ISBN: 978-99961-50-25-8

ESCUELA ESPECIALIZADA EN INGENIERÍA ITCA – FEPADE

DIRECCIÓN DE INVESTIGACIÓN Y PROYECCIÓN SOCIAL

PROGRAMA DE INVESTIGACIÓN APLICADA

INFORME FINAL DE INVESTIGACIÓN

"Sistema Electrónico para el Registro Administrativo y Optimización de los Recursos Energéticos en el MEGATEC Zacatecoluca"

SEDES Y ESCUELAS PARTICIPANTES: **ESCUELA DE INGENIERÍA ELÉCTRICA**
CENTRO REGIONAL MEGATEC ZACATECOLUCA

AUTOR: TÉC. MANUEL DE JESÚS GÁMEZ

ZACATECOLUCA, ENERO 2015

ISBN: 978-99961-50-25-8

ESCUELA ESPECIALIZADA EN INGENIERÍA ITCA – FEPADE

DIRECCIÓN DE INVESTIGACIÓN Y PROYECCIÓN SOCIAL

PROGRAMA DE INVESTIGACIÓN APLICADA

INFORME FINAL DE INVESTIGACIÓN

"Sistema Electrónico para el Registro Administrativo y Optimización de los Recursos Energéticos en el MEGATEC Zacatecoluca"

SEDES Y ESCUELAS PARTICIPANTES: ESCUELA DE INGENIERÍA ELÉCTRICA
CENTRO REGIONAL MEGATEC ZACATECOLUCA

AUTOR: TÉC. MANUEL DE JESÚS GÁMEZ

ZACATECOLUCA, ENERO 2015

Rectora
Licda. Elsy Escolar SantoDomingo
Vicerrector Académico
Ing. Carlos Alberto Arriola
Vicerrectora Técnica Administrativa
Inga. Frineé Violeta Castillo

Edición:
Dirección de Investigación y Proyección Social
Ing. Mario Wilfredo Montes
Ing. David Emmanuel Agreda
Lic. Ernesto José Andrade
Sra. Edith Cardoza

Director Coordinador del Proyecto
Ing. René Flores Monroy

Autor
Téc. Manuel de Jesús Gámez López

Docentes Investigadores
Ing. Wilfredo Antonio Santamaría
Téc. José Alfonso Ortiz

FICHA CATALOGRÁFICA

621.395
G192s Gámez López, Manuel de Jesús.
Sistema Electrónico para el Registro Administrativo y Optimización
sv de los Recursos Energéticos en el MEGATEC Zacatecoluca /
Manuel de Jesús Gámez López, Wilfredo Antonio Santamaría, José
Alonso Ortiz. - 1ª ed. – San Salvador, El Salvador: ITCA Editores, 2015.
136 p. : il. ; 28 cm.

ISBN: 978-99961-50-25-8

1. Electrónica digital. 2. Sistemas de Información. I. Santamaría, Wilfredo Antonio, coaut. II. Ortiz, José Alfonso, coaut. III. Título.

Este documento es una publicación de la Escuela Especializada en Ingeniería ITCA–FEPADE, tiene el propósito de difundir conocimiento y resultados de proyectos entre la comunidad académica y el sector empresarial. El contenido de este Informe de Investigación puede ser reproducido parcial o totalmente, previa autorización escrita de la Escuela Especializada en Ingeniería ITCA–FEPADE. Para referirse al contenido, debe citar la fuente de información. El contenido de este documento es responsabilidad de los autores y los docentes investigadores citados.

Sitio web: www.itca.edu.sv
Correo electrónico: bibliotecologos@itca.edu.sv
PBX: (503) 2132 – 7400 /FAX: (503) 2132 – 7423

Tiraje: 16 ejemplares
ISBN: 978-99961-50-25-8
Año 2015

CONTENIDO

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

1. INTRODUCCIÓN.

Los sistemas de Control de Acceso Físico Basados en Tarjetas Inteligente para el manejo de acceso a recursos están adquiriendo una importancia cada vez mayor para organizaciones en todas partes del mundo, desde pequeñas compañías hasta grandes empresas corporativas y cuerpos gubernamentales de todos los tamaños.

La administración de acceso a recursos significa controlar tanto el acceso físico como el acceso lógico, ya sea como un esfuerzo independiente o a través de un abordaje integrado. El control de acceso físico protege contra robo o usurpación tanto de bienes tangibles como intelectuales. El control de acceso lógico permite a las empresas y organizaciones limitar el acceso a los datos, a las redes y las estaciones de trabajo solamente para aquellos que están autorizados para tener dicho acceso.

El sistema de control de acceso físico es una red coordinada de tarjetas de identificación, lectores electrónicos, bases de datos especializadas, software y computadoras diseñadas para monitorear y controlar el tráfico a través de puntos de acceso.

Los sistemas de control de acceso físico basados en tarjetas inteligentes son una herramienta de seguridad poderosa, eficiente para proteger los bienes de una empresa. A cada empleado o contratista se le emite una tarjeta de identidad inteligente que muestra la información de la empresa y diseños impresos, tanto para limitar la posibilidad de falsificación como para identificar que la tarjeta es oficial. Generalmente, la tarjeta muestra una foto de su portador. Cada tarjeta almacena información protegida sobre la persona y sobre los privilegios de esta persona. Cuando la persona se registra inicialmente y acepta la tarjeta, estos privilegios son diseminados a través de todo el sistema de forma veraz y segura (si tales privilegios cambian, la nueva información puede ser inmediatamente actualizada de manera segura a través de la red). Cuando la tarjeta es colocada dentro o cerca de un lector electrónico, el acceso se brinda o se niega de forma segura y precisa a todos los espacios adecuados (por ejemplo, un campo, un garaje de estacionamientos, un edificio o una oficina). Cuando un empleado deja la organización, todos los privilegios de acceso físico son removidos de una sola vez. Cualquier tentativa futura por esta persona de reingresar al establecimiento usando una tarjeta expirada o revocada, puede ser negada y este hecho registrado automáticamente.

Tanto las empresas privadas como las agencias de gobierno están implementando cada vez más los sistemas de control de acceso basados en tarjetas inteligentes.

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

2. PLANTEAMIENTO DEL PROBLEMA.

2.1 DEFINICIÓN DEL PROBLEMA

En las aulas de clases de MEGATEC - ZACATECOLUCA, se utilizan diversos recursos, para realizar la actividad de enseñanza. En cada hora de clases o laboratorio, el aire acondicionado y las luminarias, se utilizan al 100%; lo que genera el consumo indispensable de energía eléctrica; generando elevados costos de este recurso. En ocasiones, las personas que utilizan el aula, no apaga el aire acondicionado y/o las luminarias, por olvido, o porque no existe un mecanismo, que le permita ejecutar siempre dicha acción, lo que genera un consumo extra de energía.

El recurso humano, es otro recurso indispensable, para el desarrollo del servicio de enseñanza. Para el control de las horas clases, y generación de la planilla de pago de los docentes, se deben de elaborar diversos reportes; acción, que genera tiempo y papelería, para el área administrativa.

El proyecto busca, hacer más eficientes los procesos de control relacionados, con el uso de los recursos: De energía eléctrica y de recurso humano; a través de, un mecanismo automatizado, que permita conocer y optimizar los recursos, más vitales, en el servicio de enseñanza, lo que ayudará a la institución, a ser más eficiente y a obtener información precisa, para la toma de decisiones.

2.2 JUSTIFICACIÓN.

La Escuela Especializada en Ingeniería ITCA-FEPADE regional Zacatecoluca se siente comprometida con el ahorro energético, la optimización de recursos y el uso e integración de nuevas tecnologías, en atención al **Direccionamiento Estratégico** de nuestra Institución para el quinquenio 2010 – 2014 y a los objetivos específicos del programa **ITCA ambiente**. En dicho Direccionamiento Estratégico en su objetivo No. 10 se plantea “disponer de instalaciones, equipos y facilidades de calidad plenamente integrados”, presentando cinco iniciativas estratégicas, dentro de las cuales destacamos las siguientes tres:

- Plan de *racionalización* y *optimización* de espacios y equipos.

- Favorecer la *accesibilidad*.

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

- *Modernización* y ampliación de la infraestructura física y tecnológica.

Y uno de los objetivos específicos englobados en el programa **ITC ambiente** expone:

- Promover a la institución como un ente que es parte de la solución al problema ambiental.

El *ahorro energético* es una solución de vital importancia para resolver el problema ambiental.

La regional toma la decisión de buscar metodologías dentro de las cuales se pueda optimizar el uso de recursos energéticos y al mismo tiempo modernizar la infraestructura de las instalaciones de la misma.

El uso de recursos energéticos y tecnológicos en un aula es indispensable para el proceso de enseñanza-aprendizaje, sin embargo, existen situaciones dentro de la regional en donde se dificulta controlar el uso de dichos recursos cuando no se está desarrollando ninguna actividad dentro del aula. Esto conlleva a un desperdicio energético y deterioro de los recursos disponibles en el aula, pues permanecen activados más tiempo del necesario.

El proyecto que se presenta plantea desarrollar un sistema de control electrónico que habilite la alimentación eléctrica dentro de las aulas el tiempo necesario para que se lleven a cabo las actividades académicas dentro de las mismas, sin ningún inconveniente.

El sistema así planteado, permitirá que los recursos dentro del aula se optimicen, generando ahorro energético y una mayor durabilidad y aprovechamiento de los recursos disponibles en el aula. Contribuyendo así a cumplir lo planteado en los direccionamientos estratégicos de nuestra Institución y en los objetivos del programa ITCA ambiente y a promover a la institución como un ente comprometido con el medio ambiente y consciente de la crisis energética mundial que se vive hoy en día.

3. OBJETIVOS.

OBJETIVO GENERAL

Diseñar sistema electrónico para el registro administrativo y la optimización de los recursos energéticos en las instalaciones del MEGATEC Zacatecoluca.

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

OBJETIVOS ESPECIFICOS.

- Elaborar el diseño de la propuesta de solución tecnológica que contribuya a controlar y aprovechar de manera más efectiva el uso del recurso de energía en las aulas de clase.
- Identificar la información que se utilizará para el registro y control de la utilización del recurso energético y seguimiento administrativo del recurso humano.
- Desarrollar una aplicación informática que ayude a la administración del recurso humano, en relación a las horas de clases.

4. HIPOTESIS - PREGUNTA PROBLEMA

HIPOTESIS

- Se tendrá un mejor aprovechamiento del recurso energético en las aulas de clase mediante el apoyo de un sistema electrónico para el control de dicho recurso.

PREGUNTA PROBLEMA.

- ¿Cómo optimizar la utilización de la energía eléctrica en las aulas de clase del ITCA regional Zacatecoluca?

5. MARCO TEORICO DE LA INVESTIGACIÓN.

El proyecto desarrollado consiste en controlar el suministro de energía a un aula de clases específica, de manera que éste se habilite única y exclusivamente en los horarios en que se llevan a cabo actividades académicas, tales como: sesiones de clases, prácticas de taller y prácticas de laboratorio. Esto se logra a través de una tarjeta con un lector adecuado para ella, el lector interactúa con un control electrónico el cuál es el encargado de habilitar o deshabilitar el suministro de energía eléctrica al aula. El control electrónico también interactúa con un sistema informático de bases de datos ubicado en un servidor remoto con el cual se comunicará mediante el protocolo de red inalámbrica WIFI (IEEE 802.11). El propósito de comunicar el sistema de control con un servidor tiene como objetivo principal llevar un registro estadístico del uso del aula que se está controlando. Los datos a registrar pueden incluir: hora de entrada y

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

salida al aula por parte del docente, cuáles docentes y en qué días y/o horarios utilizan el aula, etc. Para poder desarrollar este proyecto se hizo necesario el conocimiento y dominio de ciertas tecnologías de las cuáles se presenta a continuación una breve descripción:

5.1 Microcontroladores y sistemas de control electrónicos.

El Microcontrolador es un computador construido dentro de un dado de silicio que se encuentra encapsulado como circuito integrado. Por ello es que se conoce como un circuito integrado programable, capaz de ejecutar las órdenes grabadas en su memoria a través de un código de programa. En el interior del microcontrolador se encuentran las tres principales unidades funcionales de una computadora: Unidad Central de Procesamiento, memoria y periféricos de entrada/salida.

En la memoria del microcontrolador se almacena un único programa destinado a controlar o ejecutar una aplicación concreta.

El CPU es la unidad más compleja del microcontrolador, dentro de ella recae la lógica para la decodificación y ejecución de las instrucciones planteadas en el programa, determina parámetros tales como el tipo de conjunto de instrucciones, velocidad de ejecución, tiempo del ciclo de máquina y tipo de buses que puede tener el sistema.

Los periféricos de entrada/salida son la parte del micrcocontrolador capaz de soportar el conexionado físico de sensores y actuadores del sistema a gobernar o controlar y todos los recursos complementarios disponibles. Tiene como finalidad exclusiva atender los requerimientos de la tarea a la que se dedica el microcontrolador. En el caso del presente proyecto, sería a través de los periféricos de entrada/salida que el sistema de control del aula se comunicaría con el lector de la tarjeta para poder determinar si se habilita o no el suministro de energía eléctrica al aula.

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

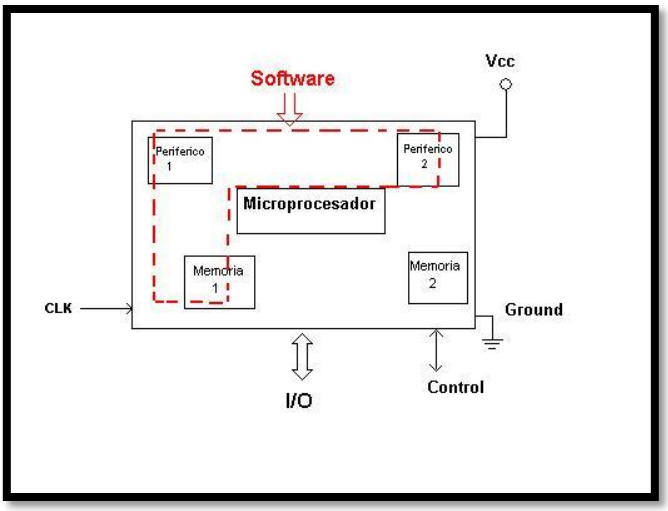


Fig. 1 Representación a bloques de la estructura interna básica de un microcontrolador.

5.2 Instrumentación y sistemas de adquisiciones de datos.

La instrumentación electrónica es una rama de la electrónica encargada del diseño y manejo de los aparatos electrónicos y eléctricos, principalmente para su uso en mediciones. Su aplicación principal se desarrolla en el censado y procesamiento de información proveniente de variables que se encuentran en la naturaleza y que de alguna forma han pasado a ser objetos de estudio. Tal es el caso de las diferentes variables físicas y químicas que encontramos en los diversos campos de las ciencias aplicadas. Para el censado de dichas variables físicas y químicas se hace necesario el uso de dispositivos denominados sensores. El **sensor** es el encargado de convertir la señal a ser censada o monitoreada en una variable eléctrica. Dicha variable eléctrica (analógica) debe de recibir un tratamiento digital para poder ser leída o desplegada en un panel, proporcionando información coherente exacta y confiable. Al proceso de tratar digitalmente una señal analógica, arrojada por un sensor, para su procesamiento en un ordenador mediante una aplicación de software o un hardware especializado (sistema digital) se le conoce como Adquisición de Datos. Básicamente el proceso consiste en tomar un conjunto de señales físicas, convertirlas en tensiones eléctricas y digitalizarlas de manera que se puedan procesar mediante una computadora u ordenador o un controlador de automatización programable. Se requiere una etapa de acondicionamiento, que adecua la señal a niveles compatibles con el elemento que hace la transformación a señal digital. El elemento que hace dicha transformación es el módulo de digitalización o tarjeta de Adquisición de Datos (DAQ). El

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

acondicionamiento de señales suele ser necesario si la señal desde el transductor no es adecuado para la DAQ hardware que se utiliza. La señal puede ser amplificada o des amplificada, o puede requerir de filtrado, o un cierre patronal, en el amplificador se incluye para realizar demodulación. Varios otros ejemplos de acondicionamiento de señales podría ser el puente de conclusión, la prestación actual de tensión o excitación al sensor, el aislamiento, linealización, etc. este pre tratamiento de la señal normalmente lo realiza un pequeño módulo acoplado al transductor.

DAQ hardware son por lo general las interfaces entre la señal y un PC. Podría ser en forma de módulos que pueden ser conectados a la computadora de los puertos (paralelo, serie, USB, etc...) o ranuras de las tarjetas conectadas a (PCI, ISA) en la placa madre. Por lo general, el espacio en la parte posterior de una tarjeta PCI es demasiado pequeño para todas las conexiones necesarias, de modo que una ruptura de caja externa es obligatorio. Las tarjetas DAQ a menudo contienen múltiples componentes (multiplexores, ADC, DAC, TTL-IO, temporizadores de alta velocidad, memoria RAM). Estos son accesibles a través de un bus por un micro controlador, que puede ejecutar pequeños programas. El controlador es más flexible que una unidad lógica dura cableada, pero más barato que una CPU de modo que es correcto para bloquear con simples bucles de preguntas.

Driver software normalmente viene con el hardware DAQ o de otros proveedores, y permite que el sistema operativo pueda reconocer el hardware DAQ y dar así a los programas acceso a las señales de lectura por el hardware DAQ. Un buen driver ofrece un alto y bajo nivel de acceso.

5.3 Programación Orientada a Objetos.

La Programación Orientad a Objetos o POO, es una propuesta tecnológica que está adoptada por una comunidad de programadores para resolver de forma particular uno varios problemas claramente delimitados. La POO, como muy bien lo indica su nombre utiliza objetos en sus interacciones, para diseñar aplicaciones y programas informáticos. Los objetos son entidades que tienen un determinado: estado, comportamiento (método) e identidad:

El estado está compuesto de datos o informaciones; serán uno o varios atributos a los que se habrán asignado unos valores concretos (datos).

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

El comportamiento está definido por los métodos o mensajes a los que sabe responder dicho objeto, es decir, qué operaciones se pueden realizar con él.

La identidad es una propiedad de un objeto que lo diferencia del resto; dicho con otras palabras, es su identificador (concepto análogo al de identificador de una variable o una constante). Un objeto contiene toda la información que permite definirlo e identificarlo frente a otros objetos pertenecientes a otras clases e incluso frente a objetos de una misma clase, al poder tener valores bien diferenciados en sus atributos. A su vez, los objetos disponen de mecanismos de interacción llamados métodos, que favorecen la comunicación entre ellos. Esta comunicación favorece a su vez el cambio de estado en los propios objetos. Esta característica lleva a tratarlos como unidades indivisibles, en las que no se separa el estado y el comportamiento.

Los métodos (comportamiento) y atributos (estado) están estrechamente relacionados por la propiedad de conjunto. Esta propiedad destaca que una clase requiere de métodos para poder tratar los atributos con los que cuenta. El programador debe pensar indistintamente en ambos conceptos, sin separar ni darle mayor importancia a alguno de ellos. Hacerlo podría producir el hábito erróneo de crear clases contenedoras de información por un lado y clases con métodos que manejen a las primeras por el otro. De esta manera se estaría realizando una programación estructurada camuflada en un lenguaje de programación orientado a objetos. La POO difiere de la programación estructurada tradicional, en la que los datos y los procedimientos están separados y sin relación, ya que lo único que se busca es el procesamiento de unos datos de entrada para obtener otros de salida. La programación estructurada anima al programador a pensar sobre todo en términos de procedimientos o funciones, y en segundo lugar en las estructuras de datos que esos procedimientos manejan. En la programación estructurada solo se escriben funciones que procesan datos. Los programadores que emplean POO, en cambio, primero definen objetos para luego enviarles mensajes solicitándoles que realicen sus métodos por sí mismos.

5.4 Redes informáticas inalámbricas WIFI.

Una red inalámbrica informática, no es más que un conjunto de ordenadores o computadoras, o de cualquier otro dispositivo informático, comunicados entre sí mediante soluciones que no requieran el uso de cables de interconexión. Para disponer de una red inalámbrica sólo hace falta instalar una tarjeta de red inalámbrica en los ordenadores involucrados, hacer configuración y todo queda listo para funcionar de forma óptima. Este proceso resulta mucho

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

más rápido y flexible que instalar una red cableada. Una vez instalada una red inalámbrica, su utilización es prácticamente idéntica a la de una red cableada. Los ordenadores o computadoras que forman parte de la red pueden comunicarse entre sí y compartir toda clase de recursos. Se pueden compartir archivos, directorios, impresoras, unidades de disco, o incluso, el acceso a otras redes, como puede ser el Internet. Para el usuario final en general, no hay diferencia entre estar conectado a una red cableada o a una red inalámbrica. De la misma forma, al igual que ocurre con las redes cableadas, una red inalámbrica puede estar formada por tan sólo dos computadoras o por miles de ellas.

Existen diferentes tipos de redes inalámbricas, dentro de las cuales destacan las redes inalámbricas de área local (WLAN: Wireless Local Area Network), las cuáles se caracterizan por tener cobertura de unos cientos de metros solamente. Este tipo de redes busca utilizarse para crear una red de entorno local entre computadoras o terminales informáticas situadas en un mismo edificio o grupo de edificios. Dentro de las distintas tecnologías utilizadas para desarrollar redes inalámbricas de área local, una de las más utilizadas a nivel doméstico y comercial es la tecnología conocida como Wi-Fi (Wireles Fidelity) la cual se encuentra regulada o normada por el estándar IEEE 802.11.

¿Qué es una red Wi-Fi?. Wi-Fi es una marca de la Wi-Fi Alliance (anteriormente la WECA: Wireless Ethernet Compatibility Alliance), la organización comercial que adopta, prueba y certifica que los equipos cumplen los estándares 802.11 relacionados a redes inalámbricas de área local. En concreto Wi-Fi es un mecanismo de conexión de dispositivos electrónicos de forma inalámbrica. Los dispositivos habilitados con Wi-Fi, tales como: un ordenador personal, una consola de videojuegos, un smartphone o un reproductor de audio digital, pueden conectarse a Internet a través de un punto de acceso de red inalámbrica. Con el sistema WiFi se pueden establecer comunicaciones a una velocidad máxima de 11Mbps, alcanzándose distancias de hasta varios cientos de metros. No obstante, versiones más recientes de esta tecnología permiten alcanzar los 22, 54 y hasta los 100 Mbps.

5.5 Sistemas de bases de datos.

Una base de datos o banco de datos es un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso. En este sentido, una biblioteca puede considerarse una base de datos compuesta en su mayoría por documentos y textos impresos en papel e indexados para su consulta. Actualmente, y debido al desarrollo

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

tecnológico de campos como la informática y la electrónica, la mayoría de las bases de datos están en formato digital (electrónico), y por ende se ha desarrollado y se ofrece un amplio rango de soluciones al problema del almacenamiento de datos.

Existen programas denominados sistema gestor de bases de datos, abreviado SGBD, que permiten almacenar y posteriormente acceder a los datos de forma rápida y estructurada. Las propiedades de estos SGBD, así como su utilización y administración, se estudian dentro del ámbito de la informática. Las aplicaciones más usuales son para la gestión de empresas e instituciones públicas. También son ampliamente utilizadas en entornos científicos con el objeto de almacenar la información experimental.

XBEE PRO. Los Xbee son pequeños dispositivos que pueden comunicarse entre sí, de manera inalámbrica. Son fabricados por Digi International, los cuales ofrecen una gran variedad de combinaciones de hardware, protocolos, antenas y potencias de transmisión.

ZigBee. Es un protocolo de comunicaciones inalámbricas basado en el estándar 802.15.4, está pensado para comunicaciones a baja velocidad entre dos o varios dispositivos, se pueden formar redes con miles de dispositivos comunicándose entre sí, por lo que es ideal para muchas aplicaciones. En las redes ZigBee encontramos tres tipos de dispositivos:

Coordinador: En toda red sea de doscientos o de dos dispositivos, debe haber un coordinador, sólo puede haber uno por red y entre sus tareas están las de formar y gestionar la red.

Router: Son dispositivos de la red que tienen la capacidad de enviar, recibir y enrutar información. Pueden actuar como mensajeros entre dispositivos que están muy alejados para establecer una comunicación directamente; los dispositivos ZigBee no están pensados para comunicaciones de largas distancias, sino para trabajar en redes de sensores y cubrir esas largas distancias pasando la información entre los distintos nodos.

End device: Estos serían los dispositivos de bajo consumo. El coordinador y los routers deben estar siempre encendidos ya que pueden actuar como mensajeros entre otros dispositivos, por lo que lo normal puede ser conectarlos a la red eléctrica. Los end devices pueden enviar y recibir información pero no pueden actuar como mensajeros entre otros dos dispositivos de la red, lo normal es que el end device esté en un modo de bajo consumo y se despierte cuando quiere enviar o recibir información, alargando la duración de sus baterías durante mucho tiempo. Como los end device pueden estar dormidos en un modo de bajo consumo, necesitan

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

estar asociados a un coordinador o a un router, que guarden los mensajes que han sido enviados para ellos mientras estaban dormidos y se los hagan llegar cuando despierten. En una red ZigBee debe haber un coordinador (sólo uno) y todos los routers y end devices que queramos, la red más sencilla sería un coordinador más un router o end device.

XBee Explorer USB. Esta placa nos va a permitir comunicar el pc con el módulo XBee, es un chip FTDI que hace de puente entre el USB del PC y la UART del microcontrolador. Esta se utiliza para actualizar, descargar firmware y configurar los módulos XBee que utilizamos en el presente proyectos. También la vamos a utilizar para dotar a nuestro PC de conexión ZigBee y conectarlo a la red de dispositivos para enviar y recibir datos, conectamos un módulo a la placa conectada al puerto USB del PC. Para cambiar el firmware y configurar los módulos utilizamos el X-CTU, un programa de Digi.

Breakout board. Si queremos pinchar el módulos XBee en una placa de prototipos para hacer pruebas debemos utilizar un placa que adapte el paso de los pines del módulo al paso de los pines de la protoboard. Además de los conectores correspondientes que debemos soldar a la placa adaptadora y un intercambiador de niveles de tensión si el microcontrolador externo va a funcionar a 5V.

RFID Reader ID-12LA. Pequeño módulo lector RFID con antena integrada muy sencillo de utilizar, podemos alimentar el módulo y acercar un tarjeta RFID, como resultado devuelve su código de identificación mediante su puerto serie, por lo que podremos recuperarlo de forma sencilla mediante cualquier micro controlador con UART o hacia un PC utilizando un conversor USB/Serie.

Características:

- Alimentación: 5V
- frecuencia de lectura: 125kHz
- Compatible con EM4001 64-bit RFID tag
- Conexión série: 9600bps TTL y RS232
- Magnetic stripe emulation output
- Distancia de lectura: 100mm aprox.
- Dimensiones: 25x26mm

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

Tipos de Memorias Usadas en las Tarjetas Inteligentes

Memoria de sólo lectura - ROM. Contiene el sistema operativo del circuito integrado. El sistema operativo o el juego de comandos controla todas las comunicaciones entre el chip el dispositivo lector. El sistema operativo controla el acceso a los archivos del sistema o applets. La memoria es escrita durante su producción por el productor manufacturero y una vez escrito, no puede ser alterado.

Memoria de sólo lectura programable y borrable - EEPROM. Es una memoria no volátil y es memoria lectura/escritura para el almacenamiento de datos. El acceso a la memoria EEPROM es controlado por el sistema operativo del circuito integrado. La memoria puede contener 128 Kbyte de memoria con el potencial para más de 256 Kbyte. La memoria puede contener datos como el número de identificación personal (PIN) que solo puede ser acezado por el sistema operativo, otros datos, como el numero serial de la tarjeta, pueden ser escritos en la memoria EEPROM durante su fabricación. EEPROM es típicamente usado para aplicaciones de datos y para ciertas funciones filtradas. La mayoría de las memorias EEPROM son usadas para almacenar datas como registros biométricos, datos financieros, tarjetas de pago, información demográfica y registro de transacciones. La memoria puede ser programada o borrada de decenas hasta cientos de miles de veces.

Memoria de acceso aleatoria - RAM. Es una memoria volátil, usada para almacenamiento temporal de registros por el microcontrolador.

Memoria RAM – Ferro Eléctrica. (También llamada Fe-RAM). Es otro tipo de memoria no volátil. Esta memoria puede leer datos cientos de veces más rápido a bajo voltaje. Esta memoria combina la velocidad de lectura y escritura de una memoria dinámica RAM con la de almacenar datos cuando se apaga la fuente de poder. Como es una memoria rápida con bajos requerimientos de poder, tiene muchas aplicaciones en dispositivos de pequeños consumidores. FRAM es más veloz que una memoria flash. Se espera que remplace las memorias EEPROM y SRAM para algunas aplicaciones y tiene el potencial para convertirse en una componente clave en aplicaciones inalámbricas futuras.

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

Memorias Flash. Es un tipo de memoria permanentemente energizada, no volátil que puede ser borrada y reprogramada en unidades de memoria llamadas bloques. Las memorias flash son menos costosas que las memorias EEPROM, pero no puede ser programada y borrada tantas veces y por lo general no puede programarse o borrarse bytes sencillos de memoria.

Estándar internacional relacionado con las tarjetas de identificación electrónicas

Normativa: ISO/IEC 7816.

La norma ISO/IEC 7816 define los estándares para la fabricación y uso de las tarjetas inteligentes. Está compuesta por 15 apartados que tratan cada uno de los aspectos a tener en cuenta a la hora de diseñar, fabricar u operar con esta tecnología.

ISO 7816-2: Tamaño y localización de los contactares. En este punto se define la dimensión y ubicación de los contactares en la tarjeta de PVC. También se describe el número de contactos que deben existir, así como su función y posición.

ISO7816-3: Señales electrónicas y protocolos de transmisión. Potencia, forma de señal e intercambio de información entre una tarjeta inteligente y un sistema lector. Incluye los siguientes sub-apartados: ISO7816 - 3.1 Valores de corriente y tensión, ISO 7816-3.2 Procedimiento operativo para tarjetas con circuitos integrados, ISO7816-3.3 Respuesta aun reseteo ATR (Answer to Reset), ISO7816-3.4 Selección de tipo de protocolo (PTS, Protocol Type Selection), ISO 7816-3.5 Tipo de protocolo T=0, protocolo de transmisión de caracteres asíncrono half- duplex.

ISO 7816-4: Organización, seguridad y comandos para el intercambio de información. Contenido de los mensajes intercambiados entre tarjeta inteligente y dispositivo lector, así como los comandos, la estructura del sistema de archivos y los datos que albergan, métodos de acceso a los datos y métodos de seguridad.

ISO 7816-6: Interoperabilidad en los elementos de datos para el intercambio. Elementos de datos (DEs) utilizados para el intercambio inter-industrial basado en tarjetas de circuitos integrados (ICC) con contactos y sin contactos. Se proporciona el identificador, nombre,

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

descripción, formato, la codificación y la disposición de cada DE y define los medios de recuperación de las de la tarjeta.

ISO7816-7: Interoperabilidad en los comandos de la tarjeta (SCQL). Método seguro de base de datos relacional para tarjetas inteligentes basadas en interfaces SQL.

ISO7816-8: Comandos para operaciones de seguridad. Comandos para tarjetas de circuitos integrados, ya sean con contactos o sin contactos, que se pueden utilizar para operaciones criptográficas. Estos comandos son complementarios y se basan en los comandos descritos es el apartado ISO7816-4.

ISO 7816-9: Comandos para la gestión de la tarjeta. Comandos para tarjetas de circuitos integrados, con contactos y sin contactos, para la gestión de archivos. Estos comandos abarcan todo el ciclo de vida completo de la tarjeta y, por lo tanto, algunos comandos pueden ser utilizados antes de que la tarjeta haya sido expedida subtitular o después de la tarjeta haya caducado.

ISO7816-10: Señales electrónicas para operación síncrona. Métodos utilizados por las tarjetas de memoria para aplicaciones tales como tarjetas telefónicas prepago o máquinas expendedoras.

ISO 7816-11: Verificación de la identidad personal a través de métodos biométricos. Uso de los comandos y objetos de datos relacionados con la verificación personal a través de métodos biométricos en tarjetas inteligentes. Los comandos utilizados se definen en la norma ISO 7816-4.

Los objetos de datos están parcialmente definidos en la parte importada de la norma ISO/IEC 19785-1

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

ISO7816-15: Aplicación de información criptográfica. Aplicación que contiene información sobre la funcionalidad criptográfica. Por otra parte, se define una sintaxis común (en ASN.1) y formato de la información criptográfica y mecanismos para compartir esta información cuando proceda.

Este resumen únicamente recoge la normativa que se aplica directamente sobre las tarjetas inteligentes y dispositivos estándar que operan con ellas. Para aplicaciones específicas sobre tarjetas inteligentes existen normas que se deben tener en cuenta como la EMV (Europa y MasterCard VISA) para trabajar con sistema de pago o GSM para trabajos basados en tarjetas SIM.

Módulo RFID RC522 - 13.56Mhz

Fig. 2. Lector de tarjetas RFID para Arduino.

Un lector de tarjetas es un dispositivo intermedio entre la tarjeta inteligente y el sistema que interactúa con ella. Permite la lectura y escritura en las tarjetas inteligentes y, como consecuencia de la gran expansión que están experimentando las tarjetas en todos los sectores, cada vez resultan más útiles e imprescindibles este tipo de dispositivos.

Existen distintos tipos de lectores de tarjetas dependiendo de sus características principales y de su capacidad operativa. A continuación se clasifican según diversas características:

Según su capacidad operativa

- **Solo lectores:** son dispositivos que solo son capaces de leer datos de una tarjeta. Mantiene un proceso de comunicación que termina con una extracción de datos.

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

- **Lectores/grabadores:** además de leer datos también son capaces de grabarlos en la memoria de la tarjeta inteligente. Tienen un precio superior a los anteriores pero permiten un mayor rango de operaciones con las tarjetas.

Según su conexión con el sistema

- **Integrados o internos:** son lectores diseñados para ser instalados de forma permanente dentro del sistema que hará uso de ellos. Por ejemplo: un cajero automático.

- **Externos:** se trata de lectores portátiles. Son fáciles de transportar dado su reducido tamaño y son más económicos que los lectores fijos. Su conexión con el sistema anfitrión suele ser por USB o por medio de una interfaz PCMCIA (Personal Computer Memory Card International Association).

Según su compatibilidad con las tarjetas:

- **Específicos:** son lectores específicos para trabajar con un solo tipo de tarjeta. Normalmente son para uso doméstico o situaciones en las que todos los usuarios posean el mismo tipo de tarjeta. Son lectores asequibles y sencillos de usar.

- **Multi-tarjeta:** lectores capaces de operar con tarjetas que poseen distintas tecnologías. Las más habituales son tarjetas con contactos, sin contactos o RFID y tarjetas de banda magnética. Son lectores diseñados para entornos empresariales o comerciales.

Estas son las tres grandes características que se deben tener en cuenta a la hora de diseñar o adquirir un lector de tarjetas inteligentes. Tomando una de las opciones de cada uno de los grupos se puede obtener el lector acorde con las necesidades del proyecto que lo requiere.

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

Plataforma de hardware libre, basada en una placa con un microcontrolador.

Fig. 3. Forma física de una placa de Arduino

Descripción

Arduino y MEGA es una plataforma de hardware libre, basada en una placa con un microcontrolador y un entorno de desarrollo, diseñada para facilitar el uso de la electrónica en proyectos multidisciplinares.

El hardware consiste en una placa con un microcontrolador Atmel AVR y puertos de entrada/salida.[4] Los microcontroladores más usados son el Atmega168, Atmega328, Atmega1280, ATmega8 por su sencillez y bajo coste que permiten el desarrollo de múltiples diseños. Por otro lado el software consiste en un entorno de desarrollo que implementa el lenguaje de programación Processing/Wiring y el cargador de arranque que es ejecutado en la placa.

Arduino se puede utilizar para desarrollar objetos interactivos autónomos o puede ser conectado a software tal como Adobe Flash, Processing, Max/MSP, Pure Data). Las placas se pueden montar a mano o adquirirse; el entorno de desarrollo integrado libre se puede descargar gratuitamente. Arduino puede tomar información del entorno a través de sus entradas y controlar luces, motores y otros actuadores. El microcontrolador en la placa Arduino se programa mediante el lenguaje de programación Arduino (basado en Wiring) y el entorno de desarrollo Arduino (basado en Processing). Los proyectos hechos con Arduino pueden ejecutarse sin necesidad de conectar a una computadora.

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

Aplicaciones

El módulo Arduino ha sido usado como base en diversas aplicaciones electrónicas:

- Xoscillo: Osciloscopio de código abierto.
- Equipo científico para investigaciones.
- Arduinome: Un dispositivo controlador MIDI.
- OBDuino: un económetro que usa una interfaz de diagnóstico a bordo que se halla en los automóviles modernos.
- Humane Reader: dispositivo electrónico de bajo costo con salida de señal de TV que pueden manejar una biblioteca de 5000 títulos en una tarjeta microSD.
- The Humane PC: equipo que usa un módulo Arduino para emular un computador personal, con un monitor de televisión y un teclado para computadora.
- Ardupilot: software y hardware de aviones no tripulados.
- ArduinoPhone: un teléfono móvil celular construido sobre un módulo Arduino.

Lenguaje de programación Arduino

La plataforma Arduino se programa mediante el uso de un lenguaje propio basado en el lenguaje de programación de alto nivel Processing. Sin embargo, es posible utilizar otros lenguajes de programación y aplicaciones populares en Arduino, debido a que Arduino usa la transmisión serial de datos soportada por la mayoría de los lenguajes mencionados. Para los que no soportan el formato serie de forma nativa, es posible utilizar software intermediario que traduzca los mensajes enviados por ambas partes para permitir una comunicación fluida. Algunos ejemplos son:

- 3DVIA Virtools: aplicaciones interactivas y de tiempo real.
- Adobe Director
- BlitzMax (con acceso restringido)
- C
- C++ (mediante libSerial o en Windows)
- C#
- Cocoa/Objective-C (para Mac OS X)
- Flash (mediante ActionScript)

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

- Gambas
- Isadora (Interactividad audiovisual en tiempo real)
- Instant Reality (X3D)
- Java
- Liberlab (software de medición y experimentación)
- Mathematica
- Matlab
- MaxMSP: Entorno gráfico de programación para aplicaciones musicales, de audio y multimedia
- Minibloq: Entorno gráfico de programación, corre también en las computadoras OLPC
- Perl
- Php
- Physical Etoys: Entorno gráfico de programación usado para proyectos de robótica educativa
- Processing
- Pure Data
- Python
- Ruby
- Scratch for Arduino (S4A): Entorno gráfico de programación, modificación del entorno para niños Scratch, del MIT)
- Squeak: Implementación libre de Smalltalk
- SuperCollider: Síntesis de audio en tiempo real
- VBScript
- Visual Basic .NET
- VVVV: Síntesis de vídeo en tiempo real

Estructuras de control

Condicionales: if, if...else, switch case

Bucles: for, while, do... while

Bifurcaciones y saltos: break, continue, return, goto

Variables

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

En cuanto al tratamiento de las variables también comparte un gran parecido con el lenguaje C

Constantes

HIGH/LOW: representan los niveles alto y bajo de las señales de entrada y salida. Los niveles altos son aquellos de 3 voltios o más.

INPUT/OUTPUT: entrada o salida.

false (falso): Señal que representa al cero lógico. A diferencia de las señales HIGH/LOW, su nombre se escribe en letra minúscula.

true (verdadero): Señal cuya definición es más amplia que la de *false*. Cualquier número entero diferente de cero es "verdadero", según el álgebra de Boole, como en el caso de -200, -1 o 1. Si es cero, es "falso".

Tipos de datos

void, boolean, char, unsigned char, byte, int, unsigned int, word, long, unsigned long, float, double, string, array.

Conversión entre tipos**.**

Estas funciones reciben como argumento una variable de cualquier tipo y devuelven una variable convertida en el tipo deseado.

char(), byte(), int(), word(), long(), float()

Calificadores y ámbito de las variables

static, volatile, const

Utilidades

sizeof()

Funciones Básicas

E/S Digital

pinMode(pin, modo)

digitalWrite(pin, valor)

int digitalRead(pin)

E/S Analógica

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

analogReference(tipo)

int analogRead(pin)

analogWrite(pin, valor)

E/S Avanzada

shiftOut(dataPin, clockPin, bitOrder, valor)

unsigned long pulseIn(pin, valor)

Tiempo

unsigned long millis()

unsigned long micros()

delay(ms)

delayMicroseconds(microsegundos)

Números aleatorios

randomSeed(semilla), long random(máx), long random(mín, máx)

Las funciones de manejo del puerto serie deben ir precedidas de la palabra "Serial" aunque no necesitan ninguna declaración en la cabecera del programa. Por esto se consideran funciones base del lenguaje. Estas son las funciones para transmisión serial: begin(), available(), read(), flush(), print(), println(), write()

Interrupciones

Las señales de interrupción son las siguientes:

cli(): desactiva las interrupciones globales

sei(): activa las interrupciones

Esto afectará al temporizador y a la comunicación serial. La función delay Microseconds () desactiva las interrupciones cuando se ejecuta.

Temporizadores

La función delayMicroseconds () crea el menor retardo posible del lenguaje Arduino que ronda los 2µs. Para retardos más pequeños se debe utilizar la llamada de ensamblador 'nop' (no

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

operación). Cada sentencia 'nop' se ejecutará en un ciclo de máquina (16 MHz) de aproximadamente 62.5ns.

Manipulación de puertos.

La manipulación de puertos con código AVR es más rápida que utilizar la función digitalWrite () de Arduino.

Establecer Bits en variables.

Cbi y sbi son mecanismos estándar (AVR) para establecer o limpiar bits en PORT y otras variables.

Diferencias con Processing.

La sintaxis del lenguaje de programación Arduino es una versión simplificada de C/C++ y tiene algunas diferencias respecto de Processing. Debido a que Arduino está basado en C/C++ mientras que Processing se basa en Java, existen varias diferencias en cuanto a la sintaxis de ambos lenguajes y el modo en que se programa:

Ejemplo sencillo de programación en Arduino. Con el dispositivo, se recomienda abrir el ejemplo “led_blink” el cual crea una intermitencia por segundo en un led conectado en el pin 13. El código necesario es el siguiente:

```
# define LED_PIN 13
void setup () {
 // Activado del contacto 13 para salida digital
 pinMode (LED_PIN, OUTPUT);
}
// Bucle infinito
void loop () {
 // Encendido del diodo LED enviando una señal alta
 digitalWrite (LED_PIN, HIGH);
 // Tiempo de espera de 1 segundo (1000 ms)
```


DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

```
 delay (1000);
 // Apagado del diodo LED enviando una señal baja.
 digitalWrite (LED_PIN, LOW);
 // Tiempo de espera de 1 segundo
 delay (1000);
}
```

Bibliotecas en Arduino

Las bibliotecas estándar que ofrece Arduino son las siguientes:

Serial

Lectura y escritura por el puerto serie.

EEPROM

Lectura y escritura en el almacenamiento permanente.

read(), write()

Ethernet

Conexión a Internet mediante “Arduino Ethernet Shield“. Puede funcionar como servidor que acepta peticiones remotas o como cliente. Se permiten hasta cuatro conexiones simultáneas. Los comandos usados son los siguientes:

Servidor: Server(), begin(), available(), write(), print(), println()

Cliente: Client(), connected(), connect(), write(), print(), println(), available(), read(), flush(), stop()

Firmata

Es una biblioteca de comunicación con aplicaciones informáticas utilizando el protocolo estándar del puerto serie.

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

LiquidCrystal

Control de LCDs con chipset Hitachi HD44780 o compatibles. a biblioteca soporta los modos de 4 y 8 bits.

Servo

Biblioteca para el control de servomotores A partir de la versión 0017 de Arduino la biblioteca soporta hasta 12 motores en la mayoría de las placas Arduino y 48 en la Arduino Mega. Estos son los comandos usados:

attach(), write(), writeMicroseconds(), read(), attached(), detach()

Software Serial

Comunicación serie en contactos digitales. Por defecto Arduino incluye comunicación sólo en los contactos 0 y 1 pero gracias a esta biblioteca puede realizarse esta comunicación con los restantes.

Creación de bibliotecas

Los usuarios de Arduino tienen la posibilidad de escribir sus propias bibliotecas; ello permite disponer de código que puede reutilizarse en otros proyectos, mantener el código fuente principal separado de las bibliotecas y la organización de los programas construidos es más clara. Mecanismo de conexión de dispositivo electrónico de forma inalámbrica.

5.6 Mecanismo de conexión de dispositivos electrónicos de forma inalámbrica.

Fig. 4. Logotipo del wifi

En algunos países hispanohablantes /' wifi/) es un mecanismo de conexión de dispositivos electrónicos de forma inalámbrica. Los dispositivos habilitados con Wi-Fi, tales como: una

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

computadora personal, una consola de videojuegos, un smartphone o un reproductor de audio digital, pueden conectarse a Internet a través de un punto de acceso de red inalámbrica. Dicho punto de acceso (o hotspot) tiene un alcance de unos 20 metros en interiores y al aire libre una distancia mayor. Pueden cubrir grandes áreas la superposición de múltiples puntos de acceso.

Wi-Fi es una marca de la Wi-Fi Alliance (anteriormente la *WECA: Wireless Ethernet Compatibility Alliance*), la organización comercial que adopta, prueba y certifica que los equipos cumplen los estándares 802.11 relacionados a redes inalámbricas de área local.

Estándares que certifica Wi-Fi

Los estándares IEEE 802.11b, IEEE 802.11g e IEEE 802.11n disfrutan de una aceptación internacional debido a que la banda de 2.4 GHz está disponible casi universalmente, con una velocidad de hasta 11 Mbit/s, 54 Mbit/s y 300 Mbit/s, respectivamente.

En la actualidad ya se maneja también el estándar IEEE 802.11a, conocido como WIFI 5, que opera en la banda de 5 GHz y que disfruta de una operatividad con canales relativamente limpios. La banda de 5 GHz ha sido recientemente habilitada y, además, no existen otras tecnologías (Bluetooth, microondas, ZigBee, WUSB) que la estén utilizando, por lo tanto existen muy pocas interferencias. Su alcance es algo menor que el de los estándares que trabajan a 2.4 GHz (aproximadamente un 10%), debido a que la frecuencia es mayor (a mayor frecuencia, menor alcance).

Existe un primer borrador del estándar IEEE 802.11n que trabaja a 2.4 GHz y a una velocidad de 108 Mbit/s. Sin embargo, el estándar 802.11g es capaz de alcanzar ya transferencias a 108 Mbit/s, gracias a diversas técnicas de aceleramiento. Actualmente existen ciertos dispositivos que permiten utilizar esta tecnología, denominados *Pre-N.*

Existen otras tecnologías inalámbricas como Bluetooth que también funcionan a una frecuencia de 2.4 GHz, por lo que puede presentar interferencias con la tecnología Wi-Fi. Debido a esto, en la versión 1.2 del estándar Bluetooth por ejemplo se actualizó su especificación para que no existieran interferencias con la utilización simultánea de ambas tecnologías, además se necesita tener 40 000 k de velocidad.

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

Seguridad y fiabilidad

Uno de los problemas a los cuales se enfrenta actualmente la tecnología Wi-Fi es la progresiva saturación del espectro radioeléctrico, debido a la masificación de usuarios, esto afecta especialmente en las conexiones de larga distancia (mayor de 100 metros). En realidad Wi-Fi está diseñado para conectar ordenadores a la red a distancias reducidas, cualquier uso de mayor alcance está expuesto a un excesivo riesgo de interferencias.

Un muy elevado porcentaje de redes son instalados sin tener en consideración la seguridad convirtiendo así sus redes en redes abiertas (o completamente vulnerables ante el intento de acceder a ellas por terceras personas), sin proteger la información que por ellas circulan. De hecho, la configuración por defecto de muchos dispositivos Wi-Fi es muy insegura (Router, por ejemplo) dado que a partir del identificador del dispositivo se puede conocer la clave de éste; y por tanto acceder y controlar el dispositivo se puede conseguir en sólo unos segundos.

El acceso no autorizado a un dispositivo Wi-Fi es muy peligroso para el propietario por varios motivos. El más obvio es que pueden utilizar la conexión. Pero además, accediendo al Wi-Fi se puede monitorizar y registrar toda la información que se transmite a través de él (incluyendo información personal, contraseñas).

Dispositivos

Existen varios dispositivos Wi-Fi, los cuales se pueden dividir en dos grupos: Dispositivos de Distribución o Red, entre los que destacan los Router, puntos de acceso y Repetidores; y Dispositivos Terminales que en general son las tarjetas receptoras para conectar a la computadora personal, ya sean internas (tarjetas PCI) o bien USB.

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

Fig. 5. Router WiFi.

Dispositivos de Distribución o Red.

Los puntos de acceso son dispositivos que generan un "set de servicio", que podría definirse como una "Red Wi-Fi" a la que se pueden conectar otros dispositivos. Los puntos de acceso permiten, en resumen, conectar dispositivos en forma inalámbrica a una red existente. Pueden agregarse más puntos de acceso a una red para generar redes de cobertura más amplia, o conectar antenas más grandes que amplifiquen la señal.

Los repetidores inalámbricos son equipos que se utilizan para extender la cobertura de una red inalámbrica, éstos se conectan a una red existente que tiene señal más débil y crean una señal limpia a la que se pueden conectar los equipos dentro de su alcance. Algunos de ellos funcionan también como punto de acceso.

Los Router inalámbricos son dispositivos compuestos, especialmente diseñados para redes pequeñas (hogar o pequeña oficina). Estos dispositivos incluyen, un Router (encargado de interconectar redes, por ejemplo, nuestra red del hogar con internet), un punto de acceso (explicado más arriba) y generalmente un switch que permite conectar algunos equipos vía cable (Ethernet y USB). Su tarea es tomar la conexión a internet, y brindar a través de ella acceso a todos los equipos que conectemos, sea por cable o en forma inalámbrica.

El wifi puede ser desactivado por un terminal del dispositivo.

Las tarjetas PCI para Wi-Fi se agregan (o vienen de fábrica) a los ordenadores de sobremesa. Hoy en día están perdiendo terreno debido a las tarjetas USB. Dentro de este grupo también pueden agregarse las tarjetas MiniPCI que vienen integradas en casi cualquier computador portátil disponible hoy en el mercado.

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

Las tarjetas PCMCIA son un modelo que se utilizó mucho en los primeros ordenadores portátiles, aunque están cayendo en desuso, debido a la integración de tarjeta inalámbricas internas en estos ordenadores. La mayor parte de estas tarjetas solo son capaces de llegar hasta la tecnología B de Wi-Fi, no permitiendo por tanto disfrutar de una velocidad de transmisión demasiado elevada

Las tarjetas USB para Wi-Fi son el tipo de tarjeta más común que existe en las tiendas y más sencillo de conectar a un pc, ya sea de sobremesa o portátil, haciendo uso de todas las ventajas que tiene la tecnología USB. Hoy en día puede encontrarse incluso tarjetas USB con el estándar 802.11N (Wireless-N) que es el último estándar liberado para redes inalámbricas.

También existen impresoras, cámaras Web y otros periféricos que funcionan con la tecnología Wi-Fi, permitiendo un ahorro de mucho cableado en las instalaciones de redes y especialmente, gran movilidad.

Ventajas y desventajas

Las redes Wi-Fi poseen una serie de ventajas, entre las cuales podemos destacar:

Al ser redes inalámbricas, la comodidad que ofrecen es muy superior a las redes cableadas porque cualquiera que tenga acceso a la red puede conectarse desde distintos puntos dentro de un rango suficientemente amplio de espacio.

Una vez configuradas, las redes Wi-Fi permiten el acceso de múltiples ordenadores sin ningún problema ni gasto en infraestructura, ni gran cantidad de cables.

La Wi-Fi Alliance asegura que la compatibilidad entre dispositivos con la marca *Wi-Fi* es total, con lo que en cualquier parte del mundo podremos utilizar la tecnología Wi-Fi con una compatibilidad total.

Pero como red inalámbrica, la tecnología Wi-Fi presenta los problemas intrínsecos de cualquier tecnología inalámbrica. Algunos de ellos son:

La desventaja fundamental de estas redes existe en el campo de la seguridad. Existen algunos programas capaces de capturar paquetes, trabajando con su tarjeta Wi-Fi en modo promiscuo, de forma que puedan calcular la contraseña de la red y de esta forma acceder a ella. Las claves de tipo WEP son relativamente *fáciles de conseguir* con este sistema.

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

La potencia de la conexión del Wi-Fi se verá afectada por los agente físicos que se encuentran a nuestro alrededor, tales como: arboles, paredes, arroyos, una montaña, etc. Dichos factores afectan la potencia de compartimiento de la conexión Wi-Fi con otros dispositivos.

Xbee Shield

Fig. 6. Forma física del Xbee shield

Descripción: La Xbee shield permite a una placa Arduino comunicarse de forma inalámbrica usando Zigbee. El módulo puede comunicarse hasta 100ft (30 metros) en interior o 300ft (90 metros) al aire libre (en visión directa). Puede ser usado como reemplazo del puerto serie/usb o puedes ponerlo en modo de comandos y configurarlo para una variedad de opciones de redes broadcast o malladas. La shield tiene pistas desde cada pin del Xbee hasta un orificio de soldar. También provee conectores hembra para usar los pines digitales desde 2 hasta 7 y las entradas analógicas, las cuales están cubiertas por la shield (los pines digitales de 8 a 13 no están cubiertos por la placa, así que puedes usar los conectores de la placa directamente).

De forma simplificada los módulos XBee son dispositivos que integran un transmisor -receptor de ZigBee y un procesador en un mismo módulo, lo que le permite a los usuarios desarrollar aplicaciones de manera rápida y sencilla. Zigbee es un protocolo de comunicaciones inalámbrico basado en el estandar de comunicaciones para redes inalámbricas IEEE_802.15.4. Creado por Zigbee Alliance, una organización, teóricamente sin ánimo de lucro, de más de 200 grandes empresas (destacan Mitsubishi, Honeywell, Philips, Motorola, Invensys).Muchas de ellas fabricantes de semiconductores. Zigbee permite que dispositivos electrónicos de bajo consumo puedan realizar sus comunicaciones inalámbricas. Es especialmente útil para redes de sensores en entornos industriales, médicos y, sobre todo, domóticas.

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

Componentes de la interfaz de control electrónica

Diodo

Fig. 7. Forma física de un diodo Rectificador

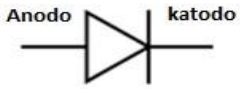


Fig. 8. Símbolo de electrónico

Descripción: Un **diodo** es un componente electrónico de dos terminales que permite la circulación de la corriente eléctrica a través de él en un solo sentido. Este término generalmente se usa para referirse al diodo semiconductor, el más común en la actualidad; consta de una pieza de cristal semiconductor conectada a dos terminales eléctricos. El diodo de vacío (que actualmente ya no se usa, excepto para tecnologías de alta potencia) es un tubo de vacío con dos electrodos: una lámina como ánodo, y un cátodo.

De forma simplificada, la curva característica de un diodo (I-V) consta de dos regiones: por debajo de cierta diferencia de potencial, se comporta como un circuito abierto (no conduce), y por encima de ella como un circuito cerrado con una resistencia eléctrica muy pequeña. Debido a este comportamiento, se les suele denominar rectificadores, ya que son dispositivos capaces de suprimir la parte negativa de cualquier señal, como paso inicial para convertir una corriente alterna en corriente continua. Su principio de funcionamiento está basado en los experimentos de Lee De Forest.

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

Transistor

Fig. 9. Forma física de un Transistor BJT

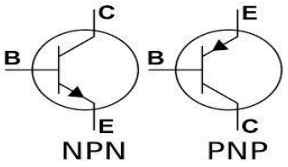


Fig. 10. Símbolo electrónico

Descripción: El transistor de unión bipolar (del inglés Bipolar Junction Transistor, o sus siglas BJT) es un dispositivo electrónico de estado sólido consistente en dos uniones PN muy cercanas entre sí, que permite controlar el paso de la corriente a través de sus terminales. La denominación de bipolar se debe a que la conducción tiene lugar gracias al desplazamiento de portadores de dos polaridades (huecos positivos y electrones negativos), y son de gran utilidad en gran número de aplicaciones; pero tienen ciertos inconvenientes, entre ellos su impedancia de entrada bastante baja.

Los transistores bipolares son los transistores más conocidos y se usan generalmente en electrónica analógica aunque también en algunas aplicaciones de electrónica digital, como la tecnología TTL o BICMOS.

Un transistor de unión bipolar está formado por dos Uniones PN en un solo cristal semiconductor, separados por una región muy estrecha. De esta manera quedan formadas tres regiones:

Emisor, que se diferencia de las otras dos por estar fuertemente dopada, comportándose como un metal. Su nombre se debe a que esta terminal funciona como emisor de portadores de carga.

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

Base, la intermedia, muy estrecha, que separa el emisor del colector.

Colector, de extensión mucho mayor.

Opto-acoplador

Fig. 11. Forma Física de un Opto-acoplador

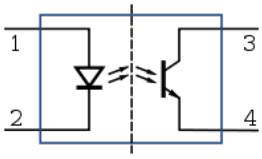


Fig. 12. Símbolo electrónico

Descripción

Un **opto-acoplador**, también llamado optoaislador o aislador acoplado ópticamente, es un dispositivo de emisión y recepción que funciona como un interruptor activado mediante la Luz emitida por un diodo LED que satura un componente opto-electrónico, normalmente en forma de fototransistor o fototriac. De este modo se combinan en un solo dispositivo semiconductor, un foto-emisor y un foto-receptor cuya conexión entre ambos es óptica. Estos elementos se encuentran dentro de un encapsulado que por lo general es del tipo DIP. Se suelen utilizar para aislar eléctricamente a dispositivos muy sensibles.

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

Led

Fig. 13. Led (diodo emisor de luz)

Fig. 14. Símbolo electrónico de un led

Descripción: Un led es un diodo emisor de luz, un componente opto-electrónico pasivo. Se usan como indicadores en muchos dispositivos y en **iluminación**. Los primeros led emitían luz roja de baja intensidad, pero los dispositivos actuales emiten luz de alto brillo en el **espectro infrarrojo**, **visible** y **ultravioleta**.

Relé electrónico

Fig. 15. Forma física de un relé electrónico

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

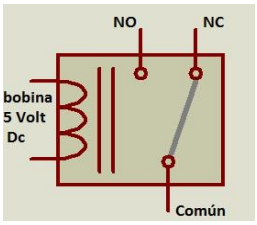


Fig. 16. Símbolo de relé

Descripción. El relé o relevador es un dispositivo electromecánico. Funciona como un interruptor controlado por un circuito electrónico en el que, por medio de una **bobina** y un **electroimán**, se acciona un juego de uno o varios contactos que permiten abrir o cerrar otros circuitos eléctricos independientes. Fue inventado por **Joseph Henry** en 1835. Dado que el relé es capaz de controlar un circuito de salida de mayor potencia que el de entrada, puede considerarse, en un amplio sentido, como un amplificador eléctrico. Como tal se emplearon en **telegrafía**, haciendo la función de **repetidores** que generaban una nueva señal con corriente procedente de pilas locales a partir de la señal débil recibida por la línea. Se les llamaba "relevadores

5.7 Electrónica de potencia

La expresión **electrónica de potencia** se utiliza para diferenciar el tipo de aplicación que se le da a dispositivos electrónicos, en este caso para transformar y controlar voltajes y corrientes de niveles significativos. Se diferencia así este tipo de aplicación de otras de la electrónica denominadas de baja potencia o también de corrientes débiles.

En este tipo de aplicación se reencuentran la electricidad y la electrónica, pues se utiliza el control que permiten los circuitos electrónicos para controlar la conducción (encendido y apagado) de semiconductores de potencia para el manejo de corrientes y voltajes en aplicaciones de potencia. Esto al conformar equipos denominados convertidores estáticos de potencia. De esta manera, la electrónica de potencia permite adaptar y transformar la energía eléctrica para distintos fines tales como alimentar controladamente otros equipos, transformar la energía eléctrica de continua a alterna o viceversa, y controlar la velocidad y el funcionamiento de máquinas eléctricas, etc. mediante el empleo de dispositivos electrónicos, principalmente semiconductores. Esto incluye tanto aplicaciones en sistemas de control, sistemas de compensación de factor de potencia y/o de armónicos como para suministro eléctrico a consumos industriales o incluso la interconexión de sistemas eléctricos de potencia de distinta

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

frecuencia. El principal objetivo de esta disciplina es el manejo y transformación de la energía de una forma eficiente, por lo que se evitan utilizar elementos resistivos, potenciales generadores de pérdidas por efecto Joule. Los principales dispositivos utilizados por tanto son bobinas y condensadores, así como semiconductores trabajando en modo corte/saturación (on/off, encendido y apagado).

Contactor

Fig. 17. Contactor eléctrico

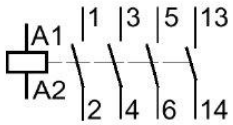


Fig. 18. Símbolo esquemático de un contactor eléctrico

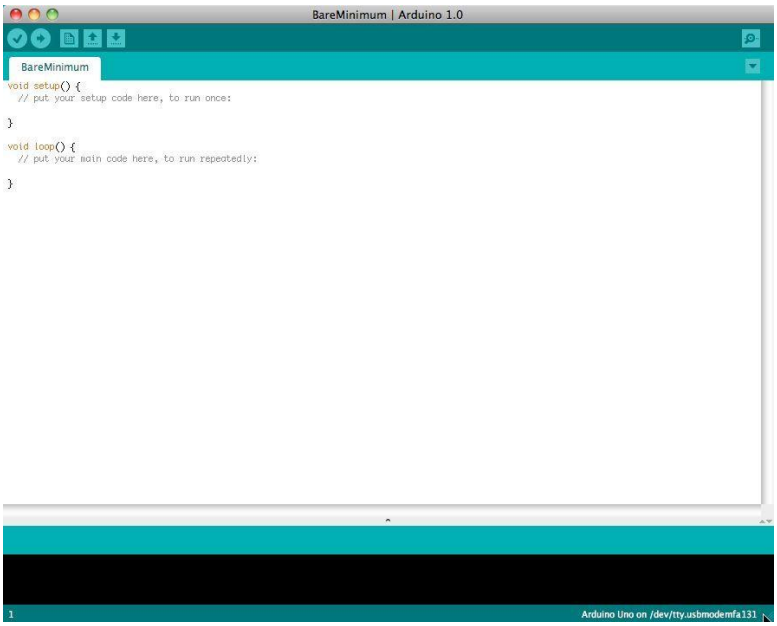
Descripción: Un contactor es un componente electromecánico que tiene por objetivo establecer o interrumpir el paso de corriente, ya sea en el circuito de potencia o en el circuito de mando, tan pronto se dé tensión a la **bobina** (en el caso de ser contactores instantáneos). Con capacidad de cortar la **corriente eléctrica** de un receptor o instalación, con la posibilidad de ser accionado a distancia, que tiene dos posiciones de funcionamiento: una estable o de reposo, cuando no recibe acción alguna por parte del circuito de mando, y otra inestable, cuando actúa dicha acción. Este tipo de funcionamiento se llama de "todo o nada". En los esquemas eléctricos, su simbología se establece con las letras KM seguidas de un número de orden.

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

6. METODOLOGIA DE LA INVESTIGACIÓN.

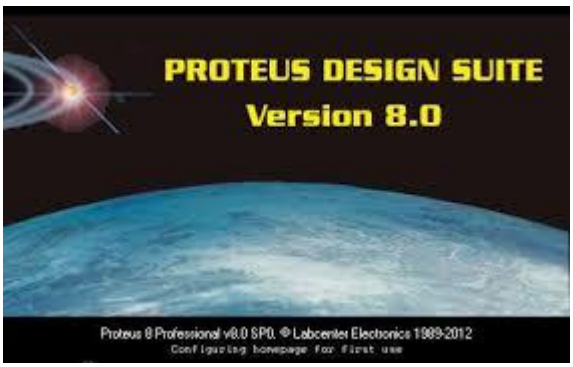
El sistema tecnológico, para la administración del recurso energético en un aula o laboratorio de clase, se desarrolló considerando las siguientes fases:

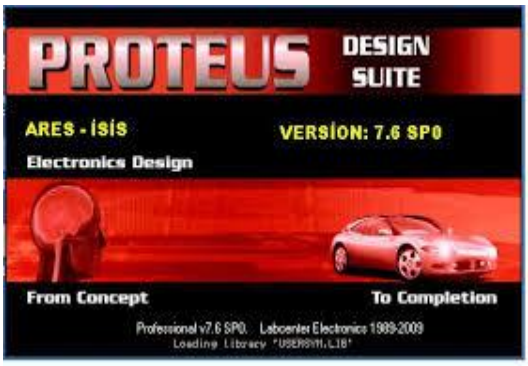
Creación del programa en arduino: En el proyecto, se desarrolló la tecnología de los microcontroladores, pero para poder llegar a la funcionabilidad del sistema diseñado, se dispuso del Software y Hardware de arduino, para dar los lineamientos a procesar dentro del microcontrolador.



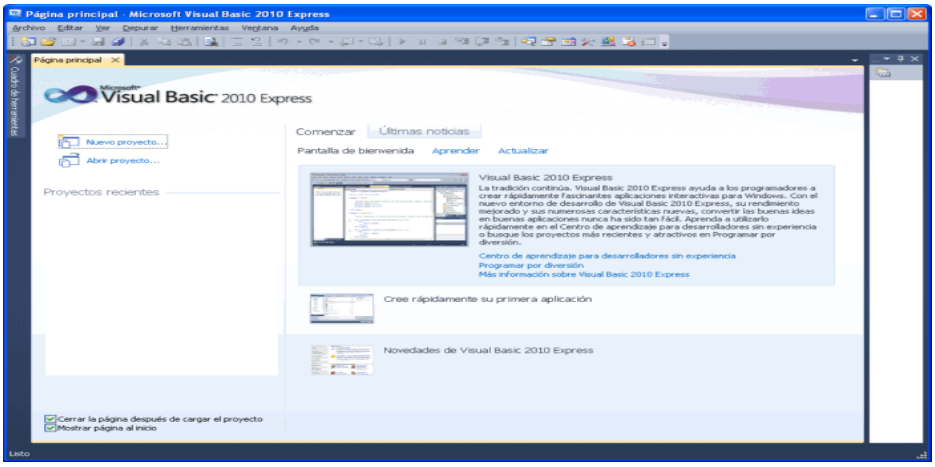
Simulación en Proteus: Para el ensayo de la función del micro controlador, se utilizó el Software de simulación de ISIS PROTEUS evaluando la conversión de datos que el sistema empezara a desarrollar, a partir de un programa hecho en arduino. De esta manera se puede evaluar las funciones del envió de datos desde las señales de control al µc.

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS



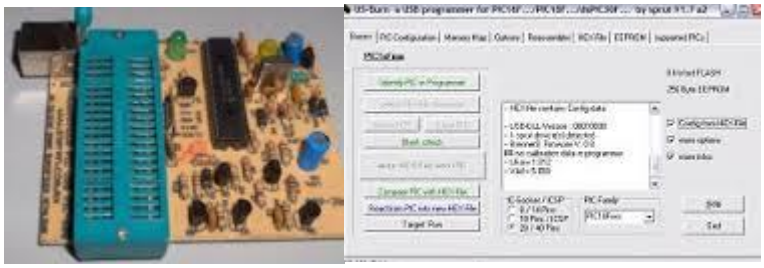


Construcción De La Interfaz Gráfica: Esta recibe los datos del circuito, utilizando el Software de Visual Basic, el cual tiene como función mostrar los códigos de tarjetas RFID y la vez registrar en la base de datos de mysql los registros de los docentes que hacen uso del aula o laboratorio de clase.

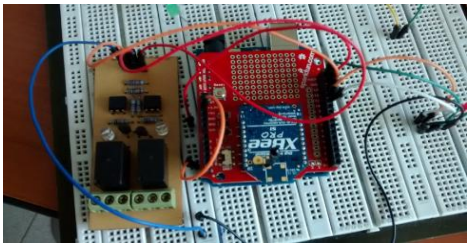


DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

Grabado Del Código: luego de verificar la simulación y definir la función a desarrollar por el micro controlador ATMEL, dentro del sistema, se procedió al grabado del código por medio de un Software llamado ARDUINO, que cargara el programa (código .HEX) previamente simulado en ISIS Proteus, a través de su programador de conector USB. Verificando la comunicación del mismo con la computadora.



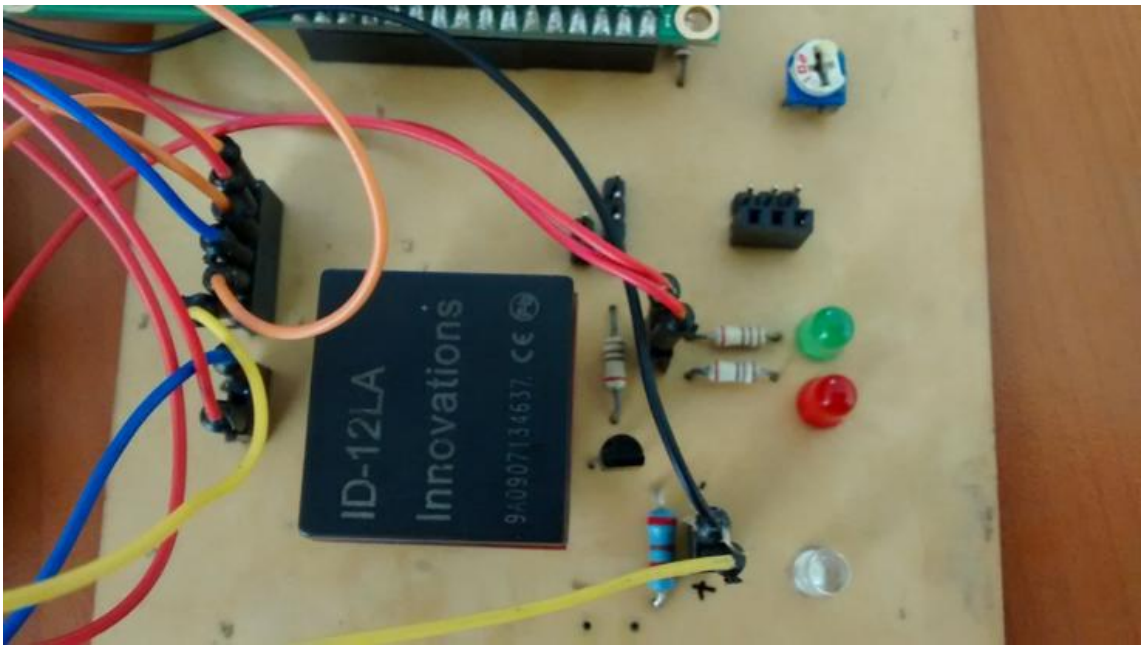
Armado del Circuito De Ensayo: Se utilizó una tabla Breadboard, para montar los componentes de la simulación del proyecto que fue hecho en el Software de ISIS PROTEUS, LIVEWIRE, PCB WIZARD, se conectan y se energizan para poder verificar el procesamiento de los datos, comunicación, comprobación, funcionalidad etc. de todo el sistema.



Circuito receptor inalámbrico **Circuito receptor de control de cargas**

Conexión De La RFID Reader ID-12LA al µc: luego de las pruebas efectuadas con el Pic se procede a la instalación del lector de tarjetas RFID para efectuar las pruebas de lectura del código de las tarjetas y la comunicación de los códigos con el microcontrolador ATMEL para su posterior enlace y recepción de datos en el ordenador.

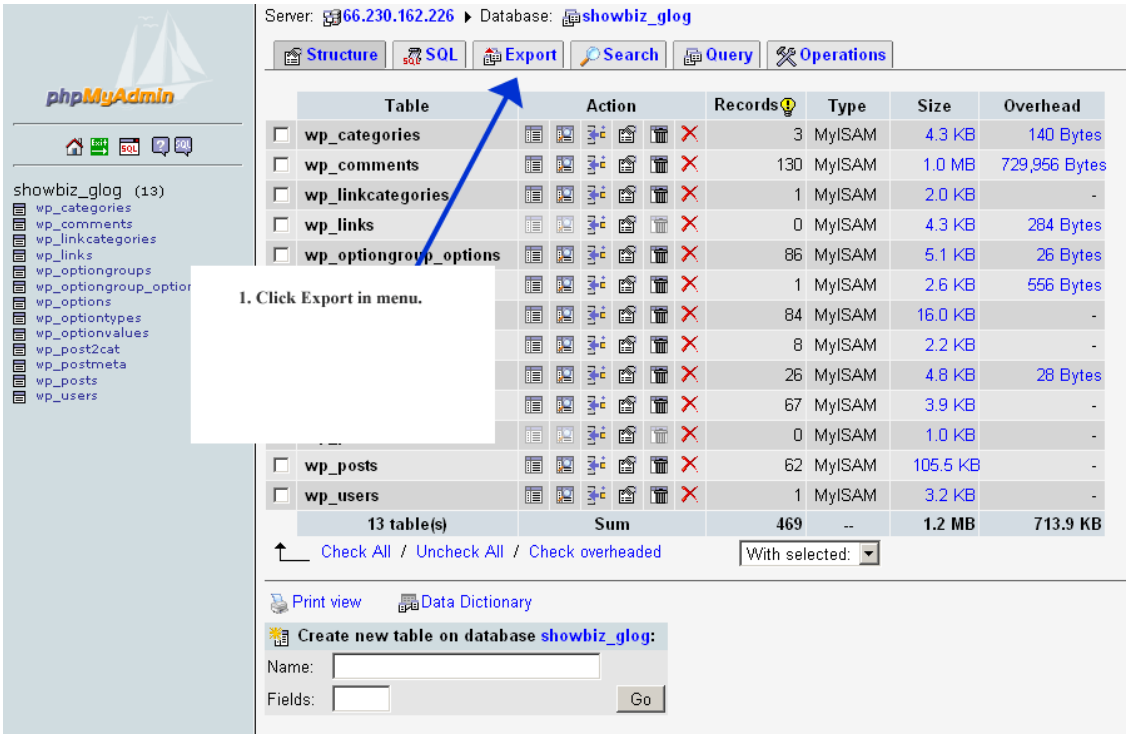
DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS



Circuito lector de tarjeta RFID

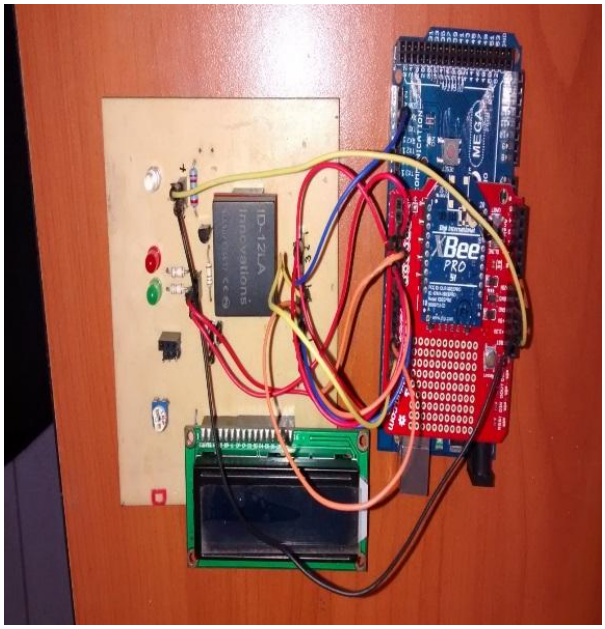
Creación De La Base De Datos: Se utiliza el programa Microsoft Access, en donde se usan aplicativos, para poder efectuar un enlace de los resultados que se muestran en V.B, directamente, para una base de datos. A la vez se genera un programa en Visual Studio, para que interactué tanto con Access como con Agilent Vee, de esta manera cuando el circuito electrónico envía los datos a la DAQ la variedad de software utilizado refleja los identificadores del terminal junto a los pedidos con sus respectivas fechas y horas. Se realizan varias pruebas para el logro de las expectativas en la interconexión Hardware-Software y se corrigen problemas imprevistos en esta etapa.

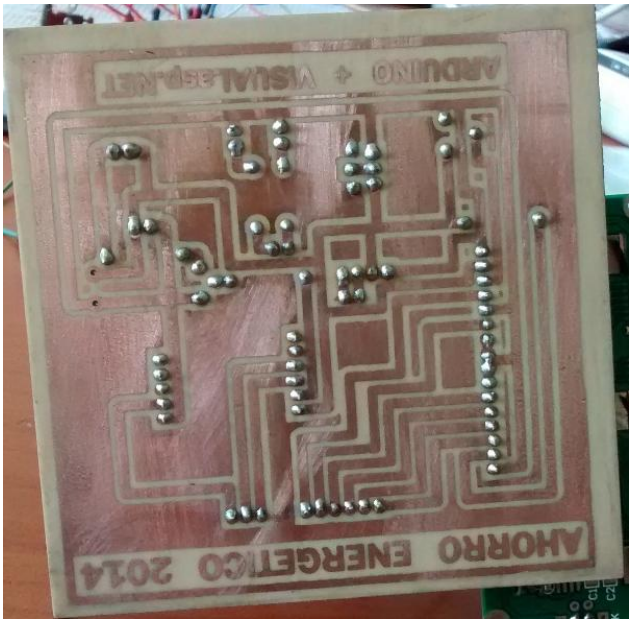
DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS



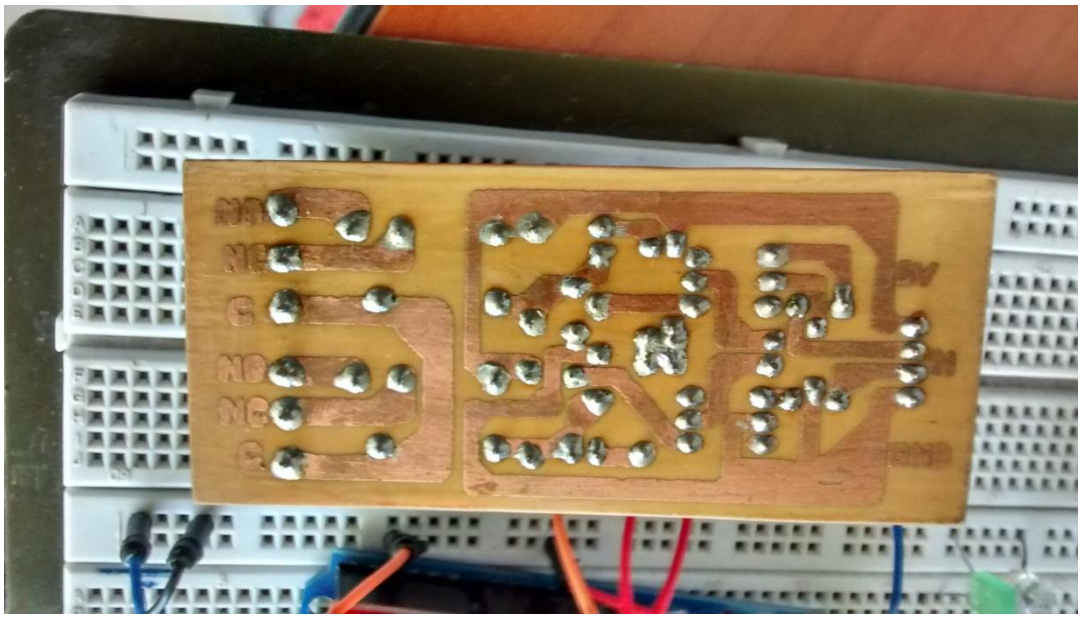
Diseño del prototipo. El proyecto consiste en implementar un sistema electrónico para el registro administrativo y optimización de los recursos energéticos en el MEGATEC ZACATECOLUCA.

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS





DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS



Componentes del sistema de control

El sistema de control acceso está compuesto de los siguientes componentes:

Una credencial de identificación (tarjeta inteligente)

Un lector de tarjeta inteligente

Panel de Control

Servidor de control de acceso

Software

Base de datos

La siguiente figura ilustra cómo estos componentes básicos están interconectados. Cada componente será descrito en las siguientes secciones.

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

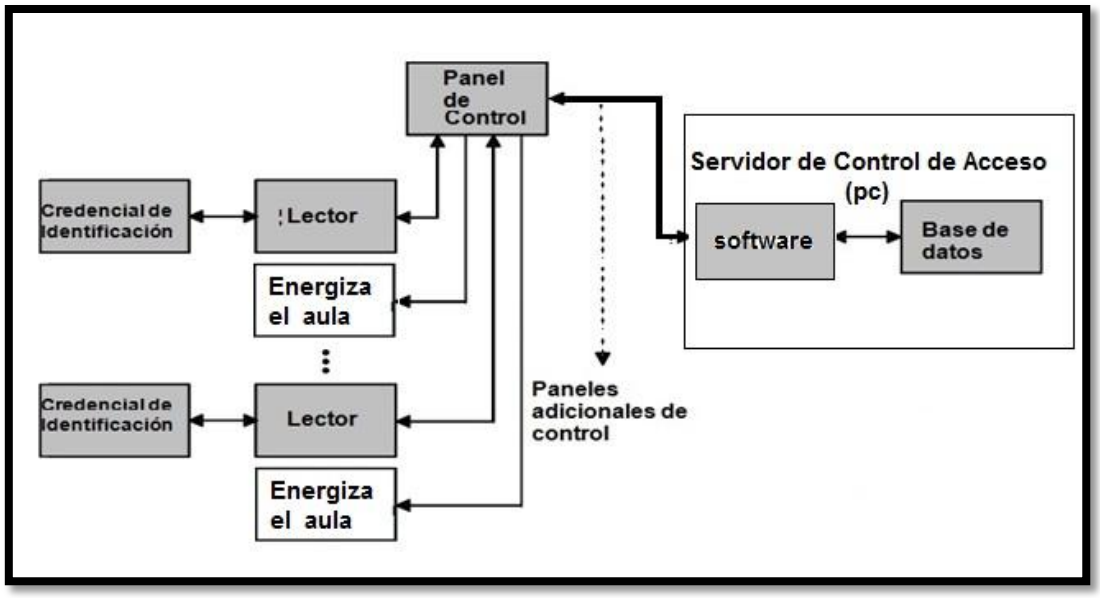


Fig. 19. Diagrama en bloque de sistema electrónico para el registro administrativo y optimización de los recursos energéticos.

Etapa 1: Credencial de Identificación

Una amplia gama de tecnología de identificación está actualmente siendo usado para control de acceso: cintas magnéticas, cintas Wiegang, Bariun Ferrite, tecnología de proximidad de 125KHz3, las tarjetas inteligentes de contacto y sin contacto. Esas tecnologías pueden ser empaquetadas en diferentes formatos, desde un llavero o una insignia del empleado hasta formas más exóticas, como un reloj de pulso o un anillo. Sin embargo, todas las credenciales operan básicamente de la misma forma: ellos almacenan datos que autentican la credencial y/o el usuario. La tecnología de tarjeta inteligente de contacto definido, por ISO/IEC 7816 y la tecnología de tarjeta inteligente sin contacto definido, por ISO/IEC14443eISO/IEC15693, tienen capacidad tanto para leer como escribir y almacenar datos. Las credenciales que usan estas tecnologías son dispositivos inteligentes. Ellos pueden almacenar privilegios, autorizaciones y registros de asistencia. Ellos pueden almacenar los PINs y los patrones biométricos, ofreciendo una capacidad de autenticación de dos o tres factores simultáneamente. La credencial ya no es solo un portador de un número único; pero pasa a ser también, un cargador seguro y portátil de datos.

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

Etapa 2: Panel de Control

El panel de control (frecuentemente conocido como el controlador o simplemente el panel) es el punto central de comunicaciones para el sistema de control de acceso. El panel de control típicamente suple energía y establece interfaces con múltiples lectores en diferentes puntos de acceso. El panel puede estar conectado a diferentes alarmas (por ejemplo, sirenas, digitalizadores automáticos, luces). Y finalmente, el panel de control generalmente está conectado a un servidor de control de acceso.

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

Dependiendo del diseño del sistema, el panel de control puede procesar datos del lector de tarjetas y del servidor de control de acceso y tomar la decisión última sobre autorización, o él puede pasar los datos al servidor de control de acceso para que él tome esa decisión. Típicamente, el panel de control toma la decisión de energizar toma corrientes, permitir el encendido de luminarias y aire acondicionado. Pasa los datos de ésa transacción a la computadora base y envía una señal de desbloquear hacia el lector. Es importante que sea el panel de control (y no el lector) el que genere la señal de activar, ya que el panel de control está localizado dentro del establecimiento en un cuarto seguro.

Finalmente, el panel de control realiza almacenamiento de información sobre los formatos de datos. Esa información identifica que porción del flujo de datos recibidos de una tarjeta es usada para tomar decisiones de control de acceso. Tarjetas y lectores con diferentes tecnologías pueden intercambiar datos en diferentes formatos. Sin embargo, el panel de control necesita saber cómo interpretar y procesar estos datos. Por ejemplo, si un lector envía 35 bits de data y el panel de control está diseñado para leer solamente 26 bits, el panel debe rechazar los datos o truncar 9 bits. El formato de los datos controla como el panel interpreta los datos recibidos

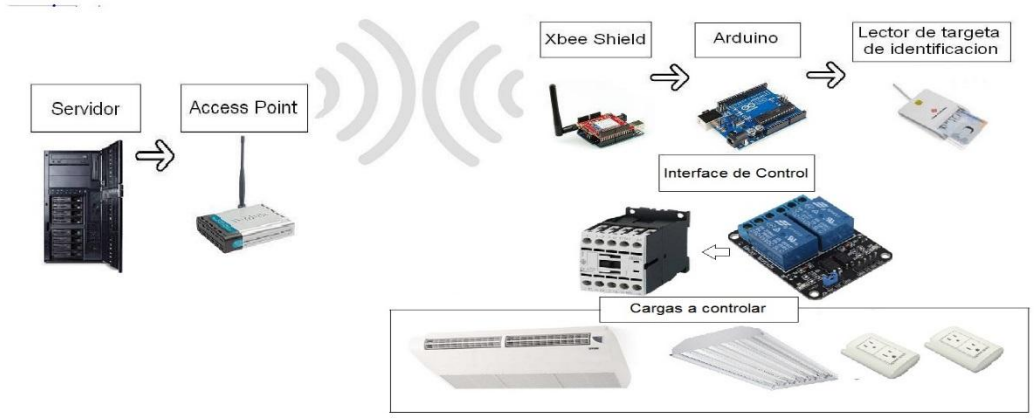


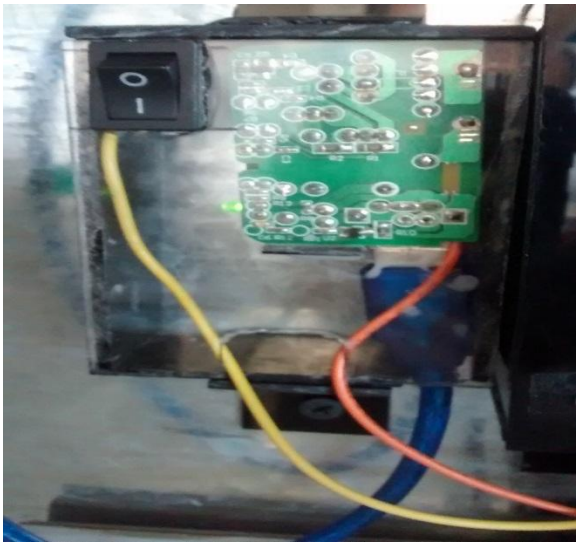
Fig. 20. Esquema que representa el diseño de toda la comunicación del Sistema.

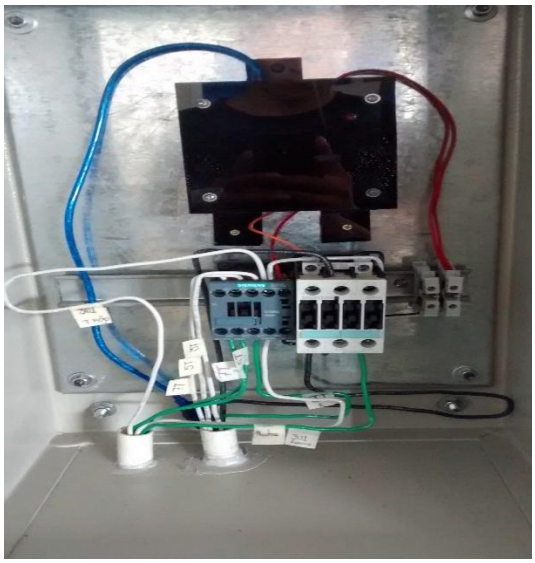
DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

El sistema de control de carga eléctrica, utiliza el lector de tarjetas inteligente en conjunto con una placa con un microcontrolador llamada Arduino y una interface de control (relé) para determinar si se habilita o deshabilita el suministro de energía a las aulas en donde se instalará el sistema. Para ello se determinó utilizar, como actuadores del sistema, contactores encargados de interrumpir el suministro de energía eléctrica.

Dentro de la etapa eléctrica se tuvo que considerar la distancia y el medio de comunicación entre la central de control (plataforma Arduino y lector de tarjeta) y los actuadores (contactores). Se plantearon dos propuestas:

Interrumpir con los contactores las líneas de alimentación en las propias aulas a partir de las cajas de registros que se encuentran en el cielo falso (luminarias y aire acondicionado) y en el piso (toma corrientes).





Interrumpir con los contactares las líneas de alimentación a partir del tablero eléctrico central desde donde parten los circuitos derivados de todas las aulas aledañas (dentro de las que están incluidas las aulas a trabajar dentro del proyecto).

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

Fig. 21. Fotografía del tablero central que controla las luminarias, tomacorrientes y aires acondicionados.

Las aulas que se consideraron en el proyecto son:

Aulas D-201 y D-301; dentro de éstas aulas se encuentran las cargas a ser controladas.

Laboratorios D-202 y D-302; dentro de éstos laboratorios se encuentran los paneles eléctricos desde donde se tiene acceso a las protecciones termo-magnéticas de los circuitos derivados.

Se realizó un levantamiento de la instalación eléctrica de las aulas y de los tableros de control para poder determinar las canalizaciones que habría que intervenir para instalar el sistema de control del aula. Se identificaron los interruptores termo-magnéticos de los circuitos de toma corrientes, luminarias y aire acondicionado. Los interruptores termo-magnéticos que controlan las cargas eléctricas a ser interrumpidas o intervenidas se detallan a continuación:

Laboratorio D-302:

Espacios 7, 9 y 11 en tablero central, para toma corrientes y luminarias.

Espacio 2 en tablero de tomas UPS.

Caja de registro en cielo falso para aire acondicionado.

Laboratorio D-202:

Espacios 7, 8 y 9 en tablero central, para toma corrientes y luminarias.

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

Espacio 2 en tablero de tomas UPS.

Caja de registro en cielo falso para aire acondicionado.

Después de los resultados obtenidos del levantamiento de la instalación eléctrica del segundo y tercer nivel del edificio “D”, se concluyó que la mejor opción para intervenir las cargas eléctricas es la número 2 (interrumpir desde el tablero eléctrico). Las razones se listan a continuación:

Ubicación más centralizada del control eléctrico: se facilita la revisión de los actuadores en caso de fallas o averías, al tener el control eléctrico en una ubicación accesible para el personal de mantenimiento.

Fig. 22. Fotografía donde está ubicada la protección del aire acondicionado

Fácil instalación: El control eléctrico se instala de forma más fácil desde una sola ubicación en contraparte a instalarlo desde cada caja de registro de cada carga eléctrica a ser controlada disminuyendo el trabajo significativamente.

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

Fig. 23 Fotografía real de donde están ubicados los tableros de las protecciones.

Fácil Comunicación: El cableado de control encargado de comunicar los actuadores con la plataforma Arduino y el número de contactores a utilizar, se reduce también de forma significativa y se aprovecha la canalización para el cableado de control para distribuir la alimentación eléctrica directa para la plataforma Arduino y el lector de tarjetas inteligentes.

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

Fig. 24. Fotografía donde están ubicado el tablero que alimenta los tomas del uso de UPS

Del anterior se parte, para para diseño del diagrama eléctrico; que se muestra en la figura 25

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

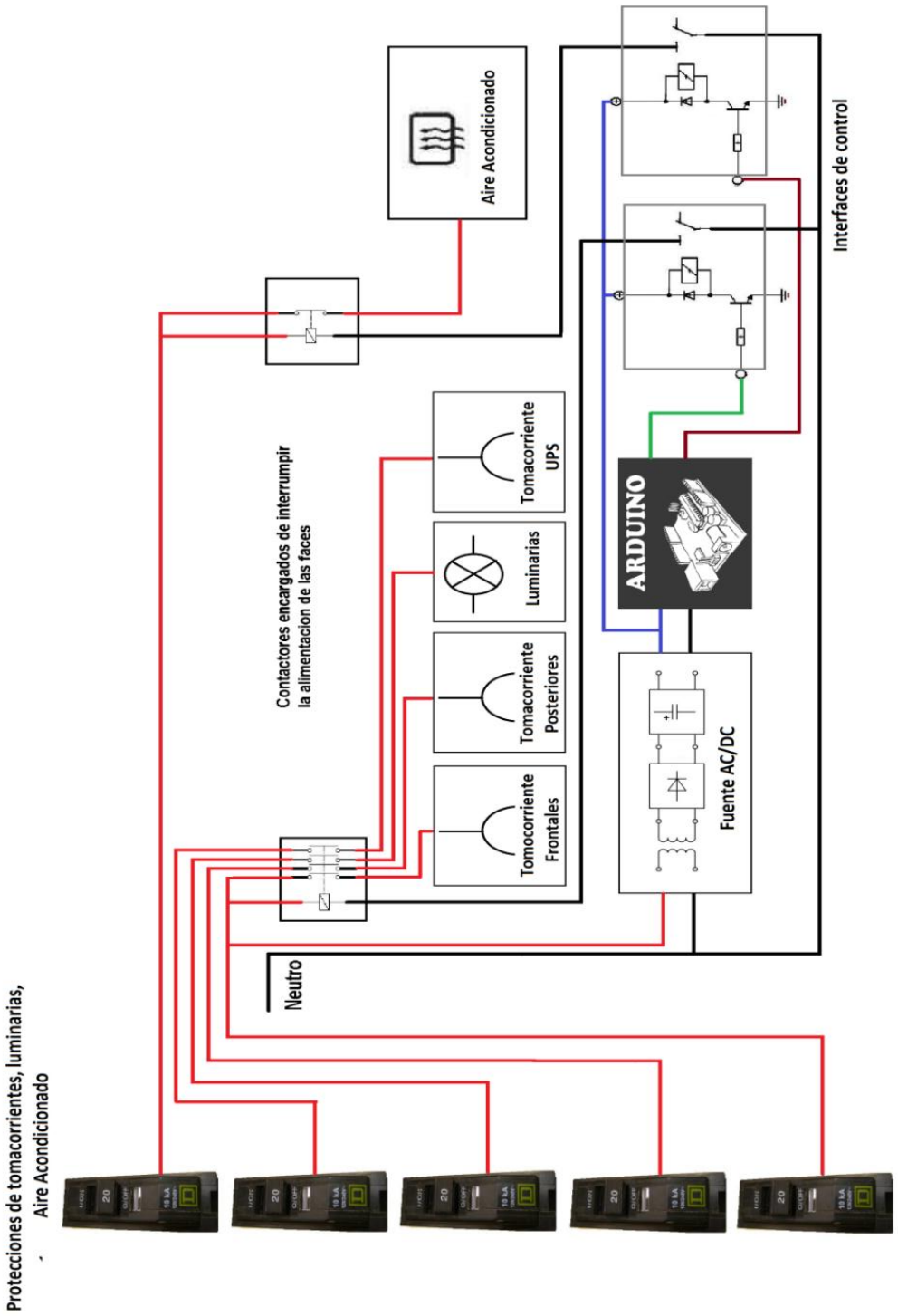


Fig. 25. Diseño de la conexión eléctrica del proyecto.

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

Etapa 3: Servidor de Control de Acceso.

En términos informáticos se conoce como sistema de cabeza de red (también conocido como sistema de “backend”, o sistema huésped “Hostsystem”) incluye el servidor de control de acceso, el software y una base de datos. La base de datos contiene información actualizada sobre los derechos de acceso de los usuarios.

En un sistema centralizado, el servidor de control de acceso recibe los datos de la tarjeta del panel de control. El software correlaciona los datos de la tarjeta con los datos en la base de datos, determina los privilegios de acceso de la persona, e indica si la persona puede o no ser admitida. Por ejemplo, si una persona está autorizada a ingresar a un edificio solamente entre las 8:00 a.m. y 5:00 p.m. y son las 7:45 a.m., está persona no puede ser admitida. Sin embargo, si son las 8:01a.m., entonces la computadora debe responder al panel de control, indicando la decisión de energizar toma corrientes, permitir el encendido de luminarias y el del aire acondicionado.

La mayoría de los sistemas son descentralizados. En un sistema descentralizado, el servidor de control de acceso periódicamente envía información de control de acceso actualizada a los paneles de control y les permite operar independientemente, tomando la decisión de autorización para las credenciales presentadas, basadas en los datos almacenados en el panel.

Las características operacionales en sistemas centralizados o descentralizados, son determinadas por los requerimientos específicos de implementación de control de acceso de la institución. Existen dos tipos de sistemas con los que el panel de Control valida y luego acepta los datos transmitidos por el lector.

Sistema centralizado. En un sistema centralizado el panel de control transmite los datos al servidor de control de acceso. El servidor de control de acceso compara los datos recibidos de la tarjeta con la información sobre él.

Este informe utiliza el término “credencial” para referirse a la identificación general del dispositivo (tanto el dispositivo físico como los datos que él porta). Este es comúnmente referido como “la ficha de identificación” en el sistema de control de acceso físico.

El usuario que está almacenado en la base de datos. El programa de control de acceso determina los privilegios de acceso del usuario y su autorización, la hora, la fecha y la determinación de a que laboratorio o aula se está ingresando y cualquier otra información que

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

la institución pueda requerir para asegurar su seguridad. Cuando se autoriza el acceso, el servidor de control de acceso envía una señal al panel de control para: Energizar Toma corrientes, permitir el encendido de luminarias y aire acondicionado y emite un sonido audible u otro tipo de señal que indica al usuario que puede entrar.

Sistema distribuido**.** En un sistema distribuido, el panel de control permite o niega la entrada. El servidor de control de acceso periódicamente provee datos al panel de control, que habilita al software del panel de control a determinar si el usuario está autorizado o no para tener acceso. El panel de control, entonces, realiza las funciones del servidor de control de acceso descrito arriba y toma la decisión de permitir o negar la entrada. El habilitar el panel de control para realizar la función de decisión, tiene la ventaja de requerir menor comunicación entre los paneles de control y el servidor de control de acceso central, mejorando el desempeño y la confiabilidad del sistema como un todo.

Si una función biométrica o un PIN se incorpora al sistema, el lector típicamente auténtica estos datos. La validez puede ser determinada por el lector o desde dentro de la misma tarjeta inteligente al comparar el dato con un patrón biométrico o un PIN almacenado en la tarjeta. (En algunos casos los datos biométricos pueden ser enviados al panel de control para su procesamiento). Si la información adicional es válida, el lector envía el número de identificación de la credencial al panel de control. Si la información no es válida, entonces el lector de la tarjeta indica que la entrada es negada.

La respuesta a una tarjeta inválida es definida por la política y procedimiento de seguridad de la institución. El servidor de control de acceso o panel de control pueden ignorar el dato y no enviar un código para energizar toma corrientes ni permitir el encendido de luminarias y aire acondicionado. Él puede enviar una señal para que el lector emita un sonido diferente, para indicar que el acceso fue negado. Él podría notificar y activar otro sistema de seguridad (por ejemplo circuito cerrado de alarmas), indicando que una tarjeta no autorizada está siendo presentada al sistema.

Características Importantes De La Operación Del Sistema

Radio de Acción Operacional. Una característica importante de la operación del sistema del control de acceso es la distancia del lector en la cual la credencial es efectiva (llamado radio de acción operacional). Está característica puede afectar la percepción final del usuario sobre la

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

conveniencia de utilizar el sistema. Para los sistemas que utilizan las tarjetas inteligentes de contacto, el radio de acción operacional no es un problema; ya que el contacto entre la tarjeta y el lector es físico (la tarjeta se debe de insertar dentro del lector). El radio de acción operacional es determinado por múltiples factores, incluyendo, tanto las especificaciones del diseño del sistema como el ambiente en el cual el lector es colocado. Entre los factores que afectan el radio de acción operacional se incluyen la forma de la antena, número de vueltas de la antena, el material de la antena, los materiales que se encuentran a su alrededor, la orientación de la credencial en relación con el lector, los parámetros eléctricos del chip, características anti-colisión y la fuerza de campo del lector. El campo de acción operacional puede ser incrementado reforzando la antena (por ejemplo, aumentando el número de espirales de la antena, el tamaño de la antena, o la energía transmitida por la antena). La localización del lector puede afectar el campo de acción operacional de un lector sin contacto. Por ejemplo, la proximidad del lector al metal puede distorsionar el campo de recepción e inclusive bloquearlo de la tarjeta. Si el lector es montado sobre una sólida placa de metal, próximo a una puerta hecha totalmente de metal o puesto dentro de una cajilla de metal (para protegerlo de actos vandálicos), puede que tenga un campo de acción operacional muy corto. El campo de acción operacional de la credencial de identidad, para muchas tecnologías sin contacto es una decisión crítica de diseño para un sistema de control de acceso físico. El campo de acción operacional adecuado será determinado como parte de la política de seguridad general de la organización de la arquitectura de seguridad y de sus requerimientos.

Consideraciones de Seguridad. Para mitigar los riesgos contra accesos no autorizados o ataques deliberados, la seguridad de todo el sistema de control de acceso debe ser tomada en cuenta. Eso comienza con el proceso inicial de emisión de las tarjetas, incluye los componentes del sistema (tal como la red, la base de datos, software, cámaras, lectores, tarjetas) los procesos del sistema (por ejemplo los procedimientos para los guardias) y la protección de los datos dentro de los componentes del sistema y durante la transmisión. El diseño del sistema debe considerar qué características de seguridad son necesarias para ser implementadas, dado el ambiente del sistema y de la probabilidad real de un ataque.

Seguridad de la Tarjeta. Las tarjetas inteligentes pueden ayudar a detener la falsificación o impedir la manipulación, con una tarjeta de identificación y prevenir el uso de una tarjeta no

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

autorizada. Las tarjetas inteligentes incluyen una variedad de capacidades de hardware y software que detectan y reaccionan ante intentos de manipulación y pueden contrarrestar posibles ataques, incluyendo: sensores de voltaje, frecuencia; luz y temperatura; filtros de reloj, memoria barajada (scrambled); fuentes constantes de energía, diseños del chip para resistir análisis por inspección visual, micro- sondeos o manipulación del chip. Donde las tarjetas inteligentes se han de utilizar para verificación de identidad manual, hay que adicionar al cuerpo de la tarjeta inteligente características de seguridad tales como, fuentes únicas, color de tinta y arreglos multicolores, microimpresiones, tinta ultravioleta de alta calidad en la frente o en la parte de atrás de la tarjeta, imágenes fantasmas, (una fotografía secundaria del portador en una localización alternativa de la tarjeta) y hologramas de múltiples planos, incluyendo imágenes tridimensionales. Cuando son adecuadamente diseñadas e implementadas, las tarjetas inteligentes son casi imposibles de falsificar o duplicar, y los datos en el chip no pueden ser modificados sin una autorización adecuada (por ejemplo, con palabras claves, con autenticación biométrica o con llaves de acceso criptográfico). En la medida que los sistemas de implementación tengan una política de seguridad efectiva e incorporen los servicios de seguridad necesarios, ofrecidos por las tarjetas inteligentes organizaciones y portadores de identidad pueden tener un alto grado de confianza en la integridad de la información de identidad y de su uso autorizado seguro.

Protección de Datos. Uno de los argumentos más fuertes para el uso de sistemas basados en tarjeta inteligentes para control de acceso físico, es su capacidad de usar mecanismos para mezclar datos (data Scrambling) o la criptografía para proteger la información, tanto en el chip como durante la transmisión. La seguridad y confiabilidad de la información requerida para la identificación de una persona y sus derechos y privilegios es clave para el éxito del sistema de control de acceso físico. Las tarjetas inteligentes pueden respaldar algoritmos criptográficos simétricos, que aseguran una protección sustancial y tiempos de procesamiento excelentes. La criptografía de llave simétrica es ampliamente usada para control de acceso físico y utiliza la misma llave para la encriptación y la decrepitación, haciendo quesea extremadamente rápido y confiable. Cuando un sistema de control de acceso incluye acceso lógico y privilegios PKI y cuando el tiempo de procesamiento no es problema, los algoritmos criptográficos asimétricos pueden ser usados. Múltiples llaves pueden ser almacenadas en un chip único para atender las necesidades de seguridad para uso en múltiples aplicaciones, brindándole esta forma mayor seguridad para la creciente complejidad de los sistemas de hoy.

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

Autentificación de Tarjeta de datos: Un sistema de acceso físico seguro debe asegurarse de forma imparcial que tanto la tarjeta de identificación presentada al lector como los datos que el contiene son auténticos. En algunos casos es importante verificar que él es un auténtico también (como es determinado por la tarjeta) para prevenir terminales falsificadas que puedan extraer los datos. Aparte del uso de un PIN y/o sistema biométrico para activar la tarjeta o autenticar la persona, las tarjetas inteligentes tienen la capacidad única de ofrecer una autenticación interna, basada en el chip que usa mecanismos criptográficos simétricos o asimétricos, para ofrecer soluciones altamente confiables para demostrar que la tarjeta y los datos son genuinos. Para una autenticación segura de la tarjeta, las tarjetas inteligentes tienen la capacidad única de usar técnicas criptográficas activas para responder a una señal del lector probando que la tarjeta posee una contraseña secreta que puede autenticar la validez de la tarjeta.

Comunicación entre Tarjetas y Lectores de Tarjetas. Como sucede con cualquier proceso que envuelve señales electrónicas, los datos transmitidos entre componentes también pueden ser monitoreados. Esta posibilidad debe ser considerada en el diseño de seguridad del sistema en términos del ambiente (por ejemplo, esta área está bajo observación o podría alguien físicamente insertar otro dispositivo o colocar un dispositivo de monitoreo dentro del radio de acción de la señal) y la probabilidad real de que tal ataque o esfuerzo se realice. Dependiendo del ambiente y del perfil de riesgos, una organización puede estar preocupada de que la información enviada por una tarjeta de identificación de contacto o sin contacto hacia un lector de tarjeta pueda ser monitoreada, permitiendo que se efectúe una entrada ilegal, si una tarjeta o un dispositivo furtivo pudiese duplicar los datos. Las tarjetas inteligentes respaldan técnicas de encriptación y seguridad estandarizados establecidos al nivel de la industria; que aseguran tantas comunicaciones entre la tarjeta y el lector así como permiten métodos de autenticación entre la tarjeta y el lector.

Las claves de seguridad usadas tanto para encriptar como autenticar son guardadas en fichas seguras (módulos de tarjetas inteligentes) tanto en la tarjeta como en el lector y son altamente resistentes a los ataques.

Comunicación entre el Lector de Tarjeta y el Panel de Control. Cuando un lector de tarjetas está localizado en un punto de acceso que no tiene un sistema de cableado físicamente seguro, la institución puede estar preocupada de que un invasor pueda remover el lector de tarjeta de su montura y leer el flujo de datos que este envía al panel de control o colocar una

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

computadora personal u otro dispositivo; en estos alambres y mimetizar la inserción de una tarjeta válida para ganar autorización de acceso. La mayoría de las tarjetas de los lectores de tarjetas actualmente transmiten datos al panel de control usando uno de dos formatos: Wiegand o cinta magnética. El formato Wiegand utiliza dos líneas de señales: D0, para transmitir “cero” pulso de datos; D1, para transmitir pulsos de un dato. El formato de cintas magnéticas utiliza dos líneas de señales – una para datos y otra para el reloj. Estas cintas de datos no son consideradas seguras.

El proveer un canal seguro desde la tarjeta hacia el lector y del lector hacia el panel de control, sobrelleva está amenaza potencial a la seguridad. El proveer canales seguros se neutraliza la mayoría de las amenazas serias porque el lector y la tarjeta son los dos elementos que están expuestos y disponibles físicamente a alguien que desea atacar el sistema. El canal de comunicación del lector hacia el panel de control puede ser asegurado de una forma similar a la que se usa para un canal seguro entre la tarjeta y el lector. Los datos intercambiados entre los dos dispositivos pueden ser encriptados para mayor seguridad. El lector y el panel pueden ser autenticados durante la transacción.

Debido a que la conexión entre el panel de control y el sistema de control de acceso es interna en un edificio o localizada en un cuarto seguro, normalmente no es tan susceptible a ser atacado. Sin embargo, si así se desea, esta conexión también puede ser asegurada usando las técnicas descritas en esta sección, de forma que todo el sistema tiene un canal de datos seguros de punta a punta. La siguiente figura se ilustra como el sistema de control de acceso físico basado en tarjetas inteligentes puede brindar una seguridad de punta a punta.

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

Lector RFID Instalado Dentro del aula **Tablero principal de Recepción y control**

7. RESULTADOS

El proceso de investigación para la elaboración de un prototipo basado en tarjetas inteligentes, tecnología wifi - Xbee, Arduino, escudos para Arduino, red cableada, Router entre otros y que permitirá un control seguro (privilegios de acceso) a los recursos físicos y lógicos, será de gran utilidad para la institución debido a que se contara con tecnología de punta que permitirá llevar un control detallado de la administración y uso de los recursos físicos (aire acondicionado, luminarias, toma corrientes entre otros que se desee incorporar posteriormente) en áreas que el sistema basado en tarjetas inteligentes controle (esto de acuerdo a políticas, normativas o simplemente prioridad de seguridad en un área determinada de la institución).

En base a la investigación realizada se descubrió que los Gobiernos, las corporaciones y las universidades están implementando el uso de las tarjetas de identificación inteligente y se ha llegado a concluir que pueden satisfacer sus necesidades para aplicaciones como un sistema electrónico para el registro administrativo y optimización de los recursos energéticos. Un

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

sistema a base de tarjetas inteligentes brinda beneficios a través de una organización, mejorando la seguridad, la conveniencia del usuario, a la vez que reduce los costos generales de gestión y administración. La tecnología de tarjetas inteligentes brinda una plataforma flexible y costo-efectiva no solo para control de acceso físico sino también para nuevas aplicaciones y procesos que pueden beneficiar a la organización como un todo.

El sistema cuenta con un dispositivo lector de la tarjeta RFID-Reader donde el usuario (personal que labora en la institución) deslizara una tarjeta la cual previamente fue programada con un ID único para un determinado usuario, una vez el lector identifica el código toma su decisión en base a lo programado y entre las posibilidades se tendrá: Por un lado y en el caso de ser una tarjeta inteligente con un ID valido el sistema le permitirá el acceso al aula y empezara a habilitar el aire acondicionado, los toma corrientes y luz, dentro de estos elementos pueden incluirse más pero que por motivos de prueba en este diseño (prototipo) se mencionan dos aulas que son las que el sistema controlara en un principio aunque no está demás aclarar que el sistema estará diseñado de una manera flexible a nuevas ideas o elementos que se deseen incorporar en este, además el sistema en tiempo real llevara un historial de uso de recursos físicos y del usuario que hizo uso de esos recursos, tiempo de uso entre otras, a través de una base de datos que incorporara el sistema en su diseño.

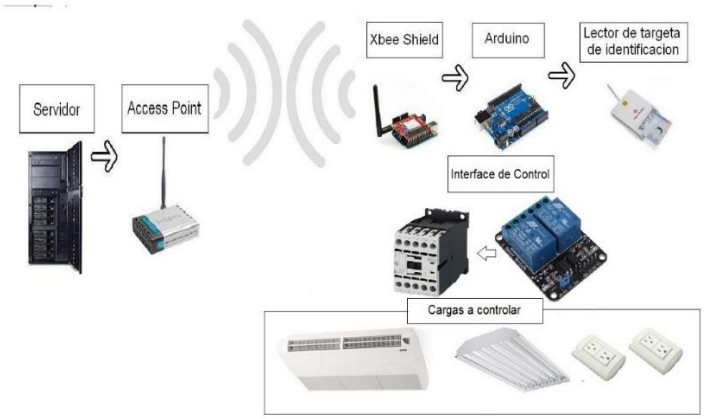
Por otra parte el sistema en el caso de detectar que la tarjeta inteligente deslizada en su lector no contiene un ID valido, el sistema mostrara o indicara de forma sonora audible y en pantalla LCD que es una ID invalido y por ende el sistema no habilitara el acceso y recursos físicos disponibles.

Por todo lo antes mencionado podemos decir y concluir que es un sistema el cual contribuirá a la institución en áreas donde se requiera de mayor seguridad de acceso y una administración más rigurosa de los recursos físicos y del personal o usuarios de dichas áreas.

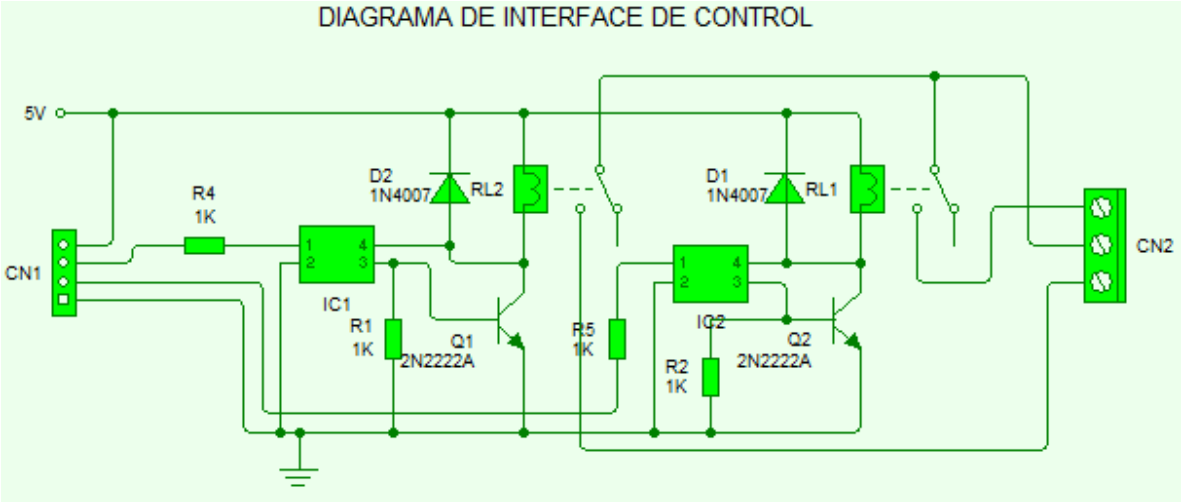
DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

ELEMENTOS DISEÑADOS EN EL PROYECTO:

1. **Diseño de la comunicación de todo el Sistema**



2. **Diagrama diseñado para la etapa de control.**



Para el diseño de la interface de control, se utiliza un transistor y un relé, debido a que los pines (en la mayoría de los casos) de salida del microcontrolador (Arduino), solo son capaz de entregar entre 10 y 30 mA, las exigencia de corrientes superiores pueden dañar el pin programado como salida, tomando en cuenta dicha situación, se utilizan transistores para manejar corrientes mayores, y se utiliza un relé para manejar corrientes mucho mayores a las que se puede manejar un transistor BJT, además de proveer de aislamiento para manejar corriente alterna. En el diagrama se muestra un opto-acoplador conectado a un transistor NPN

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

haciendo lo que se conoce como transistor darlington que permite que la bobina del relé se energice, se utiliza una optocupla para aislar las corrientes del transistor y de la salida del microcontrolador, para que este maneje un simple led que alimentara la base del transistor atreves de la optocupla.

De manera simplificada funciona como un interruptor controlado por un circuito electrónico. Y ese circuito electrónico está compuesto por resistencias limitadoras de corriente una optocupla, un transistor un diodo que protege al transistor. El transistor se utiliza como switch electrónico en el que controla la del relé y el electroimán interno se acciona, permitiendo abrir o cerrar los contactos siendo capaz de controlar un circuito de salida de mayor potencia que el de entrada, en un amplio sentido, como un amplificador eléctrico.

COMPONENTES DEL SISTEMA DE LA INTERFACE DE CONTROL DE ACCESO

- Una credencial de identificación (tarjeta RFID).
- Un lector de acceso (lector de tarjeta inteligente)
- Panel de Control.
- Servidor de control de acceso.
- Software (ARDUINO, V.B, V.B.NET ETC).
- Base de Datos (SGBD MYSQL).
- Circuito emisor y receptor
- Xbee pro S1.
- XBee Explorer USB.
- RFID Reader ID-12LA O RFID - RC522
- Xbee Shield.
- usb xbee regulated
- converter volt
- led
- diodo
- transisor
- rele
- contactor
- optoacoplador
- resistencia

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

- bornera
- header macho y hembra.
- jumper
- fuente

LISTA DE COMPONENTES DEL SISTEMA DE INTERFACE DE CONTROL.

MATERIALES	CANTIDAD	DESCRIPCION
Arduino uno R3	1	Microcontrolador y cerebro del sistema.
Arduino MEGA	1	Microcontrolador y cerebro del sistema.
Shield XBee	2	Plataforma que sirve de base para facilitar la conexión y comunicación entre el dispositivo XBee Pro y el uc.
XBee Pro S1	2	Dispositivo que hace posible la comunicación inalámbrica del sistema ahorro energético.
Pantalla LCD 16X2	1	Dispositivo de visualización de mensajes.
Potenciometro preset	1	Dispositivo electrónico que tiene como función el ajuste de tensiones variando su resistencia óhmica asc / desc.
Opto-aisladorores	4	Dispositivo electrónico que tiene como función aislar etapas de un circuito de potencia y otro TTL. Sirve para proteger el sistema electrónico de control.
Rele 5V	2	Dispositivo electrónico que tiene la función de conmutar (cambiar estado) abrir o cerrar un interruptor a través del campo magnético generado al momento de energizar convenientemente la bobina del mismo. Tiene la función de servir como actuador para cargas de potencia. Activa y desactiva un

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

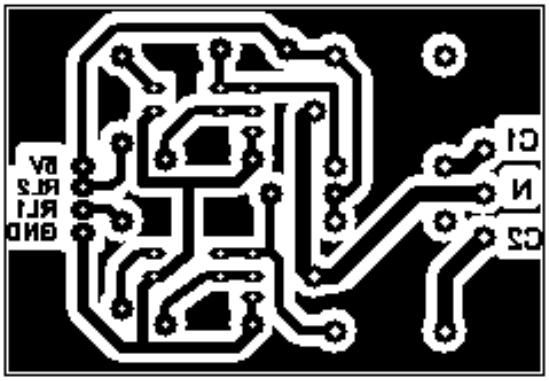
		actuador.
Contactores	2	Dispositivo eléctrico / electrónico que funciona de igual manera que un relé pero con la diferencia que viene preparado para soportar mayores voltajes y corrientes tanto en sus contactos como en su bobina.
RFID Reader ID-12LA Innovations O RFID - RC522	1	Dispositivo electrónico que sirve como lector de las tarjetas de identificación por radio frecuencia RFID.
Tag RFID.	10	Tarjeta que se utiliza como ID de usuarios (docentes) para hacer uso del sistema ahorro energético.
XBee Explorer USB o xBee Explorer Dongle USB	1	Dispositivo electrónico que se utiliza para programar / configurar los XBee Pro. Además a través de este dispositivo se puede cambiar el firmware de XBee Pro.
Breakout board for XBee Pro	1	Se utiliza esta placa para facilitar la conexión del dispositivo XBee Pro en una protoboard.
Breakout board for Reader ID-12LA Innovations	1	Se utiliza esta placa para facilitar la conexión del dispositivo ID-12LA en una protoboard.
Router	1	Deposito que tiene la función de generar un punto de acceso para hacer uso de servicios web a través de otros dispositivos que se enlazan a el de manera inalámbrica. Permite a los usuarios que cuentan con dispositivos con tecnología inalámbrica como laptop, Tablet, Teléfono, etc. Enlazarse al sistema a través de una página web para verificar la información procesada por el sistema en una

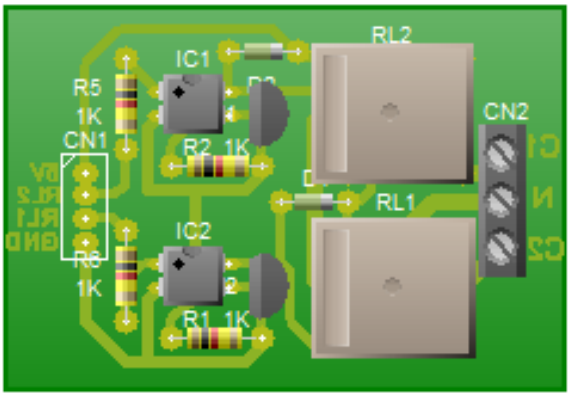
DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

		base de datos.
Cable UTP	2 mts	Cable que se utiliza para hacer de puente entre los componentes electrónicos del sistema.
Resistencia 220 – 330 ohm	5	Dispositivo electrónico que sirve de oposición al paso de la corriente.
Resistencia 1k ohm	6	Dispositivo electrónico que sirve de oposición al paso de la corriente.
Diodo 1n4007	2	Dispositivo electrónico semiconductor que sirve de protección del transistor ante corrientes de fuga.
LED	5	Dispositivo que sirve para indicar el estado de una salida especifica. Alto / Encendido o Bajo / Apagado.
Transistor 2N222 o 2N3904	3	Dispositivo electrónico semiconductor que sirve para conmutar y amplificar pequeñas corrientes en altas corrientes para control de otros dispositivos.
Header Hembra	xx	Terminales que se utilizan para facilitar la conexión entre dispositivos electrónicos.
Header Macho	xx	Terminales que se utilizan para facilitar la conexión entre dispositivos electrónicos.
Bornera.	xx	Terminales que se utilizan para facilitar la conexión entre dispositivos electrónicos.
Cable banana	xx	Terminales que se utilizan para facilitar la conexión entre dispositivos electrónicos.

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

3. Pista de la interface electrónica (modo espejo) Y Simulación de la vista real

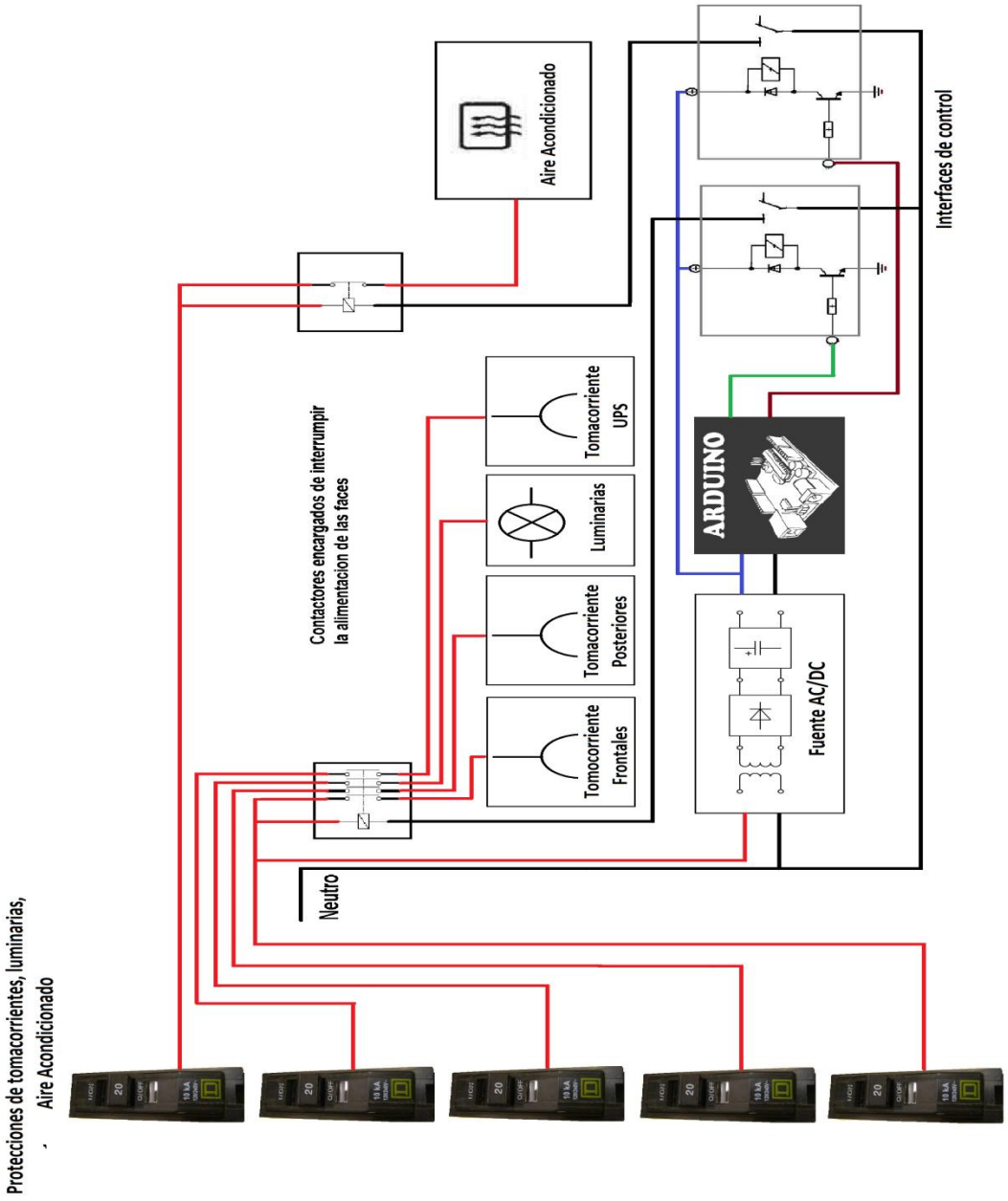




4. Pista del circuito lector de tarjetas RFID

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

5. Diseño de la conexión eléctrica del proyecto



DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

6. Software de Desarrollo

1- **Arduino IDE:** utilizado para programar los microcontroladores ATMEL.
2- **V.B.NET IDE:** Utilizado para desarrollar la aplicación web.
3- **WampServer IDE:** Aplicación utilizada para desarrollar la base de datos.
4- V.B FORMS IDE: Aplicación utilizada para desarrollar la aplicación que monitorea el ID RFID registrado al sistema.

Programación de dispositivos XBee Pro.

CTU-X software (XCTU)

Digi ha desarrollado X-CTU, que es un software utilizado para configurar y probar productos Digi RF módems.

Características:

- Soporte para todos los productos de Digi.
- Ventana de terminal integrado.
- Fácil de usar la prueba de rango de bucle invertido.
- Visualización de Recibir intensidad de la señal Indictator (RSSI).
- Actualiza módulo RF firmware en el campo en todos los productos de RF Digi.
- Mostrar ASCII y caracteres hexadecimales en la ventana de terminal.
- Componer paquetes de prueba en ASCII o hexadecimal para la transmisión en la interfaz de terminal.
- Guardar y recuperar configuraciones de módulos de uso común (perfiles).
- Detectar automáticamente el tipo de módulo.
- Restaurar parámetros por defecto de fábrica.

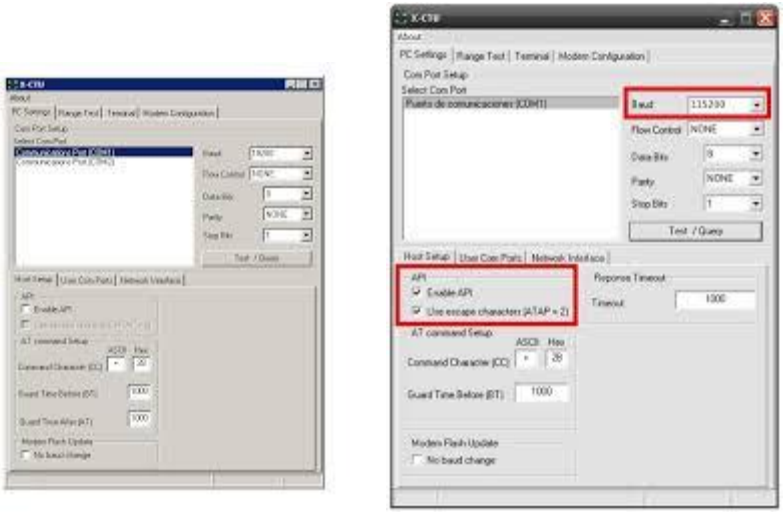
DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

- Muestra la ayuda de cada uno de los parámetros de radio.
- Perfiles de radio Programa en un entorno de producción mediante la interfaz de línea de comandos.
- Integrar con LabVIEW y otros software de prueba de producción a través de la interfaz de línea de comandos.

El software es fácil de usar y permite a los clientes de Digi para poner a prueba los módems de radio en el entorno real con sólo un ordenador y los usb reader xbee con los módems de radio.

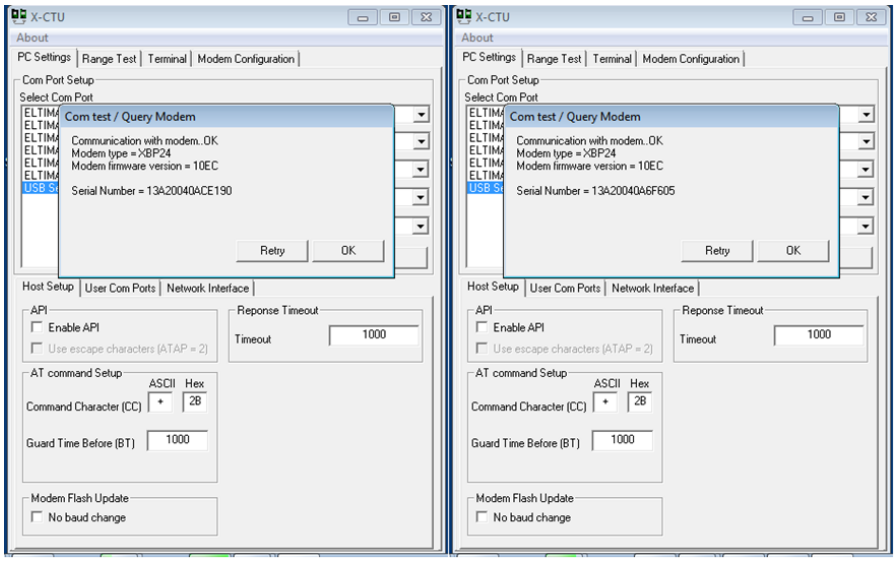
A continuación se muestra la interfaz del IDE del software x-ctu que se utilizó con la finalidad de configurar y programar los modulos xbee pro s1 para establecer la comunicación entre los dispositivos emisor y receptor xbee. Se configura la red.

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS



Interfaz gráfica del software de configuración X-CTU**.**

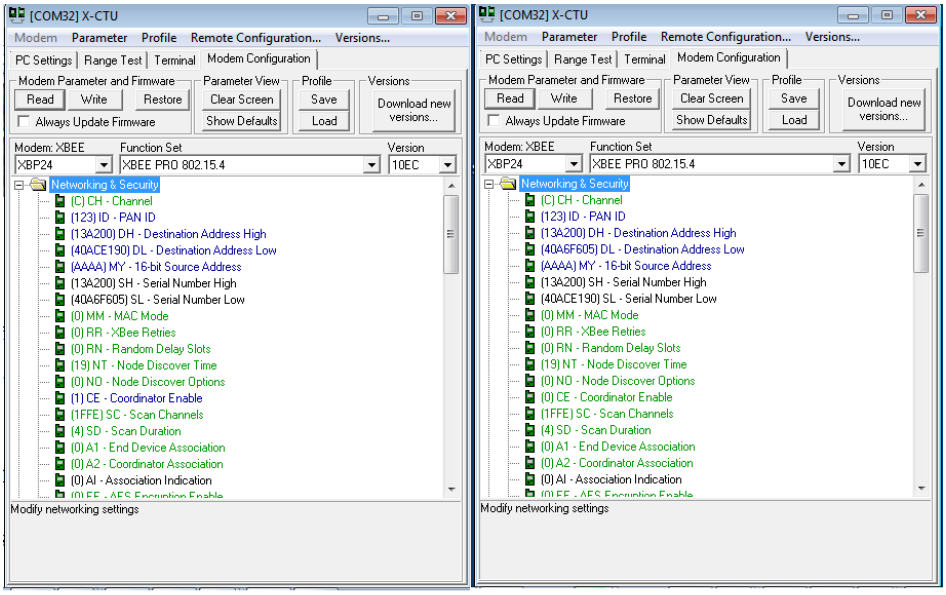
En la siguiente ilustración es donde se obtuvieron los ID o códigos de referencia de cado módulo xbee con la finalidad de utilizarlos en la configuración y programación de los parámetros para la implementación de la red entre ellos.



DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

Identificación de ID de módulos XBee pro

Una vez conocidos los ID de cada módulo XBee Pro Se procedió a configurar los parámetros de programación de cada uno de ellos para que se lograran comunicar entre sí. En la presente ilustración esta la configuración realizada a cada módulo.



MODULO COORDINADOR - RED ZIGBEE 2.4 G.

MODULO END DEVICE - RED ZIGBEE 2.4 G.

Programación / Configuración de los parámetros de los dispositivos XBee Pro.

Se puede visualizar la información obtenida con el Software X-CTU de manera física en cada módulo. La información viene impresa en una pegatina que viene de fábrica. A continuación la imagen de cada módulo donde se pueden visualizar los ID.

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

ID de los módulos XBee Pro. Parte trasera

De los parámetros más importantes a conocer de cada módulo XBee son los códigos SH y SL los cuales son las direcciones que se utilizan para realizar la correcta programación de cada uno de los módulos que requiera el sistema en sí. A continuación se puede visualizar de manera física de la siguiente manera.

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

8. CONCLUSIONES

Las tarjetas inteligentes están teniendo cada vez más aceptación como la credencial de preferencia para controlar el acceso físico con seguridad. Las tarjetas de identificación inteligentes basadas en estándares pueden ser usadas para fácilmente autenticar la identidad de una persona, determinar el nivel de acceso adecuado y admitir físicamente al portador de la tarjeta a un servicio, a un establecimiento y concebir que el lector de tarjeta que actué como un reloj que marca el tiempo de entrada y salida de los usuarios de la credencial (tarjeta inteligente). A través, del uso adecuado de tecnología de tarjetas inteligentes de contacto o sin contacto, en el diseño general de sistemas de acceso físico, los profesionales de seguridad pueden implementar las políticas de seguridad más altas posibles para cualquier situación. Y no solo en temas administrativos o de seguridad sino que también como un mecanismo que permita restringir adecuadamente el uso de recursos energéticos de la institución, optimizando el uso de aires acondicionados, equipos electrónicos e informáticos y luminarias en pasillos y aulas. De ésta manera se logra crear un sistema integral que contribuya al mejor manejo del recurso humano y a un ahorro energético significativo.

Más de una aplicación de acceso puede ser realizada en una tarjeta única de identificación inteligente, permitiendo a los usuarios tener acceso a recursos físicos y lógicos sin la necesidad de portar múltiples credenciales. La seguridad puede cambiar dinámicamente los derechos de acceso, dependiendo del nivel de amenaza percibido, la hora del día o cualquier otro parámetro que sea adecuado. La Tecnología de Informática. Puede registrar y actualizar privilegios desde una localización central. Recursos Humanos, puede procesar empleados que entran y que salen rápidamente, dando o retirando todos los derechos de acceso de una sola vez, en una sola transacción. Las tarjetas inteligentes no solo aseguran acceso a los recursos físicos o lógicos, como pueden almacenar datos sobre el portador de la tarjeta, pagar una cuota o tarifa, si fuese requerido, certificar transacciones y rastrear las actividades del portador de la identificación para propósitos de auditoria. Debido a que los componentes que respaldan el sistema pueden ser colocados en red, las bases de datos compartidas y la comunicación entre computadoras; permiten que áreas separadas funcionalmente dentro de una organización puedan intercambiar y coordinar información automáticamente e instantáneamente distribuir información veraz a través de una amplia área geográfica.

La tecnología de tarjetas inteligentes está basada en estándares maduros (de contacto y sin

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

contacto). Las Tarjetas que cumplen con estos estándares son desarrolladas comercialmente y tienen una presencia establecida en el mercado. Múltiples vendedores son capaces de suplir los componentes basados en estándares, necesarios para implementar sistemas de acceso físico sin contacto, brindando a los compradores equipo interactivo y tecnología a un costo competitivo.

La funcionalidad y el aprendizaje que deja dicho proyecto es el hecho de contar con nuevas tecnologías de ID en un sistema eléctrico / electrónico por medio de tarjetas magnéticas RFID con códigos de identificación pregrabados y con la posibilidad de reprogramar dicho código o identificador. Dicho sistema es una evolución o alternativa del famoso código de barras con que muchos sistemas de ID funcionan actualmente. Cabe destacar que cada sistema tiene sus propias ventajas y desventajas en entornos determinados de aplicación. Queda a criterio del lector hacer un estudio previo de dichas técnicas de identificación para el diseño de un sistema con funcionalidad semejante al presente proyecto. Además existen otros sistemas de identificación pero se seleccionó el medio de RFID por lo conveniente que resultaba para ejecutar este proyecto.

9. RECOMENDACIONES.

Áreas de conocimientos necesarias a considerar para el desarrollo o la expansión del presente proyecto:

- ✓ Electrónica, Base de Datos y programación (Microprogramacion)
- ✓ Microcontroladores de microchip o atmel
- ✓ Electrónica de potencia.
- ✓ Electrónica básica
- ✓ Prototipos
- ✓ Tecnología RFID
- ✓ Tecnología inalámbrica
- ✓ Instalaciones eléctricas
- ✓ Microsoft Access, Mysql, SQL Server u otros.
- ✓ Instrumentación electrónica.
- ✓ Manejo de aplicaciones para la comunicación serial

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

- ✓ Redes de computadoras
- ✓ Redes XBee**.**

10. REFERENCIAS BIBLIOGRAFICAS

Tarjeta inteligente RFID

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

Informe de la Smart Card Alliance Latin América (SCALA)

http://www.smartcardalliance.org/latinamerica/translations/Secure_Physical_Access_Spanish.pdf

Universidad Autónoma de Madrid

Proyecto: Elaboración de lector de tarjetas Smart Card (diagramas & códigos)

http://arantxa.ii.uam.es/~jms/pfcsteleco/lecturas/20130206JoseRubenIbanezSanchez.pdf

Información sobre Smart Card

http://es.wikipedia.org/wiki/Tarjeta_inteligente

Tarjetas inteligentes

http://www.monografias.com/trabajos10/tarin/tarin.shtml

Lector y grabador de tarjetas RFID EBay

http://www.ebay.com/itm/ACR122U-smart-card-reader-NFC-RFID-escritor-USB-5-Mifare-Contactless-FeliCa-SDK-/321210024351?pt=LH_DefaultDomain_186&hash=item4ac99c019f

Lector y grabador de Smart Card de contacto

Contact Smart IC Chip Reader Writer 1

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

http://www.ebay.com/itm/Contact-Smart-IC-Chip-Reader-Writer-1-/290589220301?pt=LH_DefaultDomain_0&hash=item43a8779dcd

Información sobre conexión inalámbrica

http://es.wikipedia.org/wiki/Wi-Fi

Iinformación de Arduino

http://es.wikipedia.org/wiki/Arduino

Electrónica de potencia

http://es.wikipedia.org/wiki/Electr%C3%B3nica_de_potencia

Transistor BJT

http://es.wikipedia.org/wiki/Transistor_de_uni%C3%B3n_bipolar

Diodo Emisor de luz

http://es.wikipedia.org/wiki/Led

Diodo rectificador

http://es.wikipedia.org/wiki/Diodo

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

11. ANEXOS.

Secuencia de desarrollo del proyecto AHORRO ENERGETICO

1. Reconocimiento de elementos del proyecto.
2. Investigación de configuración de terminales de los componentes
3. Características eléctricas de los componentes.
4. Sensores Radio Frecuencia. Tipos y características.
5. Tecnología arduino
6. Técnicas de adquisición de datos por radio frecuencia.
7. Escudos o Shield for arduino.
8. Converter level for arduino
9. Pantalla LCD.
10. Programación de arduino para adquisición de datos (RFID)
11. Especificaciones eléctricas de operación y funcionamiento de los sensores.
12. Sensores PIR.
13. Escudo XBEE Xplorer (transmisión alámbrica de la información).
14. Configuración y programación de escudos Xbee para la comunicación inalámbrica.
15. Diseño de la interfaz gráfica para la adquision de datos en V.B. (aplicación de escritorio)
16. Codificación de la aplicación.
17. Diseño de la interfaz gráfica para mostrar información del docente que hace uso de un aula. (aplicación de web – acceso vía red con tecnología móvil wifi).
18. Codificación de la aplicación.
19. Preparación, Instalación y configuración de Windows SERVER en un PC.
20. Promover el servidor.
21. Instalación del servicio DNS en Windows SERVER.
22. Instalación del servicio web en el servidor (IIS y Apache).
23. Configuración de Router para enlace vía red wifi con tecnología móvil)
24. Pruebas de comunicación entre los dispositivos de comunicación y sensores / actuadores.
25. Depuración de errores.
26. Instalación y configuración del SMBD.

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

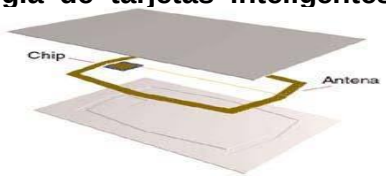
27. Elaboración del diseño de la Base de datos.
28. Creación de la BD.
29. Enlace del sistema con la base de datos.
30. Pruebas de comunicación todo el sistema y BD.
31. Depuración de errores.
32. Instalación del sistema en el aula.
33. Pruebas de funcionalidad en el aula.
34. Mejoras de observaciones realizadas al sistema (Fallos en el sistema al irse energía eléctrica y estar operando el sistema, Mostrar solo información del docente que está haciendo uso del aula en la aplicación web, etc.).
35. Sistema instalado en aula en pruebas de funcionalidad por bloques de horas clase.
36. Visualizar información procesada por el sistema desde dispositivos móvil u otros con tecnología wifi.

Introducción de sistemas de identificación de acceso basado en una tarjeta de Identidad u otra credencial de identidad que incluya inteligencia integrada.

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

Visión General del Sistema de Control Acceso Físico	Para el usuario, un sistema de control de acceso está compuesto de 4 elementos: Una tarjeta o ficha (una credencial de identidad) que se presenta al lector de la puerta de acceso. • Un lector de puerta de acceso que indica si la Tarjeta es válida y se autoriza la entrada. ✓ Una computadora y software que incorporan una funcionalidad robusta de seguridad (una base de datos. ✓ Un micriocontrolador (placa Arduino). Ejecutará las instrucciones programadas una vez que la computadora compruebe si la información es correcta enviada por el lector es valida
Componentes del Sistema de Control Acceso	Un sistema de control acceso típico está compuesto de los siguientes componentes: • Una credencial de identificación (tarjeta inteligente). • Un lector de puerta de acceso (lector de tarjeta inteligente) • Panel de Control. • Servidor de control de acceso. • Software. • Base de Datos

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

Tecnología de tarjetas inteligentes  	Está basada en estándares (de contacto y sin contacto).Están teniendo cada vez más Aceptación como la credencial de preferencia para controlar el acceso físico con seguridad.
¿Cómo funciona el sistema de control de acceso físico?	El sistema de control de acceso físico es una red coordinada de tarjetas de identificación, lectores electrónicos, bases de datos especializadas, software y computadoras diseñadas para monitorear y controlar el tráfico a través de puntos de acceso.
¿Qué papel juegan las tarjetas inteligentes en un sistema de control de acceso físico?	Los sistemas de control de acceso físico basados en tarjetas inteligentes son una herramienta de seguridad poderosa, eficiente para proteger los bienes de una empresa o institución. Cada tarjeta almacena información protegida sobre la persona y sobre los privilegios de esta persona.

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

¿Cuáles son los temas centrales que deben ser considerados cuando se implementa un sistema de control de acceso físico en base a las tarjetas inteligentes?	Componentes a utilizar en el Sistema • Tecnologías de Tarjetas de identidad u otra credencial de identidad que incluya Inteligencia Integrada. • Comunicaciones Entre Tarjetas y Lectores de Tarjetas • Comunicaciones entre el Lector de Tarjeta y el • Panel de Control • Como funciona un Servidor de Control de Acceso • Proceso de Control de Acceso • Beneficios de las Tarjetas de Identificación Inteligentes • Encriptación de datos (En tarjetas Smart Card y RFID) • Consideraciones a Nivel de Sistema (base de datos) • Costos y Beneficios

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

FIRMWARE DEL DISPOSIVO DE CONTROL TRANSMISOR (UC ATMEGA2560)

```
#include <LiquidCrystal.h>

LiquidCrystal lcd(12, 11, 7, 6, 5, 4);

//LiquidCrystal lcd(12, 11, 2, 7, 8, 9, 10);

/* Configuración de LCD

 RS Enable R/W D4 D5 D6 D7 VSS VDD Vo

 12  11  Gnd 5 4 3 2 Gnd Vcc Pot

String docente="";

int RFIDResetPin = 13;

int bandera=0;

int bandera1=0;

//const int ledPin = 13;

int buttonState = 0;

int flag=1;

//Register your RFID tags here

char tag1[13] = "6F005CA55ACC";  //Dato transmitido serialmente con esta Tag 1

char tag2[13] = "6F005CC67D88";  //Dato transmitido serialmente con esta Tag 2

char tag3[13] = "710024DF8309";  //Dato transmitido serialmente con esta Tag 3

char tag4[13] = "6F005CC07487";  //Dato transmitido serialmente con esta Tag 4

char tag5[13] = "6F005C81A311";  //Dato transmitido serialmente con esta Tag 5 ---- la pongo como tarjeta desconocida por no tenerla en la BD Registrada.

char tag6[13] = "6F005C94ED4A";  //Dato transmitido serialmente con esta Tag 6

char tag7[13] = "6F005C5D4B25";  //Dato transmitido serialmente con esta Tag 7

char tag8[13] = "6F005C9401A6";  //Dato transmitido serialmente con esta Tag 8

char tag9[13] = "6F005CBFA529";  //Dato transmitido serialmente con esta Tag 9

char tag10[13] = "6F005C7B0F47";  //Dato transmitido serialmente con esta Tag 10
```


DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

```
char tag11[13] = "6F005CC347B7";  //Dato transmitido serialmente con esta Tag 11
char tag12[13] = "6F005CBE109D";  //Dato transmitido serialmente con esta Tag 12
char tag13[13] = "71002534BADA"; //Dato transmitido serialmente con esta Tag 13
char tag14[13] = "6F005C656335"; //Dato transmitido serialmente con esta Tag 14
char tag15[13] = "6F005C94FE59"; //Dato transmitido serialmente con esta Tag 15
char tag16[13] = "6F005C846ADD"; //Dato transmitido serialmente con esta Tag 16
char tag17[13] = "6F005CB569EF"; //Dato transmitido serialmente con esta Tag 17
char tag18[13] = "6F005C9F44E8"; //Dato transmitido serialmente con esta Tag 18
char tag19[13] = "6F005CBD29A7"; //Dato transmitido serialmente con esta Tag 19
char tag20[13] = "6F005CA773E7"; //Dato transmitido serialmente con esta Tag 20
char tag21[13] = "6F005CB60F8A"; //Dato transmitido serialmente con esta Tag 21
char tag22[13] = "6F005C6FE6BA"; //Dato transmitido serialmente con esta Tag 22
void setup(){
 Serial.begin(9600);
 Serial1.begin(9600);
 lcd.begin(16, 2);// Configurando el numero columnas y filas de LCD
 lcd.print("BIENVENIDOS / AS...");
 lcd.setCursor(0, 1);
 lcd.print("INTRO TAG READER");
 pinMode(RFIDResetPin, OUTPUT);
 digitalWrite(RFIDResetPin, HIGH);
 pinMode(2, OUTPUT);
 pinMode(3, OUTPUT);
 pinMode(4, OUTPUT);
 pinMode(5, OUTPUT);
```


DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

```
 pinMode(6, OUTPUT);
 pinMode(7, OUTPUT);
 pinMode(8, OUTPUT);
 pinMode(9, OUTPUT);
 pinMode(10, OUTPUT);
 pinMode(11, OUTPUT);
}
void loop(){
 char tagString[13];
 int index = 0;
 boolean reading = false;
 while(Serial1.available()){
  int readByte = Serial1.read();
  if(readByte == 2) reading = true;
  if(readByte == 3) reading = false;
  if(reading && readByte != 2 && readByte != 10 && readByte != 13){
   //store the tag
   tagString[index] = readByte;
   index ++;
  }
  if (bandera=1)
  {
   lcd.clear();
   lcd.setCursor(0, 0);
   lcd.print("BIENVENIDO / AS...");
```


DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

```
   //C, F
   lcd.setCursor(0, 1);
   lcd.print(docente);
  }
  else{
   lcd.clear();
   lcd.setCursor(0, 0);
   lcd.print("BIENVENIDO / AS...");
   //C, F
   lcd.setCursor(0, 1);
   lcd.print("INTRO TAG READER");
  }
}
 //if (flag==1) lightLEDoff(2);
 checkTag(tagString);
 //clearTag(tagString);
 resetReader();
 comprobarexitag();
 clearTag(tagString);
 notag();
}
void checkTag(char tag[]){
 //bandera=0;
 if(strlen(tag) == 0) return; //empty, no need to contunue
 bandera=0;
```


DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

```
if(compareTag(tag, tag1)){ // 6F005CA55ACC - Ing. Ortiz
 //lightLED(2);
 ActivarCargas(2,3);
 //Serial.print("1");
 docente="ING. ALFONSO ORT";
 bandera=1;
 Serial.print(tag1);
 //lcd.setCursor(0, 1);
 //lcd.print(docente);
}
else if(compareTag(tag, tag2)){ // 6F005CC67D88 - Ing. Gustavo Raul Alfaro
 //lightLED(2);
 ActivarCargas(2,3);
 //Serial.print("2");
 docente="ING. GUSTAVO ALF";
 bandera=1;
 Serial.print(tag2);
 //lcd.setCursor(0, 1);
 //lcd.print(docente);
}
else if(compareTag(tag, tag3)){ // 710024DF8309 - Lic. Manuel de Jesús Gámez López
 //lightLED(2);
 ActivarCargas(2,3);
 //Serial.print("3");
 docente="LIC. MANUEL G.L.";
```


DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

```
 bandera=1;
 Serial.print(tag3);
 //lcd.setCursor(0, 1);
 //lcd.print(docente);
}
else if(compareTag(tag, tag4)){ // 6F005CC07487 - Ing. Wuilfredo Santamaria
 //lightLED(2);
 ActivarCargas(2,3);
 //Serial.print("4");
 docente="ING. WILFREDO S.";
 bandera=1;
 Serial.print(tag4);
 //lcd.setCursor(0, 1);
 //lcd.print(docente);
 /*}else if(compareTag(tag, tag5)){ // 6F005C81A311 - Desconocida
  //lightLED(2);
  ActivarCargas(2,3);
  //Serial.print("5");
  Serial.print(tag5);*/
 //=========================================================================
}
else if(compareTag(tag, tag6)){
 //lightLED(2);
 ActivarCargas(2,3);
 //Serial.print("6");
```


DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

```
 //docente="INTRO TAG READER";
 bandera=0;
 Serial.print(tag6);
}
else if(compareTag(tag, tag7)){
 //lightLED(2);
 ActivarCargas(2,3);
 //Serial.print("7");
 //docente="INTRO TAG READER";
 bandera=0;
 Serial.print(tag7);
}
else if(compareTag(tag, tag8)){
 //lightLED(2);
 ActivarCargas(2,3);
 //Serial.print("8");
 //docente="INTRO TAG READER";
 bandera=0;
 Serial.print(tag8);
}
else if(compareTag(tag, tag9)){
 //lightLED(2);
 ActivarCargas(2,3);
 //Serial.print("9");
 //docente="INTRO TAG READER";
```


DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

```
 bandera=0;
 Serial.print(tag9);
}
else if(compareTag(tag, tag10)){
 //lightLED(2);
 ActivarCargas(2,3);
 //Serial.print("A");
 //docente="INTRO TAG READER";
 bandera=0;
 Serial.print(tag10);
}
else if(compareTag(tag, tag11)){
 //lightLED(2);
 ActivarCargas(2,3);
 //Serial.print("B");
 //docente="INTRO TAG READER";
 bandera=0;
 Serial.print(tag11);
}
else if(compareTag(tag, tag12)){
 //lightLED(2);
 ActivarCargas(2,3);
 //Serial.print("C");
 //docente="INTRO TAG READER";
 bandera=0;
```


DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

```
 Serial.print(tag12);
}
else if(compareTag(tag, tag13)){
 //lightLED(2);
 ActivarCargas(2,3);
 //Serial.print("D");
 //docente="INTRO TAG READER";
 bandera=0;
 Serial.print(tag13);
}
else if(compareTag(tag, tag14)){
 //lightLED(2);
 ActivarCargas(2,3);
 //Serial.print("E");
 //docente="INTRO TAG READER";
 Serial.print(tag14);
}
else if(compareTag(tag, tag15)){
 //lightLED(2);
 ActivarCargas(2,3);
 //Serial.print("F");
 //docente="INTRO TAG READER";
 bandera=0;
 Serial.print(tag15);
}
```


DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

```
else if(compareTag(tag, tag16)){
 //lightLED(2);
 ActivarCargas(2,3);
 //Serial.print("G");
 // docente="INTRO TAG READER";
 bandera=0;
 Serial.print(tag16);
}
else if(compareTag(tag, tag17)){
 //lightLED(2);
 ActivarCargas(2,3);
 //Serial.print("H");
 //docente="INTRO TAG READER";
 bandera=0;
 Serial.print(tag17);
}
else if(compareTag(tag, tag18)){
 //lightLED(2);
 ActivarCargas(2,3);
 //Serial.print("I");
 //docente="INTRO TAG READER";
 bandera=0;
 Serial.print(tag18);
}
else if(compareTag(tag, tag19)){
```


DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

```
 //lightLED(2);
 ActivarCargas(2,3);
 //Serial.print("J");
 //docente="INTRO TAG READER";
 bandera=0;
 Serial.print(tag19);
}
else if(compareTag(tag, tag20)){
 //lightLED(2);
 ActivarCargas(2,3);
 //Serial.print("K");
 //docente="INTRO TAG READER";
 bandera=0;
 Serial.print(tag20);
}
else if(compareTag(tag, tag21)){
 //lightLED(2);
 ActivarCargas(2,3);
 //Serial.print("L");
 //docente="INTRO TAG READER";
 bandera=0;
 Serial.print(tag21);
}
else if(compareTag(tag, tag22)){
 //lightLED(2);
```


DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

```
 ActivarCargas(2,3);
 //Serial.print("M");
 //docente="INTRO TAG READER";
 bandera=0;
 Serial.print(tag22);
}
else{
 Serial.print(tag);  //Imprimo codigo de tarjeta RFID en caso de ser desconocida.
 //lcd.clear();            //Borramos todos los datos de la lCD
 docente="TAG UNKNOW,CHECK";
 bandera=0;
 //Serial.println("Desconocida");
}
//C, F
//lcd.setCursor(0, 1);
//lcd.print(docente);
}
void ActivarCargas(int contactor1, int contactor2){
 digitalWrite(contactor1, HIGH);
 digitalWrite(contactor2, HIGH);
 delay(1000);
}
void DesactivarCargas(int contactor1, int contactor2){
 digitalWrite(contactor1, LOW);
 digitalWrite(contactor2, LOW);
```


DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

```
}
void resetReader(){
 digitalWrite(RFIDResetPin, LOW);
 digitalWrite(RFIDResetPin, HIGH);
 delay(1000);
}
void comprobarexitag(){
 buttonState = digitalRead(RFIDResetPin);
 if (buttonState == HIGH)
 {
  digitalWrite(2, LOW);
  digitalWrite(3, LOW);
  //bandera=0;
  lcd.clear();
  lcd.setCursor(0, 0);
  lcd.print("BIENVENIDO / AS...");
  //C, F
  lcd.setCursor(0, 1);
  lcd.print("INTRO TAG READER");
 }
 else{
  digitalWrite(2, HIGH);
  digitalWrite(3, HIGH);
  //delay(5000);
 }
```


DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

```
}
void clearTag(char one[]){
 for(int i = 0; i < strlen(one); i++){
  one[i] = 0;
 }
}
boolean compareTag(char one[], char two[]){
 if(strlen(one) == 0) return false;
 for(int i = 0; i < 12; i++){
  if(one[i] != two[i]) return false;
 }
 return true;
}
void notag() {
 while (Serial1.available() <= 0) {
  Serial.print('?');  // send a capital A
  delay(1000);
 }
}
=====================================================================
    ***** Pin layout should be as follows: ******
 * Signal   Pin       Pin       Pin
 *      Arduino Uno   Arduino Mega   MFRC522 board
 * ------------------------------------------------------------
 * Reset     9         5         RST
```


DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

```
 * SPI SS    10        53        SDA
 * SPI MOSI  11        51        MOSI
 * SPI MISO  12        50        MISO
 * SPI SCK   13        52        SCK
 *
 * The reader can be found on eBay for around 5 dollars. Search for "mf-rc522" on ebay.com.
 */
/*
CONFIGURACION PARA EL ARDUINO UNO CHOVI GAMEZ....
Modulo rfid MF522-AN
Reset > Pin 5
SS > Pin 10
MOSI > Pin 11
MISO > Pin 12
SCK > Pin 13
Ground > Ground
3.3v > 3.3v
zumbador 5v - pin 7
led rojo con r 520 ohmios - pin 3
led verde con r 520 ohmios - pin 4
tarjeta rele 5v - pin 4
activar monitor serie para ver estado
detecta tarjeta numero 2 - enciende led rojo 2s y muestra en monitor "acceso denegado"
detecta tarjeta numero 206 - enciende led verde y rele 2s y muesta "acceso autorizado"
*/
```


DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

```
#include <SPI.h>
#include <MFRC522.h>
#include <LiquidCrystal.h>
#define         uchar   unsigned char
#define         uint      unsigned int
#define PCD_IDLE       0x00       //NO action; cancel current commands
#define PCD_AUTHENT      0x0E       //verify password key
#define PCD_RECEIVE      0x08       //receive data
#define PCD_TRANSMIT     0x04       //send data
#define PCD_TRANSCEIVE    0x0C       //send and receive data
#define PCD_RESETPHASE    0x0F       //reset
#define PCD_CALCCRC      0x03       //CRC check and caculation
//Mifare_One card command bits
#define PICC_REQIDL      0x26       //Search the cards that not into sleep mode in the antenna area
#define PICC_REQALL      0x52       //Search all the cards in the antenna area
#define PICC_ANTICOLL     0x93       //prevent conflict
#define PICC_SElECTTAG    0x93       //select card
#define PICC_AUTHENT1A    0x60       //verify A password key
#define PICC_AUTHENT1B    0x61       //verify B password key
#define PICC_READ       0x30       //read
#define PICC_WRITE      0xA0       //write
#define PICC_DECREMENT    0xC0       //deduct value
#define PICC_INCREMENT    0xC1       //charge up value
#define PICC_RESTORE     0xC2       //Restore data into buffer
#define PICC_TRANSFER     0xB0       //Save data into buffer
```


DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

```
#define PICC_HALT       0x50        //sleep mode
#define MAX_LEN 16
//////////////////////////////////////////////////////////////////
//set the pin
//////////////////////////////////////////////////////////////////
const int chipSelectPin = 53;  //SPI SS o SDA del dispositivo rfid-RC522
const int NRSTPD = 9;   //9=0()   //Aca especifico el pin de reset del dispositivo rfid-RC522
LiquidCrystal lcd(8, 7, 6, 5, 4, 3);
/*Configuración de LCD
 RS Enable R/W D4 D5 D6 D7 VSS VDD Vo
 8   7  Gnd 6 5 4 3 Gnd Vcc Pot*/
int comprobarTAG=0;
bool flag1=false;
int id=0;
#define lectura 2
#define relay1 12
#define relay2 13
#define PCD_IDLE        0x00
#define PCD_AUTHENT    0x0E
#define PCD_RECEIVE     0x08
#define PCD_TRANSMIT    0x04
#define PCD_TRANSCEIVE  0x0C
#define PCD_RESETPHASE 0x0F
#define PCD_CALCCRC     0x03
#define PICC_REQIDL      0x26
```


DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

```
#define PICC_REQALL      0x52
#define PICC_ANTICOLL     0x93
#define PICC_SEIECTTAG    0x93
#define PICC_AUTHENT1A    0x60
#define PICC_AUTHENT1B    0x61
#define PICC_READ       0x30
#define PICC_WRITE      0xA0
#define PICC_DECREMENT    0xC0
#define PICC_INCREMENT    0xC1
#define PICC_RESTORE     0xC2
#define PICC_TRANSFER     0xB0
#define PICC_HALT       0x50
#define MI_OK         0
#define MI_NOTAGERR      1
#define MI_ERR        2
//------------------MFRC522---------------
//Page 0:Command and Status
#define   Reserved00      0x00
#define   CommandReg      0x01
#define   CommIEnReg      0x02
#define   DivlEnReg       0x03
#define   CommIrqReg      0x04
#define   DivIrqReg       0x05
#define   ErrorReg        0x06
#define   Status1Reg      0x07
```


DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

```
#define   Status2Reg      0x08
#define   FIFODataReg     0x09
#define   FIFOLevelReg    0x0A
#define   WaterLevelReg   0x0B
#define   ControlReg      0x0C
#define   BitFramingReg   0x0D
#define   CollReg         0x0E
#define   Reserved01      0x0F
//Page 1:Command
#define   Reserved10      0x10
#define   ModeReg         0x11
#define   TxModeReg       0x12
#define   RxModeReg       0x13
#define   TxControlReg    0x14
#define   TxAutoReg       0x15
#define   TxSelReg        0x16
#define   RxSelReg        0x17
#define   RxThresholdReg  0x18
#define   DemodReg        0x19
#define   Reserved11      0x1A
#define   Reserved12      0x1B
#define   MifareReg       0x1C
#define   Reserved13      0x1D
#define   Reserved14      0x1E
#define   SerialSpeedReg  0x1F
```


DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

```
//Page 2:CFG
#define   Reserved20      0x20
#define   CRCResultRegM     0x21
#define   CRCResultRegL     0x22
#define   Reserved21      0x23
#define   ModWidthReg       0x24
#define   Reserved22      0x25
#define   RFCfgReg        0x26
#define   GsNReg          0x27
#define   CWGsPReg              0x28
#define   ModGsPReg       0x29
#define   TModeReg        0x2A
#define   TPrescalerReg     0x2B
#define   TReloadRegH       0x2C
#define   TReloadRegL       0x2D
#define   TCounterValueRegH   0x2E
#define   TCounterValueRegL   0x2F
//Page 3:TestRegister
#define   Reserved30      0x30
#define   TestSel1Reg       0x31
#define   TestSel2Reg       0x32
#define   TestPinEnReg      0x33
#define   TestPinValueReg   0x34
#define   TestBusReg      0x35
#define   AutoTestReg       0x36
```


DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

```
#define   VersionReg      0x37
#define   AnalogTestReg     0x38
#define   TestDAC1Reg      0x39
#define   TestDAC2Reg      0x3A
#define   TestADCReg      0x3B
#define   Reserved31      0x3C
#define   Reserved32      0x3D
#define   Reserved33      0x3E
#define   Reserved34      0x3F
//-----------------------------------------------
uchar serNum[5];
//int serNum[5];
uchar writeData[16]={0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 100};
uchar moneyConsume = 18 ;
uchar moneyAdd = 10 ;
 uchar sectorKeyA[16][16] = {{0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF},
              {0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF},
              //{0x19, 0x84, 0x07, 0x15, 0x76, 0x14},
              {0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF},
             };
 uchar sectorNewKeyA[16][16] = {{0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF},
               {0xFF,  0xFF,  0xFF,  0xFF,  0xFF,  0xFF,  0xff,0x07,0x80,0x69,
0x19,0x84,0x07,0x15,0x76,0x14},
                //you can set another ket , such as " 0x19, 0x84, 0x07, 0x15, 0x76, 0x14 "
               //{0x19,  0x84,  0x07,  0x15,  0x76,  0x14,  0xff,0x07,0x80,0x69,
0x19,0x84,0x07,0x15,0x76,0x14},
```


DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

```
            // but when loop, please set the sectorKeyA, the same key, so that RFID module can read the card
            {0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xff,0x07,0x80,0x69, 0x19,0x33,0x07,0x15,0x34,0x14},
            };
void setup() {
  lcd.begin(16, 2);// Configurando el numero columnas y filas de LCD
  lcd.print("Sist. Energetico");
   Serial.begin(9600);          // RFID reader SOUT pin connected to Serial RX pin at 2400bps
  // start the SPI library:
  SPI.begin();
  pinMode(chipSelectPin,OUTPUT);          // Set digital pin 10 as OUTPUT to connect it to the RFID /ENABLE pin
 digitalWrite(chipSelectPin, LOW);     // Activate the RFID reader
 pinMode(NRSTPD,OUTPUT);          // Set digital pin 10 , Not Reset and Power-down
 digitalWrite(NRSTPD, HIGH);
   pinMode(lectura,OUTPUT);
  //LED ON MIENTRAS ESTE PUESTA EN EL LECTOR LA TARJETA.
  pinMode(relay1,OUTPUT);
  pinMode(relay2,OUTPUT);

  digitalWrite(relay1,LOW);
  digitalWrite(relay2,LOW);
 MFRC522_Init();
}
void loop()
```


DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

```
{
    comprobarTAG=0;
    flag1=false;
       id=0;
      byte llavero[] = {
            0x14, 0xA0, 0x94, 0x5B, // 14,A0,94,5B,  //14A0945B7B
            0x7B          // 7B
           };
      byte tarjeta[] = {
             0xA5, 0xDB, 0x1F, 0xD1,  // A5,DB,1F,D1, //A5DB1D1B0
             0xB0           // B0
            };
         uchar i,tmp;
         uchar status;
    uchar str[MAX_LEN];
    uchar RC_size;
    uchar blockAddr;
    String mynum = "";
                  status = MFRC522_Request(PICC_REQIDL, str);
                  if (status == MI_OK)
                  {
          /*Serial.println("Tarjeta detectada:");
                        Serial.print(str[0],HEX);
          Serial.print(":");
                        Serial.print(str[1],HEX);
```


DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

```
Serial.println(" ");
digitalWrite(7,HIGH);
delay(100);
digitalWrite(7,LOW);*/
        status = MFRC522_Anticoll(str);
        memcpy(serNum, str, 5);
        if (status == MI_OK)
        {
Serial.println("CODIGO TARJETA: ");
                /*Serial.print(serNum[0],HEX);
                Serial.print(serNum[1],HEX);
                Serial.print(serNum[2],HEX);
                Serial.print(serNum[3],HEX);
                Serial.print(serNum[4],HEX);
Serial.println(" ");
delay(1000);*/
//COMPROBANDO CODIGO DE TARJETA
for (int k=0;k<5;k++){
  if (serNum[k]==tarjeta[k]) {
    flag1=true;id=1;
      if (flag1==true && id==1){
            comprobarTAG=comprobarTAG+1;
            }
    Serial.print(tarjeta[k],HEX);
  }
```


DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

```
          if (serNum[k]==llavero[k]) {
            flag1=true;id=2;
              if (flag1==true && id==2){
               comprobarTAG=comprobarTAG+1;
               }
             Serial.print(llavero[k],HEX);
           }//else{id=5;}
         }
         Serial.println("");
         digitalWrite(lectura,HIGH);
         delay(2000);          //Aca defino el tiempo de parpadeo (Lectura, escaneo o verificacion de tarjeta RFID puesta)
                               //en el lector RFID. En caso de no parpadear el LED Indicador que la tarjeta no esta puesta.
         digitalWrite(lectura,LOW);
         delay(1000);
               }
      }
       cargas(flag1,comprobarTAG,id);    //LLamando a la Funcion "cargas" para que ejecute la tarea asignada a la TAG RFID.
                MFRC522_Halt();
}
  void cargas(bool senal, int total, int ide)
  {
    if (senal==true && total==5 && ide==1){
      msgok();
```


DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

```
      lcd.print("Lic.Chovi Gamez");
    }else if (senal==true && total==5 && ide==2){
        msgok();
        lcd.print("Ing. Wilfredo...");
    }else if (senal==false && total==0 && ide==5){
        lcd.setCursor(1, 2);
        lcd.print("UN-KNOW TAG RFID");
    }else{
        msgno();
       }
  }
  void msgok(){
    digitalWrite(relay1,HIGH);
    digitalWrite(relay2,HIGH);
    lcd.setCursor(1, 2);
  }
  void msgno(){
   digitalWrite(relay1,LOW);
   digitalWrite(relay2,LOW);
   lcd.setCursor(1, 2);
   lcd.print("Whats Your TAG?");
  }
/*  : Write_MFRC5200 */

void Write_MFRC522(uchar addr, uchar val)
{
```


DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

```
        digitalWrite(chipSelectPin, LOW);
        //0XXXXXX0
        SPI.transfer((addr<<1)&0x7E);
        SPI.transfer(val);

        digitalWrite(chipSelectPin, HIGH);
}
/* Read_MFRC522 */
uchar Read_MFRC522(uchar addr)
{
        uchar val;
        digitalWrite(chipSelectPin, LOW);
        // : 1XXXXXX0
        SPI.transfer(((addr<<1)&0x7E) | 0x80);
        val =SPI.transfer(0x00);

        digitalWrite(chipSelectPin, HIGH);

        return val;
}
/* : SetBitMask */
void SetBitMask(uchar reg, uchar mask)
{
  uchar tmp;
```


DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

```
  tmp = Read_MFRC522(reg);
  Write_MFRC522(reg, tmp | mask); // set bit mask
}

/* : ClearBitMask */

void ClearBitMask(uchar reg, uchar mask)
{
  uchar tmp;
  tmp = Read_MFRC522(reg);
  Write_MFRC522(reg, tmp & (~mask)); // clear bit mask
}

/* : AntennaOn */

void AntennaOn(void)
{
        uchar temp;
        temp = Read_MFRC522(TxControlReg);
        if (!(temp & 0x03))
        {
                SetBitMask(TxControlReg, 0x03);
        }
}

/* : AntennaOff */

void AntennaOff(void)
{
        ClearBitMask(TxControlReg, 0x03);
```


DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

```
}
/* ResetMFRC522 */
void MFRC522_Reset(void)
{
  Write_MFRC522(CommandReg, PCD_RESETPHASE);
}
/* nitMFRC522 */
void MFRC522_Init(void)
{
        digitalWrite(NRSTPD,HIGH);
        MFRC522_Reset();
        //Timer: TPrescaler*TreloadVal/6.78MHz = 24ms
  Write_MFRC522(TModeReg, 0x8D);              //Tauto=1; f(Timer) = 6.78MHz/TPreScaler
  Write_MFRC522(TPrescalerReg, 0x3E); //TModeReg[3..0] + TPrescalerReg
  Write_MFRC522(TReloadRegL, 30);
  Write_MFRC522(TReloadRegH, 0);
        Write_MFRC522(TxAutoReg, 0x40);                 //100%ASK
        Write_MFRC522(ModeReg, 0x3D);           //CRCx6363
        //ClearBitMask(Status2Reg, 0x08);           //MFCrypto1On=0
        //Write_MFRC522(RxSelReg, 0x86);                //RxWait = RxSelReg[5..0]
        //Write_MFRC522(RFCfgReg, 0x7F);                //RxGain = 48dB
        AntennaOn();
}
/*
 * MFRC522_Request
```


DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

```
 *       TagType--              0x4400 = Mifare_UltraLight
 *                              0x0400 = Mifare_One(S50)
 *                              0x0200 = Mifare_One(S70)
 *                              0x0800 = Mifare_Pro(X)
 *                              0x4403 = Mifare_DESFire
 * MI_OK
 */
uchar MFRC522_Request(uchar reqMode, uchar *TagType)
{
        uchar status;
        uint backBits;
        Write_MFRC522(BitFramingReg, 0x07);             //TxLastBists = BitFramingReg[2..0]
        ???

        TagType[0] = reqMode;
        status = MFRC522_ToCard(PCD_TRANSCEIVE, TagType, 1, TagType, &backBits);
        if ((status != MI_OK) || (backBits != 0x10))
        {
                status = MI_ERR;
        }
        return status;
}
/*
 * MFRC522_ToCard
 * command--MF522
 *                      sendData--RC522
```


DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

```
 *                      sendLen--
 *                      backData-
 *                      backLen--
 * MI_OK
 */
uchar MFRC522_ToCard(uchar command, uchar *sendData, uchar sendLen, uchar *backData,
uint *backLen)
{
  uchar status = MI_ERR;
  uchar irqEn = 0x00;
  uchar waitIRq = 0x00;
  uchar lastBits;
  uchar n;
  uint i;
  switch (command)
  {
    case PCD_AUTHENT:
                {
                        irqEn = 0x12;
                        waitIRq = 0x10;
                        break;
                }
                case PCD_TRANSCEIVE:
                {
                        irqEn = 0x77;
                        waitIRq = 0x30;
```


DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

```
                    break;
                }
                default:
                    break;
  }
  Write_MFRC522(CommIEnReg, irqEn|0x80);     //
  ClearBitMask(CommIrqReg, 0x80);
  SetBitMask(FIFOLevelReg, 0x80);                    //FlushBuffer=1, FIFO
       Write_MFRC522(CommandReg, PCD_IDLE);       //NO action
  for (i=0; i<sendLen; i++)
  {
                Write_MFRC522(FIFODataReg, sendData[i]);
       }
       Write_MFRC522(CommandReg, command);
  if (command == PCD_TRANSCEIVE)
  {
                SetBitMask(BitFramingReg, 0x80);          //StartSend=1,transmission of data
starts
       }
       i = 2000;
  do
  {
                //CommIrqReg[7..0]
                //Set1 TxIRq RxIRq IdleIRq HiAlerIRq LoAlertIRq ErrIRq TimerIRq
    n = Read_MFRC522(CommIrqReg);
    i--;
```


DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

```
}
while ((i!=0) && !(n&0x01) && !(n&waitIRq));
ClearBitMask(BitFramingReg, 0x80);                    //StartSend=0

if (i != 0)
{
  if(!(Read_MFRC522(ErrorReg) & 0x1B))          //BufferOvfl Collerr CRCErr ProtecolErr
  {
    status = MI_OK;
    if (n & irqEn & 0x01)
    {
                                status = MI_NOTAGERR;                    //??
                        }
    if (command == PCD_TRANSCEIVE)
    {
       n = Read_MFRC522(FIFOLevelReg);
       lastBits = Read_MFRC522(ControlReg) & 0x07;
     if (lastBits)
     {
                                        *backLen = (n-1)*8 + lastBits;
                                }
     else
     {
                                        *backLen = n*8;
                                }
```


DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

```
        if (n == 0)
        {
                                        n = 1;
                                }
        if (n > MAX_LEN)
        {
                                        n = MAX_LEN;
                                }
        for (i=0; i<n; i++)
        {
                                        backData[i] = Read_MFRC522(FIFODataReg);
                                }
     }
    }
    else
    {
                        status = MI_ERR;
                }

  }
  //SetBitMask(ControlReg,0x80);      //timer stops
  //Write_MFRC522(CommandReg, PCD_IDLE);
  return status;
}
/*
```


DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

```
 * MFRC522_Anticoll
 *MI_OK
 */
uchar MFRC522_Anticoll(uchar *serNum)
{
  uchar status;
  uchar i;
        uchar serNumCheck=0;
  uint unLen;
  //ClearBitMask(Status2Reg, 0x08);                 //TempSensclear
  //ClearBitMask(CollReg,0x80);                     //ValuesAfterColl
        Write_MFRC522(BitFramingReg, 0x00);               //TxLastBists = BitFramingReg[2..0]
   serNum[0] = PICC_ANTICOLL;
  serNum[1] = 0x20;
  status = MFRC522_ToCard(PCD_TRANSCEIVE, serNum, 2, serNum, &unLen);
  if (status == MI_OK)
        {
                for (i=0; i<4; i++)
                {
                        serNumCheck ^= serNum[i];
                }
                if (serNumCheck != serNum[i])
                {
                        status = MI_ERR;
                }
```


DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

```
  }
  //SetBitMask(CollReg, 0x80);                  //ValuesAfterColl=1
  return status;
}
/* CalulateCRC */
void CalulateCRC(uchar *pIndata, uchar len, uchar *pOutData)
{
  uchar i, n;
  ClearBitMask(DivIrqReg, 0x04);                        //CRCIrq = 0
  SetBitMask(FIFOLevelReg, 0x80);                             //FIFO
  //Write_MFRC522(CommandReg, PCD_IDLE);
  for (i=0; i<len; i++)
  {
                Write_MFRC522(FIFODataReg, *(pIndata+i));
        }
  Write_MFRC522(CommandReg, PCD_CALCCRC);
        //
  i = 0xFF;
  do
  {
    n = Read_MFRC522(DivIrqReg);
    i--;
  }
  while ((i!=0) && !(n&0x04));                          //CRCIrq = 1
        //CRC
```


DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

```
  pOutData[0] = Read_MFRC522(CRCResultRegL);
  pOutData[1] = Read_MFRC522(CRCResultRegM);
}
/* MFRC522_SelectTag */
uchar MFRC522_SelectTag(uchar *serNum)
{
  uchar i;
        uchar status;
        uchar size;
  uint recvBits;
  uchar buffer[9];
        //ClearBitMask(Status2Reg, 0x08);                    //MFCrypto1On=0
  buffer[0] = PICC_SElECTTAG;
  buffer[1] = 0x70;
  for (i=0; i<5; i++)
  {
        buffer[i+2] = *(serNum+i);
  }
        CalulateCRC(buffer, 7, &buffer[7]);          //??
  status = MFRC522_ToCard(PCD_TRANSCEIVE, buffer, 9, buffer, &recvBits);
  if ((status == MI_OK) && (recvBits == 0x18))
  {
                size = buffer[0];
        }
  else
```


DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

```
  {
                    size = 0;
          }
  return size;
}
/*
 *  : MFRC522_Auth

 *  : authMode-

        0x60 =

        0x61 =

       BlockAddr--

       Sectorkey--

       serNum--

       MI_OK
 */
uchar MFRC522_Auth(uchar authMode, uchar BlockAddr, uchar *Sectorkey, uchar *serNum)
{
  uchar status;
  uint recvBits;
  uchar i;
         uchar buff[12];
  buff[0] = authMode;
  buff[1] = BlockAddr;
  for (i=0; i<6; i++)
```


DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

```
  {
        buff[i+2] = *(Sectorkey+i);
    }
  for (i=0; i<4; i++)
  {
        buff[i+8] = *(serNum+i);
    }
  status = MFRC522_ToCard(PCD_AUTHENT, buff, 12, buff, &recvBits);
  if ((status != MI_OK) || (!(Read_MFRC522(Status2Reg) & 0x08)))
  {
        status = MI_ERR;
    }
  return status;
}
/*
 *  : MFRC522_Read
 * blockAddr--recvData--
 * MI_OK
 */
uchar MFRC522_Read(uchar blockAddr, uchar *recvData)
{
  uchar status;
  uint unLen;
  recvData[0] = PICC_READ;
  recvData[1] = blockAddr;
```


DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

```
  CalulateCRC(recvData,2, &recvData[2]);
  status = MFRC522_ToCard(PCD_TRANSCEIVE, recvData, 4, recvData, &unLen);
  if ((status != MI_OK) || (unLen != 0x90))
  {
    status = MI_ERR;
  }
  return status;
}
/*
 *  : MFRC522_Write

 *  : blockAddr--;writeData--

 * MI_OK
 */
uchar MFRC522_Write(uchar blockAddr, uchar *writeData)
{
  uchar status;
  uint recvBits;
  uchar i;
  uchar buff[18];
  buff[0] = PICC_WRITE;
  buff[1] = blockAddr;
  CalulateCRC(buff, 2, &buff[2]);
  status = MFRC522_ToCard(PCD_TRANSCEIVE, buff, 4, buff, &recvBits);
  if ((status != MI_OK) || (recvBits != 4) || ((buff[0] & 0x0F) != 0x0A))
```


DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

```
  {
                status = MI_ERR;
        }
  if (status == MI_OK)
  {
    for (i=0; i<16; i++)
    {
        buff[i] = *(writeData+i);
    }
    CalulateCRC(buff, 16, &buff[16]);
    status = MFRC522_ToCard(PCD_TRANSCEIVE, buff, 18, buff, &recvBits);
                if ((status != MI_OK) || (recvBits != 4) || ((buff[0] & 0x0F) != 0x0A))
    {
                        status = MI_ERR;
                }
  }
  return status;
}
/* : MFRC522_Halt */
void MFRC522_Halt(void)
{
        uchar status;
  uint unLen;
  uchar buff[4];
  buff[0] = PICC_HALT;
```


DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

```
  buff[1] = 0;
  CalulateCRC(buff, 2, &buff[2]);
  status = MFRC522_ToCard(PCD_TRANSCEIVE, buff, 4, buff,&unLen);
}
```

FIRMWARE DEL DISPOSIVO DE CONTROL RECEPTOR (UC ATMEGA328)

```
#define contactor1 13
#define contactor2 12
#define coderror 11
#define x 10
int estado=0;
int flag=0;
char mio;
char tag1 = '6F005CA55ACC';  //Dato transmitido serialmente con esta Tag 1
char tag2 = '6F005CC67D88';  //Dato transmitido serialmente con esta Tag 2
char tag3 = '710024DF8309';  //Dato transmitido serialmente con esta Tag 3
char tag4 = '6F005CC07487';  //Dato transmitido serialmente con esta Tag 4
char tag5 = '6F005C81A311';  //Dato transmitido serialmente con esta Tag 5 ---- la pongo como tarjeta desconocida por no tenerla en la BD Registrada.
//char tagx = "";
void setup() {
 //Serial.begin(9600);
 pinMode(contactor1,OUTPUT);
 pinMode(contactor2,OUTPUT);
 pinMode(coderror,OUTPUT);
 pinMode(x,INPUT);
 Serial.begin(9600);
```


DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

```
 //Serial1.begin(9600);
}
void loop() {
 flag=0;
 mio='?';
 //""""""""""""""""""""""""""""""""""""""""""
 if(Serial.available()>0)
 {
  char dato=Serial.read();
  Serial.print(dato);
  if (dato == '?')
    {
     digitalWrite(contactor1, LOW);
     digitalWrite(contactor2, LOW);
     digitalWrite(coderror, HIGH);
    }
   if (mio == '?')
    {
     digitalWrite(contactor1, LOW);
     digitalWrite(contactor2, LOW);
     digitalWrite(coderror, HIGH);
    }
  }
  //""""""""""""""""""""""""""""""""""""""""""
estado=digitalRead(x);
```


DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

```
 if (estado==HIGH)
 {
  flag=1;
 }
while(flag==1){
if(Serial.available()>0)
 {
  char dato=Serial.read();
  Serial.print(dato);
  if (dato == tag3) //Si el boton de power... apagamos el led
   {
    digitalWrite(contactor1, HIGH);
    digitalWrite(contactor2, HIGH);
    digitalWrite(coderror, LOW);
    //delay(1000);
   }else{
      if (dato == tag2)
        {
         digitalWrite(contactor1, HIGH);
         digitalWrite(contactor2, HIGH);
         digitalWrite(coderror, LOW);
         //delay(1000);
        }else{
           if (dato == tag1)
             {
```


DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

```
 digitalWrite(contactor1, HIGH);
 digitalWrite(contactor2, HIGH);
 digitalWrite(coderror, LOW);
 //delay(1000);
}else{
   if (dato == tag4)
    {
     digitalWrite(contactor1, HIGH);
     digitalWrite(contactor2, HIGH);
     digitalWrite(coderror, LOW);
     //delay(1000);
    }else{
       if (dato == tag5)
        {
         digitalWrite(contactor1, LOW);
         digitalWrite(contactor2, LOW);
         digitalWrite(coderror, HIGH);
         //delay(500);
        }else{
           if (dato == '?')
            {
             digitalWrite(contactor1, LOW);
             digitalWrite(contactor2, LOW);
             digitalWrite(coderror, HIGH);
             //delay(1000);
```


DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

```
                    }
}}}}}


}}
}
```

CODIGO DE LA APLICACIÓN WINDOWS FORM

```
Imports MySql.Data
Imports MySql.Data.MySqlClient
Imports System.Threading.Thread
Public Class UsoAula
  Dim az As String
  Dim sib As Integer
  Dim msn(100000) As String
  Public bandera As Boolean = False
  Dim f As Integer = 0
  Dim codigoRFID As String
  Dim caracteres As Integer = 0
  Public Sub guardarUsoAula()
    Dim oConexion As New MySqlConnection
    Dim oDataAdapter As MySqlDataAdapter
    'Dim oDataAdapter1 As MySqlDataAdapter
    Dim oDataSet1 As New DataSet
    Dim oDataTable As New DataTable
    Dim sSQL As String
    Dim sSQL1 As String
```


DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

```
    Dim sw As Boolean = False
    REM System.Threading.Thread.Sleep(1000)
    Try
      Dim cn As New MySqlConnection("Server=localhost;Database=ahorroenergetico;Uid=mjesus;Pwd=123456;")
      sSQL = "select * from docentes where codigoRFID ='" & txtcodigo1.Text & "'"
      'sSQL1 = "select nombre from docentes where codigoRFID ='" & txtcodigo1.Text & "'"
      cn.Open()
      oDataAdapter = New MySqlDataAdapter(sSQL, cn)
      oDataSet1.Clear()
      oDataAdapter.Fill(oDataSet1, "docentes")
      '************************************************************************
      'oDataAdapter = New MySqlDataAdapter(sSQL, cn)
      oDataAdapter.Fill(oDataTable)
      Dim names As String = oDataTable.Rows(0).Item("nombre")
      '************************************************************************
      If (oDataSet1.Tables("docentes").Rows.Count <> 0) Then
        Dim oDataset As New DataSet
        Dim StrQuery As String
        StrQuery = "insert into aula(codigoRFID,Aula,Fecha,Hora) values(@cod,@au,@fe,@ho)"
        Dim CmdPa As New MySql.Data.MySqlClient.MySqlCommand(StrQuery, cn)
        'cn.Open()
        oDataset.Clear()
        'Datos parametrisados que se muestran en la caja de texto
        Dim hora, fecha As String
        Dim aul As String = "C-301"
```


DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

```
        hora = Date.Now().ToLongTimeString
        fecha = Date.Now().ToLongDateString
        CmdPa.Parameters.AddWithValue("@cod", Me.txtcodigo1.Text)
        CmdPa.Parameters.AddWithValue("@au", aul)
        CmdPa.Parameters.AddWithValue("@fe", fecha)
        CmdPa.Parameters.AddWithValue("@ho", hora)
        CmdPa.ExecuteNonQuery()
        cn.Close()
        'MessageBox.Show("Registro Procesado del Acceso al Aula", "SISTEMA DE AHORRO ENERGÉTICO", MessageBoxButtons.OK, MessageBoxIcon.Information)
        lblAcciones.Text = "Bienvenido / a:, Docente Identificado. Planta Energética Trabajando..." & vbCrLf & _
                "Docente: " & names & "." & vbCrLf & "ID: " & txtcodigo1.Text & "." & _
                vbCrLf & "Aula: " & aul & "."
        señalizador.Text = 1
    Else
        'MessageBox.Show("Lo sentimos!!!! No se ha almacenado registro debido a que la tarjeta" _
        '         & vbCrLf & "no ha sido IDENTIFICADA por el sistema ahorro energético." & vbCrLf & vbCrLf & "Consulte con el administrador del sistema.", _
        '         "ERROR. Tarjeta no Identificada", MessageBoxButtons.OK)
        lblAcciones.Text = "Lo sentimos!!!! Su tarjeta está mala o Ud. no es un miembro de esta CEDE" & _
                vbCrLf & "Planta Energética deshabilitada." & _
                vbCrLf & "ID Tag: " & txtcodigo1.Text & "." & _
                vbCrLf & "Consulte con el administrador del sistema por cualquier duda."
    End If
```


DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

```
    Catch ex As Exception
     'MessageBox.Show("Error. Posiblemente existe un dupicado de registro", "Warninig", MessageBoxButtons.OK, MessageBoxIcon.Information)
     'Exit Sub
     'lblAcciones.Text = "Lo sentimos!!!! Su tarjeta está mala o Ud. no es un miembro de esta CEDE" & _
     '          vbCrLf & "Planta Energética deshabilitada." & _
     '          vbCrLf & "ID Tag: " & txtcodigo1.Text & "." & _
     '          vbCrLf & "Consulte con el administrador del sistema por cualquier duda."
     Call mensaje()
     señalizador.Text = 0
    Finally
    End Try
    'MsgBox("Un docente encontrado")
    'Dim cmd5 As New MySql.Data.MySqlClient.MySqlDataAdapter(SQL5, cn)
    'Dim dt5 As New DataTable
    'cmd5.Fill(dt5)
    'cn.Close()
    'Dim cantidad As Integer
    'cantidad = dt5.Rows.Count
    'Dim cod As String = dt5.Rows(0).Item("codigoRFID")
    'Label4.Text = cod
    's = "Okkkkkk"
    REM If (cod.Text = txtcodigo1.Text) Then
    'If dt5.Rows.Count > 0 Then
  End Sub
```


DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

```
  Public Sub mensaje()
    lblAcciones.Text = "Es docente miembro de esta CEDE de MEGATEC - ZACATECOLUCA?" & vbCrLf & _
                vbCrLf & "Haga lo siguiente en caso de poseer una tarjeta válida y " & _
                vbCrLf & "quiera hacer uso del recurso energético de un Salón de Clase" & vbCrLf & _
                vbCrLf & "* Acerque y deje su tarjeta puesta en el lector de identificación." & vbCrLf & _
                vbCrLf & "Estado Actual del suministro eléctrico:" & _
                vbCrLf & "Planta Energética deshabilitada." & _
                vbCrLf & "ID Tag: " & txtcodigo1.Text & "." & _
                vbCrLf & "Consulte con el administrador del sistema por cualquier duda."
  End Sub
  Private Sub BtnAbrirPuerto_Click(ByVal sender As System.Object, ByVal e As System.EventArgs) Handles BtnAbrirPuerto.Click
    Try
      If BtnAbrirPuerto.Text = "Conectar" Then
        BtnAbrirPuerto.Text = "Desconectar"
        Setup_Puerto_Serie()
      Else
        If SerialPort1.IsOpen Then
          SerialPort1.Close()
        End If
        BtnAbrirPuerto.Text = "Conectar"
      End If
    Catch ex As Exception
```


DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

```
    End Try
  End Sub
  Private Sub BtnActualizar_Click(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles BtnActualizar.Click
    GetSerialPortNames()
  End Sub
  Private Sub BtnNuevaCaptura_Click(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles BtnNuevaCaptura.Click
    Array.Clear(msn, 0, 100000)
    Txtcodigo.Text = ""
    sib = 0
    az = ""
    lblAcciones.Text = "Esperando Tarjeta ID : ..."
  End Sub
  Private Sub UsoAula_Load(ByVal sender As System.Object, ByVal e As System.EventArgs)
Handles MyBase.Load
    Txtcodigo.Text = ""
    GetSerialPortNames()
    CheckForIllegalCrossThreadCalls = False ' DESACTIVA ERROR POR SUBPROCESO
    lblAcciones.Text = "Esperando Tarjeta ID : ..."
  End Sub
  Private Sub SerialPort1_DataReceived(ByVal sender As Object, ByVal e As
System.IO.Ports.SerialDataReceivedEventArgs) Handles SerialPort1.DataReceived
    Try
      az = SerialPort1.ReadExisting
      msn(sib) = az
```


DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

```
    'Do
    Txtcodigo.Text += msn(sib)
    codigoRFID = Mid(Txtcodigo.Text, 1, 12)
    txtcodigo1.Text = codigoRFID
    'Loop Until sib <= 12
    sib = sib + 1
    caracteres = Len(txtcodigo1.Text)
    If caracteres = 12 Then
      guardarUsoAula()
      caracteres = 0
      txtcodigo1.Text = ""
      Txtcodigo.Text = ""
      sib = 0
      Array.Clear(msn, 0, 1000)
      System.Threading.Thread.Sleep(1000)  '1 minuto.
      'System.Threading.Thread.Sleep(300000) '5 minutos
      If (caracteres = 0) Then
        Call mensaje()
      End If
    End If
  Catch ex As Exception
    MsgBox(ex.Message)
  End Try
End Sub
Sub Setup_Puerto_Serie()
```


DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

```
  Try
    With SerialPort1
      If .IsOpen Then
        .Close()
      End If
      .PortName = ComboPorts.Text
      .BaudRate = 9600          '// 19200 baud rate
      .DataBits = 8             '// 8 data bits
      .StopBits = IO.Ports.StopBits.One  '// 1 Stop bit
      .Parity = IO.Ports.Parity.None   '
      .DtrEnable = False
      .Handshake = IO.Ports.Handshake.None
      .ReadBufferSize = 2048
      .WriteBufferSize = 1024
      '.ReceivedBytesThreshold = 1
      .WriteTimeout = 500
      .Encoding = System.Text.Encoding.Default
      .Open()               ' ABRE EL PUERTO SERIE
    End With
  Catch ex As Exception
    MsgBox("Error al abrir el puerto serial: " & ex.Message, MsgBoxStyle.Critical)
  End Try
End Sub
Sub GetSerialPortNames()
  ' muestra COM ports disponibles.
```


DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

```
    Dim l As Integer
    Dim ncom As String
    Try
      ComboPorts.Items.Clear()
      For Each sp As String In My.Computer.Ports.SerialPortNames
        l = sp.Length
        If ((sp(l - 1) >= "0") And (sp(l - 1) <= "9")) Then
          ComboPorts.Items.Add(sp)
        Else
          'hay una letra al final del COM
          ncom = sp.Substring(0, l - 1)
          ComboPorts.Items.Add(ncom)
        End If
      Next
      If ComboPorts.Items.Count >= 1 Then
        ComboPorts.Text = ComboPorts.Items(0)
      Else
        ComboPorts.Text = ""
      End If
    Catch ex As Exception
    End Try
  End Sub
  Private Sub Btnlisto_Click(ByVal sender As System.Object, ByVal e As System.EventArgs)
Handles Btnlisto.Click
    'Me.Hide()
    'Registrodocentes.Show()
```


DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

```
    'MI IDEA ES QUE AL TRATAR DE GUARDAR EN LA BASE DE DATOS SE COMPARE SI LA TAG PUESTA EN EL LECTOR
    'ES DIFERENTE DE OTRA TAG Y SI ES CIERTO QUE GUARDE UN NUEVO REGISTRO POR TAG PUESTA EN EL LECTOR
    Registrodocentes.TxtRFID.Text = Me.txtcodigo1.Text
  End Sub
End Class
```

CODIGO DE LA APLICACIÓN WEB ASP.NET

```
Imports MySql.Data
Imports MySql.Data.MySqlClient
Public Class principal
  Inherits System.Web.UI.Page
  Protected Sub Page_Load(ByVal sender As Object, ByVal e As System.EventArgs) Handles Me.Load
    'SqlDataSource1.DataBind()
    Timer1.Enabled = True
  End Sub
  Protected Sub Timer1_Tick(ByVal sender As Object, ByVal e As EventArgs) Handles Timer1.Tick
    SqlDataSource1.DataBind()
    GridView1.DataBind()
  End Sub
End Class
```


DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

12. GLOSARIO

Microcontroladores	Es un computador construido dentro de un Dado de silicio que se encuentra encapsulado como circuito integrado. Por ello es que se conoce como un circuito integrado programable, capaz de ejecutar las órdenes grabadas en su memoria a través de un código de programa.
Sistemas de **control electrónicos.**	Son la parte del microcontrolador capaz de Soportar el conexionado físico de sensores y actuadores del sistema a gobernar o controlar y todos los recursos complementarios disponibles. Tiene como finalidad exclusiva atender los requerimientos de la tarea a la que se dedica el microcontrolador.
Sistemas de adquisiciones de datos.	Básicamente el proceso consiste en tomar un conjunto de señales físicas, convertirlas en

DOCUMENTO PROPIEDAD DE ITCA-FEPADE. DERECHOS RESERVADOS

Escuela Especializada en Ingeniería

ITCA FEPADE

SANTA TECLA · ZACATECOLUCA · SAN MIGUEL · SANTA ANA · LA UNIÓN

megatec
EDUCACIÓN TÉCNICA, TECNOLÓGICA Y SUPERIOR

MINISTERIO DE EDUCACIÓN
GOBIERNO DE
EL SALVADOR
UNÁMONOS PARA CRECER

Sede Central Santa Tecla
Km. 11 Carretera a Santa Tecla.
Tel. (503) 2132-7400
Fax. (503) 2132-7599

Centro Regional
MEGATEC La Unión
C. Santa María, Col. Belén, atrás del Instituto Nacional de La Unión.
Tel. (503) 2668-4700

Centro Regional
MEGATEC Zacatecoluca
Km. 64 1/2, desvío Hacienda El Nilo, sobre autopista a Zacatecoluca y Usulután. Tel. (503) 2334-0763, (503) 2334-0768
Fax. (503) 2334-0462

Centro Regional San Miguel
Km. 140, Carretera a Santa Rosa de Lima.
Tel. (503) 2669-2292, (503) 2669-2299
Fax. (503) 2669-0961

Centro Regional Santa Ana
Final 10a. Av. Sur, Finca Procavia
Tel. (503) 2440-4348, (503) 2440-2007
Tel. Fax. (503) 2440-3183

Escuela Especializada en Ingeniería
ITCA FEPADE