliza esta capacidad que le permite cargar el Código con sólo pulsar el Botón de Carga en el Entorno Arduino.

3.2.6 USB Protección contra Sobrecorriente

Arduino UNO tiene un Fusible reajustable que protege a los Puertos USB de la Computadora de pequeños Cortos y de Sobrecorriente. Aunque la mayoría de las Computadoras ofrecen su protección interna, el Fusible proporciona una capa adicional de protección. Si hay más de 500 mA aplicados al Puerto USB, el Fusible automáticamente corta la conexión hasta que el Cortocircuito o una Sobrecarga se han eliminado.

3.2.7 Dimensiones físicas del Arduino UNO

Las dimensiones externas de la Placa Arduino UNO son 70x50 milímetros (las Unidades mostradas en la Figura 3.2 se encuentran en milésimas de pulgada).

Figura 3.2 Dimensiones de la placa Arduino UNO

3.3 Shield Ethernet

Este shield permite conectar Arduino a la red, utilizando para ello un puerto Ethernet. Está basado en el chip de ethernet Wiznet W5100 con funcionalidades de IP tanto para TCP como UDP. El Shield Ethernet para arduino soporta hasta 4 conexiones simultáneas. Arduino utiliza la librería Ethernet para escribir rápidamente programas que se conecten a la red empleando este shield. El shield posee un conector RJ45 estándar para Ethernet, mediante el cual es posible conectarse a la red para realizar tareas de comunicación [9].

Esta tarjeta incluye un slot para memorias micro-SD, la cual puede ser empleada para almacenar archivos que pueden ser accesados a través de la red. La librería para el manejo de la tarjeta todavía no está incluida en la distribución estándar de Arduino pero se puede emplear la desarrollada por Bill Greiman Sdfatlibl. Este shield también se incluye un controlador de reset, esto es para asegurarse que el módulo W5100 Ethernet inicie correctamente al conectarlo a la electricidad. La versión original de este shield requerían reset manual después de conectarlo. No se debe confundir el controlador de reset con el botón de reset en la tarjeta, ya que este último inicializa tanto el shield como el Arduino.

El Arduino UNO utiliza los pines digitales 11, 12 y 13 (SPI) para comunicarse con esta tarjeta. El Mega emplea los pines 50,51 y 52. En ambas tarjetas (UNO y Mega) el pin 10 es empleado para seleccionar el W5100 y el pin 4 para la tarjeta SD. Por lo tanto, mientras se utilicen las funcionalidades de Ethernet, estos pines no estarán disponibles. Debido a que el W5100 y la tarjeta SD comparten el mismo bus SPI solo uno podrá estar activo a la vez, esto es, si se está utilizando ambos periféricos en el programa, se debe tomar en cuenta este aspecto. Para deshabilitar la tarjeta SD, se debe configurar el pin 4 como salida y activarlo en HIGH.

3.4 Sockets TCP y UDP

Hoy en día existe mucho entusiasmo sobre Internet y las posibilidades de interconectar todas las cosas. El Internet vincula el mundo de la información en conjunto. Los avances de la época

hacen que Internet sea fácil de usar compartiendo recursos con otras entidades. Java proporciona una serie de capacidades de red integradas que facilita el desarrollo de aplicaciones basadas en Internet para permitir que los programas obtengan información y de esta manera colaboren con otras entidades en la red ya sea interna o externa [10].

Java se utiliza a menudo como un vehículo de aplicación en los cursos de redes de computadoras ya que proporciona las herramientas necesarias para un rápido desarrollo de aplicaciones que tienen comunicación en red. Las capacidades fundamentales son declaradas por clases e interfaces del paquete java.net, a través del cual Java ofrece comunicaciones que permiten a las aplicaciones inspeccionar los flujos de datos en la red. Las clases e interfaces de paquete java.net también ofrecen las comunicaciones basadas en paquetes para realizar *streaming*, técnica comúnmente utilizada para transmitir audio y vídeo a través de Internet.

El análisis de redes se centra en los dos lados de la relación cliente / servidor. El cliente solicita que se realice alguna acción, y el servidor realiza la acción y da una respuesta al cliente. Una aplicación común del modelo de solicitud-respuesta se observa en los navegadores y servidores web. Cuando un usuario selecciona un sitio web a través de un navegador web (la aplicación de cliente), se envía una petición al servidor apropiado (la aplicación de servidor). El servidor normalmente responde al cliente mediante el envío de una página web apropiada HTML.

Una técnica común para realizar comunicaciones son los llamados Sockets, los cuales permiten que las aplicaciones vean la red como si se tratara de archivos de E/S que un programa puede leer o escribir. El socket es simplemente una construcción de software que representa un punto final de una conexión. Con los sockets, un proceso establece una conexión con otro proceso y mientras la conexión esté activa, el flujo de datos entre los procesos es continuo. El protocolo mas utilizado para transmisión es el TCP (*Transmission Control Protocol* por sus siglas en inglés).

Existen también los sockets de Datagramas, los cuales transmiten los paquetes individuales de información. Esta técnica no es muy apropiada ya que protocolo UDP (User Datagram

Protocolo por sus siglas en inglés), es un servicio de conexión, y por lo tanto no garantiza que los paquetes llegan en un orden particular. Con UDP, los paquetes pueden incluso ser perdidos o duplicados. Se requiere programación adicional significativa para hacer frente a estos problemas (si decide hacerlo). UDP es más apropiado para aplicaciones de red que no requieren la comprobación de errores o la fiabilidad que aporta TCP.

3.4.1 Servidor de sockets

Para establecer conexión mediante sockets se requieren tres elementos: una dirección IP, un puerto y un protocolo. La dirección IP usualmente es la del servidor pues es quien contiene las instrucciones que serán realizadas una vez requeridas por el usuario. El puerto es el punto de entrada al servidor. Cada servidor puede tener varios puertos lo cual garantiza que varios usuarios pueden interactuar con el servidor sin interferir unos con otros. Finalmente el protocolo puede ser TCP o UDP. La selección del protocolo depende esencialmente de la aplicación.

El establecimiento de un servidor sencillo en Java requiere cinco pasos. El primer paso es para crear un objeto de servidor de socket. Una llamada al constructor de ServerSocket, como

```
ServerSocket Servidor= new ServerSocket (portNumber, MaxConn);
```

Esta instrucción registra un número de puerto disponible y especifica el número máximo de clientes que pueden esperar para conectar con el servidor (es decir, la longitud de la cola). El número de puerto es utilizado por los clientes para localizar la aplicación de servidor en el equipo servidor. El constructor establece el puerto en el que el servidor espera para las conexiones de los clientes; un proceso conocido como vinculante el servidor al puerto. Cada cliente pedirá al conectar con el servidor en este puerto. Sólo una aplicación a la vez se puede enlazar a un puerto especifico en el servidor.

Capítulo 4

Desarrollo del sistema

Tomando en cuenta los requerimientos del Departamento de Ingeniería Industrial en cuanto a Control de Acceso se refiere, se ha desarrollado el sistema Inteligente de Control de Acceso así como los diagramas de mantenimiento para el mismo. En el presente capítulo se detallarán los elementos del desarrollo del sistema, los cuales consisten en:

1. Diagrama funcional del sistema
2. Sistema inteligente de control de acceso para el aula
3. Diagramas de Mantenimiento
4. Pruebas y verificación

4.1. Diagrama funcional del sistema

Como se mencionó anteriormente, el Departamento de Ingeniería Industrial de la Universidad de Sonora (Hermosillo, México) utiliza un sistema RFID para acceder a las aulas. El sistema cuenta con una gran cantidad de problemas que se pretenden solucionar en este trabajo. El primer paso es la elaboración del diagrama funcional para visualizar mejor la relación de los elementos dentro del sistema. Hay tres principales componentes interconectados: el lector RFID, la chapa electrónica y el controlador. La Figura 4.1 muestra el diagrama funcional con la interacción entre los elementos mencionados.

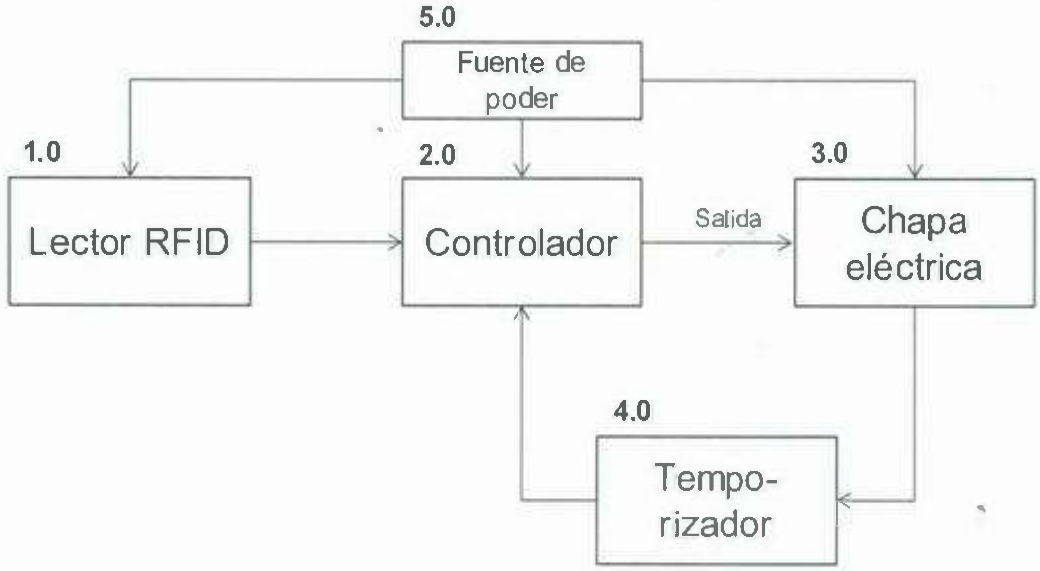

Figura 4.1. Diagrama funcional del sistema de control de acceso

De la figura 4.1 podemos observar que la parte principal del sistema es el controlador, que se compone de un microcontrolador, etapa de comunicación, puertos y una etapa de potencia. La fuente de alimentación es un componente externo que debe aparecer en el diagrama con el fin de comprender mejor cómo los elementos están interconectados. El tiempo de retraso es utilizado para activar la cerradura eléctrica por un tiempo determinado y que el usuario sea capaz de abrir la puerta. El lector RFID se encarga de la lectura de la tarjeta y de mandar los datos de la misma al controlador. Una vez que el controlador valida la información contenida en la tarjeta, envía una señal para activar la chapa eléctrica. La figura 4.2 muestra los elementos internos del controlador así como sus interacciones.

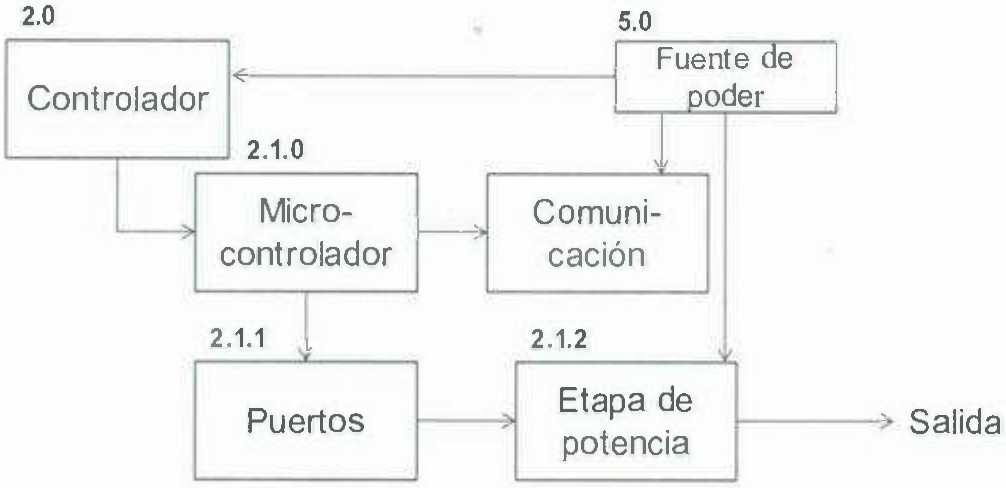

Figura 4.2. Diagrama funcional del Controlador

Como se puede observar en la figura 4.2, el microcontrolador se encarga de procesar la información recolectada a través del sensor. Esta información es comparada con las reglas internas programadas en el microcontrolador y, de requerirse, una señal es enviada por medio de los puertos. Los puertos se encargan de acondicionar la señal ya sea de entrada o de salida para que sea utilizada en la siguiente etapa. En el caso del sistema de control de acceso, los puertos entregan una señal digital (5 VDC) la cual es transmitida a la etapa de potencia. Ya que la chapa electrónica requiere un voltaje y corriente que no pueden ser proporcionados por los puertos del controlador, la etapa de potencia es requerida, esta etapa recibe la señal digital de los puertos y transforma dicha señal de control en una señal de potencia que puede utilizarse para activar la chapa eléctrica. En el caso del sistema de control de acceso, la etapa de potencia está formada por una serie de relevadores. La tarea del relevador es tomar la potencia necesaria de la fuente de voltaje y proporcionar dicha potencia a la bobina de la chapa eléctrica. Finalmente el módulo de comunicación, el cual está integrado en el controlador, se encarga de mantener una línea de enlace con el mundo exterior para poder llevar un registro de las actividades realizadas por el controlador o para enviar una orden al mismo, por ejemplo para abrir la puerta de manera remota.

4.2 Sistema inteligente de control de acceso para el aula

Después de desarrollar y analizar el diagrama funcional, el siguiente paso es crear el sistema para ser probado. Para llevar a cabo un desarrollo rápido y robusto, la plataforma de desarrollo Arduino UNO fue utilizada como controlador principal. Esta plataforma contiene el microcontrolador y los puertos necesarios para crear fácilmente un prototipo del sistema e inspeccionar su funcionalidad. La etapa de potencia se lleva a cabo mediante el uso de un conjunto de relevadores adaptados para el IDE, lo que significa que se pueden activar con la señal proporcionada por los puertos. El lector RFID utilizado fue el RFID-RC522, este es un lector de alta frecuencia compatible con el Arduino IDE. La razón para elegir este lector (aparte del hecho de que es compatible con el Arduino IDE), es porque es configurable y puede ser utilizado como escritor y el lector al mismo tiempo. Por último, la cerradura eléctrica es de marca Masterlock y trabaja con 12 VDC y 1 ampere, por lo que tenemos que

utilizar la etapa de potencia antes mencionada ya que la plataforma Arduino no puede proporcionar dicha potencia.

La figura 4.3 muestra el sistema utilizado en el Departamento de Ingeniería Industrial de la Universidad de Sonora. Como se puede observar, la tarjeta monolítica contiene todos los elementos aglomerados, por lo que es difícil de reparar, encontrar alguna falla o simplemente proporcionar mantenimiento. Como se puede observar, este sistema cuenta con un microcontrolador, una etapa de potencia y puertos de comunicación sin embargo, aunque son identificables, es difícil determinar las fronteras o las interfaces para interacción entre los elementos. Más aún, cualquier tipo de mantenimiento requerido ocupa de personal altamente capacitado con un profundo conocimiento del sistema, el cual solo puede ser encontrado en la empresa que instaló el sistema. Cabe destacar que el sistema mostrado nunca ha sido conectado a la red por lo cual no se cuenta con evidencia de que el módulo de comunicación funcione. Finalmente se debe destacar que la instalación del sistema no fue realizada de la manera correcta. Este último punto será tratado más adelante en el presente trabajo como una de las oportunidades de mejora tanto del sistema como de los elementos que lo rodean.

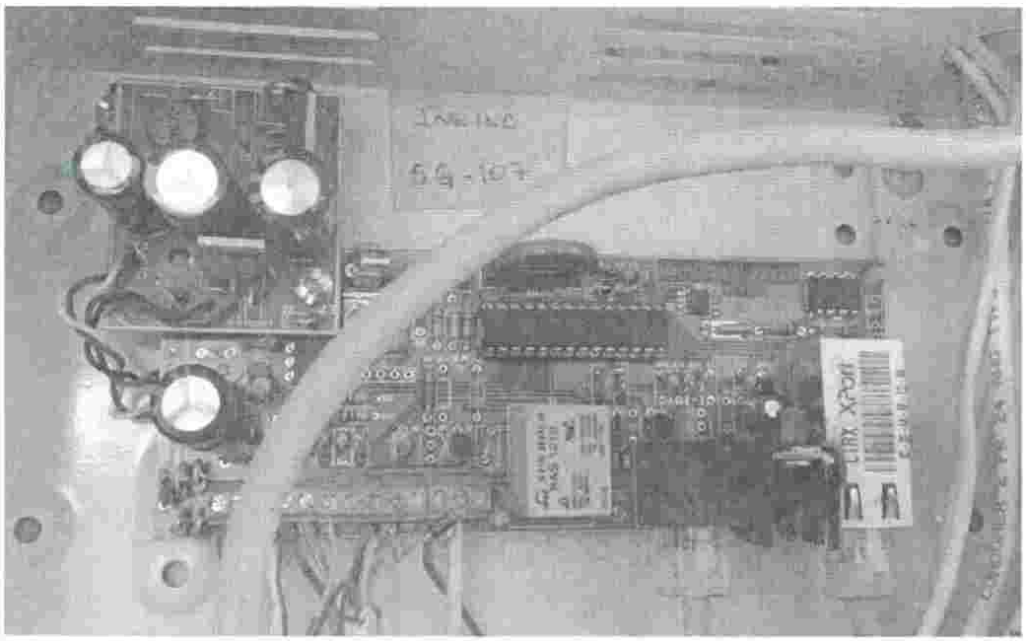

Figura 4.3. Tarjeta de control de acceso actual

La figura 4.4 muestra el nuevo sistema en el que todos los elementos funcionales están claramente identificados con el fin de proporcionar una mejor comprensión del sistema y, al mismo tiempo, para que sea más fácil de reparar o proporcionar mantenimiento cuando sea necesario. Los elementos mostrados son 1) Arduino UNO, 2) etapa de potencia y 3) fuente de poder.

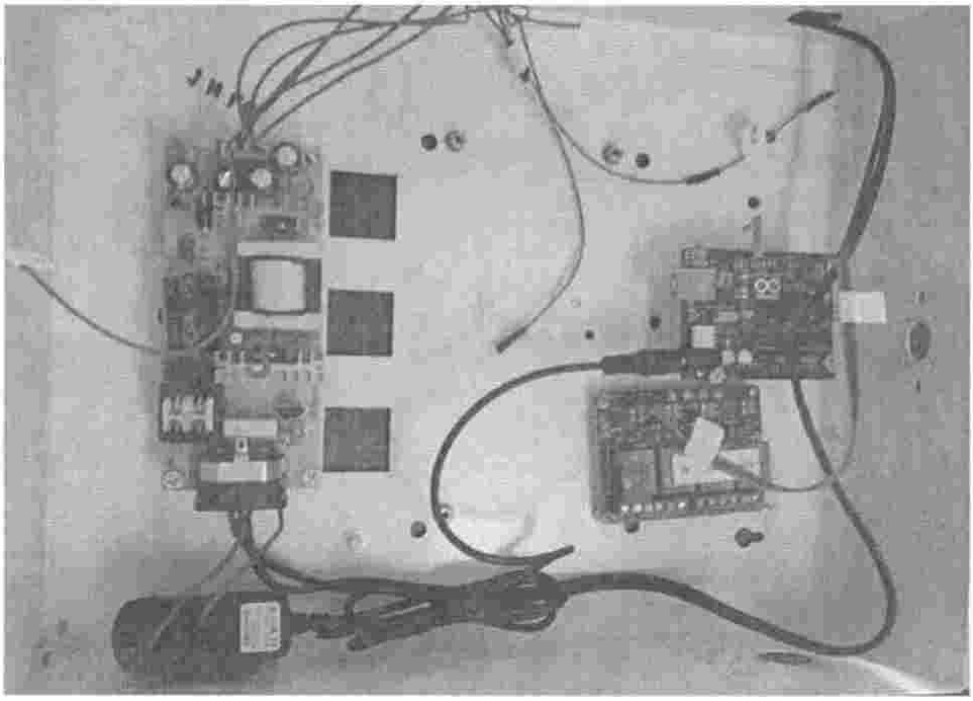

Figura 4.4. Sistema diseñado

4.2.1 Sensor RFID

El sensor RFID-RC522 mostrado en la figura 4.5 se encarga de la lectura de las tarjetas. El sensor emite una señal de alta frecuencia activando la tarjeta la cual responde con el número contenido en esta.

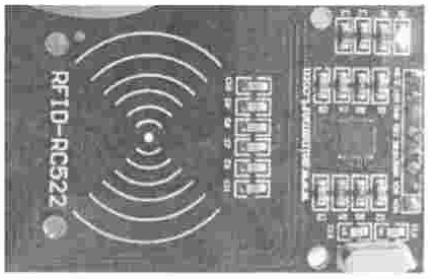

Figura 4.5. Lector de tarjetas RFID

La configuración así como la conexión del sensor hacia la plataforma de desarrollo Arduino se muestra en la tabla 4.1.

Tabla 4.1 Conexión de RFID-RC522 con Arduino UNO

Terminal RFID-RC522	Descripción	Pin Arduino UNO
RST	Reset	9
SPI SS	Selección en modo esclavo	10
SPI MOSI	Maestro-Esclavo (Master Out Slave In)	11
SPI MISO	Esclavo-Maestro (Master In Slave Out)	12
SPI SCK	Reloj serial	13
VCC	Voltaje	3.3V
GND	Tierra	GND

4.2.2 Controlador

Como se mencionó anteriormente, el controlador abarca al microprocesador, la etapa de comunicación, los puertos y la etapa de potencia. El microcontrolador contiene el programa principal, el cual corre en tiempo real y es utilizado para validar la información contenida en la tarjeta. La figura 4.6 muestra la parte principal del código en Arduino.

```
void loop() {
    s="";
    // Esperar por tarjetas
    if ( ! mfrc522.PICC_IsNewCardPresent()) return;
    // Seleccionar tarjetas
    if ( ! mfrc522.PICC_ReadCardSerial())  return;
    // Imprimir tarjeta leida
    Serial.print(F("Card ID: "));
    cardValue(mfrc522.uid.uidByte, mfrc522.uid.size);
    s.toUpperCase();
    Serial.println(s);
    if(validateCard()){ //validar tarjeta
       digitalWrite(doorPin, HIGH);
       delay(1000);
       digitalWrite(doorPin, LOW);
    }
   delay(1000);
} //end loop
```

Figura 4.6. Programa principal

El microcontrolador está directamente conectado a los puertos los cuales proporcionan las entradas y salidas necesarias para una correcta comunicación con el entorno. La figura 4.7 muestra un acercamiento a la plataforma de desarrollo Arduino donde se muestra la conexión del sensor hacia los puertos.

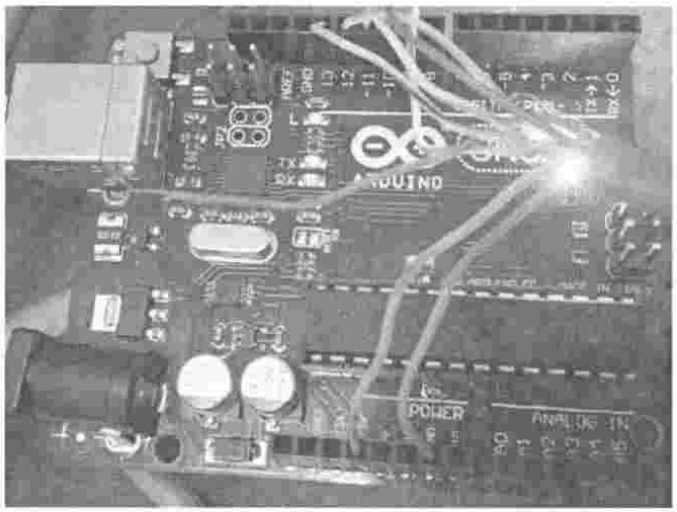

Figura 4.7. Acercamiento a los puertos de comunicación conectando el sensor

El microcontrolador, utilizando los puertos, se encuentra conectado con el shiel Ethernet para comunicación (ver figura 4.8). La configuración de este shield incluye la dirección IP de la tarjeta, el puerto y el protocolo, en nuestro caso es el protocolo UDP. La comunicación se realiza por medio de sockets y en una estructura maestro-esclavo donde el maestro es la plataforma Arduino y el esclavo es una computadora que alberga el programa de comunicación.

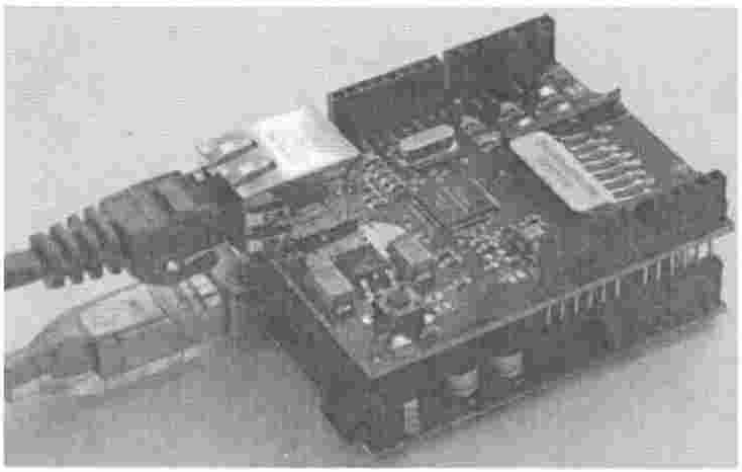

Figura 4.8. Shield Ethernet conectado con Arduino

Un elemento importante dentro del controlador es la etapa de potencia, la cual se encarga de transferir la potencia necesaria de la fuente a la chapa eléctrica. En nuestro caso la etapa de potencia es realizada por medio de relevadores que conmutan su estado de encendido a apagado de acuerdo a la señal recibida desde los puertos. La figura 4.9 muestra un acercamiento a la etapa de potencia utilizada.

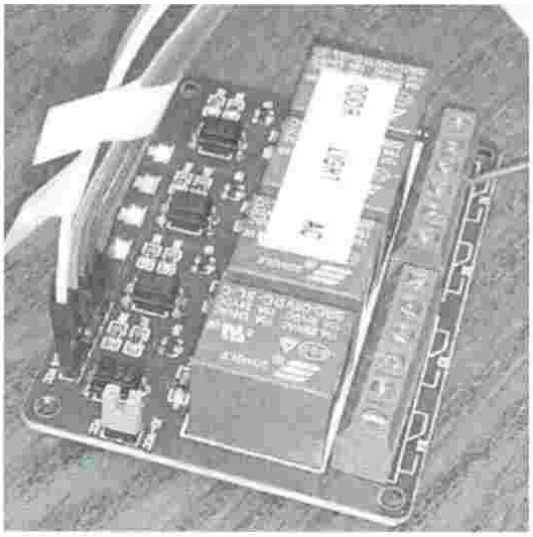

Figura 4.9. Etapa de potencia

La acción de conmutación cierra el circuito de la fuente de energía con la bobina de la chapa eléctrica provocando un accionamiento mecánico en esta última. Otra mejora hecha al sistema fue el etiquetado. Todas las conexiones y los componentes están etiquetados con el fin de evitar cualquier problema cuando se trata de sustituir cualquier elemento, realice una prueba o dar mantenimiento. La figura 4.10 muestra algunas de las etiquetas.

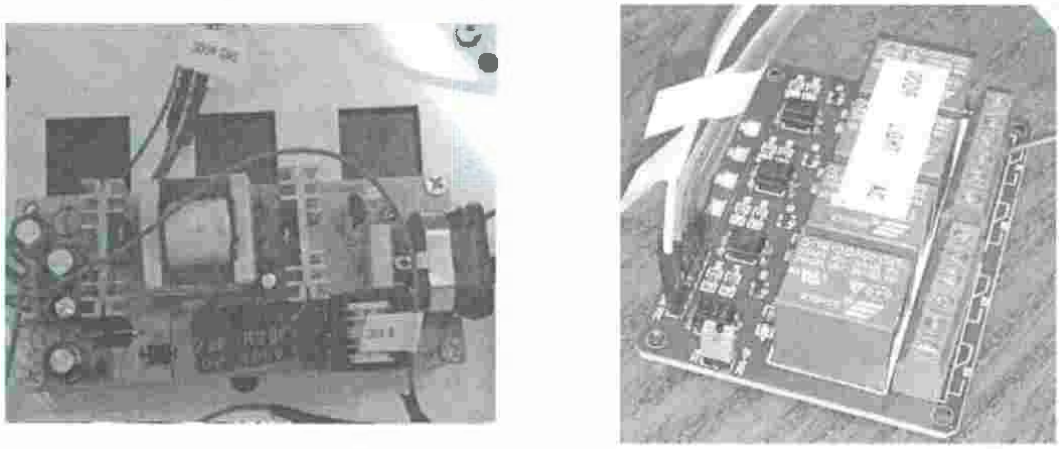

Figura 4.10. Etiquetas del sistema

4.3. Diagramas de Mantenimiento

Hay cuatro elementos que requieren mantenimiento, el lector RFID, el controlador, la etapa de potencia y la chapa eléctrica, la etapa de comunicación se considera parte del controlador mientras que la etapa de potencia, a pesar de ser parte del controlador, es también una interfaz entre 3 componentes del sistema. Las figuras 4.11 a 4.14 muestran los diagramas de mantenimiento para los elementos ilustrados en el diagrama funcional de la figura 4.1.

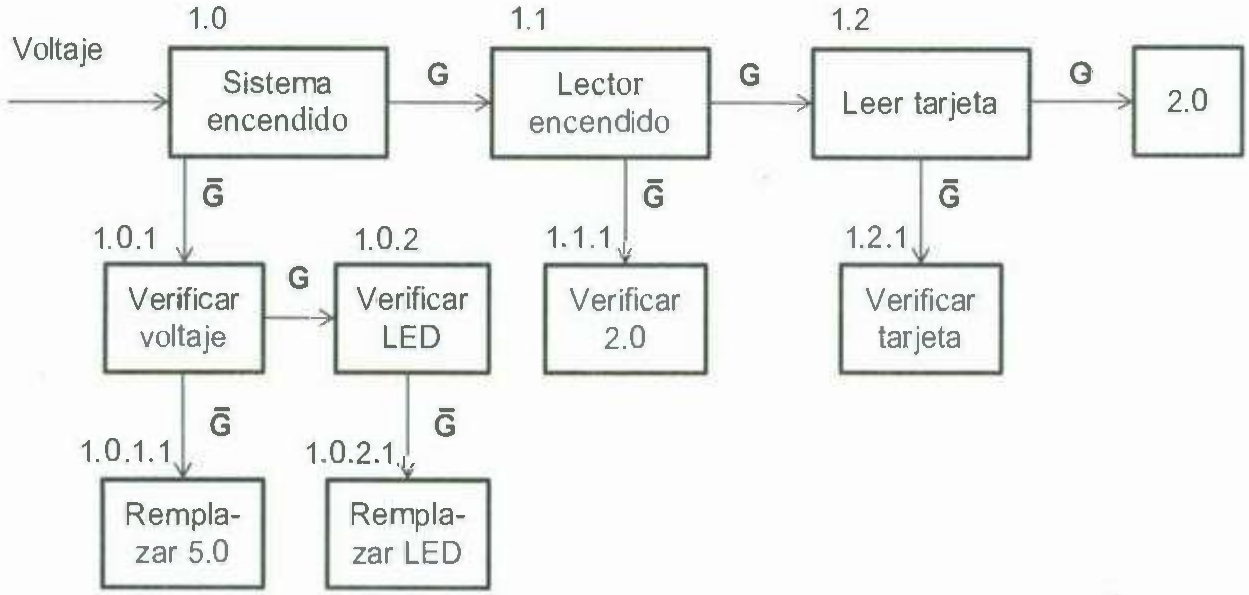

Figura 4.11. Diagrama de mantenimiento para el lector RFID

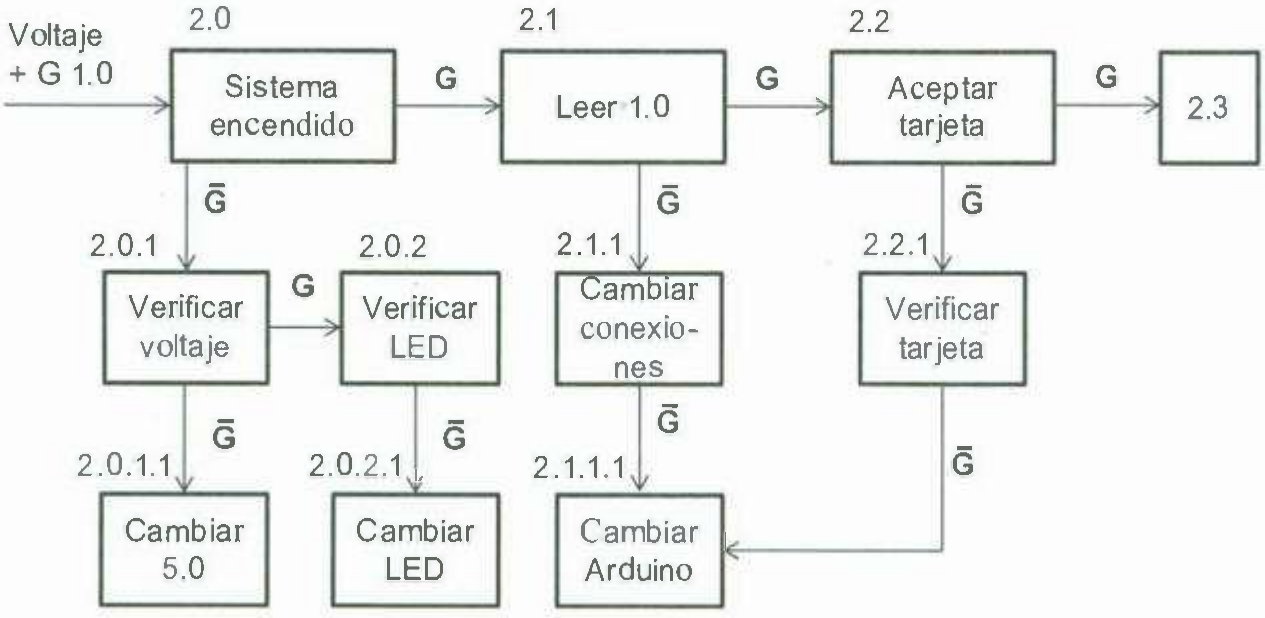

Figura 4.12. Diagrama de mantenimiento para el controlador

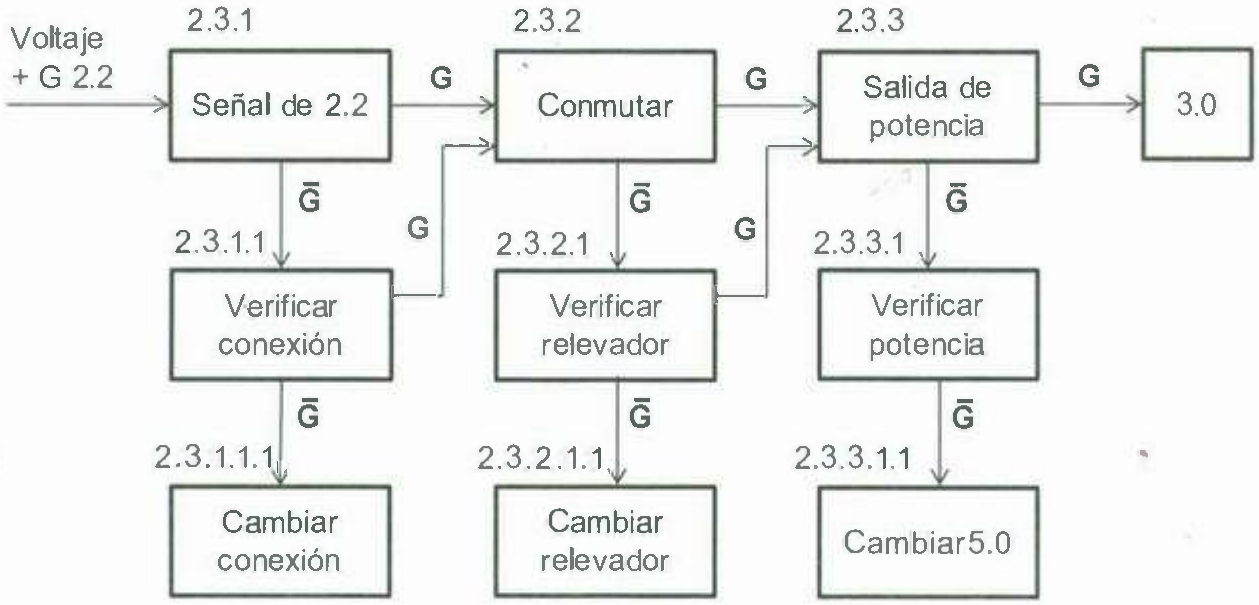

Figura 4.13. Diagrama de mantenimiento de la etapa de potencia

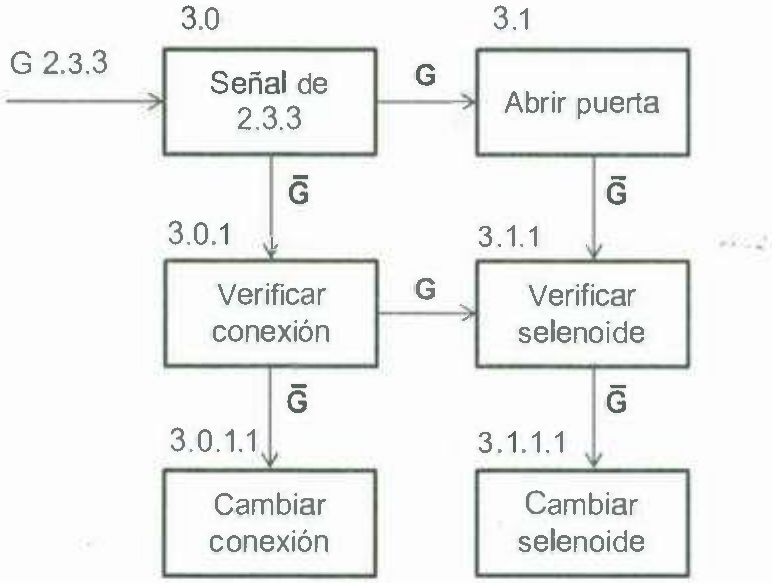

Figure 4.14. Diagrama de mantenimiento para etapa de potencia

4.4 Pruebas y verificación

Con el sistema desarrollado se han podido resolver los problemas establecidos al principio. Después de atender los requerimientos y especificaciones, la solución planteada cumple con los requerimientos del Departamento de Ingeniería Industrial. Las consideraciones tomadas en cuenta para el diseño de la solución fueron:

- El sistema debe trabajar con un voltaje de entre 12 y 15 VCD.
- El sistema debe utilizar tecnología RFID.
- El precio del nuevo sistema debe estar por debajo de los 10 mil pesos.
- La temperatura de operación debe ser de entre 0 y 50 °C.
- El sistema debe operar en salones de clase.
- El tiempo máximo requerido para llevar a cabo cualquier tipo de mantenimiento debe ser 20 minutos.
- El sistema será usado al menos una vez al día y cuando mucho 50 veces por día.
- El tiempo de respuesta no debe exceder 5 segundos.
- La comunicación hacia el exterior se probará con una sola terminal.
- El sistema debe poder recuperarse después de un corte de energía eléctrica.

Las consideraciones anteriores pueden ser formuladas como límites para el sistema, lo cual es útil para realizar algunas pruebas y verificar tanto la operación como la confiabilidad del sistema. La tabla 4.1 muestra los escenarios en los cuales fue probado el sistema y los resultados obtenidos. Como se puede apreciar en dicha tabla, algunos de los escenarios no se pudieron probar ya que no se contaba con el equipo de laboratorio necesario para realizar los experimentos requeridos, sin embargo la aproximación es suficiente para poder demostrar la confiabilidad y robustez del sistema, así como el cumplimiento de las expectativas que se tienen para el diseño.

Tabla 4.1. Escenarios y procedimientos para pruebas y verificación

Escenario	Procedimiento de prueba/verificación	Resultado
La chapa debe ser activada sin errores	Una tarjeta válida se presentó frente al lector (sensor) 100 veces durante dos días (50 veces por día)	El 100% de las veces que se presentó la tarjeta, la chapa fue activada
La puerta no abrirá si se presenta una tarjeta incorrecta	Algunas tarjetas no válidas fueron presentadas frente al lector 50 veces	La chapa no se activa con la tarjeta incorrecta
El Sistema se debe comunicar con una terminal remota	Comandos de apertura de puerta y lectura de información fueron enviados al controlador desde una terminal remota conectada en red	El sistema puede ser controlado y monitoreado a distancia
El Sistema debe recuperarse de un corte de energía eléctrica	El Sistema fue desconectado del suministro de energía eléctrico por 10 minutos y reconectado de nuevo	El Sistema opera inmediatamente después de recibir el voltaje requerido
El tiempo de respuesta del Sistema no debe exceder 5 segundos	Una tarjeta válida fue presentada frente al lector 50 veces y se midió el tiempo de respuesta.	El tiempo promedio de respuesta es de 1 segundo
El sistema debe operar a una temperatura de entre 0 y 50 grados centígrados	El Sistema fue operado a distintas horas desde las 6:00 am hasta las 9:00 pm.	El Sistema trabaja correctamente para temperaturas entre 15 y 40 grados centígrados

4.5 Análisis de los resultados

Después de realizar las pruebas descritas en la tabla 4.1, se puede constatar que el sistema cumple con los requerimientos funcionales del Departamento de Ingeniería Industrial de la Universidad de sonora. Si bien algunos experimentos no se pudieron realizar al 100% por falta de equipo especializado para realizar las pruebas necesarias, el hecho de haber operado el sistema en un ambiente cotidiano, garantiza la confiabilidad del mismo, por ejemplo, para la prueba de temperatura, nunca se alcanzaron los límites establecidos, sin embargo estas fronteras no suelen ser típicas en un ambiente de salón de clases. Otra observación de los resultados obtenidos fue el hecho de que el sistema se recuperó de manera inmediata después de un corte en el suministro de energía, lo cual es deseable, sin embargo para mejorar esta condición de operación se puede buscar la manera de operar el sistema con una batería de respaldo.

Capítulo 5

Conclusiones y trabajo futuro

5.1 Conclusiones

Como se pudo apreciar en las pruebas, el sistema cumple con los requerimientos establecidos en un principio. El sistema propuesto tiene la ventaja de que utiliza módulos claramente identificables que pueden ser reemplazados e inspeccionados de manera aislada mientras el sistema sigue funcionando (con las partes reemplazadas). Otra ventaja del sistema propuesto sobre el sistema que se utiliza actualmente es que la tecnología utilizada en nuestra propuesta es actual y las partes se pueden obtener de varios proveedores, lo cual elimina la limitante de tener un solo proveedor el cual puede establecer los precios de partes y servicios a conveniencia.

Las pruebas de verificación de tarjetas válidas indican que el sistema es capaz de identificar una tarjeta válida de una no válida o con una tecnología diferente. El tiempo promedio de respuesta es de un segundo cumpliendo con las expectativas de respuesta en tiempo que se solicitaban.

Las pruebas de resistencia al corte de suministro y de comunicación fueron exitosas. Toda vez que existe un corte en el suministro eléctrico, el sistema es capaz de recuperarse de manera instantánea una vez que la energía eléctrica se ha restablecido. En cuanto a las pruebas de comunicación, el sistema es capaz de establecer comunicación con una terminal para recibir instrucciones a distancia o para proporcionar los datos de las tarjetas leídas.

Finalmente, se crearon los diagramas de mantenimiento necesarios para que un usuario no experto pudiera proporcionar el mantenimiento necesario en un tiempo no mayor a 20 minutos, lo cual se corroboró realizando prácticas de medición de parámetros y de reemplazo de partes.

5.2 Trabajos futuros

La tendencia actual de los sistemas embebidos es formar parte del llamado Internet de las Cosas por lo que se sugiere que en un futuro se emplee el sistema diseñado para formar parte de esta nueva tendencia conocida como la siguiente evolución del internet. Las ventajas de formar parte de esta evolución incluyen el hecho de poder monitorear y controlar los elementos que no fueron conectados en este trabajo, como son el aire acondicionado, proyector y lámparas de iluminación.

Se debe considerar también el hecho de que los puertos analógicos de la plataforma Arduino no fueron utilizados, dando la oportunidad de agregar sensores de temperatura, corriente y movimiento, los cuales se pueden utilizar en un futuro dentro del mismo esquema del Internet de las Cosas. Un posible escenario consistiría en poder monitorear el estado del aula después de las horas de clase para asegurar que no hay puertas abiertas, aires o lámparas encendidas o incluso si hay movimiento dentro del aula en horas en las cuales se supone que no debería haber actividad. De esta forma se puede hacer un uso inteligente de las instalaciones de nuestra Universidad, específicamente hablando de las aulas.

Bibliografía

[1] Universidad Rovira I Virgili, "Avances en la investigación de la tecnología RFID y sus aplicaciones", Sociedad Española de trazabilidad, 2011. ISBN: 8461544552, 9788461544554

[2] Q. Zhou and J. Zhang, "Research prospect of Internet of Things geography," in Proceedings of the 19th International Conference on Geoinformatics. IEEE, 2011, pp. 1–5.

[3] Proveedores en la ciudad de Hermosillo, investigación de campo realizada en mayo de 2015 por medio de muestreo in situ.

[4] Universitat Politecnica de Catalunya, "El código PBIP", Iniciativa Digital Politecnica, 2008. ISBN: 8498803934, 9788498803938

[5] X. Shi, W. Zhao y Y. Shen, "Automatic License Plate Recognition System Based on Color Image Processing", College of Computer Science and Technology, Zhejiang University, 2005.

[6] Luis Cerdá, Tomás Iturralde, "Procesos en instalaciones infraestructuras comunes de telecomunicaciones", Ediciones Paraninfo, S.A. ISBN: 8428337160, 9788428337168.

[7] Esqueda y Palafox, "Fundamentos para el Procesamiento de imágenes, Universidad Autónoma de Baja California", 2005.

[8] Arduino UNO, página de internet consultada el 10 de julio de 2015, liga: https://www.arduino.cc/en/Main/ArduinoBoardUno

[9] Arduino Ethernet Shild, página de internet consultada el 10 de julio de 2015, liga: https://www.arduino.ce/en/Main/ArduinoEthernetShield

[10] José Ordax, Pilar Ocaña, "Programación web en Java", Ministerio de Educación, 2012. ISBN: 8436954300, 9788436954302