UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN ELÉCTRICO-MECÁNICA CON MENCIÓN EN GESTIÓN EMPRESARIAL INDUSTRIAL

TEMA:

"Estudio para la elaboración del diseño de un sistema domótico de seguridad para el Laboratorio de Electricidad de la Facultad de Educación Técnica para el Desarrollo"

Previo la obtención del Título de:

INGENIERÍA EN ELÉCTRICO-MECÁNICA

CON MENCIÓN EN GESTIÓN EMPRESARIAL INDUSTRIAL

ELABORADO POR:

CHRISTIAN XAVIER PAREDES FRANCO

DIRECTOR DEL PROYECTO

ING. RAFAEL HIDALGO AGUILAR

GUAYAQUIL – ECUADOR

Febrero 2014

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

CERTIFICACIÓN

Certifico que el presente trabajo fue realizado en su totalidad por el Sr. CHRISTIAN XAVIER PAREDES FRANCO como requerimiento parcial para la obtención del título de INGENIERO EN ELÉCTRICO-MECÁNICA CON MENCIÓN EN GESTIÓN EMPRESARIAL INDUSTRIAL

Guayaquil, Febrero de 2014

_____
Ing. Rafael Hidalgo Aguilar
DIRECTOR

REVISADO POR

_____
Ing. Pedro Tutiven López, Mgs.

_____
Ing. Juan Carlos López Cañarte

_____
Ing. Miguel Heras Sánchez
RESPONSABLE ACADÉMICO

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

INGENIERÍA EN ELÉCTRICO-MECÁNICA CON MENCIÓN EN GESTIÓN EMPRESARIAL INDUSTRIAL

DECLARACIÓN DE RESPONSABILIDAD

YO, CHRISTIAN XAVIER PAREDES FRANCO

DECLARO QUE:

El proyecto de grado denominado "Estudio para la elaboración del diseño de un sistema domótico de seguridad para el Laboratorio de Electricidad de la Facultad de Educación Técnica para el Desarrollo", ha sido desarrollado con base a una investigación exhaustiva, respetando derechos intelectuales de terceros conforme las citas que constan al pie de las páginas correspondientes, cuyas fuentes se incorporan en la bibliografía.

Consecuentemente este trabajo es de mi autoría.

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

Guayaquil, Febrero de 2014

EL AUTOR

_____

CHRISTIAN XAVIER PAREDES FRANCO

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

INGENIERÍA EN ELÉCTRICO-MECÁNICA CON MENCIÓN EN GESTIÓN EMPRESARIAL INDUSTRIAL

AUTORIZACIÓN

Yo, CHRISTIAN XAVIER PAREDES FRANCO

Autorizo a la Universidad Católica de Santiago de Guayaquil, la publicación, en la biblioteca de la institución del proyecto titulado: "Estudio para la elaboración del diseño de un sistema domótico de seguridad para el Laboratorio de Electricidad de la Facultad de Educación Técnica para el Desarrollo", cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y autoría.

Guayaquil, Febrero de 2014

EL AUTOR

_____

CHRISTIAN XAVIER PAREDES FRANCO

DEDICATORIA

A Dios, por darme la vida y la recompensa de culminar con éxito, una carrera profesional.

A mi madre, la Sra. Mónica Isabel Franco Rodríguez, por darme siempre ese soporte emocional en todo el transcurso de mi vida estudiantil y ahora más que nunca en mi etapa universitaria, a ella le dedico este trabajo de graduación.

El autor

CHRISTIAN XAVIER PAREDES FRANCO

AGRADECIMIENTO

Al finalizar un trabajo tan arduo y lleno de dificultades como el desarrollo de una tesis, debo agradecer de manera especial y sincera. A mi madre, la Sra. Mónica Isabel Franco Rodríguez, por su lucha día a día y sacrificio durante toda mi carrera.

También debo agradecer A la Lcda. Rosa Angélica Pérez Vera, por la magnitud de su aporte a lo largo de mi carrera estudiantil, por su incondicionalidad y por ese aliento del día a día para seguir adelante y no desmayar en la culminación de mi carrera. A la Econ. Martha Pacheco, por el apoyo y confianza, que ha permitido poder culminar con éxito, el objetivo de ser un profesional.

A mis profesores de la FET por compartir experiencias, conocimiento respeto y su afecto, a sus autoridades y en especial a mi tutor de tesis Ing. Rafael Hidalgo, por su apreciable gestión de tutoría para finalizar este trabajo de graduación.

El autor

CHRISTIAN XAVIER PAREDES FRANCO

INDICE GENERAL

INDICE DE FIGURAS

RESUMEN

Este trabajo de investigación pretende realizar el diseño de un sistema de seguridad domótico mediante la utilización de sensores con comunicación inalámbrica y tecnología ZigBee lo que permite que sean vistos en la pantalla de un computador por internet en cualquier lugar.

En la primera parte se verá el problema de investigación, la justificación de este trabajo y la hipótesis con la posible solución. Después se analizan las tecnologías comerciales de los elementos a utilizarse en el diseño, esto es los sensores y cámaras, así como también las normas de comunicación y los módulos a utilizarse para la transmisión y recepción en radiofrecuencia.

ABSTRACT

This research aims to develop the design of a home automation security system using sensors with ZigBee wireless communication technology which allows them to be viewed on a computer screen anywhere online.

The research problem will be in the first part, the rationale for this work and the hypothesis with the possible solution. After commercial technologies of the elements used in the design are discussed, namely sensors and cameras, as well as communication standards and modules used for radio frequency transmission and reception.

INTRODUCCIÓN

Actualmente la seguridad es un tema muy relevante en la sociedad, donde se ha perdido el respeto y los valores, deben adoptarse formas de neutralizar estos hechos para dar seguridad a los usuarios.

Cualquier previsión para protección en Ecuador es frágil contra ataques, siendo necesaria una seguridad para impedir pérdidas.

Hay diversas tecnologías y mecanismos comercialmente para protección según los requerimientos individuales que dan seguridad a los locales y con diferentes grados de protección.

Esta tesis se basa en la aplicación de estos sistemas visto desde un punto de vista general para brindar seguridad al laboratorio de electricidad de la Facultad de Educación Técnica para el Desarrollo (FET) de la Universidad Católica de Santiago de Guayaquil (UCSG), usando dispositivos simples y económicos que se pueden conseguir en tiendas locales y supermercados sin disminuir en el proceso el grado de confiabilidad necesaria.

ANTECEDENTES

En el laboratorio de electricidad de la FET se presentan situaciones problemáticas debidas a la infraestructura y organización actual, entre estas se puede mencionar las siguientes:

Ingreso de personas no autorizadas: los estudiantes de la Facultad Técnica o de otras unidades académicas de la UCSG pueden ingresar al laboratorio de electricidad para realizar trabajos de investigación o aplicaciones de los temas tratados en las clases teóricas, simplemente con la autorización del supervisor del mismo y operar los instrumentos y equipos sin ningún control, lo cual puede causar inconvenientes como pérdidas o averías en el hardware y/o software del equipamiento del laboratorio.

Necesidad de controlar la entrada y salida de estudiantes y personal docente y administrativo: en el laboratorio no se lleva un registro de ingreso al mismo, excepto la asistencia de los estudiantes a sus clases mediante el Sistema Integrado Universitario (SIU) realizada por el docente respectivo, pero no hay control sobre el ingreso y salida en otros casos de profesores o personal de mantenimiento y limpieza. Además no se realiza el inventario de los elementos usados en las prácticas realizadas por los alumnos.

Uso del equipamiento del laboratorio de electricidad: esta dependencia cuenta con equipos tales como multímetros, osciloscopios, computadoras, generadores de señal y diferentes módulos de pruebas, los cuales deben ser usados adecuadamente por lo que quienes los utilizan deben tener el conocimiento necesario acerca de su operación para evitar errores y daños de los mismos, en caso de estos producirse no es posible indicar al responsable.

Seguridad contra pérdidas de equipos: el equipamiento instalado en el laboratorio de electricidad tiene un alto precio, y existe la posibilidad de sufrir un acto delictivo que provocaría pérdidas económicas, por lo que es recomendable invertir en la instalación de un sistema de seguridad para el laboratorio.

Acceso por puertas y ventanas: el laboratorio cuenta con ventanas y puertas enrejadas lo que le da un determinado grado de seguridad cuando el mismo está cerrado, pero existe la posibilidad de que hayan copias de las llaves del mismo, lo cual permitiría el ingreso a esta dependencia.

Resumiendo lo indicado, esta investigación trata acerca de las seguridades que es necesario brindar al laboratorio de electricidad de la FET.

DEFINICIÓN DEL PROBLEMA

El laboratorio de electricidad de la FET posee un equipamiento costoso que puede ser averiado por errores en su operación o robado, ya que durante su horario de atención a docentes y estudiantes no hay un control en el interior de esta dependencia pues la UCSG solo cuenta con guardias de seguridad en los exteriores pero no dentro del laboratorio.

OBJETIVO GENERAL

Realizar un diseño de un sistema domótico de seguridad con comunicación inalámbrica con una computadora que permita la evaluación del sistema y la observación de las novedades que se presenten en el interior del laboratorio de electricidad de la FET de la UCSG.

OBJETIVOS ESPECIFICOS

- Realizar un estudio de los fundamentos tecnológicos que permitan desarrollar este proyecto.
- Determinar los elementos de control necesarios para un sistema domótico de seguridad.
- Establecer la ubicación adecuada para los sensores y cámaras que conformen el sistema de seguridad.
- Elaborar el diseño del sistema domótico de seguridad con tecnología inalámbrica.

JUSTIFICACIÓN

Un sistema domótico de seguridad como el que se plantea diseñar en este proyecto de investigación se basa en la utilización de sensores que permitan detectar irregularidades en el interior del laboratorio de electricidad de la FET generando la alarma ante la eventualidad de que se produzca algún hecho de esta naturaleza.

El diseño de este sistema también incluirá una alarma al producirse un incendio mediante un detector de humo lo cual permitirá que el mismo sea apagado a tiempo.

HIPÓTESIS

La presentación de un diseño que permita la implementación de un sistema domótico de seguridad para el laboratorio de electricidad de la Facultad de Educación Técnica para el Desarrollo de la Universidad Católica de Santiago de Guayaquil, brindará protección a los costosos equipos instalados en él ya que actualmente no posee ningún tipo de seguridad ante irregularidades que puedan suscitarse en su interior durante las horas de atención a docentes y estudiantes.

CAPITULO I FUNDAMENTACIÓN TEÓRICA

En un ambiente donde se trabaja con electricidad es indispensable tener en consideración los riesgos que implica operar elementos que conducen corriente eléctrica, y en consecuencia la errónea utilización de esos equipos puede causar accidentes que pueden ser graves y en determinada circunstancias mortales.

Los docentes, estudiantes y en general las personas que realicen algún trabajo en el laboratorio de electricidad deben considerar que se corre el riesgo de que se produzca un incendio a causa de la electricidad en la eventualidad de que se produzca alguna de las siguientes circunstancias:

- Exceso de carga en conductores generando sobrecalentamiento del cableado y dispositivos.
- Calentamiento de los equipos del laboratorio por fallas de los dispositivos de control.
- Fallas en la aislación de los conductores.
- La inflamación de materiales combustibles ubicados junto a aparatos eléctricos o a causa de chispas, arcos fotovoltaicos, temperatura, etc.

Comercialmente pueden encontrarse sistemas inalámbricos de seguridad basados en sensores de alto costo, dificultando su adquisición y utilización especialmente en sitios como los laboratorios donde no se generan utilidades económicas.

En el laboratorio de la FET, existen aparatos de alto valor, como computadoras, osciloscopios, analizadores de espectro, multímetros, etc., que podrían dañarse o ser robados, considerando que es un local permanentemente con presencia de estudiantes y docentes. Adicionalmente, esta dependencia únicamente tiene seguridades físicas, es decir rejas en las puertas y ventanas.

La UCSG consciente de la inseguridad latente en el campus, ubica guardias en diferentes áreas, pero no suficientes para ubicarlos cerca de los laboratorios y más bien se dedican a los ingresos y parqueaderos, esto causa que no se controle la salida de algún bien de la universidad en los carros que transitan por el área.

Domótica es una agrupación de métodos para mecanizar un inmueble proveyendo utilidades de control de energía, protección, comodidad e intercambio de información, permitiendo su integración con redes internas y externas, mediante cables o inalámbricas, con gestión desde dentro y fuera del lugar. Básicamente es la unificación de la técnica con el esquema inteligente de un local.

Para la seguridad esta técnica brinda a los usuarios mejor acceso a sus aparatos tecnológicos y una mayor protección contra los peligros dados al instalar sistemas automáticos para incendios, ingresos, etc., y en general métodos para mejorar la comodidad a los usuarios. Hoy en día, los componentes automáticos son más independientes gracias al desarrollo tecnológico con lo que se alcanza más eficacia en los procedimientos dirigidos a satisfacer a los usuarios.

Continuando con el mismo tema, es claro que la seguridad es un factor muy importante que debe considerarse para la protección del usuario y sus bienes a causa de los riesgos que pueden ocurrir, especialmente en aquellos ambientes donde se realizan trabajos que presentan peligro en la operación del equipamiento existente en esas dependencias, por las razones expuestas anteriormente, bajo esta perspectiva, aplicando la domótica al ámbito de la seguridad se encontrará que comercialmente existen variedad de sistemas para brindar protección a las personas y también al equipamiento en el caso del laboratorio de electricidad motivo de este trabajo de investigación. Estos sistemas utilizan señales recibidas mediante sensores y generan una respuesta por medio de actuadores, por ejemplo pueden producir alarmas, mensajes de texto que pueden enviarse al celular del encargado del laboratorio, incluso podría generarse una señal que corte el suministro de energía eléctrica en caso de ser necesario por la clase de amenaza presentada.

1.1 Técnicas de seguridad

La implementación de una técnica domótica para proteger una dependencia se basa en la utilización de sensores y localizadores para descubrir un ingreso no autorizado, lo cual podría convertirse en una sustracción, de esta manera es posible comunicar el hecho a tiempo y neutralizarlo. Esta técnica también puede emitir alarmas en caso de fuego o humo evitando así mayores consecuencias al habérselo detectado a tiempo.

Los dispositivos para este tipo de instalación son variados, siendo los más utilizados los sensores de actividad y las cámaras.

Para determinar los mejores elementos a utilizarse, hay que averiguar y evaluar las diferentes técnicas y propiedades de los dispositivos y elegir los más convenientes para este proyecto, considerando precios, capacidades y desempeño, por ejemplo en lo que respecta a las cámaras, su resolución, accionamiento al detectar actividad, etc.

Es importante también la determinación del sitio adecuado para la ubicación de los elementos de protección a instalarse en el laboratorio de electricidad considerando parámetros tales como visibilidad, proximidad a fuentes potenciales de fuego, accesos, etc.

Para la transferencia de información también deben examinarse aquellas técnicas para enlazar los dispositivos con el computador de control, el cual presenta los datos detectados y genera las alertas correspondientes. La evaluación del sistema de comunicación debe considerar la facilidad, aptitud y desempeño de acuerdo a las necesidades de la dependencia, el protocolo adecuado, velocidades de propagación de datos, alcance de la señal y estructura cableada o inalámbrica.

Los datos generados al activarse las alertas del laboratorio deben ser utilizados y direccionados adecuadamente, por ejemplo en caso de robo a la policía, si es fuego a los bomberos y a los guardias del campus en todos los casos, estas técnicas también pueden

incluir transmisión directa al supervisor de esta dependencia de las actividades que se produzcan en la misma y su grabación correspondiente.

A continuación se presentarán las unidades que se necesitan para implementar un sistema de seguridad para el laboratorio de electricidad de la FET y las opciones que es posible encontrar comercialmente para su utilización.

1.1.1 Comunicaciones

Antes de establecer el equipamiento que se utilizarán para este bloque del sistema es necesario conocer acerca de los protocolos de comunicación o de red aplicables, es decir las normas determinadas para la transmisión de información en la red LAN (*Local Area Network*, Red de Área Local), del laboratorio. Entre las más populares se puede mencionar las siguientes:

ZigBee: es un modelo de transmisión inalámbrica creado por la *ZigBee Alliance*, y consiste en un grupo de recursos para su aplicación por cualquier fabricante, se fundamenta en el estándar IEEE 802.15.4 (*Institute of Electrical and Electronics Engineers*) para redes WPAN (*Wireless Personal Área Network*) para utilización en transmisiones seguras con bajas velocidades y larga vida útil de las baterías empleadas en los dispositivos. Por sus características es apropiado para usos domóticos donde evita la multiplicación de sensores/actuadores individuales. Es un modelo de bajo precio para redes inalámbricas para transmitir paquetes cortos de datos, reducido consumo, infalible y fiable.

Este estándar se utiliza en la banda (2.4Ghz) ISM (*Industrial, Scientific and Medical Bands*) en aplicaciones en la industria, ciencia y medicina, también como ya se anotó en sistemas de costo reducido por su implementación con pocos dispositivos para transmisiones de datos a baja velocidad, brindando vida útil extendida de las baterías. Generalmente se emplean en redes conectadas en malla.

En la figura 1.1 se muestra un esquema de las aplicaciones del estándar *Zigbee*.

Figura 1.1 Aplicaciones del estándar *Zigbee*

Fuente: www.slideshare.net

Bluetooth, es una especificación empleada en redes WPAN para transmitir voz y datos entre dispositivos a través de una conexión RF (Radio Frecuencia) en la banda ISM, facilitando las conexiones entre dispositivos inalámbricos de consumo reducido y un alcance aproximado de 10 metros, de esta manera se evitan cableados y conectores entre equipos, así es posible implementar pequeñas redes inalámbricas y proporcionar sincronización de datos entre equipos personales, tales como PDA (*Personal Digital Assistant*), celulares, *laptops*, impresoras o cámaras digitales. Un ejemplo de conexión de dispositivos mediante *Bluetooh* se presenta en la figura 1.2

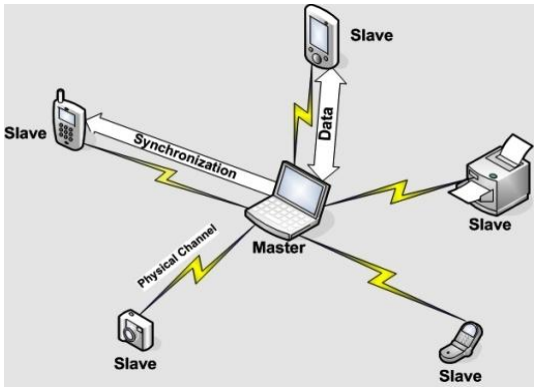


Figura 1.2 Conexión de dispositivos mediante *Bluetooh*

Fuente: profesores.elo.utfsm.cl

Wi-Fi, es una conocida técnica para intercomunicar datos de un dispositivo electrónico o enlazarse a *internet* inalámbricamente a través de ondas de radio. Esta técnica inalámbrica es empleada en redes LAN, celulares, PDA, entre otros que de esta manera están capacitados para enlazarse a *internet* mientras están en el alcance del AP (*Access Point*), o pueden utilizarse en enlaces punto a punto. La figura 1.3 representa un esquema de las conexiones Wi-Fi.

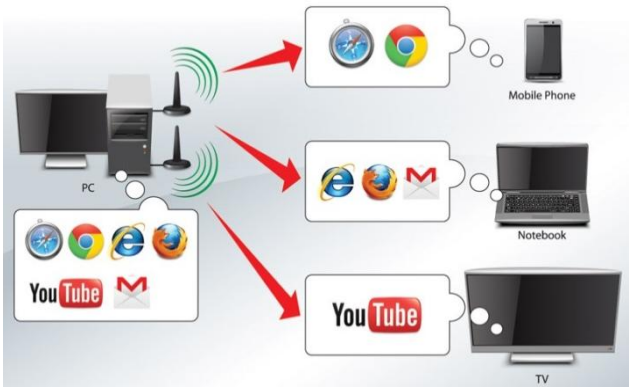


Figura 1.3 Enlaces Wi-Fi

Fuente: www.gigabyte.com.mx

Especificación *Wireless* USB (W-USBE), se refiere a una ampliación inalámbrica del modelo USB (*Universal Serial Bus*) para incrementar los recursos de conectividad. Utiliza señales RF con un extenso ancho de banda en frecuencias de 3.1 y 10,6 GHz, armonizando la sencillez del USB con la variabilidad de las redes inalámbricas, pudiendo enlazarse más de 100 terminales a un host con velocidades de 480 Mbs y alcances de 3 metros o 110 Mbs a 10 metros. Entre sus aplicaciones se tiene impresoras, *scaners*, etc.

En la figura 1.4 puede verse la utilización de dispositivos *Wireless* USB para la interconexión de equipos electrónicos como computadoras, discos duros, cámaras digitales, teclados y *mouses*.

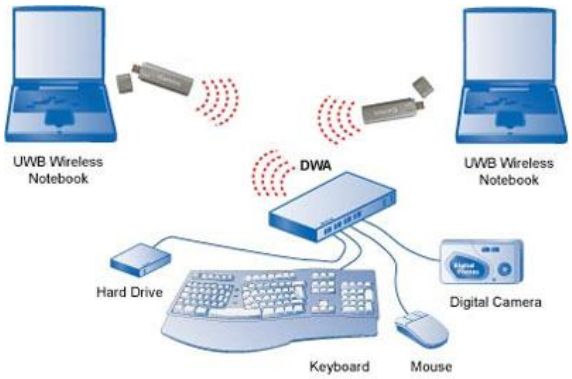


Figura 1.4 Utilización del *Wireless* USB

Fuente: www.everythingusb.com

X10, es un protocolo de comunicaciones utilizado para controlar remotamente aparatos eléctricos, emplea la red eléctrica existente en la propagación de señales de control entre equipos domóticos. En el mercado se encuentran dispositivos X10 para empleo particular y con alcances de 250 metros cuadrados, tiene restricciones de ancho de banda por lo que puede controlar hasta 256 equipos. El protocolo X-10 extendido permite transmisiones bidireccionales y confirmación del acertado envío de tramas de datos con bits de direccionamiento y gestión. Permite el encendido y apagado de equipos eléctricos y en iluminación puede controlar la potencia de la misma. Emite andanadas de impulsos RF a una frecuencia de 120Khz empleando las líneas eléctricas. Se presentan en aplicaciones tales como controladores por *keypad* y *keychain*, que controlan hasta 4 módulos X10, equipamiento. La figura 1.5 muestra un esquema de las aplicaciones domóticas de dispositivos X10.

1.1.2 Sensores y localizadores

Ahora corresponde analizar los mecanismos de protección que se pueden encontrar comercialmente a fin de determinar el equipamiento adecuado para el laboratorio

Videocámaras: Comercialmente se puede adquirir variedad de estos aparatos para los requerimientos del caso del laboratorio.

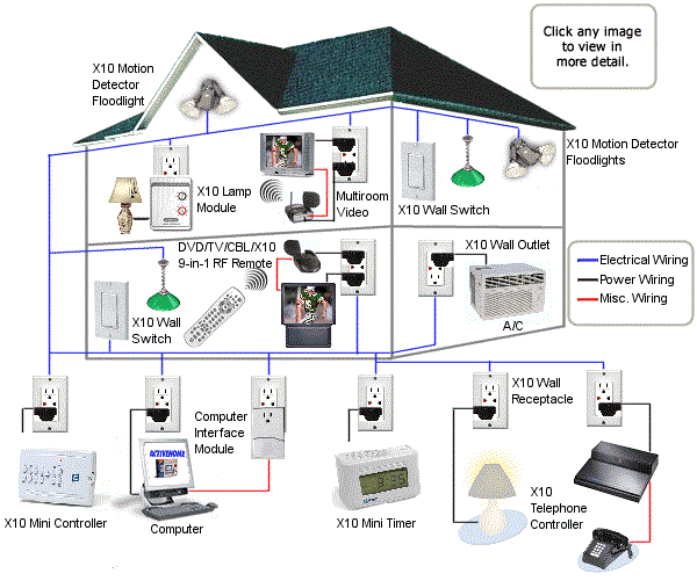


Figura 1.5 Automatización de un hogar con X10

Fuente: www.x10-store.com

Este equipo debe adquirirse de acuerdo al entorno en que va a operar y desempeñarse de acuerdo a las necesidades del mismo. Entre estas propiedades puede mencionarse:

Discreción: equipos modelo Domo

Visibilidad en la oscuridad: equipadas con tecnología infrarroja

Encubiertas: pequeñas y escondidas

Uso interno y externo: armazón resistente

Acercamiento: equipadas con *zoom* adecuado

Transmisión/recepción inalámbrica

Posibilidad de acceso por *internet*: equipadas con protocolo IP (*Internet Protocol*)

Equipadas con sensores de actividad

Audio: en caso de ser necesario

Generación de alertas: en caso de ser necesario

Conectables en circuito cerrado

Sensores de fuego o humo: determina estos peligros en el local y produce una alerta audible, también es posible incluir avisos al Servicio Integrado de Seguridad Ecu911 el cual informa al cuerpo de bomberos, a algún número telefónico establecido o por internet.

Para cubrir las características indicadas, pueden utilizarse detectores ópticos o iónicos. Los primeros son capaces de descubrir humo y estar equipados con tecnología infrarroja y transmitir y recibir información, en cambio los segundos son más baratos y son capaces de determinar corpúsculos muy pequeños que no intervienen en la luminosidad. Estos equipos funcionan con electricidad o a baterías, en este caso se agotan y deja de operar por lo que hay que inspeccionarlas dos veces al año.

Detectores de actividad: son dispositivos que sienten la actividad física en un entorno y generan una señal con capacidad de activar mecanismos de seguridad o iluminación o alertas audibles. Existen de tecnología infrarroja y de microondas. Los primeros pueden ser activos si poseen una fuente de iluminación y un detector infrarrojo que capta el cambio de la señal recibida cuando un cuerpo físico obstaculiza el rayo infrarrojo; o pasivos si captan el calor de la entidad extraña moviéndose frente al detector; en ambos su limitación es el alcance.

Los detectores de actividad que emplean microondas lo hacen con tecnología de radar y tienen un mayor alcance, generan constantemente una señal de microondas y contrastan la frecuencia enviada con la recibida, si hay un movimiento se produce un cambio determinándose el ingreso no autorizado.

Sensores para puertas y ventanas: estos pequeños elementos captan la apertura de una ventana o puerta provocando una alerta. Está compuesta de un elemento instalado en la puerta o ventana a proteger y la otra en el marco de la misma, estas pueden operar mediante contactos magnéticos o con tecnología infrarroja.

Alertas: incluyen sirenas, timbres u otros elementos que notifican mediante una señal audible de alto volumen si se produce un ingreso no autorizado, humo, fuego o por la señal de algún mecanismo conectado al sistema de alerta. Pueden estar enlazados a una central que se encarga de las comunicaciones correspondientes por la generación de la alerta u operar sin enlace, es muy básico simplemente genera la alerta audible sin comunicarla.

Supervisión de ingresos: su función es autorizar o no el ingreso a una determinada área que puede corresponder a procedimientos físicos o lógicos. En este trabajo de investigación se trata de la supervisión de individuos al laboratorio de electricidad de la FET, lo cual puede hacerse mediante presentación del carnet universitario con cinta magnética o código de barras, que al pasar por el lector enlazado a una computadora de control que determina si consta en la nómina de ingresos autorizados, accediendo o no la entrada y procediendo a la apertura o bloqueo de la puerta. Otro tipo de control es el empleo de tarjetas con un circuito LC que al acercarse a una descifradora produce un campo electromagnético que carga al condensador y generando un código de ingreso.

Actualmente también están disponibles las tarjetas inteligentes con o sin conexión, las cuales poseen un microprocesador y memoria para guardar la identificación y además sistemas operativos para ejecutar procesos diversos. En otra categoría, puede instalarse en el ingreso mecanismos con código de identificación de 4 a 8 números que deben ser digitados por el personal al ingresar. De la misma categoría son los controles biométricos que funcionan en base a las huellas dactilares del personal, determinando si pueden ingresar o no. Actualmente este modo de supervisión se emplea en la UCSG para controlar el horario de asistencia y salida del personal administrativo.

1.1.3 Comunicación visual con el personal

Se realiza mediante una interfaz mediante un servidor, el cual brinda servicios usuales con archivos para guardar datos, ingresar a ellos y otras utilidades para el usuario. De esta

manera el personal no debe preocuparse por la forma de almacenamiento de la información, incluso por la organización de las bases de datos no se tiene información redundante, siendo importante la protección de los datos guardados en esa base incluyendo la creación de copias de respaldo y evitar que personal no autorizado acceda a ella.

Los procesos organizados de esta manera simplifican la gestión de grandes cantidades de datos gracias a la alta velocidad del computador, garantizando la autonomía del proceso de los datos y su protección ante personas sin autorización, se evita la repetición de los datos al verificárselos al momento de su ingreso.

1.2 Organización y estrategia de protección

De lo expresado hasta ahora se concluye la relevancia de controlar la entrada, salida y hechos ilícitos en el laboratorio que se debe resguardar, con este antecedente se deben establecer las medidas a adoptarse, las propiedades de los dispositivos que se elegirán para alcanzar este objetivo. Para empezar se considerará el sistema a implementarse como un diagrama de bloques, siendo el primero el que corresponde a los detectores para el ingreso en la puerta del laboratorio que deben producir una señal inalámbrica hacia la computadora de control. En razón de que las ventanas del laboratorio de electricidad de la FET están protegidas con rejas que impiden el ingreso por esa vía, se ha determinado que no es necesario instalar sensores en las mismas.

El siguiente bloque corresponde a los detectores de actividad no autorizada en el interior del laboratorio, estos dispositivos al descubrir un movimiento transmiten una señal a la computadora de control y aquí se la evaluará y se adoptarán las acciones que correspondan.

El tercer bloque corresponde al sistema de video que debe situarse para permitir un enfoque total del laboratorio, mediante una videocámara encendida y apagada por el supervisor de la dependencia, pero con mecanismos de activación ante las señales de los

detectores de actividad iniciándose la grabación en la memoria del computador únicamente cuando una anomalía se produce.

De acuerdo a los factores de protección a considerarse, es necesario un bloque de alerta ante la presencia de humo o fuego en el laboratorio, el detector instalado debidamente transmite la señal de alerta a la computadora de control y al mecanismo audible de alarma.

Todos los dispositivos indicados en los bloques descritos se enlazarán inalámbricamente con la computadora de control para obviar el cableado adicional en el laboratorio y son comercialmente disponibles.

1.3 Resumen del trabajo

Por las razones expuestas en este trabajo se establece que debe ejecutarse un procedimiento domótico de protección de acuerdo a las necesidades del laboratorio, las cuales se especificaron en el numeral anterior, descubrimiento de entrada o salida no autorizada, almacenamiento de señales de la videocámara activada por los detectores de actividad implementados.

Además, se mencionó la necesidad de contar con detectores de humo y fuego para que se adopten de inmediato las acciones que correspondan.

Una vez definidos los elementos que intervienen en este diseño, se establecerán los detectores a instalarse y el sitio en que se lo hará, el protocolo de comunicación a utilizarse para el envío de datos debe satisfacer los parámetros de protección que se requiere, el alcance de las señales, resolución del video, tasas de datos, precios y disponibilidad comercial de los equipos.

1.4 Modelo de investigación

En primer lugar se determinó que para este trabajo de investigación se empleará un modelo mixto que permite la integración de los enfoques cualitativo y cuantitativo, los cuales se combinarán en el proceso de investigación. Esto implica que se aplicarán los esquemas de pensamiento inductivo y deductivo.

Se aplicó la técnica observación para determinar los datos y aspectos necesarios para levantar el diagnóstico inicial del entorno a investigar, esto es el laboratorio de electricidad de la FET. Es decir que se fundamentó en una observación sistemática para establecer la situación actual de esta dependencia, es decir un método descriptivo porque se procedió a describir las partes que conforman este entorno.

Se empleó una técnica cualitativa para analizar los datos recopilados y luego se interpretó los resultados de una manera cualitativa. Se aplicó el método inductivo para deducir y establecer conclusiones de las observaciones realizadas y los problemas de seguridad determinados.

CAPITULO II ELABORACIÓN DE LA PRIMERA ETAPA DEL PROYECTO

Este trabajo de investigación se ha considerado importante porque el laboratorio de electricidad de la FET posee elementos caros y sin ningún dispositivo de protección, razón por la cual se presenta este proyecto domótico con elementos disponibles comercialmente y empleando un estándar de comunicación libre, para evitar peligros y haciendo de esta dependencia un lugar seguro gracias a la gestión de protección que se realice.

La protección actual del laboratorio cuenta únicamente con enrejados en la puerta y en las ventanas y ninguna seguridad ante la incorrecta utilización de los aparatos que podrían provocar daños, siendo imposible saber quiénes son los causantes, evidenciando la necesidad de un proyecto que ofrezca remedios al respecto, el mismo que contará con videocámaras, detectores de actividad y de apertura de la entrada, con un sistema de gestión adecuado para ofrecer seguridad a esta dependencia.

Como ya se indicó anteriormente se realizará escogerán los aparatos, su localización, se determinará el estándar de comunicación y la interface de usuario, factores necesarios para brindar la protección requerida.

Para escoger los aparatos que se emplearán se considerará su disponibilidad comercial, precios y su desempeño ante las necesidades del proyecto: alcance, resolución, etc. Determinar la localización correcta de los equipos a instalarse impide errores y permite el alcance suficiente de los detectores.

En el capítulo uno se analizó los principales protocolos existentes, de esta evaluación se ha determinado utilizar *Zigbee* para comunicaciones entre los elementos del sistema y la computadora de control, por precio y ahorro energético.

Este trabajo pretende presentar un proyecto para brindar protección al laboratorio de electricidad de la FET mediante detectores y videocámaras disponibles comercialmente a

bajo precio enlazados con tecnología inalámbrica y un estándar en la banda de utilización libre y con una computadora de control para examinar y evaluar las señales que se produzcan.

2.1 Pasos a seguir en la elaboración del proyecto

En primer lugar deben escogerse los aparatos necesarios para el proyecto considerando su disponibilidad en el mercado, sus precios y su desempeño ante los requerimientos establecidos.

A continuación se determinarán las ubicaciones adecuadas de los aparatos a instalarse a fin de dar cobertura en cada punto del laboratorio. El siguiente paso consiste en proyectar la red inalámbrica para el laboratorio, con el estándar correcto para el alcance que se requiere, tasas de datos y apropiadas para instalarse en los emisores y receptores.

Recomendar la disminución de la resolución de la videocámara para mejorar su eficacia y simplificar la grabación de los datos en la memoria. También es necesario poder observar en la computadora las variaciones generadas por los detectores en ventanas emergentes (*pop-up*) con la programación adecuada.

La gestión y administración del laboratorio incluye la anotación de ingresos y salidas, asistencia de los docentes y estudiantes, supervisión en prácticas individuales y de errores en los aparatos y determinación de comprometidos.

2.2 Elaboración del proyecto

Ya se indicó que el proyecto está constituido por bloques, cada uno con sus propiedades. Así, en un primer paso se configurarán los detectores, esto implica aplicar cambios de potencial en los circuitos de esos dispositivos, por las variaciones que se producen en las captaciones del detector, esto puede realizarse con el potencial de la alerta audible del

aparato, con un diodo LED (*Light Emitting Diode*) o un circuito integrado, el cambio de voltaje constituye un código binario de ceros y unos mediante dispositivos electrónicos, esta es la entrada digital al siguiente bloque.

En este segundo bloque se transmite y recibe datos inalámbricamente mediante reglas de comunicación RF, *Xbee*, pues como ya se indicó se empleará el estándar *Zigbee* por su capacidad y beneficios.

En el siguiente bloque se proyectará la forma de observación del usuario, esto es recibir los datos en el receptor inalámbrico a través de un puerto del procesador y mediante un medio gráfico elaborar un software para producir las ventanas de alarma cuando se recibe una señal de algún detector.

A continuación, en la figura 2.1 se muestra el esquema general de la solución plantea para brindar seguridad al Laboratorio de Electricidad de la Facultad de Educación Técnica para el Desarrollo de la Universidad católica de Santiago de Guayaquil.

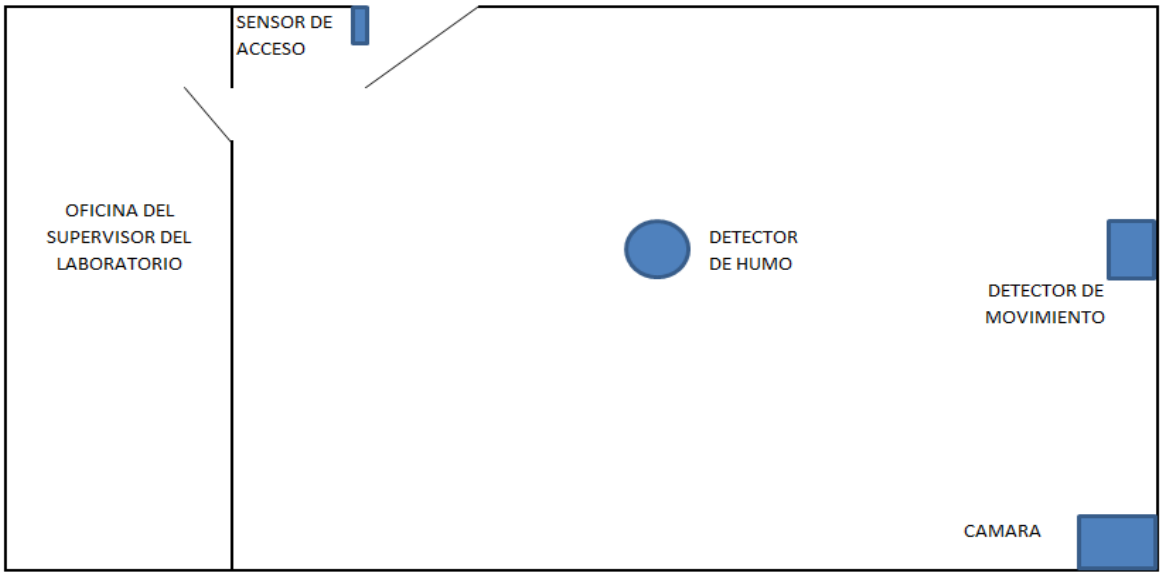


Figura 2.1 Solución integral propuesta

Fuente: Autor

2.3 Configuración de los detectores

En primer lugar se analizarán las diversas tecnologías utilizadas en los dispositivos detectores.

Circuito CMOS (*Complementary Metal-Oxide-Semiconductor*): en estos la actividad lógica se establece de manera redundante con dos circuitos: uno con transistores pMOS (P-*type Metal-Oxide-Semiconductor*) y el segundo con dispositivos Nmos (P-*type Metal-Oxide-Semiconductor*). El primero se usa para enviar el dígito uno, y el segundo el número cero. Son dispositivos de reducido empleo de energía, resistente al ruido, fácil de configurar, precio reducido, extenso rango de voltajes de entrada. En la figura 2.2 se presenta un ejemplo de esta aplicación con un inversor.

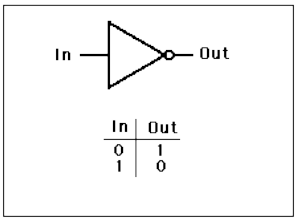


Figura 2.2 Símbolo del circuito inversor y tabla de verdad

Fuente: hyperphysics.phy-astr.gsu.edu

Circuito NOT (Inversor o Negador): es un circuito lógico que genera un uno si la entrada es cero y viceversa. Se emplea para convertir una subida en una bajada.

Zener: es un diodo hecho para trabajar en el área de quiebre. Es muy usado en reguladores de voltaje generando salidas casi constantes sin importar que hayan altos cambios del voltaje de la red, impedancia de carga o temperatura. En la figura 2.3 puede observarse el símbolo de un diodo zener y su estructura de materiales semiconductores.

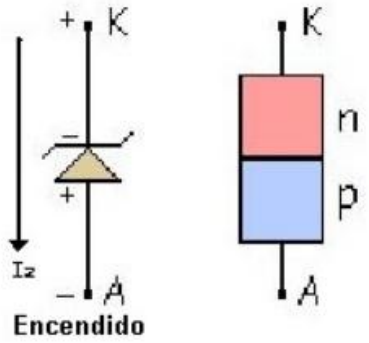


Figura 2.3 Símbolo de un diodo zener y su estructura

Fuente: http://www.slideshare.net

Transistor: puede emplearse como conmutador si se lo hace operar en la región de saturación mediante la manipulación de la corriente de base, utilizando una resistencia de colector diez veces mayor que la de base. Se puede ver en la figura 3.4 los símbolos y estructuras de transistores pnp y npn.

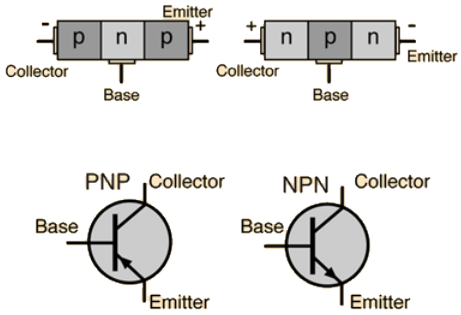


Figura 2.4: Símbolos y estructuras de transistores pnp y npn.

Fuente: hyperphysics.phy-astr.gsu.edu

2.3.1 Configuración del detector de actividad

Ya se indicó anteriormente que la localización del detector de actividad debe permitir descubrir la actividad de alguien en el laboratorio y debe tener una alerta que significará

la transmisión de los datos de activación con un circuito de preparación y el transmisor inalámbrico.

En el caso específico de este proyecto se ha revisado las características técnicas ofrecidas por algunos fabricantes y considerando además su accesibilidad en el mercado local tanto para su adquisición como para los repuestos en caso de mantenimiento o fallas, bajo este concepto se ha escogido un detector de movimiento marca Honeywell, modelo 5897-35, que corresponde a un detector de movimiento dual TEC, cuyas propiedades técnicas son las siguientes:

- Detector inalámbrico de movimiento dual
- Cobertura 11m x 9m
- Compensación de temperatura
- Microondas ajustables
- Inmunidad a mascotas de 22 Kg.
- Lentes opcionales incluidos
    - Protección de 11x3 metros
    - Lente inmune a mascotas de 11x9 metros
- Temperatura de operación 10 a 50 grados.
- Batería de litio de 3 voltios.
- Dimensiones 12.7cm alto x 7.3 cm ancho x 5.9 cm profundidad.

Para esta elección también se consideró que Honeywell es en la actualidad una de las empresas líderes en la fabricación de sistemas electrónicos de seguridad en el mundo. Ofrece al mercado una amplia gama de dispositivos con diversas capacidades y servicios de seguridad para residencias, oficinas e industrias. Además, esta empresa cuenta con un equipo de técnicos especializados y con amplia experiencia que se dedican a brindar a sus clientes el soporte técnico necesario, este personal ofrece además asesoría tecnológica, sugerencias para la elección de los productos requeridos, compatibilidad y colaboración en la solución de inconvenientes que se presenten en los dispositivos de su marca.

En la figura 2.5 se muestra el detector de movimiento marca Honeywell modelo 5897-35, cuyas características ya se describieron.

Figura 2.5: Detector de movimiento marca Honeywell modelo 5897-35.
Fuente: http://www.security.honeywell.com/clar/esp/documents/L_SRCEBKSP_D.pdf

En la figura 2.6 se muestra el patrón de cobertura del detector de movimiento marca Honeywell modelo 5897-35.

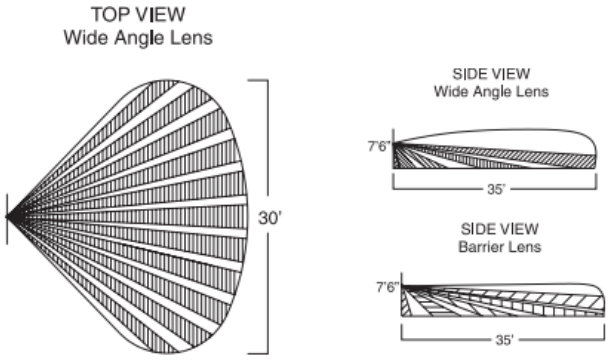


Figura 2.6: Patrón de cobertura del detector de movimiento Honeywell modelo 5897-35.
Fuente: http://www.security.honeywell.com/clar/esp/documents/L_SRCEBKSP_D.pdf

2.3.2 Configuración del detector de humo

En el caso del detector de humo, éste debe localizarse muy cerca del área con mayor probabilidad de que se produzca una anomalía. Para el laboratorio de electricidad de la FET se ha determinado que su ubicación debe ser en el centro del local con lo cual se considera que se tendrá una cobertura total del mismo. Se incluye una alerta que genera una señal de activación a través de un módulo de preparación y el de transferencia inalámbrica.

Para el caso específico de este proyecto de seguridad se ha determinado entre las diferentes opciones disponibles en el mercado un detector de humo marca Honeywell. Las ventajas tecnológicas que posee esta empresa ya fueron descritas en el numeral anterior y como ya se indicó éstas apoyan la elección realizada. Se ha elegido el detector fotoeléctrico de humo modelo 5806W3, el cual presenta las siguientes características técnicas:

- Permite la confirmación de incendios para reducir las falsas alarmas de acuerdo a los estándares ANSI/SIA CP-01 (*American National Standards Institute/ Security Industry Association Control Panel-01*)
- Remite señales de prevención, protección, mantenimiento y situación de la batería al destinatario del procedimiento.
- Cuenta con diodos LED de doble posición con colores verde y rojo
- Sensor de bajo perfil
- Temperatura de operación de 0 a 37.8 grados
- UL (*Underwriters Laboratories*) 268: para instalación comercial y residencial
- Incluye batería de litio de 3 voltios
- Dimensiones: diámetro de 13.4 cm

En la figura 2.7 se puede observar el detector fotoeléctrico de humo modelo 5806W3 de la marca Honeywell, cuyas características técnicas se han descrito.

Figura 2.7: Detector fotoeléctrico de humo modelo 5806W3 de la marca Honeywell
Fuente: http://www.security.honeywell.com/clar/esp/documents/L_SRCEBKSP_D.pdf

2.3.3 Configuración del sensor de apertura de la puerta

Como ya se indicó anteriormente, en el laboratorio solo existe una puerta de madera protegida por otra enrejada, las ventanas son fijas y poseen rejas, por lo indicado solo se ha considerado implementar un sensor de apertura en la puerta de acceso a esta dependencia.

Para el proyecto que se está diseñando, se ha determinado la utilización de una cerradura electromagnética marca Anson de 600 libras, tomando en cuenta igual que en los casos de los dispositivos ya descritos, su disponibilidad en el mercado local.

Este dispositivo es distribuido por la empresa ACECONTROL, especializada en control de accesos peatonales y vehiculares. Emplea y distribuye las mejores marcas de automatismos y sistemas de control.

Las características técnicas del este dispositivo son las siguientes:

- Energía de absorción 600 libras

- Altamente duradera, sin abrasión mecánica.
- Led indicador de estado: rojo para abierto, verde para cerrado.
- Alimentación 12V DC (*Direct Current*).
- La corriente de iniciación 850mA; La corriente de trabajo es 450mA.
- Áreas de aplicación: Con sistemas del control de acceso, control de la entrada-salida, sistemas de vigilancia de la seguridad.
- Para usar en puertas de madera, aluminio, vidrio, metal y en puertas de seguridad

En la figura 2.7 se puede observar la cerradura electromagnética marca Anson de 600 libras.

Figura 2.8: Cerradura electromagnética marca Anson de 600 libras.
Fuente: http://www.acecontrol.com.ec/

2.3.4 Configuración de la videocámara

Continuando con la elección de los dispositivos adecuados para el diseño del sistema de seguridad para el laboratorio de electricidad de la FET, corresponde ahora a la cámara de vigilancia. Para elegir este dispositivo adecuadamente se han realizado las mismas consideraciones que para los otros dispositivos de seguridad que ya se han determinado hasta el momento, es decir sus características técnicas y su disponibilidad en el mercado local.

Bajo estas consideraciones, se ha determinado para el diseño de este proyecto la utilización de una videocámara con protocolo IP modelo cubo y diseño compacto para uso interno, con resolución para día/noche y tecnología inalámbrica. De acuerdo a estas características y entre algunas alternativas revisadas, se estableció emplear la marca VIVOTEK, una *cube network camera* IP8131W, la cual es de tamaño compacto y cumple las especificaciones 802.11 WLAN (*Wireless Local Area Network*).

Ésta es una cámara IP, compacta tipo cubo, que cuenta con WiFi y diseñada para supervisión de interiores. Se puede utilizar en oficinas, comercios o residencias. Posee un micrófono integrado que aumenta el grado de seguridad al grabar los ruidos con un alcance de 5 m. Este equipo cuenta con diodos LEDs infrarrojos para alta resolución en medios oscuros. Éstaa cámara emplea la norma H.264 para compresión, emplea WiFi con estándar 802.11 b/g/n, sencillo de instalar y trae el software para grabar ST7501 que permite 32 canales, la marca VIVOTEK también ofrece servicios para teléfonos celulares inteligentes *iViewer*.

Para el modelo elegido de ste dispositivo, sus propiedades más importantes son las siguientes:

- Detector CMOS 1-Megapixel
- Diseño cerrado
- Compresión en tiempo real H.264 y MJPEG (*Motion Joint Photographic Experts Group*) *Dual Codec*
- 30 fps @ 1280x800 pixels
- Sonido en dos direcciones
- Filtro de corte IR (*Infrared*) intercambiable para operación día/noche
- Iluminación infrarroja incorporada para una distancia de 6 m.
- Terminal MicroSD/SDHC (*Micro Secure Digital /Secure Digital High Capacity*) para acumulación interior

- Opera con WLAN 802.11b/g/n
- Disposición Wifi salvaguardada WPS (*Wi-Fi Protected Setup*) para un enlace sencillo y seguro

De acuerdo a lo indicado, esta cámara IP VIVOTEK IP8131W tiene un diseño compacto modelo cubo, que posee WiFi, creada para la seguridad de interiores. Se utiliza en oficinas, comercios y residencias. Considerando que aplica la norma H.264 para compresión, para disminuir el tamaño de los ficheros y reduce el ancho de banda de la red.

La figura 2.8 presenta una vista frontal y lateral de la cámara IP VIVOTEK IP8131W, cuyas características técnicas se han descrito.

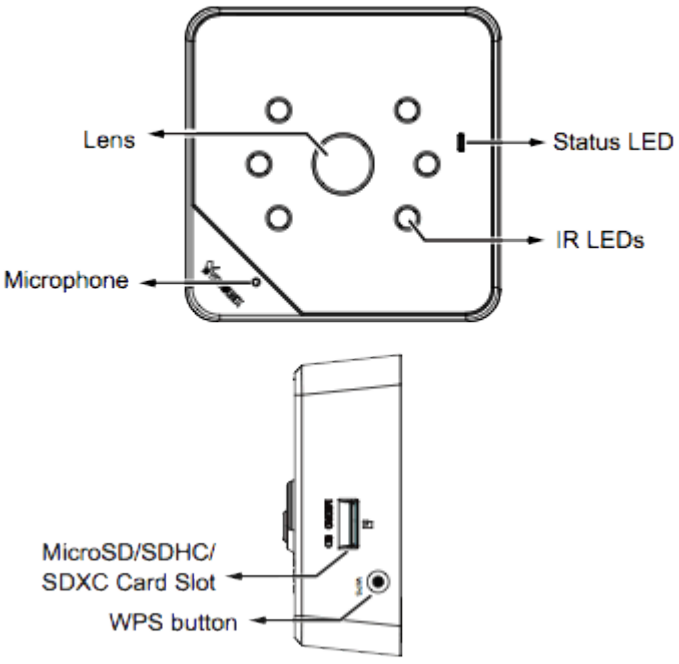


Figura 2.9: Cámara IP VIVOTEK IP8131W

Fuente: http://www.vivotek.es/

Las características técnicas de la cámara IP VIVOTEK IP8131W se describen a continuación:

Modelo IP8131W

Método

CPU (*Central Processing Unit*):

Multimedia SoC (System-on-Chip)

Flash:

16 MB

RAM (*Random-Access Memory*):

128 MB

Propiedades de la videocámara:

Detector imagen:

CMOS 1/4" Progresivo

Máxima Resolución:

1280x800 pixels

Lente:

Focal fija

Alcance Óptico:

f = 3.6 mm

Apertura:

F1.8

Ángulo visual:

61° (horizontal)

38° (Vertical)

73° (Diagonal)

Tiempo de cierre:

1/5 seg. a 1/32,000 seg.

Día Noche:

Filtro infrarrojo movible para servicio diurno y nocturno

Mínima luminosidad:

0.3 Lux, 50 IRE (*Institute of Radio Engineers*) Color

0,001 Lux, 50 IRE B/N (Blanco/Negro)

PTZ:

ePTZ (*Electronic Pan/Tilt/Zoom*)

Servicios:

16x zoom digital (4x en IE plug-in, 4x integrado)

Iluminadores infrarrojos:

Iluminadores infrarrojos incluidos, alcance 6 m

Memoria interna:

Terminal Micro SD/SDHC/SDXC (*Secure Digital Extended-Capacity*)

Vídeo

Compresión:

H.264 y MJPEG

Máxima Velocidad imagenes:

H.264: 30 fps (fotogramas por segundo) a 1280x800

MJPEG: 30 fps a 1280x800

***Streams* Máximos:**

2 *streams* simultáneamente

Relación S/R (Señal/Ruido):

Más de 62 dB

Video *Streaming*:

Resolución, calidad y tasa de bits ajustables

Corte de video graduable para conservar ancho de banda

Disposición de imagen:

Dimensión de imagen, eficacia y velocidad graduable, impresión de tiempo y texto, iluminación, contraste, impregnación, brillantez, control de blancos, registro de exposición, ganancia.

Audio

Capacidades de Audio:

Entrada/Salida Audio (*full duplex*)

Compresión:

G.711

Interfaz:

Micrófono incluido

Distancia:

5 metros

Red

Usarios:

Enfoque hasta diez usuarios

Normas:

IPv4, IPv6, TCP/IP (*Transmission Control Protocol/Internet Protocol*), HTTP (*Hypertext Transfer Protocol*), HTTPS (*Hypertext Transfer Protocol Secure*), UPnP (*Universal Plug and Play*), RTSP/RTP/RTCP (*Real Time Streaming Protocol/ Real-time Transport Protocol/ Real Time Control Protocol*), IGMP (*Internet Group Management Protocol*), SMTP (*Simple Mail Transfer Protocol*), FTP (*File Transfer Protocol*), DHCP (*Dynamic Host Configuration Protocol*), NTP (*Network Time Protocol*), DNS (*Domain Name System*), DDNS (*Dynamic Domain Name System*) , PPPoE (*Point-to-Point Protocol over Ethernet*), CoS, QoS (*Quality of Service*), SNMP (*Simple Network Management Protocol*), 802.1X

Interfaz:

10Base-T/100 BaseTX Ethernet (RJ-45)

ONVIF:

Características utilizables en www.onvif.org

Localización de Movimiento en Vídeo:

Tres ventanas de localización

Alarmas

Arranque de alarma:

Localización de movimiento, arranque manual, acceso digital, arranque constante, aviso grabación, descubrimiento de deterioro de la videocámara

Programas de alarma:

Aviso mediante HTTP, SMTP, FTP y NAS (*Network Access Server*)

Subida ficheros con HTTP, SMTP, FTP y NAS

General

Conectores:

RJ-45 para enlace de red

Componente terminal con un acceso digital

Componente terminal con una salida de audio

Conector de acceso de suministro 12V CC

Diodo LED:

Suministro del sistema y situación

Acceso de suministro:

12V CC

Consumo Máximo:

3.0W

Tamaño:

46mm x 80mm x 80mm

Peso:

123 g

Documentos Seguridad:

CE, LVD, FCC Class B, VCCI, C-Tic

Temperatura de operación:

0°C - 40°C

Necesidades del procedimiento

Sistema Operativo:

Microsoft Windows 7/Vista/XP/2000

Navegador:

Mozilla Firefox 7~10 (Solo streaming)

Internet Explorer 7.x ó 8.x

Más repetidores:

VLC: 1.1.11 o más

QuickTime: 7 o más

Adjuntos contenidos

Disco compacto:

Guía de usuario y de implementación ligera, *Installation Wizard* 2, programa de grabación ST7501 32 canales

Suministrador:

12V, CC, 1.5A

Servicios

SDK utilizable para mejora de servicios.

Alcanza 50 a 90 m en línea directa.

La cámara se localizará a la derecha en la parte superior del local considerando que permite la utilización del rango completo de visibilidad que se obtiene y la importancia de vigilancia de la puerta de acceso al laboratorio.

La figura 2.9 muestra las dimensiones de la cámara IP VIVOTEK IP8131W.

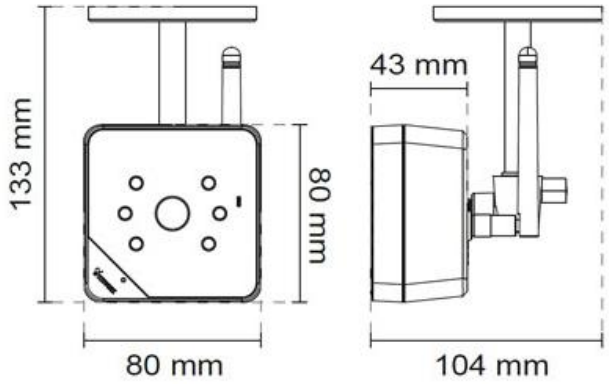


Figura 2.10: Dimensiones de la cámara IP VIVOTEK IP8131W

Fuente: http://www.vivotek.es/

A continuación se muestra en la figura 2.10 la sección posterior de la cámara IP VIVOTEK IP8131W, en la cual se pueden observar los controles y terminales de conexión que posee:

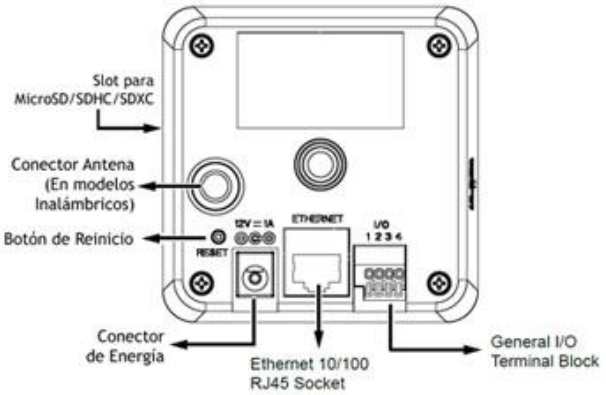


Figura 2.11: Sección posterior de la cámara IP VIVOTEK IP8131W

Fuente: http://www.vivotek.es/

Una vista de la cámara IP VIVOTEK IP8131W, se presenta en la figura 2.11.

Figura 2.12: Cámara IP VIVOTEK IP8131W

Fuente: http://www.vivotek.es/

2.4 Módulo de comunicación

En párrafos anteriores se indicó que se utilizará el estándar *Zigbee* 802.15.4, razón por la cual se aplicarán los módulos de RF *Xbee*, que permiten un consumo reducido de energía y tomar la información de los aparatos instalados en sus puertos y enrutarlos vía inalámbrica al resto del sistema incluyendo la computadora de control donde se ejecuta la gestión de los datos recibidos.

Ideas & Tecnología es una empresa radicada en la ciudad de Guayaquil que brinda soluciones electrónicas a sus clientes. En lo referente a este proyecto, ofrece el módulo adaptador Xbee-TTL I&T de comunicación serial para adecuar los potenciales de un módulo XBee a rangos TTL (*Transistor-Transistor Logic*). Entre sus características se puede mencionar que posee un LED indicador de prendido, Bus de 4 pines para energía y comunicación serial, tasa de datos de 300 Baudios hasta 3MBaudios, emplea de 7 a 8 bits. Se utiliza en interfaces de comunicación serial con tangos TTL en los módulos XBee, también para toma y transmisión de datos seriales con módulos XBee. Emplea alimentación de 5 Voltios dc y el control se realiza con las siguientes señales: (Ideas&Tecnología, 2013)

- 3V3: es un indicador de tensión
- TX: corresponde al indicador para el envío de información
- RX: este indica la recepción de información
- DRX: para recibir información en rangos TTL
- DTX: para envío de información en rangos TTL
- +5V: Tensión de entrada de 5 Voltios dc
- GND: Tierra, tensión de referencia 0 Voltios
- RSS: para señalar actividad XBee

En la figura 2.12 se observa el módulo XBee y se han señalado los puntos correspondientes a las señales de control.

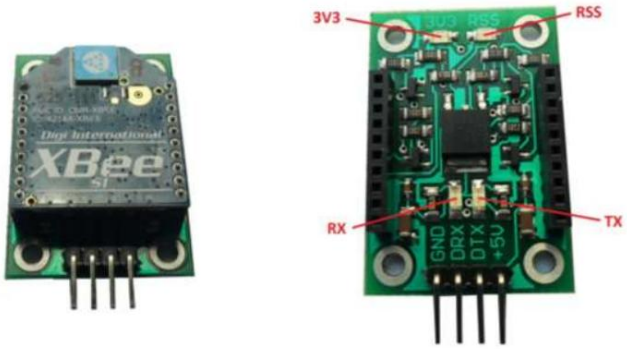


Figura 2.13 Módulo XBee
Fuente: (Ideas&Tecnología, 2013)

Esta tecnología emplea el protocolo IEEE 802.15.4 para redes WPAN en utilidades de transmisiones confiables de reducida velocidad de datos, extensión del tiempo de vida de las pilas, aplicable a proyectos domóticos pues evita la multiplicación de dispositivos y su precio es aceptable.

Se emplea en enlaces punto a punto y multipunto, enrutamiento de datos, opera en un rango libre ISM correspondiendo 2.4 GHz en casos inalámbricos y con reducidas velocidades de transmisión, brinda enlaces confiables gracias a un código de 128 bits y su precio es aceptable. Entre sus limitaciones hay que señalar su reducida velocidad de transmisión privándose de ancho de banda, únicamente opera mensajes cortos aunque esto es suficiente para señales de sensores, no interactúa con Bluetooth por la diferencia en las velocidades de transmisión, por corresponder a redes WPAN su alcance es pequeño.

2.4.1 Módulo de recepción

Es necesario uno de estos por red y se ocupa de la gestión de la red y el enrutamiento de los aparatos para interconectarse, necesita memoria y atributos de procesamiento. Se

encarga de organizar la recepción de datos de los detectores y presentarla en la computadora PC con el programa X-CTU empleado para organizar los módulos Xbee y además posee un dispositivo de envío y recepción de información a través del puerto enlazado al Xbee. En la figura 2.13 se presenta el diagrama esquemático del módulo de recepción del proyecto.

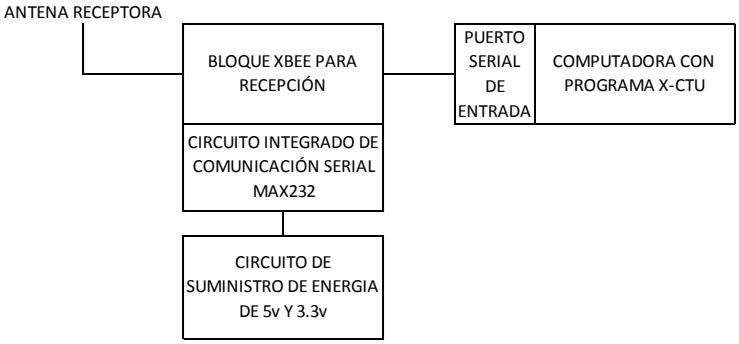
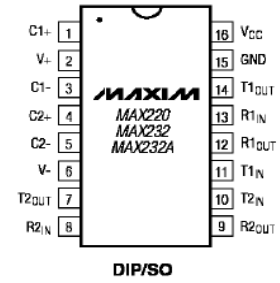


Figura 2.14 Diagrama esquemático del módulo de recepción

Elaborado por: Autor

Puede observarse que este módulo está constituido por el bloque Xbee para recepción, el suministro de 5 y 3.3 Voltios y el circuito integrado de comunicación serial MAX232, éste corresponde a un modelo empleado como interfaz entre los rangos TTL y RS232 y necesita sólo un suministro de 5 Voltios. Posee dos entradas TTL y salida RS232 y también dos entradas RS232 y salida TTL como puede verse en la figura 2.14. El MAX232 está capacitado para transferir información a 120 kbps. (TecMikro, 2014)



CAPACITANCE (μF)					
DEVICE	C1	C2	C3	C4	C5
MAX220	4.7	4.7	10	10	4.7
MAX232	1.0	1.0	1.0	1.0	1.0
MAX232A	0.1	0.1	0.1	0.1	0.1

Figura 2.15 Circuito integrado de comunicación serial MAX232

Fuente: (TecMikro, 2014)

2.4.2 Módulo de transmisión

Se encarga de ejecutar las acciones para comunicarse y transmitir los datos de los detectores al bloque de recepción, pero no la de otros aparatos. Esto significa que está inactivo casi todo el tiempo por lo que se incrementa la vida de las pilas. No necesita mucha memoria y es de bajo precio. En la figura 2.15 se observa el diagrama esquemático del módulo de transmisión.

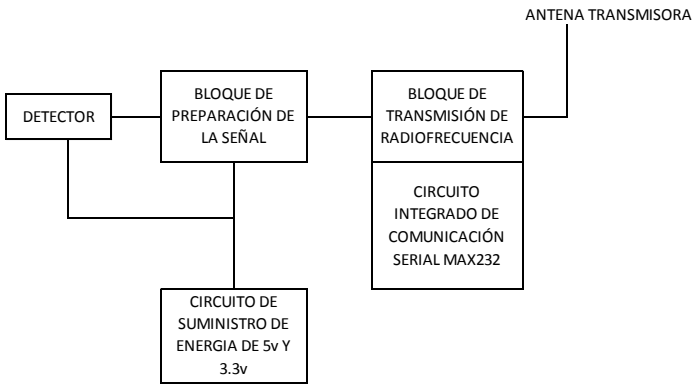


Figura 2.16 Diagrama esquemático del bloque de transmisión.

Elaborado por: Autor

En la figura puede observarse que posee un bloque Xbee de transmisión, el circuito de suministro de energía de 5 voltios y 3.3 voltios y el bloque de preparación de la señal.

2.5 Interfaz de usuario

Es el que permitirá la observación por parte del usuario de las novedades ocurridas en el laboratorio o simplemente observar esta dependencia.

Por ejemplo se permitirá observar el área del laboratorio en la pantalla del computador o ingresar a un block de notas para verificar el registro de los últimos acontecimientos. También en el caso de que se generen las ventanas emergentes de alerta, es posible ingresar a un block de notas con el registro de los últimos sucesos y proceder a cerrar tales ventanas.

CAPITULO III DISEÑO GENERAL DEL PROYECTO

El software X-CTU se encarga de configurar los bloques Xbee y establecerlos como receptor o transmisor. También se definirán otras características como la comunicación serial, observación de tramas, etc.

Como ya se indicó anteriormente se recomienda la utilización del módulo adaptador XBee -TTL de la empresa Ideas y Tecnología. En el caso del software X-CTU que lo gestionará, se presenta a modo de ejemplo el programa creado por Digi International para operar con XBee IO gráficamente, además posee una consola para información con instrucciones AT. Puede descargarse en el siguiente enlace:
http://www.digi.com/support/productdetail?pid=3352&osvid=57&type=utilities

3.1 Uso de X-CTU

XBee IO se configura a través de su conector serial. Se recomienda usar el programa X-CTU y consolas como Hyper Terminal, con instrucciones AT. En la figura 3.1 se muestra la ventana principal de X-CTU

3.1.1 Pasos a seguir con XBee IO.

El trabajo se inicia escogiendo el puerto serial, para lo cual se elige la alternativa *Test/Query* para comprobar la adecuada operación del bloque. Ahora se hace *click* en el icono *Modem Configuration*/*Read*, una vez establecidos los cambios se hace *click* en *Write*, almacenando la disposición. En la figura 3.2 se muestra un ejemplo de este proceso. Los datos almacenados pueden cambiarse fácilmente marcándolos, haciendo *click* y escogiendo otra alternativa entre las que se ven en los menús desplegables. (MCI, 2011)

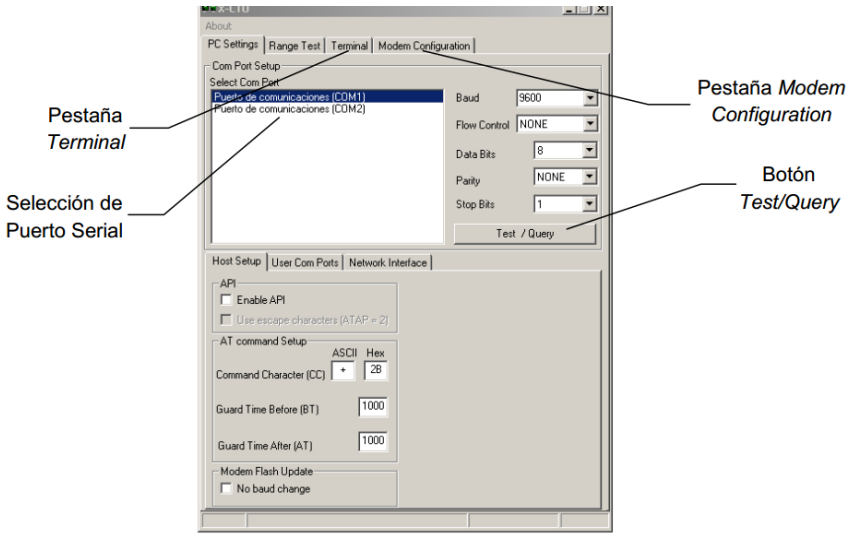


Figura 3.1 Ventana principal de X-CTU

Fuente: (MCI, 2011)

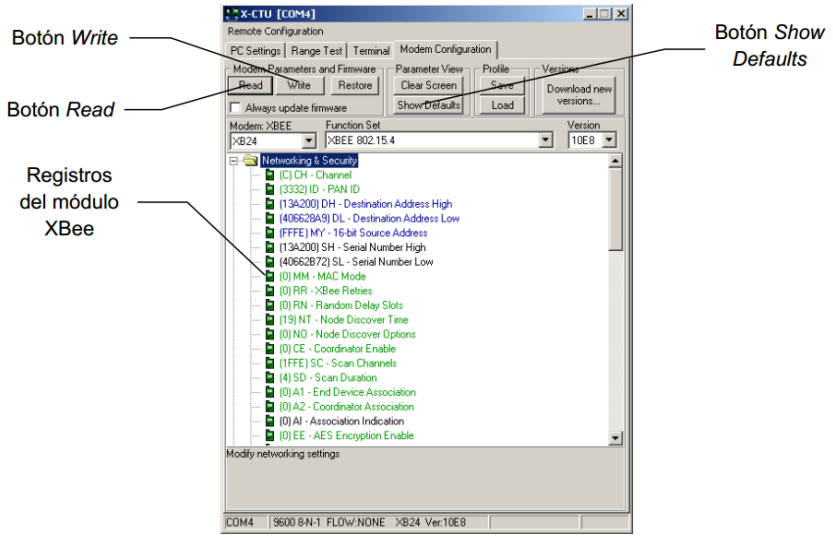


Figura 3.2 Disposición de XBee IO

Fuente: (MCI, 2011)

3.1.2 La tarjeta XBee IO.

XBee IO se creó para ofrecer tres operaciones fundamentales para satisfacer variados requerimientos. Es posible programarlo para substitución de cables, y a través del puerto

serial se gestiona el XBee IO local y otros XBee IO remotos vía inalámbrica. Además es posible utilizar XBee *Explorer* enlazado a la computadora para gestionar otros XBee IO remotos.

3.2 Programación preliminar

Se inicia este proceso para emplear el módulo colocando XBee en el conector de XBee IO, de acuerdo a lo indicado en la placa, después se conectan los ingresos de contacto seco, las salidas de *relay* y el suministro de energía de 9 a 35 Vdc al bloque XBee IO.

3.2.1 Sustitución de cables

Esta programación admite que uno o más bloques remotos reproduzca el dato lógico del ingreso de otro bloque especialmente en la salida de *relay* respectiva, como si los bloques estuvieran cableados entre ellos. La figura 3.3 muestra la programación para sustitución de cables, esto es muy útil si se cuenta con dos o más bloques y se necesita que operen igual ante un cierto evento.

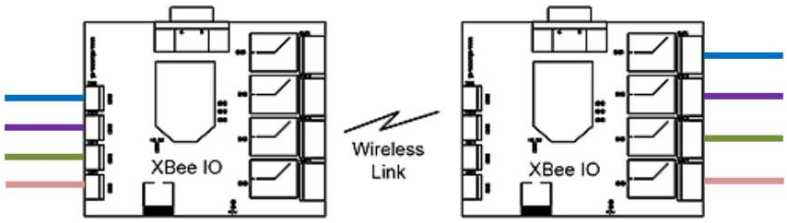


Figura 3.3 Programación para sustitución de cables.
Fuente: (MCI, 2011)

Esto puede ejecutarse sin necesidad de que la computadora esté conectada al bloque y sólo se lo requiere al programar el bloque anterior y luego de la programación los bloques operan por ellos mismos. Es importante anotar que XBee IO opera sólo con entradas digitales.

3.2.2 Programación para gestión local y remota.

Esta programación permite gestionar los bloques con el conector serial DB9 contenido en la placa.

3.2.3 Programación para gestión local

De esta manera se puede gestionar la activación y apagado de los *relays* de la placa enlazada a la computadora y averiguar el estado de sus ingresos con el puerto serial. La figura 3.4 presenta un diagrama esquemático de gestión local con puerto serial.

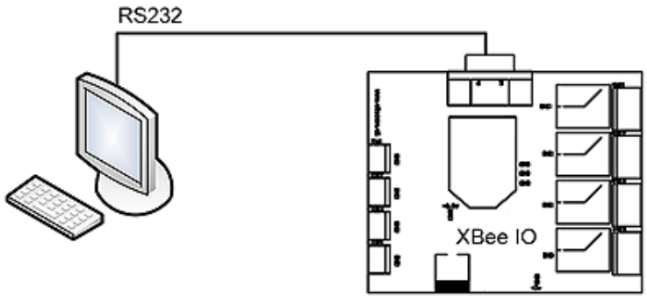


Figura 3.4 Diagrama esquemático de gestión local con puerto serial.
Fuente: (MCI, 2011)

Este procedimiento es apropiado si hay solo un bloque XBee IO enlazado a la computadora. Se emplean instrucciones AT o XBee IO *Controller*.

3.2.4 Programación para gestión remota

Es la programación es la más poderosa pues con ella el usuario gestiona muchos bloques XBee IO remotos teniendo solo una de ellas enlazada a la computadora. La figura 3.5 presenta un esquema de administración remota con puerto serial.

Esta operación es útil si se cuenta con varios bloques XBee IO y se desea administrarlos individualmente y también saber el estado de sus ingresos de manera remota.

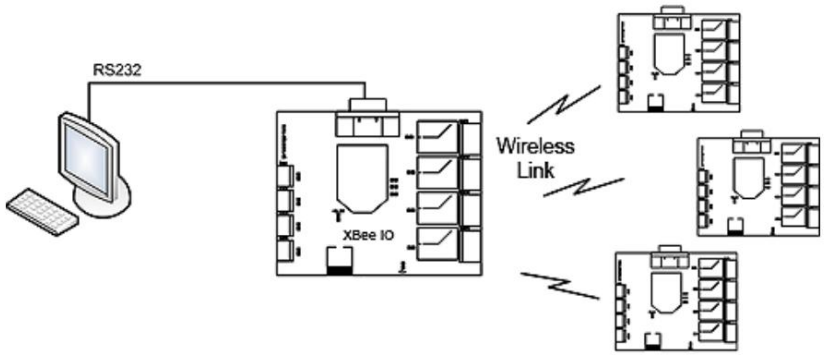


Figura 3.5 Esquema de administración remota con puerto serial.
Fuente: (MCI, 2011)

3.2.5 Programación de los bloques para gestión local y remota

Para emplear estas operaciones, todos los bloques considerados deben tener sus switchs en estado 0 y programar los datos del XBee con X-CTU como se presenta en la figura 3.6:

D8 = 0	D3 = 3
D7 = 4	D2 = 3
D6 = 4	D1 = 3
D5 = 4	D0 = 3
D4 = 4	AP = 1

Figura 3.6 Programación de datos del XBee para gestión local y remota
Fuente: (MCI, 2011)

Es recomendable usar la programación por *default* mediante las instrucciones S*how Defaults/Write* y variar los datos de acuerdo a lo indicado en la tabla.

3.3 Utilización del programa MCI XBEE IO *Controller*

Es un software de MCI para gestionar administrar el módulo XBee IO emplea una interface visual para que el usuario gestione un número ilimitado de bloques XBee IO de manera sencilla e instintiva.

Con este software se puede gestionar el estado de los *relays* y conocer el de los ingresos conectados ópticamente de varios bloques XBee IO locales o remotos. También posee un método de gestión de bloques para que el usuario almacene diversos registros de bloques, con denominaciones diferentes y escogidos por él y aplicarlos cuando sea necesario. Los ficheros son clase XML (*eXtensible Markup Language*), de manera que son portables y sencillos.

La figura 3.7 presenta la ventana principal de esta aplicación

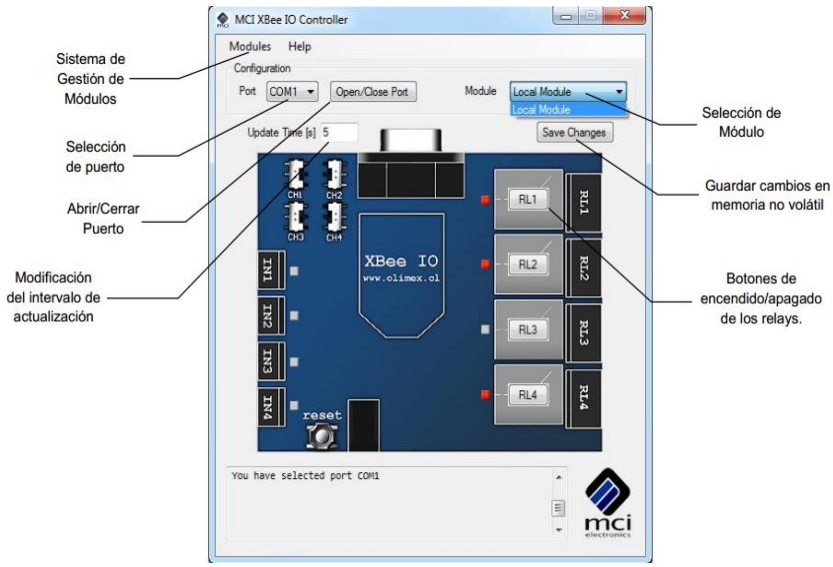


Figura 3.7 Ventana principal de *XBee IO Controller*

Fuente: (MCI, 2011)

3.3.1 Lectura y escritura en tarjetas XBEE IO

Para ejecutar *XBee IO Controller* primero hay que escoger el puerto serial que se quiere utilizar en la viñeta arriba a la izquierda y se oprime *click* en la opción *Open/Close Port*. A continuación se determina el bloque que se va a emplear y en el inicio únicamente se observa el bloque local.

El software actualiza la condición de los LEDs en la pantalla cada cinco segundos de manera automática. Ese lapso está establecido por *default* y para cambiarlo se lo realiza en la parte superior izquierda de la ventana en la opción *Update Time.*
A continuación, para activar y desactivar los *relays* del bloque elegido se oprime *click* en uno de los pulsadores RL1 a RL4 a la derecha de la ventana.

3.3.2 Añadir y excluir bloques remotos individualizados

Para ingresar al menú de edición de bloques es suficiente oprimir click en la viñeta *Modules*. La figura 3.8 muestra la ventana de edición de bloques.

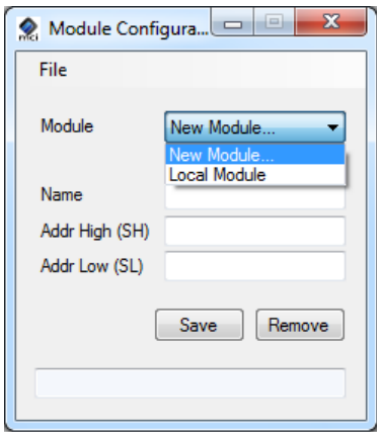


Figura 3.8 Ventana de edición de bloques

Fuente: (MCI, 2011)

Esta interfaz contiene áreas para las denominaciones o alias y la dirección MAC (*Media Access Control*) del bloque que se va a añadir, esta acción faculta al usuario para acceder a la dirección del bloque por una sola vez y después olvidarse de la misma. Para ejecutar el bloque más tarde, solo se requiere oprimir *click* en la denominación correspondiente asignada por el cliente en la ventana central del programa.

Al agregar un módulo, el software de manera automática almacenará la información en un fichero externo. Otra posibilidad es poder editar las áreas de los bloques o inclusive eliminarlos si así se lo requiere.

3.3.3 Añadir un bloque remoto

Para realizar esta aplicación, se escoge la alternativa *New Module*. A continuación se digita una denominación a elección del usuario y las cifras *Serial Address High* (SH) y *Serial Address Low* (SL), los cuales es posible verlos en X-CTU o en la placa localizada en la parte inferior del bloque XBee tal como se muestra en la figura 3.9.

Figura 3.9 Seriales Sl y SH en la parte de abajo del bloque Xbee

Fuente: (MCI, 2011)

Finalmente se oprime *click* en *Save* para almacenar la información ingresada. De esta manera los bloques añadidos permanecerán almacenados en el disco duro y se los podrá utilizar en la siguiente ocasión que se ingrese al software.

En la figura 3.10 se muestra la pantalla correspondiente al caso de añadir un bloque

Si se desea borrar un bloque es suficiente con elegirlo y oprimir *click* en la opción *Remove*.

3.4 Empleo de ficheros XML externos

Ya se había indicado que este software emplea ficheros XML para almacenar los bloques individualizados, para lo cual se relaciona una denominación personalizada o alias a cada dirección MAC.

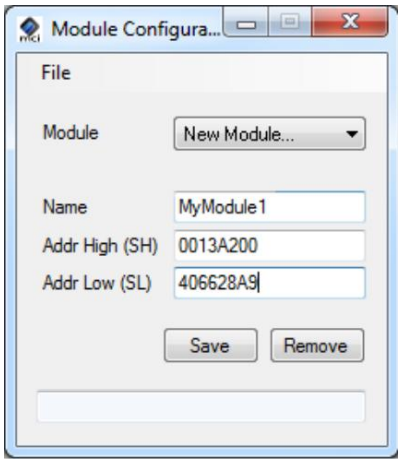


Figura 3.10 Añadir un bloque

Fuente: (MCI, 2011)

Esto proporciona la ventaja de que de esta manera es posible generar algunos registros de bloques, así a modo de ejemplo se pude indicar que para diferentes negocios es posible cargar el fichero respectivo en el sitio.

También el programa contiene una interfaz de administración de ficheros que posibilita generar nuevos ficheros o cargar otros ya existentes. Por *default* el software emplea el fichero *Modules*.xml.

En cada ocasión que se trabaje con el software éste tratará de leer el fichero y si el mismo no consta, procederá a generarlo en la misma carpeta del *software* principal.

3.4.1 Generación de un nuevo fichero

Para llevar a cabo esta aplicación del software, se oprime *click* en la opción *Modules*. A continuación se oprime *click* en la viñeta *New File*, ahora se procede a escoger una denominación para el fichero y se pulsa aceptar.

Una vez realizados estas acciones se genera un fichero por *default* que únicamente contiene el bloque local.
En la figura 3.11 se muestra la carga y generación de ficheros XML externos,

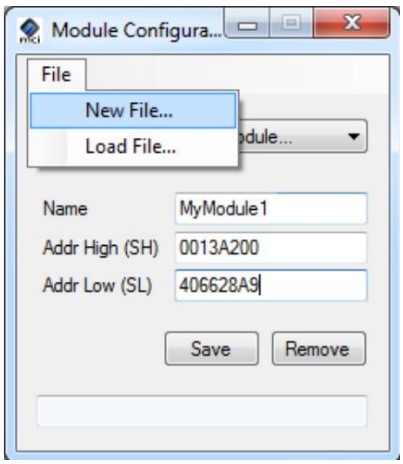


Figura 3.11 Carga y generación de ficheros XML externos

Fuente: (MCI, 2011)

Si se tienen ficheros existentes, éstos podrán ser cargados mediante la alternativa *Load File*

3.4.2 Carga de un fichero existente

Para acceder a este tipo de ficheros, se pulsa *click* en la opción *Modules*. A continuación se oprime *click* en la viñeta *Load File*, se elige el fichero que se quiere abrir y se pulsa aceptar.

De esta manera, el software cargará en memoria todos los bloques para ser utilizados a través de la interfaz gráfica principal.

3.5 Almacenamiento de cambios en memoria no-volátil

En primer lugar es necesario especificar que una memoria no volátil es aquella que no requiere de energía para mantenerse. Así, para aplicaciones que necesiten ser resistentes ante suspensiones de la energía eléctrica, se tiene la oportunidad de almacenar los datos de los relés en la memoria no-volátil del módulo XBee, para que éste recuerde los valores después de un reajuste o un corte en el suministro de energía.

Para almacenar los cambios es suficiente pulsar *click* en *Save Changes* y el software presentará un “Ok” si la instrucción fue exitosa.

3.5.1 Variación del tiempo de reajuste *(Update Time)*

Ya se había indicado que este sistema después de abrir un acceso el programa establece el dato de los terminales del módulo XBee IO consecutivamente, con un espacio entre lecturas de acuerdo al indicador *Update Time,* el lapso establecido por *default* es de cinco segundos y la interfaz contiene una alternativa para modificar ese lapso cuando el usuario lo necesite.

3.5.2 Ubicación y alcance los dispositivos de seguridad recomendados en este proyecto

Como ya se indicó en el capítulo 2, los dispositivos de seguridad cuya implementación se recomienda para este laboratorio son los siguientes:

- Detector de movimiento marca Honeywell modelo 5897-35
- Detector fotoeléctrico de humo modelo 5806W3 de la marca Honeywell
- Cerradura electromagnética marca Anson de 600 libras
- Cámara IP VIVOTEK IP8131W

3.5.3 Ubicación y alcance del detector de movimiento marca Honeywell modelo 5897-35

El detector de movimiento marca Honeywell modelo 5897-35 será ubicado en la parte central de la pared al fondo del laboratorio, de tal manera que con el ángulo de cobertura y el correspondiente alcance se cubran los espacios necesarios, especialmente el que corresponde a la puerta de ingreso a esta dependencia.

En la figura 3.12 se muestra la ubicación y cobertura del detector de movimiento marca Honeywell modelo 5897-35, observándose que cumple con el propósito de su implementación.

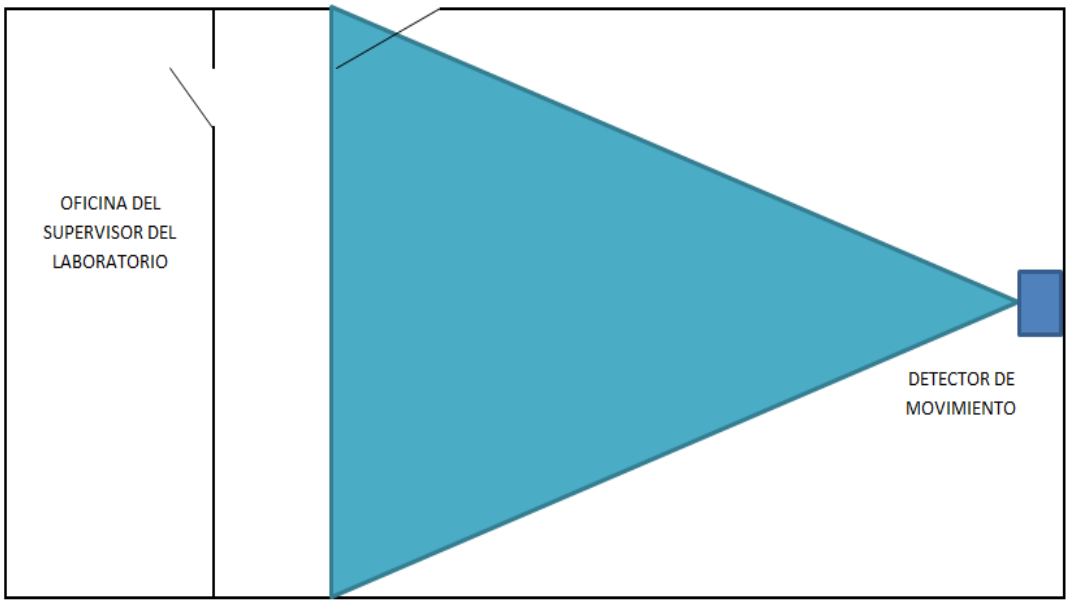


Figura 3.12 Ubicación y cobertura del detector de movimiento marca Honeywell modelo 5897-35

Elaborado por: Autor

La fotografía mostrada en la figura 3.13 indica la posición recomendada del detector de movimiento marca Honeywell modelo 5897-35.

Figura 3.13 Fotografía de la ubicación recomendada del detector de movimiento marca Honeywell modelo 5897-35

Elaborado por: Autor

En la figura 3.14 se muestra una fotografía tomada desde la ubicación recomendada del detector de movimiento marca Honeywell modelo 5897-35 y se puede observar la cobertura aproximada de dicho sensor.

Figura 3.14 Fotografía desde la ubicación recomendada del detector de movimiento marca Honeywell modelo 5897-35 y su cobertura
Elaborado por: Autor

3.5.4 Ubicación y alcance del detector fotoeléctrico de humo modelo 5806W3 de la marca Honeywell

A fin de cumplir los requerimientos de seguridad para este tipo de sensor, el mismo será ubicado en el centro del laboratorio de manera que pueda captar cualquier emisión de humo que se produzca en el interior de esta dependencia.

La ubicación y cobertura del detector fotoeléctrico de humo modelo 5806W3 de la marca Honeywell se puede observar en la figura 3.15.

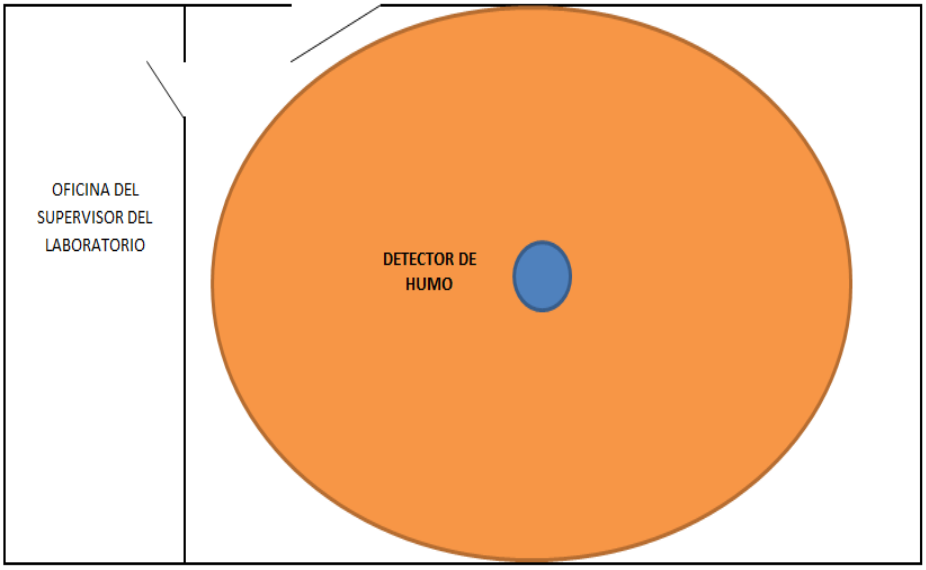


Figura 3.15 Ubicación y cobertura del detector fotoeléctrico de humo modelo 5806W3 de la marca Honeywell

Elaborado por: Autor

La fotografía presentada en la figura 3.16 muestra la ubicación recomendada para el detector fotoeléctrico de humo modelo 5806W3 de la marca Honeywell

Figura 3.16 Ubicación recomendada del detector fotoeléctrico de humo modelo 5806W3 de la marca Honeywell

Elaborado por: Autor

3.5.5 Ubicación y alcance de la cerradura electromagnética marca Anson de 600 libras

Considerando que el Laboratorio de Electricidad de la facultad de Educación Técnica para el Desarrollo tiene una sola puerta exterior de ingreso, la cual es de madera y adicionalmente existe una puerta enrejada externa a ella, lo cual ofrece un grado adicional de seguridad, se ha establecido en este proyecto que solo es necesario un sensor de apertura y en este diseño se recomienda la cerradura electromagnética marca Anson de 600 libras que será ubicada en la puerta de madera mencionada.

Cabe indicar adicionalmente que todas las ventanas de esta dependencia tienen instaladas rejas fijas externas, razón por la cual se considera que no es necesario instalar dispositivos de seguridad en ellas.

En la figura 3.17 se observa la ubicación de la puerta de acceso al laboratorio y la localización recomendada para la instalación de la cerradura electromagnética marca Anson de 600 libras.

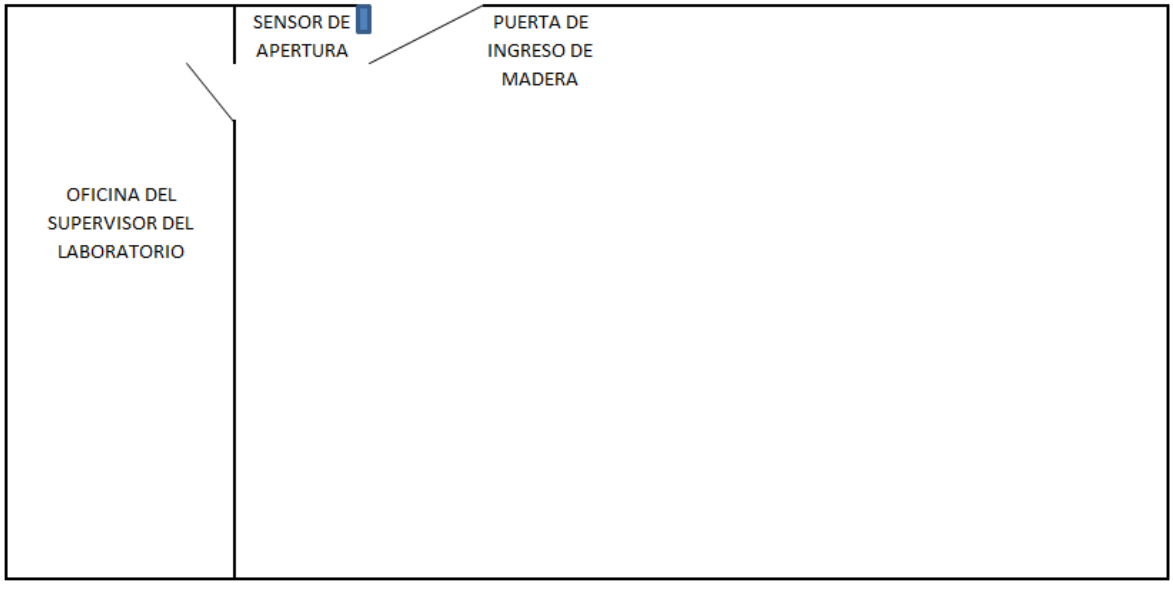


Figura 3.17 Ubicación y cobertura de la cerradura electromagnética marca Anson de 600 libras

Elaborado por: Autor

La fotografía presentada en la figura 3.18 muestra la ubicación recomendada en este proyecto para la cerradura electromagnética marca Anson de 600 libras.

Figura 3.18 Ubicación recomendada de la cerradura electromagnética marca Anson de 600 libras

Elaborado por: Autor

3.5.6 Ubicación y alcance de la cámara IP VIVOTEK IP8131W

Se pretende que la cámara IP VIVOTEK IP8131W, cubra la mayor área posible del interior del laboratorio de electricidad, razón por la cual se ha establecido que debe estar localizada en la pared opuesta a la puerta de ingreso, puesto que es la sección que mayor cobertura de video debe tener.

En la figura 3.19 se muestra la ubicación y cobertura de la cámara IP VIVOTEK IP8131W

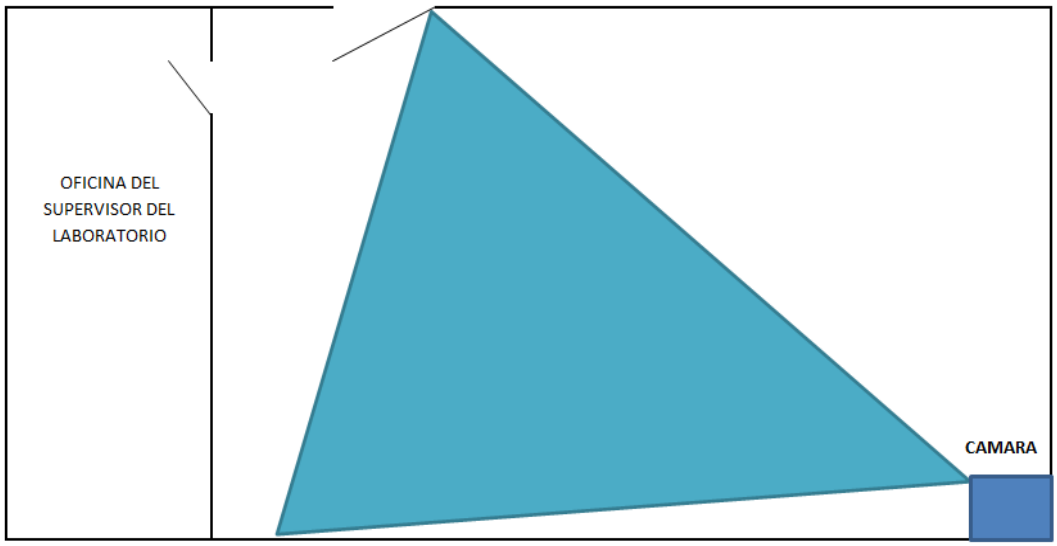


Figura 3.19 Ubicación y cobertura de la cámara IP VIVOTEK IP8131W

Elaborado por: Autor

En la figura 3.20 se muestra una fotografía en que se enfoca el ángulo de cobertura que abarcaría la cámara IP VIVOTEK IP8131W.

Figura 3.20 Fotografía tomada desde la ubicación recomendada de la cámara IP VIVOTEK IP8131W

Elaborado por: Autor

En la fotografía mostrada en la figura 3.21 se indica la ubicación de la cámara con un círculo rojo.

Figura 3.21 Fotografía de la ubicación recomendada de la cámara IP VIVOTEK IP8131W

Elaborado por: Autor

3.6 Presupuesto referencial

De acuerdo a los precios de mercado local, se ha elaborado un presupuesto referencial para la implementación de los dispositivos de seguridad detallados anteriormente:

Dispositivo	Valor Unitario
Detector de movimiento marca Honeywell modelo 5897-35	$ 280.00
Detector fotoeléctrico de humo modelo 5806W3 de la marca Honeywell	$ 290.00
Cerradura electromagnética marca Anson de 600 libras	$ 250.00
Cámara IP VIVOTEK IP8131W	$ 350.00
Total	$ 1.170.00

3.7 Dispositivos adicionales

Considerando que los equipos con que cuenta el Laboratorio de Electricidad son costosos y frágiles, se recomienda que se implemente un Sistema Biométrico de acceso para puertas. Con esta premisa y con las mismas consideraciones que se aplicaron para los otros dispositivos recomendados en este proyecto de investigación, se buscó información acerca de terminales de control de presencia y/o accesos y se estableció que se debía recomendar el dispositivo para detectar la huella dactilar del usuario MA300 fabricado por la empresa ZKSoftware, que ofrece soluciones biométricas avanzadas.

El detector MA300 es un terminal para huella dactilar muy sencillo para control de accesos. El registro se efectúa mediante la huella dactilar y también presenta la opción de emplear una tarjeta de proximidad RFID (*Radio Frequency IDentification*). Adicionalmente, ofrece diversos servicios mediante su relé, por ejemplo la apertura de puerta.

Permite comunicarse con la computadora mediante un puerto Ethernet y también brinda la opción de trabajar de manera "*stand-alone*". La figura 3.22 muestra el modelo para huella dactilar MA300 de ZKsoftware.

Figura 3.22 Modelo para huella dactilar MA300 de ZKsoftware
Fuente: http://www.zksoftware.es/

Se recomienda utilizar uno de estos dispositivos para entrada y otro para marcar la salida de los usuarios. Este control de acceso biométrico digital brinda un tiempo de reconocimiento de un segundo y puede almacenar hasta 1.500 huellas dactilares

CONCLUSIONES:

Durante la ejecución de este trabajo de investigación se realizó un estudio de los fundamentos tecnológicos que permitieron desarrollar este proyecto.

En base a los fundamentos recabados, se determinó los elementos de control necesarios para un sistema domótico de seguridad.

En el Laboratorio de Electricidad de la facultad de Educación Técnica para el Desarrollo de la Universidad Católica de Santiago de Guayaquil, se estableció la ubicación adecuada para los sensores y cámara que conforman el sistema de seguridad recomendado.

En base a la información recabada y que se ha detallado ampliamente durante el desarrollo de este trabajo de investigación, se elaboró el diseño del sistema domótico de seguridad con tecnología inalámbrica.

De acuerdo a lo indicado, se cumplió con el objetivo general planteado para este trabajo, que consistía en la realización de un diseño para un sistema domótico de seguridad con comunicación inalámbrica controlado mediante una computadora que permita la evaluación del sistema y la observación de las novedades que se presenten en el interior del laboratorio de electricidad de la FET de la UCSG.

RECOMENDACIONES

Al implementar el sistema de seguridad recomendado en este proyecto, deben ubicarse los dispositivos en las ubicaciones indicadas puesto que para establecer las mismas se hicieron algunas pruebas para determinar la cobertura apropiada de los mismos.

Así por ejemplo, la cámara debe ubicarse como se indicó en el proyecto en un sitio alto, para que no quede expuesta al alcance de las personas que acuden al laboratorio. Además debe programarse la cámara mediante el software respectivo para establecer la resolución mínima y que inicie la grabación al detectarse movimiento, de esta manera se economiza la memoria de almacenamiento.

Debe revisarse continuamente las baterías, esto podría hacerse semanalmente para evitar que por agotamiento de la energía algún dispositivo deje de funcionar. De la misma manera la operación del sistema debe comprobarse una vez al mes.

BIBLIOGRAFÍA

Agé, M., Baudru, S., Crocfer, N., Crocfer, R., Ebel, F., Hennecart, J., y otros. (2013). *Seguridad informática: conocer el ataque para una mejor defensa (Ethical hacking) Nueva edición.* ENI.

Alliance, Z. (2006). *ZigBee specification.* Recuperado el 6 de Enero de 2014, de URL: http://www. zigbee

Alliance, Z. (2007). *ZigBee 2007 specification.* Recuperado el 5 de Enero de 2014, de http://www. zigbee. org/Specifications/ZigBee/Overview. aspx.

Alliance, Z. (2007). *ZigBee 2007 specification.* Recuperado el 5 de Enero de 2014, de http://www. zigbee. org/Specifications/ZigBee/Overview. aspx.

Alliance, Z. (2009). *IEEE 802.15. 4, ZigBee standard.* Recuperado el 5 de Enero de 2014, de http://www. zigbee. org.

ANAYA. (2012). *Hacker. Edición 2012.* ANAYA MULTIMEDIA.

Anderson, N., & Doherty, J. (2009). *Introducción a las redes CISCO.* ANAYA MULTIMEDIA.

Anfinson, D. (2009). *Fundamentos de la tecnología de la información: hardware y software para PC.* PRENTICE-HALL.

Arboledas, D. (2013). *BACKTRACK 5.* RA-MA.

Ardila, S. (2009). Estado actual del monitoreo remoto de pacientes usando redes de sensores inalámbricas. *Entérese Boletín Científico Universitario dic2009, Issue 27*, 64-69.

Baker, N. (2005). ZigBee and Bluetooth strengths and weaknesses for industrial applications. *Computing & Control Engineering Journal 16(2)*, 20-25.

Baronti, P., Pillai, P., Chook, V., Chessa, S., Gotta, A., & Hu, F. (2007). Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards. *Computer Communications, Volume 30, Issue 7, 26 May 2007*, 1655–1695.

Bluetooth, S. (2001). *Specification of the Bluetooth System, version 1.1.* . Recuperado el 6 de Enero de 2014, de http://www. bluetooth. com.

Bluetooth, S. (2007). *Bluetooth specification.* Recuperado el 6 de Enero de 2014, de annotare.googlecode.com

Campoverde, J., & Arias, X. (Septiembre de 2008). *Diseño y construcción de un prototipo de control y monitoreo industrial por medio de una red inalámbrica.* Recuperado el 5 de Enero de 2014, de repositorio digital epn: http://bibdigital.epn.edu.ec/handle/15000/934

Carroll, J., Monrroy, I., Rivera, C., & Gomez, Y. (2009). *Diseño, simulación y construcción de una antena para la propagación de señales a una frecuencia de 2.4 GHZ.* Recuperado el 5 de Enero de 2014, de Repositorio Colecciones Digitales Uniminuto: http://hdl.handle.net/10656/2617

Cazarez, J. (s.f.). *La Evolución de la Tecnología Móvil.* Recuperado el 1 de Julio de 2013, de Slideshare: http://www.slideshare.net/jcazarez/historia-de-los-mviles

Chávez, C. (2007). Influencia de la radiación solar sobre el desempeño de las redes WI-FI en la banda de los 5 Ghz (802.11a) . *Télématique*, 32-52.

Colobran, M., Arqués, J., & Galindo, E. (2008). *Administración de sistemas operativos en red.* Editorial UOC.

EcuRed. (s.f.). *Tecnología Celular.* Recuperado el 1 de Julio de 2013, de www.ecured.cu: http://www.ecured.cu/index.php/Tecnolog%C3%ADa_celular

Egan, D. (2005). The Emergence of ZigBee in building automation and industrial controls. *Computing and Control Engineering, 16(2),* 14-19.

Eslava, A. (Octubre de 2003). *Análisis comparativo de la red Lan contra las redes inálambricas.* Recuperado el 5 de Enero de 2014, de eprints.uanl.mx: http://eprints.uanl.mx/1251/1/1020149259.PDF

Fernández, v. (2004). *El hogar digital: necesidades que atiende, servicios que presta, tecnologías que utiliza.* Creaciones Copyright.

Gallego, A. (2009). *Routers CISCO: Edición revisada y actualizada 2010 (Guia practica).* ANAYA MULTIMEDIA.

Gómez, A. (2011). *Auditoria de seguridad informática.* STARBOOK EDITORIAL.

Gómez, A. (2011). *Gestión de incidentes de seguridad informática.* STARBOOK EDITORIAL.

Gómez, A. (2011). *Seguridad en equipos informáticos MF0486-3 Certificado de profesionalidad.* STARBOOK EDITORIAL.

Gómez, J. (2010). *Guía de campo hackers: aprende a atacar y a defenderte.* RA-MA.

Guerrero, A., & Ruiz, E. (Mayo de 2013). *Análisis, diseño y simulación de una red inalámbrica de sensores Wsn en el patio de tanques en la empresa petrolera "Grupo Synergy E & P Ecuador".* Recuperado el 5 de Enero de 2014, de Repositorio Digital - UPS: http://dspace.ups.edu.ec/handle/123456789/4351

Harke, W. (2010). *Domótica para viviendas y edificios.* Marcombo.

Harrington, J. (2006). *Manual práctico de seguridad de redes (Hardware y redes)* . ANAYA MULTIMEDIA.

Hernández, R., Fernández, c., & Baptista, P. (2003). *Metodología de la Investigación* (Tercera ed.). México D.F.: McGraw Hill.

Huidrobo, J., & Millán, R. (2004). *Domótica: edificios inteligentes.* . Creaciones Copyright.

Huidrobo, J., & Millán, R. (2010). *Manual de Domótica.* Creaciones Copyright.

Ideas&Tecnología. (2013). *Módulo adaptador Xbee-TTL I&T* . Recuperado el 6 de Enero de 2014, de www.ideastechnology.com: www.ideastechnology.com

Junestrand, S., Passaret, X., & Váz, D. V. (2004). *Domótica y hogar digital.* Madrid: Paraninfo.

Katz, M. (2013). *Redes y seguridad.* Marcombo S.A.

Kernighan, B., & Pike, R. (1984). *The UNIX programming environment.* Prentice Hall.

Kinney, P. (2 de Octubre de 2003). *ZigBee Technology: Wireless Control that Simply Works.* Recuperado el 5 de Enero de 2014, de Communications Design Conference (Vol. 2): http://www.mouser.cn/pdfdocs/ZigBeeTechnology.pdf

Lee, J.-S., Su, Y.-W., & Shen, C.-C. (2007). A Comparative Study of Wireless Protocols: Bluetooth, UWB, ZigBee, and Wi-Fi. *In Industrial Electronics Society, 2007. IECON 2007. 33rd Annual Conference of the IEEE,* 46-51.

Lockhart, A. (2007). *Seguridad de redes: los mejores trucos (O REILLY).* ANAYA MULTIMEDIA.

Martín, J. (2009). *Instalaciones domóticas.* Editex.

Martinez, E. (mayo de 2001). *Telecomunicaciones.* Recuperado el 1 de Julio de 2013, de eveliux.com: http://www.oocities.org/es/laurasayago/hw/tel5.htm

MCI. (2011). *Manual de Usuario X Bee IO.* Recuperado el 10 de Enero de 2014, de MCI electronics. Ingeniería MCI Ltda.: http://www.olimex.cl/pdf/Manual%20del%20Usuario%20MCI-WIR-00787.pdf

Mcmahon, R. (2003). *Introducción a las redes.* ANAYA MULTIMEDIA.

Mcnab, C. (2008). *Seguridad de redes.* ANAYA MULTIMEDIA.

Meyer, G. (2005). *Domótica: los mejores trucos.* Grupo Anaya Comercial.

Meyers, M. (2003). *Redes: administración y mantenimiento.* ANAYA MULTIMEDIA.

Meyers, M. (2005). *Redes: gestión y soluciones.* ANAYA MULTIMEDIA.

Miller, B., & Bisdikian, C. (2001). *Bluetooth Revealed* (2nd ed.). Prentice Hall PTR Upper Saddle River, NJ, USA ©2001.

Parra, A., Pérez, J., & Zhagui, L. (2007). *Análisis y Diseño de una Wireless LAN para la Empresa SIEETE D.C.* Recuperado el 4 de Enero de 2014, de Repositorio Digital - UPS : http://dspace.ups.edu.ec/handle/123456789/779

Plasencia, Z. (2010). *Introducción a la informatica (Guía practica)* (2010 ed.).

Plasencia, Z. (2013). *Introducción a la informática* (2013 ed.). ANAYA MULTIMEDIA.

Polanco, C., González, C., & Quintero, V. (2011). INTERFAZ PILOTO PARA LA INTEGRACIÓN DE BLUETOOTH Y RADIO MÓVIL. *Gerencia Tecnologica Informatica Vol. 10 Issue 26*, 15-25.

Rabago, J. (2010). *Guía práctica ANAYA MULTIMEDIA: Redes locales* (2010 ed.). ANAYA MULTIMEDIA.

Ramirez, J., & Lemus, M. (15 de Abril de 2013). *Diseño de un dispositivo localizador por medio de comunicación inalámbrica.* Recuperado el 4 de Enero de 2014, de Biblioteca Digital Universidad de San Buenaventura: http://hdl.handle.net/10819/1274

Serna, A., Ros, F., & Rico, J. (2010). *Guía práctica de sensores.* Creaciones Copyright SL.

Silberschatz, A., & Peterson, J. (1994). *Operating system concepts.* Addison-Wesley.

Stallings, W. (2003). *Fundamentos de seguridad en redes: aplicaciones y estándares.* Pearson Educación.

Stallings, W. (2007). *Network security essentials: applications and standards.* Prentice Hall.

Stallings, W. (2009). *Operating systems: internals and design principles, 6/E.* . Pearson Educación.

TecMikro. (Febrero de 2014). *Circuito integrado MAX232*. Recuperado el 15 de Febrero de 2014, de www.programarpicenc.com: http://www.programarpicenc.com/libro/cap10-usart-uart-microcontroladores-pic-max232.html

GLOSARIO

ANSI/SIA CP-01:	*American National Standards Institute/ Security Industry Association Control Panel-01*
AP:	*Access Point*
B/N:	Blanco/Negro
CMOS:	*Complementary metal-oxide-semiconductor*
CPU:	*Central Processing Unit*
DC:	*Direct Current*
DHCP:	*Dynamic Host Configuration Protocol*
DDNS:	*Dynamic Domain Name System*
DNS:	*Domain Name System*
ePTZ:	*Electronic Pan/Tilt/Zoom*
FET:	Facultad de Educación Técnica para el Desarrollo
Fps:	fotogramas por segundo
FTP:	*File Transfer Protocol*
HTTP:	*Hypertext Transfer Protocol*
HTTPS:	*Hypertext Transfer Protocol Secure*
IEEE:	*Institute of Electrical and Electronics Engineers*
IGMP:	*Internet Group Management Protocol*
IP:	*Internet Protocol*
IR:	*Infrared*
IRE:	*Institute of Radio Engineers*
ISM:	*Industrial, Scientific and Medical Bands*
LAN:	*Local Area Network,* Red de Área Local
LED:	*Light Emitting Diode*
MicroSD/SDHC:	*Micro Secure Digital /Secure Digital High Capacity*
MJPEG:	*Motion Joint Photographic Experts Group*
NAS:	*Network Access Server*
nMOS:	*n-type Metal-Oxide-Semiconductor*
NTP:	*Network Time Protocol*

PDA:	*Personal Digital Assistant*
pMOS:	*p-type Metal-Oxide-Semiconductor*
PPPoE:	*Point-to-Point Protocol over Ethernet*
QoS:	*Quality of Service*
RAM:	*Random-Access Memory*
RF:	Radio Frecuencia
RTCP:	*Real Time Control Protocol*
RTP:	*Real-time Transport Protocol*
RTSP:	*Real Time Streaming Protocol*
RTSP/RTP/RTCP:	*Real Time Streaming Protocol/ Real-time Transport Protocol/ Real Time Control Protocol*
SD:	*Secure Digital*
SDHC:	*Secure Digital High Capacity*
SDXC:	*Secure Digital Extended-Capacity*
SIU:	Sistema Integrado Universitario
SMTP:	*Simple Mail Transfer Protocol*
SNMP:	*Simple Network Management Protocol*
SoC:	*System-on-Chip*
S/R:	Señal/Ruido
TCP/IP:	*Transmission Control Protocol/Internet Protocol*
TTL:	*Transistor-Transistor Logic*
UCSG:	Universidad Católica de Santiago de Guayaquil
UL:	*Underwriters Laboratories*
UPnP:	*Universal Plug and Play*
USB:	*Universal Serial Bus*
WLAN:	*Wireless Local Area Network*
WPAN:	*Wireless Personal Área Network*
WPS:	*Wi-Fi Protected Setup*
W-USBE:	*Wireless* USB