UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO.

FACULTAD DE INGENIERÍA.

CENTRO DE DISEÑO Y MANUFACTURA.

"DISEÑO DE UN SISTEMA DE CONTROL DE ACCESO Y PROTECCIÓN DE EQUIPO".

TESIS PARA OBTENER EL TÍTULO DE INGENIERO
MECÁNICO ELECTRICISTA AREA ELÉCTRICA ELECTRÓNICA.

PRESENTAN:

Javier Cuahutle Ramírez
Gerardo Neri Roa.

DIRECTOR: Dr. Saúl Daniel Santillán Gutierrez. JULIO 2004

Índice.

Índice i
Agradecimientos v

Capítulo 1.

ANTECEDENTES E INTRODUCCIÓN 1
ANTECEDENTES 1
Funcionamiento del sistema de acceso del CDM 2
Planteamiento del problema 2
Análisis de los diversos sistemas de seguridad electrónica 3
Estudio de las instalaciones 10
Propuesta del sistema 13

Capítulo 2

OBJETIVO, ALCANCES Y RESOLUCIÓN DEL PROBLEMA 15
OBJETIVO Y ALCANCES 15
RESOLUCIÓN DEL PROBLEMA 16
Estrategia 16
Análisis por zonas 17
Análisis del edificio en general 18
Descripción de los niveles de seguridad 18
Modificaciones al edificio 20
Alternativas de diseño del sistema 23
Instalación 24

Capítulo 3.

SELECCIÓN DE DISPOSITIVOS 25
Selección de los sistemas de identificación 26
Selección de sensores 27
Selección de actuadores 29

Capítulo 4.

DISEÑO DEL SISTEMA 31
DISEÑO DEL HARDWARE 31
Elección de sensores y actuadores 31
Elección del protocolo de transmisión de datos 33
Elección de los dispositivos del sistema de protección de equipo 35
DISEÑO DE LAS ANTENAS DE BAJA FRECUENCIA 39
Elección de los dispositivos del sistema de acceso de personal 46
Ubicación de la antena de protección de equipo y lector de acceso de personal 47
Consideraciones a tomar en la integración final de los sistemas 48

DISEÑO DE LAS TARJETAS TAG-PC Y MODULO DE POTENCIA..... 49
Diseño de la tarjeta TAG-PC 50
Diseño del MODULO DE POTENCIA..... 53
DISEÑO DEL FIRMWARE..... 57
Descripción del firmware residente en el modulo TAG-PC..... 57
Subrutinas para recibir información..... 58
Lectura de sensores..... 59
Lectura del lector de acceso de personal..... 59
Habilitación/deshabilitación de actuadores 60
Subrutinas para enviar información 60
Subrutina de emergencia 60
Otra característica del firmware..... 61
DISEÑO DEL SOFTWARE PRUEBA INTEGRAL PARA LECTORES (PIL)..... 64
Prueba Integral para Lectores 66
DISEÑO DE SAPPE 73
Módulo de comunicaciones 73
Estructura del hardware del sistema 77
Integración del software y el hardware 81
Interfaz para base de datos 86
Interfaz para comunicaciones 92

Capítulo 5

INSTALACION Y PRUEBAS DEL SISTEMA..... 99
DETERMINACION DEL TIPO DE CANALIZACION 99
Canalización para la alimentación eléctrica 99
INSTALACION FISICA DEL SISTEMA 100
Instalación de las tuberías 100
Instalación de las puertas 100
Instalación de sensores y actuadores..... 100
Instalación de las antenas de baja frecuencia 102
Instalación de los transponders..... 102
Instalación de los registros..... 106
REALIZACIÓN DE LA PRUEBAS..... 117
Pruebas de operación de dispositivos..... 117
Pruebas con los TAG-PC y módulos de potencia..... 118
Pruebas preliminares de comunicación..... 119
Pruebas en la instalación..... 121
Pruebas de comunicación..... 121
Pruebas de lectura de sensores y activación / desactivación de actuadores con el programa PIL..... 121
Pruebas en el sistema de acceso de personal..... 122
Pruebas en el sistema de protección de equipos..... 122
Pruebas con el programa de aplicación SAPPE..... 123

Capítulo 6

ANALISIS DE RESULTADOS Y CONCLUSIONES..... 129
ANALISIS DE RESULTADOS..... 129
CONCLUSIONES 136

Apéndices

A. CONFIGURACION DEL SERIES 2000..... 141
B. GRABACION DE TRANSPONDERS DE ACCESO DE PERSONAL..... 149
C. GRABACION DE TRANSPONDER DE PROTECCION DE EQUIPO..... 155
D. PROTOCOLOS DE COMUNICACIÓN DE LECTORES..... 159
HOST PROTOCOL S6000..... 159
PROTOCOLO SERIES 2000..... 163
E. HOJAS DE ESPECIFICACIONES..... 171

Bibliografía

BIBLIOGRAFIA..... 195

AGRADECIMIENTOS.

A nuestro director de tesis Dr. Saúl Daniel Santillán, Gutiérrez, jefe del CDM, por su paciencia e interés en la terminación de la presente.

Al Ing. Serafín Castañeda Cedeño, responsable de la sección de electrónica del CDM, por su apoyo y asesoria para la realización del proyecto...

...pero muy por encima de esto último, por su invaluable amistad que nos ha brindado hasta hoy, la cual esperamos conservar por siempre...¡Gracias Serafo!

A nuestro compañero de tesis Javier García García, por su apoyo e inigualable y desinteresada amistad, además de sus ingeniosas ocurrencias, que nos hicieron más ameno el desarrollo del proyecto y la realización del presente trabajo.

A nuestras compañeras Gaby y Claus, por su amistad y compañerismo obtenida durante el proyecto.

A todos los que integran el CDM por su compañerismo y amistad otorgada durante nuestra estancia como integrantes de servicio social y después como tesistas.

A nuestra Alma Mater, la Universidad Nacional Autónoma de México, nuestra querida Facultad de Ingeniería, y nuestros compañeros de aula y profesores, que nos enseñaron a amar y ser orgullosos de nuestras raíces universitarias.

"QUE BIEN SABE LA VICTORIA, CUANDO YA NO HAY MUCHO QUE GANAR..."

Vince Lombardi.

In memoriam

A dos seres humanos que decidieron traer al mundo a su octavo hijo de nueve, por el cual se preocuparon y otorgaron el mismo amor y cuidado, como si hubiera sido el primero o último de la tribu.

Felisa Roa Santos.
Delfino Neri Martínez.

Que sin los valores inculcados, el amor a un Dios, la lucha y el empeño para enfrentar la vida aún en la agresiva tormenta de adversidades que todo humano tiene que enfrentar alguna vez en la vida; no deje de navegar hasta encontrar la luz de un sol de nuevas oportunidades con un cielo libre de nubes cargadas de contratiempos, preparándome ahora más fuerte para la siguiente tormenta.

Aquí les entrego queridos padres que viven en mi corazón y de mis hermanos, este trabajo, del cual ustedes fueron mi fuente de inspiración para no dejar de luchar, hasta verlo terminado.

Dedicatoria:

A mi hermana Irma que al sufrir la falta de nuestros padres, me dio un lugar donde descansar mi cabeza, un plato donde alimentarme, y un resguardo para cubrirme de la intemperie, gracias por tu apoyo, paciencia, llamadas de atención, preocupación y desvelo, producto de tu amor, bendita seas!

A mis hermanos: Irma, Pablo, Vic, Mario, Jorge, Tere, Maru y Laura así como a sus respectivas familias por el impulso que me dieron, viendo en cada uno de ellos a los autores de nuestras vidas y sentirnos orgullosos de nuestros apellidos.

A ti, que por temor a cometer la terrible descortesía de olvidar tu nombre, agradezco tu apoyo e impulso (a veces de una forma no muy amable y mucho menos constructiva) para continuar adelante.... sabes que me refiero a ti..

Y finalmente un agradecimiento a mi querido, estimado, amigo y compañero de tesis Javier Cuahutle Ramírez, con quien he tenido el gran privilegio y honor de realizar el presente trabajo, en verdad, pocos son los que pueden presumir de haber tenido un buen compañero de tesis, como el que el destino me otorgo contigo... gracias!

Gerardo Neri Roa.

Dedico este trabajo:

A ti señor, por que siempre has estado junto a mi, y me has dado la fortaleza y paciencia para seguir adelante.

Con un especial cariño a mis padres Cándida y Juan, por su apoyo, comprensión, paciencia y preocupaciones, además de sus llamadas de atención, por la oportunidad que me dieron de seguir estudiando y las facilidades para hacerlo, ya que sin ustedes no hubiese podido terminar la carrera, son muchas las cosas que les tengo que agradecer y que nunca terminaría de agradecérselos.

A mi hermano Saúl† que a pesar de tu carácter, siempre supiste ser un buen hermano y en los momentos malos siempre conté con tu apoyo y comprensión, y como decías "Más vale tardado pero seguro". Seguí ese ejemplo, y aquí esta plasmado en este trabajo.

A mis hermanas Leticia y Verónica que han soportado mi carácter y mis burlas, le agradezco el apoyo y comprensión que me han servido para poder ser una mejor persona y un mejor hermano.

A mis sobrinas Yolotzi y Yoali por darme su cariño sin pedir nada a cambio, a Michelle y Vanesa por su comprensión y cariño.

A Serafín que además de ser mi "jefecito" en el CDM, a demostrado ser un verdadero amigo.

A mis amigos Ana, Sergio, Verónica, Alfonso, Ignacio, Karla, Alejandra, Gerardo y en especial a Liliana por todo lo que pasamos durante la carrera.

A los amigos del CDM Chucho, Reyes, Alfredo, Daniel, Luis, Antonio, Sabrina y Guadalupe, que hicieron más amena mi estancia en las instalaciones.

A los "tigesito(a)s" por brindarme su amistad, su apoyo, por todas las cosas que hemos vivido juntos y que "jamás" voy a olvidar "cual debe" ser.

A Guadalupe por ser la persona especial que hacia falta a mi vida y llenármela de amor y de alegría, por tu apoyo y comprensión y me has enseñado a ver la vida desde otro punto de vista.

A todas aquellas personas que han estado a mi lado y que me han brindado su ayuda, su confianza, su amistad y su cariño.

Javier Cuahutle Ramírez.

"El reloj de arena, de estudiante en Ingeniería, esta a punto de dejar caer el último grano...
la hora de volar, que se retraso con mucho tiempo, ha llegado...
dejare tu cobijo, para buscar ser cobijo de otros...

Gracias Facultad de Ingeniería UNAM.

1

ANTECEDENTES E INTRODUCCIÓN.

ANTECEDENTES

Este trabajo surgió como una necesidad de modernizar el sistema de acceso de personal que se tenia en el Centro de Diseño y Manufactura (CDM), el anterior sistema usaba credenciales que al reverso tenían impreso un código de barras, este método tenia la gran desventaja que se podía falsificar fácilmente, haciendo la copia fotostática del código de barras y colocándolo en una superficie plana que pudiera ser deslizada por el lector, se podía tener acceso al CDM.

Otra desventaja que presentaba este sistema, era la unidad lectora de código de barras, ya que para poder dar acceso al CDM, se tenia que pasar dos o tres veces la credencial por dicha unidad, para que se tuviera una buena lectura del mismo, teniendo en consecuencia que el acceso fuera lento.

Se empezó a buscar algún sistema que ofreciera mayor seguridad, fuera más rápido y que los elementos que los conformara tuvieran más durabilidad, seguros y de un costo accesible.

La investigación nos llevo a los sistemas de **identificación por radiofrecuencia (RFID)[1],** los cuales ofrecían muchas ventajas, una era que por su forma de lectura no existe contacto físico entre la unidad lectora y el transponder[2], por lo que no sufren desgaste, como es el caso del sistema que se utilizaba anteriormente (código de barras), esta característica reduce de manera significativa errores en la lectura.

El sistema que esta actualmente trabajando en el CDM, es un control de acceso, basado en la tecnología (RFID), en la cual por medio del uso de credenciales, se hace dicha identificación.

---

[1] Radio Frecuency IDentification (RFID). Estos sistemas en particular de los que hablamos son de Texas Instruments, más adelante haremos referencia más extensa de ellos, por ser parte central en el sistema desarrollado.

[2] Transponder: Componente electrónico que contiene información (también llamado TAG).

Funcionamiento del sistema de acceso del CDM.

El usuario acerca su credencial (transponder) a la unidad lectora, la información contenida dentro de la credencial (código de identificación), es leída y enviada a la PC para ser validada en la base de datos con información de todo el personal del CDM, esta se encarga de validar dicha información, y decidir si se le permitirá o no, el acceso a las instalaciones.

De acuerdo a la lectura del código de identificación en la credencial, podemos saber quien es la persona a la que se le confió dicha credencial (profesor, académico, trabajador, prestador de servicio social o tesista), además de quedar registrada su hora de entrada y salida.

Por último, en el caso de robo o extravío de la credencial, se da de baja a la misma en la base de datos, así, si alguien quiere tener acceso con esta credencial, la computadora acciona una alarma sonora, avisando de que una persona intenta entrar con una credencial no autorizada.

Planteamiento del problema

Descripción del problema.

Teniendo en cuenta que el campus universitario es una zona abierta, el control adecuado de personas propias y extrañas en algunas áreas dentro de la universidad y en particular dentro de la Facultad de ingeniería es a veces muy difícil.

En los últimos años los ilícitos en la Facultad de Ingeniería de la UNAM se han incrementado de manera significativa, estos robos se presentan de diferentes maneras:

- Material bibliográfico en las bibliotecas.
- Equipo de los diferentes laboratorios con que cuenta la Facultad, como equipos de medición (osciloscopios, multímetros) y herramientas.
- Equipo audiovisual (cañones de proyección, proyectores).
- Equipo de computo (desde la desaparición de un mouse, hasta la desaparición del equipo completo).
- Vehículos particulares y de la universidad dentro del campus universitario.
- Y algunos otros que no hemos contemplado aquí.

Todas estas pérdidas son muy dolorosas, como es el caso de equipos de computo, donde la información contenida en ellas, es producto de investigaciones que se han llevado mucho tiempo en obtener, existe también el caso que dentro de las computadoras se colocan tarjetas de adquisición de datos, donde el costo de dicha tarjeta supera por mucho el valor de la misma y que decir del acervo bibliográfico con que cuenta nuestra casa de estudios.

Posibles consecuencias si no se soluciona el problema.

Al ser la universidad una institución publica, sus recursos se obtienen principalmente del gobierno federal y cada año, el presupuesto que se le destina ya no es suficiente para cubrir sus necesidades, por lo que podría sufrir cada vez más con la pérdida de recursos materiales o humanos, en consecuencia, la universidad se verá obligada a

destinar fondos adicionales para reponer estos, entorpeciendo así sus actividades de investigación y enseñanza.

Por lo que es necesario, proponer soluciones al problema de seguridad en la comunidad universitaria y en particular en la Facultad de Ingeniería, para un mejor desarrollo en un ambiente de seguridad para la comunidad y al mismo tiempo contar con el material que se requiere para las investigaciones, actividades docentes y administrativas.

Presentación de la necesidad de realizar el sistema de seguridad.

Para intentar reducir los problemas de inseguridad, se han implementado varias medidas de seguridad, tales como tener más personal de vigilancia, en la entrada de algunos de los edificios que tiene esta Facultad donde se tiene equipo costoso (laboratorios de computo, audiovisuales, etc.), como en los estacionamientos, la adquisición de vehículos que patrullen las instalaciones, de equipo de radio comunicación, la colocación de protecciones o rejas para protección de los inmuebles.

El contar con más elementos de vigilancia en la universidad, no parece ser una solución muy eficiente, ya que se incrementaría el numero de trabajadores en la institución esto implica, el aumento en la nomina de pago, por ejemplo.

Por lo anteriormente descrito, se planea el diseño e implementación de un sistema que contribuya a mantener la seguridad dentro de las instalaciones de la Facultad de Ingeniería. El prototipo funcional de este sistema será instalado en el algún edificio de la FI.

El sistema a implantar deberá de verificar el acceso del personal a las áreas de este edificio (control de acceso), e impedir la sustracción indebida del equipo que ahí se tiene, y de cuidar las instalaciones cuando no haya gente laborando dentro de las mismas (protección de equipos y contra intrusos).

Dado que la delincuencia es cada vez más especializada en diversos delitos, el sistema a diseñar será con tecnología de punta, económico y en gran medida autónomo, capaz de contribuir al resguardo de los bienes en el edificio.

Análisis de los diversos sistemas de seguridad electrónica.

En la actualidad existen una gran variedad de sistemas de identificación y controles de acceso comerciales, los costos de dichos sistemas varían dependiendo del grado de seguridad que se quiera tener en las instalaciones donde será colocado el sistema, al hablar de nivel de seguridad nos referimos a que tan fáciles son de violar o burlar, o en un momento dado que tan fácil puede ser, el falsificar u obtener información para poder entrar a las instalaciones.

Los sistemas electrónicos de acceso: son sistemas orientados a la seguridad en entradas o salidas de algún establecimiento o empresa, estos sistemas se utilizan también para llevar el control (entrada/salida) o existencia de algún objeto.

Sistemas de identificación.

Los sistemas de identificación por medios electrónicos que encontramos fueron los siguientes:

- Código de barras.
- Banda magnética.
- Biométricos.
- Radiofrecuencia.

En estos sistemas, encontramos que todos cuentan con opción de comunicación por puerto ethernet o serial, además de capacidad de usar una base de datos. Las características principales de los sistemas se presentan en la tabla 1.1.

Características del sistema.	Código de barras	Banda magnética	biométricos	Radiofrecuencia (RFID)
Lugar donde se coloca la información.	Impresas en una etiqueta.	Se ubica en la cara posterior de una tarjeta con material magnético similar al de las cintas de audio o video.	Es alguna característica morfológica de la persona	Se coloca en dispositivos llamados transponder que son leídos por radiofrecuencia.
Codificación de la información.	Consiste en una serie de barras negras y espacios en blanco de diferentes anchos.	La información es magnéticamente codificada en la banda.	La información sobre alguna característica fisiológica es digitalizada y almacenada en la computadora.	Se encuentra codificada en un chip o circuito de memoria dentro del transponder, capaz de ser leída.
Aplicaciones comunes.	Préstamo de material bibliográfico, identificación de productos y control de tiempo y asistencia.	Tarjetas de crédito, licencias de conducir, documentos de identidad de instituciones gubernamentales o privadas.	Estas tecnologías se usan generalmente para aplicaciones de control de acceso y seguridad.	Se usa principalmente para identificación de productos inanimados o seres vivos.
Seguridad de la información.	En este sistema es fácil de duplicar la información, al fotocopiar el código de barras	Actualmente en México se han reportado casos de clonación de tarjetas.	La seguridad es casi del 100% al ser partes del cuerpo de una persona la información.	La seguridad es de casi del 90% al ser los transponders de código único en algunos casos[3].
Desgaste del sistema	El desgaste se encuentra en la unidad lectora y el dispositivo a leer.	El desgaste se encuentra en la unidad lectora y el dispositivo a leer.	El desgaste se encuentra en la unidad lectora.	El desgaste es casi nulo al no haber contacto entre la unidad lectora y el dispositivo a leer.

Tabla 1. 1: Tabla comparativa de los diferentes sistemas de control de acceso.

[3] Existen transponder de solo lectura que tienen un código único e irrepetible, y otros de lectura y escritura al los que se les puede asignar el código, aquí, el sistema es vulnerable si se tiene el equipo para conocer el código.

Identificación por Radio Frecuencia (RFID).

RFID, es un método electrónico que asigna un código de información a un producto, proceso o persona y usa esta información para identificar o tener acceso a información adicional al respecto, consisten de un "chip" o circuito con memoria de datos, capaz de ser leído y escrito sin contacto, vía ondas de radio con el uso de antenas.

Los sistemas de identificación por radio frecuencia consisten generalmente de dos componentes:

1. El "transponder" que esta de alguna manera unido al elemento a ser identificado y
2. El lector que detecta la identidad del "transponder".

La tecnología del transponder se basa en la aplicación de un transmisor/receptor, el lector genera un campo magnético cuya señal de RF es captada por el receptor del "transponder". Este a su vez, activará al transmisor, el cual enviará un mensaje codificado único. Este mensaje es decodificado por el lector y enviado a una PC, donde es almacenado.

Clasificación de los transponder de RFID:

Activo / Pasivo: Un transponder **activo** usa baterías, esto hace que la distancia de lectura sea grande en comparación a los pasivos. Un transponder **pasivo,** emplea la energía recibida de la antena lectora para transmitir sus datos, esta característica hace que los "transponders" **pasivos** sean de menor costo, más pequeños y con una vida teóricamente indefinida; aunque con una distancia de lectura más corto.

Solo lectura / Lectura-escritura: Una transponder de solo lectura ha sido grabado "de fabrica", o previamente en su primer uso con un código de identificación único, que no podrá ser cambiado. Los transponder de lectura-escritura, ofrecen la habilidad de poder grabar en ellos diferentes códigos, además de otra información de interés para el administrador del sistema y por lo tanto son aplicables para requerimientos de información variable.

Existe una amplia variedad de aplicaciones de esta tecnología:

- Control de maquinas herramientas, inventario, activos, desechos tóxicos...
- Identificación de líneas de tuberías, de animales, de personas, vehículos robados, de antigüedades...
- Monitoreo de líneas de producción, de parqueo de vehículos...
- Producción de carrocerías.
- Análisis de aguas.
- etc.

La siguiente generación de esta tecnología son las llamadas **tarjetas inteligentes**; mientras que en los sistemas RFID, los "transponders" en su interior tienen una memoria, las tarjetas inteligentes tienen en su interior un microprocesador capaz de hacer diferentes cálculos, guardar información y manejar programas, que están protegidos a través de mecanismos avanzados de seguridad.

Este tipo de tarjetas, pueden ser utilizadas para aplicaciones que requieren altos niveles de seguridad, Una ventaja que tienen estos sistemas sobre los dos anteriores, es que estos pueden ser leídos a mayor distancia, sin que tengan contacto físico con el lector.

Alarma contra intrusos

De los sistemas de alarmas contra intrusos que se investigaron, encontramos que han contribuido a reducir la cantidad de robos y hurtos producidos en empresas y comercios, presentando la ventaja directa de la seguridad que brinda a las personas y sus bienes. La mayoría de estos sistemas se pueden encontrar como:

Sistemas monitoreados: Son aquellos sistemas de que en caso de que se active una alarma, la central envía un mensaje a través de la línea telefónica (incluso hay algunos sistemas que se comunican vía Internet), a una estación central de vigilancia, que funciona las 24 horas del día. Enviando personal de seguridad para revisar dichas instalaciones y resguardarlas en caso de un intento de robo (ver figura 1.1).

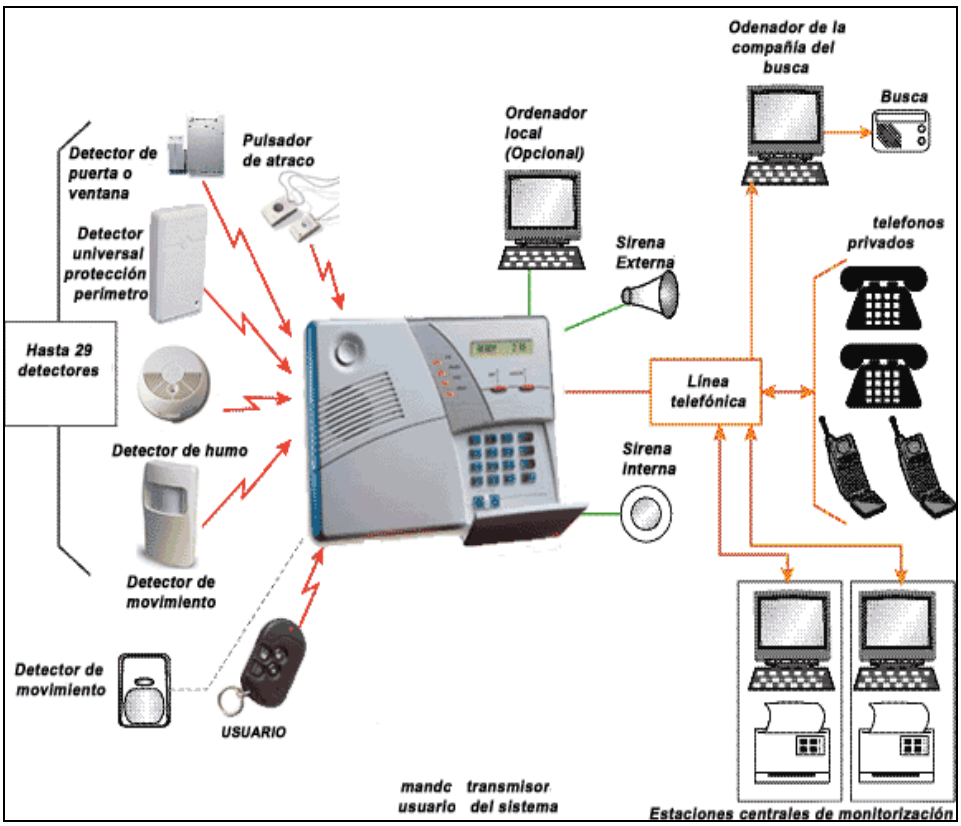


Figura 1. 1: Sistema de alarma contra intrusos comercial.

Sistemas sin monitoreo: típicamente, poseen alarmas en el lugar y/o luces destellantes que indican que el sistema de seguridad ha sido violado. Y depende de un responsable quien se hará cargo de revisar las instalaciones, desactivar la alarma y ponerse en contacto con la policía.

Pueden contener los siguientes elementos:

- Central de alarma.
- Batería y cargador.
- Consola de activación/desactivación.
- Alarma.
- Avisador telefónico.
- Botones de pánico/asalto
- Sensores (infrarrojos, microondas, ruptura de vidrio, sonido etc.)

En ciertos modelos comerciales, algunos de estos elementos se encuentran debidamente integrados dentro de la central de alarma. A continuación se presentan las características más destacadas de cada tipo de elemento.

Central de alarma: la central de alarma es la parte medular del equipamiento, ya que es el elemento que se encarga de controlar automáticamente el funcionamiento general del sistema de alarma, recogiendo información del estado de los distintos sensores y accionando eventualmente los sistemas de aviso de la presencia de intrusos en el área protegida.

La central en sí es una tarjeta electrónica con sus distintas entradas y salidas, que se encuentra resguardada en un gabinete con protección antidesarme, el que generalmente también incluye la batería y su cargador.

Las centrales se clasifican de acuerdo a la cantidad de zonas independientes a proteger, por lo que podemos encontrar productos de 2 zonas, 6 zonas, 16 zonas, etc. Cada zona puede ser activada y desactivada en forma individual, lo cual permite que en el lugar donde sea instalado podamos proteger las áreas que no tienen presencia humana prevista y deshabilitar la protección en aquellas zonas ocupadas o en uso.

Asimismo, se suele incorporar un retardo de activación de la alarma en al menos una zona (zona temporizada), para dar tiempo a que pueda desactivarse el sistema, al ingresar gentes autorizadas al lugar.

Sin embargo, esto no es necesario en los casos en que se dispone de un control remoto por ondas de radio.

Batería y cargador: Estos elementos sirven para proveer un sistema de alimentación eléctrica sin interrupción (UPS), de manera que ante una falta del suministro eléctrico de red (normal o provocado por un ladrón), el sistema de alarma contra intrusos continúe brindando protección en forma absolutamente normal.

Panel de activación / desactivación: Este panel habitualmente contiene un teclado que permite programar todas las funciones del sistema. Esta interfase de control cuenta con teclas alfanuméricas, que tiene otras funciones de señalización de estados, por lo que constituye una pieza importante para el usuario del sistema.

Existen señalizadores de dos tipos, los de led o luces, y también los de pantalla de cristal líquido. En ambos casos brindan información de cada una de las zonas que están conectadas (áreas de protección exterior, puertas, ventanas, áreas interiores, etc.).

También existen modelos en que se dispone un control remoto por ondas de radio codificadas, que permite la activación / desactivación de la central, y eventualmente puede accionar las sirenas y hacer llamados telefónicos en caso de asaltos.

Alarma**:** El elemento de alarma está formado generalmente por una sirena que advierte que alguien sin autorización fue detectado por el sistema, mediante una señal sonora de alto nivel. En algunos casos, también puede incluir algún tipo de señalización visual, luces destellantes (flash) o señales luminosas, para aquellas personas que tienen problemas de audición o cuando existe un alto nivel de ruido ambiental.

La sirena exterior se coloca dentro de un gabinete para su protección, y se instala en la fachada de la casa, comercio o industria a proteger. Además de su función de alertar en los casos en que se ha detectado un intruso, la sirena exterior es un elemento disuasivo de por sí, ya que advierte de la existencia de un sistema de alarma instalado en el domicilio.

Por otro lado, la sirena interior sirve para actuar como auxiliar de la sirena exterior, de manera que las dos sirenas suenen al mismo tiempo. Si el intruso destruye la sirena exterior, queda funcionando la sirena interior dentro del lugar protegido.

En todos los casos, estas sirenas emiten un sonido de unos 120 decibeles (equiparable al sonido de una ambulancia) y tienen una protección antidesarme que envía una señal a la central, en los casos en que se pretenda sabotear su correcto funcionamiento.

Para determinar el tipo de alarma a instalar debe tenerse en cuenta algunos factores como el nivel de ruido ambiental, el tipo y calidad del sonido ambiental, la duración de la señal requerida, el nivel acústico deseado y la alimentación eléctrica disponible.

Por ello, para su correcta instalación hay que tener en cuenta la presencia de fuentes de sonido en los locales a proteger, como por ejemplo equipos de aire acondicionado, sistemas estereofónicos, televisores, etcétera, que eventualmente impidan la audición de las sirenas de alarma.

Informador telefónico: En los sistemas de alarma más modernos, también se suele instalar un elemento que ante la ocurrencia de una anormalidad, efectúa un llamado al número telefónico programado previamente. Este llamado puede incluir un mensaje de voz grabado en una memoria no volátil o ser simplemente una secuencia de tonos característicos (bip-bip).

Botones de pánico/asalto: Estos dispositivos de seguridad contra asalto deben ser colocados estratégicamente y de manera oculta, cerca de cajas registradoras, mostradores, baños, cajas de seguridad, armarios, etc. De tal manera que al momento del asalto se puedan presionar los botones correspondientes en forma disimulada, para enviar una señal a la central de alarma, que ordene una acción de respuesta silenciosa, como por ejemplo la ejecución de un llamado telefónico o la activación de una señal luminosa en el puesto central de vigilancia.

Sensores: Los sensores se fabrican con diversas técnicas que operan bajo principios de funcionamiento diferentes.

En la mayoría de los casos se dispone de un elemento sensor que analiza la alteración de alguna magnitud física. Esta alteración es detectada por un circuito electrónico asociado que opera un contacto normalmente cerrado o normalmente abierto, que al cambiar de estado, envía la información de su estado a la central, la que acciona la alarma acústica y/o lumínica del sistema, para advertir la presencia de intrusos en el ambiente en que se halla instalado.

Estos sensores deben ser cuidadosamente seleccionados en función del tipo de alteración a identificar, para evitar falsas alarmas (ver tabla 1.2). Por lo general, el detector está concebido para dar una rápida advertencia a un costo razonable, de manera que brinda un oportuno preaviso. Esta advertencia sólo es posible si el sensor está correctamente localizado, instalado y mantenido.

Los sensores no pueden dar aviso si el intruso no atraviesa el campo de acción de ellos. Por ello es aconsejable instalar sensores, en los lugares estratégicos como puertas, ventanas, balcones, bardas, teniendo cuenta las condiciones ambientales del lugar (limpieza, trafico de personas, animales o insectos).

Hay sensores que funcionan en forma autónoma, pues poseen su propia sirena y batería, formando una pequeña central completa que brinda protección aún cuando se interrumpe el suministro de energía, siempre que la batería esté cargada y correctamente instalada.

Sensor	Principio de funcionamiento	Forma de actuarlos	Lugares de uso.	Comentarios
movimientos infrarrojo pasivo (PIR)	Detecta la señal infrarroja emitida por los cuerpos ubicados dentro de su campo de acción.	Sensa los movimientos que se producen de cuerpos calientes.	En lugares cerrados, no es tan eficiente en alguna zonas al aire libre, con ráfagas de aire	Alcance de 10m a lo largo y de 6 m de alto, con ángulo de cobertura de 90º a 180º
dual-tech (doble tecnología) Infrarrojo-microonda.	Además del funcionamiento del PIR. Al ser interrumpida la señal por una persona o animal, la señal regresa más rápido y el sensor detecta la anormalidad	Solo si la parte de microondas y la parte de infrarrojo detectan una anormalidad en su área de cobertura se activa el sistema.	En lugares cerrados y abiertos.	Es uno de los más confiables en la actualidad, ya que son dos sensores en uno.
Ultrasonido.	Se basa en el efecto doppler	Resulta similar al componente de microondas.	En zonas al aire libre	Resulta efectivo donde no lo son otro tipo de sensores
Ruptura de cristal.	Es un detector de frecuencias.	Detecta la frecuencia que produce la ruptura de cristal, mediante un micrófono.	En lugares como ventanales, puertas de o con recepción, se coloca en techos o paredes.	Su cobertura es de $4m^2$
Barrera infrarroja.	Trabaja por la transmisión y recepción de rayos infrarrojos	Detecta la presencia de un intruso al ser interrumpidos los rayos infrarrojos.	En lugares donde se tenga que cuidar una entrada.	
Contacto magnético	Se compone de dos partes que forman un circuito cerrado que forman un circuito cerrado con switch magnético.	Si alguien abre el circuito, alejando el imán, se da aviso al controlador.	Se coloca en ventanas o puertas, que al alejar el imán abre el circuito.	Existen dos tipos básicos, el normal y el oculto.

Tabla 1. 2: Tabla comparativa de sensores más empleados.

Una vez definido algunas de las características de las diferentes tecnologías de identificación y seguridad se hará una descripción del lugar que se quiere proteger

Estudio de las instalaciones

Se hicieron varias visitas a los laboratorios de la FI, en donde se implantaría el sistema, en una de estas visitas que se hicieron a las instalaciones, el responsable del laboratorio nos comento sobre su interés de tener protegidas cuatro áreas del edificio.

El edificio consta de dos plantas y cuenta con un total de cinco áreas, cada una de ellas es independiente una de la otra, viendo el edificio de frente podemos distinguir cada una ellas, por lo que nosotros las nombramos como:

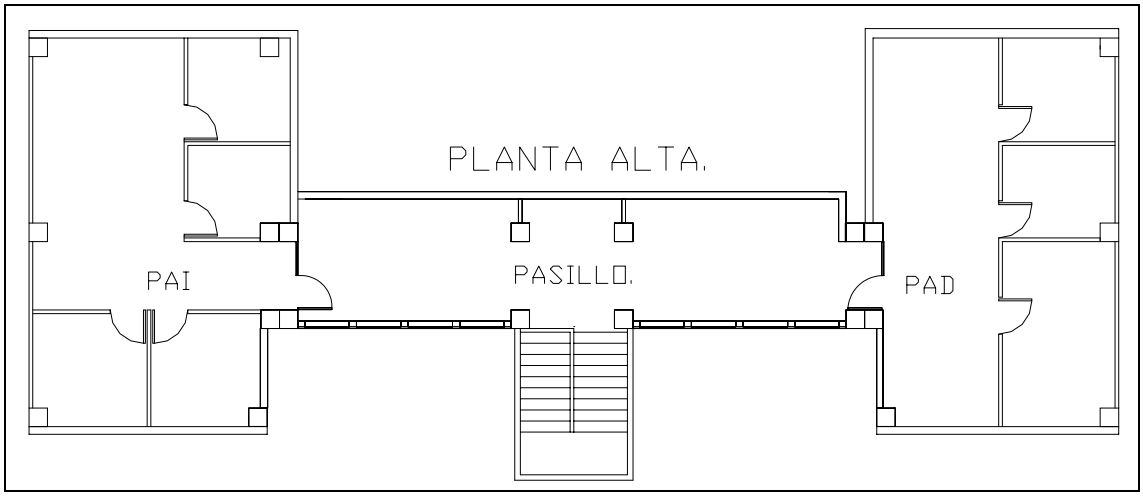
- Planta Alta Derecha PAD (plano 1.1).
- Planta Alta Izquierda PAI (plano 1.1).
- Planta Baja Derecha PBD (plano 1.2).
- Planta Baja Izquierda PBI (plano 1.2) y
- Planta Baja Central PBC (plano 1.2).

Las áreas a controlar son PAD, PAI, PBD y PBI.

Planta alta.

Funciones: Aquí se ubica la parte administrativa de los laboratorios, se encuentra la jefatura y se tienen además cubículos para los profesores y alumnos que están desarrollando alguna investigación o tesis (de licenciatura o posgrado), se cuenta también con una sala de cómputo. Asimismo algunos de ellos tienen en su interior tarjetas o dispositivos para adquisición de datos, el costo de dichos dispositivos superan por mucho el costo del equipo que los contiene.

Características físicas: La planta alta cuenta con dos áreas: PAD, PAI, (ver plano 1.1), se localizan subiendo las escaleras que terminan en medio de un pasillo de 18 m. que comunica a las dos áreas, este pasillo tiene dos ventanales de 8.5 x 1.5 m., en ambas áreas existen cuatro ventanas de aproximadamente 0.5 x 0.5 m. Sin protección y con una altura al nivel del piso de 8 m.



Plano 1. 1: Planta alta sin modificaciones.

Trafico de personal: Dado que en la planta alta se encuentra el área administrativa (PAD), existe un flujo constante de gente que entra y sale de esta área, en su mayoría son alumnos que van en busca de algún profesor, de la misma forma, hay transito constante entre las áreas PAD Y PAI. Las personas no tienen que registrarse para ingresar a cualquiera de las áreas, solo dirigirse a alguna de ellas, tocar la puerta si esta cerrada y entrar.

Protección: La única protección contra intrusos que se tiene, es una reja metálica ubicada al inicio de la escalera para subir al siguiente nivel, que se cierra con un candado en los días y horas no laborables, las puertas que tienen doble cerradura se mantienen cerradas, en la mayoría de las veces con seguro. Sin embargo en las horas de comida, algunas veces las instalaciones se encuentran vacías, propiciando que si no se puso el seguro de la cerradura en alguna de las puertas, se pueda ingresar a ellas fácilmente.

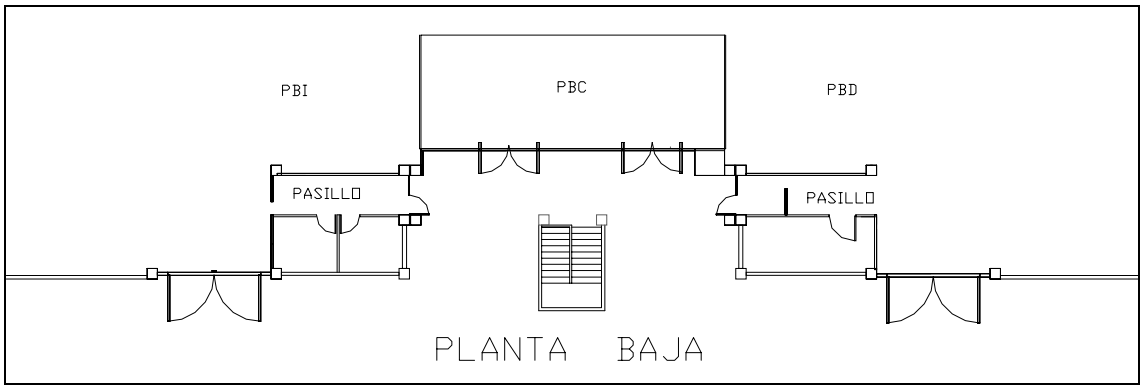
Planta baja.

Funciones: El área de PBD cuenta con el equipo especialmente diseñado para llevar a cabo los experimentos básicos de los cursos de las áreas académicas en los laboratorios.

El área de PBI, tiene como objetivo principal el poder llevar a cabo los proyectos de investigación básica y aplicada que sirvan para lograr una aportación al conocimiento en las área de investigación.

Por último el área de PBC, tiene como objetivo principal desarrollar proyectos de desarrollo e innovación tecnológica en otra área de investigación.

Características físicas: Puesto que el área de PBI y el área de PBD tiene características similares, solo haremos referencia al área de PBI, haciendo las diferencias, cuando así sea pertinente.



Plano 1. 2: Planta baja, antes de colocar el sistema **.**

El área de PBI y PBD (ver plano 1.2), cuenta con dos accesos, una entrada principal que da acceso a un pasillo de 6 m., en el cual, al final de este se encuentra una reja metálica (en el área de PBD esta reja se encuentra a la mitad del pasillo) que permite la entrada al área de los laboratorios. El segundo acceso es una puerta de 2.5 x 2.5 m.

Existen cuatro ventanas de aproximadamente 0.5 x 0.5 m., a una altura de 2 m., sobre el nivel del piso con protección que comunican al exterior de los laboratorios, dentro de estas áreas, se encuentran unas ventanas que comunican con la planta alta, estas ventanas tiene una altura de 6 m. del nivel del piso.

En el área de PBI, en el pasillo se ubican los baños y un almacén que solo tienen un acceso sin ventanas, también encontramos dos áreas acondicionadas para tomar clases dentro del laboratorio.

En el área de PBD, en el pasillo, se tiene un cuarto y en su interior se tiene una subestación eléctrica y un compresor, dentro de la PBD existe un almacén y un aula para el alumnado.

En el área de PBC, se tienen dos portones de 2.5 x 2.5 m., para ingresar a esta área.

Trafico de personal: para ingresar a la PBD se tiene que tocar un timbre para que el encargado abra la puerta, ciertos días y horas de la semana la puerta permanece abierta por que en este laboratorio se realizan la mayoría de las practicas, por lo que existe mucho movimiento dentro de esta área, se nos comento, que se ha llegado a perder algún equipo en la instalación.

Aun cuando el área de PBI, este destinada para los profesores, también ahí se realizan practicas, aunque no tan frecuentes como en el área de PBD, el flujo de gente es por que se encuentran ahí los baños. Si no se tiene llave, hay que ir a avisarle al encargado del área de PBD para que abra la puerta.

Protección: A parte de que las puertas principales tienen doble cerradura, las rejas metálicas que se encuentran en los pasillos para entrar a los laboratorios de la PBD y la PBI se cierran con un candado, los portones que existen en estas áreas son cerradas también con un candado.

Al igual que la planta alta, no se tiene un registro del flujo del personal que ingresa a las áreas, además del riesgo de que los candados se pueden abrir y sustraer equipo de los laboratorios.

Conclusiones.

Nos dimos cuenta de que el acceso dentro de las instalaciones era relativamente fácil, ya que no se tenia un control de la entrada y salida del personal al edificio, por lo que seria fácil de sustraer equipo en algunas zonas del recinto.

La vigilancia de la instalación es llevada a cabo por personal de auxilio-UNAM ya fuera por vigilantes a pie o en patrullas, pero esta se presta en ciertas horas (rondines), dejándose a solas el edificio durante algún tiempo, es decir, no había una vigilancia constante del lugar.

Una parte que consideramos vulnerable dentro de la planta alta, son los ventanales que se encuentra en el pasillo, también que las puerta metálica al ser cerrada con un candado este puede ser abierto con relativa facilidad.

La importancia relevante de las áreas de la planta baja a proteger es que, se tiene equipo muy importante tanto por su valor comercial como académico.

Propuesta del sistema.

En base a lo estudiado, se hicieron varias propuestas, entre las cuales se decidió por la siguiente:

Un sistema que estaría dividido en tres pequeños subsistemas:

- control de acceso.
- protección de equipos.
- alarma contra intrusos.

Control de acceso.

El sistema será capaz de dar o restringir el acceso al personal en cualquiera de las cuatro áreas protegidas, por medio de horarios y días en las que el personal podría hacer uso de las instalaciones llevando un registro. Así como también saber si una persona quiso entrar en un área que para el no esta autorizada, y llevar un control en donde sabríamos el día, la hora y cuantas veces intento entrar.

Dicho sistema daría la facilidad de hacer los cambios pertinentes en los horarios, días y áreas de acceso.

Protección de los equipos

Se pondrá especial atención en la protección de equipo que el responsable de laboratorio considere importante. Los equipos podrán ser movidos de su lugar sin ninguna restricción dentro del área en donde se este resguardando el equipo, pero solamente podrán salir del área siempre y cuando lo autorice el responsable del área en cuestión.

Cuando un equipo salga del área sin autorización el sistema tomara las medidas necesarias para impedir la salida del equipo protegido y dará aviso al personal y administrador del sistema de que esta ocurriendo un intento de robo por medio de algún medio sonoro.

Protección contra intrusos.

Contara con algunos sensores que se activaran durante la noche y desactivándose durante el día, en días no laborables dichos sensores se activaran todo ese tiempo, otro tipo de sensores se usaran, para proteger los ventanales que tienen estas instalaciones, estos estarán activos las veinte y cuatro horas del día.

Para proteger los accesos principales, se colocaran sensores, encargados de dar aviso si una de las puertas o accesos que se tienen en el laboratorio esta abierta, todo el sistema tendrá respaldo de energía eléctrica en caso de suspensión del suministro principal. También se buscaran medios para dar acceso a personas que no laboran en el laboratorio.

Tanto el sistema de control de acceso de personal de equipo y el sistema de protección contra intrusos, serán controlados por una computadora con un software diseñado expresamente para ello.

2

OBJETIVO, ALCANCES Y RESOLUCIÓN DEL PROBLEMA.

OBJETIVO Y ALCANCES:

El objetivo del presente trabajo es reportar, el diseño e implantación del prototipo de un sistema de control de acceso a personal y protección de equipo, que fue instalado en un edificio de la FI.

El sistema propuesto cumple con necesidades propias de la Facultad, en cuestión de seguridad y se basa principalmente en:

1) Controlar el acceso a personas ajenas a las instalaciones.
2) Resguardar las instalaciones de la Facultad.
3) Proteger y resguardar el equipo con el que se cuenta.

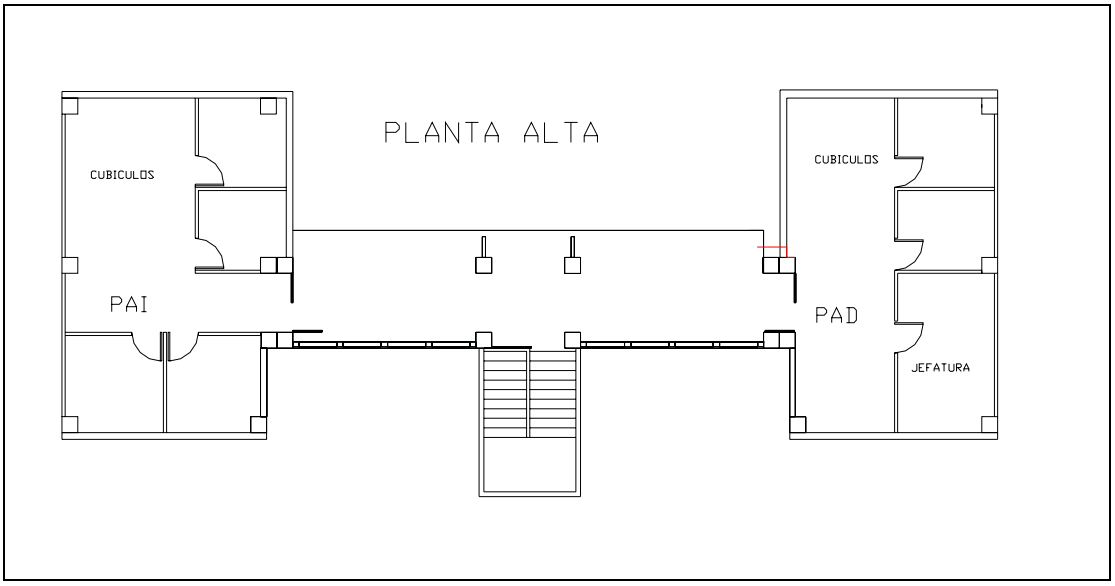
El prototipo será de arquitectura abierta, es decir, que sea una plataforma en la cual se pueda hacer crecer el sistema, haciéndole innovaciones que lo hagan cada vez más eficiente.

Se quiere desarrollar e implementar un sistema de protección diferente a los que se ofrecen en el mercado, ya que estos sistemas se concretan a un solo tipo de protección, es decir, existen sistemas que solo se dedican a protección contra intrusos, (por ejemplo en casas u oficinas los cuales protegen bienes materiales, en centros comerciales donde se protege ropa, equipos electrónicos, discos compactos), o sistemas de control de acceso (donde se utilizan para este fin, cámaras de circuito cerrado de TV, credenciales de código de barras o de banda magnética, Teclado de acceso etc.).

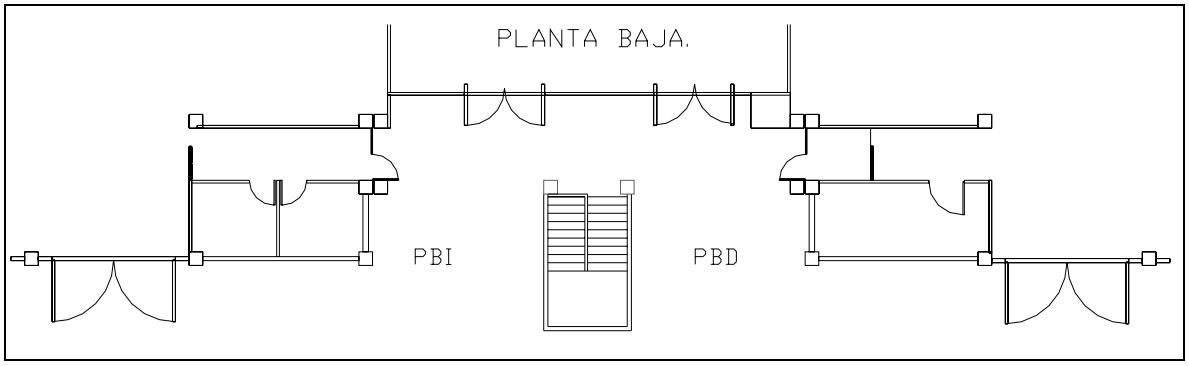
Nuestro diseño contempla la integración de los sistemas de protección comerciales, con sistemas de identificación RF, de tal forma que este sistema puede ir creciendo dependiendo de las necesidades del usuario, ya que se le pueden ir adicionando nuevos dispositivos de protección por ejemplo sensores de humo, barreras infrarrojas o adicionar nuevas áreas de protección.

Resolución del problema.

Después de haber hecho el análisis de las instalaciones del edificio, se localizaron los lugares sensibles (o vulnerables) del edificio y con la ayuda de los planos arquitectónicos (ver plano 2.1, plano 2.2), comenzamos hacer la planeación y ubicación de los dispositivos, así como señalar las modificaciones pertinentes que se le harán al inmueble.



Plano 2. 1: planta alta sin modificaciones.



Plano 2. 2: planta baja sin modificaciones.

ESTRATEGIA

El sistema ha sido concebido en tres niveles de seguridad:

- Nivel 1: acceso de personal y protección de equipo.
- Nivel 2: sistema de protección contra intrusos.
- Nivel 3: Sistema contra eventos.

Cabe señalar que para el nivel 3, solo se han sentado las bases para implementarlo. Es decir, que el sistema tendrá la capacidad de hacerle las adaptaciones necesarias para alcanzar este último nivel de seguridad.

Para entender la situación que imperaba en el edificio y detectar los problemas de seguridad, se hizo un análisis por área de las zonas a proteger y después uno del edificio en lo general, para proponer los niveles de seguridad necesarios.

Análisis por zonas

Se presenta una tabla donde se observa el análisis de la situación por zona y el problema que presenta.

ZONA	SITUACIÓN	PROBLEMAS
PAD y PAI.	En esta zonas esta el área administrativa, una sala de computo (PAD) y cubículos destinados a profesores del área en donde cada cubículo se encuentran también equipos de computo (PAD y PAI), continuamente se reciben visitas de propios y extraños, en horas de comida la zona se encuentra desierta, hay ocasiones en que algún investigador se encuentra después del horario de trabajo o trabajan en vacaciones o sábados y domingos.	En las áreas no se tiene un registro de las personas que ingresan a las instalaciones, a que hora ingresan y a que hora salen en cual de las áreas se encuentran, si estuvieron en las instalaciones los días laborables y en que horario.
PBD y PBI.	Hay horarios del día en que la zona PBD se encuentra con mucha gente dentro, por la realización de prácticas, sin embargo, la mayoría del día se encuentra solo el encargado de la zona, en la zona PBI que esta destinada a los investigadores y parte del día se encuentra sin ninguna persona dentro de ella, en ambas instalaciones se encuentra equipo de trascendencia académica y docente importante	No se tiene un registro del personal que entra a las instalaciones, siendo crítico el horario en que se realizan prácticas docentes dentro de la áreas y cuando se encuentran totalmente desiertas, ya que podría facilitar el robo de algún equipo importante dentro de las zonas

Tabla 2. 1: Análisis por zonas del edificio.

De la tabla 2.1, observamos que las zonas de la planta alta (PAD y PAI), presentan problemas del control del personal que ingresan a estas zonas, por lo que la solución propuesta es un sistema de acceso de personal.

En la planta baja (PBD y PBI), el problema principal que se presenta es el cuidado del equipo que se encuentra dentro de las zonas a proteger, además de que el control del personal a ciertas horas del día hace la situación más crítica, por lo que se propone además de un sistema de acceso de personal, un sistema de protección de equipo.

En conclusión en las cuatro áreas, se propone implementar un nivel de seguridad 1, esto quiere decir que en la planta alta además del sistema de acceso de personal, se colocara también el sistema de protección de equipo.

Análisis del edificio en general.

Las zonas de acceso para ingresar al edificio son:

- Para ingresar a la planta alta, hay que subir por unas escaleras, pero antes se encuentra una reja metálica que se cierra con un candado, al estar ya en la planta alta para ingresar a cualquiera de las zonas, las puertas se encuentran cerradas con doble cerradura.
- Para ingresar a la zona PBD (los mismos accesos se encuentran en PBI), se cuenta con dos accesos, un portón de doble hoja de 2.5 x 2.5m., que se encuentra cerrado con un candado por dentro, y el acceso principal que es una puerta de doble hoja que tiene doble cerradura, pasando esta puerta se encuentra una reja metálica que se cierra con un candado.
- Para ingresar a la zona PBC existen dos portones de doble hoja de 2.5 x 2.5m., que cuentan con cerraduras para ingresar a la zona.

Los puntos vulnerables del edificio son los accesos, principalmente los que contienen candados, ya que estos son muy fáciles de abrir, los portones podrían abrirse sin avisar al responsable, otro punto vulnerable son los ventanales existentes en el pasillo de la planta alta, pues podría romperse un cristal de este ventanal.

Durante las horas o días en que no hay labores dentro del edificio las instalaciones son vigiladas por AUXILIO UNAM en rondines que se hacen a ciertas horas, por lo que hay momentos que se encuentran sin vigilancia, ya que no existe un vigilante de planta en el edificio.

Dado que es importante proteger las áreas contra intrusos en las horas en que el edificio no se encuentre en horas laborables, se propone como solución colocar un sistema nivel de seguridad 2 que contempla un sistema de alarma contra intrusos que trabajará parcialmente en las horas laborables y en las horas o días que no haya actividades estará funcionando totalmente.

Es primordial señalar que, dado que es un sistema de acceso y protección (de equipo y contra intrusos), nos hemos concentrado en la protección de las puertas de acceso, ventanas y pasillos que hay en las cuatro áreas.

Descripción de los niveles de seguridad

Nivel 1: Sistema de acceso de personal

El sistema de control de acceso a personal propuesto, estará colocado en las puertas principales de las cuatro áreas.

Se utilizarán credenciales para realizar la identificación, al personal que ahí labora se les proporcionara una credencial que contendrá la fotografía, nombre y el cargo que desempeña.

Los datos recibidos por el lector serán enviados a una PC. La PC validara esta información, comparándola con su base de datos y mandara una señal para que pueda o no ingresar dentro de las instalaciones.

La base de datos generara la siguiente información:

- El registro de acceso por áreas, horario y día.
- Todas las entradas y salidas que el usuario haya hecho por área autorizada, día y hora.
- Los intentos de ingreso a zonas no autorizadas o fuera del horario establecido.

Puesto que en las áreas de la planta baja son áreas donde se imparten clases, el sistema dará acceso sin alguna restricción en los horarios y días en que el administrador del sistema designe, restringiendo el paso fuera de estos horarios, sin embargo el sistema de protección de equipo continuara funcionando.

Nivel 2: Sistema de protección de equipo

Aun cuando se puso especial interés en los equipos de la planta baja (PBI y PBD), también se pensó en proteger el equipo contra robo de las áreas de la planta alta.

El sistema de protección de equipo, controlara la entrada y salida de equipos que son de mayor interés para el edificio de laboratorios. Los equipos a proteger se les implantara un identificador de acuerdo a las características físicas del equipo. Con el código del identificador que el equipo contenga, se tendrá registrado en una base de datos la siguiente información:

- La descripción del equipo.
- Ubicación.
- Responsable.
- Autorización de salida del equipo de la zona.

El dispositivo lector estará colocado en la entrada principal de cada área, pero a diferencia del lector de acceso de personal, este se mantendrá oculto.

Sistema de protección contra intrusos.

Como ya se menciono al principio de este capítulo el sistema se concentrara en las puertas, pasillos y ventanas.

En los pasillos de las cuatro áreas se colocaran sensores, de tal manera que detecten la entrada de intrusos al área controlada en ciertos horarios definidos por el sistema, se activaran solo cuando no haya labores dentro de la zona en la que se esta controlando.

Las puertas principales y los portones de las áreas de la planta baja (PBI, PBC Y PBD), contaran con otro tipo de sensores que detecten cuando una puerta se encuentra abierta. En las puertas principales se hará uso de una cerradura que se activara o desactivara de forma remota, además cada puerta contara con un interfono para que puedan preguntar por alguien que labore dentro del área, y si fuera el caso, se le de acceso desde el aparato de interfono.

En la planta alta, se pondrán sensores para proteger los ventanales, estos sensores estarán activados las veinticuatro horas del día. En cuanto a las ventanas que se encuentran en la planta baja, estas se encuentran protegidas con canceles metálicos internos, por lo que no se considera poner alguna protección adicional.

Nivel 3 Sistema contra eventos.

A sabiendas de que el nivel de seguridad 3, no se ha contemplado en este proyecto, se han tomado en consideración algunas acciones para este fin. Se usaran dos tipos de alarma sonoras con sonidos diferentes, para cada una de las cuatro zonas a controlar, serán llamadas alarma general y alarma local respectivamente.

La alarma general se activara:

- Cuando hay un intento de extracción de equipo de alguna zona controlada sin autorización previa.
- Se ha detectado la entrada de algún intruso en la zona en que se activo la alarma.
- Se ha roto alguna ventana exterior o de la puerta principal de acceso a la zona restringida.

En la zona donde se ha registrado el incidente, la puerta se mantendrá cerrada hasta que la alarma haya sido desactivada.

La alarma local se activara en los siguientes casos:

- La puerta se ha mantenido abierta más de lo necesario después de dar acceso a algún usuario.
- Se accionó un botón de emergencia local.

Se instalará una botón de emergencia en cada una de las áreas controladas, en caso de que un botón de emergencia sea activado, se abrirán todas las puertas de acceso principal, pero el sistema de protección de equipo seguirá funcionando normalmente.

También se colocara un interruptor en la puerta, por el lado exterior, para que en caso de fallo en la cerradura de acceso, esta se deshabilite y permita el libre acceso, que al igual que en el caso anterior, el sistema de protección de equipo se mantendrá activo.

Un último aspecto a considerar, es el de usar respaldo de energía para el sistema en general, en caso de la suspensión de suministro de energía de la línea principal, que permitirá que el sistema continué funcionando.

Modificaciones al edificio.

Dándonos cuenta de que la mejor forma de protección es la de prevención y en cierta forma desalentar al intruso potencial, se tomaron la siguientes medidas:

Planta alta.

Se colocara una reja al final de la escalera y puertas de doble hoja nuevas en cada área, la característica de estas puertas, es que en una de las hojas estará una ventana pequeña para tener contacto visual con la persona que pide el acceso, además contendrán los lectores de acceso de personal y el interfono; otro punto a destacar es que en el marco estará oculto el lector del sistema de protección de equipo (figura 2.1).

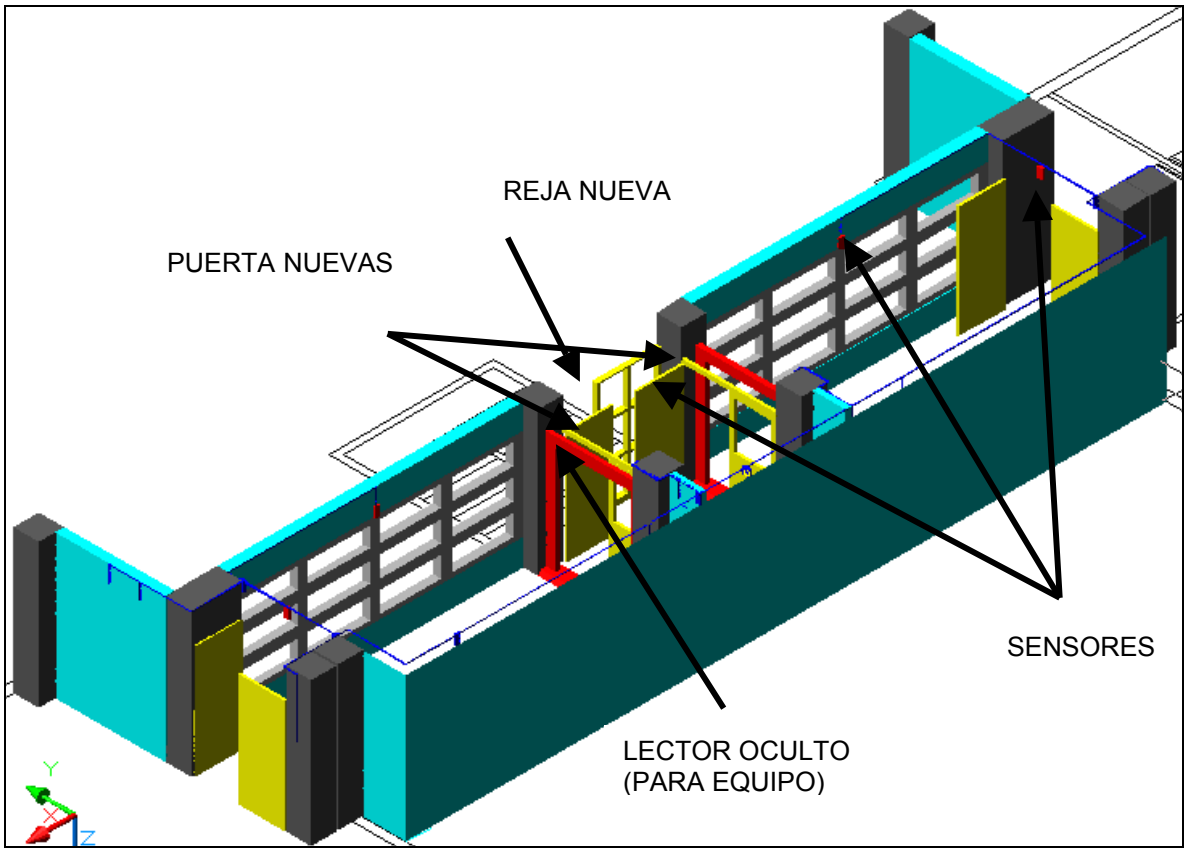


Figura 2. 1: Planta alta con modificaciones.

Planta baja.

En el área PBD se conservara la reja metálica que se encuentra en la mitad del pasillo, la puerta nueva de doble hoja se colocara en el final del mismo pasillo, colocando en una de las hojas de la puerta el lector del sistema de control de acceso y dentro del marco de la puerta el lector del sistema de protección de equipo (ver figura 2.2).

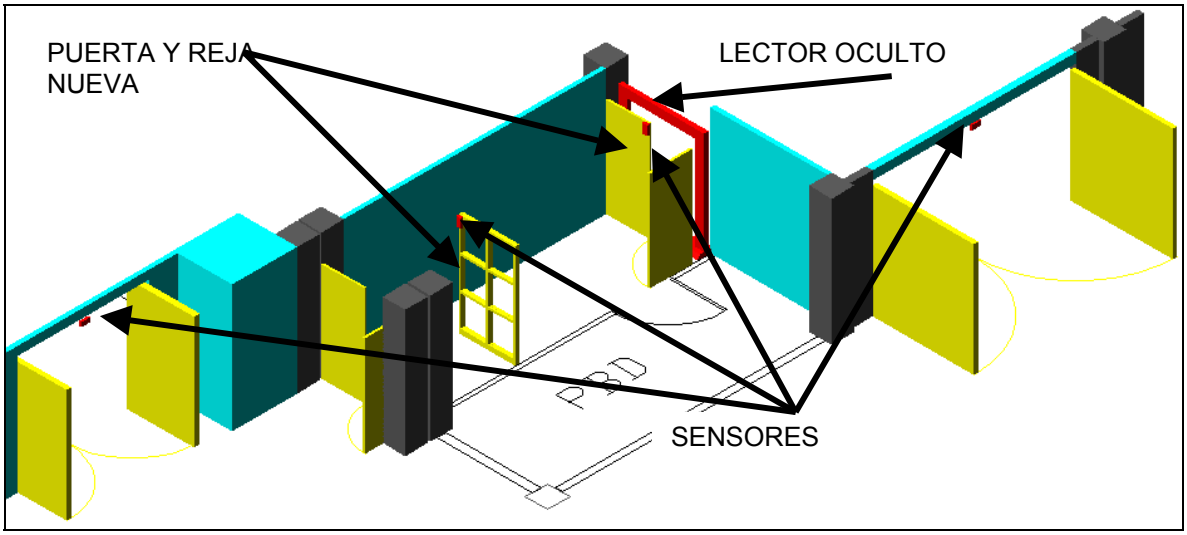


Figura 2. 2: Planta baja (PBD) con las modificaciones.

En cuanto al área de PBI se colocaran una nueva puerta con las mismas características de la PBD, solo que la reja que se encontraba la final se colocara más adelante (ver figura 2.3).

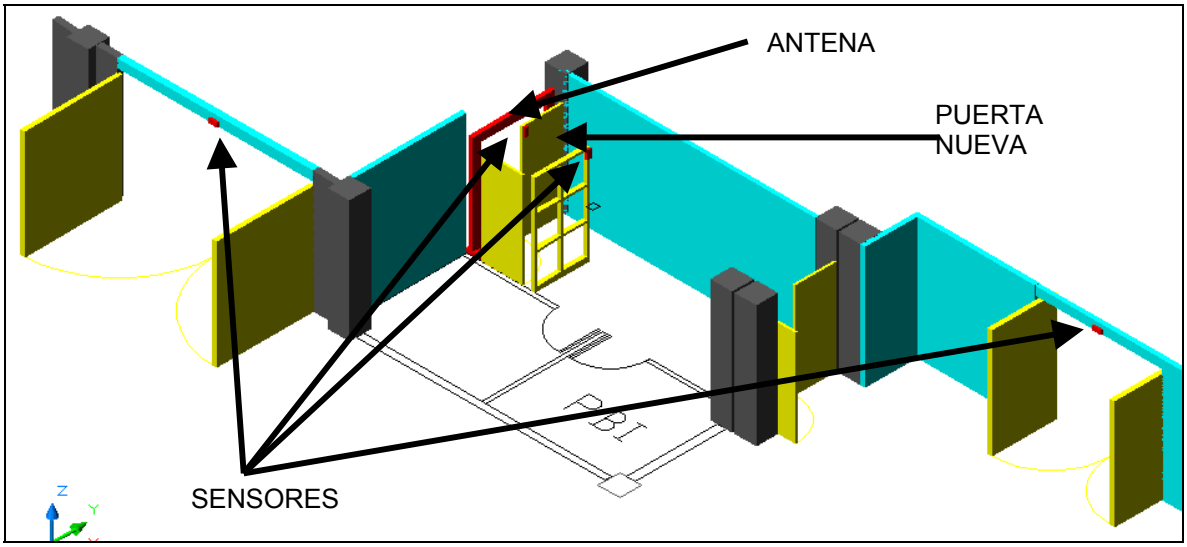


Figura 2. 3: Planta baja (PBI) con las modificaciones.

Software

Todo el sistema completo (acceso de personal, protección de equipos y alarma contra intrusos) será controlado por una computadora dedicada a este fin, el software que se vaya a utilizar, será diseñado por otro grupo de colaboradoras del mismo proyecto.

Este software tendrá por función controlar cualquier dispositivo que este conectado a la computadora (lectores, sensores y actuadores), también dentro de esta misma, se tendrán el nombre de los poseedores de una credencial de acceso, así como de los equipos que se protegerán con el sistema.

Una de las características de este programa, es que en su base de datos se encontraran registrados los eventos que se presenten en ese día, por hora, fecha y dispositivo, también se podrán activar y desactivar la mayoría de los dispositivos involucrados e incluso un sistema completo, dará permiso de salida de equipos de alguna zona de control, todo esto lo controlara un administrador del sistema.

Alternativas de diseño del sistema.

Alternativa 1.

Se pensó en desarrollar una tarjeta de control que seria capaz de tener comunicación y control con: lectores RFID de acceso de personal y protección de equipo, sensores y actuadores del sistema de alarma contra intrusos en las cuatro áreas a proteger, asimismo dicha tarjeta de control tendría comunicación con la PC (control maestro), y estaría colocado dentro de un gabinete con un respaldo de energía (diagrama 2.1).

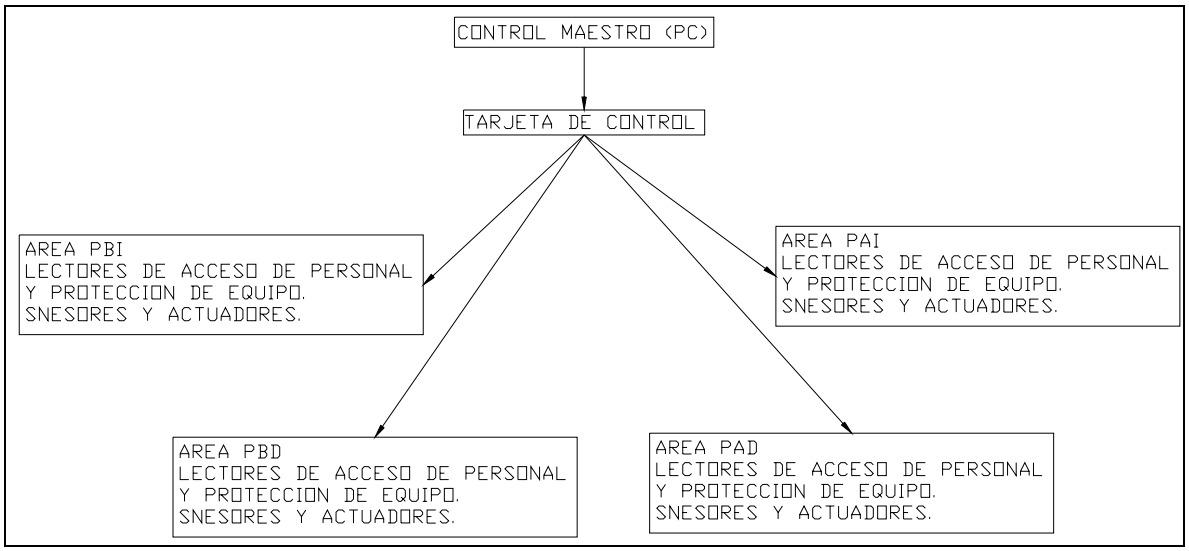


Diagrama 2. 1: alternativa de diseño1.

El gabinete se colocaría en la mitad del pasillo de la planta alta, con el fin de tener distancias proporcionales con cada una de las áreas.

Sin embargo encontramos alguna deficiencias en esta forma de conexión

- Al tener el gabinete instalado a la mitad del pasillo, hacia más vulnerable al sistema pues tenia el riesgo de ser desactivado o saboteado.
- La tarjeta de control tendría la limitante de tener un numero finito de elementos a controlar, si se requería adicionar más dispositivos no seria posible.

Alternativa 2.

Se concibe el sistema en forma modular, es decir, un modulo que controle el lector de protección de equipo, y módulos en cada área protegida, que controlen los lectores de acceso de personal, sensores y actuadores. Esta forma de diseñar el sistema nos daría la posibilidad, de anexarle más dispositivos al sistema y un mejor mantenimiento de los mismos (diagrama 2.2).

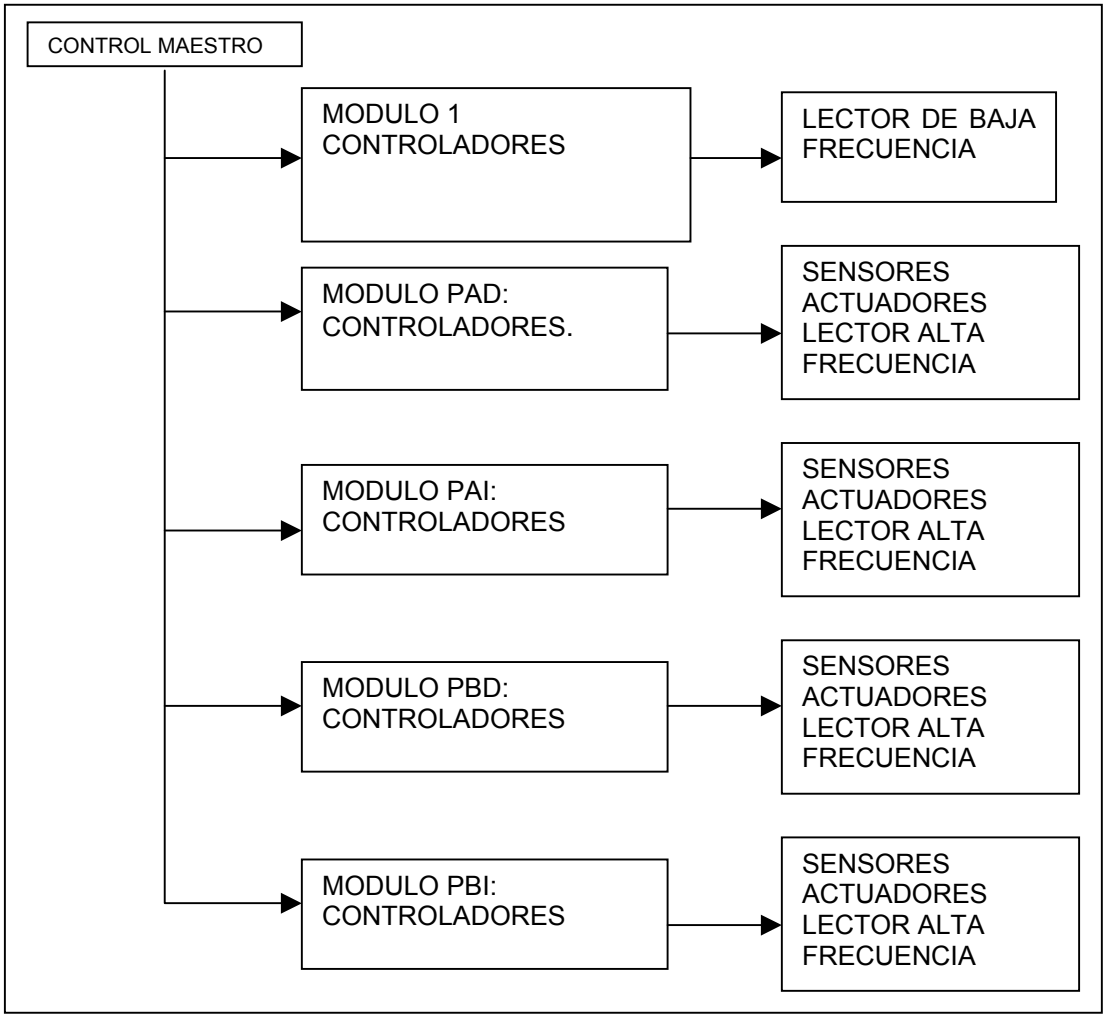


Diagrama 2. 2: diagrama a bloques de la alternativa 2.

Instalación.

Se pondrá una instalación independiente de todas las demás, con tubería nueva, incluso para la alimentación, esto es con el fin de que no exista interferencia con las instalaciones ya puestas anteriormente, se usaran cajas metálicas con uso exclusivo del sistema, además la computadora que se este usando, estará dedicada exclusivamente para el sistema.

3

SELECCIÓN DE DISPOSITIVOS.

En este capitulo se muestra la selección de los dispositivos que se utilizaron. Estos debían de cumplir la mayoría de las características.

- Costo inicial.- El valor del dispositivo, incluyendo su instalación.
- Costo de operación.- Es el costo adicional que se genera en capacitación en el uso de equipo o sistema que se vaya a emplear
- Costo de mantenimiento.- que tan caro (dinero) nos cuesta su mantenimiento y los tiempos en la cual se aplica.
- Disponibilidad.- si es posible que haya distribuidores en México, y en particular en el distrito federal, tiempo de entrega.
- Que tanta **seguridad** existe en la información enviada y recibida, en su calibración etc.
- **Velocidad** en la respuesta, ante un evento.
- La **flexibilidad** que tiene con la forma de **comunicación** entre el dispositivo y su controlador .
- La alimentación del dispositivo, para este caso debe de ser 12Vdc.

La selección se hizo usando un método tabular de asignación de factores de ponderación, (ver tabla 3.1), se tomaron en consideración la características mas sobresalientes de cada dispositivo a evaluar, de acuerdo a nuestros parámetros de diseño, cada factor se comparo en forma subjetiva, asignándole un peso de 50 a 100 [D.R. Sule, instalaciones de manufactura].

Selección de los sistemas de identificación.

FACTORES		SISTEMAS DE IDENTIFICACIÓN			
		RFID	BIOMETRICOS	BANDA MAGNETICA	CODIGO DE BARRAS
COSTO	Inicial	80	60	100	100
	De operación	80	90	80	70
	Mantenimiento	100	90	80	80
Disponibilidad		100	90	100	100
Seguridad		90	100	70	60
Velocidad de respuesta		100	80	90	90
Comunicación		100	100	100	100
Flexibilidad		100	000	50	80
TOTAL		**750**	610	670	680

Tabla 3.1: Selección del sistema de identificación.

En la tabla 3.2, se muestra el mismo método de selección de los sistemas de identificación de RFID con el tipo de transponder que usan, para decidir que tipo de transponder se iba a ocupar:

		FACTORES										
		COSTO										
		Inicial	operación	Mantenimiento	disponibilidad	distancia de lectura	velocidad	Vida útil	Flexibilidad	Información técnica	Frecuencias diferentes	TOTAL
RFID	Transponder pasivo	100	100	100	100	70	100	100	100	100	100	970
	Transponder activo	100	100	100	90	100	100	90	90	80	70	900

Tabla 3. 2: Selección del transponder en sistemas RFID

De las tablas 3.1 y 3.2 anteriores se tienen las siguientes conclusiones:

- Se utilizaran los sistemas de identificación por radiofrecuencia, por que se puede utilizar para identificar tanto para personal como para equipo.
- En comparación con los sistemas de identificación biométricos el costo de los sistemas RFID son menos costosos.

- Los sistemas RFID en comparación con los sistemas de identificación por banda magnética y código de barras son mas difíciles de falsificar.
- Al utilizar transponders activos (utilizan baterías), Las distancias de lectura se incrementan, pero son más caros y los transponders tienen una vida útil de cinco años, en cambio los transponders pasivos son mas baratos y tienen una vida útil mínima en promedio de 10 años.

El sistema de identificación RFID se va a usar tanto para control de acceso de personal, como de protección de equipo, serán de dos frecuencias diferentes para cada sistema, las razones fueron la siguientes:

- El área de la antena lectora para los sistemas de baja frecuencia (protección de equipo), dependiendo de la unidad lectora puede ser hasta 200 x 200 cm., en el caso de los sistemas de alta frecuencia esta área es de 20 x 20 cm[1].
- Los lectores de baja frecuencia no tienen la capacidad de leer mas de dos transponder a la vez, por lo que por seguridad se hace uso de un lector de diferente frecuencia para el control de acceso.

Selección de sensores

Dada la variedad de dispositivos para sensores que se podían ocupar para el cuidado de los pasillos de las áreas controladas, y detectar la entrada de intrusos, para tomar una decisión de cual ocupar (ver tabla 3.3), se uso también el método tabular de asignación de factores de ponderación, los sensores evaluados, son los ya comentados en la tabla 1.2 del capitulo uno de la presente tesis .

Para seleccionar un sensor que nos indicara cuando la puerta había sido abierta, encontramos que se podía hacer uso de dos sensores que se evaluaron en la siguiente tabla.

Factores	Sensor magnético.	Barrera de infrarrojos.
Costo inicial	100	70
Costo de mantenimiento	100	90
Disponibilidad	100	100
Velocidad	90	100
Seguridad	100	90
Comunicación	100	100
Alimentación	100	100
Cobertura de detección	100	100
Total	**790**	750

Tabla 3.3: sensores considerados para la protección de apertura de puertas.

Los sensores magnéticos se utilizarán para detectar que las puertas, estén cerradas o abiertas, ya que su costo es muy inferior con respecto a la barrera de infrarrojos, además de que ofrecen mayor seguridad contra sabotajes al poderlos ocultar dentro de la puerta y los marcos.

[1] Es de especial interés para nosotros, ya que se decidió tener oculto el lector de protección de equipo por razones de seguridad.

Para la protección del espacio abierto de los pasillos, se consideraron los siguientes dispositivos (ver tabla 3.4):

	PIR	Dual Tech	Ultrasonido	Barrera de infrarrojos.
Costo inicial	100	60	70	80
Costo de mantenimiento	100	90	90	90
Disponibilidad	100	80	80	100
Velocidad	90	100	100	100
Seguridad	80	100	90	60
Comunicación	100	100	100	100
Alimentación	100	100	100	100
Cobertura de detección	80	80	80	50
Total	**750**	710	710	680

Tabla 3. 4: Selección de dispositivos para el espacio de los pasillos.

De la tabla anterior encontramos que si bien es cierto que los sensores de movimiento Dual Tech y los sensores de ultrasonido son de mayor seguridad que los PIR o los de barrera de infrarrojos, son mas caros, mientras que los de barrera de infrarrojos, su cobertura de detección para el espacio de los pasillos es muy limitado, por lo tanto el sensor de movimiento PIR, es el que más se ajusta a nuestras necesidades.

El sensor PIR (sensor de movimientos por infrarrojos) estará colocado para proteger el espacio de los pasillos al detectar el movimiento de personas, el dispositivo que se eligió tiene un ángulo de detección de 90 grados, y la cobertura de detección de este dispositivo es de 15m x 12m.

Los sensores considerados para la protección la ventana del pasillo y de la puerta, fueron los de sensor de ruptura de cristal y de barrera de infrarrojos (tabla 3.5).

	Sensor ruptura de cristal	Barrera de infrarrojos.
Costo inicial	100	60
Costo de mantenimiento	90	90
Disponibilidad	100	100
Velocidad	90	100
Seguridad	80	100
Comunicación	100	100
Alimentación	100	100
Cobertura de detección	100	100
Total	**760**	750

Tabla 3.5: sensores considerados para la protección de apertura de puertas.

De la tabla anterior observamos que el total es muy parecido, y aun cuando el la barrera de infrarrojos es mas segura, no es la mejor para nuestro proyecto, ya que con un solo sensor de ruptura de cristal, podemos proteger, al mismo tiempo la ventana del pasillo y de la puerta, mientras que con la barrera de infrarrojos, necesitaríamos dos, uno para la ventana del pasillo, y otro para la puerta.

El sensor de ruptura de cristal se utilizará para la protección del área de los ventanales y de la ventana que tiene una de las hojas de las puertas de la planta alta, al ser los pasillos un espacio cerrado, estos dispositivos tendrán un mejor desempeño, ya que estos detectaran la ruptura de un vidrio, se eligió un sensor de ruptura de cristal con área de protección de 12 m^2.

Para la planta baja, donde no hay ventanas, solo se consideraron los sensores de movimiento y los magnéticos.

Selección de actuadores.

Cerradura.

El cierre y apertura de las puertas, será en forma remota, los dos tipos de cerradura que encontramos en el mercado, fueron electromagnéticas y electromecánicas la característica entre una y otra, es que la cerradura electromecánica es muy parecida a una cerradura puramente mecánica, incluso pueden ser abiertas con una llave convencional, mientras que las cerraduras magnéticas, solo pueden ser abiertas en forma eléctrica.

Se decidió utilizar una cerradura electromagnética ya que esta es muy confiable, existen de diferentes capacidades de carga 300 Lb. (136 Kg.), 600 Lb. (272 Kg.) y 1200 Lb. (545 Kg.), son silenciosas y requieren un costo de mantenimiento casi nulo, así como de una vida útil muy alta a diferencia de las cerraduras electromecánicas.

Alarmas

Las alarmas que se usaron fueron de dos tipos, y habrá dos por zona controlada,

La alarma local, será un vibrador con un sonido de mediana intensidad, que tendrá la función de avisar cuando alguna de las puertas de la zona controlada se encuentre abierta mas del tiempo especificado.

La alarma general de alta intensidad que se usara para avisar, cuando se encuentre una situación de robo de equipo, o salida indebida de este.

Por último, tenemos los interfones, dentro del mercado, encontramos de diferentes tipos, de entre los cuales elegimos los de un timbre y dos teléfonos, asimismo cuentan con un botón para abrir la puerta desde cualquiera de los teléfonos.

4

DISEÑO DEL SISTEMA.

Este capítulo se dividirá en tres partes que son:

1. Diseño del Hardware: tratara sobre el diseño de dos tarjetas electrónicas, una tarjeta de control a la que hemos denominado TAG-PC y otra más a la que hemos denominado ETAPA DE POTENCIA y diseño de las antenas lectoras del sistema RFID de identificación de equipos.
2. Diseño del software: explicaremos el funcionamiento del programa Prueba Integral de Lectores (PIL), que fue un programa diseñado para realizar las pruebas del sistema y, el programa SAPPE[1], que es la aplicación final, que será la que administre el sistema.
3. Diseño del firmware: en esta parte explicaremos sobre el diseño del programa residente en el microcontrolador que se encuentra en la tarjeta de control TAG-PC.

DISEÑO DEL HARDWARE

Elección de sensores y actuadores.

Dentro de la gran diversidad de marcas de dispositivos que se encontraron en el mercado, elegimos los que cumplieron con la mayoría de los siguientes requerimientos (ver tabla 4.1):

- Voltaje de operación de 12VDC.
- Alámbricos.
- Bajo consumo de corriente.
- Con suficiente información y soporte técnico.
- Disponibilidad del equipo en el distrito federal y entrega inmediata.
- De precio accesible y garantizados.
- Buena calidad y presentación.
- Comunicación serial (lectores de RFID).

[1] SAPPE : Sistema de Acceso a Personal y Protección de Equipos, software desarrollado en el Centro de Diseño y Manufactura, FI, UNAM, registrado ante derechos de autor ISBN 970-32-0446-5.

Dispositivo	Marca y modelo[2]	Consumo corriente (mA).	Voltaje de operación (V).	Característica	Ubicación.
Sensor movimiento tipo PIR	IntelliSense IS-150	20 mA a 12VDC	10-14 DC	Rango de protección. 15 m x 12 m. relevador de alarma forma A (NC).	En los pasillos de cada área (figura 4.1 y 4.2).
Sensor Ruptura de cristal	IntelliSense Flex Guard	25mA a 12VDC	10-14 DC	Rango de protección 9 m. relevador de alarma forma C (NC o NA).	En los ventanales de la planta alta (figura 4.2).
Sensor magnético.			10-14DC	Sensor de tipo oculto. La forma de operar de este dispositivo, nos permite utilizarlo como un relevador de forma A (NC).	En las puertas principales de control de acceso de cada área (figura 4.1 y 4.2). En la planta baja también se colocarán en los portones (figura 4.1).
Cerradura magnética.	ENFORCER E-941SA-600	500 mA a 12VDC	12-24DC	Fuerza de retención. 272Kg. (600 Lb.)	En las puertas de control de acceso de cada área (figura 4.1 y 4.2).
Interfon.	Commax DP-RA01	1.14mA	127 AC	Distancia cuarto a cuarto 30m.	Timbre a la entrada de cada área. Teléfonos dentro del área.
Sirena para alarma general.	System sensor PA400	12mA a 12VDC	9.6-33 DC	Sonido de 90 dBA a 12 VDC.	Dentro del área, a un lado de la puerta de control de acceso.
Sirena para alarma local.	Steren BGD10	8mA a 12VDC	1.5-16 DC	Sonido de 85dB.	Dentro del área, a un lado de la puerta de control de acceso.

Tabla 4. 1: Dispositivos seleccionados con algunas de sus características propias.

En las figuras 4.1 y 4.2 vemos la ubicación de los sensores y actuadores en la planta baja. y la planta alta

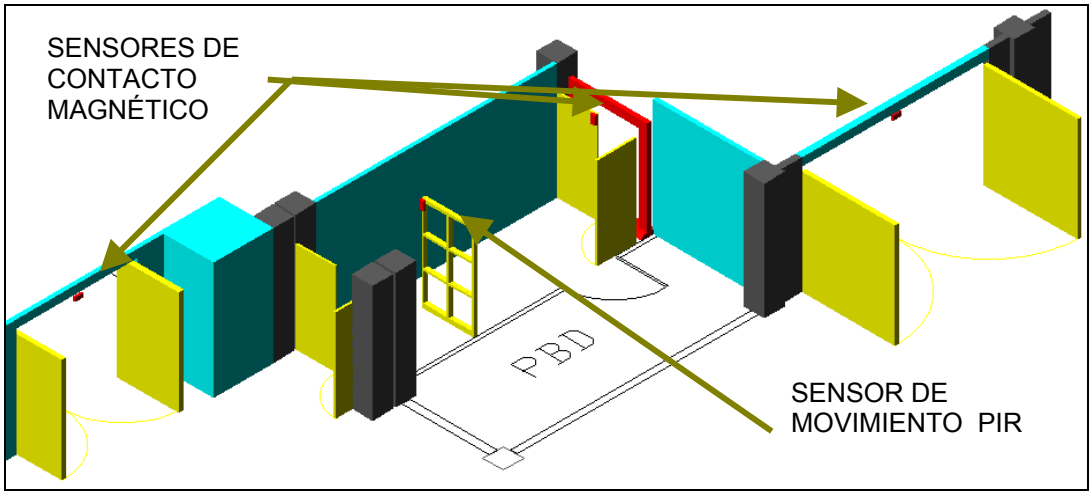


Figura 4.1: Área PBD ubicación de los sensores.

[2] Para conocer las características más detalladas de los dispositivos usados en la tabla, referirse al apéndice "hojas de especificaciones de los sensores y actuadores"

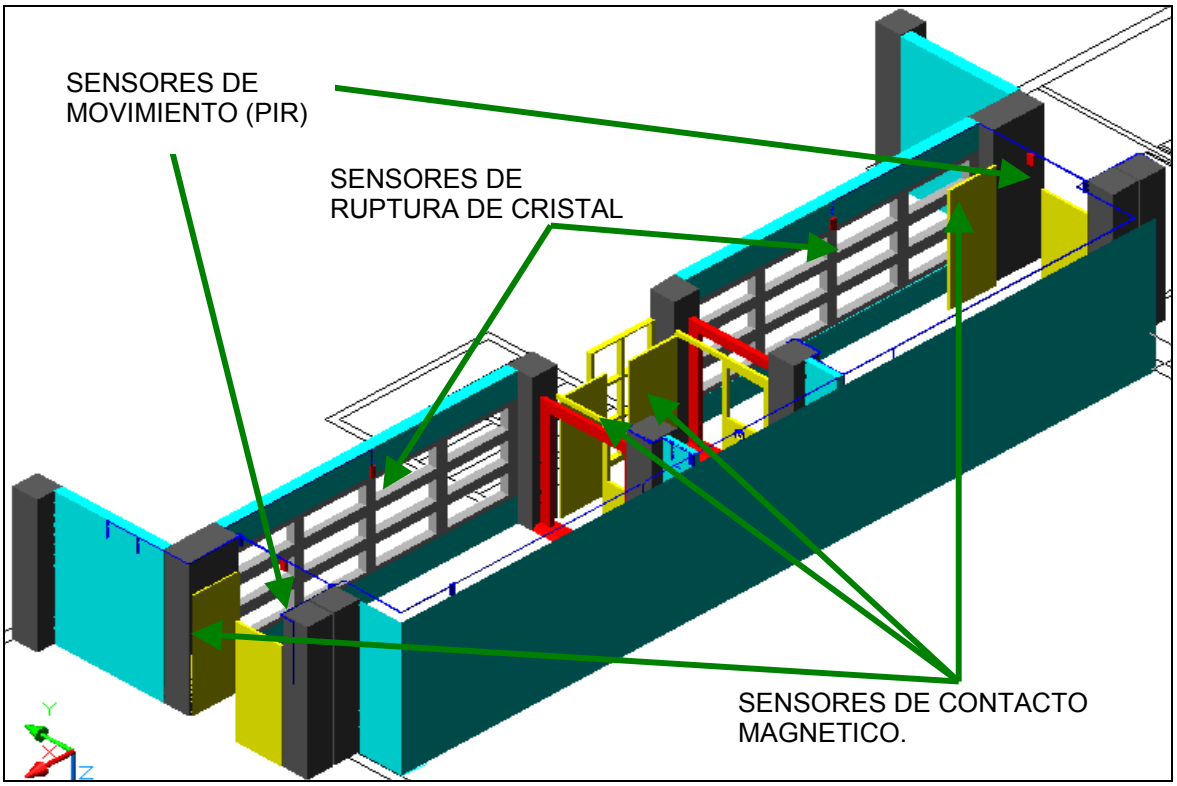


Figura 4.2: colocación de los sensores en la planta alta del edificio.

Elección del protocolo de transmisión de datos.

Para la selección del tipo de transmisión de datos del sistema, este deberá de cumplir con las siguientes especificaciones de diseño:

- Comunicación a gran distancia entre control maestro PC y dispositivos esclavos.
- Capacidad de comunicación con todos los módulos utilizando un solo bus de datos.
- Crecimiento futuro del sistema, utilizando el mismo protocolo de transmisión.
- Facilidad para el desarrollo de un sistema modular.

Existen dos formas de transmitir los datos en forma muy general: la transmisión paralela y la transmisión serial, una de las diferencias palpables de una con respecto a la otra, es el número de cables que se utilizan para establecer la transmisión, mientras que la paralela necesita de ocho hilos, la serial necesita como máximo de cinco.

Otra diferencia, es la distancia de comunicación entre dispositivos: en la transmisión de datos paralela, la distancia máxima de transmisión es de 10 metros[3] mientras que en la serial, dependiendo del estándar de transmisión, se pueden tener distancias de más de 1 Km.

[3] Serial Port Complete, Jan Axelson Pág. 6

Por lo que de acuerdo a nuestros requerimientos de diseño, utilizaremos una transmisión serial (ver tabla 4.2).

Características	Num. De transmisores y receptores conectados en una línea (bus de datos)	Longitud máxima de cable (m.)	Velocidad de transmisión	Voltajes de salida (mínimo)	Voltaje de salida (Máximo)	Tipo de comunicación.	Número de hilos para la transmisión.	Forma de comunicación
RS232	1 Transmisor 1 Receptor	15.24	20 Kb/s	± 5	± 25	Punto / punto	3 Hilos	Full duplex
RS422	1 Transmisor 10 Receptor	1219.2	10 Mb/s	± 2	-0.25V a 6V	multipunto	5 Hilos	Full duplex
RS485	**32 Transmisor 32 Receptor**	**1219.2**	**10 Mb/s**	**± 5**	**-7V a 12V**	**multipunto**	**2 Hilos**	**Half duplex**
USB[4]	126 dispositivos	5	1.5 a 12 Mb/s	± 0.3	± 2.8	multipunto	4 Hilos	Half duplex

Tabla 4.2 : Comparativa de los diferentes estandares de comunicacion.

De la tabla anterior observamos que el estándar de comunicación RS485, es el que mejor se adapta a nuestro diseño, ya que las ventajas para nuestro sistema nos ofrece, esta la distancia (1219.2 m) entre emisor y receptor, con un número mínimo de 2 hilos, una comunicación multipunto y tener 32 transmisores y receptores involucrados en la misma línea de comunicación.

Sistemas RFID.

Un sistema de identificación RFID básico (figura 4.3), ya sea de protección de equipo o de acceso de personal se basa básicamente de cuatro partes:

- La computadora: que se encarga de la organización de la información proveniente del lector.
- El lector: cuya función es leer la información proveniente de la antena.
- La antena: tiene la misión de energizar el transponder pasivo y recibir la información proveniente del transponder.
- El transponder.- que una vez energizado, responde con un código de identificación captado por la antena.

[4] USB: Universal Serial Bus.

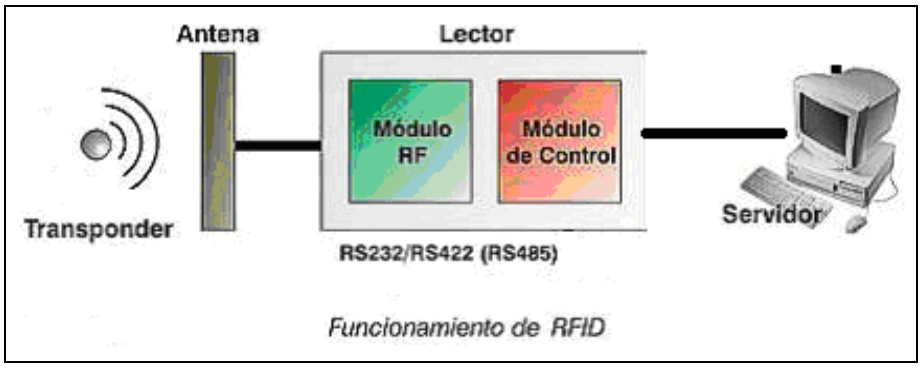


Figura 4. 3: Sistema básico de un sistema de identificación.

Ya teniendo esta información hicimos la elección de los sistemas RFID, para los sistemas de protección de equipos y acceso de personal.

Elección de los dispositivos del sistema de protección de equipo.

Para la elección del tipo de lector a usar en la protección de equipo, nos decidimos por los sistemas de identificación de la compañía TEXAS INSTRUMENTS, ya que además de ser pioneros en este tipo de tecnología, ofrecen una gran gama de readers (lectores) de alta y baja frecuencia, además de que todos sus productos son de arquitectura abierta, un aspecto importante para continuar cumpliendo con el objetivo del proyecto.

Para poder seleccionar los equipos que se utilizarían para el desarrollo del proyecto debemos de tomar en cuenta los siguientes parámetros de diseño:

- Los lectores de identificación RFID estarán colocados dentro de un gabinete lejos de las antenas lectoras por seguridad, para darnos una idea de la distancias requeridas las antenas estarán colocas entre 16 metros (mínimo) y 50 metros (máximo) alejadas de los lectores.
- Las antenas que se utilizarían las hemos llamado como antenas de tipo portal, ya que estarán colocadas en la entrada de cada área.
- El tipo de comunicación que se utilizará para la transmisión y recepción de la información en las líneas será con el estándar RS485.

Dentro de la gran gama que ofrece la tecnología TI-RFID (Texas Instruments Radio Frecuency IDentification), encontramos que el modelo **SERIES 2000** era la más apropiada para nuestras necesidades de diseño del sistema de protección de equipos.

La decisión de usar un sistema de baja frecuencia en nuestro sistema de protección de equipo, además de las razones expuestas anteriormente (ver página 26), añadimos que en la gama de baja frecuencia (134.2 Khz.), el sistema tienen una mayor penetración, es decir “este termino es usado para indicar la habilidad de una frecuencia de radio en particular, de atravesar superficies no metálicas[5]”.

Para el caso que nos ocupa, el sistema tiene la habilidad de leer los transponders que estarán ocultos dentro de los equipos a proteger, ya que tienen esa propiedad de buena

[5] Traducción de: TI-RFID *Product Manuals, Terms & Abbreviations* pag. 10

penetración, a diferencia de los sistemas de alta frecuencia, que tienen menos capacidad de penetración.

Los sistemas que conforman el sistema de protección de equipos son:

- Lectores de baja frecuencia Series 2000.
- Tuning Box.
- Antenas tipo portal[6].
- Transponders.

Los lectores de baja frecuencia Series 2000 se componen de dos módulos:

- Módulo de control series 2000.
- Módulo de radio frecuencia TIRIS[7].

Módulo de control series 2000.

Se encarga de mantener la comunicación serial con la computadora además de codificar y decodificar la señal de radio frecuencia que genera y recibe del módulo de radio frecuencia TIRIS, asimismo controla la información obtenida de los pines I/O con que cuenta el módulo.

Estos módulos, están disponibles para una comunicación punto a punto con una interfase serial RS232 o una comunicación serial multipunto RS422/485 (ver tabla 4.3).

Modelo.	Interfase de comunicación.	Arquitectura del sistema
RI-STU-MB2A	RS232	Punto a punto
RI-STU-MB6A	RS422/485	Punto a multipunto.

Tabla 4.3: Módulos de control para el Series 2000

De acuerdo a las especificaciones de diseño, elegimos el módulo RI-STU-MB6A (ver figura 4.4), cuyas características principales son[8]:

Suministro de potencia	7 a 24 VDC
Frecuencia de transmisión (RF)	134.2 Khz.
Protocolos de comunicación	ASCII con Xon/Xoff, TIRIS Bus Protocol
Parámetros de comunicación	600-57600 Baud, 7/8 bits de datos
Entradas/salidas	8 configurables digitalmente como I/O, 2 salidas de colector abierto,
Tipo de transponder	Solo lectura (RO), lectura/escritura (R/W)
Tiempo de lectura típico	70 milisegundos para RO y R/W.

Tabla 4. 4: características del módulo.

[6] Nombre dado por nosotros a las antenas que diseñamos.
[7] (TIRIS) Texas Instruments Registration and Identification System.
[8] Para informacion más detallada de este módulo consultar la bibliografia.

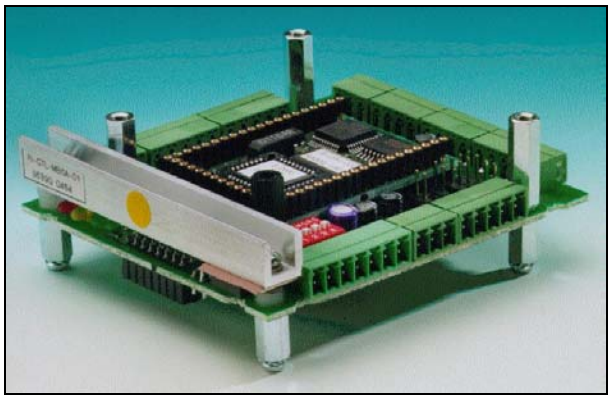


Figura 4. 4: Módulo de control RI-STU-MB6A

Módulo de radio frecuencia (TIRIS).

Este módulo de RF se encargara de transmitir y recibir información proveniente de un transponder, la frecuencia que manejan estos equipos es de 134.2 Khz.

"Contiene todos las funciones análogas de un lector TI-RFID necesarias para inicializar a un transponder TI-RFID, proporcionar datos y señales de reloj para identificación y proceso de datos.

"El RA-RFM también envía las señales de programación y direccionamiento necesarias a los transponders de lectura/escritura y multipagina.

"Las líneas de datos de entrada y salida, que son conectados a la unidad de procesamiento de datos son compatibles con lógica low-power Schottky TTL y HCMOS."[9]

Los módulos de RF (TIRIS) de baja frecuencia que se encontraron de Texas Instruments fueron los siguientes:

Nombre del dispositivo/ parte	**RI-RFM-007B**	**RI-RFM-008B**	**RI-ACC-008B**
Descripción del modelo	Standard RFM	Remote Antenna RFM	Antenna Tuning Module
Voltaje de operación regulado.	7-24 VDC	7-24 VDC	7-24 VDC
Frecuencia RF de transmisión	134.2 Khz.	134.2 Khz.	134.2 Khz.
Voltaje de resonancia en antena	380 Vp máx.	380 Vp máx.	380 Vp máx.
Rango de sintonización de la antena (mH).	26 a 27.9	26 a 27.9	8 a 80 (incluye cable)
Antenna Tunning Module RI-ACC-008B (recomendado)	No	Si	No
Digital Reader Module RI-CTL-010A (recomendado)	Si	Si	No

Tabla 4. 5: comparativa de módulos RF[10].

[9] Traducción del ingles de: Texas Instruments, *High Perfomance Remote Antenna-Reader Frecuency Module RI-RFM-008B, Antenna Tuning Board RI-ACC- 008B, Reference Guide, Pág. 10.*
[10] Traducción del ingles de tabla tomada parcialmente de: Texas Instruments, Product bulletin *High Prefomance LF Radio Frecuency Modules.*

De acuerdo a nuestras especificaciones de diseño, elegimos el modelo RI-RFM-008B, que es un modelo usado para antenas remotas con una distancia de hasta 120 metros entre el lector y la antena, también usaremos el módulo RI-ACC-008B, que tiene la función de entrar en resonancia con la antena, es decir, podemos realizar los ajustes necesarios para obtener una mayor potencia de transmisión, de la antena al lector, como se vera más adelante.

Módulo RI-ACC-008B (Tuning Board).

El módulo RI-ACC-008B, también conocido como un Tuning Board es un arreglo de capacitores en paralelo y un inductor variable que sirve de ajuste (ver figura 4.5) cuyo propósito es alcanzar un alto voltaje de resonancia y también un campo adecuado para energizar a los transponder, dichos módulos estarán colocados cerca de las antenas lectoras, para poder alcanzar los niveles de potencia adecuados, los módulos cuentan con puentes (jumpers) que nos permite seleccionar el mejor arreglo de capacitores, que dependiendo del tamaño de la antena y su distancia al reader, podremos seleccionar la configuración de los puentes más adecuada.

El tuning board cuenta además con un led emisor, que nos indicara de forma inmediata la potencia que esta recibiendo del módulo de RFM, es decir aunque no sabremos directamente el valor de voltaje que existe en las terminales de la antena, la intensidad del led emisor nos puede dar una idea del valor de voltaje, entre más intensa sea esta luz la presencia de voltaje es más alta.

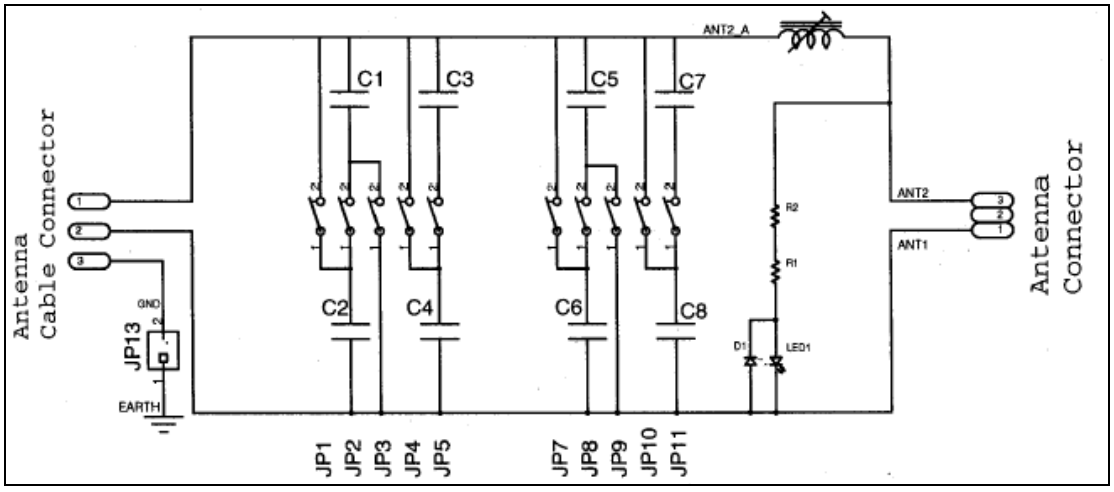


Figura 4.5: Esquema del Tuning Box.

A continuación presentamos el diagrama de conexión utilizando el RI-RFM-008B y el Tuning board:

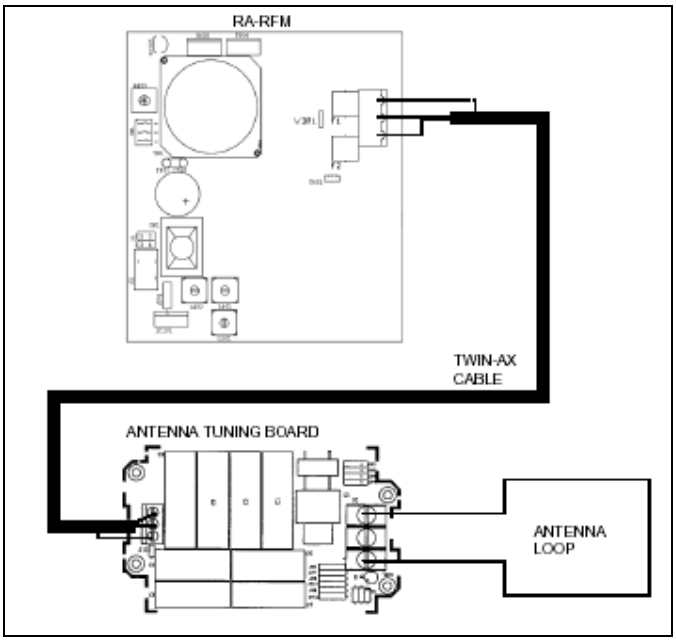


Figura 4.6: Diagrama de conexión del sistema series 2000

En nuestro diseño tenemos contemplado el uso de cuatro antenas, que se encontraran en las puertas de control de acceso (una antena por puerta), cada sistema lector S2000 tiene la limitante de controlar una sola antena. Por lo que se usaran cuatro lectores S2000.

DISEÑO DE LAS ANTENAS DE BAJA FRECUENCIA.

Las antenas tiene dos funciones principales:

1. El envió de una señal de carga para el transponder.
2. La recepción de una señal de regreso por parte del transponder que contiene el ID de este último.

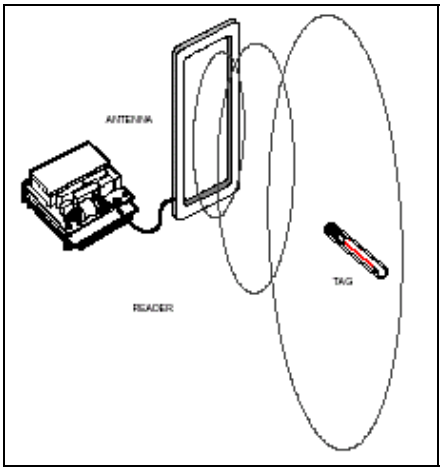


Figura 4.7: Carga de la antena al transponder.

El módulo RF, genera a través de la antena, un campo electromagnético, que cuando el transponder pasa por este, se carga un capacitor dentro del transponders a un cierto voltaje, la energía con la que se ha cargado este capacitor es usada para enviar un código-ID de regresó a la antena, es importante decir que es necesario un mínimo de 5V en el capacitor, para que pueda cumplir con esta función. Entre tanto el módulo RF cambia a modo de recepción y captura la respuesta del transponder.

Texas Instruments (TI) ofrece antenas lectoras para sus equipos de RF, la limitante de ellas es el tamaño, teniendo tres tamaños diferentes:

- RI-ANT-G01E: 715mm x 270mm.
- RI-ANT-G02E: 200mm x 200mm.
- RI-ANT-G04E: 1018mm x 518mm.

Para nuestra aplicación, requeríamos unas antenas de mayores dimensiones, ya que nuestro propósito era que abarcarán toda el área que ocuparían las nuevas puertas de control de acceso, por lo que nos propusimos diseñarlas, para ello los asesores de TI nos proporcionaron la literatura[11] necesaria para la construcción de estas. Ya con esta información, definimos las especificaciones de diseño de nuestras antenas.

- Antenas de tipo loop.
- Tanto la inductancia (L) como su factor de calidad (Q), deberían de estar entre los rangos vistos en la tabla 4.6
- Transmisión de frecuencia a 134.2 Khz.
- Dimensiones de 2.5 m. x 1.8 m.

Una característica de la antenas que se diseñaron, es que su inductancia propia (L) y su factor de calidad (Q), varían de acuerdo a las características físicas de las antenas (dimensiones y número de vueltas), así como también del tipo de cable utilizado[12] por lo que al realizar su diseño y construcción, las antenas deben cumplir con lo siguiente:

Parámetro	Condiciones	Min.	Típico.	Máx.	Unidades
L_ANT	Rango de inductancias con el cual la antena puede ser sintonizada.	8	27	80	mH.
Q_ANT	Factor Q recomendado para la correcta operación de la antena.	40		450	----

Tabla 4.6: inductancia y factor de calidad, requeridos en las antenas.

Un factor muy importante que debemos considerar para el buen desempeño de las antenas es el medio ambiente donde van a operar (presencia de elementos ferrosos y ruido eléctrico). Por lo que es importante que las antenas diseñadas fueran construidas y probadas en el lugar en donde quedaran instaladas, de no ser así se tendrá como consecuencia que el campo magnético generado no sea lo suficientemente fuerte como para que los transponder puedan “responder”.

[11] “ TIRIS Antenna Design” manual de referencia
[12] Al hablar del tipo de cable nos referimos a las características físicas del mismo (calibre, material con que esta construido, resistencia).

El cable para el diseño de las antenas debía de tener las siguientes características: cable de baja resistencia e inductancia, para tener un factor de calidad alto, los cables recomendados por TI son los siguientes:

Cable	Diámetro del cable	Número de hilos y diametro
Cobre recubierto de pulíoretano	0.20 mm.	36 awg
Litze	2.5 y 1.5 mm²	600 X 0.07 y 120 X 0.1
Estañado Pirelli 854/ Delta CL4C	2.5 mm²	50 X 0.25
Figura de ocho OFC[13]	2.5 mm²	322 X 0.1

Tabla 4.7: Cables propuestos por Texas Instruments.

En la búsqueda de estos cables, tuvimos los siguientes inconvenientes:

- No se encuentran en existencia la mayoría de ellos, en la Republica Mexicana.
- Los fabricantes que se localizaron no tienen filiales en México.
- Se pueden importar pero el costo de ellos son muy elevados.
- Los tiempos de entrega eran largos (8 a 10 semanas).

Lo que los hace que sean de difícil adquisición, por lo que decidimos buscar cables con las características de baja resistencia e inductancia que se tuviese en existencia en México y de entrega inmediata. Para esto, Nuestro proveedor de Texas Instruments en México nos recomendó el cable de la marca PRODEL, 8 AWG.

Detalles de construcción.

Para darles cierta rigidez a las antenas al momento de instalarlas, estas se colocarían dentro de tubos de PVC, y se fijaron dentro de los marcos de las puertas, esto es para asegurar que el transponder quede energizado antes de cruzar la puerta, además de mantenerlas ocultas.

Una vez que estén colocadas en las puertas, se procederá a sintonizarlas para que se encuentren en óptimo funcionamiento.

En la fotografía 1, se muestra la colocación de una de las antenas de baja frecuencia, así como la presentación final de una entrada a un área.

[13] OFC (Oxigen Free Cable), cable libres de oxigeno

Fotografía 4. 1: Colocación de la antena de baja frecuencia inicial y presentación final de la puerta.

Proceso de sintonización de las antenas.

La sintonización de las antenas es importante en el desempeño del sistema de protección de equipo, ya que la antena debe ser capaz de emitir una señal de radio frecuencia lo suficientemente fuerte para poder activar a un transponder que este cerca o dentro del campo de Radio Frecuencia (RF), que emite la antena, del mismo modo la antena debe tener la capacidad de recibir la información que emite el transponder, si se tiene poca potencia, las distancias de lectura de los transponders se reducen.

Para la sintonización de las antenas se tomaron los siguientes pasos:

Antes de comenzar con las sintonización de las antenas se deben de tomar las siguientes acciones:

1. Configuración previa del SERIES2000[14],
2. Determinación de la Capacitancia del Tuning box, para su configuración.
3. Elección de uno de los métodos de sintonización de las antenas.

Determinación de la Capacitancia del Tuning box.

Para el cálculo de la Capacitancia de las antenas se hizo uso de las siguientes fórmulas encontradas en el manual antes citado (RI-RFM-008BREFGUIDE de Texas Instruments Pág. 35), Una vez que teníamos el valor de la inductancia de las antenas se calculaba la Capacitancia en la antena ($C_{RES.}$) por medio de la siguiente fórmula:

$$C_{RES.} = \frac{1406.45}{L_{ANT}+3} \quad (\mu H/nF). \qquad (1)$$

[14] Ver apéndice A referente a la configuración de los SERIES 2000.

El siguiente paso es obtener la Capacitancia del cable C_{CAB} , esto lo logramos obteniendo el producto de la Capacitancia por metro del cable por la distancia en metros del cable que va del Tuning box al Multiplexor de antenas.

$C_{CAB.}$= Capacitancia cable x distancia en metros (pF/metro). (2)

Ya con estos datos se hace uso de la siguiente formula:

$$C_{TUNB.} = C_{RES} - C_{CAB} - 2.2 \ (nF) \qquad (3)$$

Ya con estos valores como se dijo anteriormente se busco en la tabla 4.8 el valor aproximado al calculado.

Jumper Setting	C_tunb (nF)	C_deviation (nF)	Tuning Range (uH)	Cable Length (Meter)	V-RF_max (V)
JP2	16.5	+/- 0.5			800 Vpp
JP2, JP11	21.5	+/- 0.7			800 Vpp
JP2, JP8	23.5	+/- 1			800 Vpp
JP2, JP5	33	+/- 1.5			800 Vpp
JP2, JP5, JP11	38	+/- 2.3			800 Vpp
JP2, JP5, JP8, JP11	45.5	+/- 3	27	5 to 40	800 Vpp
JP3, JP4	66	+/- 7			560 Vpp
JP2, JP4, JP7, JP10	74.5	+/- 7	16	5 to 40	560 Vpp
JP1, JP3, JP5	82.5	+/- 10			560 Vpp
JP1, JP3, JP5, JP10	92.5	+/- 12			560 Vpp
JP1, JP3, JP4, JP7, JP10	124	+/- 20	8	5 to 120	560 Vpp

Tabla 4. 8: Rango de capacitancias C_{TUNB}, disponible en el Tunning Box.

y definimos los jumpers que se deberán de cerrar en cada Tuning Board para configurarlo.

Métodos de sintonización.

Utilizando una bobina: La primera es utilizar una bobina de 1mH conectar las terminales de la bobina a un osciloscopio, también se puede utilizar un voltímetro para realizar las mediciones (ver figura 4.8):

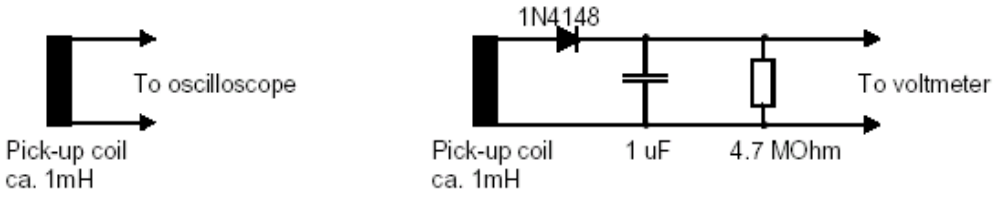


Figura 4. 8 Sintonización de la antena utilizando una bobina.

Para poder sintonizar la antena el módulo Series 2000 debe de estar en modo de lectura continua, colocar alguna de las configuraciones anteriores al centro de la antena y realizar las mediciones de voltajes utilizando un osciloscopio o voltímetro, para variar el voltaje presente en la antena, realizamos los ajustes necesarios por medio del inductor variable que se encuentra en el tuning Board, hasta obtener el valor máximo en caso de no obtener dicho voltaje cambiar la configuración de puentes y volver a realizar lecturas, los voltajes medidos deben ser de 5 a 7 Volts[15].

Utilizando Antenna Tuning Indicador (ATI): Este dispositivo permite de manera más directa de realizar la sintonización de las antenas, el ATI es conectado directamente al conector 2 del módulo de RA-RFM para poder realizar la sintonización (figura 4.9) .

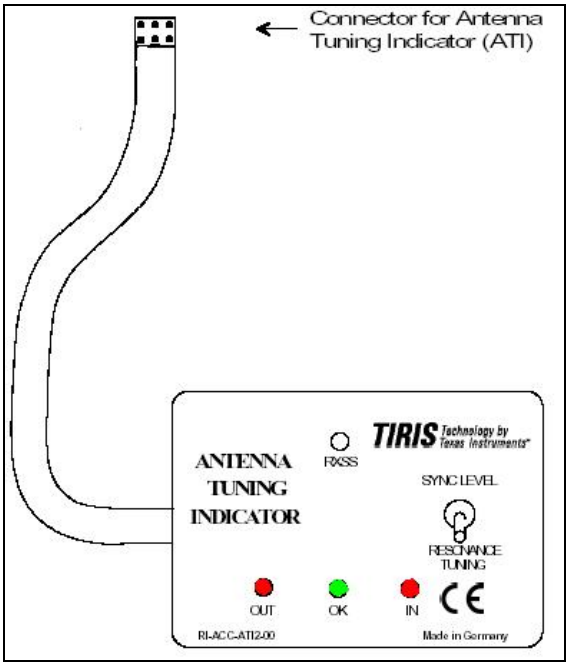


Figura 4. 9: Antenna Tuning indicator.

se cuenta además con tres leds (OUT , OK, IN), que nos indicara:

- Que se necesita variar la inductancia (leds out, in).
- La antena esta sintonizada (Led Ok).

[15] Tomado del guía de referencia “Antenna Referente Guide 11-08-21-001” Pág. 3, y “Antenna Desing” Pág. 27

Para realizar la sintonización se realizan los siguientes pasos[16]

- Apagar el módulo Series 2000.
- Conectar el ATI en el conector número 2 del módulo RFM.
- Encender el módulo Series 2000.
- Colocar el Switch del ATI en la posición "'RESONANCE TUNING'".
- Activar el módulo series 2000 en modo de lectura continua.
- Si esta encendido el led izquierdo (OUT), con un desarmador de plástico, destornillar el núcleo de la bobina que se encuentra en el tuning Board.
- Si esta encendido el led derecho (IN), atornillar el núcleo de la bobina que se encuentra en el tuning Board.
- En caso de no se pueda sintonizar la antena, se incrementa o decrementa la capacitancia del tuning board por medio de la tabla 4.8, y se repiten los pasos anteriores.
- Cuando el led Verde indica "OK" la antena esta sintonizada.

Teniendo sintonizada la antena procedemos a desconectar el ATI.

- Apagar el módulo Series 2000.
- desconectar el ATI en el conector número 2 del módulo RFM.
- Encender el módulo Series 2000.

Por último, cuando la antena ya se encuentre entonada por medio del ATI, se hace una prueba con los transponders, para verificar que se hallen en estos con la energía necesaria para responder a la antena.

Transponders.

Tanto el sistema de protección de equipo como el de acceso de personal usan un transponder para el registro e identificación de personas, objetos y equipos. Los transponder también nombrados TAG, pueden ser de solo lectura pues tienen un código de escritura ya sea preestablecido por el fabricante o de lectura / escritura donde el usuario puede introducir un código propio de identificación, entre otros datos.

Los transponders que se usan en el sistema de protección de equipo (ver tabla 4.9), están diseñados para ser leídos a una frecuencia de 134.2 Khz. el lector series 2000.

[16] Tomado de "Referente Guide Antenna Tuning RI-ACC-ATI2 Indicator" Pág. 7

	Transponder	Característica.
	Transponder MOUNT-ON- METAL	Este tipo de transponder tienen la característica de que puede ser colocado en cualquier material metálico, y esto no afecta su funcionamiento. Su rango de lectura es menor o igual a 120 cm*. Están disponibles en solo lectura (RI-TRP-R9VS) o lectura y escritura (RI-TRP-W9VS).
	Transponder cilíndrico de 120mm	Un transponder especialmente encapsulado para resistir ambientes severos, ofreciendo superior alcance de lectura pudiendo ser fijado por medio de abrazaderas no metálicas en camiones o contenedores. Su rango de lectura es menor o igual a 200 cm*. Están disponibles en solo lectura (RI-TRP-R9TD) o lectura y escritura (RI-TRP-W9TD).
	Transponder tipo disco de 85mm.	Este transponder se diseñó para aplicaciones internas, por ejemplo: anexado al parabrisas de un automóvil. Su forma plana es ideal para control de acceso. Su rango de lectura es menor o igual a 150 cm*. Están disponibles en solo lectura (RI-TRP-R9UR) o lectura y escritura(RI-TRP-W9UR).

Tabla 4. 9: transponder usados en el sistema de protección de equipos.

Elección de los dispositivos del sistema de acceso de personal.

Aquí la elección, entre un lector de Texas Instruments y de otra compañía, fue el precio y presentación del producto final ver figura 4.10, presentamos algunas características del lector **ET-RS de Secura Key:**

- Frecuencia de transmisión 13.56Mhz.
- Compatible con Texas Instruments.
- Interfase de comunicación RS232 a 19200 Bauds.
- De arquitectura abierta.

* Esta distancia depende de las condiciones de interferencia de los dispositivos.

- Voltaje de operación de 12-15 Volts.
- Protocolo de comunicación **Tag-it Host Protocol.**

El que fuera compatible con Texas Instruments, nos daba la posibilidad de poder usar el software de esta compañía.

Figura 4. 10: lector de alta frecuencia **ET-RS.**

Este lector tiene también la ventaja de que la antena se encuentra dentro de la misma base que contiene al lector.

Transponders de alta frecuencia (credenciales).

Este transponder trabaja a una frecuencia de 13.56 Mhz. Que es una frecuencia estandarizada para este tipo de sistemas. En el proyecto se usaron transponder tipo credencial de solo lectura y lectura / escritura, este último tiene una memoria donde el usuario puede introducir la información que le parezca pertinente[17].

Figura 4. 11: transponder de alta frecuencia.

Ubicación de la antena de protección de equipo, y lector de acceso de personal.

Para el sistema de protección de equipos se usaran cuatro lectores de baja frecuencia (134.2 Khz.), para controlar las dos áreas de la planta alta y las dos áreas de la planta baja, estos lectores se encontraran en el área PAD, en un gabinete metálico.

[17] El procedimiento de escritura de estos transponder, así como también los de baja frecuencia, los podrá revisar en el apéndice: **"Escritura de transponders de alta y baja frecuencia"**

Mientras que los lectores de alta frecuencia (13.56 Mhz.) serán cuatro, que se encontraran ubicados en las cuatro áreas a controlar, en cada puerta de control de acceso (ver figura 4.12), también en esta misma área se encontraran ocultas las antenas tipo portal dentro del marco de la puerta.

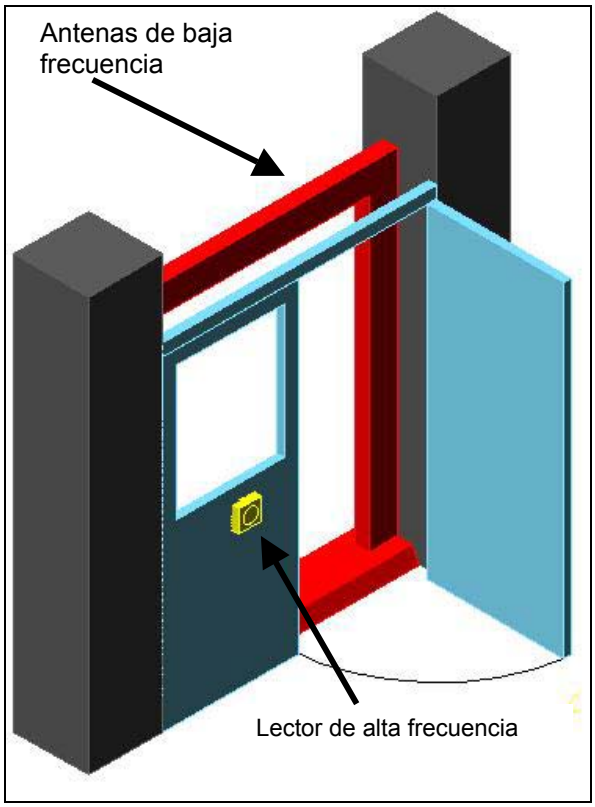


Figura 4. 12: Ubicación de la antena y lector de alta frecuencia

Consideraciones a tomar en la integración final de los sistemas.

Una vez elegido el estándar de transmisión y los dispositivos a ocupar, nos encontramos con los siguientes inconvenientes:

- La computadora que usamos, y el lector de alta frecuencia elegidos, no estaban habilitados para una transmisión de datos RS485.
- Los sistemas RFID tienen un protocolo de comunicación diferente (TIRIS BUS PROTOCOL para el lector de baja frecuencia y HOST PROTOCOL SERIES 6000 para el lector de alta frecuencia).
- Para operar actuadores se necesitan de un voltaje de 12V y una corriente de 1 A.

Para dar solución a los puntos anteriores se hizo lo siguiente: Ya que la computadora tiene un puerto serial RS232, se utilizara un conversor externo[18] RS232 a RS485 para homologar la transmisión.

Se diseñaran tarjetas de control llamadas módulo **TAG-PC** cuya tarea será:

- Hacer la conversión de RS485 a RS232 para el lector de alta frecuencia .
- Hacer la conversión de protocolos del lector de alta frecuencia al protocolo que se usara para comunicar con la computadora y los demás dispositivos.

Y un **Módulo de potencia***,* cuya tarea será:

- Saber cuando uno de los sensores cambia de estado[19] y enviar la información (Módulo TAG-PC) a la computadora.
- Activar y desactivar a los actuadores previa orden del TAG-PC que a su vez recibió la instrucción de la computadora.

Definición del protocolo de comunicación en el bus de datos.

El lector RFID de baja frecuencia para el sistema de protección de equipo puede transmitir datos en RS485, esta característica fue la que nos hizo que nos decidiéramos por el protocolo usado en este lector (TIRIS BUS PROTOCOL) para que se comunicarán todos los módulos del sistema en el bus de datos con la computadora, para más referencia de estos protocolos, referirse al apéndice protocolos de comunicación de lectores.

DISEÑO DE LAS TARJETAS TAG-PC Y MÓDULO DE POTENCIA.

Para poder entender mejor la parte de diseño de las tarjetas TAG-PC y el Módulo de Potencia explicaremos a grandes rasgos el funcionamiento del sistema.

Tomando como base el diagrama 4.1, vemos que la comunicación entre los módulos y a la computadora se hace por un solo bus de datos con un estándar de transmisión de datos RS485 y con un protocolo de comunicación TIRIS BUS PROTOCOL. La forma en que se efectúa la comunicación, es que la computadora sea el maestro y los módulos los esclavos, donde los módulos solo pueden comunicarse con la computadora pero no entre ellos.

La computadora envía información dirigida a un solo módulo mediante un número de identificación (ID) incluido en la trama de datos enviada, así, aunque la información llegue todos los módulos, solo el que tenga ese número de identificación la tomara, la interpretara y la procesara, respondiendo con la información solicitada[20].

[18] Aunque existen también conversores internos, su costo es más elevado.

[19] Cuando el sensor se activa, el relevador cambia de estado, en el caso de que fuera NC (normalmente cerrado) cambia de circuito cerrado a circuito abierto.

[20] La forma en que se tratara la información, lo veremos más adelante, cuando hablemos del firmware.

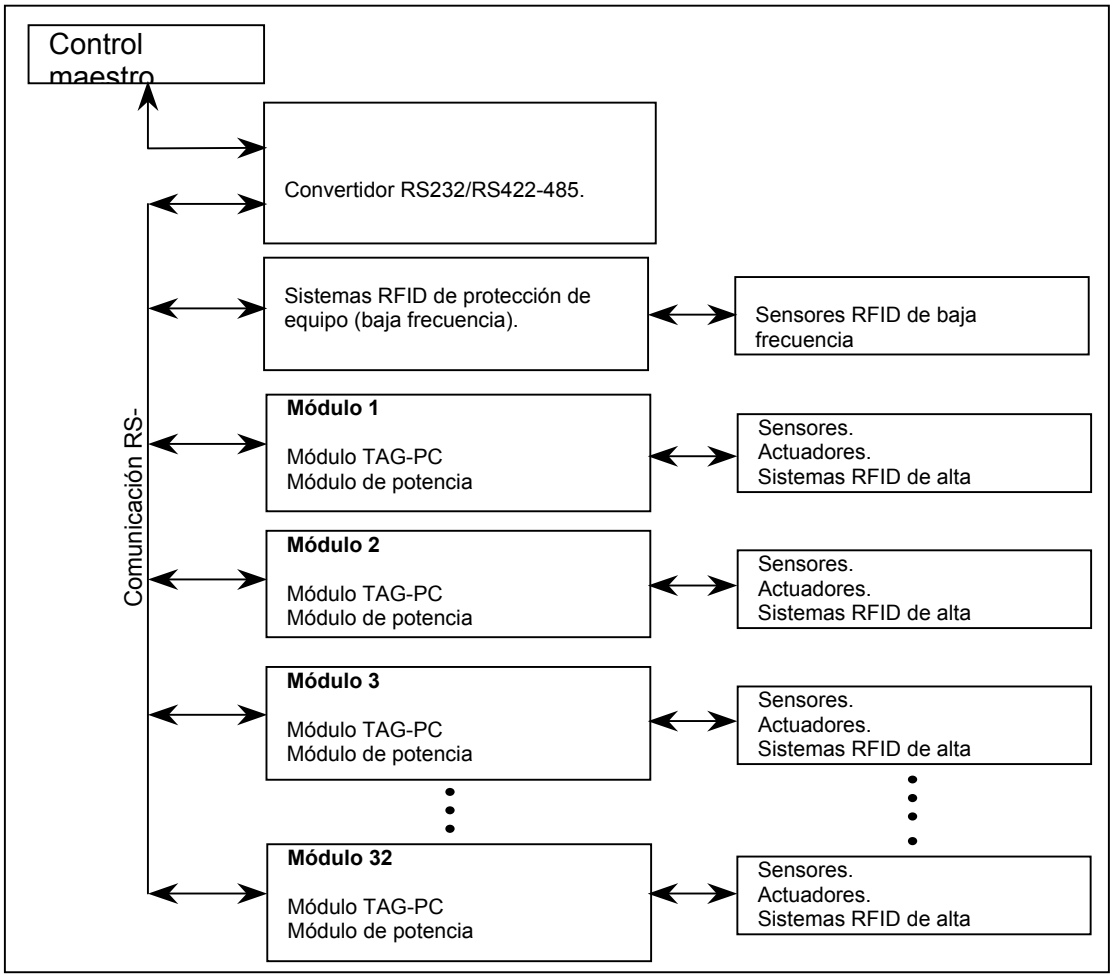


Diagrama 4. 1: A bloques de la conexión de distintos dispositivos.

Diseño de la Tarjeta TAG-PC.

Estas tarjetas fueron diseñadas para controlar a los sensores, actuadores y control de acceso de cada una de las áreas a las que se quiera proteger, su funciones a realizar son las siguientes:

- Tener comunicación serial con la PC vía RS-485.
- Establecer comunicación vía RS-232 con un el protocolo de comunicación llamado Host protocol con el módulo de acceso de personal.
- Obtener información proveniente de los sensores (ruptura de cristal, Magnéticos , de movimiento).
- Activar o desactivar a los actuadores (cerradura magnética, alarma general y local).

Como todos los sistemas TAG-PC y SERIES 2000 comparten el mismo bus de comunicación (utilizando el estándar RS485), cada uno de estos módulos tiene un número de identificación (ID) propio, por lo que cuando se quiera establecer comunicación con cada uno de estos módulos, el bloque de datos que envía la PC deberá contener dicho número de identificación.

A continuación mostramos un diagrama a bloques del funcionamiento del módulo TAG-PC.

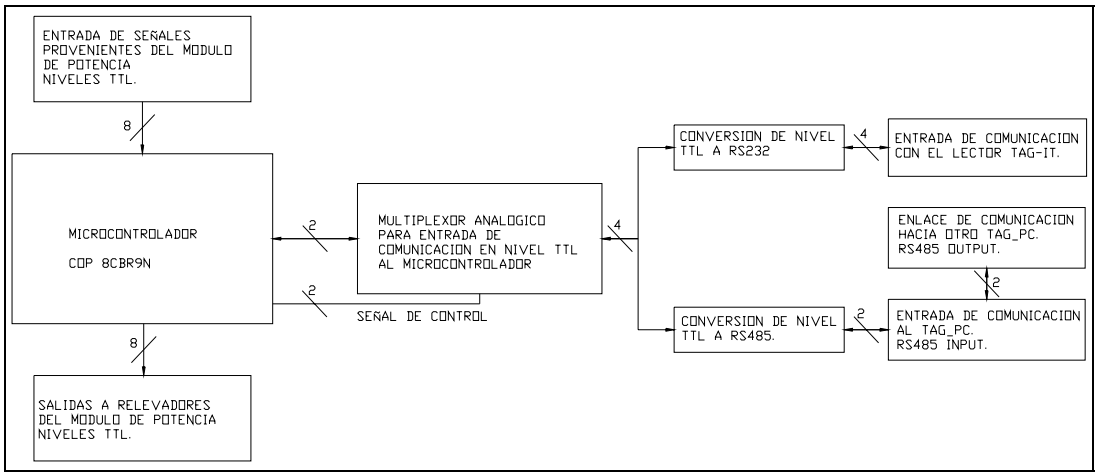


Diagrama 4. 2: A bloques de la tarjeta TAG-PC

De acuerdo al diagrama a bloques (diagrama 4.2) observamos que la tarjeta tiene un microcontrolador, que recibe las señales de los sensores vía módulo de potencia en voltaje TTL, de la misma forma a través del mismo módulo de potencia, el módulo TAG-PC controla a los relevadores, encargados de habilitar/deshabilitar el suministro de potencia a los actuadores.

También establece comunicación con la computadora y el lector de alta frecuencia (control de acceso). Esto se lleva a cabo, por medio de "multiplexar" las entradas de la comunicación, entre el lector TAG y la computadora. Por último nótese que los voltajes que se ocupan internamente de la tarjeta TAG-PC son en nivel TTL.

Implementación de la tarjeta PC-TAG.

Se presentan la tabla 4.10, los dispositivos que se utilizaron para implementar la tarjeta TAG-PC, en todos estos circuitos se busco, que tuvieran una alimentación de 5VDC.

CI seleccionado.	Función.
COP8CBR9N	Microcontrolador
HC4097BF(24)	Multiplexor analógico
MAX233A	Conversor de nivel TTL a RS232
DS3695	Conversor de nivel TTL a RS485

Tabla4.10: Dispositivos seleccionados y su función.

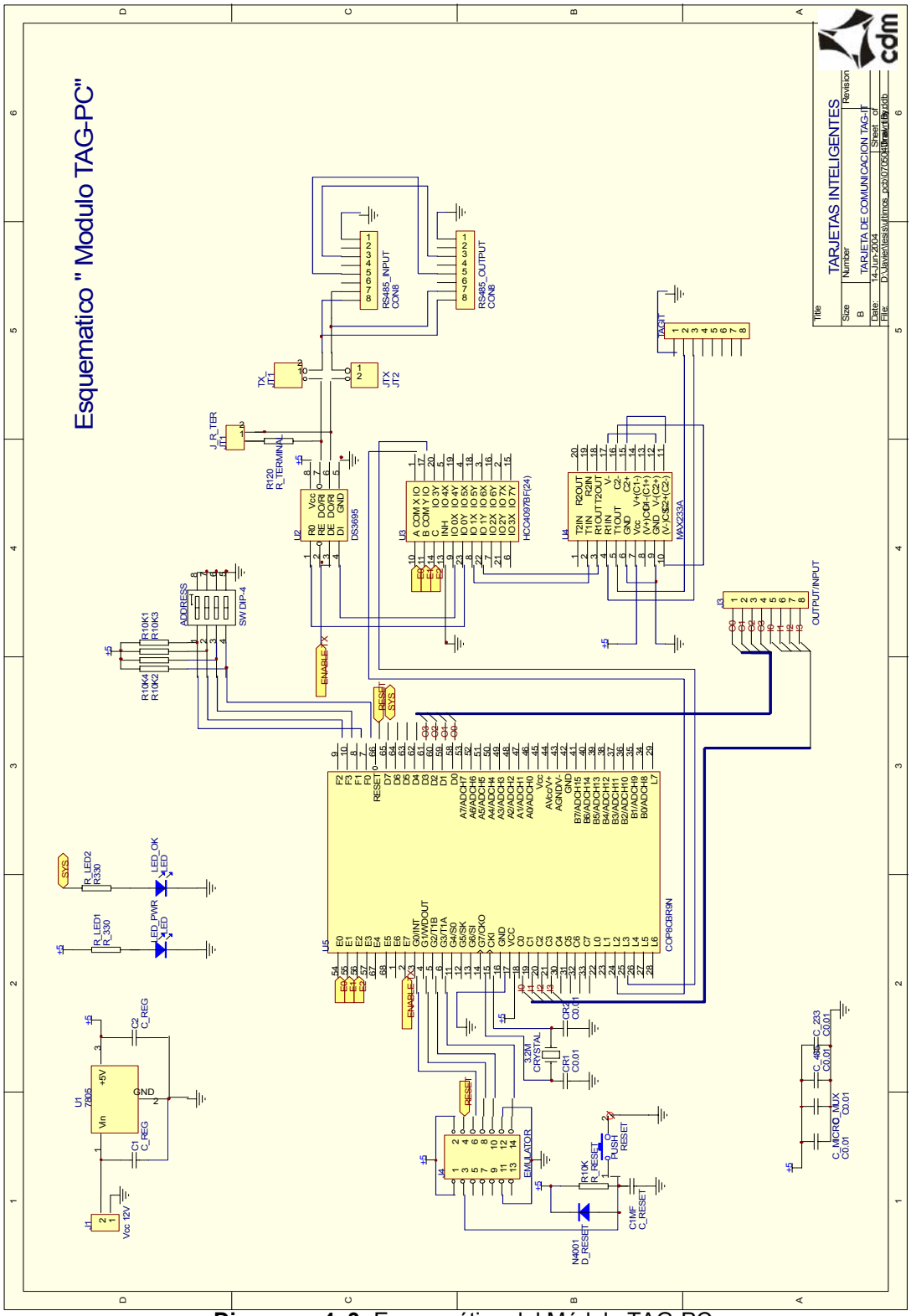


Diagrama 4. 3: Esquemático del Módulo TAG-PC.

Diseño del PCB del circuito.

Mediante el programa de computadora EDA Protel 99SE, se llevo a cabo el diseño del circuito esquemático (ver diagrama 4.3) y enrutamiento de las pistas de la tarjeta TAG-PC; en la figura 4.13, vemos al TAG-PC visto desde arriba.

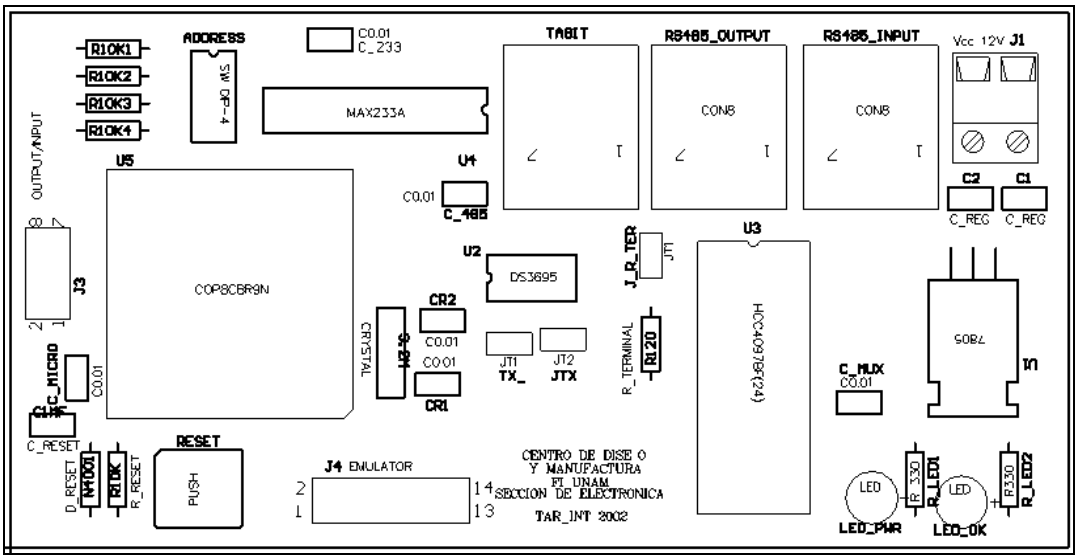


Figura 4. 13: Módulo TAG-PC visto desde arriba.

Diseño del MÓDULO DE POTENCIA.

Este módulo, tiene dos funciones principales:

- Detectar cuando los relevadores de alarma de los sensores han cambiado de estado y,
- Habilitar /deshabilitar los actuadores con la señal de mando proveniente del TAG-PC.

Detección del cambio de estado de los sensores.

Cuando un sensor que se tiene en el sistema, ha detectado un cambio en el área de sensado que tiene asignado, su circuito interno envía una señal eléctrica al común de su relevador interno de alarma, esto provoca que el relevador tenga un cambio de estado; los sensores involucrados en el sistema tienen sus relevadores internos en un estado inicial de **normalmente abierto** (por sus siglas en inglés: NO). Entonces para detectar cuando uno de estos relevadores cambian de estado, se diseño un circuito, para llevar a cabo esta tarea.

Circuitos de habilitación /deshabilitación de los actuadores.

Para habilitar y deshabilitar los actuadores, necesitamos que la tarjeta maneje los 12VDC con que operan los actuadores, sin embargo, la tarjeta recibe señales TTL provenientes de la tarjeta TAG-PC, por lo que se buscara tener una etapa de potencia, que al mismo tiempo este aislada de la etapa lógica de control, por lo que se diseño un circuito expresamente para ello.
En conclusión, la tarjeta deberá de tener una etapa que detecte cuando los relevadores internos de los sensores cambian de estado, otra etapa que controle la habilitación / deshabilitación de los actuadores, y una etapa lógica de control para la etapa de potencia que al mismo tiempo sirva de aislamiento de la parte lógica del módulo de potencia.

Implementación del MÓDULO DE POTENCIA.

Los dispositivos que principalmente se ocuparon para la implementación del MÓDULO DE POTENCIA, fueron:

- 2 CI latch transparente MC74HC373AN tipo D, cuya función será la de aislar el módulo de potencia del TAG-PC.
- 8 BC547C transistor NPN, para controlar la conmutación de los relevadores.
- 8 Relevadores RAS-1210, usados para la habilitación/deshabilitación de los actuadores.

Circuito para detección del cambio de estado de los relevadores internos de los sensores

Mientras que el interruptor del relevador del sensor se encuentre cerrado (ver diagrama 4.4), la corriente, se irá a tierra por la condición de corto circuito existente, cuando se abre el relevador por una señal interna a su común, se presenta una condición de circuito abierto y la corriente ahora se dirige al circuito, MC74HC373AN que son Filp flops D, en este circuito, tenemos un 1 lógico; que es detectado por el TAG-PC, que es la forma en que este se entera de que el sensor se ha activado.

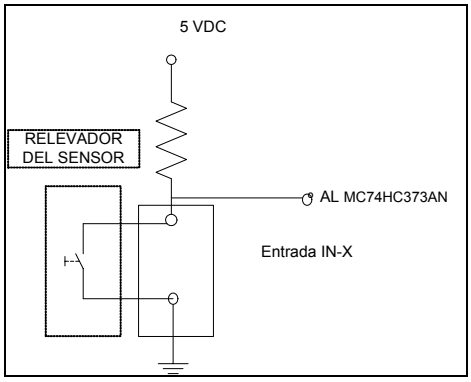


Diagrama 4. 4: Detector de cambio de estado de sensor.

Circuito para habilitar/deshabilitar.

Para habilitar / deshabilitar los actuadores, se utiliza unos circuitos diseñados para tal efecto, que están controlados por el microcontrolador a través del Flip flops D (MC74HC373AN) que aíslan al microcontrolador de los relevadores.

Del diagrama 4.5 observamos que mientras que no se presente un 1 lógico en la base del transistor, que funciona como un interruptor, no conducirá y por lo tanto no se energizará la bobina interna del relevador que tendrá su interruptor cerrado o abierto según este configurado en la tarjeta de potencia, cuando se presente un 0 lógico, el transistor se conmutara para volver a hacer el cambio de estado en el relevador, existente.

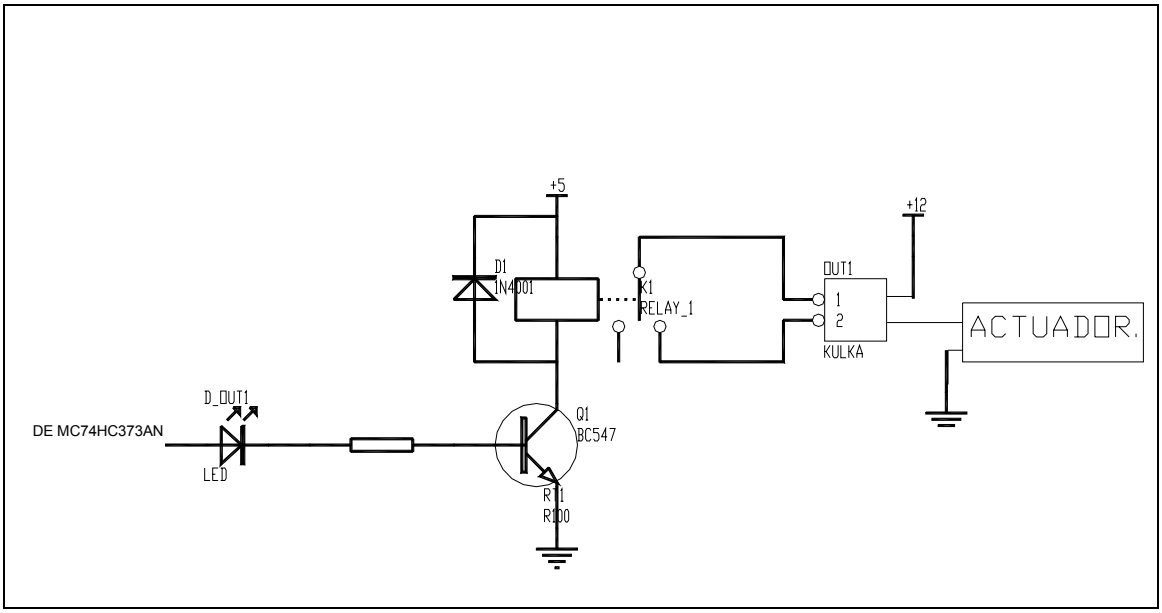


Diagrama 4. 5: Circuito para encender / apagar los actuadores

Diseño del PCB del circuito.

Mediante el programa de computadora EDA Protel 99SE, se llevo a cabo diseño del circuito esquemático (ver diagrama 4.6) y enrutamiento de las pistas de la tarjeta Módulo de potencia ver figura 4.14.

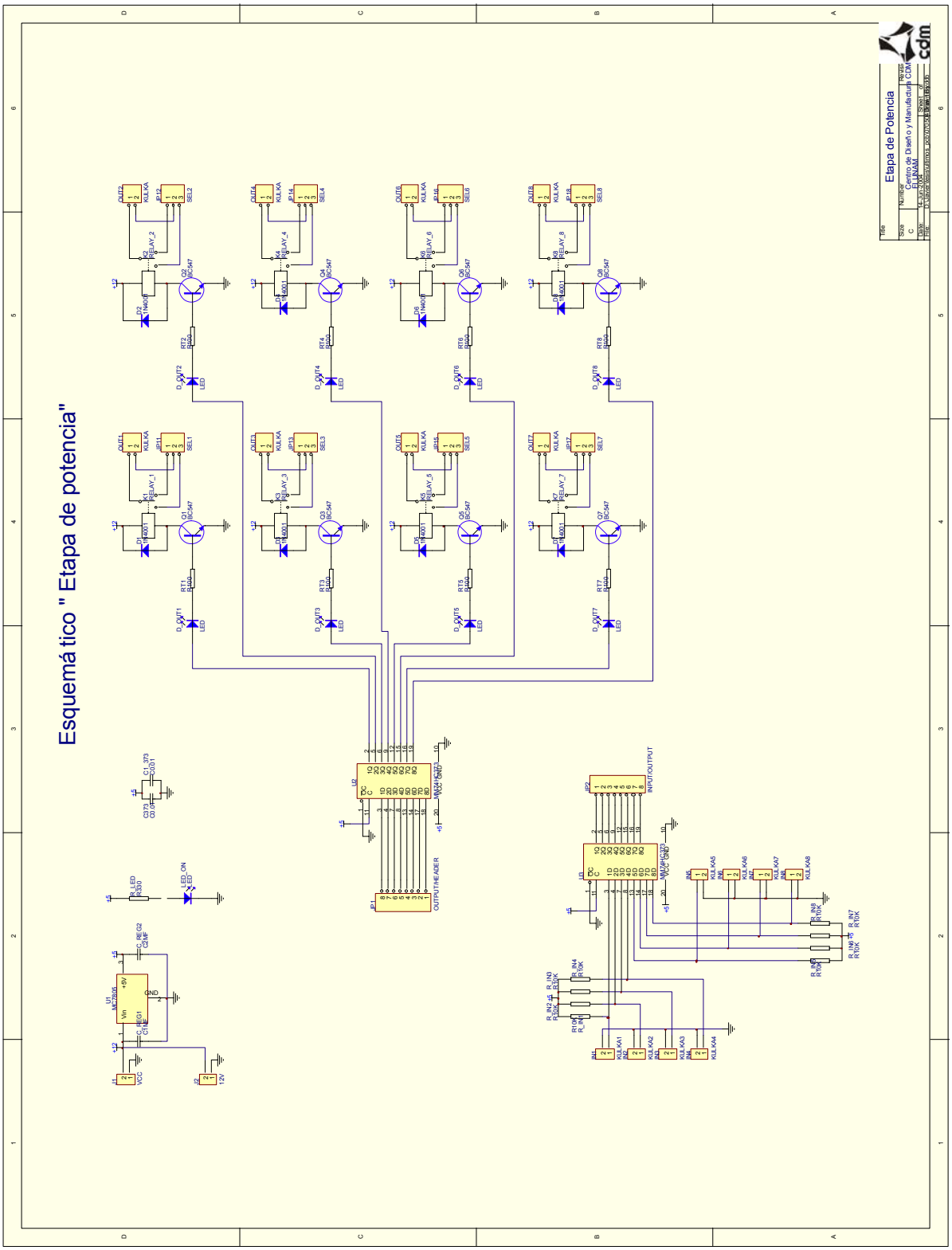


Diagrama 4. 6: Esquemático de la ETAPA DE POTENCIA

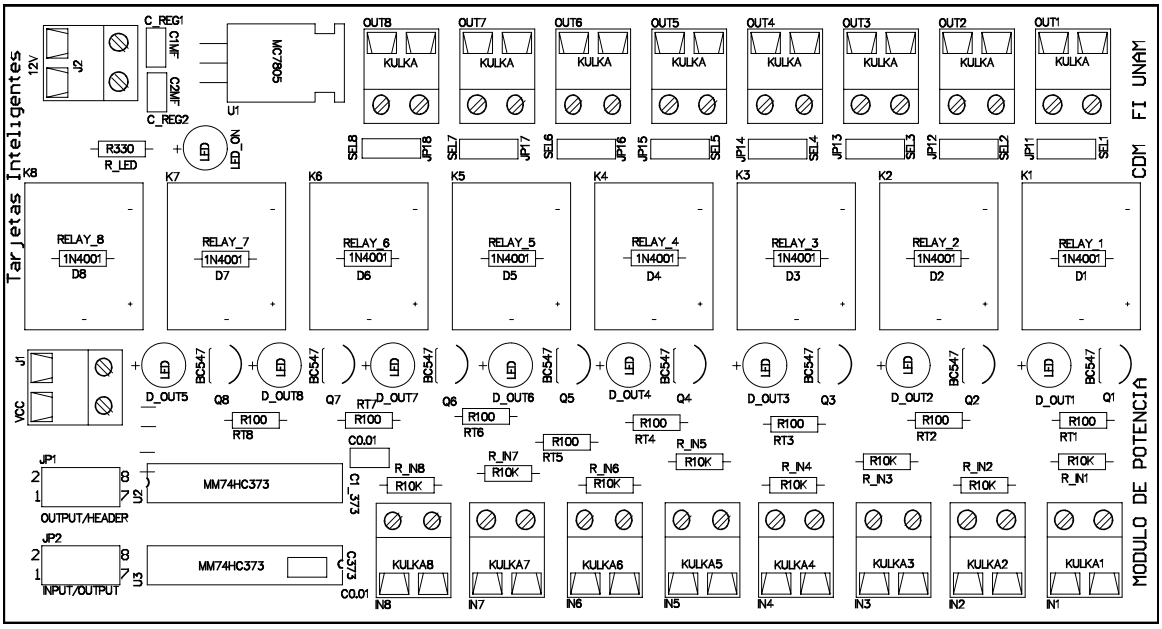


Figura 4. 14: Módulo de Potencia vista de arriba.

DISEÑO DEL FIRMWARE

Cuando la PC transmite hacia uno de los módulos TAG-PC, todos ellos recibirán y procesarán la información pero solamente uno de ellos ejecutara la instrucción que se le pida, cuando se halla ejecutado dicha instrucción responderá de dos diferentes formas:

1. Que se ejecuto exitosamente la instrucción que se pidió (en este caso cuando se activa o desactiva un actuador).
2. Mandar una respuesta a la instrucción que se pidió (lectura de sensores o lectura del sistema de identificación de personal).

En caso de que no se reciba respuesta por parte de alguno de los módulos TAG-PC, el software Sistema de Acceso a Personal y Protección de Equipos (S.A.P.P.E.), entenderá que la instrucción pedida no se ejecuto y volverá a enviarle de nuevo la instrucción, este proceso lo realizara tres veces, si no se obtuvo respuesta se generara un mensaje de error y continuará con el siguiente proceso.

La información que se transmite y se reciben de estos módulos esta en un protocolo de comunicación llamado Tiris Bus Protocol (TBP) SERIES 2000, del cual ya hablamos anteriormente, en este capítulo describiremos el funcionamiento de los módulos TAG-PC.

Descripción del firmware residente en el Módulo TAG-PC.

Los módulos estarán en espera de recibir información proveniente de la PC. Cuando la PC transmite información hacia alguno de los módulos, todos ellos lo reciben byte por

byte en su puerto de comunicaciones serial, siendo guardados en una sección de memoria RAM que esta destinada para recibir estos bloques.
Cuando se recibe el primer byte de este bloque (Star Mark), el programa interno del módulo comparara dicho valor con el inicio del mensaje que se tiene establecido.

$01_{Hex.}$ utilizando el protocolo de comunicación TIRIS BUS protocol.

La razón de realizar esta primera comparación es por que se espera el inicio de un mensaje, cualquier número diferente, la tarjeta lo tomara como mensajes incompletos o erróneos que al recibirlos los desechara y esperara a recibir un inicio de mensaje.

Cuando se recibe una trama correcta, pasa por varias subrutinas del programa en donde la instrucción contenida en el bloque de datos recibido es decodificada, validada ejecutada, ya terminadas estas tareas el módulo arma un bloque de datos en protocolo TIRIS BUS que codifica, y valida con la respuesta a la instrucción pedida por la computadora para enviársela a esta última. Estas subrutinas mencionadas, se utilizan para los comandos de lectura de sensores, habilitación y deshabilitación de actuadores.

Subrutinas para recibir información.

Decodificación: Como su nombre lo indica, esta subrutina decodifica la información proveniente del lector de acceso de personal o del bus de datos, si esta información proviene de este último, verifica que el mensaje enviado sea para la tarjeta TAG PC en cuestión, si es así, el control del firmware pasara a la siguiente subrutina, en caso contrario se desechara la información recibida y la tarjeta estará en espera de un nuevo bloque.

Esto lo hace por medio del byte destination address[21] del bloque de datos recibido en TIRIS BUS PROTOCOL y lo compara con el número de identificación propio de la tarjeta, si el byte destination address y el número de identificación de la TAG PC (ambos en hexadecimal) coinciden la información será para la TAG PC mencionada, de lo contrario, como se dijo en el apartado anterior se desechará.

Validación: esta subrutina se encarga de verificar que la información recibida no contenga algún error, esto lo realiza calculando el CRC del bloque de datos recibido y lo compara con el CRC (CRC1 y CRC2),- que esta incluido dentro del bloque de datos recibido. En caso de que no sean iguales el firmware volverá a reiniciarse para esperar una nueva trama de datos.

Para obtener el CRC del mensaje recibido, se aplica un XOR a cada uno de los bytes que comprende la trama de datos recibida (del byte 1 Destination address hasta el último byte del Data field), el resultado obtenido es la parte baja del CRC (CRC2), para obtener el CRC1 se obtiene realizando el complemento A1 del CRC2.

[21] Ver apéndice “protocolos de comunicación” referente al TIRIS BUS PROTOCOL (TBP).

Al ser iguales estos CRC, significa que no se tienen errores dentro de la trama de datos recibida y se pasa a la siguiente subrutina en la que se ejecutara la instrucción que se pide en caso de que la información provenga de la computadora; pero si viene del lector de baja frecuencia, se llevara a cabo las acciones antes indicadas en lectura del lector de acceso de personal.

Ejecución del comando[22]: en esta subrutina se lee el byte 3 (Message code), este byte nos indicara la instrucción a realizar, estas instrucciones son:

- Lectura de sensores.
- Habilitar o deshabilitar los actuadores.
- Lectura del lector de acceso de personal (la operación que se menciono anteriormente).

Lectura de sensores.

Cuando la PC requiere una **lectura de sensores**, el módulo internamente se dirigirá a uno de sus registros en donde esta contenida la información proveniente de los sensores, dicha información es obtenida a través del módulo de potencia (cabe mencionar que este módulo acondiciona las señales que emiten los sensores, a niveles de voltaje que el microcontrolador de la tarjeta TAG PC puede admitir).

Al obtener esta información el módulo TAG-PC se encargara de codificar la información obtenida, es decir armará un bloque de datos en TIRIS BUS PROTOCOL para poder mandarlo hacia la PC.

Lectura del lector de acceso de personal.

Por otro lado, cuando se recibe una trama con el comando de lectura del lector de acceso de personal, además de utilizar las subrutinas de decodificación y validación, para ejecutar la instrucción, se llevan a cabo las siguientes instrucciones:

- Se arma un bloque de datos con un protocolo diferente (HOST PROTOCOL) para enviarse al lector, y se transmite con el estándar de comunicación RS232.
- La respuesta obtenida puede ser de dos formas[23]: la primera que no se leyó alguna credencial al momento de que se pidió la información, esta respuesta tiene longitud de un byte. La segunda se leyó alguna credencial y tiene una longitud de cuatro bytes dicha respuesta.
- La respuesta obtenida del lector en HOST PROTOCOL se decodifica y se valida, para volverse a codificar, validar y enviar en TIRIS BUS PROTOCOL ahora a la computadora, haciendo el TAG PC el cambio al estándar de comunicación RS-485

[22] esta subrutina es unicamente cuando la información proviene de la computadora.
[23] Para mayor referencia ver el apartado referente al host protocol series 6000.

Habilitación deshabilitación de actuadores.

Cuando la computadora manda a habilitar o deshabilitar un actuador, en el bloque de datos recibidos viene la información (dos bytes de longitud), que especifica el número de actuador y el estado (encendido o apagado) que se quiere, el módulo internamente se direcciona para mandar la información hacia la etapa de potencia. La etapa de potencia tiene la capacidad de controlar a ocho actuadores a través de sus relevadores, y para poder encender alguno de ellos se activara con un "1" lógico y para apagarlo se tendrá un " 0 " lógico.

Al realizar el proceso anterior, el módulo procederá a enviarle a la PC un mensaje en la cual le indica que la operación que se le mando a realizar fue exitosa, dicha respuesta tiene un byte longitud y de la misma forma que en el caso anterior la respuesta pasa por la subrutinas **de Codificación, Validación y transmisión** de los datos hacia la PC.

Subrutinas para enviar información.

Codificación: Esta subrutina se encarga de codificar la información que enviará a la computadora en TIRIS BUS PROTOCOL, con la información solicitada por la computadora.

Validación: esta subrutina realiza los siguiente procesos para enviar la información hacia la PC

- Adicionarle a la trama de datos cuantos son los bytes de respuesta, Byte 4 (Data Length).
- Elaborar el CRC que contendrá la trama de datos.
- Adicionar el CRC al Bloque de datos.

Transmisión de los datos: por último la información generada por el Módulo TAG-PC es enviada hacia la PC, cuando es enviado el último byte, el programa interno se reinicializa para esperar de nuevo un bloque de datos.

Subrutina de emergencia.

El firmware controla de manera independiente un botón de emergencia, esto es el módulo tiene la capacidad de accionar dos actuadores (apertura de la puerta y encendido de la alarma local) al momento de accionar dicho botón, esta acción se realiza cuando se presente un evento anormal en el sistema (falla en la comunicación PC con el módulo TAG-PC, siniestros, incendio, temblores, etc.).

Al presentarse este caso la tarjeta TAG-PC mandará un mensaje a la PC, informándole que ha ocurrido alguna emergencia, y solo se podrá desactivarse reiniciando la tarjeta manualmente con el interruptor de reset contenido en la TAG-PC, hay que hacer notar que la PC no tiene la facultad de deshabilitar la apertura de puerta o apagar la alarma al presentarse dichos eventos.

Otra característica del firmware.

La tarjeta tiene activada una opción llamada watch dog (perro guardián) que es una característica propia del microcontrolador, la cual, si por algún motivo se pierde comunicación entre la PC y los módulos TAG-PC en un cierto intervalo de tiempo (aprox. 100 ms.), tiene la capacidad de reinicializarse.

El diagrama de flujo del programa interno de la tarjeta es el siguiente:

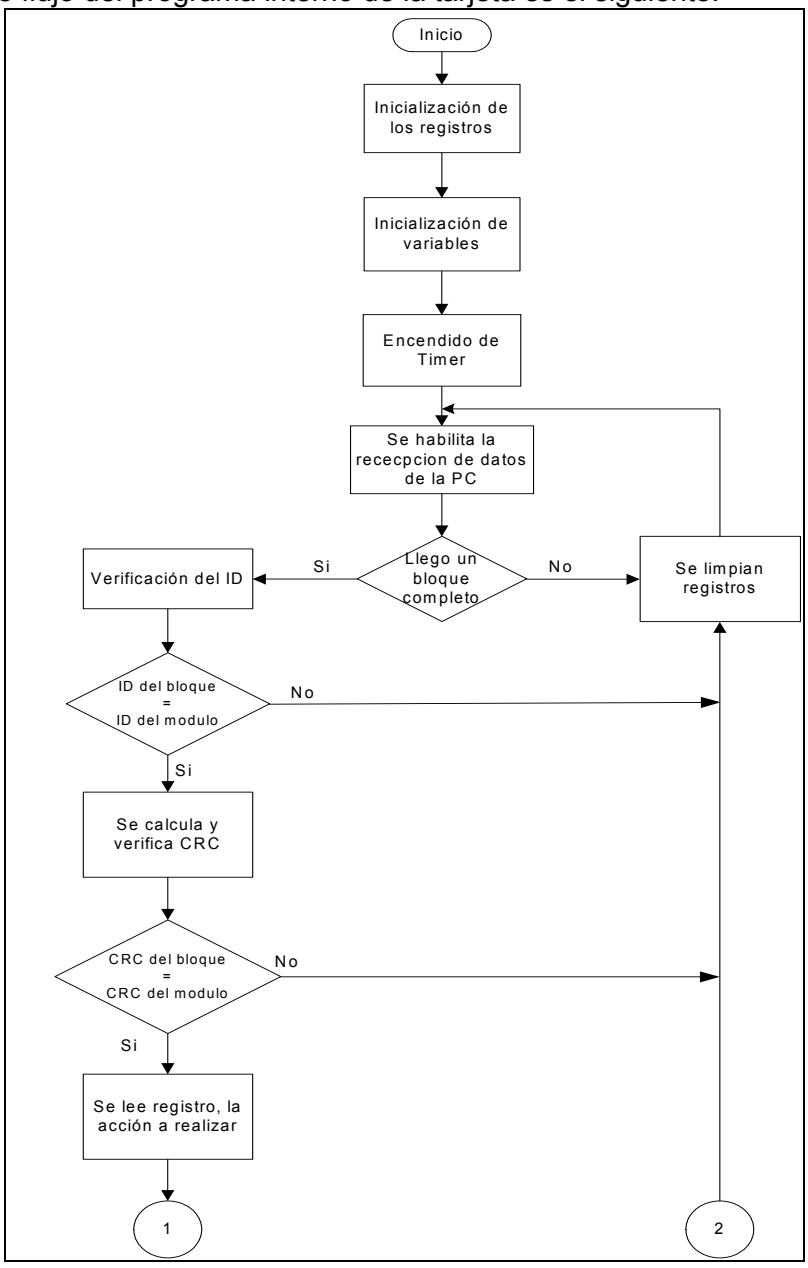


Diagrama 4. 7: De flujo del microcontrolador.

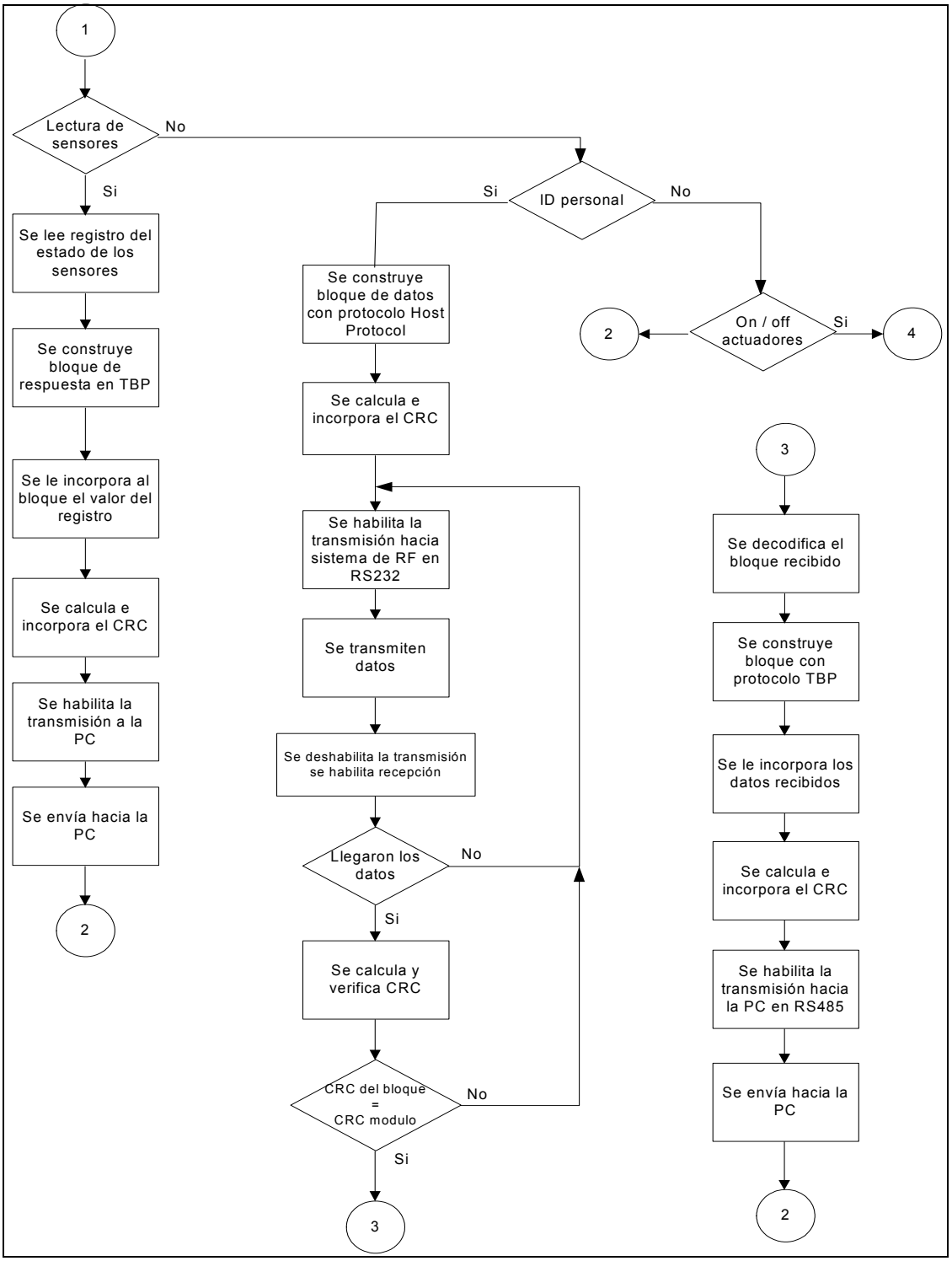


Diagrama 4. 8: De flujo del microcontrolador.

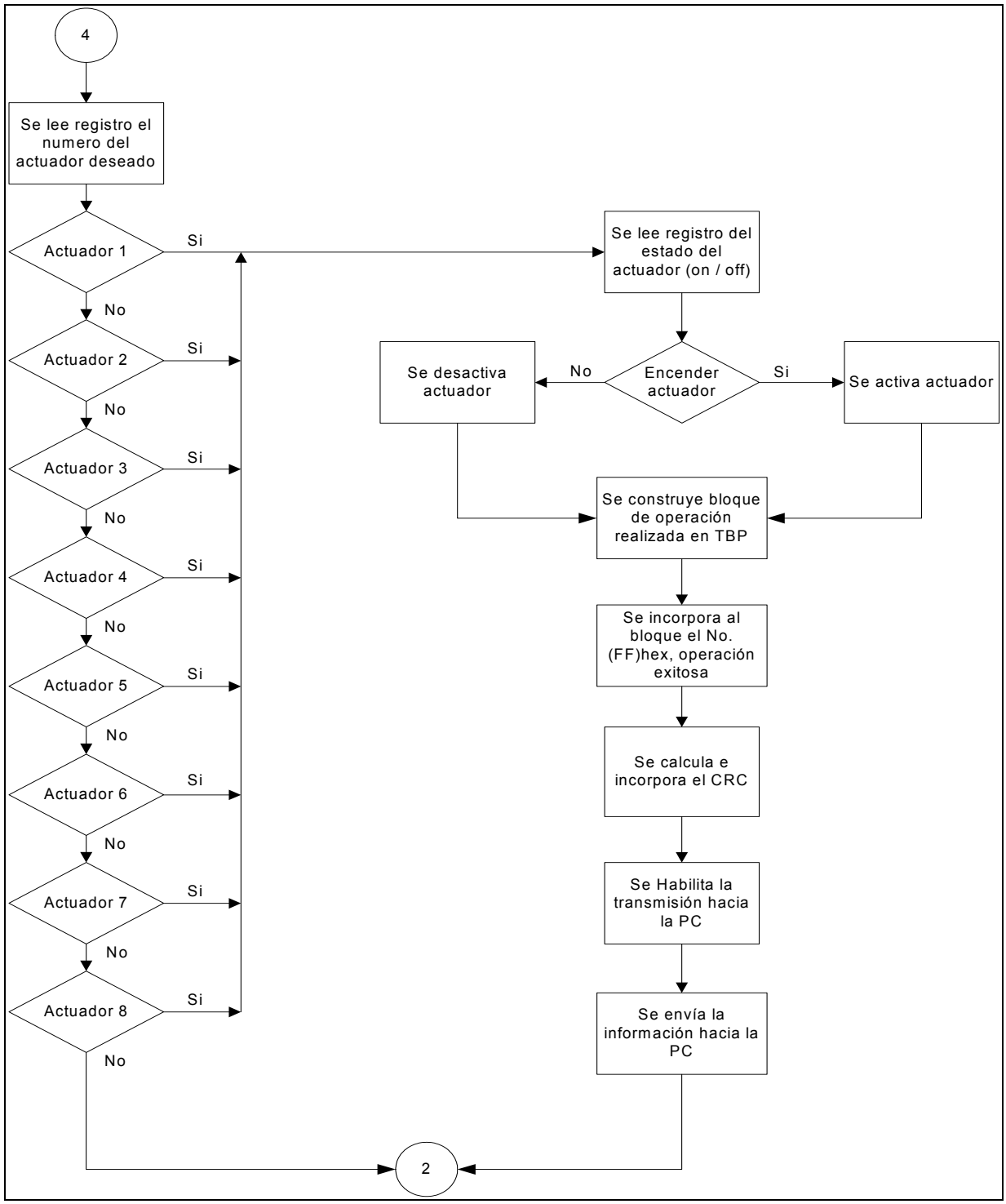


Diagrama 4. 9: De flujo del microcontrolador.

DISEÑO DEL SOFTWARE PRUEBA INTEGRAL PARA LECTORES (PIL).

Antes de comenzar como esta diseñado este programa y posteriormente las pruebas que se realizaron con este, comenzaremos por dar una explicación del puerto serial.

Puerto de comunicaciones: Las señales disponibles en un conector RS232 (ver figura 4.15 y tabla 4.11) están pensadas únicamente para asegurar la correcta transmisión y recepción de datos desde un equipo denominado DTE. (Data terminal Equipment – Equipo terminal de datos) a un DCE (Data Communication Equipment – Equipo de Comunicación de Datos), Un DTE es generalmente un ordenador y un DCE un MODEM (aunque en la aplicación son los lectores PC - TAG y S2000).

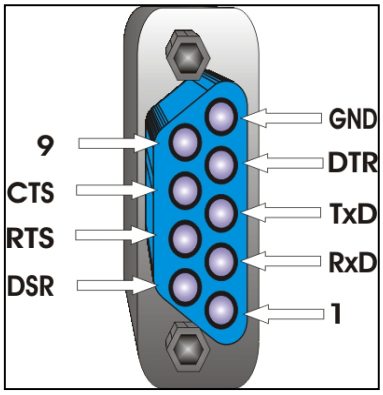


Figura 4. 15: Puerto Serie RS - 232

	Nombre de Señal	Dirección	Función
TxD	Transmited Data	Hacia DCE	Salida de datos DTE
RxD	Received Data	Hacia DTE	Entrada de datos DTE
RTS	Request to send	Hacia DCE	DTE desea cambiar a modo transmisión
CTS	Clear to send	Hacia DTE	DCE listo para transmitir
DSR	Data Set Ready	Hacia DTE	DCE listo para comunicar con DTE
GND	Signal Common		Línea común del circuito (masa)
9	Data carrier Detect	Hacia DTE	Detectar si esta conectado
DTR	Data terminal Ready	Hacia DCE	Pone a trabajar el modem
1	Ring Indicator	Hacia DTE	Anuncia una llamada

Tabla 4. 11: Función de las señales encontradas en un puerto serie.

Las señales usadas en la aplicación son:
TxD se encarga de transportar los datos serie hasta los lectores TAG-PC y S2000, para ello han tenido que activarse RTS, CTS, DSR y DTR.

RxD, recepción de datos, no depende de ninguna otra función RS232 .

RTS y CTS: tienen como función conmutar los lectores TAG-PC y S2000 trabajando en un modo Semi – Duplex en modos de recepción y transmisión. En la comunicación del sistema, dichas terminales no se tomaron en cuenta para la configuración del puerto porque el conector de conversión RS232 a 485/422 se encarga de manejar dichas señales.

Una vez que el puerto de comunicación RS232 se encuentra abierto, DTR deberá permanecer activa mientras dure la conexión; si se inhibe, se produce la desconexión, interrumpiendo bruscamente el enlace.

Comunicaciones con el puerto serie: Para la gestión de los puertos de comunicaciones. Lo primero que hay que pensar es que los datos llegan a los puertos de forma asíncrona, es decir, su llegada es imprevisible, aunque en la aplicación no es de esta manera ya que los lectores TAG-PC y S2000 son unidades esclavas y no hacen nada sino hasta que el control maestro se los ordena, pero el tiempo de respuesta varía de acuerdo a la orden ejecutada, por ejemplo: no es el mismo tiempo que se ocupa para leer un transponder que el tiempo que se emplea para leer el estado del puerto de entrada de los lectores.

Esto supone que al recibir la respuesta hay que procesarla inmediatamente para limpiar el bus de datos de entrada y salida del puerto de comunicaciones, puesto que van a enviarse y recibirse más datos. De esta tarea se encarga el Hardware de la PC, de forma que cuando detecta la llegada de un dato, interrumpe el flujo normal del proceso para ceder el control a la rutina de proceso de comunicaciones. Esta rutina tiene que ser una rutina de Windows en lugar de una rutina de la aplicación. Esto es así por dos razones:

Windows debe mantener el control de la multitarea, si la llegada de un dato hiciera que se transfiriera el control del procesador a la aplicación, Windows perdería su habilidad para gestionar la multitarea, esto quiere decir que Windows tiene que estar entre la aplicación y el hardware.

Windows no puede dirigir el dato recibido directamente a la aplicación ya que para que suceda esto, la aplicación interesada deberá de pedir la propiedad del puerto anteriormente. La razón es que los datos que se reciben en el puerto de comunicaciones no llegan con la Identidad de la aplicación que los tiene que recibir. Por lo tanto, Windows tiene que guardar en un buffer los datos que llegan para una aplicación.

Cuando una aplicación solicita a Windows la propiedad de un puerto, Windows sólo se lo dará si ninguna otra aplicación lo tiene. Por el mismo motivo, mientras una aplicación tiene el control de un puerto, Windows se lo prohíbe a las demás aplicaciones que lo soliciten, cuando la aplicación finalice la operación de Entradas y Salidas con un puerto, debe dejar el control del mismo para que otras aplicaciones puedan utilizarlo, lo cual requiere llamar a la función que permite cerrar el puerto.

De lo expuesto anteriormente, la aplicación debe haber pedido a Windows la propiedad del puerto utilizando la función correspondiente. Esta misma función establece dos búferes uno para la entrada y otro para la salida.

Para establecer una comunicación, de forma general se deben seguir los siguientes pasos:

- Abrir el puerto de comunicaciones COM1, COM2, COM3 etc.
- Establecer la máscara de comunicaciones para especificar los eventos que serán atendidos.
- Definir el tamaño de los búferes de las colas de entrada y salida.
- Construir una estructura de tipo DCB (Device Control Block) que especifique la configuración del puerto. Esta estructura contiene, entre otros, los datos velocidad de transmisión, paridad, bits por carácter y bits de parada.
- Configurar el puerto con los datos de la estructura de tipo DCB.
- Enviar datos al puerto de comunicaciones.
- Recibir datos por el puerto de comunicaciones.
- Verificar errores
- Cerrar el puerto cuando la comunicación haya finalizado.

Aunque son varias las propiedades del puerto de comunicación RS232, el Programa Integral para Lectores (P.I.L.) usa solo algunas, pero pensando en futuros proyectos que usen el puerto de comunicaciones el programa se implemento de forma que se pueda configurar el puerto de diversas maneras.

Ya que se conoce el protocolo y el funcionamiento del puerto serie se esta listo para iniciar la aplicación del Programa Prueba Integral para Lectores TAG y Series2000 (P.I.L.).

Prueba Integral para Lectores (PIL).

El lenguaje que se uso para la aplicación PIL, fue Visual Basic, porque es actualmente el lenguaje de programación más popular del mundo, se trata de un producto con una interfaz gráfica de usuario que sirve para crear aplicaciones para Windows basado en el lenguaje Basic.

La palabra Visual hace referencia al método que se utiliza para crear la interfaz gráfica de usuario instrucciones, funciones y palabras clave, muchas de las cuales están directamente relacionadas con la interfaz gráfica de Windows, en lugar de escribir numerosas líneas de código para implementar una interfaz, se utiliza el ratón para arrastrar y colocar los objetos prefabricados en el lugar deseado dentro de un formulario, permitiendo así un buen entorno para el desarrollo de PIL.

Visual Basic 6 incluye un control personalizado, Microsoft Communications Control, que permite establecer una comunicación serie entre dispositivos, basado en el estándar RS232, de una forma rápida y sencilla. Para poder utilizar este control en una aplicación, hay que añadir al proyecto el control ActiveX mscomm32.ocx para aplicaciones de 32 bits.

Diseño de las interfaces de P.I.L.

Se diseñaron cuatro Interfaces para el programa:

- Interfaz Principal.
- Interfaz NumPuerto.
- Interfaz ConfigPuerto.
- Interfaz AgregarElemento.

}Interfaz principal.

La interfaz Principal llamada así por ser la que a través de ella se logra la comunicación con las otras tres y siempre está presente mientras se ejecute P.I.L, es el contenedor para las funciones y los controles principales del programa

Menús de la interfaz principal: En la figura 4.16 se pueden ver la barra de menús de la interfaz principal y en la tabla 4.12 la descripción de las ordenes de cada instrucción.

Figura 4. 16: Menús de la Interfaz Principal.

	ORDENES.	DESCRIPCIÓN.
Fichero	Abrir	Presenta la ventana de dialogo abrir para buscar ficheros con la Información de comandos generados anteriormente, al crearlos se les asigna la extensión .sap (valor predeterminado en la caja de dialogo).
	Guardar	Si el fichero no existe se crea uno nuevo, pero si el archivo ya contiene información esta se sustituye por la contenida en la Lista de Elementos Activos.
	Guardar Como	Siempre crea un nuevo fichero, pero si se abrió un fichero y se desea conservarlo sin guardar los cambios entonces esta opción es la adecuada ya que deja intacto el fichero anterior y genera uno nuevo.
	Salir	Termina con la ejecución del programa y descarga, si los hubiera, todos los formularios.
Configurar Puerto	Configurar Puerto	Llama a la Interfaz NumPuerto (más adelante se vera la forma de la interfaz)
	Cerrar Puerto	Esta opción del menú llama a la Subrutina ChecarPuerto( ) para verificar el estado del mismo, si el puerto de comunicaciones estuviera ya en uso por P.I.L. lo cierra, pero si aún no se ha abierto no hay cambios en el puerto.
Borrar	Borrar Elemento	Borra el comando seleccionado en la Lista de Elementos Activos, si no existe elección se presenta un mensaje al usuario para que seleccione el comando.

	Borrar toda la lista	Borra todo el contenido de la Lista de Comandos Activos.
Tiempo	Buscar tiempo	Sirve para conocer el tiempo que tarda en enviarse un comando, más el tiempo de respuesta del lector. Para usarlo, es necesario seleccionar el comando y después seleccionar la orden Buscar Tiempo, el tiempo de respuesta se presenta en la caja de texto del extremo superior llamada TRespuesta (el tiempo se presenta en milisegundos).

Tabla 4. 12: Descripción de los menús de la interfaz principal.

Interfaz NumPuerto.

Se usa para seleccionar el número de puerto que se usara en la aplicación (COM1, COM2, etc.). P.I.L. busca los puertos de la PC desde el puerto 1 (COM1) hasta el puerto 15 (COM15) y sólo agrega a la lista los puertos disponibles, de la lista de puertos se puede seleccionar cualquiera de ellos, por default se presenta el primero encontrado.

Tiene un fichero con la orden Salir sin configurar la cual nos permite cancelar la operación de seleccionar el puerto, aunque es importante mencionar que cada vez que llamamos a esta interfaz se cierra el puerto de comunicaciones. La ventana de NumPuerto se puede observar en la figura 4.17

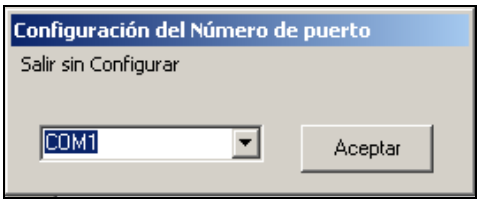


Figura 4. 17: Interfaz NumPuerto.

Interfaz ConfigPuerto.

Dicha ventana sólo se presenta si se ha seleccionado un puerto de comunicación, la llamada es automática al presionar aceptar en NumPuerto, donde se determinan las propiedades del puerto, como valores determinados se usan las propiedades del TIRIS BUS PROTOCOL (figura 4.18).

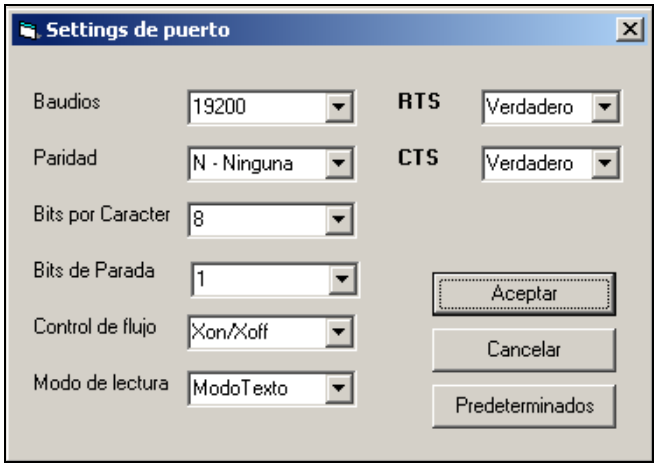


Figura 4. 18: Interfaz ConfigPuerto.

Funciones de interfaz principal: Las funciones principales de esta ventana (figura 4.19), están representadas por los botones que llaman a las rutinas de P.I.L (ver tabla 4.13).

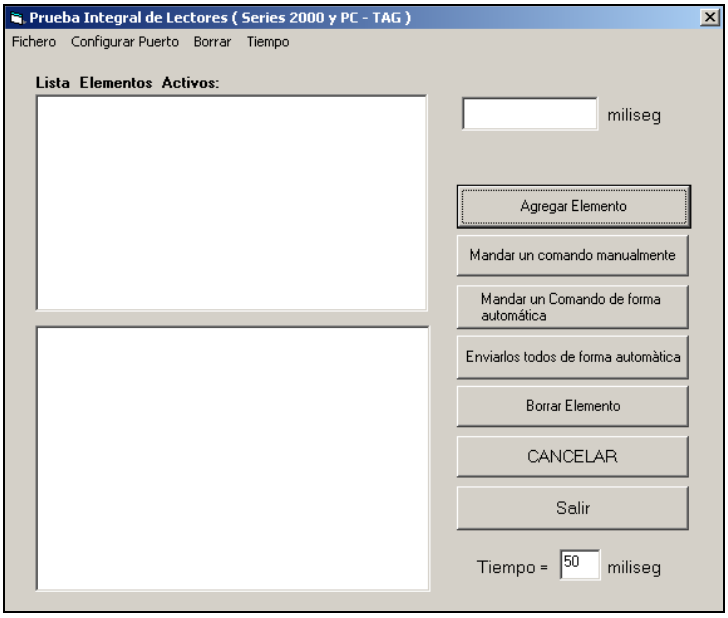


Figura 4. 19: Ventana de la Interfaz Principal.

FUNCION	DESCRIPCIÓN
Agregar Elemento	Llama a la interfaz Agregar Elemento para que se definan las características del comando a anexar (más adelante se dará una explicación más detallada).
Mandar un comando manualmente	Sólo manda una vez el comando y la respuesta se presenta en la lista de Respuestas, cada vez que se activa el botón. Si no hay un comando seleccionado se presenta un aviso (figura 4. 21).

Mandar un comando de forma automática	Esta función envía el comando continuamente y presenta las respuestas del lector en la lista de Respuestas.
Enviarlos todos de forma automática	Se envían los comandos por orden de aparición de la lista de Elementos a un mismo tiempo y las respuestas se presentan en la lista de respuestas. Si no se hay comandos entonces la función no se lleva a cabo y muestra un aviso (figura 4.22).
Borrar Elemento	Cuando es necesario borrar un comando de la lista de Elemento se selecciona el comando y después se presiona este botón, si no hay elemento seleccionado se da un aviso (figura 4.21).
CANCELAR	Detiene la ejecución de las funciones manda un comando o todos de forma automática.
Salir	Cierra la aplicación, el puerto y descarga todas las interfaces cargadas en memoria.

Tabla 4. 13: Funciones de la interfaz principal.

Tiempo : Función para variar el tiempo de envió (figura 4.20), al situar el cursor del ratón en la caja, esta se activa y se puede especificar el tiempo comprendido en el intervalo de 0 hasta 5000 ms (5 seg) no admite valores alfanuméricos, para otro valor fuera del intervalo, el tiempo especificado por la caja Tiempo retorna a 50 ms. El tiempo se puede variar en cualquier instante y se actualizara en el siguiente envió de comandos.

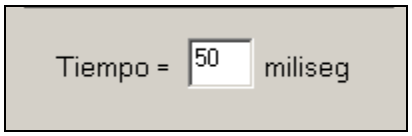


Figura 4. 20: Caja de Texto Tiempo (parte inferior izquierda de la Interfaz Principal.)

Figura 4. 21: No se selecciono un comando en la lista de Elementos.

Figura 4. 22: No Existen comandos en la Lista de Elementos.

Interfaz AgregarElemento.

Es la Interfaz encargada de adicionar en memoria y en la lista de elementos los comandos a usar en P.I.L.. El nombre del comando es opcional pero es conveniente asignarle uno para que este se anteponga a la respuesta del Lector, la dirección y código son obligatorios de otra manera no se genera el comando, el mensaje, no todos los comandos requieren de este dato.

Una vez que P.I.L. tiene los datos antes mencionados genera con ellos el comando y le anexa dos bytes con el cálculo de error XOR.

Para observar el comportamiento de esta Interfaz se mostrara con un ejemplo:

Se adicionara un comando con las siguientes propiedades (ver figura 4.23):

Orden: Leer Series2000.
Nombre: Series2000 Dir 08.
Dirección o ID de Lector: 08.
Código: 20 código de lectura de transponder.
Mensaje: ninguno.

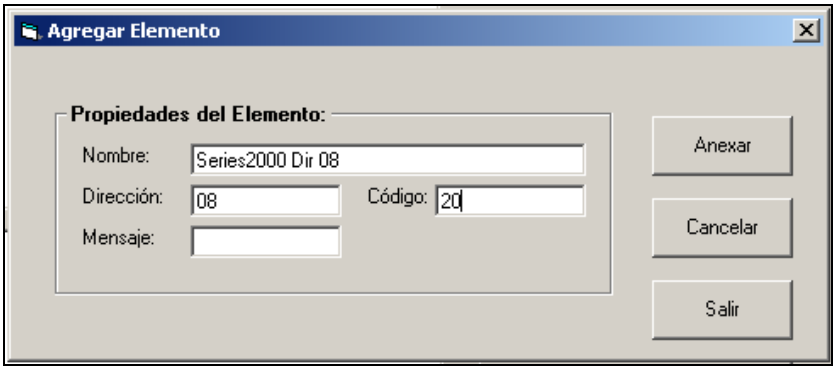


Figura 4. 23: Ventana de la Interfaz Agregar Elemento con los datos del ejemplo.

El comando generado es 0108002000D72804, este se muestra en la Lista de Elementos de la InterfazPrincipal (figura 4.24).

Figura 4. 24: Lista de Elementos con un comando.

Por último presentamos el diagrama de flujo de P.I.L para la validación de los datos.

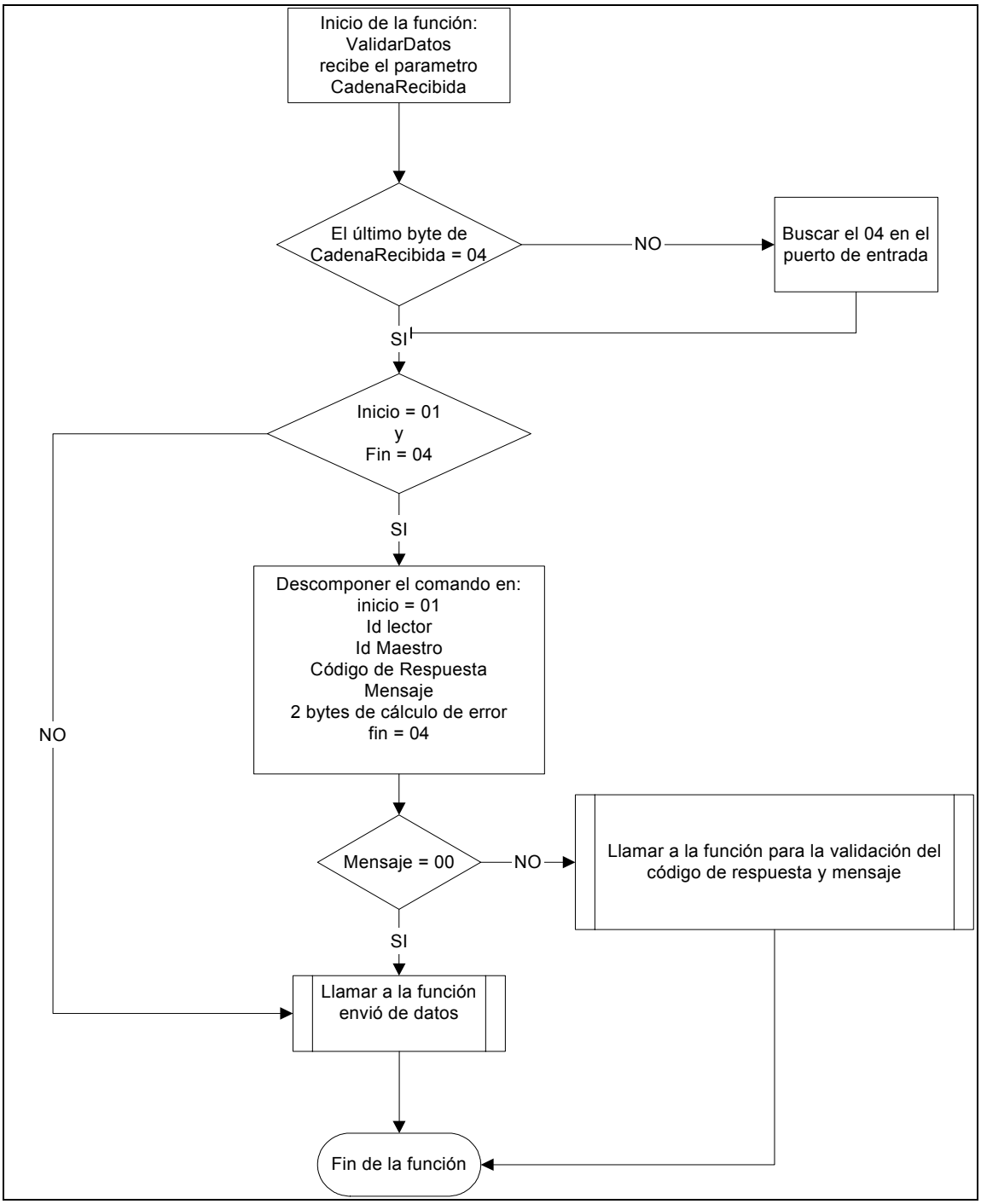


Diagrama 4. 10: de flujo de validación de datos.

DISEÑO DE SAPPE[24].

El principal objetivo de diseñar el programa de manera modular (ver diagrama 4.11), fue debido a que se deseaba obtener un sistema que pudiera ser fácilmente adaptado a otras instalaciones de la Facultad de Ingeniería, facilitando no sólo su programación sino su mantenimiento y expansión.

- Comunicaciones
- Interfaz de Usuario
- Base de Datos
- Seguridad

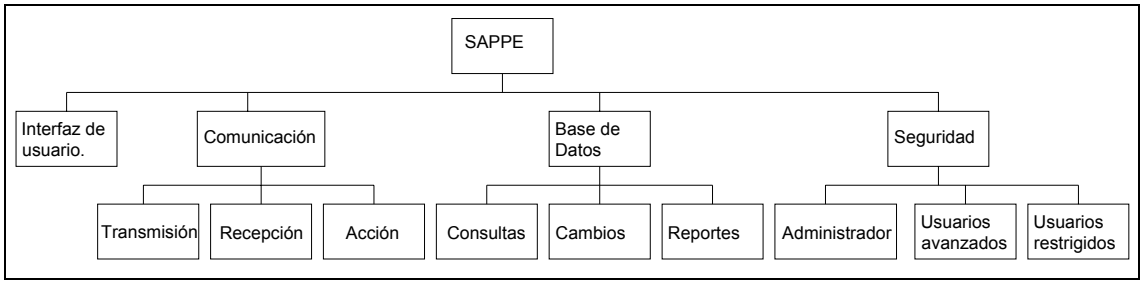


Diagrama 4. 11: a bloques del programa SAPPE.

Módulo de comunicaciones

El módulo de comunicaciones es el enlace directo entre el hardware y el software, debido a su complejidad la generación de éste módulo implicó varias etapas de diseño y reestructuración para obtener una aplicación completa y eficiente que cubriera todas las expectativas del sistema.

En el caso del proyecto, se tiene un sistema de comunicación maestro-esclavo, donde la computadora es el maestro que transmite la orden a los esclavos y recibe la respuesta dada por ellos. Por lo tanto en el módulo de comunicación se consideran los siguientes submódulos:

1. Submódulo Interfaz de Comunicaciones: es una parte de software que manipula directamente la configuración del puerto serie.
2. Submódulo Transmisión: Contempla desde la formulación del mensaje que será enviado al hardware, el cálculo de un código de detección de errores para prevenir la corrupción del mensaje y la codificación del mensaje de manera que la cadena enviada corresponda con los parámetros utilizados por el protocolo de comunicación.
3. Submódulo de Recepción: Involucra básicamente tres pasos al igual que en la transmisión, por un lado la decodificación de la cadena recibida de manera que

[24] Cabe señalar que este programa se encuentra registrado ante el Instituto de Derechos de Autor ISBN 970-32-0446-5 con derechos para la UNAM.

podamos interpretarla, posteriormente decomponer la cadena para obtener los datos importantes y finalmente aplicarle un método de detección de errores para verificar que el mensaje haya llegado correctamente.

En este módulo de comunicación se diseñaron los elementos básicos para establecer un sistema de comunicación con el hardware que involucra los TAG PC y los lectores series 2000, donde la computadora controla la transmisión de la información de manera que el hardware se mantiene como receptor a menos que la computadora le envíe una instrucción, a la que deberá de dar una respuesta a la computadora.

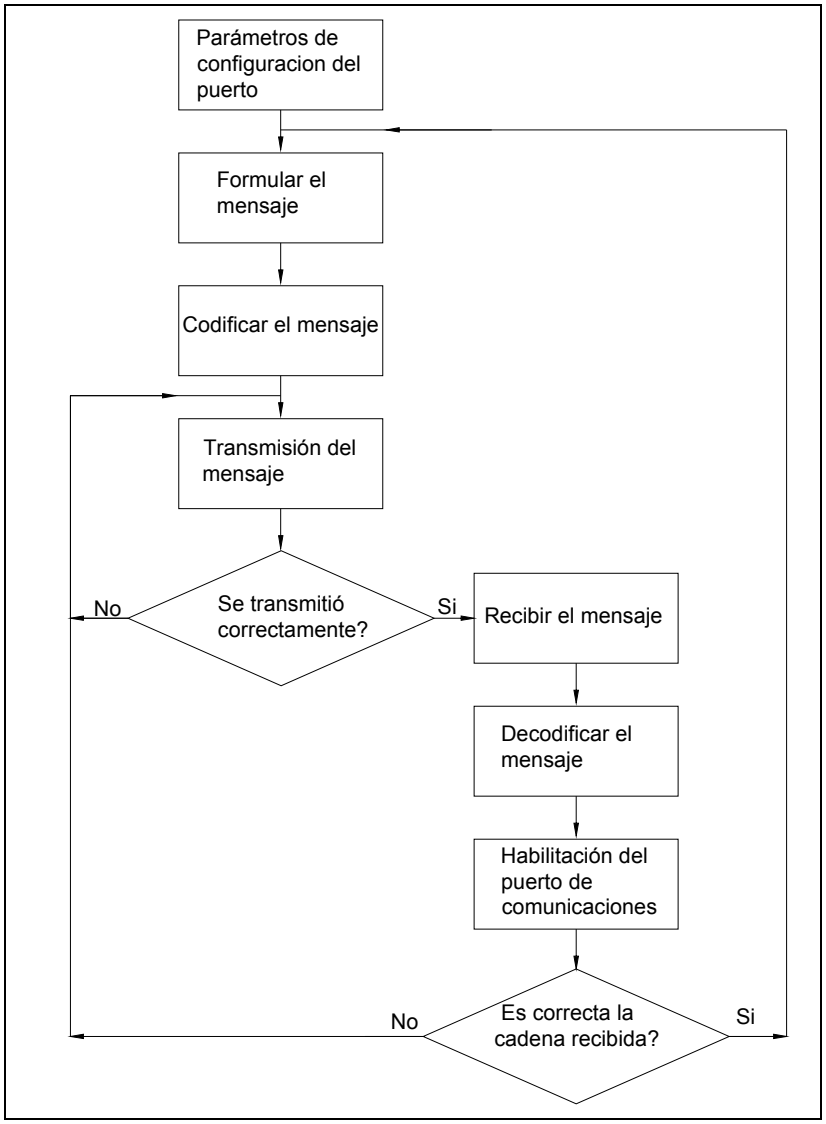


Diagrama 4. 12: de flujo del módulo de comunicaciones.

Una vez que se logro establecer con éxito la comunicación entre el hardware y la computadora (figura 4.25), el siguiente paso fue un diseño que implicó establecer los procedimientos de operación del sistema de manera que el software tuviera la capacidad de tomar decisiones ante la información recibida y ejecutar las rutinas de seguridad correspondientes.

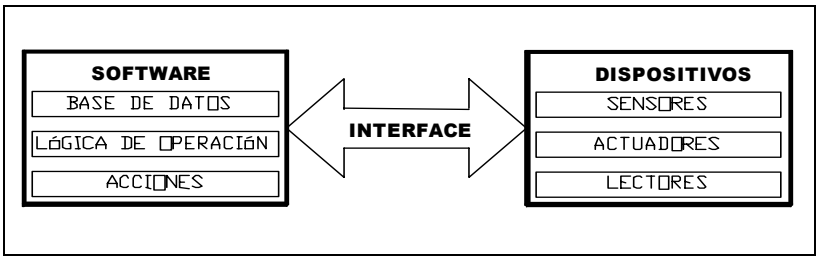


Figura 4. 25: Integración de los elementos que contemplan los dispositivos y el software

El software se diseñó con tres procedimientos adicionales: la comparación de los datos recibidos contra la Base de Datos, un proceso de validación de los datos obtenidos mediante una lógica de operación y finalmente la determinación de las acciones de emergencia para que puedan ser ejecutadas por los actuadores (diagrama 4.13).

De esta forma el sistema completo queda estructurado de la siguiente manera:

1. Envió de mensaje a una tarjeta TAG PC o lector SERIES 2000.
2. Recepción de la respuesta del mensaje enviado.
3. Validación del Mensaje Recibido.
4. Decodificación del Mensaje.
5. Comparación del ID contra la Base de Datos.
6. Evaluación de la información obtenida mediante la lógica de operación.
7. Acción a seguir de acuerdo a la lógica de operación.
8. Codificación de la instrucción.
9. Transmisión de la instrucción.

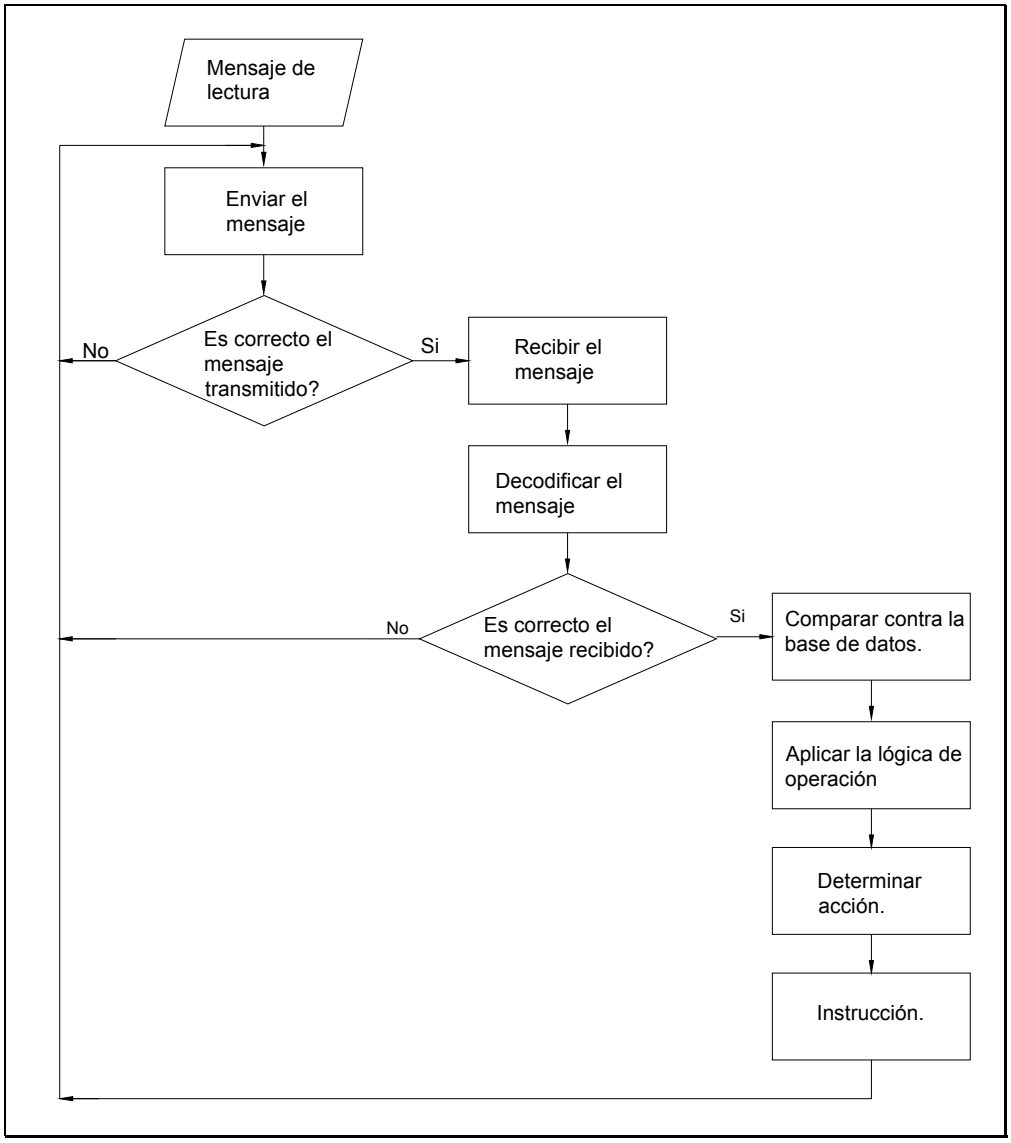


Diagrama 4. 13: De procedimientos del software.

La primer estrategia de seguridad que se diseño, se enfocó a la protección del personal así como de los bienes involucrados mediante el control de acceso. Por lo tanto la estrategia se dividió en dos funciones principales: control de accesos y salidas de personal y, control de salida de equipo (ver diagrama 4.14).

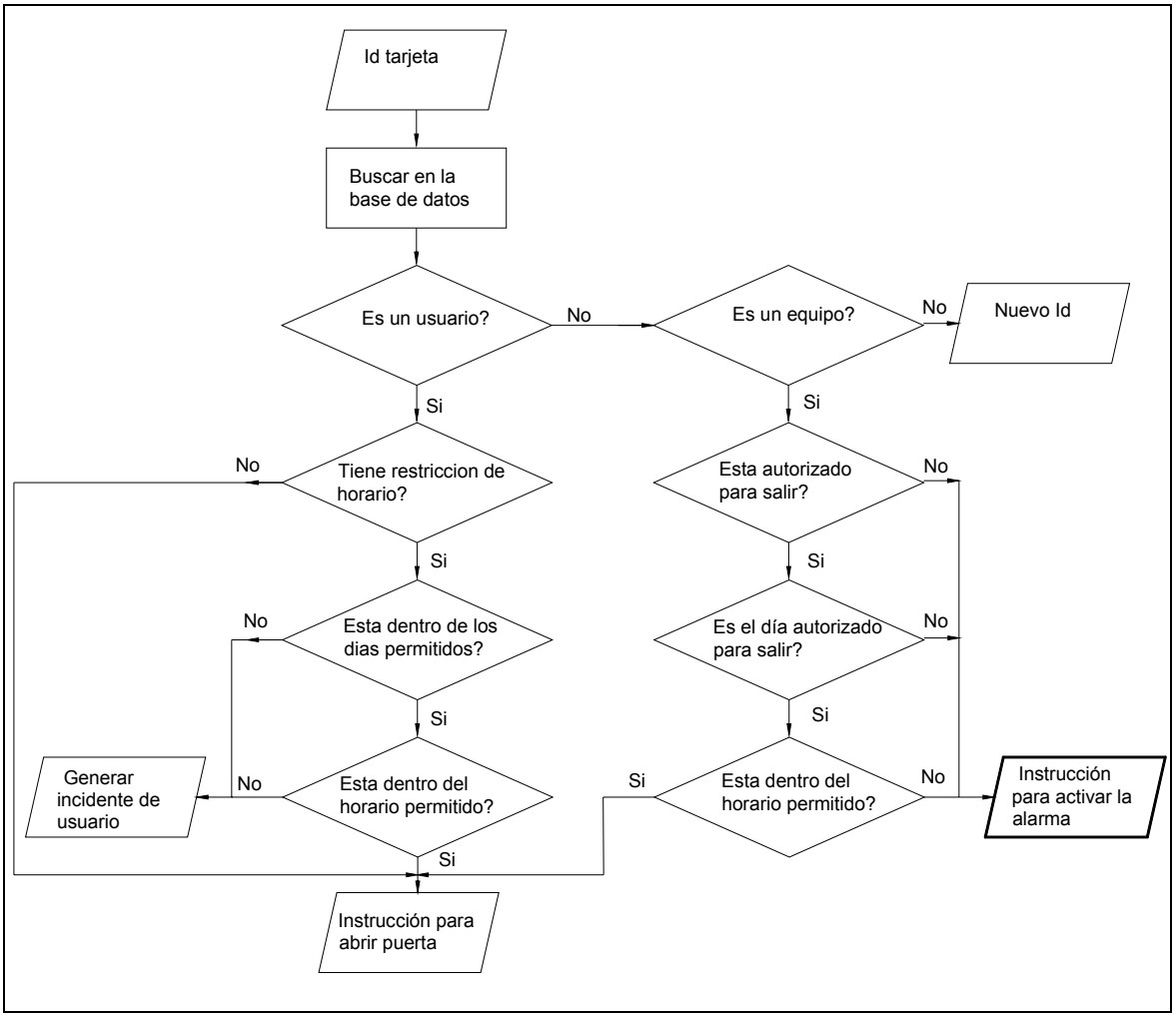


Diagrama 4. 14: de control de accesos.

Estructura del Hardware del sistema

En primer lugar se vio que el diseño estaba contemplado para un número determinado de dispositivos, lo que resultaba sumamente ineficiente. Para ello se definió los elementos del hardware, de manera que pudieran ser divididos en procesos independientes facilitando en un futuro la adición de otros dispositivos.

Como resultado de esta fragmentación del hardware se requirió una función que permitiera generar instrucciones de control específicas por cada dispositivo de acuerdo a sus características.

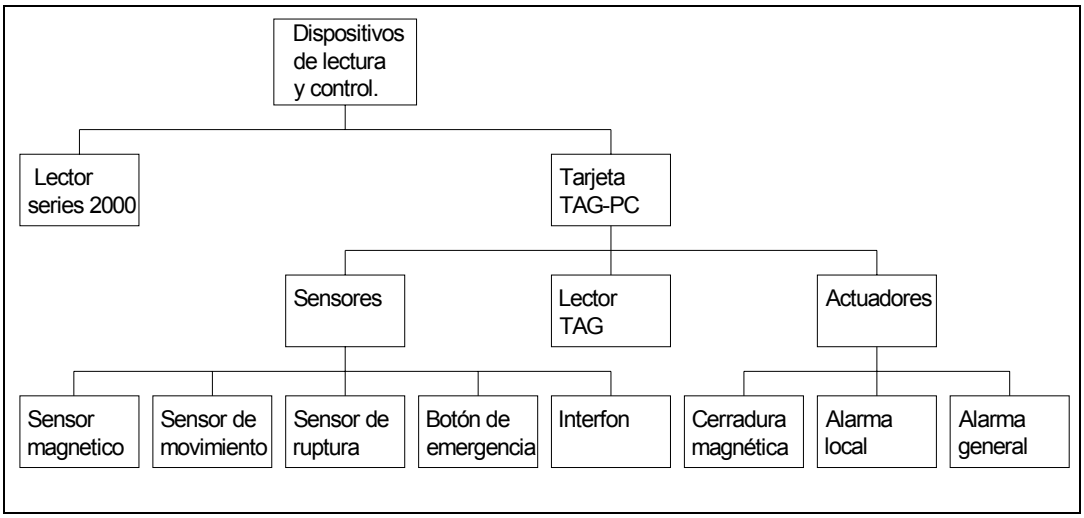


Diagrama 4. 15: Estructura del hardware del sistema.

Lógica del hardware

Por lo tanto, se definieron los comandos de operación de tal forma que permitieran obtener una secuencia lógica para la generación automática de instrucciones (Ver tabla 4. 14).

Dispositivos		Comando												
		Operación	Inicio de Mensaje	Dirección Destino	Dirección Origen	Código del Mensaje	Longitud del Mensaje	Dato 1	Dato 2	Dato3	Dato 4	CRC 1	CRC 2	Fin de Mensaje
TAG	Antena	Lectura	01	DD	DO	11	00					CRC 1	CRC 2	04
		Respuesta (Si detectó tarjeta)	01	DD	DO	01	04	ID 1	ID 2	ID 3	ID 4	CRC 1	CRC 2	04
		Respuesto (No detectó tarjeta)	01	DD	DO	01	00					CRC 1	CRC 2	04
	Dispositivos Electrónicos de Detección	Lectura	01	DD	DO	33	01	Dirección Sensor				CRC 1	CRC 2	04
		Respuesta (Activo)	01	DD	DO	33	02	Dirección Sensor	01			CRC 1	CRC 2	04
		Respuesta (Inactivo)	01	DD	DO				00			CRC 1	CRC 2	04
		Enceder	01	DD	DO	44	02	Dirección Actuador TAG	01			CRC 1	CRC 2	04
	Actuadores	Apagar	01	DD	DO	44	02	Dirección Actuador TAG	00			CRC 1	CRC 2	04
		Respuesta (Operación Correcta)	01	DD	DO	44	01	FF				CRC 1	CRC 2	04
		Respuesta (Operación Incorrecta)	01	DD	DO	44	01	CC				CRC 1	CRC 2	04
Serie 2000	Antena	Direccionar	01	DD	DO	4D	03	02	Dirección Antena	00		CRC 1	CRC 2	04
		Lectura	01	DD	DO	20	00					CRC 1	CRC 2	04
		Respuesta (Si detectó tarjeta)	01	DD	DO	20	04	ID 1	ID 2	ID 3	ID 4	CRC 1	CRC 2	04
		Respuesto (No detectó tarjeta)	01	DD	DO	20	01	40				CRC 1	CRC 2	04

Notas:

Todos los valores son dados en código Hexadecimal

DD- Dirección Lógica del Dispositivo Receptor

DO- Dirección Lógica del Dispositivo Tranmisor

Dirección Sensor- La Dirección puede estar en el rango 00-07

Dirección Actuador- La Dirección puede estar en el rango 00-07

Dirección Antena- La Dirección puede estar en el rango 00-03

Tabla 4. 14: Lógica del hardware

Asimismo las especificaciones de los requerimientos del sistema con respecto al hardware demandaban restricciones particulares para cada tipo de dispositivo electrónico.

La lógica del sistema, en consecuencia, debía agregar nuevos lineamientos de seguridad que consideraran los elementos de hardware adicionales.

Lógica operacional del sistema

Finalmente se considero que el sistema varía dependiendo de la necesidad de cobertura de acceso y de las zonas estratégicas de seguridad para cada edificio, por lo tanto se busco que el sistema, permitiera la configuración de las zonas críticas para el edificio, con la capacidad de adaptarse fácilmente a otras instalaciones.

Dispositivos			Condición	Acción	
TAG	Antena		Restringir Acceso Por hora y por fecha	Autorizado: Abrir chapa puerta Generar reporte de Entradas y Salidas de Usuarios	No Autorizado: Generar reporte de intento de acceso no autorizado
	Dispositivos Electrónicos de Detección	Sensor Magnético	Sin restricción	No Activo	Activo: Activar Alarma Local Generar reporte de incidentes
			Restringir por horario y fecha		Activar Alarma General Generar reporte de incidentes
		Sensor de Ruptura	Sin restricción		Activar Alarma General Generar reporte de incidentes
		Sensor de Movimiento	Restringir por horario y fecha		Activar Alarma General Generar reporte de incidentes
		Botón de Emergencia	Sin restricción		Abrir chapa puerta Generar reporte de incidentes
		Interfón	Sin restricción		Abrir chapa puerta
			Restringir por horario		Abrir chapa puerta
Serie 2000	Antena		Restringir Salida por hora y fecha	Autorizado: Abrir chapa puerta Generar reporte de Salida de Equipo	No Autorizado: Activar Alarma General Generar reporte

Tabla 4. 15: Lógica operacional del sistema.

Integración del software y el hardware

Un aspecto importante para el correcto funcionamiento del sistema es garantizar a través del flujo de información una sincronización total entre el hardware y el software en tiempo real. Para ello se requirió diseñar un sistema que permitiera configurar los tiempos de transmisión y recepción de manera asíncrona y asegurar que en todo momento que no se perdiera la comunicación.

Para lograrlo, el hardware siempre responde ante cualquier petición por parte del software, asimismo el tiempo de respuesta por parte de los dispositivos no es igual, debido a variables físicas como distancia y características del cable que afectan directamente la propagación de los datos. Dentro de los procesos involucrados en el sistema de comunicación se consideran tres tiempos importantes: transmisión, recepción y respuesta, con su tiempo respectivo de operación (ver figura 4.26).

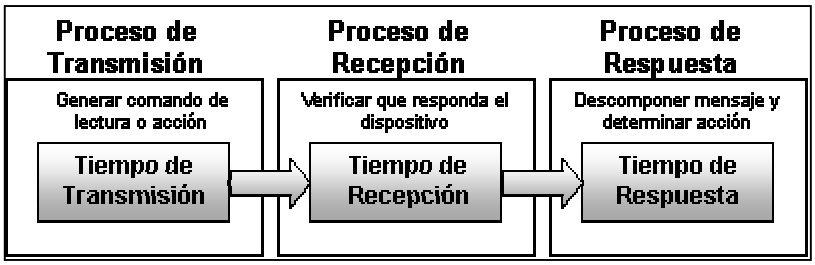


Figura 4. 26: Tiempos de procesamiento.

El proceso de recepción de datos será importante para detectar fallas en el hardware, debido a que podremos verificar si los dispositivos están o no respondiendo en el tiempo determinado.

Interfaz del usuario.

Se consideraron distintos escenarios para administrar por una parte la base de datos y por otra parte el hardware, así como una pantalla principal que unificara ambos procesos.

Interfaz Principal.

Se consideran los siguientes elementos:

- Un seguimiento y monitoreo de operaciones que muestre al usuario en cada momento las actividades que realiza el sistema.
- Un menú que permita el acceso a las funciones del sistema tal como son las administración y control de las comunicaciones y la administración de la base de datos.
- Un acceso controlado al sistema mediante restricciones de seguridad a nivel de usuario que nos aseguren que los diferentes tipos de usuarios puedan acceder a ciertas partes del sistema con determinados privilegios.

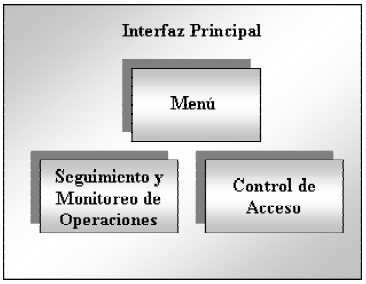


Figura 4. 27: bloques de la interfaz principal.

La interfaz principal comprendió dos etapas de diseño. La primer etapa estuvo orientada al aspecto funcional del programa mientras la segunda etapa se enfocó al aspecto estético y ergonómico de las interfaces.

Primer Etapa: Se incluyeron todos los elementos necesarios para ambientar al usuario en los servicios que podría disponer al utilizar el sistema (ver figura 4.28), tales como:

- Notificación de fallas en los dispositivos de comunicación.
- Notificación de intento de salida de equipo no autorizada.
- Monitoreo de los accesos y salidas del personal.
- Acceso al sistema.

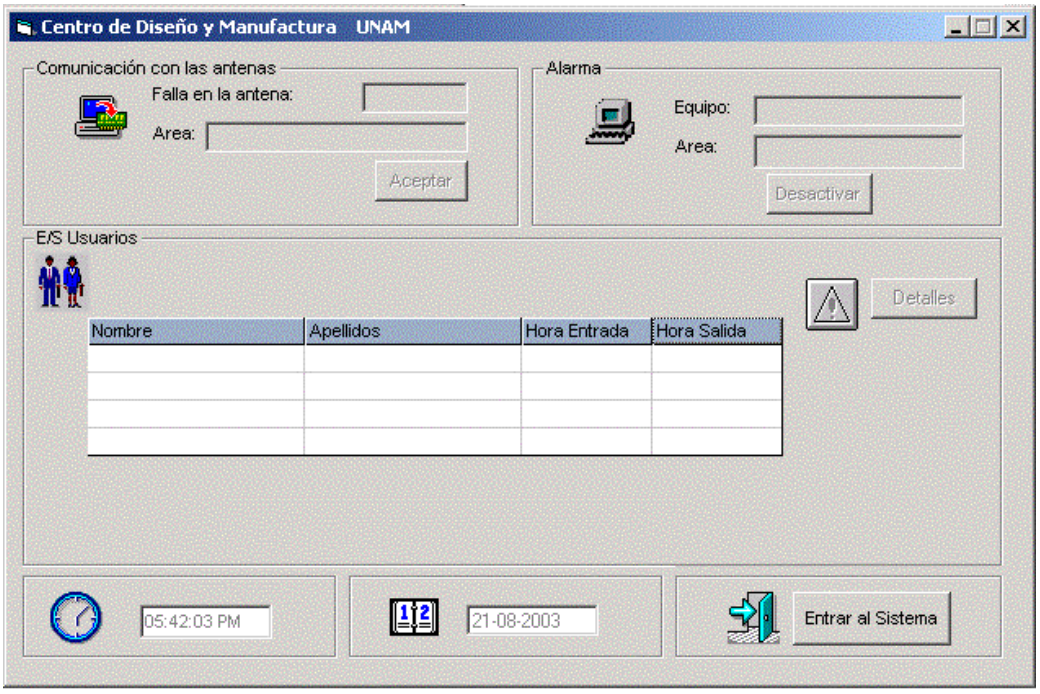


Figura 4. 28

Se usan recursos multimedia muy sencillos y cambio de colores para resaltar cuando se estuviera dando un evento trascendente tal como el robo de equipo o la manifestación de fallas en el funcionamiento del hardware.

Mediante colores vistosos se destaca el área de la pantalla dedicada al monitoreo, de una acción determinada o bien desplegamos señales de alerta y animaciones que hicieran más explicativo cada suceso logrando de esta manera atraer la atención.

En el caso de fallas en el sistema, interesó informar a los clientes de la falla de algún dispositivo, especificando su ubicación, para facilitar la tarea de reparación y mantenimiento del mismo (figura 4.29).

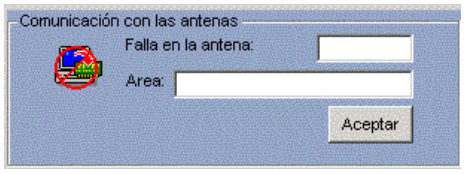


Figura 4. 29

Uno de los principales propósitos del sistema, es la protección del equipo por lo que se decidió poner mayor énfasis en la representación gráfica de este evento.
Visualmente se resalto la zona de monitoreo de equipo no sólo por la distinción de color sino haciendo uso de una animación gráfica en sincronía con una alarma sonora, que permitiera destacar un estado de alerta, haciendo uso de cuadros de texto, donde se muestra la identificación del tipo de equipo que esta siendo sustraído de las instalaciones (figura 4.30).

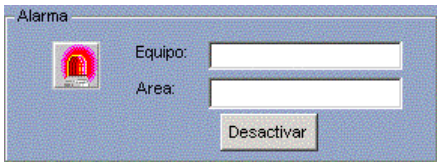


Figura 4. 30

La supervisión de acceso y salida del personal fue representada por el manejo de celdas, donde se puede apreciar la identificación del personal (figura 4.31), así como la hora en que se está entrando o saliendo de las instalaciones. Aunado a esta información, se usan íconos para representar anomalías tales como intento de accesos no autorizados, que permiten al administrador tener completo control sobre los incidentes ocurridos durante el día.

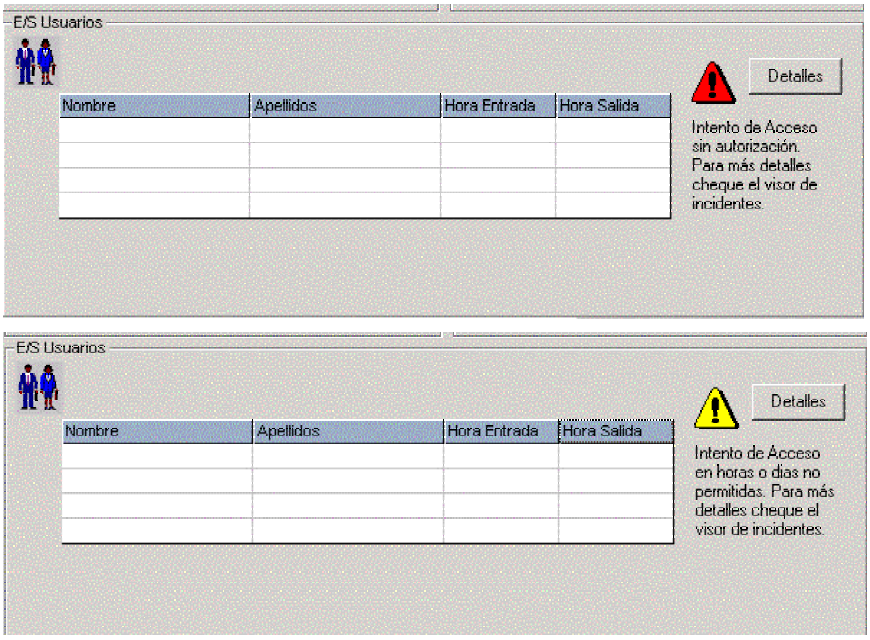


Figura 4. 31

Segunda etapa: Durante esta etapa se valoró el aspecto estético de la interfaz, reorganizando los elementos y homogeneizando visualmente sus componentes. Haciendo uso de nuevos objetos que enriquecieran el aspecto físico de la pantalla y facilitaran al usuario su interacción con el sistema (ver figura 4.32).

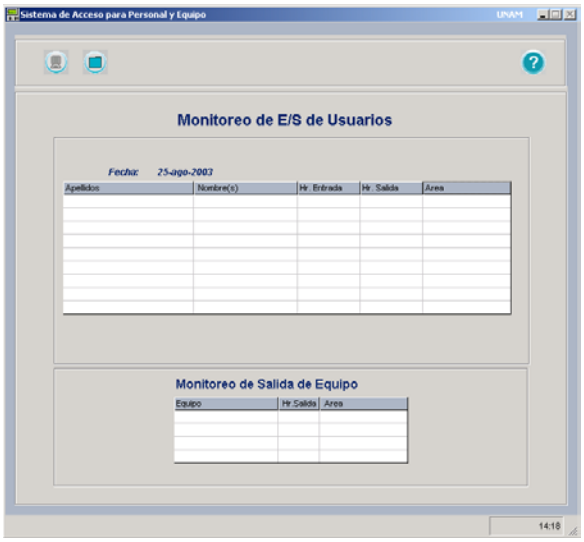


Figura 4. 32

Menú.

Considerando que el sistema tiene dos módulos principales: comunicaciones y Bases de Datos, se estructuro el menú con dos opciones para ingresar a cada uno de estos módulos así como una opción adicional de ayuda que oriente al usuario su uso. Asimismo se considero la utilización de íconos que permitieran al usuario familiarizarse simbólicamente con cada una de las opciones.

Monitoreo y Notificaciones de Alerta.

Para determinar el monitoreo de las operaciones del sistema, se tomo en cuenta las características que debe ofrecer un sistema de seguridad y la importancia de mantener al usuario informado sobre los eventos ocurridos durante su operación, para derivar finalmente en los detalles fundamentales a los cuales se debe poner singular atención:

- Monitoreo de las entradas y salidas del personal.
- Monitoreo de la salida de equipo.
- Notificaciones de alerta sobre eventos especiales.

Figura 4. 33

En el cuadro del monitoreo del personal (figura 4.31), se presenta un registro continuo de la entrada y salida de cada individuo, así como el horario y el área de su ubicación actual. Mientras que el cuadro: monitoreo de equipo, va a permitir al usuario enterarse en que momento está saliendo un equipo con permiso de las instalaciones, y tener control sobre el traslado de dicho equipo dentro de las áreas controladas del edificio.

Las notificaciones de alerta suponen una atención particular (figura 4.34), ya que SAPPE, tiene como principal objetivo prevenir y alertar sobre situaciones de riesgo como son el robo de equipo, accesos no autorizados y fallas importantes del sistema. Para ello se generan pantallas independientes que puedan notificar datos relevantes sobre un incidente de esta naturaleza como son hora, ubicación y descripción del suceso.

Figura 4. 34

Acceso al sistema.

Como se menciono anteriormente, esta etapa hará el control de acceso al sistema, determinando las capacidades de aplicación del usuario sobre el sistema de acuerdo con los privilegios otorgados por un administrador. De acuerdo a la información proporcionada durante ese proceso se revelará una capa distinta de la interfaz subsiguiente que limite o confiera propiedades para manipular la información y control del programa.

Para ello se agrego un cuadro de diálogo que se despliegue al pulsar cualquier opción del menú cuestionando sobre la identidad del usuario (figura 4.35) que se desea ingresar al sistema y comprobando la veracidad de los datos ingresados por la persona; siendo de esta manera un filtro entre la interfaz principal y las pantallas siguientes.

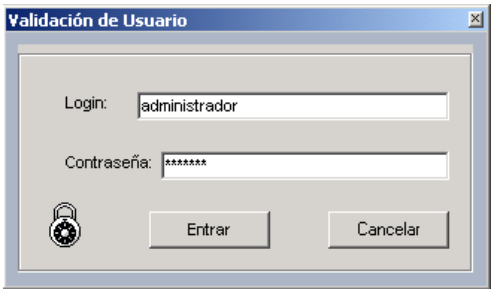


Figura 4. 35

Interfaz para Base de Datos.

La parte más extensa en despliegue de pantallas se concentró en la administración de la Base de Datos debido a que cada acción implica un conjunto de opciones específicas que, por motivos de claridad, se decidió presentar separadamente.

Como la administración de la Base de Datos implica consultas, modificaciones, altas y bajas, búsqueda de información, etc. Se determino las transacciones principales:

- Consulta de registros.
- Alta de registros.
- Baja de registros.
- Búsqueda de información.
- Reportes de Incidentes.
- Devolución de Equipo.
- Administración de usuarios del sistema.

Los componentes físicos utilizados para esta interfaz fueron botones y menú con íconos los cuales se situaron de forma estratégica y ordenada dentro de la pantalla.

Para poder llevar a cabo cada una de las transacciones principales con la Base de Datos se colocaron botones cuya acción despliega una pantalla con opciones más particulares acerca de la selección realizada.

A continuación desglosaremos de manera sencilla cada una de las opciones de la interfaz principal de la base de datos explicando sus principales características.

Consulta de registros.

La función esencial de esta opción es permitir al usuario realizar búsquedas en la base de datos (figura 4.36).

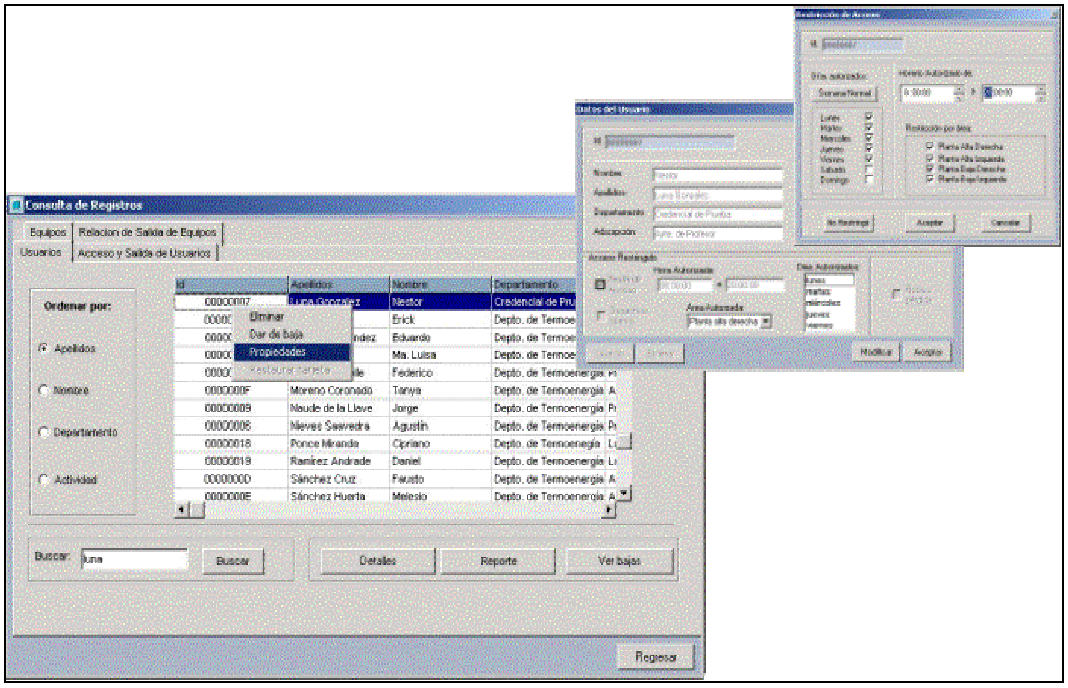


Figura 4. 36

Para facilitar la exploración de datos, se diseño una interfaz que ofrece al usuario un amplio rango de combinaciones de búsqueda, que parte de la información más general hasta datos más específicos. La información proyectada como resultado de una consulta se muestra en tablas organizadas de manera clara y precisa.

El objetivo de presentar la información en tablas es protegerla de incidentes que puedan ocasionar alteraciones no controladas en los registros o pérdida de datos. Por lo tanto esta interfaz ofrece opciones adicionales para poder operar sobre un registro particular, de manera que se puedan obtener datos más específicos o bien modificar la información, siempre que el usuario cuente con los privilegios para realizar dicha acción.

A través de esta interfaz el usuario podrá operar directamente sobre los registros teniendo la capacidad de eliminar, modificar y dar de baja registros mediante opciones desplegadas en un menú flotante.

Alta de registros (Nuevo registro).

Este formulario va a permitir al usuario crear y almacenar un nuevo registro en la base de datos (figura 4.37).

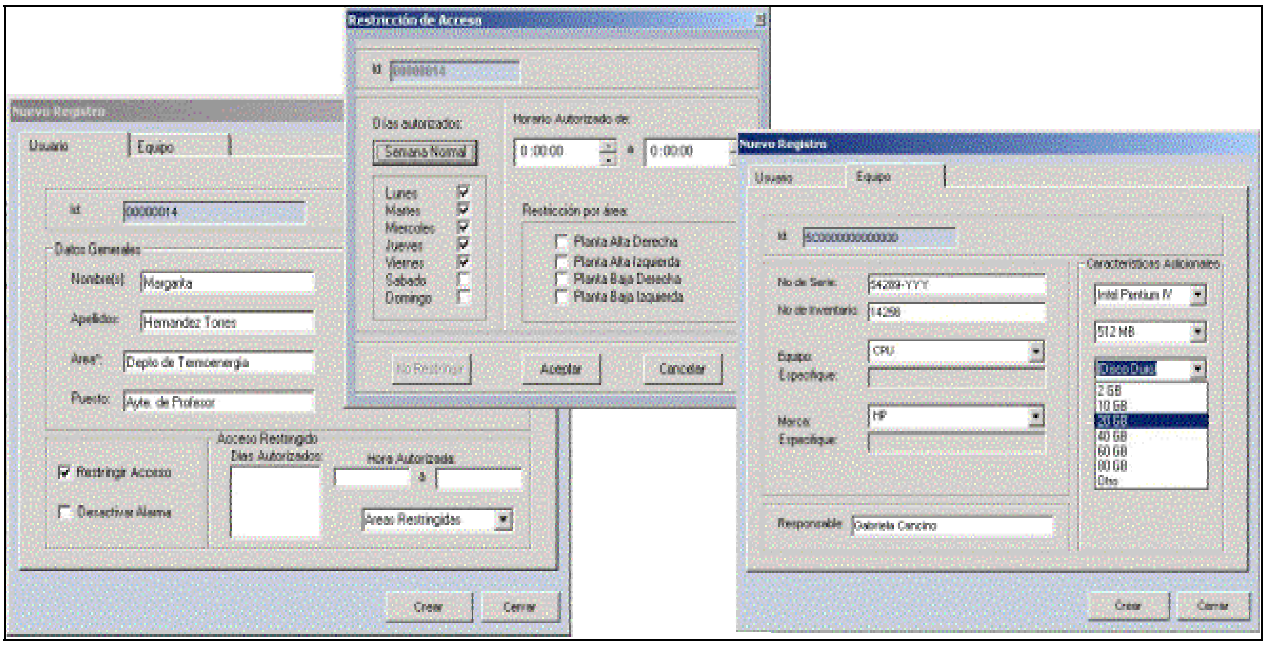


Figura 4. 37

La interfaz permite al administrador almacenar información concerniente a un usuario o equipo, orientándolo en el llenado de los campos de manera clara y precisa.

Baja de Registros (Bajas).

Mediante esta interfaz el usuario podrá dar de baja un registro de la base de datos.

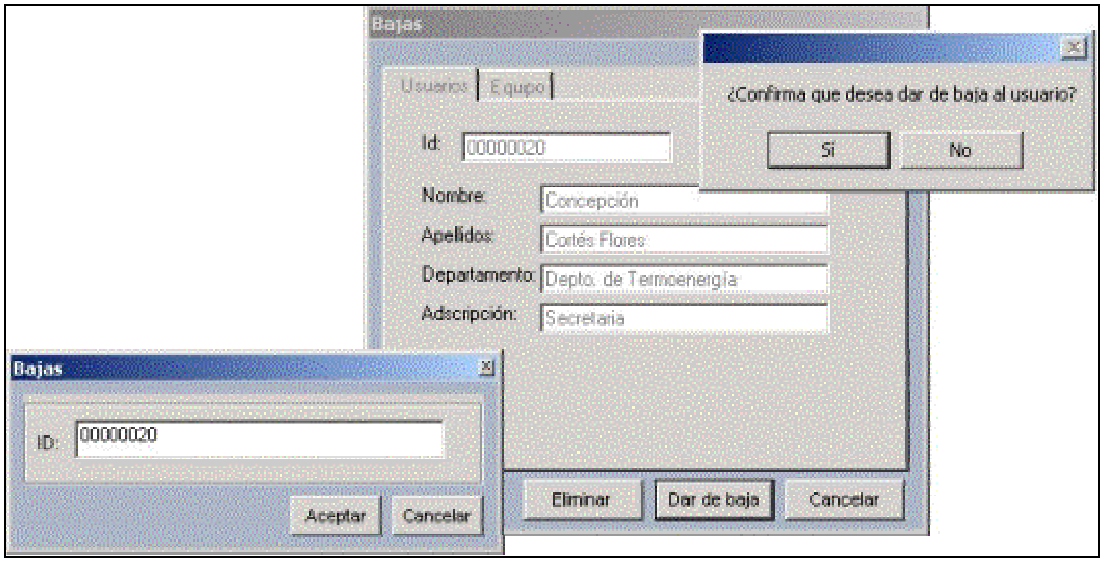


Figura 4. 38

Opciones como eliminar, modificar y dar de baja registros requieren cuestionar previamente al usuario sobre la realización o cancelación de dicha acción; previniendo, de esta manera, errores que puedan llevar a la pérdida de información (figura 4.39). En el caso particular de esta pantalla se requiere autentificar la información del usuario o equipo insertando la clave principal del registro, al que procederá un formulario con los datos completos. Una vez concluida la acción, la información correspondiente será desplazada a una tabla meramente informativa, perdiendo sus cualidades dentro del sistema.

Búsqueda de información (Buscar).

Esta interfaz es muy similar, en operación, al formulario de consulta de registros. Sin embargo, su propósito está orientado a la búsqueda general de datos correspondientes a un criterio propuesto por el usuario.

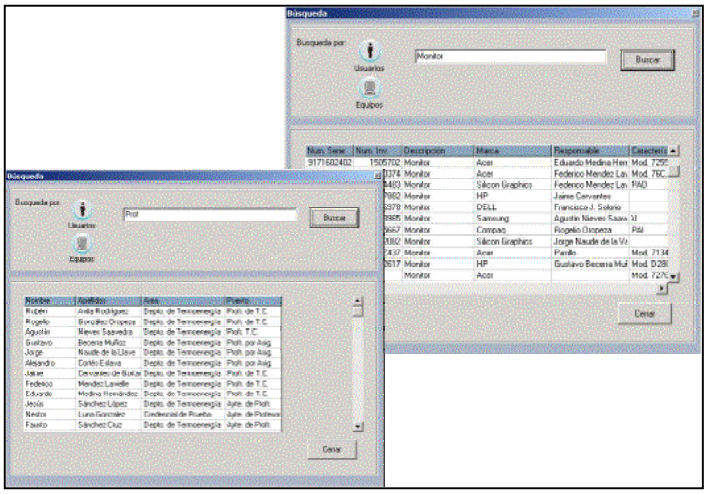


Figura 4. 39

La pantalla es muy sencilla y fácil de operar. El usuario puede elegir entre búsqueda de usuarios o equipos, para posteriormente insertar los detalles particulares de dicha búsqueda en el único campo presentado en la pantalla. La exploración se realiza en todas las tablas y los resultados son presentados ordenadamente en una tabla.

Reporte de Incidentes (Incidentes).

Este formulario despliega de manera clasificada los incidentes ocurridos de acuerdo a tres criterios: Incidentes relacionados con los usuarios, incidentes relacionados con equipos e incidentes relacionados con el sistema físico. Dicha información se expone en una tabla describiendo de manera general el suceso, la hora y fecha del incidente (figura 4.40).

Para facilitar al usuario la búsqueda específica de información se disponen de elementos que admiten la selección de fechas y horas, filtrando los datos a partir de estos criterios. Asimismo mediante un menú flotante el usuario puede acceder a detalles particulares del incidente seleccionado, los cuales son expuestos en otra pantalla.

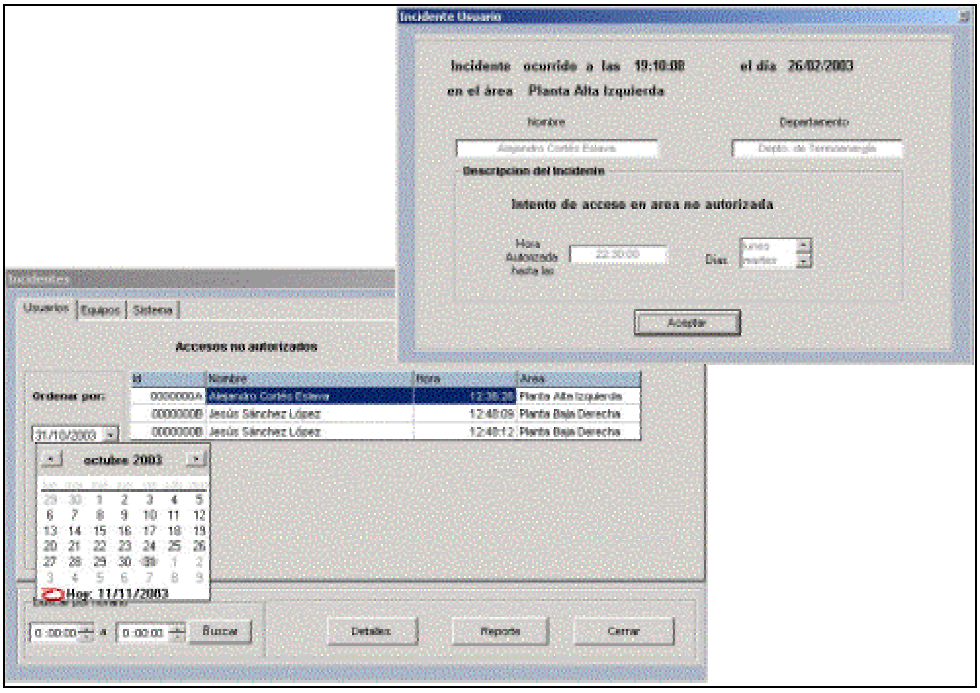


Figura 4. 40

Devolución de equipo.

Esta pantalla tiene como un único proceso registrar cuando un equipo es devuelto a las instalaciones. Por lo que su interfaz es muy simple; presentando la información concerniente a la salida del equipo así como un botón completamente identificado a través del cual se realizará el evento. Una vez que se ha ejecutado dicha acción el equipo queda protegido nuevamente por el sistema de seguridad (figura 4.41).

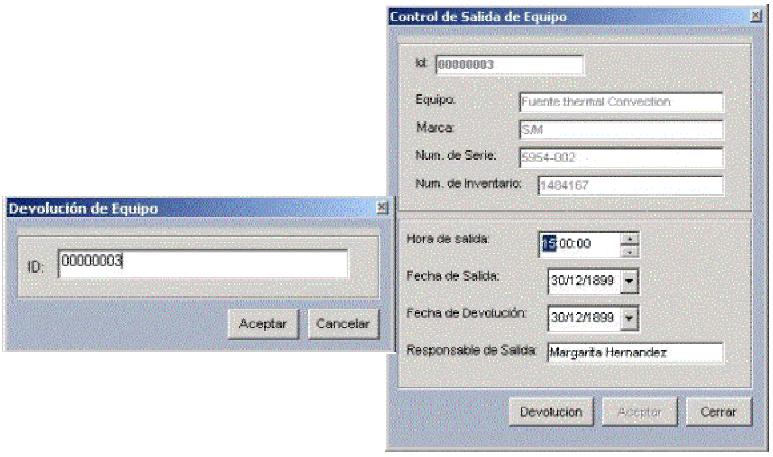


Figura 4. 41

Usuarios del sistema.

En la parte central de la interfaz principal ubicamos una opción de suma importancia: los "usuarios del sistema", que nos va a permitir consentir facultades particulares de acceso al sistema (figura 4.42).

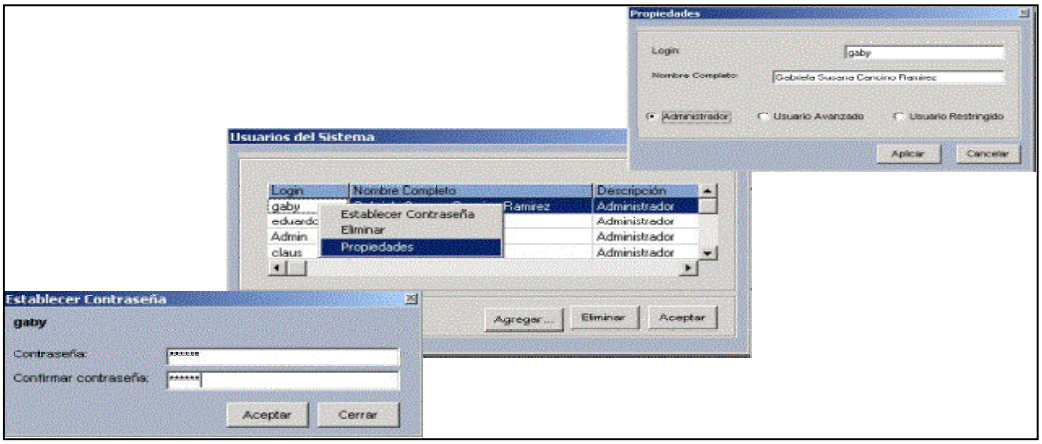


Figura 4. 42

Este formulario otorga al administrador la capacidad para agregar, modificar y eliminar información de los usuarios que pueden ingresar y administrar el sistema SAPPE.

Interfaz para Comunicaciones.

Esta interfaz tiene el objetivo de brindar, a los usuarios enfocados a la operación y administración del hardware, una herramienta que facilite estas actividades de una manera transparente y sencilla. Para ello se define la interfaz con base a dos necesidades básicas (figura 4.43):

Por una parte la operativa, es decir poder manipular y administrar los dispositivos conectados al sistema;
Y por otra parte un contenido informativo que proporcione al usuario un seguimiento total sobre el comportamiento y condición actual del sistema.

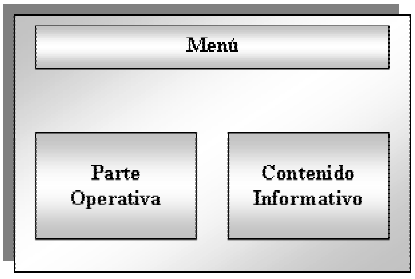


Figura 4. 43

Asimismo las políticas de seguridad implican un control de emergencias de operación del sistema de seguridad, es decir, un grupo de usuarios que tengan la capacidad de determinar las acciones a seguir una vez que se suscita un evento extraordinario, pueda reestablecer el estado normal del sistema y controle los distintos horarios de operación de los dispositivos.

Por lo tanto el contenido de la interfaz debe cubrir, por un lado, las expectativas de los administradores del hardware, y por otra parte facilitar a los administradores del sistema el control sobre su operación.

La solución fue una interfaz completamente gráfica, donde cada dispositivo del sistema es representado en la pantalla de manera virtual informando al usuario sobre su estado funcional y operativo así como su ubicación física (figura 4.44).

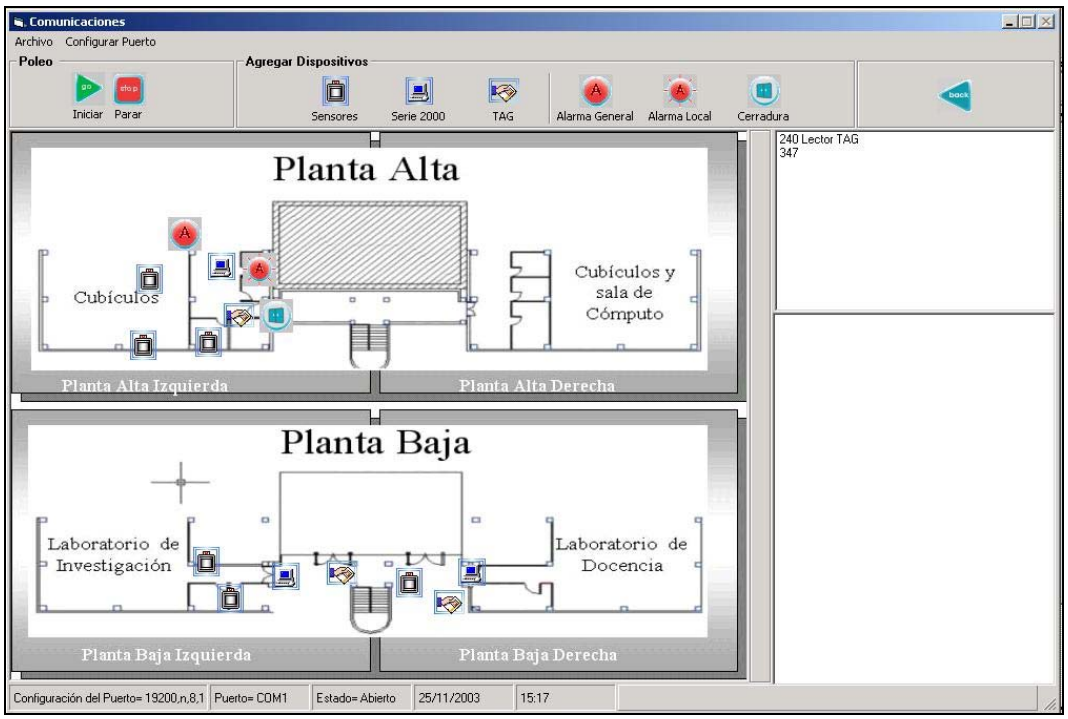


Figura 4. 44

Esta concepción del sistema permite al administrador del hardware:

- Configurar el puerto de comunicaciones.
- Instalar y desinstalar fácilmente un dispositivo.
- Realizar pruebas particulares, por área y generales de los dispositivos instalados en el sistema.
- Una rápida ubicación de fallas en los dispositivos.
- Sseguimiento total sobre el comportamiento y condición actual del sistema.

Y permite al administrador del sistema:

- Configurar los horarios de operación de los dispositivos instalados.
- Visualizar fácilmente el área y el dispositivo que esta detectando un evento irregular.
- Restituir el estado de operación normal del sistema.

La interfaz gráfica del módulo de comunicaciones esta distribuido en tres partes principales:

- Menús
- Mapa virtual de la instalación. (Parte Operativa)
- Monitoreo de la operación de los dispositivos.

Menús.

Los menús tienen el objetivo de brindar al usuario opciones más específicas como son la configuración del sistema y la administración de los dispositivos.

Esta pantalla ofrece un menú colgante con el cual el usuario podrá entrar a la configuración del puerto de comunicaciones. Una vez seleccionada la opción se despliega un formulario donde se presentan todos los parámetros que el usuario podrá manipular para realizar la comunicación con los dispositivos vía puerto serie.

Figura 4. 45

Posterior a este menú se presenta una colección de botones caracterizados por íconos que permiten, por un lado, establecer la comunicación con los dispositivos y, por otro lado, agregar nuevos dispositivos al sistema. Para ello el diseño de los íconos fue muy cuidadoso de manera que fueran expresivos y fáciles de relacionar con la operación correspondiente permitiendo al usuario habituarse a su utilización rápidamente (figura 4.46).

Figura 4. 46

Mapa Virtual de la Instalación (Parte Operativa).

El mapa virtual (figura 4.47) permitirá, tanto a los administradores del hardware como a los administradores del sistema, asociar cada uno de los dispositivos físicos con un objeto representado en la pantalla, de manera que pueda reconocer el tipo de dispositivo, la ubicación física que ocupa dentro de las instalaciones y el estado actual del dispositivo; así como su dirección lógica, información útil para los administradores del hardware, que se puede obtener al posicionar el puntero del Mouse sobre el objeto.

Otra gran ventaja del mapa virtual es que el usuario podrá identificar rápidamente la zona y el dispositivo que haya detectado una situación anormal, ya que el objeto será resaltado mediante un color distinto, y podrá ser restaurado a su estado normal con sólo dar un clic sobre el elemento activo.

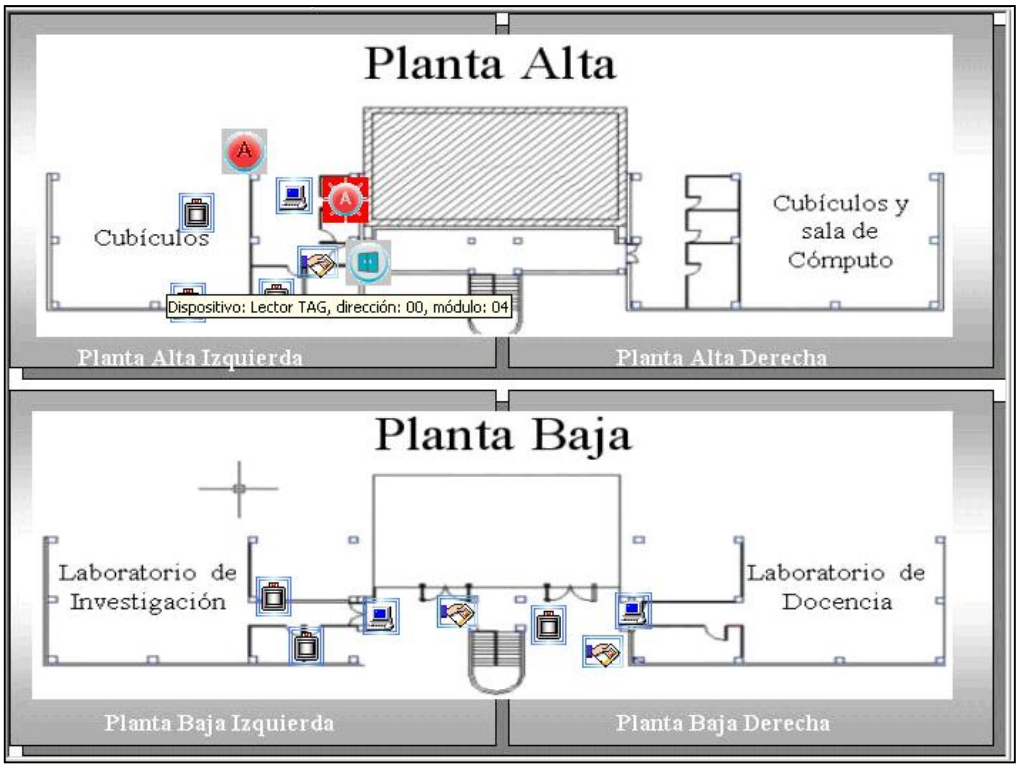


Figura 4. 47

La información presentada en esta pantalla la definimos de acuerdo con los intereses del usuario, es decir, seleccionamos aquella información que sería útil para el administrador del hardware. Mostrando en pantalla un seguimiento de los procesos que se están ejecutando entre el software y los dispositivos centrales (figura 4.48):

- Transmisión de datos y respuesta.
- Recepción de datos y acción tomada.
- Visualización de fallas en los dispositivos.

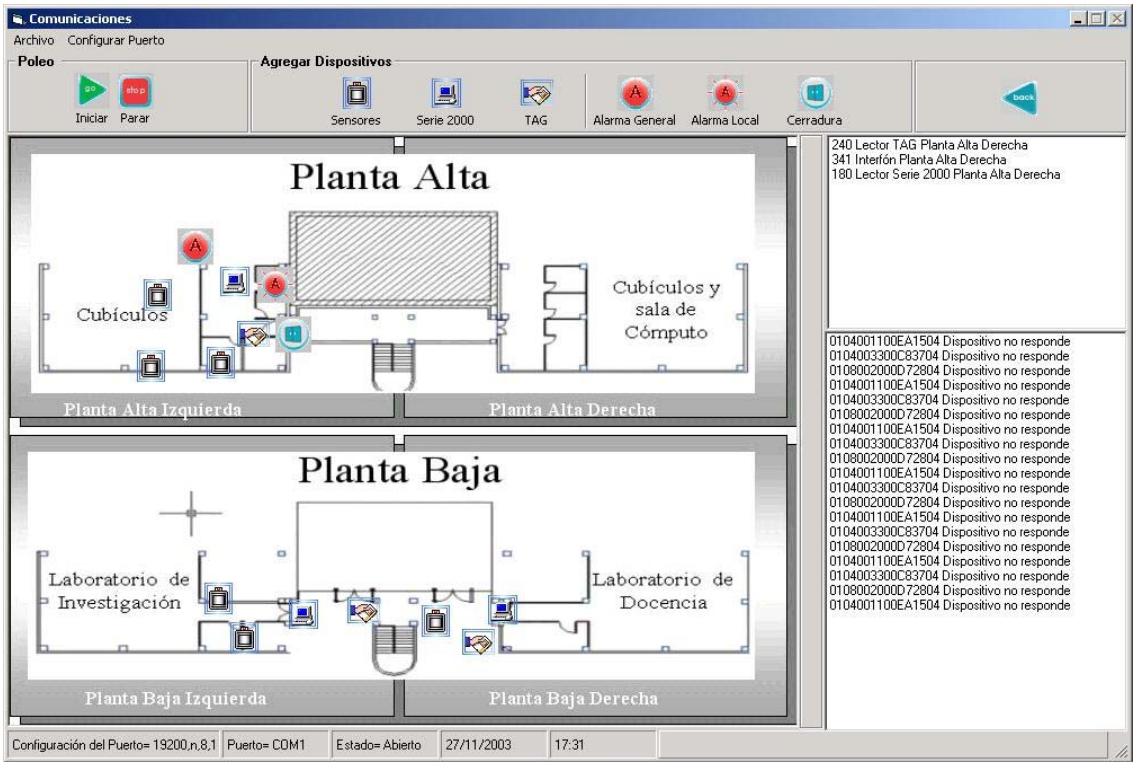


Figura 4. 48

Seguridad.

En términos operativos el sistema SAPPE es una aplicación orientada a procurar la seguridad de bienes y personas, esto implica todos los procesos que controlan los elementos de protección física. Sin embargo, existe un nivel de seguridad más abstracto que considera los elementos humanos como un factor importante para garantizar que se lleven a cabo todos esos procesos de manera exitosa.

Un sistema será mucho más seguro entre menor sea el número de usuarios que tengan acceso a él. Por ello la administración del sistema es exclusiva de usuarios facultados y restringidos por distintos niveles de interacción con el software.

Estos niveles de interacción van a determinar la capacidad del usuario para hacer modificaciones y consultas dentro del sistema. Se definen tres tipos de usuarios y los privilegios otorgados para cada uno de ellos (tabla 4.16):

DESCRIPCIÓN	NIVEL DE INTERACCION CON EL SOFTWARE
Usuario Restringido	Este tipo de usuario, tiene acceso a gran parte de las interfaces del programa, pero su interacción únicamente se limita a un nivel informativo; por ejemplo puede consultar toda la información concerniente a las Entradas/Salidas de usuarios, incluso acceder a detalles pero los procesos de manipulación de información estarán deshabilitados, este usuario no puede modificar y mucho menos borrar registros.
Usuario Avanzado	Este tipo de usuario estará autorizado para realizar consultas y manipular la información de manera limitada como puede ser: restringir accesos, permitir salidas de equipo, etc. Adicionalmente puede restaurar el sistema a su estado normal después de algún evento extraordinario.
Administrador	Tiene pleno control sobre todas las capacidades y funcionalidades de la aplicación y la Base de Datos. Cabe destacar que este usuario también tendrá decisión sobre los otros dos tipos de usuario. Operativamente el administrador es el encargado de crear e eliminar los otros dos tipos de usuario, decidir quién tendrá permisos de usuario restringido, quién de avanzado, además de tener capacidad para asignar y cambiar nombres de usuario y contraseñas en cualquier momento.

Tabla: 4. 16

5

INSTALACIÓN Y PRUEBAS DEL SISTEMA.

Enumeramos algunos aspectos considerados en la instalación tales como:

- Seguridad: La seguridad debe ser prevista desde todos los puntos de vista posibles, para usuarios en: cubículos, laboratorios, pasillos, escaleras
- Eficiencia: Se debe buscar la trayectoria más adecuada y que todos sus elementos sean de fácil acceso a fin de poder hacer cambios o realizar mantenimiento.
- Mantenimiento: Debe efectuarse en forma periódica y sistemática, la limpieza, reposición de partes, renovación y cambios de equipos.
- Distribución: No debe estorbar el espacio libre para operarios y debe permitir la libre circulación para el personal.
- Accesibilidad: Escoger zonas de fácil acceso, aunque en nuestro caso algunos equipos y registros estarán en zonas poco accesibles para personas no idóneas.

DETERMINACIÓN DEL TIPO DE CANALIZACIÓN.

Después de realizar el estudio de las instalaciones se determinó que no existían tuberías ni canalizaciones adecuadas para la instalación de los componentes y cableado del sistema, además de que, no era posible ocultar las canalizaciones, pero si era posible darle resistencia mecánica usando tubería conduit con lo que nuestra instalación sería del tipo visible entubada; y estará divididas en dos grupos:

- Canalización para la alimentación eléctrica.
- Canalización para datos.

Canalización para la alimentación eléctrica.

Comenzamos por definir el tipo de aislamiento y el calibre del conductor eléctrico a usar así como el elemento termo magnético que deberá de proteger a la instalación en caso de sobre tensiones en la instalación[1].

[1] Los cálculos matemáticos realizados para estos elementos, se pueden ver en el apéndice “calculo de la instalación eléctrica”.

Para nuestra instalación eléctrica se usaron los siguientes elementos:

- Tubería conduit galvanizada pared delgada de 19 mm (3/4").
- Licuatite: Tubo conduit flexible de acero galvanizado con recubrimiento plástico.
- Conductores eléctricos unipolo calibre # 10 AWG.
- Elemento termo magnético (pastilla) de 1 x 10 A para centro de distribución.
- Accesorios para tubo conduit en diámetro especificado de 19mm (3/4"). Estos accesorios incluyen: condulets, codos, coples, abrazaderas y todos aquellos elementos que se ocupen para la tubería.

INSTALACIÓN FÍSICA DEL SISTEMA.

Instalación de las tuberías.

La instalación de tuberías y gabinetes (que más adelante llamaremos registros) la realizo un proveedor de la UNAM, pero el cableado, la conexión (remate) y la instalación de los registros estuvo a cargo del equipo implicado en el proyecto.

Cuando la tubería estuvo lista, nuestra tarea se centró en supervisar, cablear y rematar cada uno de los componentes, además de nosotros comenzaron a trabajar los carpinteros, resanadores y el equipo que instalaría las antenas de lectura para equipos.

Instalación de las puertas.

Supervisar la colocación de las puertas era vital por que en ellas se instalarían sensores magnéticos, la cerradura magnética, el módulo Receptor/Transmisor del interfón y los dos dispositivos más importantes: la antena para protección de equipo (de la cual se hablara más adelante) y el lector TAG para credenciales de usuarios (fotografía 5.1).

Fotografía 5. 1: Instalación y terminado de las puertas de acceso en la planta alta derecha (PAD).

Instalación de sensores y actuadores.

Los sensores de movimiento se instalaron de tal manera que cubren toda el área por donde es posible que entre alguna persona (fotografía 5.2), están instalados a una cierta altura y con un ángulo de inclinación, de tal forma que se activan antes de que la puerta

se abra lo suficiente para que una persona entre, es decir, el control maestro detecta el evento antes de que el intruso o usuario tenga la perspectiva del sensor.

Estos sensores tienen un horario definido de funcionamiento ya que durante el día las instalaciones son usadas constantemente, pero llega un horario en el que nadie debe ya entrar, en este lapso de tiempo es cuando funcionan los sensores de movimiento.

Fotografía 5. 2: Sensor de movimiento ya instalado.

Los sensores de ruptura de cristal se instalaron en la parte alta de los ventanales de la planta alta de tal manera que protegen el ventanal y la ventana que se encuentra en las puertas de acceso, estos están activos las 24hrs del día.

Fotografía 5. 3: Sensor de Ruptura de cristal ya instalado.

Los sensores magnéticos están colocados en las puertas de acceso controlado por el sistema, su función es avisar cuando una puerta se ha abierto, al igual que los sensores de ruptura de cristal, están activos las 24 horas del día.

Instalación de las antenas de baja frecuencia.

Como ya se mencionó anteriormente las antenas se colocaron, antes de poner las puertas de control de acceso, se colocó una antena por puerta, una vez que se colocaron, se midió su inductancia y su factor de calidad por medio de un puente de impedancias, los cables se colocaron dentro de tubos de PVC de ½ " para darles la rigidez necesaria, estas antenas tipo loop quedaron formadas por dos espiras o vueltas cada una.

Cuando estuvieron instaladas físicamente las antenas, con ayuda de un puente de impedancias se midió tanto la inductancia propia de las antenas (L) como su factor de calidad (Q) de las mismas, se hicieron las medidas del largo del cable twinax que se ocupo y los cálculos necesarios para encontrar la configuración inicial para sintonizar las antenas (ver tabla 5.1), y cuyo procedimiento se describió en el capítulo anterior.

El tipo de cable que se utilizo para la conexión de cada uno de los tuning box a los SERIES2000 fue de tipo twinax con las siguientes características:

- Impedancia característica de 100 a 105 ohms
- Capacitancia de 50.9 pF/m.
- Diámetro 8.4 mm.

En la tabla 5.1 presentamos valores de inductancia, factor de calidad, distancia de los cables, así como los resultados arrojados por el uso de las fórmulas (1), (2) y (3), que se mencionaron en el capítulo 4 "Diseño del sistema Pág. 42", del lado derecho se muestra la configuración de los jumpers para cada antena.

Ubicación Antena	Q	L (μH)	Dist-cab (m)	C_{CAB} (nF)	C_{RES} (nF)	C_{TUNB} (nF)	Jumpers
PAI	24.1	28.70	22.13	1.2642	44.3675	41.0411	JP2,JP5,JP8,JP11
PAD	22.8	28.52	19.00	0.9671	44.6209	41.4538	JP2,JP5,JP8,JP11
PBI	32.8	33.87	36.00	1.8324	38.1462	34.1138	JP2,JP5,JP11
PBD	17.4	33.58	50.20	1.7524	38.4486	34.4961	JP2,JP5

Tabla 5. 1: Valores obtenidos, para la sintonización de las antenas.

Instalación de los transponders.

Como ya habíamos mencionado en capítulos anteriores se usaron dos sistemas de lectores, con dos frecuencias diferentes, el TAG es de alta frecuencia y el Series2000 de baja frecuencia

Para los usuarios se uso el transponder de tipo credencial (fotografía 5.4), pero para los equipos se consideraron de diversos tipos. Cada equipo a proteger en el edificio tienen formas y materiales diferentes por lo que teníamos que determinar cual transponder era el adecuado para cada equipo.

Fotografía 5. 4: Lector tag y el transponder tipo credencial

A continuación presentamos una vez más los tres tipos de Transponders del Series2000 que se instalaron en los equipos:

Small MOM (Small Mount – On – Metal Transponder), es usado para equipos que tengan un armazón de metal, por ejemplo el CPU de una computadora, este transponder responde mejor a la lectura cuando tiene una base metálica.

Disco (Large Disc), usado en equipos de laboratorio y aparatos electrónicos que no tengan armazón de metal. Este tipo se puede usar en monitores.

Cilíndrico (Cylindrical), es el transponder de mayor alcance, por lo que lo usamos en casi todos los equipos importantes, aunque fijarlo resultaba difícil, personal del CDM. nos recomendó pegamentos epóxicos para fijarlos al equipo.

En una junta realizada con personal del edificio en donde se iba a instalar el sistema y con los integrantes del proyecto se determinaron los equipos que se integrarían al sistema de protección. El número de equipos rebasaba el total de transponders que se tenían destinados para los equipos, pero se les dio prioridad a los más importantes, ya sea por su valor económico o académico.

La instalación para cada transponder y equipo fue diferente por lo que no se detallara la instalación de todos los transponders, pero comentaremos los más sobresalientes.

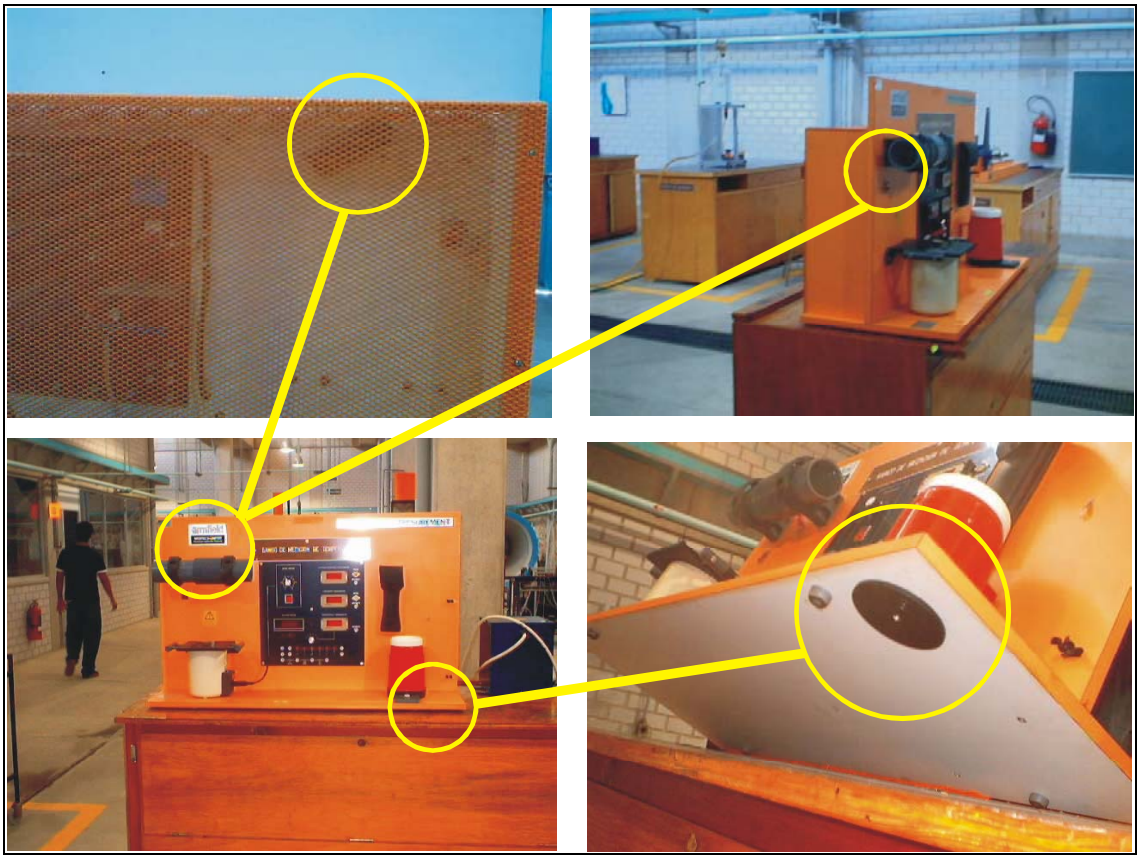
Instalación de los transponders en un sistema de computo.

Cada transponder instalado en los equipos tenía que estar en una posición estratégica, donde no pueda ser visto o de difícil acceso al usuario y que al mismo tiempo sea fácil la lectura para la antena del Lector Series2000. (en la fotografía 5.5 se ve el tipo y la posición del transponder en cada uno de los componentes en un equipo de computo).

Fotografía 5. 5: Posición de los transponders en un equipo de computo.

Instalación de varios Transponders en un aparato:

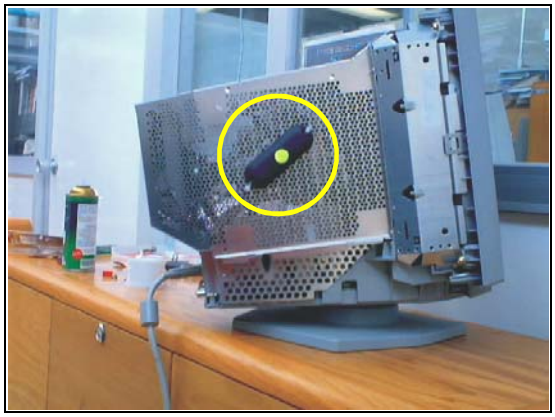
Existen aparatos que son muy fáciles de mover y por lo tanto fáciles de extraer de los laboratorios, para estos equipos se tomo la decisión de ponerle dos identificadores, uno en cada extremo (ver fotografía 5.6).



Fotografía 5. 6: Transponders, instalados en un equipo de laboratorio.

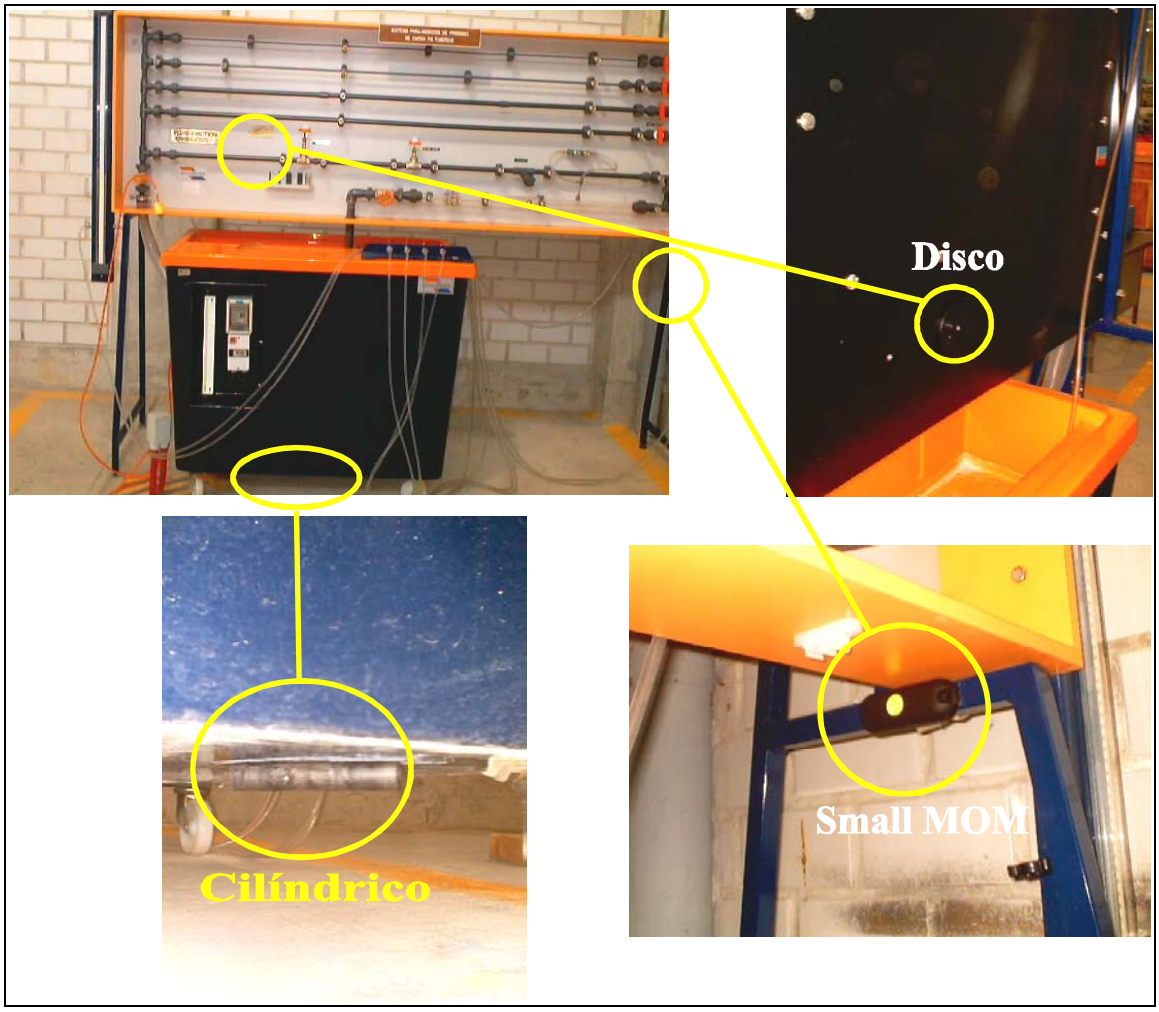
Instalación del transponder en un monitor con cubierta metálica:

Para los equipos que tienen armazón metálico el Transponder Small MOM es el ideal, el metal aumenta el área activa de lectura en las antenas (ver fotografía 5.7).



Fotografía 5. 7: Transponder Small MOM en un monitor.

Hubo casos en que los equipos están conformados por partes y se debían proteger cada una de ellas (ver fotografía 5.8).



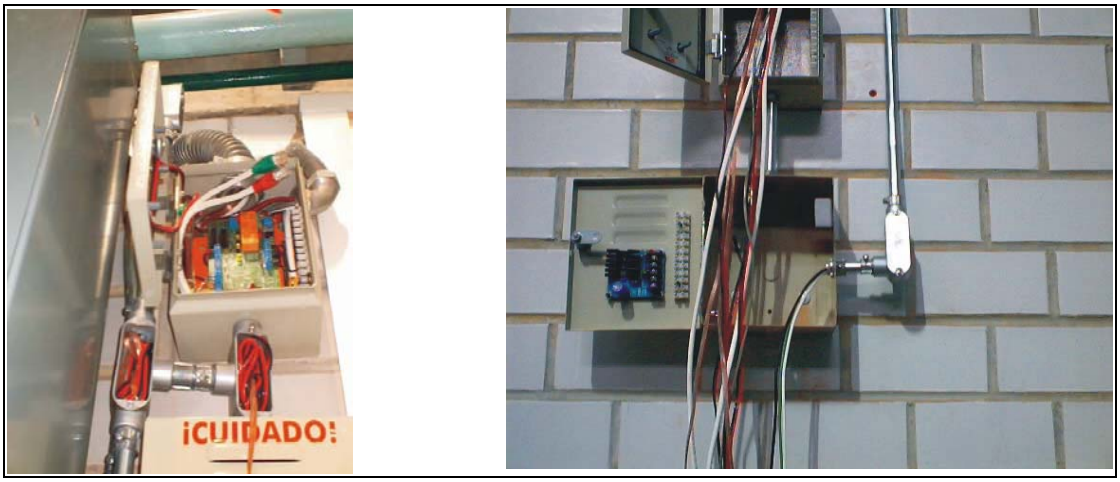
Fotografía 5. 8: Tres tipos de transponder, colocados en un equipo.

Instalación de los registros.

Los registros, son gabinetes metálicos donde están colocados los módulos que habrán de controlar las cuatro zonas del edificio. Son dos los tipos de registros que se colocaron, el registro series 2000 (fotografía 5.9) y el registro TAG, de este ultimo tenemos uno por zona controlada. Junto a cada registro TAG hay otro al que hemos llamado respaldo TAG (fotografía 5.10), que contienen una fuente de alimentación, junto con un respaldo de baterías para alimentar la cerradura magnética y la alarma general (Ver diagrama 5.1).

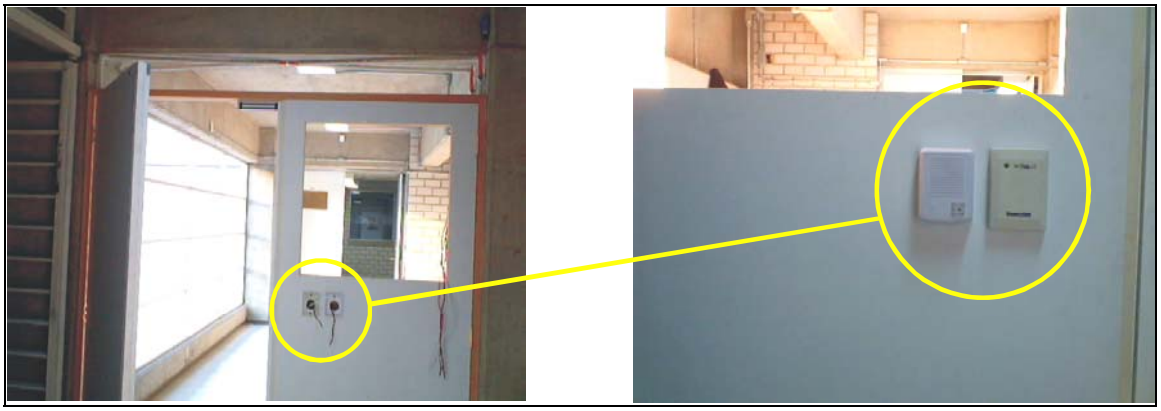
Fotografía 5. 9: Registro series 2000

.



Fotografía 5. 10: Registros TAG, izquierda registro terminado, derecha registro por terminar.

Los Lectores TAG fueron instalados en la parte externa de las puertas y a una altura de 1.20 m con respecto al nivel del piso (fotografía 5.11).



Fotografía 5. 11: Lectores TAG, antes de ser instalados y ya instalados, en la puerta de acceso.

Conexión eléctrica de los registros.

En el diagrama 5.1 se presenta la distribución eléctrica que hay en el sistema de acceso de personal y equipo, donde se indican los voltajes que entran en cada unos de los registro.

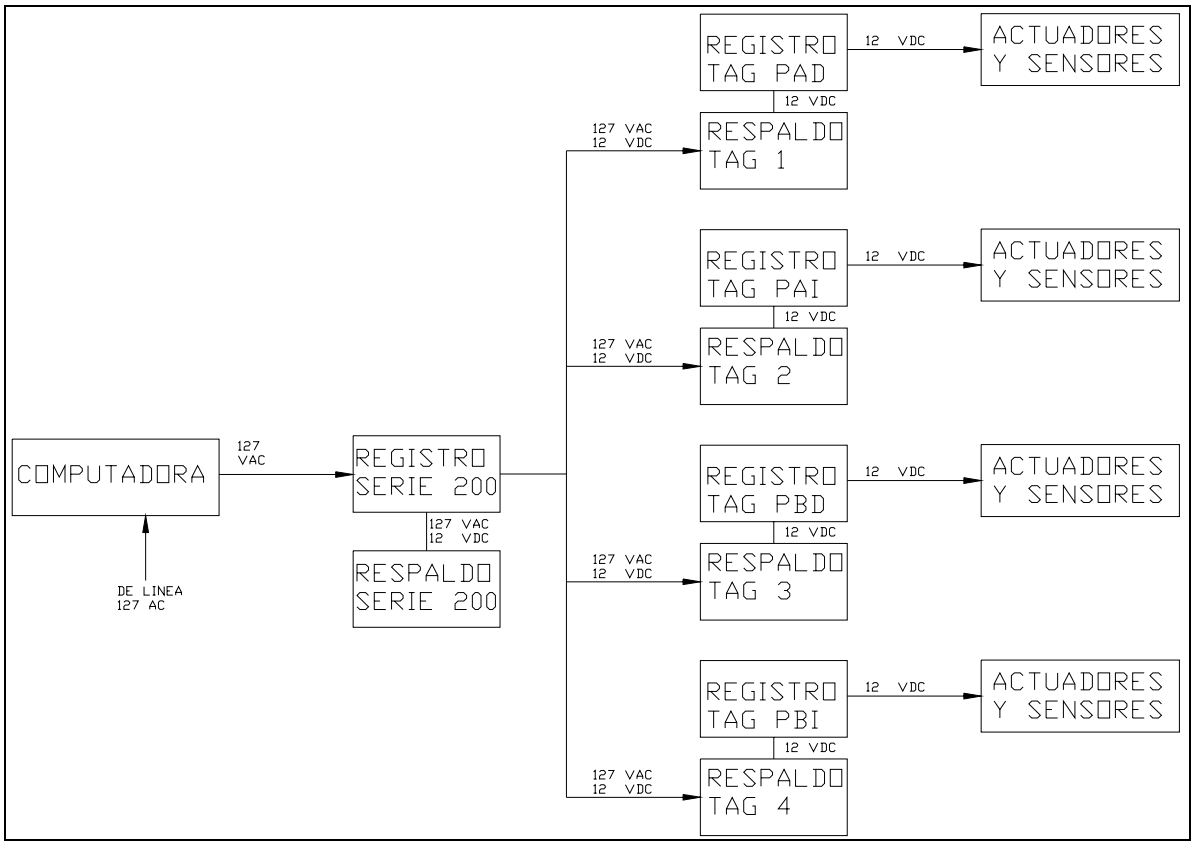


Diagrama 5. 1: A bloques de la conexión de los registros TAG.

Registro series 2000.

- El Registro Series2000 fue colocado a más de 2.50 m de altura del nivel del piso para asegurar que no estuviera al alcance de los usuarios con el equipo siguiente: Cuatro módulos Series2000, respaldo de energía con un No Break, fuente de voltaje de 12 Vdc.

Fotografía 5. 12: Registro series 2000.

En el diagrama 5.2 se presenta las conexiones eléctricas del series 2000. Se observa que la alimentación es tomada de un tablero eléctrico, y para distribuirlo al sistema se hace uso de contactos polarizados desde el cual se conecta a un respaldo de baterías, una fuente de alimentación regulada de 13.8 Vdc y la alimentación de 127 Vac, que van todos los respaldos del módulo TAG.

Asimismo observamos que hay dos voltajes de alimentación que son distribuidos al sistema por medio de dos clemas o tiras de conexión, una que distribuye un voltaje de 127 Vac y otra que distribuye un voltaje de 13.8 Vdc.

Nota: el diagrama que se muestra contiene las conexiones finales que se realizaron al sistema cuando se efectuaron las pruebas en las instalaciones, dichas correcciones se explicaran más adelante.

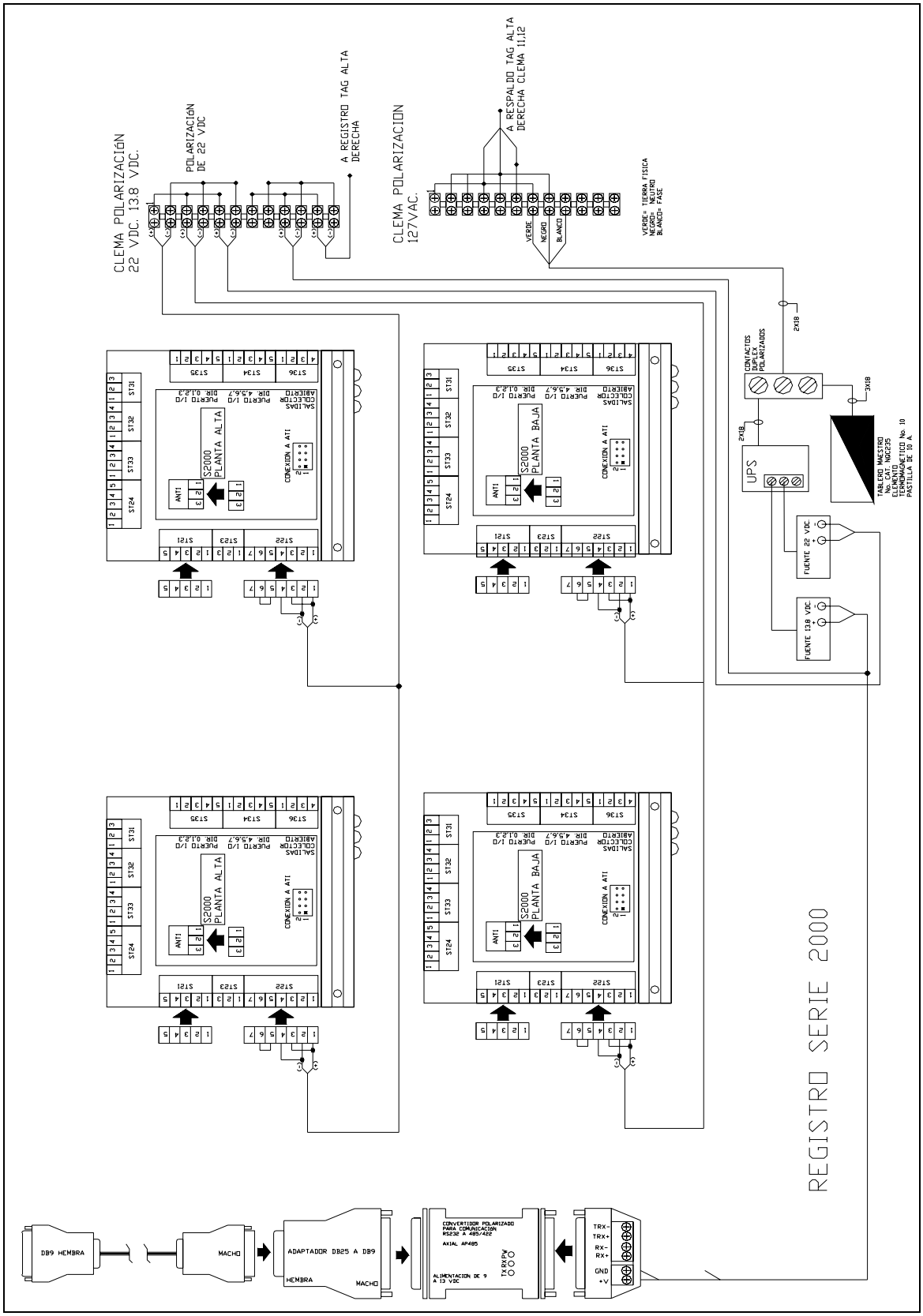


Diagrama 5. 2: de la conexión eléctrica del registro series 2000

En el diagrama 5.3 se observa la distribución del voltaje del sistema, una vez más se hace uso de una clema para distribuir los voltajes provenientes del registro series 2000, el voltaje de 127 Vac alimenta aun respaldo de batería, los elementos que conforman a este respaldo son: una fuente de alimentación, un cargador y una batería de 12 Vdc, en caso de ausencia de voltaje esta entra en funciones para dar una autonomía por espacio de 7 Hrs.

Registro y respaldo TAG.

Tanto los registros TAG como sus respectivos respaldos TAG ver figura 5.13, fueron conectados en la misma forma. Cada registro TAG, contiene los siguientes dispositivos:

- Un módulo TAG-PC.
- Un módulo de potencia

Mientras que el respaldo TAG contiene los siguientes dispositivos:

- Cargador de baterías
- Batería.

Fotografía 5. 13: registro y respaldo TAG.

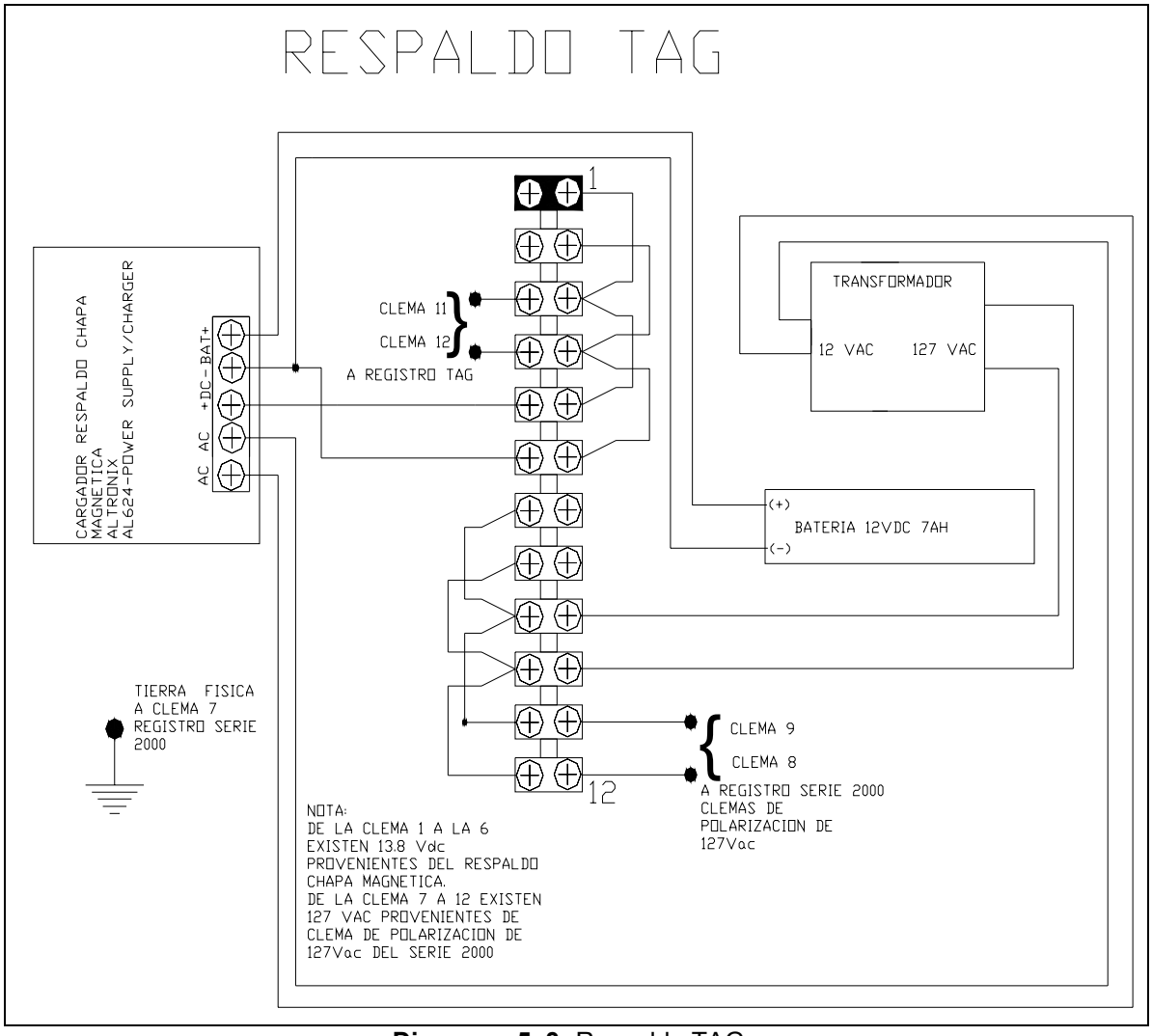


Diagrama 5. 3: Respaldo TAG.

Como se aprecia en el diagrama 5.4 a través de la clema se distribuyen los voltajes provenientes del Registro Series 2000, observamos que también a través de la misma clema se están alimentando a los actuadores y sensores que dependen del módulo de potencia. También llegan los 12 Vdc proveniente del respaldo TAG que sirven solo para alimentar la cerradura magnética y la alarma.

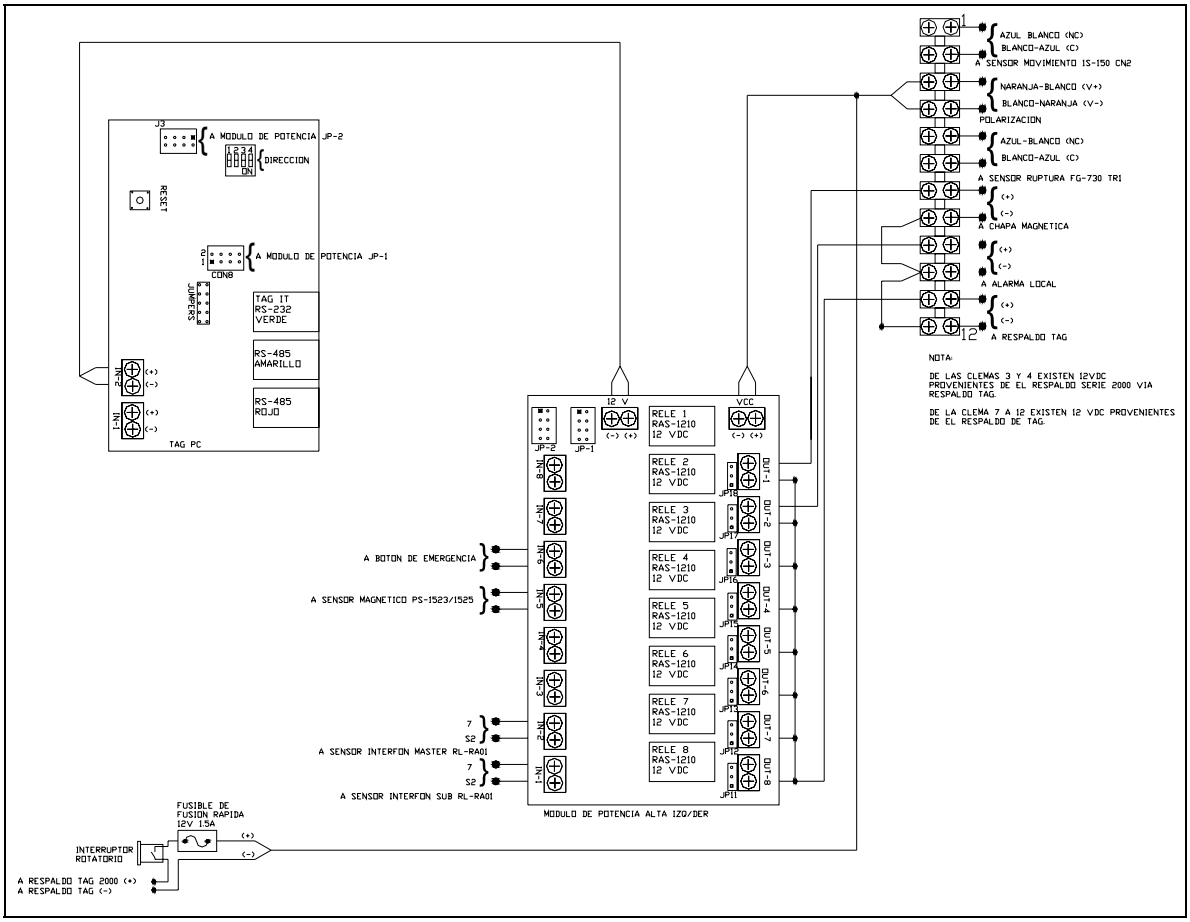


Diagrama 5. 4: De conexiones en el registro TAG.

Instalación de la comunicación física de los registros.

En el diagrama 5.5 a bloques se observa la comunicación del sistema de acceso de personal y equipo.

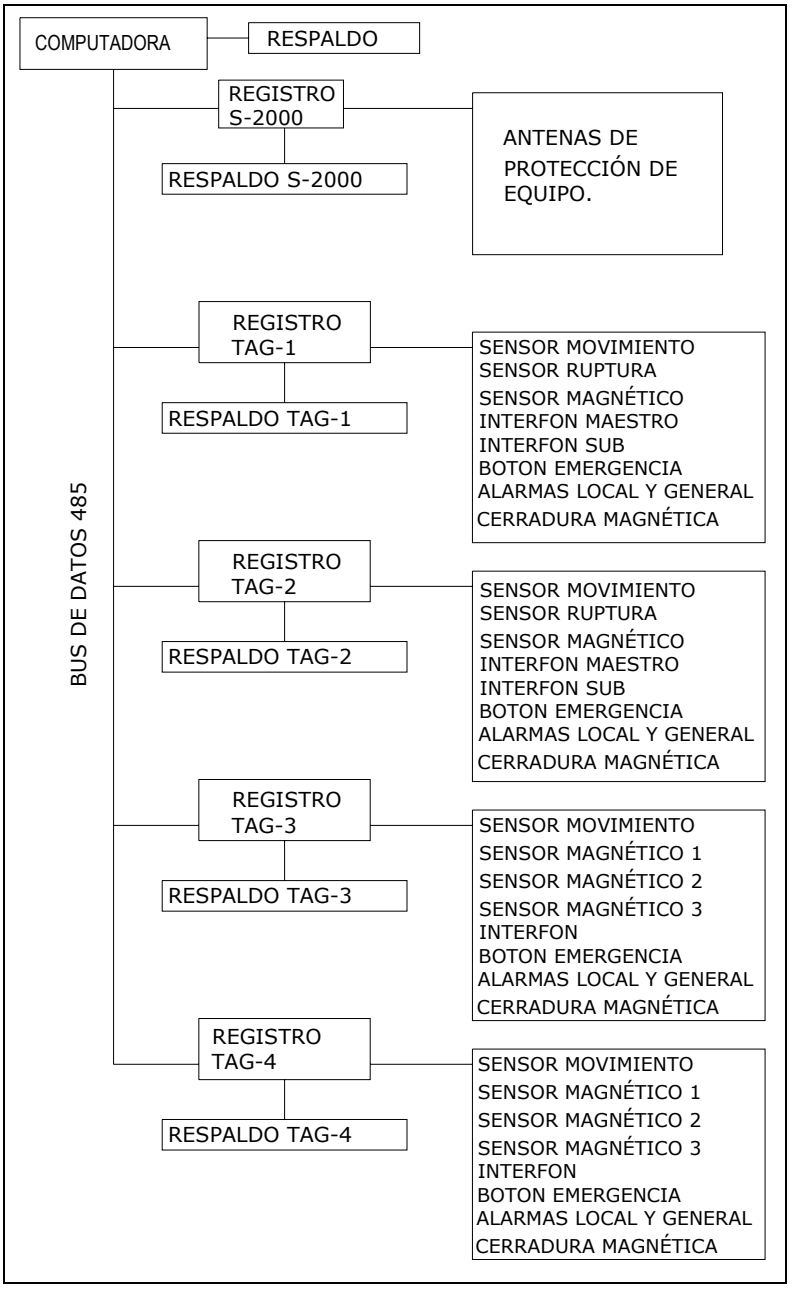


Diagrama 5. 5: A bloques de la comunicación entre los registros y la computadora.

Conexión de la comunicación del registro series 2000.

A continuación se presenta un diagrama de las conexiones de la comunicación del registro series 2000.

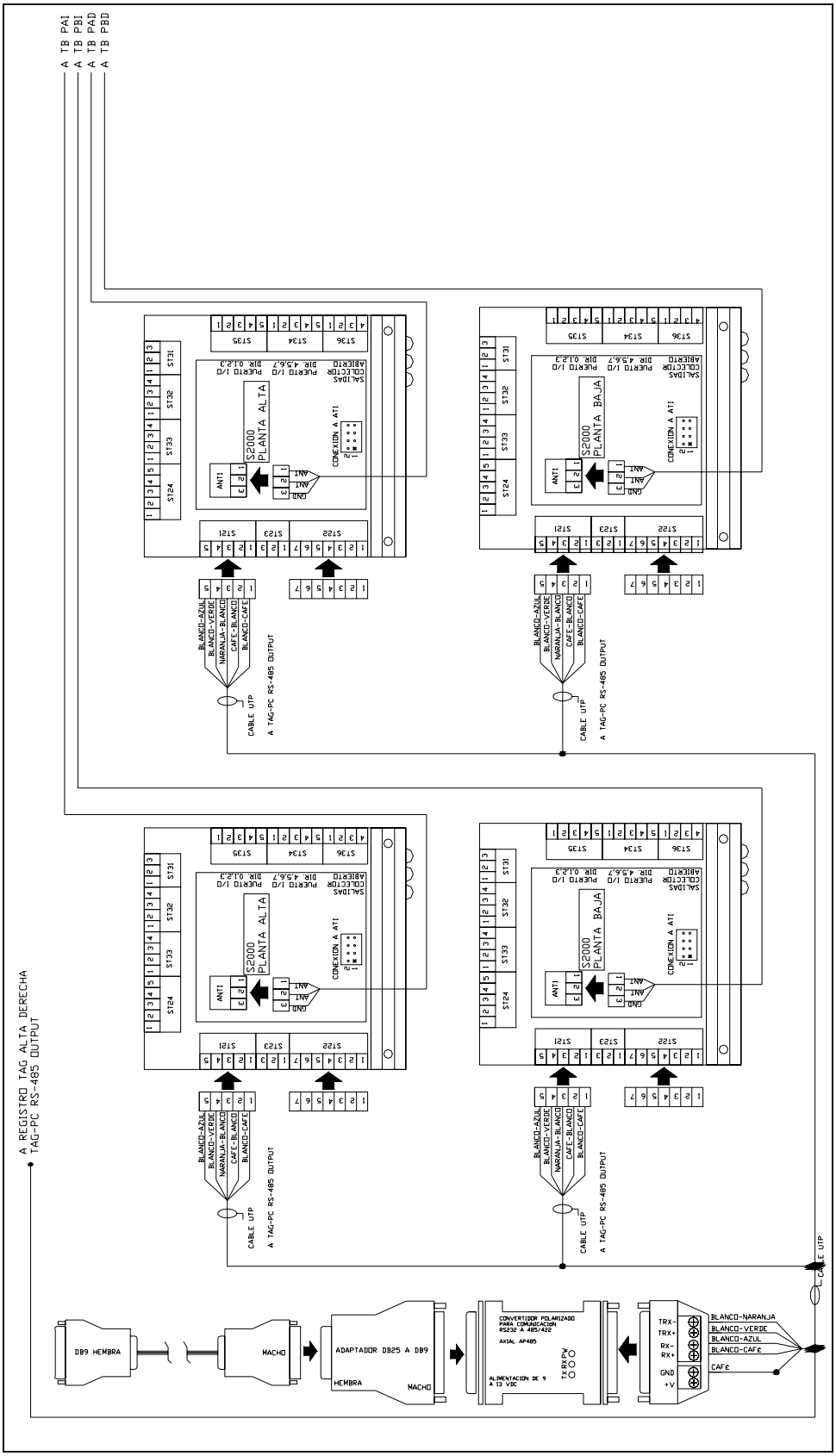


Diagrama 5. 6: comunicación del registro series 2000

Del diagrama 5.6 observamos que la comunicación RS232 con la computadora y el sistema se hace a través de un conversor RS 232 a RS485/422 autoalimentado marca AXIAL, modelo AP485[2] y de este a los series 2000 y módulos TAG PC (no se muestran en el presente plano) vía cable UTP categoría 5.

En el plano también observamos una clema en las que van conectadas las tierras provenientes de los tunning box conectados a las antenas, y estas a su vez conectadas a los series 2000.

En el diagrama 5.7 vemos las comunicación que hay entre el módulo TAG-PC y el módulo de potencia. Además que los conectores RJ45 hacen la comunicación con el lector TAG (conector verde) y la comunicación en RS485 (conector amarillo) proveniente ya sea del series 2000 o de otro TAG PC y el enlace a otro lector TAG (conector rojo) si lo hubiera.

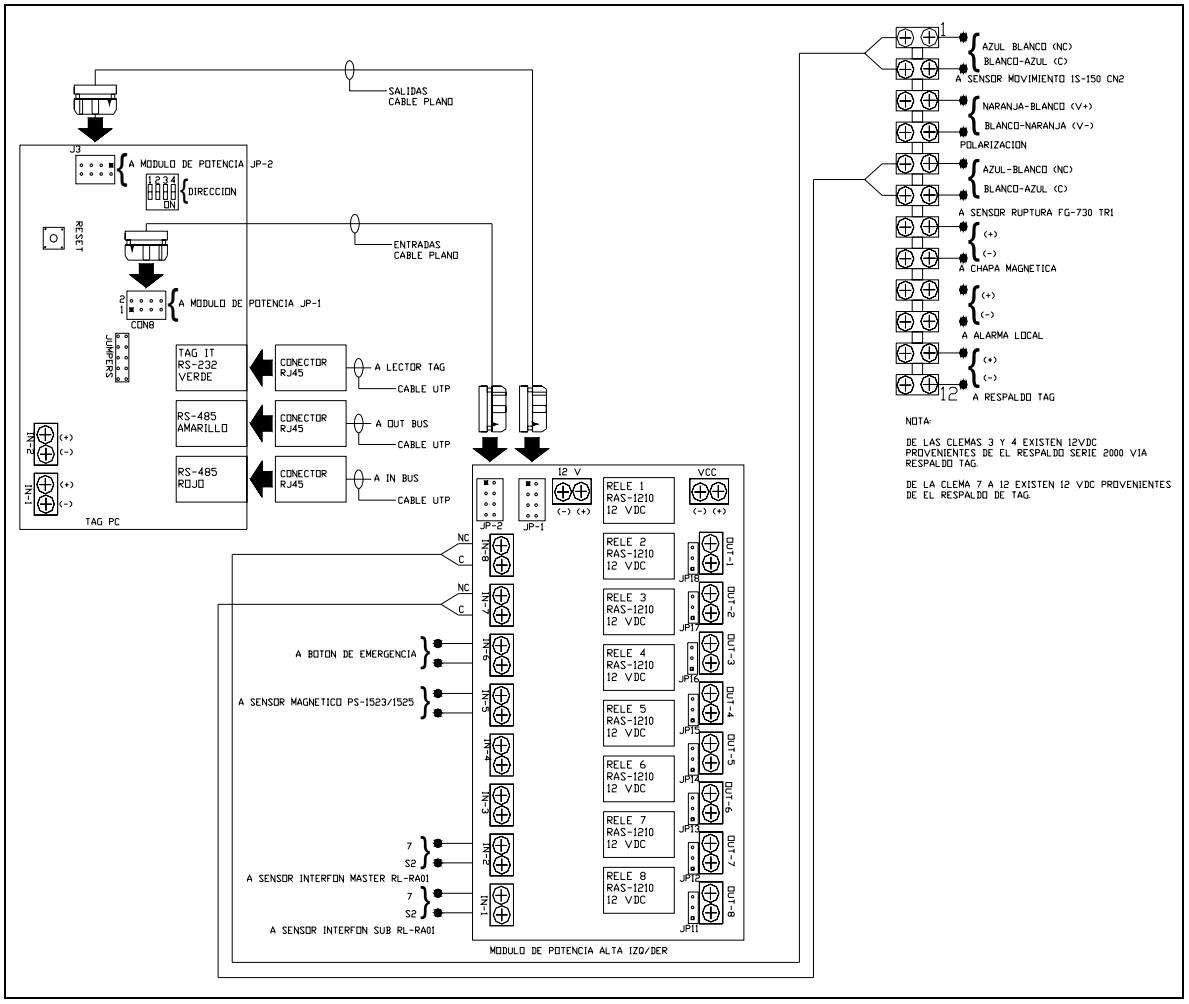


Diagrama 5. 7: Comunicación entre módulo TAG-PC y etapa de potencia

[2] Para información más detallada de este dispositivo ver el APÉNDICE E Pág. 190.

REALIZACIÓN DE PRUEBAS.

Las primeras pruebas que se realizaron al sistema fueron hechas por etapas y realizadas en el CDM[3] (ver tabla) y según los dispositivos que se tratasen:

Etapa	Dispositivos
Pruebas de operación individual de los dispositivos.	Sensores. Actuadores. Lector de acceso de personal TAG. Lector de baja frecuencia Series 2000.
Pruebas de diseño.	Módulo TAG-PC. Modulo de potencia. Antenas.
Pruebas de operación de software.	Software PIL. Software SAPPE.
Pruebas de sistemas en instalación.	De alimentación de voltaje. Módulo TAG-PC. Módulo de potencia. Sistema Contra intrusos. Sistema de acceso de personal. Sistema de protección de equipo.

Tabla 5. 2: Etapas de las pruebas.

Pruebas de operación de dispositivos.

Estas pruebas tenían por objetivo conocer la operación y buen funcionamiento del equipo adquirido, en todos ellos se hicieron pruebas de voltaje de operación, rango de detección (en el caso de los sensores) y tiempos de respuesta en la que todos los dispositivos (ver tabla), cumplieron de acuerdo a las especificaciones del fabricante y en el caso de los lectores se hicieron pruebas de comunicación.

Equipo	Dispositivos	Pruebas
Sensores:	De movimiento. De ruptura de cristal. Sensores magnéticos	Voltaje de operación, De rango de detección y Sensibilidad
Actuadores:	Cerradura magnética. Alarmas. Interfonos	Voltaje de operación Y tiempo de respuesta.
Lectores	TAG (alta frecuencia) SERIES 2000 (baja frecuencia)	Voltaje de operación, Comunicación y configuración

Tabla 5. 3: Pruebas realizadas a los sensores, actuadores y lectores.

Hay que hacer notar que los interfonos trabajan de fábrica con un voltaje de 127 Vac, pero la mayoría de nuestro sistema trabaja con un voltaje de 12 Vdc por lo que se adaptaron los interfonos, para que pudieran trabajar con este voltaje (que además estaba respaldado).

Al abrir los teléfonos, encontramos que uno de los teléfonos tenia la fuente de voltaje, mientras que el otro tenia la parte de comunicación, que trabajaba a 9 Vdc, por lo que en el teléfono que contenía la fuente, se suprimió la etapa de rectificación y conectamos los 12 Vdc directamente a la etapa de regulación a 9 Vdc.

[3] CDM: Centro de Diseño y Manufactura FI, UNAM.

Para la prueba de los lectores (ver tabla), en cuanto a comunicación, nos auxiliamos de software proporcionado por TEXAS INSTRUMENTS (TI), para el lector TAG, se utilizó el programa S6-Util, mientras que para el lector de baja frecuencia se hizo uso del programa S2-Util, en el caso del series 2000 se tuvo que configurar para su correcta operación[4], las pruebas que se hicieron a los lectores fueron de establecer comunicación con la PC de acuerdo a los estándares de comunicación establecido, del correcto envió y recepción de las tramas de información, y del rango de detección de los transponder,

Lectores	Prueba realizada.	observaciones
TAG (alta frecuencia)	Comunicación con el software proporcionado por TI.	Comunicación en RS232.
	Envío y recepción de orden al lector (por medio del programa PIL)	Se verificó que las ordenes enviadas y respuesta obtenidas, estuvieran de acuerdo al protocolo HP6000.
	Rango de detección de transponder	Detección de los transponders dentro de los rangos establecidos por el fabricante aprox. 12 cm.
SERIES 2000 (Baja frecuencia)	Comunicación con el software proporcionado por TI.	Comunicación y configuración en RS422, se tuvo que usar un convertidor de RS232 a RS422/485.
	Envío y recepción de orden al lector(por medio del programa PIL)	Se verificó que las ordenes enviadas y respuesta obtenidas, estuvieran de acuerdo al protocolo TBP 2000 en RS485.
	Rango de detección de transponder	Para la detección de transponders, se hizo uso de una antena diseñada para ser usada en las pruebas semejante a la que se iba a usar en el proyecto. todos los transponder estaban cerca de los rangos de detección.

Tabla 5. 4: Pruebas de comunicación en lectores.

Pruebas con los TAG PC y modulo de potencia.

Los diseños preliminares de los módulos TAG-PC y POTENCIA se construyeron en tarjetas perforadas esto fue con la finalidad de realizar los cambios pertinentes en su configuración final.

Las pruebas realizadas para el módulo TAG-PC fue establecer comunicación con la PC y del correcto funcionamiento del programa residente en el microcontrolador. Asimismo para el caso del módulo de potencia se realizaron pruebas de comunicación entre ella y el módulo TAG-PC.

Teniendo probados ambos módulos se mandaron a elaborar los circuitos impresos (CI), y de la misma forma que se realizaron la pruebas con las tarjetas perforadas se hizo lo mismo con los CI, las pruebas fueron las siguientes:

[4] Ver APÉNDICE A Pág. 141.

Pruebas (MODULO de POTENCIA)	Descripción
Voltaje de alimentación y continuidad del circuito.	Verificamos que en todas las pistas hubiera continuidad, además de que los voltajes de 5 Vdc para alimentar a los relevadores y demás circuitería fuera la correcta, así como comprobar que los 12 Vdc que iban a manejar a la salida los relevadores fueran los adecuados, para que no se dañaran.
Activación y desactivación de relevadores.	Se comprobó que los relevadores se habilitarán y deshabilitarán correctamente, tanto en tarjeta perforada, como en circuito impreso, primero en forma aislada y después con el TAG PC. y por último con los actuadores conectados a los relevadores.
Detección de los cambios de estado de los sensores.	Conectando los sensores al MODULO DE POTENCIA y haciéndolos cambiar de estado, se comprobó que se detectara ese cambio, primero sin el modulo de TAG PC, y después con este.
Pruebas (MODULO TAG PC)	
Continuidad del circuito, suministro y alimentación de voltaje.	Verificamos que en todas las pistas hubiera continuidad, además de que los voltajes de 5V para alimentar a la circuitería fuera la correcta.
De software.	Se verifico por medio del emulador, que el programa residente en el microcontrolador COP 8[5], del modulo TAG PC funcionara adecuadamente,
Activación y desactivación de relevadores.	Usando el emulador, mandábamos a activar y desactivar a los relevadores del MODULO DE POTENCIA.
Detección de los cambios de estado de los sensores.	Teniendo de los sensores conectados al MODULO DE POTENCIA y haciéndolos cambiar de estado, se comprobó que se detectara ese cambio, en modulo TAG PC, con el emulador.

Tabla 5. 5: Pruebas de funcionamiento del MODULO TAG PC.

Pruebas preliminares de comunicación.

Se llevaron a cabo en laboratorio, en estas se involucraron la mayoría de los elementos que se iban a considerar dentro de la instalación final:

- Lector de alta frecuencia TAG
- Lector de baja frecuencia SERIES 2000
- Modulo TAG PC
- Modulo de POTENCIA
- Conversor RS232-RS485
- Sensores
- Actuadores

Además de probar el funcionamiento adecuado de:

- Software PIL
- El protocolo Tiris Bus Protocol (TBP)
- La comunicación en RS485

Todos los módulos se colocaron de manera que tuviéramos la ventaja de poderlos manipular para las pruebas (ver fotografía 5.14)

[5] El microcontrolador utilizado llamado COP8 (Controlador Orientado a Procesos de 8 bits), de Nacional Semiconductor.

Fotografía 5. 14: Pruebas realizadas en laboratorio.

Como ya lo habíamos mencionado anteriormente, la comunicación se hizo con un protocolo de transmisión de datos RS485, y la configuración de maestro a esclavo, donde la computadora es el maestro y los lectores de baja frecuencia Series 2000 y módulos TAG PC, los esclavos. Por lo que a cada uno de los dispositivos que estuvieran conectados al bus de transmisión de datos se les asigno un numero de identificación (ID), para efectuar la comunicación adecuadamente.

En todos los casos se enviaron los comandos adecuados para obtener una respuesta de los dispositivos, para esto se les asigno previamente un ID con el cual los identificaríamos.

Pruebas de comunicación	Descripción
Con el lector series 2000	Se enviaron comandos en TBP, para que el lector SERIES 2000 respondiera con su ID, así como detectar la presencia de un transponder presente y enviara el ID de este último.
Con módulo TAG PC	Envió de comandos a un solo TAG PC, estos comandos eran los siguientes: ordenes a los lectores TAG, de lectura de transponder de acceso de personal[6], de habilitación y deshabilitación de relevadores y el estado de los sensores.

Tabla 5. 6: Pruebas de comunicación.

[6] Al igual que en el renglón anterior, los TAG en caso de haber detectado la presencia de algún transponder, debía de leerlo y enviar su ID del transponder.

Pruebas en la instalación.

Estas pruebas se realizaron cuando ya estaban colocados todos los dispositivos, en el edificio, básicamente las pruebas fueron las mismas que se realizaron en laboratorio, sin embargo surgieron algunos imprevistos de los cuales algunas de las soluciones que se le dieron las comentaremos más adelante, pero otras, debido a que se llevaron más tiempo de análisis se verán en el siguiente capítulo.

Pruebas en el cableado.

Recordando que son cuatro las áreas a proteger del edificio (PAD, PAI, PBD Y PBI) el procedimiento que se muestra a continuación, se hizo para cada una de las áreas:

Se procedió primero a revisar que todos los cables (Alimentación y de comunicación), estuviesen en perfecto estado, esto es que no presentaran algún daño físico, como rajaduras o que estuviesen muy tensos, asimismo se probó continuidad[7] en cada uno de ellos, esto se realizó con el fin de garantizar que el cableado no presentara cortos circuitos, falsos contactos o cables interrumpidos (abiertos), al momento de conectar estos cables a los dispositivos.

Una vez realizada esta prueba se procedió a conectar cada uno de los diferentes dispositivos, se revisó el voltaje de alimentación mediante un multímetro, y en el caso de los sensores se comprobó su correcto funcionamiento.

Por último se conectaron los sensores y actuadores a la Etapa de Potencia, y se revisó que los cambios de estado (activo / inactivo) generados por los sensores estuviesen presentes, así como también la activación y desactivación manual de los actuadores.

Finalmente utilizamos el programa PIL para realizar las pruebas de comunicación con la PC.

Pruebas de comunicación.

Dos de los aspectos más importantes que determinan las características del sistema son: por una parte, la distancia de los módulos TAG PC y los lectores Series 2000 en el bus de comunicación y, por otra parte, los tiempos de respuesta de estos dispositivos.

Para ambas características del sistema encontramos algunos problemas para la realización de las siguientes pruebas, la forma en que se analizaron estos problemas y como los resolvimos los veremos en el siguiente capítulo.

Pruebas de lectura de sensores y activación / desactivación de actuadores con el programa PIL.

En esta parte verificamos que no tenemos problemas de comunicación entre la PC y el módulo TAG-PC, las pruebas realizadas fueron las siguientes:

[7] Para la realización de esta prueba utilizamos un multímetro.

1. Se codificaban los comandos correspondientes con la dirección del TAG-PC y la instrucción ya fuera de lectura de sensores o activación / desactivación de actuadores a través del programa PIL.
2. En caso de ser lectura de sensores se hacia cambiar de estado alguno de ellos y se observaba en la ventana de la interfaz principal de PIL la respuesta enviada por el TAG-PC.
3. Cuando se trataba de activación / desactivación de actuadores, se mandaba la instrucción para activarlos o desactivarlos; el TAG-PC enviaba una respuesta a PIL como confirmación de que se había ejecutado la instrucción satisfactoriamente que nosotros observamos en la ventana de la interfaz principal de PIL.
4. En caso de que no se pudiera observar una respuesta del sensor o actuador que se estuvieran probando, se procedía a verificar que estuviera bien conectado, además de recibir el voltaje adecuado y verificar que el modulo de potencia y del TAG-PC estuvieran trabajando adecuadamente.

Pruebas en el sistema de acceso de personal.

La siguiente prueba a realizar fue establecer comunicación con el sistema de acceso de personal verificando lo siguiente:

1. A través del programa PIL se enviaban los comandos para realizar la lectura de los lectores de alta frecuencia (TAG) que eran recibidos por el TAG-PC.
2. Dependiendo de si existiera o no una credencial presente en el área de detección del lector TAG, este enviaba la respuesta a través del TAG-PC a la computadora.
3. Si había leído una credencial, en la ventana de PIL veíamos el ID correspondiente a la credencial, en caso de no existir una credencial, nos enviaba un comando de ausencia de lectura.

En caso de no responder el lector, revisábamos conexiones y voltajes del lector.

Pruebas en el sistema de protección de equipos.

Para la realización de las pruebas del sistema de protección de equipo se hicieron las siguientes acciones:

1. Establecer comunicación con el programa PIL.
2. La sintonía de las antenas de acuerdo al procedimiento descrito en el capítulo anterior, utilizando el ATI para verificar la sintonización.
3. Una vez sintonizadas las antenas se probaron distancias de lectura de los transponders, sin colocar en los equipos a proteger
4. Probar la distancia de lectura de las antenas con los transponder colocados dentro de los equipos.

Los puntos tres y cuatro fueron realizados con la ayuda del programa PIL, con el que obteníamos los ID de los transponders.

Estas pruebas no se pudieron concluir en su momento, ya que las antenas no trabajaron de manera satisfactoria. los resultados de esta prueba los analizamos en el siguiente capítulo.

Pruebas globales.

Después de haber realizado estas pruebas de forma independiente, realizamos una prueba final la cual consistía en leer el estado de los diferentes sensores, la activación y desactivación de los actuadores, la lectura del sistema de acceso de personal y la lectura del sistema de protección de equipos del área en cuestión.

Como se mencionó anteriormente estas pruebas se realizaron para cada una de las áreas por lo que al tener las cuatro áreas revisadas, con la ayuda del programa PIL realizamos ahora pruebas por áreas, primero la PAI y PAD, después la PAI, PAD y PBI, finalmente las cuatro áreas los resultados obtenidos al realizar estas pruebas fueron las siguientes:

- Al realizar la pruebas por área al reducir el tiempo de transmisión de cada uno de los comandos el módulo TAG-PC dejaba de responder.
- En el caso de tener más de dos áreas se debía de incrementar este tiempo ya que de lo contrario los módulos dejaban de responder.

La solución de estos problemas los veremos en el siguiente capítulo.

Pruebas con el programa de aplicación SAPPE.

Las pruebas que presentamos a continuación fueron realizadas por el equipo que desarrollo el sistema que finalmente quedaría residente en el control maestro.

Una de las etapas más delicadas de la creación de software es el proceso de pruebas, ya que, además de consumir una gran cantidad de tiempo, exige un minucioso análisis que permita detectar la mayor cantidad de errores dentro de la aplicación.

No es conveniente que la etapa de pruebas se considere como el proceso final en la creación de un programa de aplicación, puesto que a medida que crezca el sistema se volverá más complejo detectar una falla en su estructura y más aún encontrar la línea de código exacta donde se está generando el problema. Por ello, consideramos que las pruebas deben ser programadas y realizadas antes, durante y después de comenzar el proyecto con el fin de asegurar que cada parte del sistema este funcionando de la mejor manera posible.

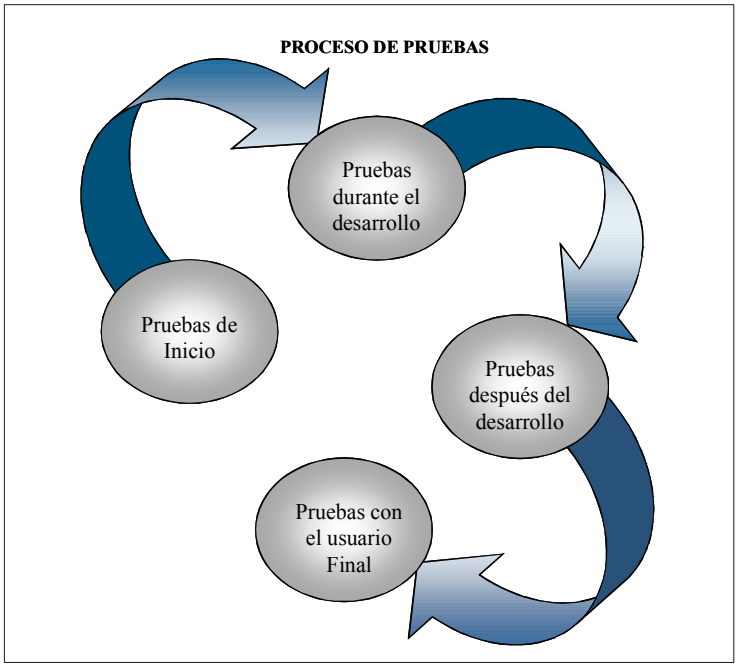


Diagrama 5. 8: Proceso de pruebas.

Con base en este diagrama determinamos un plan de pruebas descrito a continuación:

Planificación de pruebas para el SAPPE.

Bloques / Etapas	Comunicaciones	Bases de Datos	Seguridad	Interfaz
Pruebas de Inicio	ok			
Tiempo de Desarrollo	ok	ok	ok	ok
Después de la programación	ok	ok	ok	ok
Usuario Final				ok

Tabla 5. 7: Etapa de pruebas.

A continuación presentaremos las pruebas realizadas para cada uno de los bloques así como el seguimiento que se le fue dando a través de las distintas etapas.

Pruebas de Inicio

En proyectos enfocados al desarrollo de nuevas tecnologías, las pruebas anticipadas proporcionan una herramienta de exploración para comprender de manera explícita la forma en que opera cada una de las partes del sistema y la forma en que habremos de interactuar con ellas para llegar a nuestros objetivos.

En nuestro caso particular realizar pruebas antes de comenzar a estructurar SAPPE fue fundamental, ya que este programa está orientado al control y operación de hardware de innovación tecnológica. Para poder diseñar e implementar la lógica operacional del sistema de seguridad, fue necesario comprender el funcionamiento de los dispositivos, su protocolo de comunicación y sobretodo la forma en que interactuaría con el software. Por ello consideramos de suma importancia, y como primer paso para la creación del sistema, realizar pruebas directamente con los dispositivos.

Para la realización de estas pruebas generamos un programa cuyo único objetivo fue mandar instrucciones de lectura a los dispositivos, obtener las cadenas de respuesta e interpretarlas. Estas pruebas permitieron comprobar:

- La forma en que debe ser enviada la instrucción para poder comunicarnos de manera adecuada con ellos.
- La estructura de la cadena de respuesta de los dispositivos, que posteriormente serían de gran utilidad para poder descomponer adecuadamente la cadena de acuerdo a nuestros intereses.
- Nos permitió establecer el protocolo de comunicación .
- Que funcionaba correctamente la comunicación entre los dispositivos y la computadora a través del puerto serie.

Pruebas durante el desarrollo.

Las pruebas durante el desarrollo son pruebas informales que estuvimos realizando gran cantidad de veces con la finalidad de verificar que todo el código escrito hasta el momento se ejecutara correctamente.

En esta fase se probó cada uno de los módulos generados así como su integración con otros módulos. Para realizar pruebas de manera individual se simuló la entrada de datos correspondientes con los requerimientos de cada módulo.

A continuación haremos una breve explicación de las pruebas realizadas en cada uno de los módulos:

Comunicaciones.

El módulo de comunicaciones implica todos los subprocesos relacionados con la transmisión, recepción y procesamiento de datos que circulan entre el hardware y la aplicación. Por lo que fue necesario realizar las pruebas directamente con cada tipo de dispositivo que iba a estar operando dentro del sistema.

Para ello requerimos de un módulo de lectura de alta frecuencia, un módulo de lectura de baja frecuencia, sensores, y dispositivos que simularan la acción de los actuadores; así como tarjetas iguales a las que serían proporcionadas a los usuarios y chips como los que serían colocados para proteger el equipo. De esta manera pudimos recrear un sistema homólogo al que estaría operando la aplicación.

Bases de Datos.

Una vez concluido el diseño conceptual y lógico de la Base de Datos se desarrollaron los módulos que interactuarían directamente con el motor de la base de Datos (Easysoft IB6 ODBC). Cada uno de estos módulos fue probado manejando datos ficticios que simularían la información contenida en la Base de Datos real. Se realizaron:

- Altas de usuarios y equipos.
- Simulación de entradas y Salidas de Usuarios.
- Simulación de salidas de equipo.
- Modificación de datos.
- Consulta de Información.
- Generación de Reportes.

Para estas pruebas utilizamos un módulo de lectura conectado al puerto serie igual al que se utilizaría en las Instalaciones.

Interfaz.

Dentro de la interfaz estuvimos verificando cada una de las rutas posibles generadas a partir de la selección de una opción, con el objetivo de comprobar que se ejecutaran todos los botones y menús y, se desplegara la información correctamente. Asimismo confirmamos que cada pantalla se desplegara de acuerdo a los privilegios del usuario.

A medida que íbamos avanzando en la programación de los módulos realizamos pruebas de integración entre ellos.

Pruebas después de la Programación.

Después de haber revisado individualmente cada proceso de la aplicación así como la integración entre módulos, contamos con los elementos necesarios para realizar la instalación de la aplicación y las pruebas finales en el entorno real. Estas pruebas finales nos permitieron verificar que todos los procesos de la aplicación se ejecutaran correctamente en condiciones verdaderas y nos permitieron validar que la aplicación cumpliera con las especificaciones del cliente.

Durante el desarrollo se trataron de eliminar todas las posibles fallas en la ejecución de los procesos, sin embargo, al ser una aplicación dedicada a interactuar con elementos externos, se presentaron situaciones que alteraron el rendimiento de la aplicación.

Una de estas deficiencias fue el tiempo de verificación de cada uno de los dispositivos y por consiguiente la respuesta de acción de la aplicación. Al ser un sistema de seguridad, el tiempo de respuesta y acción, es un aspecto crítico. Durante el desarrollo, las pruebas se habían realizado con la computadora conectada a muy corta distancia de los dispositivos, condición que cambio totalmente en las instalaciones. A pesar de haber considerado tiempos de respuesta teóricamente, de manera real, y debido a que las distancias se incrementaban para algunos de los dispositivos, los tiempos de respuesta se habían incrementado considerablemente por lo que se tuvo que buscar una solución efectiva que proporcionara el máximo rendimiento.

Para ello tuvimos que ajustar el módulo de comunicaciones para que se adecuara a estas condiciones. La solución encontrada fue manejar tiempos de espera para cada área.

De manera general se realizaron pruebas de toda la aplicación tratando de cubrir todas sus vertientes. Para llevar un control de todas las revisiones hechas al programa definimos un plan que cubriera la mayor parte de los procesos de la aplicación. Esta exploración final la definimos en la siguiente tabla:

Bloque	Módulo	Operaciones	Resultado	Observaciones
Comunicación	Principal	✓ Monitorear los dispositivos. ✓ Controlar la lógica de los dispositivos. ✓ Restringir Horarios.	Correcto	Se modificaron los tiempos de espera para recepción de datos de acuerdo al área del edificio.
	Puerto	✓ Configuración del Puerto de Comunicaciones.	Correcto	Se cambió la configuración del Protocolo de Comunicación RS-232 a "Sin control de Flujo".
	Dispositivos	✓ Agregar y eliminar dispositivos. ✓ Generación de Instrucciones.	Correcto	Se generaron matrices con las instrucciones a enviar en ASCCI, para disminuir los tiempos de procesamiento. Se configuraron las cuatros áreas del edificio conforme a los dispositivos instalados, y realizamos varias pruebas cambiando las restricciones de cada área para verificar que la aplicación reaccionara a los nuevos parámetros de forma congruente. Estuvimos generando situaciones de emergencia como activación de sensores de ruptura, sensores de movimiento, puertas abiertas en horarios no autorizados, y salidas de equipo no autorizadas para comprobar que el sistema reaccionara correctamente a cada estado de alerta.
Bases de Datos	Altas	✓ Agregar usuarios. ✓ Agregar equipos.	Correcto	Se dieron de alta varias credenciales de prueba con datos reales del personal y con diferentes restricciones para cada uno, posteriormente se estuvieron realizando accesos y salidas en todas las áreas mediante estas credenciales para probar que el sistema respetara correctamente las condiciones para cada usuario. Se dieron de alta algunos identificadores de equipo y se estuvieron probando salidas de equipos autorizados en distintos horarios, así como salidas de equipos no autorizados. Se agregaron opciones de configuración, para facilitar la captura de información del usuario. (Específicamente agregamos un cuadro de selección donde se despliegan todos los días de la semana para restringir el acceso por días, teniendo como parámetro inicial de lunes a viernes).
	Bajas	✓ Dar de baja Usuarios. ✓ Dar de baja Equipos.	Correcto	Utilizando la misma información que generamos a partir de las pruebas de alta de usuarios, dimos de baja varias credenciales para comprobar que el usuario dado de baja perdiera todos los permisos de acceso, y únicamente se conservara su información.
	Cambios	✓ Modificar registros. ✓ Eliminar registros.	Correcto	Estuvimos modificando información de los usuarios creados para realizar las pruebas, desde datos personales del usuario hasta sus restricciones de acceso. Para verificar que los cambios se ejecutaran correctamente realizamos accesos con las nuevas restricciones del usuario.

	Incidentes	✓ Registro de Incidentes de Usuarios. ✓ Registros de Incidentes de Equipos	Correcto	Se agregaron opciones de búsqueda, que facilitaran la consulta de incidentes.
	Restricciones	✓ Restricción de Acceso a Usuarios. ✓ Restricción de Salida de Equipo.	Correcto	Se corrigieron botones del formulario que no estaban desplegando la información de manera correcta.
	Accesos y Salidas	✓ Registros de Accesos y Salidas de Usuarios ✓ Registros de Salida de Equipos.	Correcto	Se probaron todas las opciones posibles de restricción para el acceso de un usuario. Y todas las opciones posibles para salida de un equipo.
	Reportes	✓ Generación de Reportes de Usuarios, Equipos Incidentes.	Correcto	Se generaron reportes de cada opción permitida por el sistema. Se hicieron algunas modificaciones en el diseño del reporte y desplegado de la información.
	Búsqueda	✓ Consulta y búsqueda de información en la BD	Correcto	Se realizaron varias búsquedas aleatorias.
Interfaz	Principal	✓ Acceso al módulo de comunicaciones. ✓ Acceso al módulo de Bases de Datos. ✓ Monitoreo de accesos y salida de personal. ✓ Monitoreo de salida de equipo.	Correcto	Realizamos varios accesos y salidas de personal mediante credenciales dadas de alta para verificar la pantalla de monitoreo. Detectamos errores en el desplegado de accesos y salidas de personal, por lo que se modificó la función, así mismo agregamos un parámetro anteriormente no considerado (El área a la cual el usuario estaba accediendo).
	Interfaz Comunicaciones	✓ Botones y Pantallas para la administración manual de Dispositivos.	Correcto	Se comprobó que todas las opciones de configuración del módulo de comunicaciones se pudieran ejecutar.
	Interfaz Base de Datos	✓ Botones y Pantallas para las transacciones con la Base de Datos.	Correcto	Se comprobó que todos los botones desplegaran los datos, formularios y reportes de acuerdo a su propósito.

Tabla 5. 8: Pruebas realizadas al software.

6

ANÁLISIS DE RESULTADOS Y CONCLUSIONES.

ANÁLISIS DE RESULTADOS

Los resultados que se presentan aquí, fueron considerando las pruebas hechas a los equipos después de la instalación del sistema en el edificio.

Caso 1.

No todos los dispositivos respondían a las instrucciones de la computadora. Particularmente los que se encuentran en la parte final del bus de datos.

Después de revisar los datos y su incidencia, encontramos que los datos al final del bus llegaban corrompidos; se detectó que la causa era la potencia de la señal, que era tan débil que el lector ubicado al final recibía datos diferentes a los que se habían enviado desde el control maestro.

La razón por la cual los datos no llegaban con la suficiente potencia al final del bus de datos, era que al inicio del bus de datos, usamos un convertidor RS–232 a RS422/RS485 auto polarizado y la potencia a la salida del convertidor no era la adecuada para la longitud del cableado[1]. Por lo que se sustituyó el convertidor auto polarizado por uno que usara una fuente de alimentación externa que le pudiera proporcionar la potencia suficiente para llegar hasta el final del bus.

Caso 2.

El sistema se llega a trabar en algunos momentos, y se tiene que reiniciar el sistema.

Al probar la transmisión-recepción de las módulos encontramos que:

1. Cuando los módulos TAG-PC recibían una información destinada a ellos, en la cual se les pedía la lectura de una credencial, esta información era enviada hacia

[1] La distancia máxima del registro más lejano era de aprox. 60 metros.

el lector de acceso de personal, dichos lectores tardan más en responder en el caso de no encontrarse una credencial en el área de lectura del lector, ya que este ultimo hace tres lecturas para verificar si realmente no hay una credencial (transponder) en el área de lectura de la antena.

2. Los tiempos de respuesta de los lectores Series 2000 son muy cortos, comparados con los del TAG-PC, esto provocaba que los datos de respuesta de los módulos Series 2000 se añadieran en la cola de la trama recibida por los módulos TAG-PC y como la trama recibida por estos no coincidía con el protocolo, se quedaban en espera de más datos. Esto provoca que los módulos TAG-PC, ya no contestaran a ninguna orden y se tenían que reiniciar estos.

Para dar una solución al punto 2, se reviso y se depuró el firmware del módulo TAG-PC para que en caso de que no se ejecutara correctamente el programa de control, estos módulos se reiniciaran automáticamente. También se depuró la rutina de recepción de datos en el programa PIL generándose una forma diferente para leer la información proveniente de las tarjetas TAG-PC. Con esto el tiempo mínimo para recibir una nueva trama de datos bajo de 80 ms. a 35 ms.

El tiempo de respuesta máximo para cualquier comando es de 145 ms. (ver diagrama 6.1) sin embargo el tiempo fue establecido en 200 ms., y cuando no hay respuesta para un comando en el tiempo especificado, el control maestro limpia su bus de datos y se sitúa en el comando siguiente para enviarlo.

Existen instrucciones o respuestas por parte de las unidades esclavas que necesitan 30 ms para ser procesadas y podrá parecer que el tiempo de espera de datos es demasiado, considerando que el control maestro va a esperar 200 ms, pero en la lógica de P.I.L. existe una rutina que verifica si han llegado datos al bus de entrada, cuando encuentra al menos un byte empieza un conteo para que, en cuanto se reciba el último byte, inmediatamente se mande toda la trama para su valoración, con esto, el tiempo de 200 ms solo se alcanza si ninguno de los lectores contesta al comando enviado.

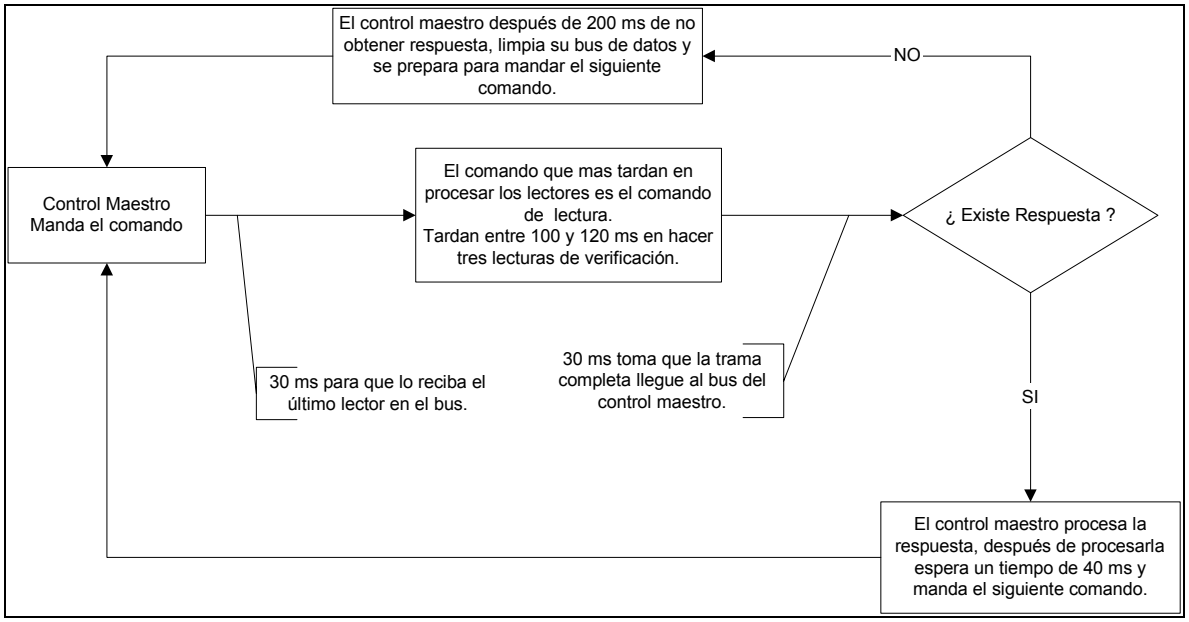


Diagrama 6. 1: del proceso con los tiempos antes mencionados.

Se puede observar que no usamos el tiempo mínimo para que el control maestro enviara el siguiente comando, esto se hizo así para evitar que los lectores se trabaran.

Caso 3.

El sistema de protección de equipo no funciona, dado que las antenas no estaban funcionando adecuadamente.

Cuando se terminó de sintonizar las antenas con el ATI[2], se realizaron pruebas de lectura con cada uno de los transponders utilizados (mount on metal , disco y cilíndrico), para verificar las distancias máximas de lectura garantizadas por el fabricante (Texas Instruments) que se pueden alcanzar con cada uno de ellos:

- Transponder cilíndrico $\leq$ 200 cm.
- Transponder mount on metal $\leq$ 120 cm.
- Transponder disco $\leq$ 150 cm.

Sin embargo, en las áreas de la planta alta las distancias obtenidas fueron:

- para el transponder cilíndrico: 30 cm.
- Para el disco aproximadamente: 20 cm.
- Y para el mount on metal la distancia era casi nula ya que sé tenía que colocar el transponder cerca de la antena.

Para las áreas de la planta baja las distancias eran aun más cortas que las de la planta alta. Otro punto a destacar fue que el led de presencia de voltaje en los tuninig box tenía una luz muy tenue.

[2] ATI: Antenna Tuning Indicator.

Después haber recalculado la tabla, para configurar los Tuning box[3] (ver tabla 6.1), se volvió a sintonizar las antenas con el ATI, pero dicho dispositivo nos indicaba que las antenas estaban sintonizadas. Entonces se revisaron las conexiones de los módulos series 2000 y tuning box con el fin de encontrar alguna mala conexión o falsos contactos pero todo se encontraba en orden aparente.

Ubicación Antena	Q	L (μH)	Dist-cab (m)	C_{CAB} (nF)	C_{RES} (nF)	C_{TUNB} (nF)	Jumpers
PAI	24.1	28.70	22.13	1.2642	44.3675	41.0411	JP2,JP5,JP8,JP11
PAD	22.8	28.52	19.00	0.9671	44.6209	41.4538	JP2,JP5,JP8,JP11
PBI	32.8	33.87	36.00	1.8324	38.1462	34.1138	JP2,JP5,JP11
PBD	17.4	33.58	50.20	1.7524	38.4486	34.4961	JP2,JP5

Tabla 6. 1: Configuración de jumpers para la sintonización de las antenas.

Para encontrar una solución al problema decidimos buscar la forma de sintonizar la antena de un área, ya que si lográbamos solucionarlo en una de ellas el procedimiento para las demás seria el mismo.

Al observar que la luz del led de los tuning box era muy tenue en las antenas de la planta alta y que en los tuning box de la planta baja ni siquiera el led encendía, se procedió entonces a medir voltajes con la ayuda de un osciloscopio[4], a la salida del módulo series 2000, en la entrada y salida del tuning box.

Al comparar los voltajes que nos proporciona el fabricante con los que nosotros medimos en el área (ver tabla 6.2), nos percatamos de que existía una diferencia significativa en el voltaje existente en la terminales de la antena lo que nos llevó a suponer que la antena no se encontraba correctamente sintonizada.

Voltajes en:	Fabicante (Vpp)	En el area (Vpp)
Series2000 (V_{2000})	500 (mínimo)	508
Tuninig Box (V_{tb})[5]	500 (aprox.)	450
Terminales de la antena	800 (máx)	90

Tabla 6. 2: Comparación de los voltajes obtenidos y del fabricante.

Decidimos entonces sintonizar la antena con el mismo método descrito en el capítulo 4 “diseño del sistema Pág. 43”, pero ahora usando el osciloscopio conectado a las terminales de la antena para monitorear el voltaje de esta última.

A medida que fuimos moviendo el núcleo de la bobina en el Tuning box observamos el cambio de voltaje en el osciloscopio, como lo habíamos hecho anteriormente, cambiamos la configuración del Tuning box, de acuerdo a la tabla 4.8 (capítulo 4 “diseño del sistema Pág. 43”), un renglón arriba o un renglón abajo, buscando donde existía más voltaje registrado por el osciloscopio, una vez encontrada la mejor configuración de las antena, se tomo la máxima distancia de lectura de los transponders (ver tabla 6.3).

[3] Los valores en la tabla fueron los mismos que los recalculados.
[4] Osciloscopio marca Tektronix modelo TDS 210 con punta de atenuación x10
[5] Este voltaje depende de la distancia del Tuning box, al lector.

Lecturas tomadas en el Área utilizando el osciloscopio	
Configuración de jumpers	2,5,8,11
Voltaje en las terminales de la antena	148Vpp.
Distancia de lecturas de transponder Mount on metal	.995 m.
Distancia de lectura de transponder de disco	1.45 m.
Distancia de lectura de transponder de cilíndro	1.56 m.

Tabla 6. 3: Valores obtenidos utilizando el osciloscopio.

Cabe mencionar que la luz del led se incremento de forma significativa, ya sintonizada la antena, buscamos incrementar la distancia de lectura de los transponders; aumentando el voltaje del módulo SERIES2000, ya que tienen la capacidad de poder polarizarlos con voltajes de 12 a 25 Volts.

La prueba se realizó de la siguiente forma:

1. Con una fuente de voltaje variable se polarizo el módulo series 2000 con un voltaje de inicial de 14 Vdc.
2. Se puso en modo de lectura continua al módulo series 2000.
3. Se sintonizo la antena con el método ya mencionado.
4. Se midió el voltaje con el osciloscopio en las terminales de la antena y se registra el voltaje obtenido (ver tabla 6.4).
5. Se vuelve a incrementar el voltaje de la antena y se repiten los puntos a partir del 3, hasta llegar a un voltaje de 22 volts.

V_{S2000} (Vdc)	14	16	18	20	22
V_{ant} (Vpp)	186	224	262	300	338

Tabla 6. 4: voltajes obtenidos con una fuente diferente a la usada en el sistema.

De acuerdo a los expresado anteriormente, se decidió poner una fuente adicional al sistema con un suministro de voltaje de 22V para alimentar al SERIES 2000, y así tener un mayor voltaje en las terminales de las antenas que se traduce en un campo electromagnético más fuerte para la lectura de transponders (ver tabla 6.5).

Área	Configuración Tuning Box.	Voltaje en terminales antena (Vpp.)
PAI	2,4,5,8	344
PAD	2,5,8,11	338
PBI	2,8	304
PBD	2,8	280

Tabla 6. 5: Voltajes obtenidos y configuración final de los jumpers.

Ya habiendo sintonizado las antenas y encontrado la máxima distancia de lectura disponible para cada antena, procedimos a hacer pruebas con los equipos que ya tenían instalados los transponders de protección de equipo; hasta aquí debemos de hacer las siguientes observaciones con respecto a estos dispositivos.

- En la realización de las pruebas, observamos que estos dispositivos, no son captados por las antenas en cierta posición

- De acuerdo al punto anterior, los transponders fueron colocados en los equipos de manera que sean captados siempre por las antenas.
- La antena solo puede leer un transponder a la vez en el área de su campo magnético.

Tal como se hizo anteriormente con los equipos, por medio del programa PIL, se probó que las antenas captaran los equipos obteniendo el ID de cada transponder contenido en ellos, si las antenas no captaban a alguno de los equipos que tenían los transponder, entonces eran cambiados de posición dentro del equipo.

Una vez que se terminaron de hacer la instalación y las pruebas, se puso a disposición del usuario final, se encontraron algunos problemas que a continuación damos a conocer y que fueron captados por los usuarios.

Caso 4.

El sistema se llega a trabar sin causa aparente.

El más importante, fue cuando en algún momento y por alguna causa el control maestro se trababa, es decir, dejaba de monitorear el sistema y no había otra solución que cerrar la aplicación o de reiniciar el sistema operativo (reiniciar Windows)

Al poco tiempo, uno de los usuarios del sistema reporto que su credencial no le permitía el acceso en un área pero en las otras tres si, además esto provoco que el sistema dejara de trabajar, esto mismo sucedió con un equipo al pasar, por una antena de protección de equipo, pero no sucedía lo mismo con las otras tres.

Observamos que los datos recuperados por la aplicación final SAPPE (y después confirmado por el programa PIL) tanto de la credencial como del equipo venia incompleta pues en el caso de la credencial el ID venia incompleto y en el del equipo, el CRC también venia incompleto.

Analizando las tramas de datos de los dos casos nos dimos cuenta que los números 11_{hex} y 13_{hex}, eran los ausentes, investigamos por que con estos números en particular se trababa la maquina.

Nos dimos cuenta que los números $11_{hex.}$ y 13_{hex} en código ASCII representan inicio de línea y avance de carro respectivamente, también que tanto los programas PIL y SAPPE así como el lector SERIES2000 los habíamos configurado para trabajar con un flujo de datos Xon / Xoff[6] que entre otros usos es el protocolo que se usa en las impresoras para su control.

De donde entendimos que al llegar los números ya mencionados el lenguaje con que fueron escritos los programas PIL y SAPPE los entendía como instrucciones que se debían de ejecutar, pero al no haber razón en el sistema para hacerlo, la computadora se

[6] Se trata de un protocolo para el control de flujo de datos entre las computadoras y otros dispositivos mediante una conexión serie asíncrona, son señales para detener o reanudar el flujo de datos, cuando lo que enviamos son números binarios, es posible que no se reconozcan, puesto que contienen caracteres codificados.

quedaba en espera de más datos para continuar y el sistema se paraba y para continuar, había que reiniciarlo.

La solución fue deshabilitar este tipo de control de flujo de datos de los programas y dejarlos sin control de flujo, después de estas acciones el sistema no se volvió a trabar.

Un segundo detalle que encontramos cuando el sistema se encontraba en funcionamiento, fue que para salir de las zonas protegidas por el sistema, a veces el lector no captaba las credencial, no era así para la entrada del personal.

Encontramos que como el lector de alta frecuencia tiene muy poca área de lectura, los transponders (credenciales) se deben poner muy cerca del lector, al entrar no había ningún problema, pues el contacto visual con ellos era evidente, sin embargo al salir no se tenía contacto visual con ellos, por los que se tuvo que poner una base a la altura de los lectores, para que las personas que salieran pudieran colocar sus credenciales y salir sin problemas.

CONCLUSIONES.

La realización de este proyecto fue una experiencia muy interesante, ya que nos involucramos desde el principio en el desarrollo de este.

El hecho de realizar juntas de trabajo, interrelacionarse con nuestras compañeras de computación que desarrollaron la aplicación para controlar el sistema , la búsqueda de dispositivos para la realización del proyecto, el tratar directamente con los proveedores de equipos o servicios, además de estar sujetos a un presupuesto para la realización del proyecto fue una oportunidad que no todos los recién egresados pueden presumir de tener.

Asimismo el tratar con las personas que intervinieron directa o indirectamente en la instalación final del sistema, (carpinteros, instaladores de tuberías, administrativos de la Facultad, proveedores de servicios) , incluso gente que tal vez nunca conoceremos personalmente, pues nuestro modo de comunicación fue por Internet o por teléfono al exterior del país y explicarles a todos ellos nuestro diseño, y escuchar (o leer) sus propuestas para la realización de los trabajos en base a su experiencia laboral nos dio una visión más clara de cómo realizar el proyecto.

En cuanto a la parte técnica, el haber desarrollado el proyecto en las instalaciones de la UNAM, y en particular en el CDM, nos facilito la realización del proyecto, pues disponíamos de equipo para la realización de este, no solo propios del área a la que pertenecemos, sino también el uso de taladros, limas, e incluso maquinas como una cortadora de lámina o tornos que en algún momento se usaron y que son de los laboratorios de la Facultad de Ingeniería.

Conocer y aprender a usar software como PROTEL para el diseño de los circuitos impresos de las tarjetas TAG-PC y del módulo de potencia. Los sistemas de desarrollo de los microcontroladores COP8, para el desarrollo del firmware de los microcontroladores que habrían de llevar las tarjetas TAG-PC. Lenguaje de programación VISUAL BASIC para el desarrollo del software de pruebas o dibujar en AUTOCAD, para el desarrollo de los planos. nos abrió un panorama más amplio de lo que es el diseño en computadora.

Por ultimo, el haber instalado nosotros mismos el cableado, de los registros, las antenas, los sensores, los actuadores, los transponder de los equipos, aprender en algunos casos a usar las herramientas, fue igualmente enriquecedor. Lo mismo que resolver los problemas que el sistema presento durante su implementación y en su funcionamiento final, no hubiera sido posible resolver sin la formación que nos brindo la Facultad de Ingeniería.

En suma como lo dijimos al principio, la experiencia fue única, pues lo concebimos, lo desarrollamos y hoy lo vemos hecho una realidad.

Con respecto al funcionamiento actual del sistema hemos observado lo siguiente:

Subsistema contra intrusos: A pesar de ser al más sencillo, lo consideramos como el más poderoso de los tres, pues cumple la función de ser disuasivo, ya que desde el primer momento en que ingresa un a persona ajena al edificio, se dará cuenta que para entrar a las zonas controladas, tendrá que hacer uso del interfono para anunciar su llegada, y

luego observar que la zona esta protegida por sensores que cuidan las instalaciones, esto puede desalentar un robo en potencia.

Hemos de reconocer que el sistema también es susceptible a falsas alarmas (que no se han presentado muchas) como el disparo de uno de los sensores de ruptura de cristal, por accidente.

Subsistema de control de acceso de personal: Se ha restringido en gran medida la entrada de persona ajenas a las instalaciones, incluso a gentes del mismo edificio que nada tienen que hacer en otra zonas de las instalaciones, sin embargo el sistema adolece de un pass-back eficaz, es decir que se registre realmente cuando una persona ha entrado o abandonado las instalaciones.

Subsistema de protección de equipo: El flujo de equipo de una área a otra, se ha hecho de una manera más controlada, pues se registra la entrada o salida del equipo de las áreas controladas, así como de quien es el responsable de ese equipo y en caso de presentarse un robo de este equipo protegido por el sistema, las alarmas se activaran, para dar aviso de que se ha presentado una anomalía.

Realización de trabajos en lo futuro:

El sistema siendo un prototipo, cuenta con algunas deficiencias que en el momento del diseño, no se habían visualizado, y por consecuencia, no se tomaron en cuenta, esto no quiere decir que pueda quedar así, el haberlo concebido como un sistema de arquitectura abierta, además de modular, nos permite el hacerle los ajuste necesarios como:

- Para evitar las falsas alarmas el software del sistema se podría modificar para que compruebe cuando ha habido una falsa alarma.

- Lograr que el sistema tenga un efectivo pass-back podrían ponerse sensores que comprueben cuando una persona esta entrando o saliendo con una credencial de acceso.

Aunque el sistema adolece de que en ciertas posiciones los transponders de protección de equipo no respondan, esto podría ser evitado, si buscamos configuraciones diferentes de antenas que logren crear un campo que lea los transponders en diferentes posiciones.

Pensamos que al ser este un primer sistema sin monitoreo (es decir no hay alguien que supervise el sistema vía remota, salvo cuando se activa una alarma sonora para avisar que se ha dado un evento a los vigilantes), se podrían crear una central vigilancia vía remota dentro de la Facultad de Ingeniería como primer paso, aprovechando la red de la universidad o el sistema telefónico, incluso un sistema de radio para poder monitorearlo, no solo a este sino a varios edificios que cuenten con un sistema de seguridad.

Por otro lado, desde el tiempo que comenzamos a diseñar el sistema, hasta el momento de escribir estas líneas, hemos visto que la industria de la seguridad electrónica en nuestro país ha crecido en forma exponencial, cada vez más en el mundo se están creando nuevos sistemas de seguridad, y nuevos sensores, pero muy pocos sistemas se han integrado en uno solo, como el nuestro.

El boom de la seguridad electrónica es cada vez más intenso, observamos como industrias extranjeras, vienen a ofrecer sus productos de seguridad, y muy pocos son las industrias mexicanas las que están intentando el desarrollo de sistemas de este tipo, esta industria es relativamente nueva, y por lo tanto apenas comienzan a agruparse las industrias para crear los estándares para los dispositivos que se están usando, o a certificar los sistemas. Nos encontramos en un buen momento para poder competir con las industrias,

Sensores para seguridad hay muchos en el mercado y muy variados (perimetrales, de presencia, de ruptura de cristal, CCTV, acceso de personal, de protección de equipo) sin embargo la oportunidad de ingresar a este mundo, no es en el desarrollo de sensores, actuadores o lectores, sino más bien en el desarrollo del control de estos dispositivos de protección, ya sea desarrollando tarjetas de control que sean capaces de integrar en uno solo, los sistemas de protección de equipo, contra intrusos, CCTV, etc.

Y también un software que nos permita controlar el sistema vía remota, dando aviso a una central de alarmas, a un teléfono ya sea convencional o celular, e incluso a una palm, las oportunidades son muchas, y creemos que hemos dado un primer paso para que otros compañeros sigan en el desarrollo de este sistema.

El sistema desarrollado dentro del CDM, como una alternativa de solución a algunos de los problemas de seguridad dentro de la Facultad de Ingeniería UNAM para cuidar su acervo material, puede ser el inicio de una serie de investigaciones para seguir desarrollando más sistemas de seguridad de este tipo a un bajo costo.

APENDICES

APÉNDICE A.

A. CONFIGURACION DEL MÓDULO SERIES 2000.

Para establecer comunicación con este módulo, conectamos el puerto de comunicación ST21 al host (en este caso la computadora) colocando el **S1.1** en OFF. Se configura el módulo series 2000 dependiendo de las necesidades del usuario usando el programa S2_Util, y una vez terminados, salvamos estos. Damos un reset al series módulo series 2000 (ver figura A.1) y colocamos el **S1.1** en posición ON

Para establecer la comunicación, del series 2000 se llevaron a cabo los siguientes pasos:

Se hizo una interfase con la computadora vía RS422 para una comunicación punto a punto (ver figura A.1). En este caso el jumper 2 (JP2) deberá de cerrarse y los jumpers JP4 y JP5 deberán de estar abiertos.

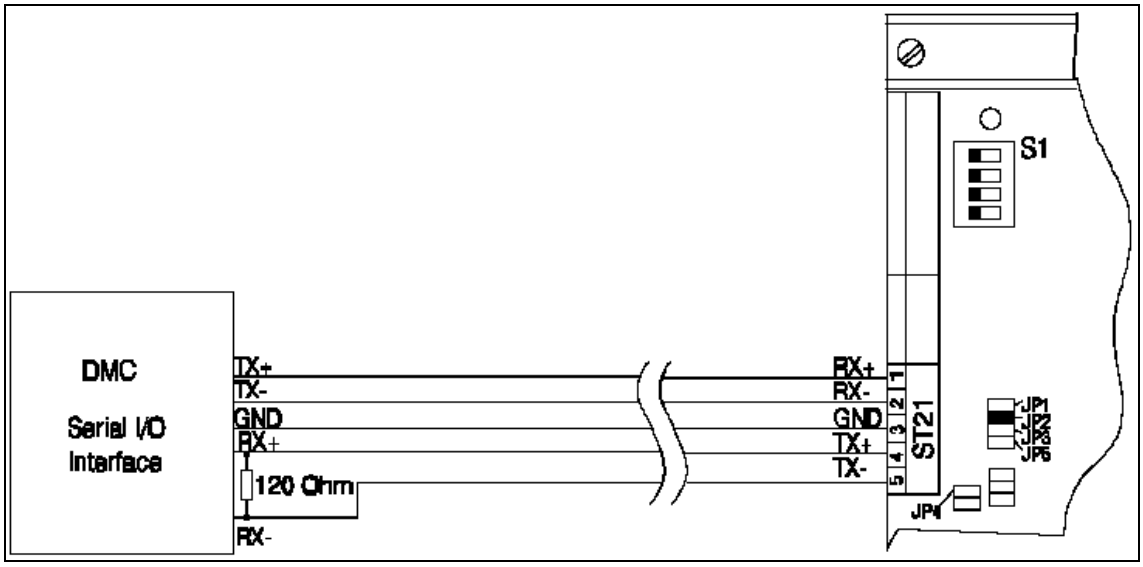


Figura A. 1: Conexiones de la Interface serial RS422.

Se enciende el módulo con el dip switch **S1.1** en OFF, luego se hace uso del programa S2_Util de Texas Instruments (que es un programa que se utiliza también para grabar los transponder que así lo requieran, como se vera mas adelante). Aquí podemos ver la pantalla de inicio del programa.

Figura A. 2: Ventana principal del programa S2_UTIL.

Elegimos el submenú **Main-Interfase-Port**.

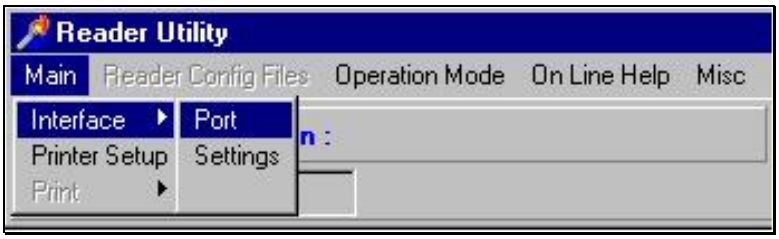


Figura A. 3: Submenú de comunicación.

Aparece la siguiente Ventana **Device Selection**, en donde elegimos el puerto de la computadora en la que hemos conectado el series 2000.

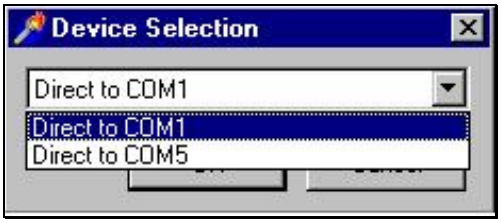


Figura A. 4: Selección del Puerto serial a utilizar.

A continuación se elige **Main-Interfase-Setting**, donde aparece la siguiente ventana.

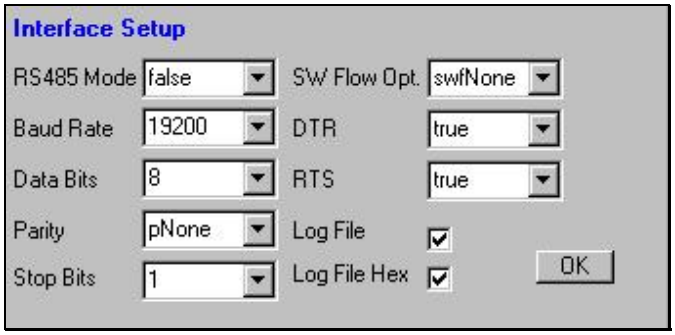


Figura A. 5: Ventana de configuración del puerto serial de la PC.

En esta pantalla **Interfase Setup** nosotros hicimos las siguientes elecciones de acuerdo a la tabla A.1:

RS485 Mode	False	**SW Flow Opt.**	SwfNone
Baud Rate	19200	**DTR**	False
Data Bits	8	**RTS**	False
Parity	Pnone	**Log File**	Habilitado
Stop Bits	1	**Log File Hex**	Habilitado

Tabla A. 1: Parámetros a configurar en el submenú Interface Setup.

Aquí vale la pena hacer algunas observaciones.

En la opción **RS 485 Mode.** elegimos **false,** que es el caso que nos ocupa ya que el módulo Series 2000 (S2000), para poder configurarlo se requiere tener una comunicación utilizando el estándar de comunicación RS422, al terminar de seleccionar las opciones se presiona el botón **OK.**

Se selecciona **Operation Mode_Config Mode**

Figura A. 6: Ventana de selección de configuración del Módulo.

y se abre la siguiente ventana de configuración.

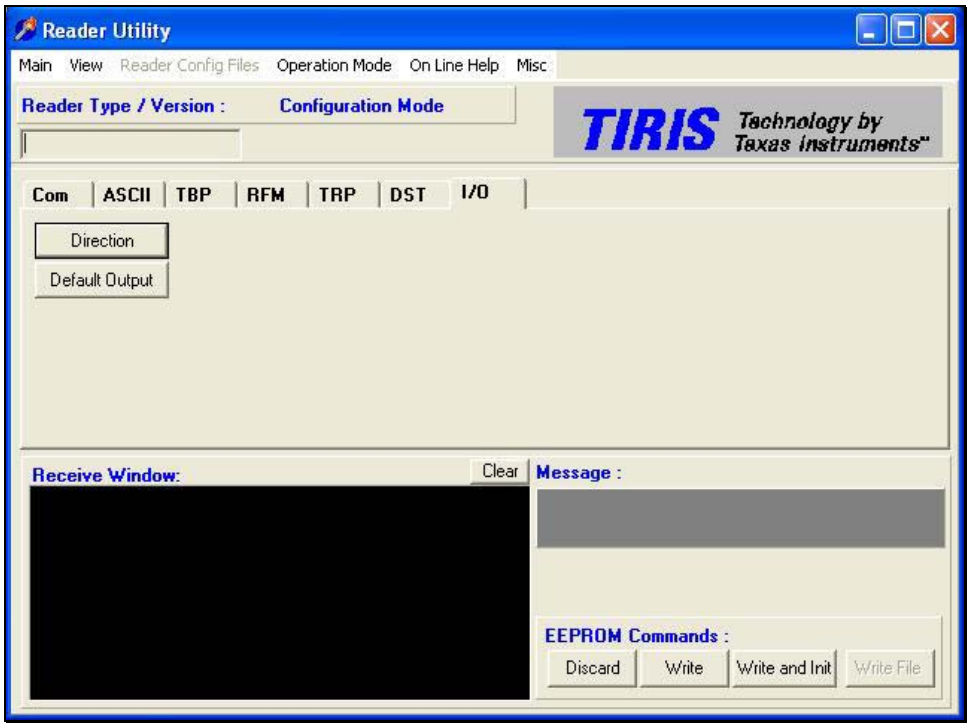


Figura A. 7: Ventana de Configuración.

Ya en esta ventana hacemos elegimos el submenú **View_Mode Expert.**

Figura A. 8: Selección de la opción modo experto.

Notamos que aparecen varias opciones, donde elegimos primero la opción **Com.,** seleccionamos la opción de **configuration**, en el apartado de **Reader** [*] **Interfase Configuration,** y hacemos los siguientes cambios *, mostrados en la tabla A.2:

[*] al terminar cada operación se debe de apretar **Send**

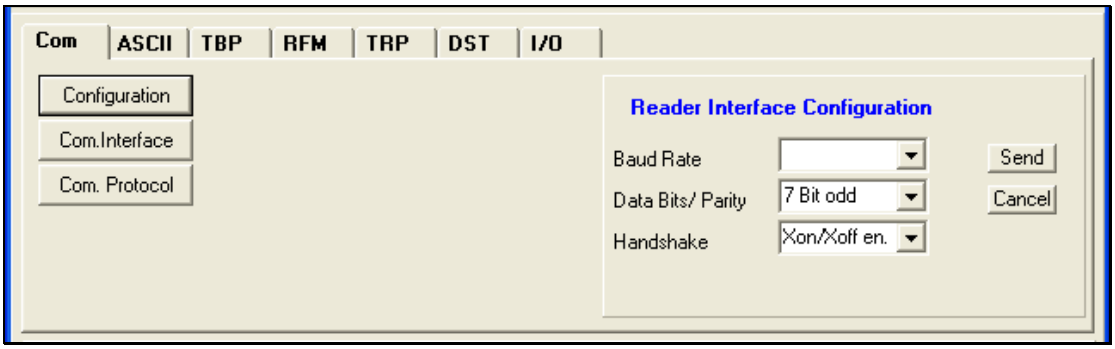


Figura A. 9: Ventana configuración de los parámetros de comunicación.

Baud Rate	19200
Data Bits / Parity	8 Bit None
Handshake	Xon / Xoff en

Tabla A. 2

En la siguiente ventana se elige **Com Interfase** apareciendo un apartado de **Communication Interfase,** en la que elegimos RS485 *.

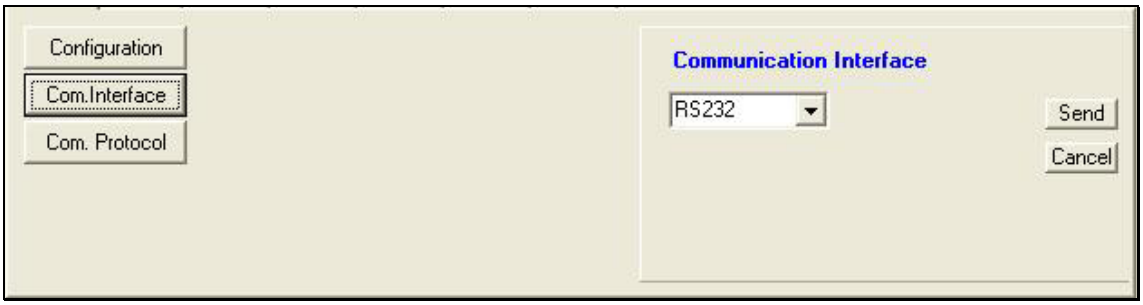


Figura A. 10: Selección de la interfaz de comunicación

A continuación apretamos el botón de **Com. Protocol** apareciendo un apartado de **Communication Protocol,** en la que elegimos TBP*.

Figura A. 11: Selección del protocolo de comunicación.

Después de haber hecho esos cambios, hacemos lo propio en la opción de **TBP,** en [*]esta ventana usamos el botón de **Reader ID** y en el apartado de **TBP Reader ID (dec)** ponemos el numero de reader con el que identificaremos a nuestro dispositivo, este numero debe de ser en decimal *.

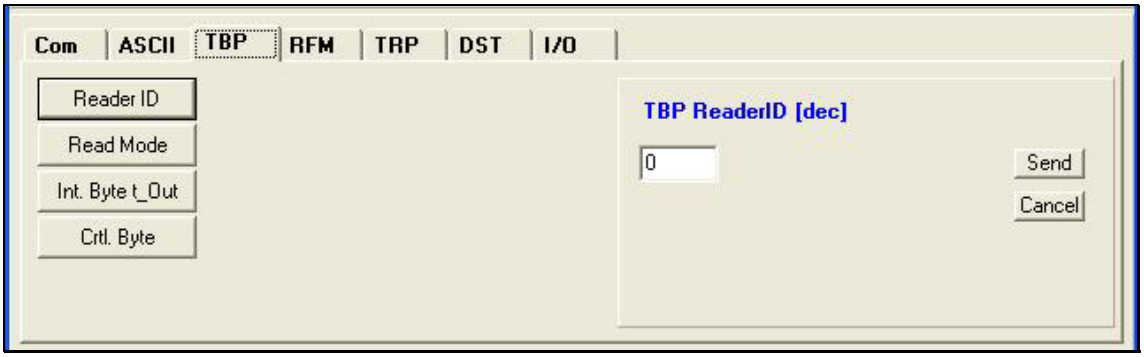


Figura A. 12: Configuración del lector.

El siguiente paso es elegir el botón de **Int. Byte t_Out,** en el apartado de **TBPInterByte TimeOut** elegimos la velocidad de transmición 19200*.

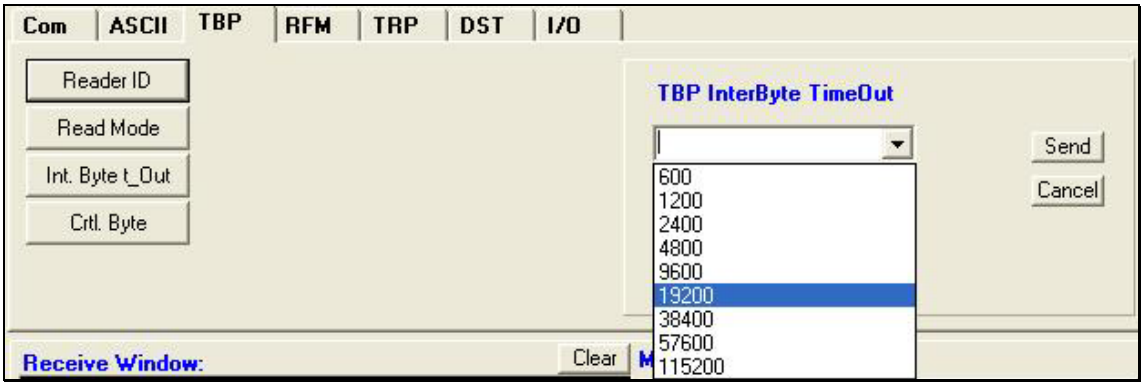


Figura A. 13: Selección de la velocidad de transmición.

[*] al terminar cada operación se debe de apretar **Send**

Después elegimos la opción de **Ctrl. Byte** aquí elegimos que tipo de detección de error queremos en nuestro sistema y en el apartado de **TBP Control Byte** elegimos XOR * .[*]

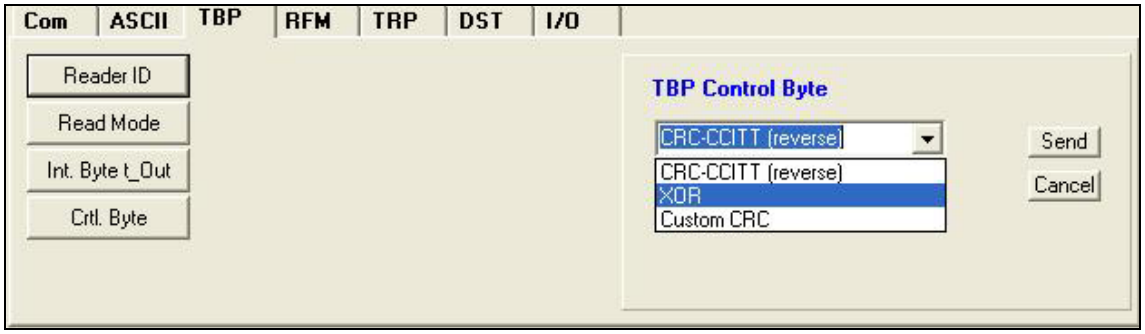


Figura A. 14: Selección del tipo de detección de errores.

NOTA:
El programa S2_Util esta diseñado para utilizar un código de errores del tipo CRC-CCITT por lo que, si se cambia este tipo de detección de errores la aplicación no reconocerá el lector S2000. Para nuestra aplicación se realizo un programa en Visual Basic 6 de Microsoft llamado **PIL** para registrar el envió y recepción de datos, el cual usa el código de error XOR.

En la opción de **I/O** elegimos como queremos que los puertos funcionen en nuestro sistema, para nuestro caso elegimos que todas quedaran como salidas (**I/O 0..3: Output I/O 4..7: Output)**. Estos puertos fueron configurados para controlar las líneas de selección del multiplexor que cada series 2000 tiene a su cargo.

[*] al terminar cada operación se debe de seleccionar **Send**

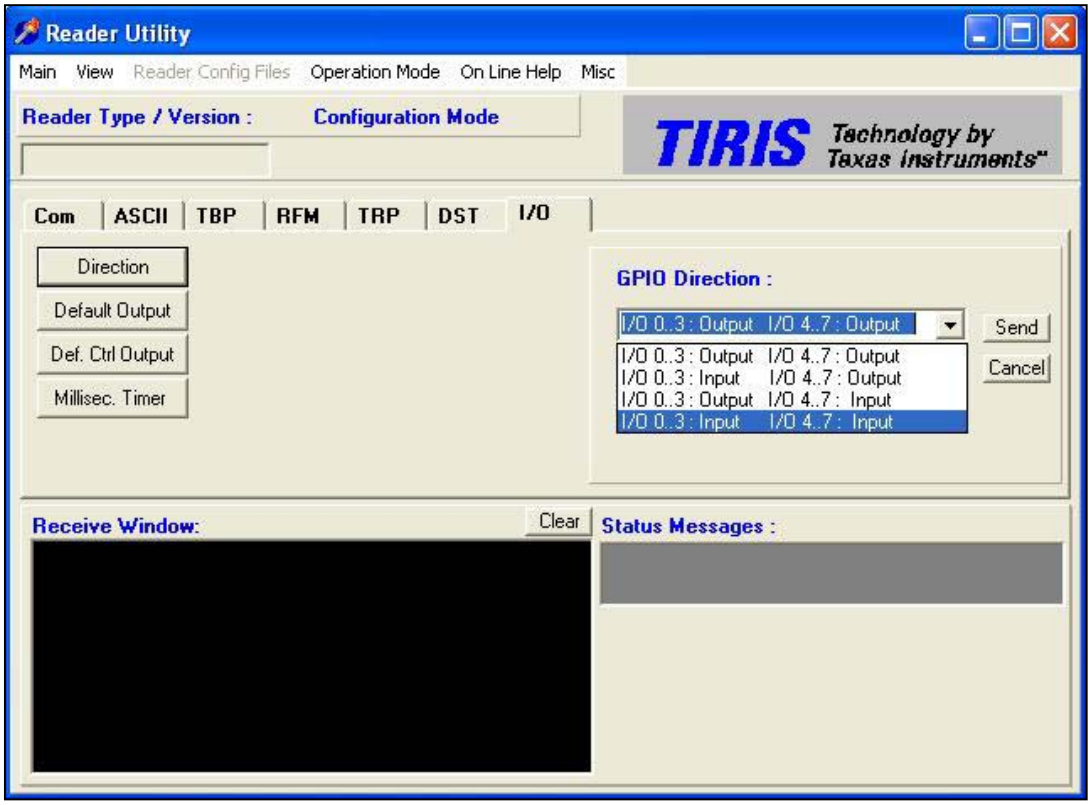


Figura A. 155: Configuración de las I/O del módulo.

Las opciones de **ASCII, RFM, TRP Y DSP** no se usan en esta aplicación.

Ya una vez que se termino la configuración se reinicia el Series 2000 y cambiamos el switch S1.1, en ON.

La operación del series 2000 se llevo a cabo por medio del programa **PIL.**

B. GRABACIÓN DE TRANSPONDER DE ACCESO DE PERSONAL.

En este apéndice, trataremos el procedimiento de escritura de ID en los transponders (credenciales) para el sistema de acceso de personal.

Para la escritura de estos transponders se hizo uso del programa S6 útil v1.02 de la compañía Texas Instruments.

Antes de abrir el programa, la computadora debe de tener conectado a su puerto serial el lector de acceso de personal, para la grabación de los transponders, una vez que se ha hecho esto, se procede a ejecutar el programa antes mencionado.

Al abrir el programa S6 útil, nos presenta la siguiente ventana de inicio.

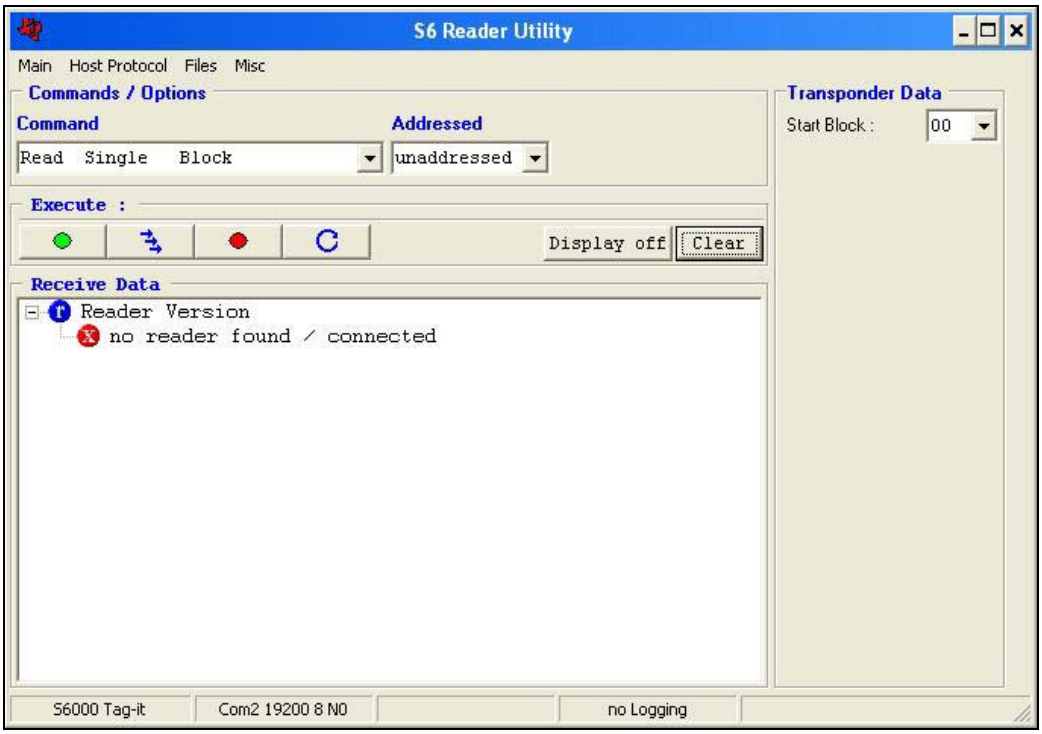


Figura B. 1: Ventana principal del programa S6_UTIL.

Elegimos **Main** y luego el submenú **Comunication**.

Figura B. 2: Submenú de comunicación.

Se presenta la siguiente ventana que contiene lo siguiente:

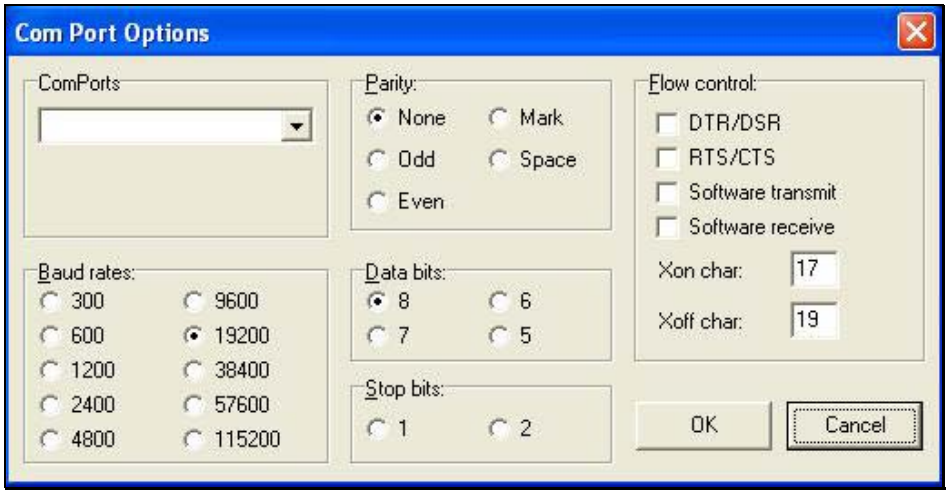


Figura B. 3: Ventana de configuración del puerto serial de la PC.

En esta ventana se elige los siguientes parámetros:

ComPorts	El puerto al cual este conectado el lector de alta frecuencia.
Baud rates	19200
Parity	None
Data Bits	8
Stop Bits	----------
Flow control	Xon char: 17 Xoff char: 19

Tabla B. 1: Parámetros a configurar en Com Port Options.

de acuerdo a la tabla B.1, lo demás puede dejarse en blanco, al terminar elija **OK**.

Ya una vez que se termino de configurar la comunicación de parte de la computadora, con el lector se procedió a la escritura de las credenciales (transponder).

En la siguiente ventana observamos que en **Command/Options.** Se despliega el menu **Command** y se pueden elegir 4 de las opciones que se indican a continuación:

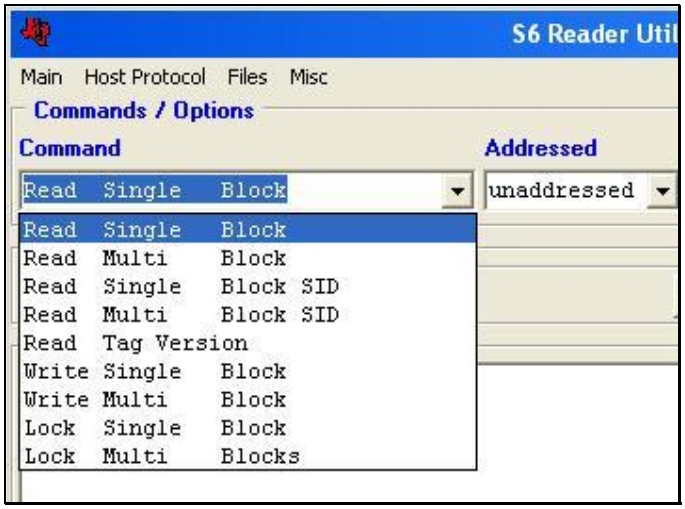


Figura B. 4: Ventana de selección de comandos.

En la ventana anterior se muestran las diferentes comandos que podemos utilizar con este equipo.

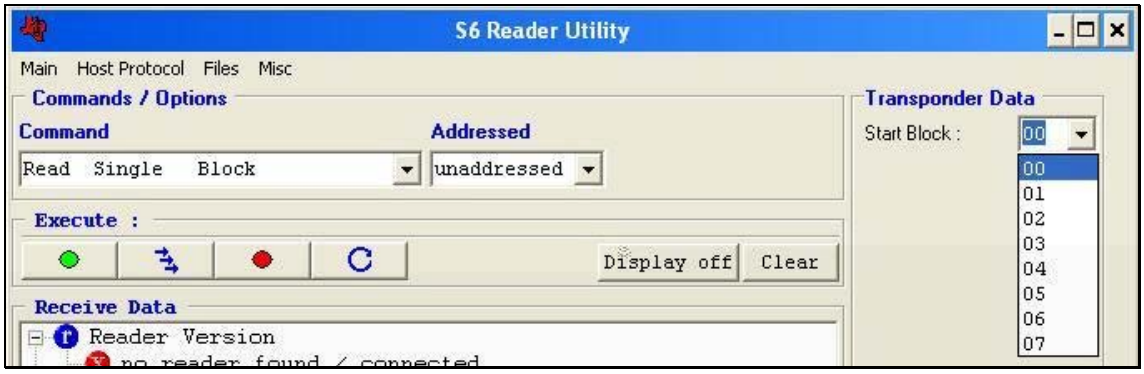


Figura B. 5: Selección del comando Read Single Block.

La opción **Read single Block**. No sir ve para poder leer un solo bloque de la memoria del tag, y podemos elegir que bloque queremos leer indicándole al programa en la ventana **Transponder Data,** el bloque de memoria que deseamos leer.

La opción **Write Single Block.** Sirve para escribir en un solo bloque de la memoria del tag, en el apartado de **Transponder Data,** en la parte de **Start Block,** se elige el bloque a escribir, en el mismo apartado, aparece otra opcion: **Write Data,** donde se escribe el dato en hexadecimal que se quiere guardar en el Tag.

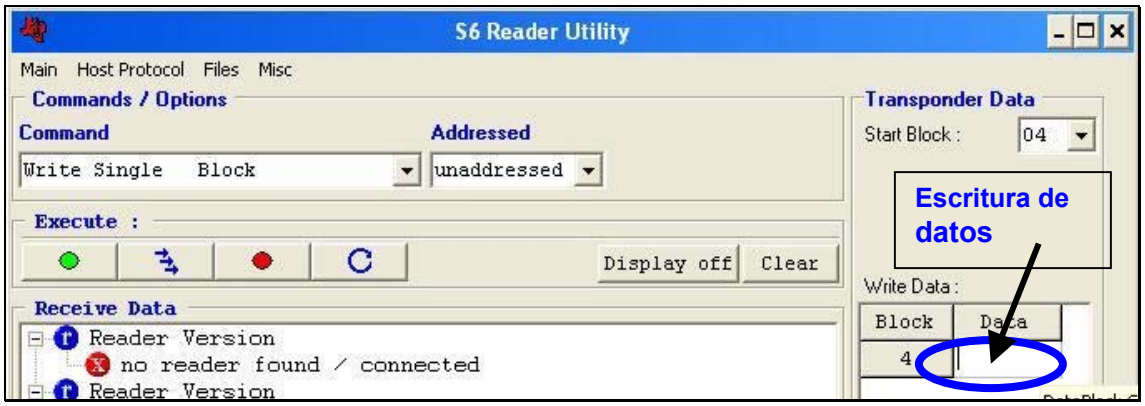


Figura B. 6: Selección del comando Write Single Block.

Al terminar cualquiera de las opciones siguientes, en la ventana **Execute** seleccionamos **Send Request** (circulo del lado izquierdo), para que se realice la operación.

Figura B. 7: Ventana de selección de inicio y paro del programa.

Para verificar con el programa que la operación de escribir el id en el transponder fue de manera satisfactoria, ahora escogemos la opcion de:

Read Single Block. En esta opción solo se lee un bloque de la memoria del tag, en el apartado de **Transponder Data** en **Start Block** desplegamos el menú y elegimos que bloque queremos leer*. La información se despliega en la ventana de **Recive Data,** donde veremos el id que ha sido grabado con anterioridad en la credencial (transponder).

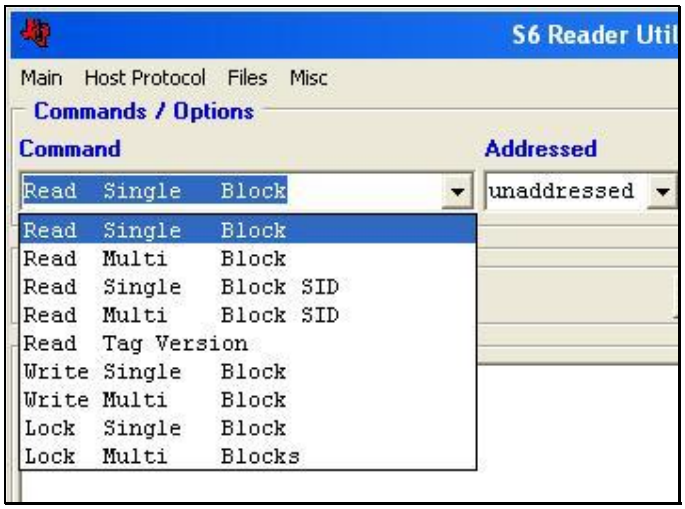


Figura B. 8: Selección del comando Read Single Block.

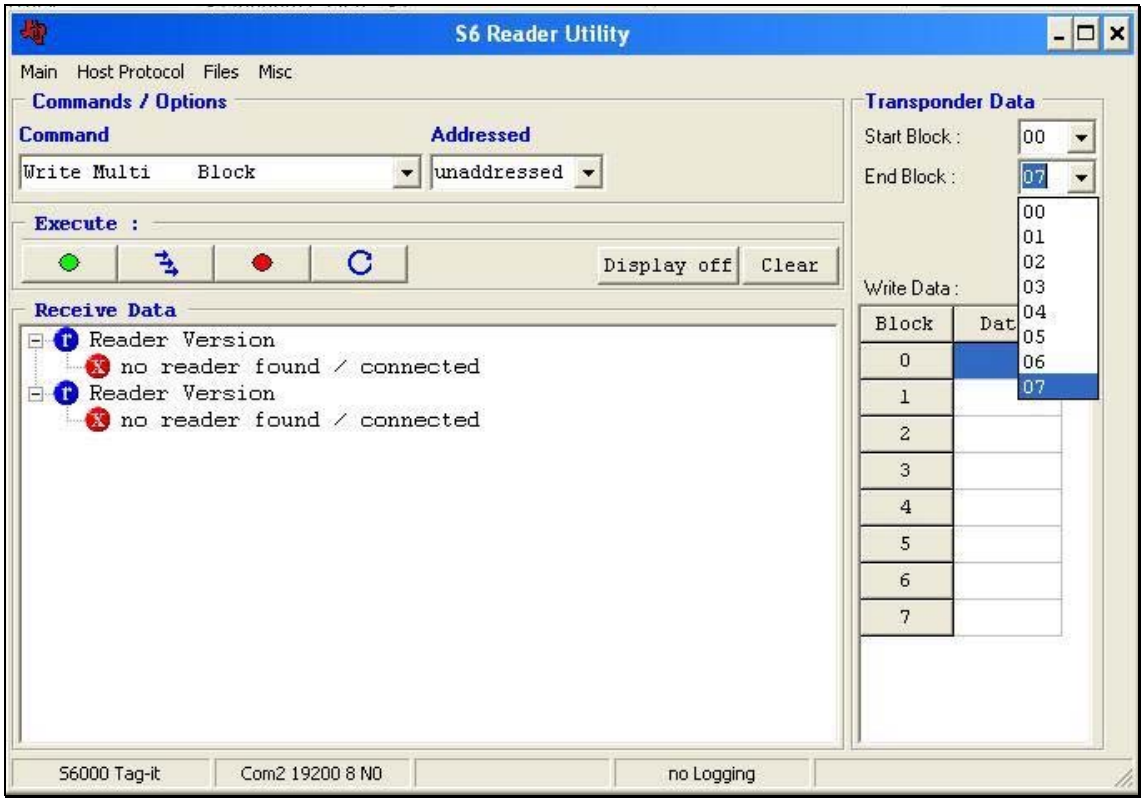


Figura B. 9: Selección del comando Write Single Block y selección de bloque.

habiendo terminado de grabar el id de los transponders, y comprobado que la información ha sido correctamente grabada, ya podemos trabajar con los transponder, ya sea con la ayuda del programa PIL o el programa administrador del sistema SAPPE.

C. GRABACIÓN DE TRANSPONDER DE PROTECCIÓN DE EQUIPO.

El procedimiento que se va a explicar a continuación trata de la forma de cómo se grabaron los transponders de lectura-escritura[1].

Para la grabación de los transponder, se hizo con un lector llamado **Microreader** de Texas Instruments, esto para comunicarnos con la computadora en comunicación serial RS-232, y no difiere mucho la forma de leer o escribir si lo hubiéramos hecho con un lector S2000, pero se debe de tomar en cuenta que dicho lector se comunica en RS-422 o RS-485.

El software que se utilizó para la grabación de los transponder fue el mismo que se uso en la configuración de los lectores del SERIES 2000.

Abrir el programa S2_Util de Texas Instruments encontramos la siguiente ventana:

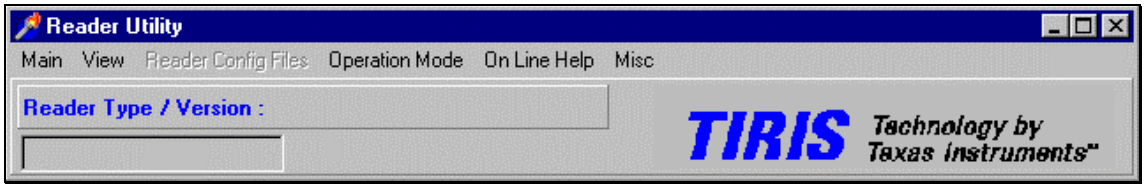


Figura C. 1: Ventana principal del programa S2_UTIL.

escoger en el menú: MAIN-INTERFACE-PORT y se elige el puerto que se va a utilizar.

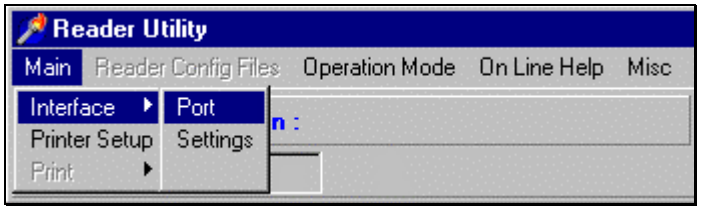


Figura C. 2: Submenú de comunicación.

[1] No todos los transponder que se usaron para la aplicación, fueron lectura y escritura, ya que también hubo de solo lectura, que como se podrá suponer, no se necesita ser escrito su id (código de identificación).

escoger en el menu: MAIN-INTERFACE-SETTING, donde saldrá la siguiente ventana:

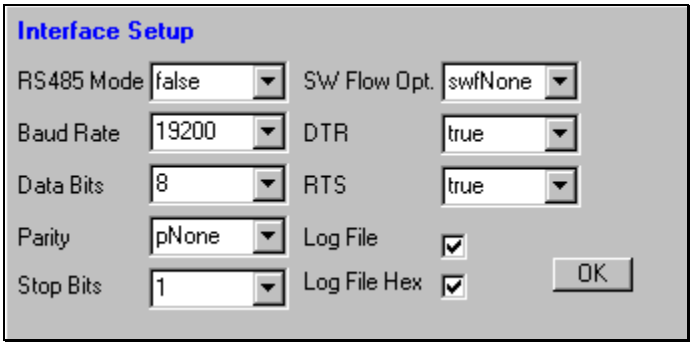


Figura C. 3: Ventana de configuración del puerto serial de la PC.

En esta ventana se introdujeron los datos de la siguiente tabla:

RS485 Mode	**False**	SW Flow Opt	**SwfNone**
Baud rate	**9600**	DTR	**False**
Data bits	**8**	RTS	**False**
Prity	**pNone**		
Stop Bits	**1**		

Tabla C. 1: Parámetros a configurar en el submenú Interface Setup.

Escoger la siguiente secuencia:

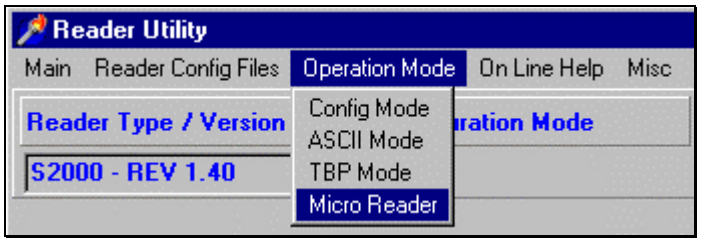


Figura C. 4: Ventana de selección de modo de operación.

Y aparecerá la siguiente ventana, este detecta el tipo de reader si hay alguno conectado y su versión,

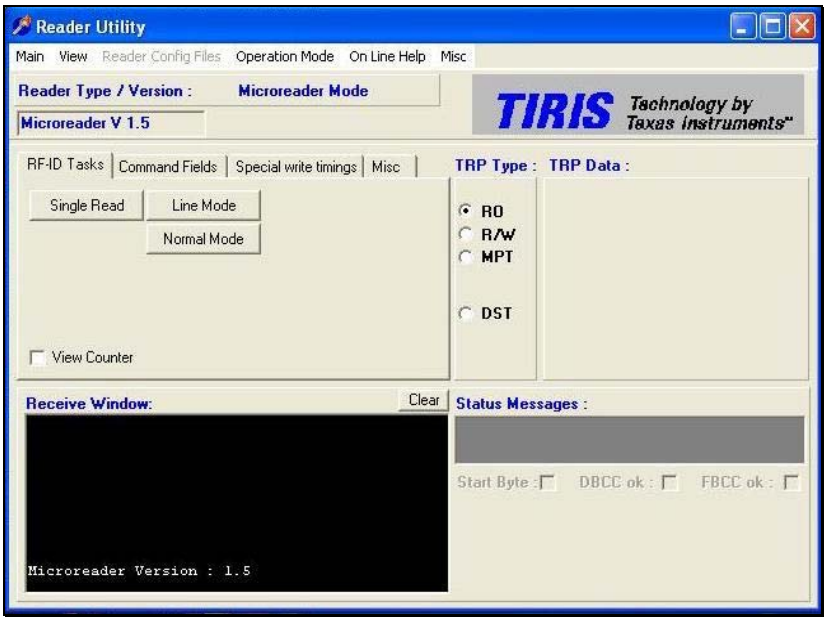


Figura C. 5: Ventana de configuración.

Al seleccionar la opción **Single Read**, y colocar un transponder en la antena, el programa detecta si el transponder es de solo lectura (RO), o de lectura y escritura R/W. En este caso en la ventana de **Recive Window** se ha detectado que se trata de un transponder R/W y su código, previamente había leído uno RO con su código, incluso en **Status Messages** también aparece que tipo de transponder es.

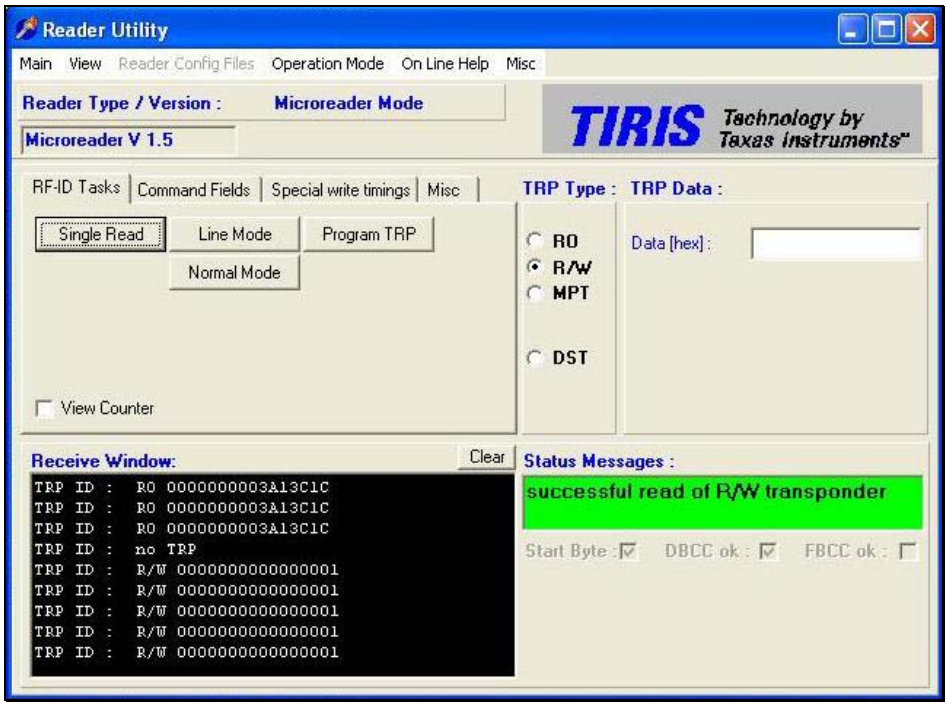


Figura C. 6: Lectura de transponders.

Para escribir en el transponder, se siguen los siguientes pasos:

- Se escoge en **TRP Type** la opción de **R/W**:
- En la ventanita de **Data hex.**, se escribe el código a ser grabado (Hexadecimal).
- Se coloca el transponder a ser escrito frente a la antena (para nuestro caso será del microreader).
- Se activa **Program TRP**
- En **Status Messages,** indica si ya se hizo la grabación del código.

Para comprobar que haya sido bien escrito el código, volvemos a seleccionar **Single Read,** entonces acercamos el transponder a la antena y verificamos que el código ID haya sido bien escrito.

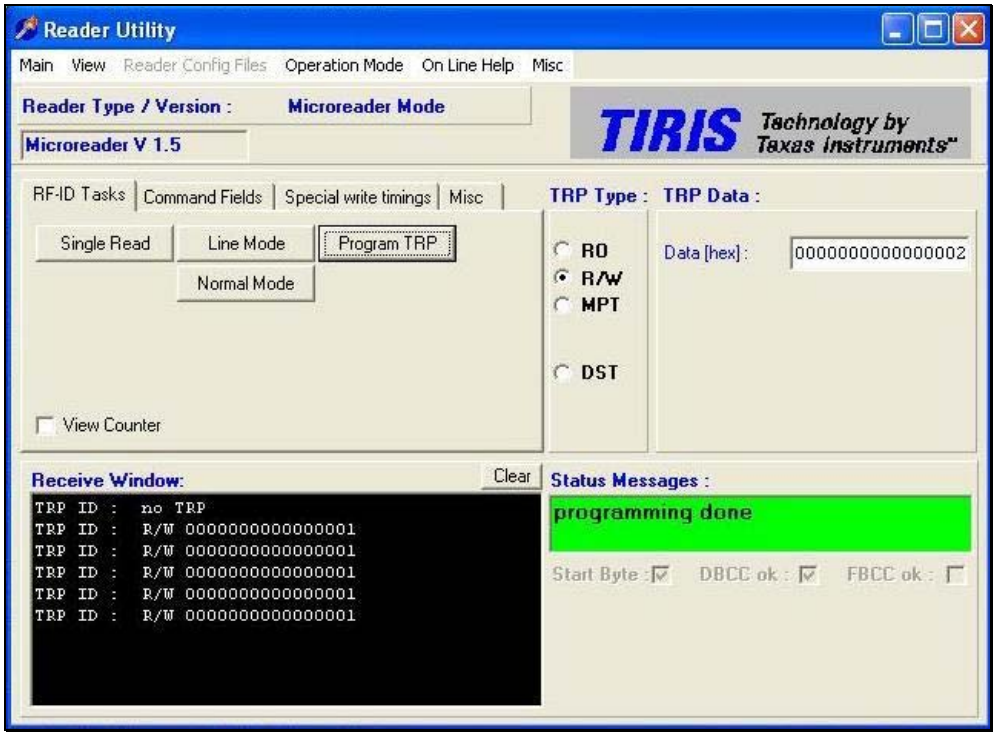


Figura C. 7: Grabación del código

y en el Status Messages se observa que el comando se ha efectuado, podemos volver a acercar el tag a la antena y observar que en la ventana Recive Window aparezca el código correcto, de ser así la operación de grabar un transponder ha sido hecha con éxito.

Nuestro transponder ya esta listo para ser utilizado en el sistema.

D. PROTOCOLOS DE COMUNICACIÓN DE LECTORES.

El objetivo de haber diseñado el firmware que se encuentra almacenado dentro de los microcontroladores COP fue liberar a la computadora de trabajos tales como la supervisión de entrada-salida, la recepción de señales de los sensores y la habilitación o deshabilitación de las actuadores.

Estas tareas las realiza el microcontrolador a través de instrucciones enviadas por la computadora y luego las ejecuta a través de la lógica almacenada, además de poder interactuar con la computadora y el lector de control de acceso de personal, interactuando con dos protocolos de comunicación distintos (Host Protocol S6000 y el Tiris Bus Protocol series 2000).

A continuación hacemos una breve descripción de los estos protocolos centrándonos en los aspectos que se usaron en nuestra aplicación.

HOST PROTOCOLO S6000[1]

El TAG-IT define la comunicación entre un sistema organizador que puede tratarse de un microcontrolador, una computadora personal o un PLC (para nuestro proyecto, se trata de la tarjeta TAG-PC[2] que contiene el COP) y el lector.

El Host protocolo tiene dos funciones principales:

- Manipular los datos de comunicación entre el TAG PC y el lector.
- Llevar las ordenes en comandos y responder a estos comandos de transponders.

Las principales características del Host Protocol son:

- Esta diseñado para comunicaciones punto a punto, half –duplex, con el TAG-PC actuando como estación primaria y el lector como la estación secundaria.
- Consiste, en muchos casos, de pares de ordenes / respuestas donde el TAG-PC espera una respuesta antes de continuar.

[1] Aquí solo se presenta un breve resumen del manual "Tag-it™ Redader System Series 6000, Host Protocol, Reference manual, TIRIS, Texas Instruments, No de parte 11-04-21-001" y solo de las funciones usadas en el proyecto.
[2] De aquí en adelante nos referiremos al host de el lector TAG-IT como la tarjeta TAG-PC.

- Es un protocolo orientado a contar bytes, esto ultimo quiere decir que en la cadena de datos enviada viene especificado, cuantos bytes vienen contenidos en ella. Permitiendo mayor flexibilidad en el control del lector.

Estructura de los comandos.

Todos los mensajes consisten de una cadena de datos, la estructura del mensaje es gobernada por el código de servicio, que esta contenido en el encabezado. Un mensaje del TAG-PC al lector es una orden, y un mensaje del lector al TAG-PC es una respuesta a ese mensaje, las ordenes solo pueden ser hechas por el TAG-PC.

Protocolo de la cadena de datos orden / respuesta.

La estructura de datos (ver tabla D.1), ese esencialmente la misma tanto para las ordenes (TAG-PC a lector) como las respuestas (lector a TAG-PC).

Bloque	Código de inicio (start code).	Largo de datos (Data Length).	Código de servicio (Service Code).	Control de banderas (Control Flag).	Mensaje (datos)	BCC
Posición de byte.	1	2,3	4	5	6 a (N-1) donde N <=4091	N+6, N+7

Tabla D.1: Estructura de la cadena de datos de la orden y la respuesta.

Definiciones de los bloques de la cadena de datos de orden y respuesta.

Start Code. Indica que comienza una cadena de datos (Start Frame Delimeter) con el valor $\mathbf{D5_{16}}$.

Data Length: Especifica el número de bytes de datos que siguen a este bloque. El rango es de 4 a 4095 bytes incluido el código de servicio (1 byte), el contol de banderas (1 byte) y el BCC (2 bytes).

Service code Este comando indica uno de los cuatro tipos de comando soportados.

01: Servicio de solo paso (no se uso en este proyecto).
02: Servicio simple.
03: Servicio compuesto (no se uso en este proyecto).
04: Servicio auxiliar.

Control de banderas[3].: Es usado en una cadena de orden, mientras que el estado de banderas es usado en la cadena de respuesta.

Para el control de banderas (ver tabla D.2), cuatro de los bits en este bloque son usados para especificar instrucciones al lector o información acerca de el mensaje. Estos bits están numerados 0 (lsb) al 7 (msb).

[3] Tanto para el control de banderas como de estado de bandera, estos estarán en ceros.

Bit	Función	Explicación
0	Reservada	
1	Bandera de espera	Si este es 1, el lector deberá esperar mas datos asociados con la orden. Si es 0, no hay mas datos asociados en la orden (mensaje único, o fin de mensaje).
2	Emulación de bandera	El bit de emulación (con un 1 lógico) permite al lector la emulación de una orden compleja por múltiples ordenes simples.
3	Auto repetición de bandera	Con un 1 lógico, le decimos al lector que repita automáticamente la orden enviada.
4	Bandera BCC	Con un 0 logico se le indica al lector que el mensaje usa un CRC-CCIT para BBC; mientras que con un 1 lógico usa un LRC para BBC.
5-7	Reservada.	

Tabla D. 2: Funciones de los bits del control de banderas.

Banderas de estado: Las banderas de estado son usadas en una cadena de respuestas.

Estas banderas describen el resultado de la orden y previa información acerca del mensaje (ver tabla D.3). Cinco de estos bits en este bloque son usados; estos bits, están numerados del 0 (lsb) a 7 (msb).

Bit	Función	Explicación
0	Bandera de excepción.	Si existe un 1, indica si la orden fue enviada con éxito al lector. En caso contrario, habrá un 1 lógico, el código de estado estará contenido en el primer byte del mensaje (ver tabla).
1	Bandera de espera	La bandera de extensión de datos informa al lector si mas datos siguen. Si es 1, el lector deberá esperar mas cadenas hasta recibir una cadena de datos con el bit de extensión de datos en 0 lógico.
2	Emulación de bandera	Con un 1 lógico indica al lector si el transponder completo la orden, usando un comando compuesto para la emulación de un comando complejo.
3	Auto repetición de bandera	Con un 0 lógico, le indica al lector que la orden la ejecuto una sola vez, mientras que con un 0 lógico, repite continuamente la orden enviada.
4	Bandera BCC	Indica con que método checo que la información llego correcta. Con un 0 lógico se le indica al lector si el mensaje usa un CRC-CCIT para BBC; mientras que con un 1 lógico usa un LRC para BBC.
5-7	Reservada.	

Tabla D. 3: Funciones de los bits del estado de banderas.

Mensaje: Esta parte de la orden trae el mensaje para el transponder. El formato depende del tipo de comando especificado en le byte de código de servicio.

BCC: Este bloque contiene el CRC (o LRC) de todos los datos precedentes, excluyendo el start block. El bit de control de banderas indica si CRC (Bit=0) o LRC (Bit=1) es usado. El BCC esta basado en el mensaje que lo acompaña. Si algún otro valor del BBC es leído, esto indica que la información esta corrompida o no es lo que se esperaba.

Código de error	Definición.
00_{16}	reservado
01_{16}	Datos de la orden corrompida, no ejecutada.
02_{16}	Aplicación no soportada.
03_{16}	Error en el formato de datos, orden abortada.
04_{16}	Modo continuo no disponible en esta orden.
05_{16} al $0E_{16}$	Reservado
$0F_{16}$	Error de sistema indefinido, orden abortada.

Tabla D. 4:estado de los códigos de excepción.

Estructura del mensaje.

Un mensaje comienza a partir del bit 6, es definido como un dato que es enviado o recibido. Este es encapsulado por una cadena que consiste de un encabezado y un BBC.

Solo el TAG-PC puede enviar un mensaje de orden al transponder, el formato depende del tipo de comando, que es especificado por el código de servicio, (Service Code)

Los tipos de ordenes son definidos como:

01: Servicio de solo paso (no se uso en este proyecto).
02: Servicio único.
03: Servicio compuesto (no se uso en este proyecto).
04: Servicio auxiliar.

Aquí solo haremos mención de los que se usaron en el proyecto, para mas detalle de los restantes, refiérase a la bibliografía.

Mensaje único (single message).

Códigos de servicio y error. este comando indica uno de los cuatro tipos de comando soportados.

01: Servicio de solo paso (no se uso en este proyecto).
02: Servicio único.
03: Servicio compuesto (no se uso en este proyecto).
04: Servicio auxiliar.

Solo haremos mención de los servicios ocupados en el proyecto.

02 Servicio único: Al recibir una orden de servicio único el lector analiza y verifica los formatos, y envía un único comando al transponder.

Cuando el lector recibe una respuesta la analiza y verifica los formatos, y envía una respuesta única al TAG-PC.

Ejemplos de comandos de servicio son:

- Lectura de bloque.
- Escritura de bloque.
- Cerrar bloque.

04 Servicio auxiliar: Al recibir una orden de servicio auxiliar el lector analiza y verifica los formatos, entonces ejecuta la orden localmente. No hay comandos a enviar al transponder. La orden de servicio auxiliar puede ser usado para bajar una nueva versión de el software del lector, o poner parámetros de comunicación y operación.

Para nuestro sistema se consideraron los comandos de lectura de un bloque, reinicio del lector (ver la tabla D.5)

Comando	Código de servicio		Código de comando
	Único	Auxiliar	
Lectura de bloque	02_{16}		01_{16}
Reinicio de lector		04_{16}	10_{16}

Tabla D. 5: Lista de códigos para las acciones consideradas en el firmware.

PROTOCOLO SERIES2000.

Lectura de bloque: leer el contenido de un único bloque de datos del transponder ver; la cadena de datos que se uso para llevar a cabo esta acción dentro del firmware en el TAG-PC fue:

D5 00 08 02 00 01 00 00 01 B0 $B9_{16}$ (tabla D.6)

.Nombre	No. De bytes	Descripción.	Valor
Start	1	Comienzo de cadena de datos	$D5_{16}$
Longitud de datos	2	8 bytes siguen a este bloque	00 08_{16}
Código de servicio	1	Único	02_{16}
Control de banderas[4]	1	More bit= no mas datos Bit de emulación = apagado Bit de auto repetición=apagado Bit BCC=CRC usado	00_{16}
Código de comando	1	Lectura de bloque	01_{16}
Formato de código	1	No direccionado	00_{16}
Sincronización	1	No sincronizado	00_{16}
Numero de bloque	1	Bloque 2	01_{16}
BCC	2	CRC calculado previamente	B0 $B9_{16}$

Tabla D. 6: Descripción de cada uno de los bytes del formato.

Reinicio del lector: este mensaje causa el reinicio del lector por software. Cualquier comando que se este ejecutando en ese momento, será completado, incluyendo la respuesta al TAG-PC.

Después de eso el lector enviara la respuesta de reinicio al TAG-PC, e inmediatamente después ejecutara el reinicio por software.

D5 00 05 04 00 10 9C 47_{16} (tabla D.7)

Nombre	No. De bytes	Descripción.	Valor
Start	1	Comienzo de cadena de datos	$D5_{16}$
Longitud de datos	2	5 bytes siguen a este bloque	00 05_{16}
Código de servicio	1	Servicio	04_{16}
Control de banderas	1	More bit= no mas datos Bit de emulación = apagado Bit de auto repetición=apagado Bit BCC=CRC usado	00_{16}
Código de comando	1	Reinicio del lector	10_{16}
BCC	2	CRC calculado previamente	9C 47_{16}

Tabla D. 7: Descripción de cada uno de los bytes del formato.

Versión del lector: el lector responde enviando la versión del firmware que esta corriendo en el lector. Este no es un dato asociado con la orden.

D5 00 05 04 00 11 8C 66_{16} (tabla D.8)

Nombre	No. De bytes	Descripción.	Valor
Start	1	Comienzo de cadena de datos	$D5_{16}$
Longitud de datos	2	5 bytes siguen a este bloque	00 05_{16}
Código de servicio	1	auxiliar	04_{16}
Control de banderas	1	More bit= no mas datos Bit de emulación = apagado Bit de auto repetición=apagado Bit BCC=CRC usado	00_{16}
Código de comando	1	Versión del lector	11_{16}
BCC	2	CRC calculado previamente	8C 66_{16}

Tabla D. 8: Descripción de cada uno de los bytes del formato.

Respuesta a los comandos enviados del TAG-PC al lector S6000 cuando la transmisión fue un éxito, son los siguientes:

Respuesta al mensaje de lectura de un bloque:

D5 00 0D 02 00 01 00 00 01 00 XX XX XX XX 78 $E6_{16}$ (tabla D.9)

Nombre	No. De bytes	Descripción.	Valor
Start	1	Comienzo de cadena de datos	$D5_{16}$
Longitud de datos	2	13 bytes siguen a este bloque	00 $0D_{16}$
Código de servicio	1	Único	02_{16}
Estado de banderas	1	No excepción	00_{16}
Código de comando	1	Lectura de bloque	01_{16}
Formato de código	1	Sin dirección y sin error	00_{16}
Sincronización	1	No sincronizado	00_{16}
Numero de bloque	1	Bloque 2	01_{16}
Estado de cerradura	1	Abierto	00
Datos del bloque	4		XX XX XX XX_{16}
BCC	2	CRC calculado previamente	78 $E6_{16}$

Tabla D. 9: Descripción de cada uno de los bytes del formato.

Respuesta a un comando de reinicio de un lector enviado correctamente:

D5 00 05 04 00 10 9C 47_{16} (Tabla D.10)

Nombre	No. De bytes	Descripción.	Valor
Start	1	Comienzo de cadena de datos	$D5_{16}$
Longitud de datos	2	5 bytes siguen a este bloque	00 05_{16}
Código de servicio	1	Servicio	04_{16}
Control de banderas	1	No excepción.	00_{16}
Código de comando	1	Reinicio del lector	10_{16}
BCC	2	CRC calculado previamente	9C 47_{16}

Tabla D. 10: Descripción de cada uno de los bytes del formato.

Respuesta a un comando de versión del lector enviado correctamente:

D5 00 09 04 00 11 02 00 00 00 3C 21_{16} (Tabla D.12)

Nombre	No. De bytes	Descripción.	Valor
Start	1	Comienzo de cadena de datos	$D5_{16}$
Longitud de datos	2	9 bytes siguen a este bloque	00 09_{16}
Código de servicio	1	auxiliar	04_{16}
Control de banderas	1	No excepción	00_{16}
Código de comando	1	Versión del lector	11_{16}
Versión del firmware	3	Versión X.XX.XX	XX XX XX
Tipo de firmware	1	Estándar	00
BCC	2	CRC calculado previamente	3C 21_{16}

Tabla D. 11: Descripción de cada uno de los bytes del formato.

TIRIS BUS PROTOCOL SERIES 2000:

El TIRIS BUS PROTOCOL define el formato, longitud y significado de mensajes (ver tabla D.12) intercambiados entre el Esclavo Series2000 y un sistema organizador (PC). El protocolo ha sido diseñado para permitir la comunicación eficaz entre un maestro y varios esclavos[5]. En esta forma de conexión el bus de datos es ocupado por un elemento a la vez, donde el maestro lleva el control al indicar quien debe contestar aun requerimiento de este ultimo, y al ser la demás unidades esclavas se evita que se presente la colisión de datos.

Start Mark	Destination address	Source Address	Message Code	Data lengt	Data Field	CRC1	CRC2	End mark
Byte 0	Byte 1	Byte 2	Byte 3	Byte 4	Byte5 ... Byte N+4	Byte N + 5	Byte N+6	Byte N+7

Tabla D. 12: función de cada uno de los bytes del formato.

Lo dicho anteriormente, nos permite que exista una comunicación no solo entre los lectores S2000, sino también con los TAG-PC que fungen como unidades esclavas, a continuación haremos referencia de este protocolo y como lo usamos en el firmware. Para mayores referencias de este manual dirigirse a la bibliografía.

[5] Para nuestro proyecto, dicha comunicación se logra en un estándar RS485.

Todos los datos se transfieren por mensajes. Sin importar la dirección todos tienen el mismo formato (ver tabla D.13).

Nombre de bytes.	Byte	Función
Start Mark (01 Hex)	0	Indica el comienzo del Comando. Esta representado por el carácter ASCII SOH (Started of Header, 01 Hex)
Dest-address, Destino del Comando	1	Dicho byte indica el destino del Comando. El valor binario corresponde al ID de la unidad (sea esclavo o maestro. El Id de la unidad tiene un valor de $0x00_{16}$ a $0xFE_{16}$ (0 a 254_{10}).
Source-Address, identificador (ID) del origen de los datos.	2	Este byte indica la fuente del mensaje. El valor binario corresponde con el ID de la unidad que envío el mensaje.
Message Code, Código del Comando a ejecutar.	3	El byte define el significado del mensaje. Dependiendo de la dirección, el código puede ser de Maestro a esclavo o viceversa.
Data-length, Longitud en Bytes del mensaje.	4	Indica la longitud del mensaje : Un 0_{16} (0_{10}), indica que no hay mensaje y después de este valor vienen todos los demás bytes. El valor máximo de este dato es de $0xFF_{16}$
Data-field. Longitud del mensaje.	Data field 5... Data field N	La longitud de los bytes de este mensaje, están indicados en Data length
CRC. (2 Bytes)	4+Data Field.	Para verificar el mensaje existen dos métodos: el CRC–CCITT y el LRC que es un XOR con los datos del mensaje, excluyendo SOH, EOT y los bytes del CRC. El segundo Byte del cálculo de error es un complemento a uno del primer byte de cálculo de error. En la aplicación utilizamos el LRC (XOR).
End mark, (EOT, 04 Hex) Fin del Comando.	4+Data Field+2 Bytes.	Indica que el Comando o la Respuesta termina.

Tabla D. 13: Descripción de cada uno de los bytes del formato.

De la tabla D10 observamos implícitamente que Message Code puede contener un **Command-Message-Code** (de Maestro a esclavo) o una **Response-Message-Code** (de Esclavo a Maestro).

A los mensajes enviados por el control Maestro se les denomina Comandos (command) y a los mensajes retornados por los esclavos se les denomina Respuestas (response).

Command-Message-Code (de Maestro a esclavo): En el firmware de la tarjeta TAG-PC, se usaron cuatro tipos de tipos de acciones a realizar (comandos), que fueron consideradas para cualquiera de los módulos TAG (ver tabla D.14), estos comandos tienen por función principal el control de los sistemas de control de acceso de personal, de los sensores y actuadores.

Comando	Código	Acción
Reset_reader	00_{16}	La computadora manda a reiniciar el lector TAG
Read_bolck	11_{16}	Lectura de transponder por parte del lector TAG
Read_input	33_{16}	Se lee la información enviada por los sensores que se encuentran en el área de protección.
Write_output	44_{16}	Se manda a activar o desactivar los actuadores que se encuentran dentro del área.

Tabla D. 14: Comandos enviados de la computadora al TAG-PC.

Data Field (de maestro a esclavo): En estos bytes se indica el mensaje enviado al TAG-PC, en este caso, solo cuando se manda a activar o desactivar un actuador (write_output= 44_{16}), se envía un mensaje de dos bytes en los que le indicamos, el numero del actuador y la acción a realizar (activar / desactivar).

Response-Message-Code: Especifica la respuesta del TG-PC a la computadora, dependiendo de command message code es la respuesta (ver tabla D.12).

Código de mensaje	Código de respuesta	Mensaje
00		
11	01	Dependiendo de si existe o no tag, es el mensaje.
33	33	Dependiendo del estado de los sensores el mensaje varia de 00 a FF.
44	FF	Indica que la operación ha sido realizada.

Tabla D. 15: Descripción de los códigos de mensajes y respuestas, correspondientes.

Ejemplos:

Comando de computadora (Maestro a esclavo)

01 04 00 11 00 EA 15 04 Lectura de transponder (Tabla D.16):

campo	bytes	Funcion	Descripción
01	1	Start mark	Comienzo de trama
04	1	Dest-address	unidad esclava, TAG-PC numero 4
00	1	Source address	unidad maestra
11	1	Message code	petición de lectura de transponder
00	1	Data Length	no hay mensaje a enviar
EA 15	2	LRC	Codigo de verificación de error
04	1	End Mark	Fin de la trama.

Tabla D. 16: Descripción de cada uno de los bytes del formato.

Respuesta de TAG-PC (no hay transponder presente):

01 00 04 01 01 00 FB 04 04_{16} (tabla D.17).

Campo	Bytes	funcion	Descripción
01	1	Start mark	Comienzo de trama
00	1	Dest-address	unidad maestra, computadora.
04	1	Source address	unidad esclava TAG-PC 04
01	1	Message code	Respuesta de lectura de transponder
01	1	Data Length	1 byte de mensaje a enviar
00	1	Data field	No hay transponder presente.
EA 15	2	LRC	Codigo de verificación de error
04	1	End Mark	Fin de la trama.

Tabla D. 17: Descripción de cada uno de los bytes del formato.

Respuesta de TAG-PC (Lectura de transponder presente):

01 00 04 01 04 00 00 00 06 F8 07 04_{16} (tabla D.18)

Campo	bytes	funcion	Descripción
01	1	Start mark	Comienzo de trama
00	1	Dest-address	unidad maestra, computadora.
04	1	Source address	unidad esclava TAG-PC 04
01	1	Message code	Respuesta de lectura de transponder
04	1	Data Length	1 byte de mensaje a enviar
00 00 00 06	4	Data field	Lectura de transponder ID: 00 00 00 06
F8 07	2	LRC	Codigo de verificación de error
04	1	End Mark	Fin de la trama.

Tabla D. 18: Descripción de cada uno de los bytes del formato.

Comando de computadora estado de los sensores:

01 04 00 33 00 C8 37 04 (tabla D.19)

Campo	bytes	funcion	Descripción
01	1	Start mark	Comienzo de trama
04	1	Dest-address	unidad esclava, TAG-PC numero 4
00	1	Source address	unidad maestra
33	1	Message code	petición de lectura de sensores.
00	1	Data Length	no hay mensaje a enviar
C8 37	2	LRC	Codigo de verificación de error
04	1	End Mark	Fin de la trama.

Tabla D. 19: Descripción de cada uno de los bytes del formato.

Respuesta de TGA-PC.

01 00 04 33 01 FF 36 C9 04_{16} (tabla D.20)

Campo	Bytes	funcion	Descripción
01	1	Start mark	Comienzo de trama
00	1	Dest-address	unidad maestra, computadora.
04	1	Source address	unidad esclava TAG-PC 04
33	1	Message code	Respuesta de lectura de transponder
01	1	Data Length	1 byte de mensaje a enviar
FF	1	Data field	Mensaje enviado del TAG PC.
36 C9	2	LRC	Codigo de verificación de error
04	1	End Mark	Fin de la trama.

Tabla D. 20: Descripción de cada uno de los bytes del formato.

Comando de computadora (activacion / desactivacion de actuadores).

01 04 00 44 02 01 00 xx xx 04_{16} (tabla D.21)

Campo	Bytes	funcion	Descripción
01	1	Start mark	Comienzo de trama
04	1	Dest-address	Dirección de unidad maestra, computadora.
00	1	Source address	Direccion de unidad esclava TAG-PC 04
44	1	Message code	Comando de activacion / desactivacion de actuadores.
02	1	Data Length	1 byte de mensaje a enviar
01 00	1	Data field	Actuador 01 , desactivalo (00)
XX XX	2	LRC	Codigo de verificación de error
04	1	End Mark	Fin de la trama.

Tabla D. 21: Descripción de cada uno de los bytes del formato.

Comando de computadora estado de los sensores:

01 00 04 FF 00 xx xx 04_{16} (Tabla D.22)

Campo	bytes	funcion	Descripción
01	1	Start mark	Comienzo de trama
00	1	Dest-address	Dirección de unidad maestra
04	1	Source address	Dirección de unidad esclava, TAG-PC numero 4
FF	1	Message code	El comando fue ejecutado satisfactoriamente.
00	1	Data Length	no hay mensaje a enviar
XX XX	2	LRC	Codigo de verificación de error
04	1	End Mark	Fin de la trama.

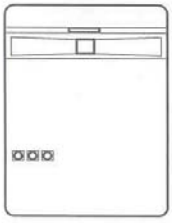
Tabla D. 22: Descripción de cada uno de los bytes del formato.

APÉNDICE E.

E. HOJAS DE ESPECIFICACIONES.

SENSOR RUPTURA DE CRISTAL.

IntelliSense™



FlexGuard™

Dual Technology Glass-Break Detector
INSTALLATION INSTRUCTIONS

Models
FG-715 15' range
FG-730 30' range

The FG-715 and FG-730 from IntelliSense are **dual technology** glass-break detectors that use flex detection and audio discrimination to detect breaking glass.

The flex and audio technologies are sensitive to different frequencies. The flex technology is sensitive to ultra low frequencies, the type generated by a blow to a glass window. The audio technology detects the frequency of breaking glass.

The audio technology remains off until the flex technology detects a blow to the glass. For an alarm condition to occur, the audio must detect the frequency of breaking glass within a defined time-window *after* the flex detects a blow to the glass. Because both technologies must detect and verify glass breakage, **false alarms are virtually eliminated.**

FEATURES

- Dual flex/audio technology
- Low 10 - 14 VDC operation
- Low 25 mA at 12 VDC current draw
- No adjustment on audio
- Adjustment on flex detection to fit characteristics of each location (FG-730 only)
- Alarm memory
- Indicator LEDs
- Energized form C alarm relay
- Circuit protection
- Cover tamper switch
- Noise burst rejection circuit
- RFI immunity
- UL listed

MOUNTING LOCATION

The FG-715 and FG-730 can be mounted on walls, in corners, even on false or suspended ceilings. Refer to the guidelines below when selecting a mounting location.

- The unit must have a direct line of sight to, and a clear view of, the protected glass.
- Locate the FG-715 **within 15'** (4.5 m) of the glass to be protected. Locate the FG-730 **within 30'** (9 m) of the glass to be protected.
- Curtains, blinds, and other window coverings will absorb energy from breaking glass. Heavy curtains, for example, will effectively block the sound signal. In these cases, mount the unit on the window frame behind the window covering, or above the window. **Make sure to test the unit thoroughly for proper detection.**
- Do not mount the unit in front of air ducts or forced air fans, or close to bells measuring 2" (or larger) in diameter.

MOUNTING PROCEDURE

Orient the unit as shown in Figure 1. Remove the screw located at its top. While depressing the latch near the top of the unit, swing the front cover forward. Use the back cover as a template to mark holes for the mounting screws and wiring, then drill the holes.

- **Note:** If you plan to corner-mount the unit, remove the printed circuit board *before* marking and drilling holes for the mounting screws.

Pull the wiring into the unit through the back cover. Using the two mounting screws, mount the rear housing at the desired location.

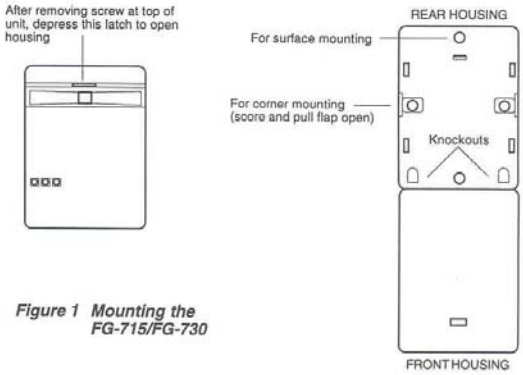


Figure 1 Mounting the FG-715/FG-730

WIRING

Observing the proper polarity, wire the unit as shown in Figure 2 (use 22 to 14 AWG). Reverse-polarity connections will not damage the unit.

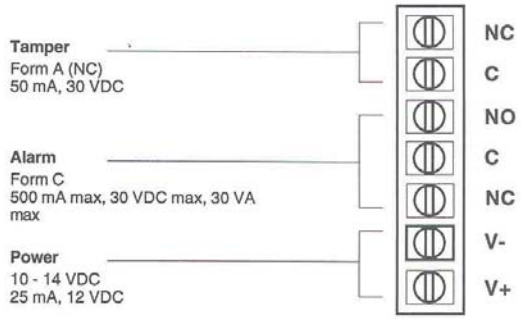


Figure 2 FG-715/FG-730 Terminal Strip

FLEX ADJUSTMENT

The flex technology of the FG-715 cannot be adjusted.

To adjust the flex technology of the FG-730: Use a screwdriver to set the flex sensitivity control (R5) at MAXIMUM by turning it all the way clockwise. Refer to Figure 3 on the back side of this page.

Turn on any heating/air conditioning system in the vicinity and observe the yellow flex LED (DS2) for approximately one minute. Excessive subsonic (inaudible) noise typically produced by air handling systems may cause the flex LED to flash randomly.

If it flashes randomly, turn the R5 control counterclockwise just until the flashing stops.

TESTING THE FG-715/FG-730

Use the FG-700 Glass-Break Simulator to test the FG-715/FG-730 detector.

Activate the simulator in MANual mode at the farthest point of the glass to be protected (15' maximum for FG-715, 30' maximum for the FG-730). If the green LED (DS1) on the detector flashes, the audio technology will detect breaking glass at that distance.

Test the flex technology by carefully striking the glass with your hand or a cushioned tool. If the yellow LED on the detector flashes, the flex technology will be sensitive enough to detect a blow to the glass at that distance.

Testing the FG-715/FG-730 (continued)

Switch the FG-700 simulator to the FLEX mode and generate a flex signal by carefully striking the glass. The simulator will automatically generate a burst of glass-break sound, and the red LED (DS3) on the FG-715/FG-730 should light to indicate an alarm condition.

See the FG-700 operating instructions for additional testing information.

FINAL TESTING

To ensure maximum protection against false alarms, activate any device in the area that may automatically cycle: pumps, generators, heating/air conditioning units, etc. If the cycling devices trigger an alarm, mount the unit in a different location.

There is no need to relocate the detector if the cycling only briefly triggers the flex technology (the yellow LED flashes).

ALARM MEMORY

The FG-715 and FG-730 are equipped with a latching circuit for the alarm LED. When the latching circuit is activated, an alarm condition will make the red alarm LED on the units latch on. This feature is particularly helpful in determining which unit alarmed in a multiple detector installation.

To activate the latching circuit, install a jumper at position W2 on the printed circuit board. Refer to Figure 3. To reset the latched alarm LED, remove then restore power to the detector.

Note: The latching circuit has absolutely no effect on the alarm relay. The alarm relay will continue to function as normal.

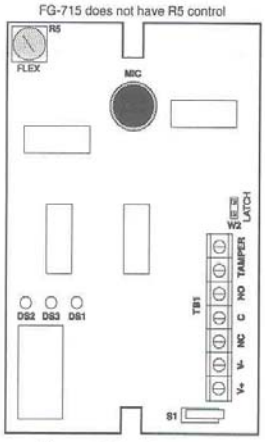


Figure 3 Testing the FG-715/FG-730

SPECIFICATIONS:

Range:
FG-715 15' (4.5 m)
FG-730 30' (9 m)

Alarm relay:
Form C
500 mA max
30 VDC max

Tamper switch:
Form A (NC)
50 mA, 30 VDC

Power requirements:
10 - 14 VDC
25 mA, 12 VDC

Dimensions:
3.9" H x 2.4" W x 0.79" D
(98 mm x 61.5 mm x 20 mm)

Weight:
3 oz (85 g)

Operating temperature:
32° to 120° F (0° to 49° C)

Glass types:
1/8", 3/16", and 1/4" plate;
1/4" laminated, wired, and tempered;
minimum size 10-7/8" x 10-7/8", single pane

Patents:
US Patents 4,853,677; 5,107,249 and 5,109,216 other international patents applied for

Approvals:
UL listed

NOTE: The FG-715/FG-730 should be tested **at least once each year** to ensure proper operation.

Important: The FG-715/FG-730 must be connected to a UL listed power supply or UL listed control unit capable of providing **a minimum of four hours** of standby power.

SENSOR DE MOVIMIENTO.

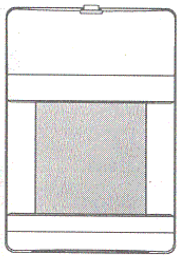
IntelliSense®

Model

IS-150/IS-150T

Passive Infrared Motion Sensor

Range: 50' x 40'(15 m x 12 m)



INSTALLATION INSTRUCTIONS

The IS-150/IS-150T passive infrared motion sensor from IntelliSense provides reliable detection coverage at an affordable price. The unit features a dense 50' x 40' pattern, including two look-down zones. Other important features include RF and white light immunity, a low 20 mA current draw and a tamper (IS-150T only).

The IS-150/IS-150T is compact, attractive, easy to install and maintain. The unit can be mounted almost anywhere **indoors**: on walls or in corners.

FEATURES

- 50' x 40' range
- Selectable detection range 50' (15m) to 32' (10m) (IS-150T only)
- Dual element PIR
- Dense detection pattern
- Wide angle lens included
- Low 20 mA current draw at 12 VDC
- 10 - 14 VDC operation
- Energized form A alarm relay
- RF and white light immunity
- Selectable PIR sensitivity
- Mounting flexibility: on walls or in corners
- Bug proof
- Tamper switch (IS-150T only)
- Remote LED Enable signal (IS-150T only)

MOUNTING LOCATION

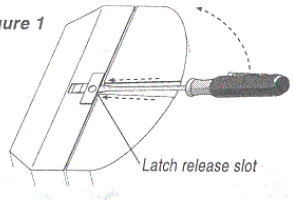
The IS-150/IS-150T is designed for use **indoors**. Make sure the sensor has a clear line of sight to the protected area. Infrared energy cannot penetrate solid objects. If the sensor is blocked, it will not alarm.

Aim the sensor toward the interior of the room, away from windows and heating/cooling sources. The unit can be corner or wall mounted at either 4', 7'6", or 10' (see Range Chart on the next page).

MOUNTING PROCEDURE

Prepare the sensor for mounting by removing the front cover and printed circuit board (PCB). To remove the front cover of the sensor, use a screwdriver to slide into the latch release slot located at the top of the unit and then gently push up. (See Figure 1.)

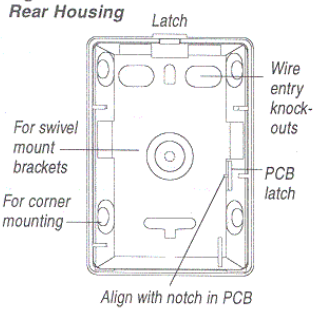
Figure 1



To remove the (PCB), press the latch holding the PCB in place and gently pull up on the PCB until it releases.

Using the rear housing as a template, use wire entry knockouts to mark holes in wall for desired mounting location. Pull several inches of wire into the housing. Drill holes and fasten rear housing to wall.

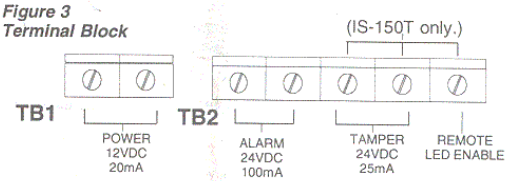
Figure 2
Rear Housing



WIRING

Terminals TB1 and TB2 are located at the top side edge of the PCB. Wire the IS-150/IS-150T as shown in Figure 3 using 22 to 14 AWG wire.

Figure 3
Terminal Block



CHANGING THE FRESNEL LENS

To install the optional pet-alley lens*:

- Remove the IS-150/IS-150T's front cover. (See Figure 4.)
- Press up on the Bug Guard latch and then pull the Bug Guard out of the front cover.
- Remove the existing lens, and place the new lens in with the SMOOTH side facing outward.
- Install the lens with the small slot at the top and the large notch at the bottom.
- Install the look-down mask (optional) over the inside of the look-down window.
- Snap the Bug Guard back into place, then reassemble the housing.

**Lens Option Kit Part Number 0-000-012-01*

Important: When using pet-alley lens, optimum mounting height is 4 feet and adjust PCB to +1 position.

Figure 4
Changing the Lens

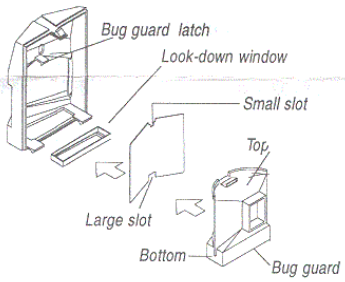
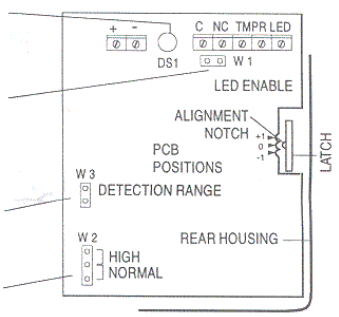


Figure 5
Printed Circuit Board



ALIGNMENT NOTCH

Important: Align with appropriate notch on the PCB (refer to Range Chart on the next page).

Using the chart below, configure the IS-150/IS-150T for the sensitivity best suited to your application.

SENSITIVITY	JUMPER W2 POSITION
High	Jumper top & center pins
Normal	Jumper center & bottom pins

WALK-TEST

Apply power to the unit and let it warm up for **three minutes**. Begin walk-testing when the alarm LED (DS1) goes out.

Walk across the protected area at the ranges to be covered. Two to four normal steps across the pattern should make the alarm LED light. Wait for the alarm LED to go out, then continue walk-testing. When there is no motion in the protected area, the alarm LED should be off.

Important: The IS-150/IS-150T should be tested at least **once each year** to ensure proper operation.

ALARM LED DISABLE (IS-150T only)

To disable the alarm LED (DS1) after walk-testing the sensor, remove the jumper from position **W1** on the PCB. See Figure 4.

Tip: Park the jumper on *one* of the **W1** pins (i.e. no short) to store for future use.

REMOTE LED ENABLE (IS-150T only)

This is an input signal to the sensor terminal block (labeled "LED") that allows the Alarm LED to be enabled remotely. As long as the signal is held low (grounded), the Alarm LED will illuminate when the sensor detects an alarm condition. Note that the alarm LED is enabled by this signal, even if the LED Disable jumper (W1) is removed.

LED ENABLE	PCB JUMPER W1	ALARM LED
Not Grounded	Shorted/Installed	On
Not Grounded	Open/Not Installed	Off
Grounded	Open/Not Installed	On
Grounded	Shorted/Installed	On

SPECIFICATIONS

Range:
50' x 40' / 32' x 40'
(15 m x 12 m) / (10 m x 12 m)

Power requirements:
10 - 14 VDC, 20 mA, 12 VDC
3V peak to peak at nominal
12 VDC

Alarm relay:
Form A (normally-closed)
100 mA, 24 VDC

Tamper Switch (IS-150T only)
Closed with cover in place
25 mA, at 24 VDC

RF immunity:
30 V/m
10 MHz - 1000 MHz

White light immunity:
6,500 LUX

PIR sensitivity:
Jumper selectable
(normal & high)

PIR fields of view:
dual element, 22 long range zones
6 intermediate, 3 lower,
2 look-down

Operating temperature:
32° to 120° F (0° to 49° C)

Relative Humidity:
5% to 95% noncondensing

Dimensions:
3-1/2" H x 2-1/2" W x 1-5/8" D
(9.0 cm x 4.4 cm x 4.12 cm)

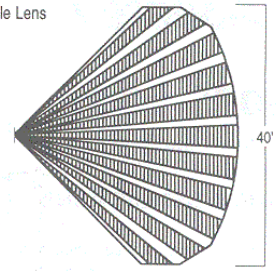
Weight:
3.0 oz (85.27g)
Packaged Product is 4.5 oz
(127.9 g)

Approvals/Listings:
CE
UL listed

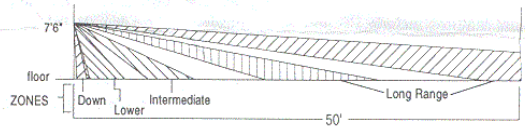
Important: The IS-150/IS-150T must be connected to a UL listed power supply or UL listed control unit capable of providing **a minimum of four hours** of standby power.

PROTECTION PATTERNS

TOP VIEW - Wide Angle Lens



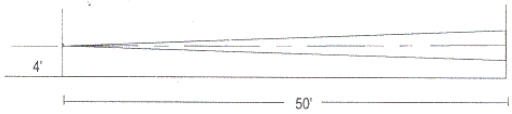
SIDE VIEW - Wide Angle Lens



TOP VIEW - Pet-Alley Lens

The TOP VIEW Pet-Alley lens is the same as the TOP VIEW Wide Angle lens.

SIDE VIEW - Pet-Alley Lens



MTG HEIGHT	PCB POSITION		
	+1	0	-1
4'	50'	N/A	N/A
7'6"	N/A	50'	N/A
10'	N/A	N/A	50'

IS-150/IS-150T RANGE CHART (50'/15m)

LIMITED WARRANTY

Seller warrants its products to be in accordance with its own plans and specifications and to be free from defects in materials and workmanship under normal use and service for **18 months** from the date stamp control on the product; or for products not having an IntelliSense Systems date stamp, for **12 months** from the date of original purchase, unless the installation instructions or catalogue sets forth a shorter period, in which case the shorter period shall apply.

Seller's obligation shall be limited to repairing or replacing, at its option, free of charge for materials or labor, any part which is proved not in compliance with Seller's specifications or proves defective in materials or workmanship under normal use and service. This warranty is void if the product is altered or improperly repaired or serviced by anyone other than an authorized IntelliSense factory service center. For warranty service contact the nearest IntelliSense Service Center.

THERE ARE NO WARRANTIES, EXPRESS OR IMPLIED, OF MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE OR OTHERWISE, WHICH EXTEND BEYOND THE DESCRIPTION ON THE FACE HEREOF. In no case shall Seller be liable to anyone for any consequential or incidental damages for breach of this or any other warranty, express or implied, or upon any other basis of liability whatsoever, even if the loss or damage is caused by Seller's own negligence or fault.

Seller does not represent that its product may not be compromised or circumvented; that the product will prevent any personal injury or property loss by burglary, robbery, fire, or otherwise; or that the product will in all cases provide adequate warning or protection. Buyer understands that a properly installed and maintained alarm system may only reduce the risk of burglary, robbery, or fire without warning, but it is not insurance or guarantee that such will not occur or that there will be no personal injury or property loss as a result. CONSEQUENTLY, SELLER SHALL HAVE NO LIABILITY FOR ANY PERSONAL INJURY, PROPERTY DAMAGE, OR OTHER LOSS BASED ON A CLAIM THAT THE PRODUCT FAILED TO GIVE WARNING. However, if Seller be held liable, whether directly or indirectly, for any loss or damage arising under this Limited Warranty or otherwise, regardless of cause or origin, Seller's maximum liability shall not in any case exceed the purchase price of the product, which shall be fixed as liquidated damages and not as a penalty, and shall be the complete and exclusive remedy against Seller.

This warranty replaces all previous warranties and is the only warranty made by IntelliSense on this product. No increase or alteration, written or verbal, of the obligation of this warranty is authorized.

C&K SYSTEMS

5-051-432-00 Rev A

CERRADURA MAGNETICA.

TROUBLESHOOTING

Problem:	Possible cause:	Solutions:
Door does not lock	No power	• Check to make sure the wires are securely tightened to the terminal block • Check that the power supply is connected and operating • Make sure the lock switch is wired correctly
Door locks, but can be easily forced open	Poor contact between electromagnet and armature plate	• Make sure the electromagnet and armature plate are properly aligned • Make sure the contact surfaces of the electromagnet and armature plate are clean and free from rust
	Incorrect voltage setting	• Check the power leads with a meter, and make sure 12VDC or 24VDC is present
Delay in door releasing	A secondary diode was installed across the electromagnet	• The electromagnet is fitted with a metal oxide varistor to prevent interference, so do not install a secondary diode

REGULAR MAINTENANCE

- Clean the contact surfaces of the electromagnet or armature plate with a soft cloth and non-abrasive, non-corrosive cleaner.
- Apply a light coat of a silicon lubricant and wipe away the excess to prevent rust.
- Check that the armature plate is securely attached to the door, yet can pivot slightly around the armature screw.
- Check that the electromagnet is securely attached to the door frame.

NOTICE

SECO-LARM® U.S.A., Inc.
16842 Millikan Ave., Irvine, CA, 92606, U.S.A.

filename: MUE941SA.P65 Dec2001

ENFORCER®

E-941SA-1200
E-941SA-600
E-941SA-300

ELECTROMAGNETIC LOCKS
INSTALLATION MANUAL

HOW THEY WORK

When power is applied to the magnetic lock, it turns on the unit's powerful built-in electromagnet. This electromagnet is attracted to the steel armature plate which is mounted on a door, holding the door fast against unauthorized entry. When power to the magnetic lock is turned off, the electromagnet releases the armature plate, allowing the door to open.

SPECIFICATIONS

	E-941SA-1200	E-941SA-600	E-941SA-300
Power	12VDC/24VDC	12VDC/24VDC	12VDC
Magnet Size	10½ x 1⅝ x 2⅝ in. (268 x 42 x 67 mm)	9⅞ x 1 1/16 x 1⅝ in. (250 x 27 x 42 mm)	6¾ x 15/16 x 1¼ in. (170 x 23 x 32 mm)
Armature Size	7¼ x ⅝ x 2⅜ in. (185 x 16 x 61 mm)	7¼ x ½ x 1½ in. (185 x 12 x 38 mm)	6 x ⅜ x 1¼ in. (152 x 10 x 32 mm)
Holding Force	1200 lb. (545kg)	600 lb. (272kg)	300 lb. (136kg)
Current Drain	500mA @ 12VDC 250mA @ 24VDC	500mA @ 12VDC 250mA @ 24VDC	315mA @ 12VDC
Voltage Tolerance	± 10%	± 10%	± 10%
Housing	Aluminum	Aluminum	Aluminum
Temperature	14°F to 131°F (-10°C to 55°C)	14°F to 131°F (-10°C to 55°C)	14°F to 131°F (-10°C to 55°C)
Weight	11 lb. (5.0 kg)	4lbs. 6oz. (2.0 kg.)	2lbs. 13.5oz. (1.29 kg.)

MOUNTING THE E-941SA-300, E-941SA-600 & E-941SA-1200

A. Drill holes for the mounting plate and armature plate (see fig. 1 and 2) by doing the following:
   1. Fold the mounting template along the dotted line.
   2. Close the door. Find a mounting location on the door frame near the upper free-moving corner of the door, as close to the corner of the door frame as possible.
   3. Place the template against the door and frame.
   4. Drill two holes in the door frame and three holes in the door as indicated on the template.

   NOTE — A filler plate or an L-bracket (optional) may be required for the electromagnet, depending on the door frame. See fig. 1.

B. Mount the armature plate to the door using at least two steel and one rubber washer (fig. 2):
   NOTE — Actual installation varies according to door style.
   1. Put one rubber washer between two steel washers, and place them over the armature screw between the armature plate and the door. This will allow the armature plate to pivot slightly around the armature screw in order to compensate for door misalignment.
   2. Tighten the sexnut bolt enough so the armature plate can withstand the force of someone attempting to break down the door while the electromagnet is engaged.
   3. Do not tighten the armature plate against the door. The plate must be able to pivot around the armature screw.
   4. Make sure the anti-spin guides are in the two guidepin holes.

C. Screw the mounting plate to the door frame or optional bracket:
   1. Screw the two short self-tapping screws in the slotted holes of the mounting plate and adjust the position of the mounting plate so that it and the armature plate form a 90-degree angle.
   2. Once the position is correct, use the long self-tapping screws to permanently mount the bracket.
   3. Remove the two short screws.

D. Drill the cable access hole.

E. Mount the electromagnet to the door frame (fig. 1) — Use the Allen wrench to screw the socket-head mounting screws through the bottom of the electromagnet into the mounting bracket. (Brass sleeves will be needed for the E-941SA-600.)

F. Connect the power leads (fig. 3):
   1. Open the electromagnet.
   2. Run two power leads from the power supply through the cable access hole into the electromagnet.
   3. Connect the power leads to the terminal block.
   4. Close the electromagnet.

   Note: E-941SA-300 is for 12VDC operation only. Connect the red wire to +12VDC, and the black wire to ground.

G. Test the unit.

H. Insert the tamper caps into the mounting screw access holes. This should be the last step, as once the tamper caps are in place, they will be difficult to remove.

ELECTROMAGNETIC LOCK Installation Manual

FIG. 1

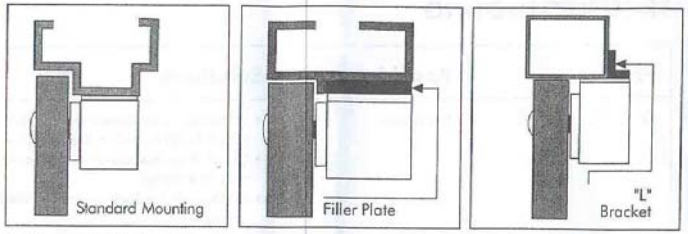


FIG. 2

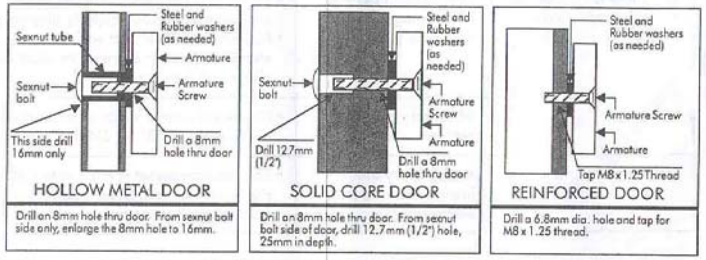
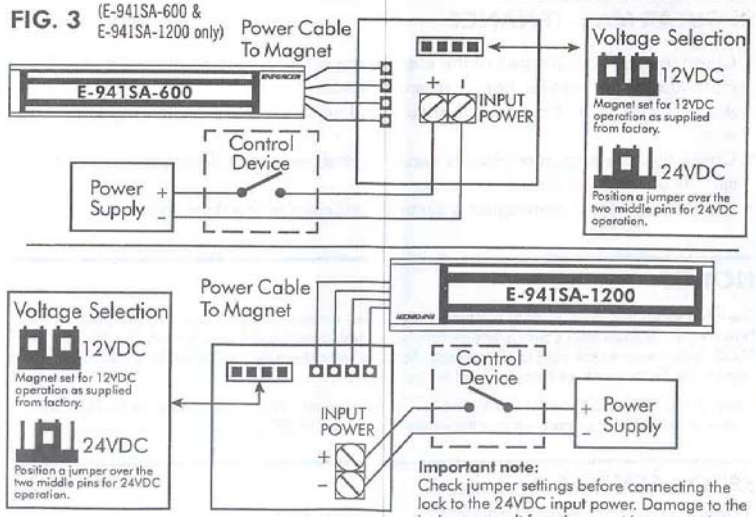


FIG. 3 (E-941SA-600 & E-941SA-1200 only)



Important note:
Check jumper settings before connecting the lock to the 24VDC input power. Damage to the lock may result from incorrect jumper settings.

ALARMA GENERAL.

INSTALLATION AND MAINTENANCE INSTRUCTIONS

PA400*, PS12LO, PS12M, PS24LO*, and PS24M* Electronic Mini-Sounders and Optional Strobes

*ULC models add suffix "A"; available in 24VDC only. Add suffix "R" for red models; "W" for white models; "B" for Beige model. PA400, add suffix "F" to models with fire printed on front.

SYSTEM SENSOR®
A Division of Pittway
3825 Ohio Avenue, St. Charles, Illinois 60174
1-800-SENSOR2, FAX: 630-377-6495
www.systemsensor.com

The Products to which this manual applies may be covered by one or more of the following U.S. Patent numbers: 5,546,293 and 5,488,462

Specifications

PA400 Sounder

Operating Voltage:	9.6VDC (absolute min.) to 33VDC (absolute max.)
Current Drain:	12 mA at 12 volts 15 mA at 24 volts
Temperature Range:	–10°C to +60°C (14°F to 140°F) 0°C to 49°C (32°F to 120°F) with strobe added
Sound Output:	Greater than 90 dBA measured in anechoic room at 10 feet, 24 volts. See Figure 1 for other voltages. 82 dBA minimum measured in UL reverbarant room (75 dBA minimum with strobe)

PS12/24 Strobe

	MODEL					
	PS12LO(W)	PS12M	PS24LO(W)	PS24M(W)	PS24LOA(W)	PS24MA(W)
Panel Voltage	12–17 VDC	12–17 VDC	22.5 - 30 VDC	22.5 - 30 VDC	22.5 - 30 VDC	22.5 - 30 VDC
Max. Current Drain @ Listed Panel Voltage	50 mA	180 mA	25 mA	75 mA	50 mA	180 mA
Min. Light Output @ 100% Viewing Angle (See Fig 2)	1.5 candela	15 candela	1.5 candela	15 candela	1.5 candela	15 candela

Figure 1:

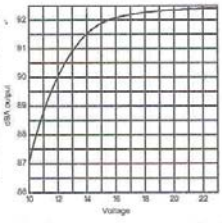
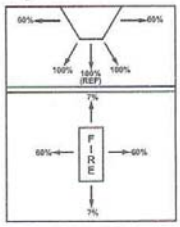


Figure 2:



Temperature Range: 0°C to 49°C (32°F to 120°F)

Under no circumstances can the PS24 voltage exceed 33VDC or be less than 18VDC.

Under no circumstances can the PS12 voltage exceed 18.7VDC or be less than 9.6VDC.

To calculate battery requirements, use current values shown above. However, note that there is an in-rush current associated with strobe power-up. The information in Figures 3 and 4 is useful when selecting fuse values.

As Figure 3 shows, 12V strobe in-rush current typically peaks at 3A and drops to nominal in 600μS. In a 24V strobe (Figure 4), in-rush current typically peaks at 7.0A and drops to nominal in 800μS.

Note: If class "A" wiring is installed, the wire length may be up to 4 times the single wire length in this calculation.

Figure 3. 12 volt strobe in-rush current:

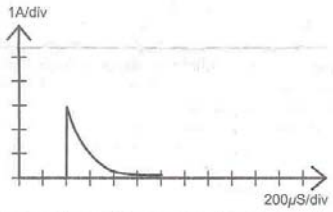
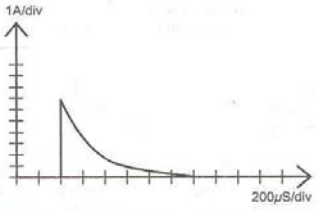


Figure 4. 24 volt strobe in-rush current:



General Information

The National Fire Protection Association has published codes, standards, and recommended practices for the installation and use of the above appliances. Therefore, the installer must be familiar with these requirements, with local codes, and any special requirements of the authority having jurisdiction.

Model PA400

The PA400W (white), PA400R (red), and PA400B (beige) Piezo Alert electronic sounder and optional supplementary signal strobes are intended to be connected to the alarm indicating circuit of a UL-listed 12 or 24 VDC fire alarm control panel. The models PS12 and PS24 optional strobe additions to the PA400 require a 12 VDC or 24 VDC panel, respectively and are able to operate from a full-wave rectified, unfiltered supply.

Installation Notes

The wiring must be in compliance with all codes and must not be of such length or wire size that would cause the appliance to operate outside of its published specifications. The appliances must also be tested after installation in accordance with the control panel manufacturer's test procedure.

NOTE: Do not loop wires under terminal screws. Wires connecting the device to the panel must be broken at the device screw terminal in order to maintain electrical supervision.

Mounting

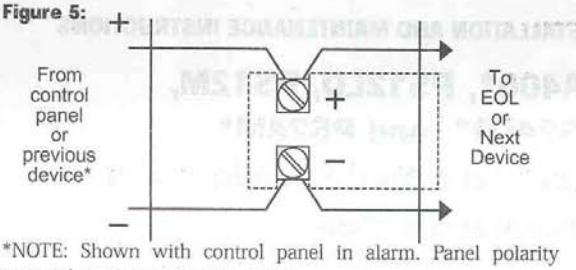
PA400 Sounders

1. The PA400 is intended for mounting to a standard 2-1/2" deep single-gang box which allows sufficient clearance for conduit entrance.
2. The PA400 is compatible with DC line supervision. The Piezo Alert is polarized and has terminals marked with polarity. Apply positive supply voltage to the (+) terminal and negative supply voltage to the (–) terminal. (See Figure 5.)
3. Mount the appliance to the electrical outlet box using the two mounting screws supplied.
4. Field repair of the PA400 should not be attempted. Return to factory for repair or replacement.

PS12 or PS24 Strobes

These optional strobes are interconnected to the PA400 by first removing the two mounting screws from the sounder. Use a small screwdriver to punch out the skinned-over areas as indicated in Figure 6. Install the adapter plate on top of the sounder and screw the combined sounder and adapter plate to the electrical outlet box. Make sure field wiring terminals are oriented in the upward position when mounted in the outlet box. Next, slide the strobe directly into the slots in the plates. The positive solder lug may be colored red or marked with a plus sign (+). This lug must be in the slot closest to the field wiring terminals. Grasp the catch area on each end of the strobe and squeeze while applying inward force. Make sure the strobe catches fully engage the slots in the adapter plate and that no gap appears at the interface between the strobe and adapter plate.

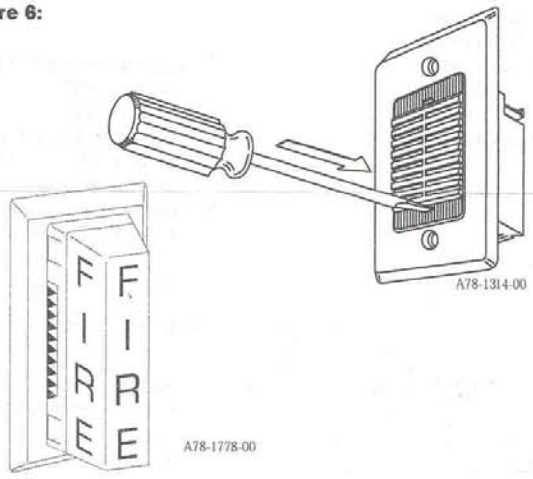
Figure 5:



*NOTE: Shown with control panel in alarm. Panel polarity reversed in supervisory condition.

A78-1315-00

Figure 6:



A78-1314-00

A78-1778-00

Please refer to insert for the Limitations of Fire Alarm Systems

⚠WARNING

The Limitations of Sounders and Strobes

System Sensor's sounder and signal strobe is designed to provide fire and security hazard warning.

The strobe is for supplementary signaling use only.

The sounder or sounder/strobe combination will not work without power. The sounder or sounder/strobe gets its power from the fire or security panel monitoring the alarm system. If power is cut off for any reason, the sounder or sounder/strobe combination will not provide the desired audible or visual warning.

The sounder may not be heard. The loudness of the sounder meets or exceeds current Underwriters Laboratories' standards, however, the sounder may not alert a sound sleeper or one who has recently used drugs or has been drinking alcoholic beverages. The sounder may not be heard if it is placed in an area which is isolated by a closed door, or if it is located on a different floor from the person in hazard or if placed too far away to be heard over the ambient noise such as traffic, air conditioners, machinery, or music appliances that may prevent alert persons from hearing the alarm. **The sounder may not be heard by persons who are hearing impaired.**

The signal strobe may not be seen. The electronic visual warning signal meets or exceeds current Underwriters Laboratories' standard 1638. The visual warning signal is suitable for direct viewing and must be installed within an area where it can be seen by building occupants. The strobe must not be installed in direct sunlight or areas of high light intensity where the visual flash might be disregarded or not seen. **The strobe may not be seen by the visually impaired.**

The signal strobe may cause seizures. Individuals who have a positive photic response to visual stimuli with seizures, such as epileptics, should avoid prolonged exposure to environments in which strobe signals, including this strobe, are activated.

Three-Year Limited Warranty

System Sensor warrants its enclosed sounder/strobe to be free from defects in materials and workmanship under normal use and service for a period of three years from date of manufacture. System Sensor makes no other express warranty for this sounder/strobe. No agent, representative, dealer, or employee of the Company has the authority to increase or alter the obligations or limitations of this Warranty. The Company's obligation of this Warranty shall be limited to the repair or replacement of any part of the sounder/strobe which is found to be defective in materials or workmanship under normal use and service during the three year period commencing with the date of manufacture. After phoning System Sensor's toll free number 800-SENSOR2 (736-7672) for a Return Authorization number, send defective units postage prepaid to: System Sensor, Repair Department, RA #_____, 3825 Ohio Avenue, St. Charles, IL 60174. Please include a note describing the malfunction and suspected cause of failure. The Company shall not be obligated to repair or replace units which are found to be defective because of damage, unreasonable use, modifications, or alterations occurring after the date of manufacture. In no case shall the Company be liable for any consequential or incidental damages for breach of this or any other Warranty, expressed or implied whatsoever, even if the loss or damage is caused by the Company's negligence or fault. Some states do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you. This Warranty gives you specific legal rights, and you may also have other rights which vary from state to state.

INTERFONOS.

SISTEMA DE TELEFONO
E
INTERFON.

MANUAL DE OPERACION.
MODELO : DP-RA01

commax

JR. ELECTRONICA S.A. DE C.V.

NOM

INTERFON.

1.-BOCINA.
2.-BOTON DE LLAMADO.
3.-SOPORTE DE MONTAJE.
4.-MICROFONO.

• CABLEADO.

• **ESPECIFICACIONES:**

FUENTE DE ALIMENTACION.	120 V CA. 60HZ.
POTENCIA DE SALIDA DE AUDIO.	70 mW.
POTENCIA DE SALIDA DE LLAMADO.	ALTO 180mW. BAJO 150 mW.
DISTANCIA EFECTIVA.	DE CUARTO A CUARTO 30 M. CAL. 22
PESO.	ESTACION MAESTRA, 461 GR. SUBESTACION, 622 GR. INTERFON, 180 GR.

• **PRECAUCIONES.**

A.-TODAS LAS INSTRUCCIONES DE OPERACION Y DE SEGURIDAD DEBERAN SER LEI-- DAS ANTES DE QUE EL QUIPO SEA OPERADO. ES CONVENIENTE QUE CONSERVE ESTE MANUAL PARA FUTURAS REFERENCIAS DE SU EQUIPO.

B.-ESTE EQUIPO NO DEBE SER OPERADO CERCA DEL AGUA, POR EJEMPLO: CERCA DE UNA TINA DE BAÑO, DE UNA REGADERA, DE UN LAVABO, DE UNA LAVADORA O DE UNA ALBERCA.

C.-ESTE EQUIPO DEBERA SER INSTALADO EN UN LUGAR Y UNA POSICION DONDE PUEDA TENER UNA VENTILACION APROPIADA, POR EJEMPLO ESTE EQUIPO NO DE- BE SER COLOCADO SOBRE LA CAMA, SOFA, ALFOMBRA O SUPERFICIES SIMILARES, ESO PUEDE BLOQUEAR LAS ABERTURAS DE VENTILACION, TAMPOCO EN UN ESTAN TE DE LIBROS O EN EL INTERIOR DE UNA CABINA DONDE SE PUEDA IMPEDIR QUE EL AIRE CIRCULE ATRAVES DE LAS AVERTURAS DE VENTILACION.

D.-EL EQUIPO NO DEBE SER SITUADO CERCA DE FUENTES QUE RADIEN CALOR, COMO REGISTROS DE ESCAPE DE CALOR, ESTUFAS U OTROS EQUIPOS QUE PRO- DUSZCAN CALOR.

E.-LA TRAYECTORIA DEL CABLE DE ALIMENTACION, DEBERA SER TRAZADA DE MANE RA QUE ESTE NO CORRA EL RIESGO DE SER PISADO, PINCHADO O DEGOLLADO EN CONTRA DE ALGUNA OTRA COSA. PONGA ESPECIAL CUIDADO EN LAS PARTES DEL EQUIPO DONDE SE REALIZAN LAS CONEXIONES DE ALIMENTACION E INTER-- CONEXION DE ELEMENTOS QUE LO INTEGRAN.

F.-EL CABLE DE ALIMENTACION DEBERA SER DESCONECTADO CUANDO EL EQUIPO PERMANEZCA LARGO TIEMPO FUERA DE OPERACION.

G.-NO TRATE DE INTRODUCIR OBJETOS AL EQUIPO, NO DERRAME LIQUIDOS SO-- BRE EL, QUE SE PUEDA INTRODUCIR A LOS CIRCUITOS, NO ROCIE LIQUIDOS NI SPRAY QUE PUDAN ENTRAR POR LAS ABERTURAS DE ESTE.

• **INSTRUCCIONES DE OPERACION.**

1.- COMUNICACION DE PUERTA A CUARTO.

A.-USTED PODRA ESCUCHAR EL SONIDO DE LLAMADO EN LAS DOS ESTACIONES SIMULTANEAMENTE CUANDO OPRIMA EL BOTON DE LLAMADO EN EL FRENTE DE CALLE. ES POSIBLE QUE USTED TENGA COMUNICACION DESDE CUALQUIERA DE SUS ESTACIONES EN LOS CUARTOS CON EL FRENTE DE CALLE, TENIENDO EL AU- RICULAR LEVANTADO.

2.-COMUNICACION DE CUARTO A CUARTO.

A.-USTED PODRA LLAMAR A LA OTRA ESTACION OPRIMIENDO EL BOTON DE LLA- MADO, EN ESTE MOMENTO PODRA ENVIAR UN MENSAJE A DICHA ESTACION EL CUAL SERA A VOZ ABIERTA. USTED TENDRA INTERCOMUNICACION HASTA QUE LA OTRA ESTACION LEVANTE EL AURICULAR.

B.-DURANTE EL USO DE LA LINEA DE ESTACION A ESTACION SI UNA PERSONA LLAMA A LA PUERTA USTED ESCUCHARA EL SONIDO DE LLAMADO DEL FRENTE DE CALLE EN EL AURICULAR.

C.-SI USTED ESTA OCUPANDO LA LINEA CON LAS DOS ESTACIONES Y ALGUIEN DESEA TENER COMUNICACION DESDE EL FRENTE DE CALLE, REGRESE LOS AURICULARES A - SU POSICION ORIGINAL Y LEVANTE CUALQUIERA DE LOS DOS PARA ATENDER LA LLA MADA.

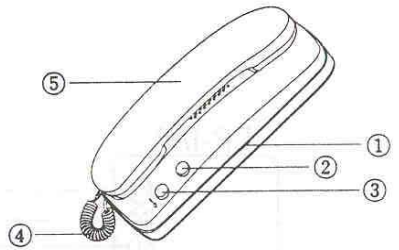
3.-ACTIVADOR DE PUERTA.

A.-DESPUES DE CONFIRMAR EL ACCESO DE SU VISITANTE, ABRA LA PUERTA PRESIO-- NANDO EL BOTON ACTIVADOR DE PUERTA DESDE CUALQUIERA DE SUS ESTACIONES

CONTROLES Y FUNCIONES.

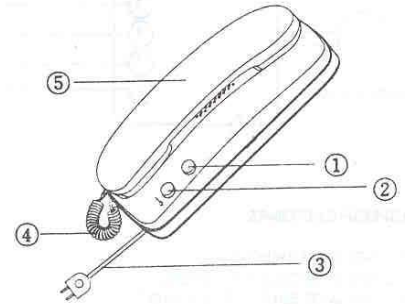
ESTACION MAESTRA PARA CUARTO.

1.-CONTROL DE VOLUMEN.
2.-BOTON DE LLAMADO A OTRA ESTACION.
3.-ACTIVADOR DE PUERTA.
4.-CORDON DEL AURICULAR.
5.-AURICULAR.



SUBESTACION PARA CUARTO.

1.-BOTON DE LLAMADO A OTRA ESTACION.
2.-ACTIVADOR DE PUERTA.
3.-CABLE DE ALIMENTACION CA.
4.-CORDON DEL AURICULAR.
5.-AURICULAR.



TRANSPONDER.

TEXAS INSTRUMENTS

RADIO FREQUENCY IDENTIFICATION SYSTEMS

Data Sheet

120mm Cylindrical Transponder

Specifications:

Part number	*RI-TRP-R9TD*	*RI-TRP-W9TD*	*RI-TRP-D9TD*
Functionality	Read Only	Read/Write	MPT
Memory (Bits)	64	80*	1360*
Memory (Pages)	1	1	17*RW
Operating Frequency	134.2 kHz		
Modulation	FSK (Frequency Shift Keying) 134.2 kHz / 123.2 kHz		
Transmission Principle	HDX (Half Duplex)		
Power Source	Powered from the reader signal (batteryless)		
Typical Reading Range	≤ 200 cm**		
Typical Programming Range	---	30 % of specified reading range	
Typical Reading Time	70 ms		86 ms
Typical Programming Time	---	309 ms	293 ms
Typical Programming Cycles	---	100,000	
Operating Temperature	-25 to +85°C	-25 to +70°C	-25 to +85°C
Storage Temperature	-40 to +100°C (Total +125°C for 1000 hours, +150°C for 100 hours, +175°C for 5 hours)		
Case Material	Reinforced Poly-Ether-Imide (PEI), black		
Protection Class	IP 67		
EMC	Programmed code is not affected by normal electromagnetic interference or x-rays		
Signal Penetration	Transponder can be read through virtually all non-metallic material		
Mechanical Shock	IEC 68-2-27, Test Ea; 200 g, half sine, 3 ms, 2 axes, 6 shocks per axis		
Vibration	IEC 68-2-6, Test Fc; 20 g, 20 - 500 Hz, 2 axes, 10 cycles per axis		
Dimensions	∅ 21 mm ± 0.8 mm * 121 mm ± 2 mm		
Weight	60 g		

* We recommend that you split each 80 bit page into 64 user programmable bits plus a 16 bit wide CRC CCITT Block Check Character as is done by TI-RFID LF readers.

** Depending on RF regulation in country of use, the Reader Antenna configuration used, and the environmental conditions.

For more information, contact the sales office or distributor nearest you. This contact information can be found on our web site at: **http://www.ti-rfid.com**

TEXAS INSTRUMENTS

RADIO FREQUENCY IDENTIFICATION SYSTEMS

Data Sheet

85mm Disk Transponder

Specifications:

Part number	*RI-TRP-R9UR*	*RI-TRP-W9UR*
Functionality	Read Only	Read/Write
Memory (Bits)	64	80*
Memory (Pages)	1	1
Operating Frequency	134.2 kHz	
Modulation	FSK (Frequency Shift Keying) 134.2 kHz / 123.2 kHz	
Transmission Principle	HDX (Half Duplex)	
Power Source	Powered from the reader signal (batteryless)	
Typical Reading Range	≤ 150 cm**	
Typical Programming Range	---	30 % of specified reading range
Typical Reading Time	70 ms	
Typical Programming Time	---	309 ms
Typical Programming Cycles	---	100,000
Operating Temperature	-25 to +85°C	-25 to +70°C
Storage Temperature	-40 to +85°C	
Case Material	Acrylate-Styrene-Acrylonitrile (ASA), black	
Protection Class	IP 53	
EMC	Programmed code is not affected by normal electromagnetic interference or x-rays	
Signal Penetration	Transponder can be read through virtually all non-metallic material	
Mechanical Shock	IEC 68-2-27, Test Ea; 15 g, 18 ms, half sine, 2 axes, 5 shocks per axis	
Vibration	IEC 68-2-6, Test Fc; 10 g, 20 – 500 Hz, 2 axes, 10 cycles per axis	
Dimensions	∅ 85.5 mm ± 0.5 mm * 5.5 mm ± 0.5 mm	
Weight	35 g	

* We recommend that you split each 80 bit page into 64 user programmable bits plus a 16 bit wide CRC CCITT Block Check Character as is done by TI-RFID LF readers.

** Depending on RF regulation in country of use, the Reader Antenna configuration used, and the environmental conditions.

For more information, contact the sales office or distributor nearest you. This contact information can be found on our web site at: **http://www.ti-rfid.com**

TEXAS INSTRUMENTS

RADIO FREQUENCY IDENTIFICATION SYSTEMS

Data Sheet

Mount-on-Metal Transponder

Specifications:

Part Number	*RI-TRP-R9VS*	*RI-TRP-W9VS*
Functionality	Read Only	Read/Write
Memory (Bits)	64	80*
Memory (Pages)	1	1
Operating Frequency	134.2 kHz	
Modulation	FSK (Frequency Shift Keying) 134.2 kHz / 123.2 kHz	
Transmission Principle	HDX (Half Duplex)	
Power Source	Powered from the reader signal (batteryless)	
Typical Reading Range	≤ 120 cm**	
Typical Programming Range	---	30 % of typical reading range
Typical Reading Time	70 ms	
Typical Programming Time	---	309 ms
Typical Programming Cycles	---	100,000
Operating Temperature	-25 to +70°C***	
Storage Temperature	-25 to +85°C	
Case Material	Polypropylene, black	
Protection Class	IP 67 (product revision –11)	
Mounting	With screws or rivets on aluminum, iron or steel	
EMC	Programmed code is not affected by normal electromagnetic interference or x-rays	
Signal Penetration	Transponder can be read through virtually all non-metallic material	
Mechanical Shock	IEC 68-2-27, Test Ea; 200 g, half sine, 3 ms, 3 axes, 6 shocks per axis	
Vibration	IEC 68-2-6, Test Fc; 20 g, 20 - 500 Hz, 3 axes, 10 cycles per axis	
Dimensions	102 mm ± 1 mm * 36 mm ± 1 mm * 16.5 mm ± 1 mm	
Weight	43 g	

* We recommend that you split each 80 bit page into 64 user programmable bits plus a 16 bit wide CRC CCITT Block Check Character as is done by TI-RFID LF readers.

** Depending on RF regulation in country of use, the Reader Antenna configuration used, and the environmental conditions.

*** Reduced operating temperature of 0 to +70°C if used with Series 2000 Standard Reader (RI-STU-MB2A/MB6A) or Standard RFM (RI-RFM-104B)

For more information, contact the sales office or distributor nearest you. This contact information can be found on our web site at: **http://www.ti-rfid.com**

LECTOR TAG.

e*Tag™ ET-RS & ET-TS

High Frequency RFID Readers & Reader/Writers

ET-RS & ET-TS

- HIGH FREQUENCY (13.56 MHz)
- COMPATIBLE WITH TEXAS INSTRUMENTS TAG-IT™
- READS MULTIPLE TRANSPONDERS IN THE FIELD
- READS UP TO 7" WRITES UP TO 5"
- RS-232 OR TTL
- OPEN ARCHITECTURE
- EXTREME WEATHER RESISTANCE

The e*Tag™ series of high frequency RFID readers and reader/writers utilize 13.56 MHz, a worldwide standard for radio-frequency identification applications. Designed to work with Tag-It™ transponders from Texas Instruments, e*Tag™ units can read multiple transponders in a field. e*Tag™ reader/writers are available with an integral antenna, capable of reading transponders up to seven inches away. e*Tag™ units are also available with a 50-ohm interface for use with custom antennas. e*Tag™ reader/writers can also write and lock data on transponders. Each Tag-It™ transponder has 256 bits of available user-defined memory.

e*Tag™ products support totally open architecture applications. Readers and reader/writers are available with RS-232 and TTL interfaces. e*Tag Host software is available to demonstrate the host-client command structure and assist systems integrators and OEMs in designing custom applications.

Secura Key also offers a line of e*Tag™ transponders packaged as credit-sized cards and key ring tags. Custom transponder packaging and four-color graphics are available.

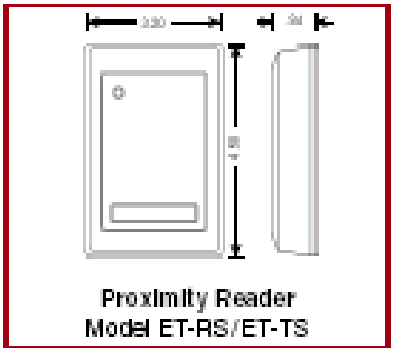
Specifications subject to change without notice

 SS-17

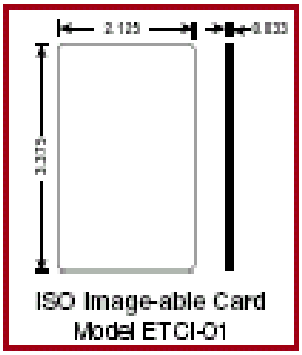
Secura Key

ET-RS & ET-TS SPECIFICATIONS

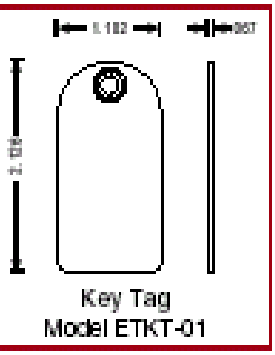
All dimensions in drawings are indicated in inches.



Proximity Reader
Model ET-RS/ET-TS



ISO Image-able Card
Model ETCI-01



Key Tag
Model ETKT-01

MODELS AVAILABLE

WITH ANTENNA		WITH 50 ohm INTERFACE
ET-RS-A	RS-232 - READ ONLY	ET-RS-A-50
ET-RS-C	RS-232, READ AND WRITE	ET-RS-C-50
ET-TS-A	TTL, READ ONLY	ET-TS-A-50
ET-TS-C	TTL, READ AND WRITE	ET-TS-C-50

PHYSICAL

Type	Reader	ISO Image-able Card	Key Tag
Model	ET-RS / ET-TS	ETCI-01	ETKT-01
Depth	0.84" (2.13 cm)	0.033" (0.08 cm)	.067" (0.17 cm)
Width	3.20" (8.13 cm)	2.125" (5.40 cm)	1.102" (2.80 cm
Height	4.50" (11.43 cm)	3.375" (8.57 cm)	2.126" (5.40 cm)
Weight	2.8 oz. (79.38 gm)	0.20 oz (5.67 gm)	.008 oz (0.23 gm)
Material	Polycarbonate (Lexan®)	PVC	PVC
Standard Color	Beige; Black Optional	White*	White*

*Also available with four color graphics and custom colored plastic.

POWER REQUIREMENTS 12-14 VDC, 300 mA maximum

ET-RS - RS-232 INTERFACE

RS-232 Output	19.2K Baud
Cable Required	Maximum Distance: 50 ft. - 6 conductor 20 gauge shielded cable

ET-TS - TTL INTERFACE

TTL Signal Level	Low = 0 to 1.5 v High = 3 v to 5 v

ENVIRONMENT

Temperature	-40° to +158°F (-40° to +70°C)
Humidity	0 to 100%

OPERATIONAL

Reading Distance	With Antenna	Up to 7" (17.78 cm)
Writing Distance	With Antenna	Up to 5" (12.70 cm)
Card/Key Tag Operation		Passive
Transmit Frequency		13.56 MHz

READER CONNECTIONS

WIRE COLOR	ET-RS-C DESCRIPTION	ET-TS-C DESCRIPTION	ET-RS-A DESCRIPTION	ET-TS-A DESCRIPTION
RED	12-14 VDC	12-14 VDC	12-14 VDC	12-14 VDC
BLACK	GROUND	GROUND	GROUND	GROUND
GREEN	TXD	TXD	TXD	TXD
WHITE	RXD	RXD	RXD	RXD
BROWN	N/A	N/A	RED LED	RED LED
ORANGE	N/A	N/A	GREEN LED	GREEN LED
BLUE	N/A	N/A	N/A	N/A
VIOLET	N/A	N/A	N/A	N/A

This product complies with UL 294 Standards and with Part 15 of the FCC Rules.

WARRANTY (U.S. and Canadian)

"This product is warranted against defects in materials and workmanship for a period of 2 years from the date of purchase. Secura Key shall, at its option, either replace or repair this product, if returned to us freight prepaid within the warranty period. This warranty does not include freight, taxes, duties, or installation expenses. THE WARRANTY SET FORTH ABOVE IS EXCLUSIVE AND NO OTHER WARRANTY, WHETHER WRITTEN OR ORAL, IS EXPRESSED OR IMPLIED. SECURAKEY SPECIFICALLY DISCLAIMS ANY IMPLIED WARRANTIES OR MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. The remedies provided herein are the buyers' sole and exclusive remedies. In no event shall Secura Key be liable for direct, indirect, special, incidental or consequential damages (including loss of profits), whether based on contract, tort or any other legal theory." Contact Secura Key for Card/Tag and Export Warranty Policies.

DISTRIBUTED BY:

Secura Key
20447 Nordhoff Street, Chatsworth, CA 91311
PHONE (818) 882-0020 • FAX (818) 882-7052
TOLL-FREE (800) 891-0020
Website: www.securakey.com
E-mail: mail@securakey.com

TRANSPONDER (CREDENCIAL)

RADIO FREQUENCY IDENTIFICATION SYSTEMS

13.56 MHz Vicinity Transponder Badge

Key features:

- ISO/IEC 15693 compliant
- 13.56MHz Operating Frequency
- Read/Write capability with data locking option
- 2k bit user memory
- Simultaneous Identification

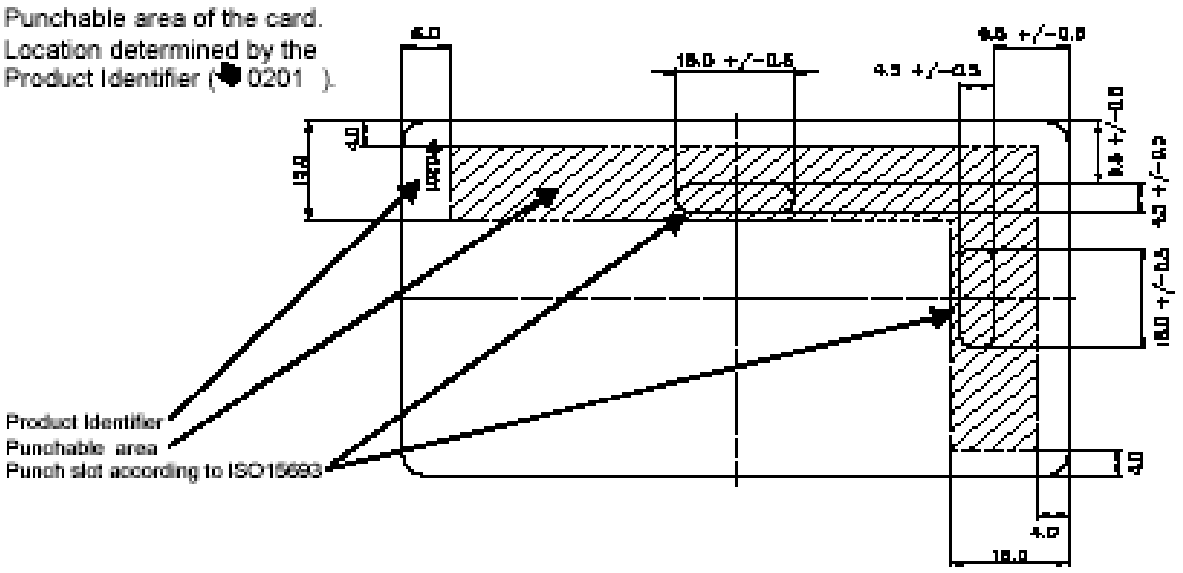
The Vicinity Transponder Badge from Texas Instruments is compliant with the ISO/IEC 15693 global standard for contactless integrated circuit cards that allows interoperability of products from multiple manufacturers operating at 13.56MHz. The badge is based on TI's Tag-it™ Smart Label technology. With a user memory of 2K bits organized in 64 blocks, the 13.56 MHz badge enables advanced solutions for the access control market. The enhanced data capacity makes it easy to handle new solutions such as biometrics authentication and advanced levels of encryption. Data written and stored on the badge, independent from a host system, means that employees carry vital information like authorization codes, certification or emergency medical histories. With TI's factory-programmed ID code, it is virtually impossible to forge or duplicate a badge, providing the assurance that no two cards – or people – anywhere in the world will be misidentified. Yet with in-the-field programmability, additional data like time stamps or new identification and access codes can be created and updated on-the-fly.

The badge can be easily customized and personalized using standard dye sublimation thermal transfer printers. Where the card needs to be used with a clip, a hole can be punched in the specified area (see drawing). Additional options include magnetic stripe, Custom data programming, and hole punching will be available.

(Print examples)

Part Number	RI-TH1-CB2A
Supported Standard	ISO 15693
Operating frequency	13.56 MHz
Typ. required activation field strength to read (at +25°C)	99 dBµA/m
Typ. required activation field strength to write (at +25°C)	102 dBµA/m
Factory programmed Read Only Number	64 bits
Memory (user programmable)	2k bits organized in 64 x 32-bit blocks
Typical programming cycles (at +25°C)	100,000
Data retention time (at +25°C)	> 10 years
Simultaneous Identification of Tags	Up to 50 tags per second (reader/antenna dependent)
Dimensions	85.6 mm x 54 mm x 0.76mm (according ISO 7810)
Weight	5 grams
Case material	PVC (Polyvinylchloride), white
Product Identifier ◆0201	3mm from the edge, TI Logo + 4 digit number (2 mm x 8 mm)
Surface finish	Glossy
Printability	Dye Sublimation Thermal Transfer, Silkscreen, Tampon
Mechanical Stability (Bending, Torsion)	According to ISO 10373
Operating temperature	-25°C to +50°C (according to ISO7810)
Storage temperature	-25°C to +50°C (according to ISO 7810)
Packing quantity	250 unit

Note: For highest possible read-out coverage we recommend to operate readers at a modulation depth of 20% or higher



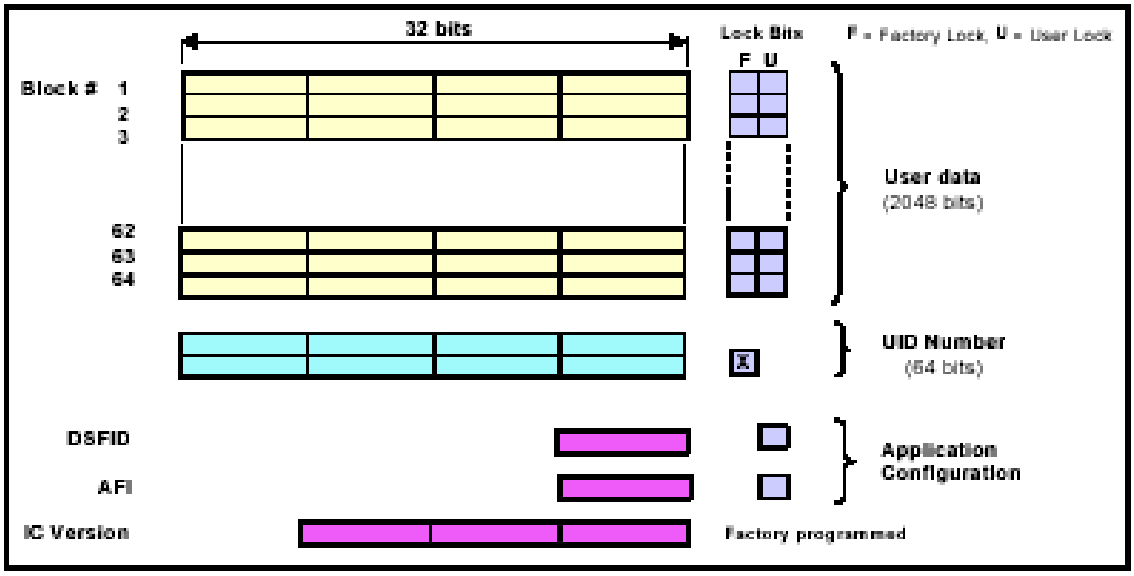
For more information, contact the sales office or distributor nearest you. This contact information can be found on our web site at: **http://www.ti-rfid.com**

Supported Command Set

Request	Request Code	Request Mode				
		Inventory	Addressed	Non-Addressed	Select	AFI
ISO 15693 Mandatory and Optional Commands						
Inventory	0x01	✔	-	-	-	✔
Stay Quiet	0x02	-	✔	-	-	-
Read_Single_Block	0x20	✔	✔	✔	✔	✔
Write_Single_Block	0x21	-	✔	✔	✔	-
Lock_Block	0x22	-	✔	✔	✔	-
Read_Multi_Blocks	0x23	✔	✔	✔	✔	✔
Write_Multi_Blocks	0x24	-	-	-	-	-
Select Tag	0x25	-	✔	-	-	-
Reset to Ready	0x26	-	✔	✔	✔	-
Write_AFI	0x27	-	✔	✔	✔	-
Lock_AFI	0x28	-	✔	✔	✔	-
Write DSFID	0x29	-	✔	✔	✔	-
Lock DSFID	0x2A	-	✔	✔	✔	-
Get_System_info	0x2B	✔	✔	✔	✔	✔
Get_M_Blk_Sec_St	0x2C	✔	✔	✔	✔	✔
TI Custom Commands						
Write_2_Blocks	0xA2	-	✔	✔	✔	-
Lock_2_Blocks	0xA3	-	✔	✔	✔	-

✔: Implemented
- : Not applicable

Memory Organization



CONVERSOR SERIAL RS232/RS485.

Figura 7. Conexión eco local.

errática puede resultar necesario poner resistores de terminación (RT). Como valor práctico se suguiere instalar dos resistores, uno en cada extremo de la linea, de valores comprendidos entre 1KΩ y 390Ω, el mayor valor que garantize la comunicación. La RT puede instalarse en la bornera o bien soldarse sobre el impreso.

TIERRA Y BLINDAJES

Las normas RS485 y RS422 operan sobre lineas balanceadas y no es necesario un conductor entre las tierras de los equipos para establecer la comunicación. Esta no demanda de blindajes especiales, si el cable dispone de una pantalla se le puede conectar a tierra en uno solo de los extremos.

PROBLEMAS DE INSTALACION

-No enciende el led PW. Verifique la presencia de DTR y/ó que la alimentación externa es la correcta.
-No encienden TX/ RX. Verifique si el módulo se halla sobre el COM correcto.
-El led RX siempre encendido. Usualmente es por inversión de la línea.

ADAPTADORES, CABLES EXTENSION

Es posible conectar AP485 mediante adaptadores: por ejemplo DB9 a DB25, o bien con cables de extensión; en ambos casos los estándares usuales de venta son válidos. Si el usuario quiera armar el cable, o verificar el que dispone, se muestra el conexiado mínimo necesario.

Figura7. Cable extensión DB25 a DB25

Figura 8. Cable extensión DB9 a D325

Figura 9. Cable extensión DB25 a DB25 conexión a unidad DCE (ejem: modem)

Nota: AP485 necesita RTS y/ó DTR.

OTROS MODELOS

-OPTO485. Conversor RS232-RS485/422 optoaislado, alimentación 4,5VCC a 28VCC, aislación ±400VCC.
-APD9-485, APDB9-422. Conversores RS232 a RS485/422 autoalimentados, conector DB9(h).
-AXI485-5/12. Conver. RS232 a RS485/422, alimentación externa 5/12VCC., conector DB25 (h).

MICRO AXIAL
DESARROLLA Y FABRICA:
ADQUISICION DE DATOS & CONTROL
Carlos Calvo 3928, (1230) Capital, Argentina
Tel: +54-11 4931-5254 microaxial@microaxial.com.ar
http://www.microaxial.com.ar

AP485

CONVERSOR RS232 a RS485/422 AUTOALIMENTADO

CARACTERISTICAS PRINCIPALES

- ✓ Conversor RS232 a RS485 / 422.
- ✓ Autoalimentado: toma energía de las líneas RS232. También acepta alimentación externa.
- ✓ Opera sobre enlaces de hasta 600m.
- ✓ Reconocimiento automático de 2 hilos RS485 ó 4 hilos RS422.
- ✓ Sin llaves ni puentes de selección.
- ✓ Operación hasta 38,4 Kbaudios.
- ✓ Comunicación con o sin eco local.
- ✓ Pequeñas dimensiones: 8,7x5,4x1,6cm.

APLICACIONES

- ✓ Enlace entre computadoras, PLCs, instrumentos, registradores, etc.
- ✓ Indispensable en enlaces extensos.

DESCRIPCION

Los módulos conversores AP485 permiten comunicar un terminal RS232 con uno o más dispositivos que operan con las normas RS485 (2 hilos) o RS422 (4 hilos).

Cada módulo AP485 cuenta con una etapa transmisora y otra receptora (figura 1), ...rmite comunicaciones semidúplex o ...lex completo. La unidad reconoce automáticamente si se trata de una conexión de 2 o 4 hilos, sin utilizar llaves ni puentes. Del lado RS232 son necesarias las líneas de datos Tx, Rx y DTR (RTS es opcional). Conector DB25: hembra conversor, conexión directa a un equipo DTE. Ver fig.9 para conexión a DCE.

ALIMENTACION

El modelo AP485 obtiene energía de las señales RS232, a tal efecto es necesaria la presencia de las líneas Tx y DTR (opcionalmente RTS), DTR debe estar siempre activa como es usual en la práctica, la línea es manejada por el software.
El modelo acepta también alimentación externa entre 8 y 10VCC (10mA). Esta se aplica entre los bornes +Vin y GND. Ambas alimentaciones pueden coexistir sin daño ninguno, el conversor seleccionará la tensión más alta. El led PW es indicador de energía.
Nota: En algunos modelos de PC en que las señales provistas por el puerto son de bajísima capacidad de corriente, es posible que el conversor no opere correctamente. En estos casos recomendamos utilizar el AP485 con alimentación externa.

Figura 1. AP485, esquema interno.

INSTALACIÓN

Con el computador apagado, inserte la unidad en el conector DB25 sujetándolo por los tornillos laterales. La línea (y la alimentación si utiliza externa) pueden conectarse sobre el módulo de bornera o bien sobre el conector DB25(M), la opción que más convenga al usuario. Si opta por la

microAXIAL

Conector DB25(H), lado RS232			Conector DB25(M), lado RS485/422			Borne
Pin		Comentario	Pins		Comentario	
2	TX	Transmisión datos	2,17	TRX-	(-)Trans/Recep datos	TRX-
3	RX	Recepción datos	14,15	TRX+	(+)Trans/Recep datos	TRX+
4	RTS	Puente con CTS	3,19	RX-	(-) Recepcion datos	RX-
5	CTS	Puente con RTS	16,18	RX+	(+) Recepcion datos	RX+
6	DSR	Puente con DTR	20	+Vout	Alimentacion interna +5V	
20	DTR	Puente con DSR	7	CGnd	Tierra comunic.lado línea	
7	Gnd	Tierra	13	Gnd	Tierra alimen.lado RS232	Gnd
9	+Vin	Alimentación	9	+Vin	Entrada alim. 4.5 a 28vcc	+Vin

Figura 2. Asignación conectores: lado RS232, lado RS485 / 422, bornera.

bornera, pase los conductores por la oreja de sujeción, un eventual tirón en el cable no afectará la instalación (figura 3). La línea se conectará según la necesidad del usuario como RS485, RS422, line driver o RS485 con eco local. Se describen todas las alternativas.

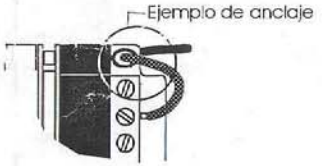


Figura 3. Oreja de sujeción cables

Conexión RS485. El enlace se realiza mediante una línea conformada por dos hilos, en la práctica un par telefónico. La figura 4 ilustra la conexión. La norma RS485 permite conectar múltiples dispositivos 'colgados' de la misma línea. La comunicación será semiduplex. El módulo habilita el transmisor cada vez que despacha un dato. Durante la transmisión se enciende el led TX, durante la recepción se activa RX.

Conexión RS422. El enlace se realiza mediante 4 hilos, en la práctica dos pares telefónicos. La figura 5 ilustra la conexión, nótese que sobre una línea debe trabajar un transmisor y uno o mas receptores. El módulo permite la comunicación duplex total. Durante la transmisión titila el led TX, durante la recepción el led RX.

Conexión 'Line Driver'. La comunicación entre equipos es impracticable si se hallan a gran distancia, se recomienda en tales casos el empleo de un módulo por cada equipo, vinculados como muestra la figura 6. Los equipos pueden ser computadores, PLCs, adquisidores remotos, etc. La conexión sugerida es de 4hilos.

Eco local. Hay transmisión con eco local (echo on) cuando el dato transmitido es retomado por el receptor local. El eco se activa al instalar los puentes indicados en la figura 7. Esta opción es válida en 2 hilos y se emplea solo en aquella situaciones (no demasiadas) indicadas en forma explicita. Durante la transmisión se encienden el led TX y Rx, durante la recepción se activa RX.

TIPO DE LINEA

Los módulos operan con conductores del tipo telefónico ya sea en la versión de pares simples o como parte de un multicable, se sugiere que el par tenga una resistencia menor a 100 Ω/Km y una capacidad menor a 50pF/m. A modo de guía y para líneas de gran distancia se sugiere los cables EIA RS485 modelo 9841 de BELDEN, o similar.

RESISTORES DE TERMINACION

En casos de líneas extensas o muy capacitivas, operando por arriba de 19.2KBaudios y si la comunicación es

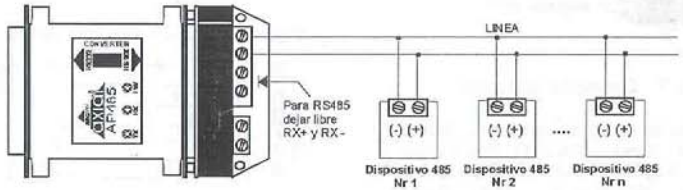


Figura 4. Conexión RS485, 2 Hilos.

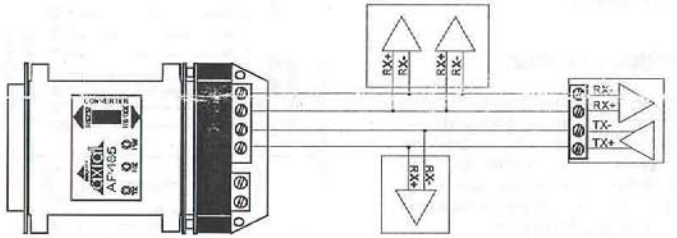


Figura 5. Conexión RS422, 4 Hilos.

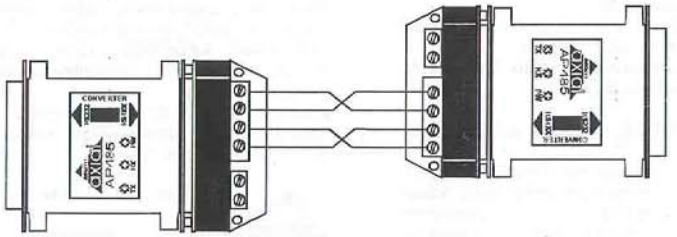


Figura 6. Conexión como line driver.

CARGADOR DE BATERIAS (RESPALDO TAG).

Altronix®

AL624 - Power Supply / Charger

Overview:

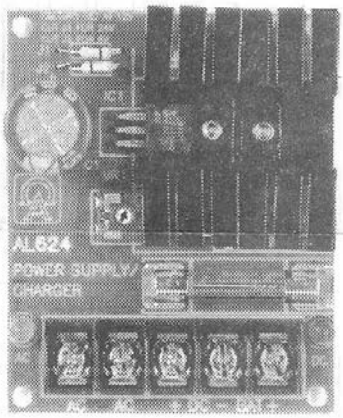
AL624 power supply/charger converts low voltage AC input into 6VDC or 12VDC @ 1.2 amps or 24VDC @ 750mA of continuous supply current (see specifications). This general purpose power supply has a wide range of applications for access control, security and CCTV system accessories that require additional power.

Specifications:

- Switch selectable 6VDC-12VDC-24VDC.
- 1.2 amp continuous supply current at 6VDC-12VDC.
- 750mA continuous supply current at 24VDC.
- Filtered and electronically regulated output.
- Built-in charger for sealed lead acid or gel type batteries.
- Maximum charge current 300mA.
- Automatic switchover to stand-by battery when AC Fails.
- Fused battery protection (circuit breakers available).
  Thermal and short circuit protection with auto reset.
- AC input and DC output LED indicators.
- Extremely compact design.
- Includes battery leads.

Board dimensions: 3"L x 2.5"W x 1.5"H

- Snap Trac compatible (order Altronix model #ST3).
- DIN Rail mount version available (order Altronix model #DPS1).



Voltage Output/Transformer Selection Table:

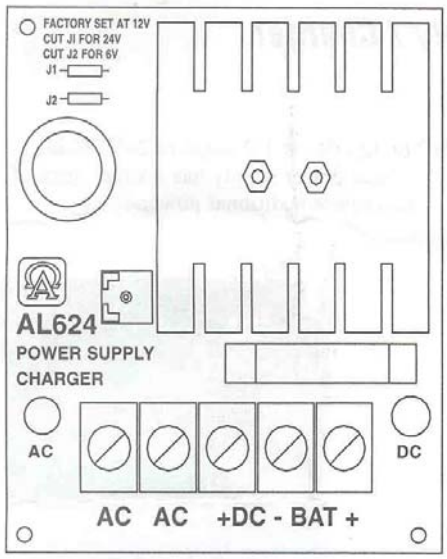
Output	Voltage Selector (JMPR)	Transformer
12VDC @ 1.2 amp continuous supply current	Leave J1 & J2 Intact	16.5VAC / 20 VA (Altronix model TP1620)
24VDC @ 750mA continuous supply current	Cut Jumper J1 Only	24VAC / 40 VA (Altronix model TP2440)
6VDC @1.2 amp continuous supply current	Cut Jumper J2 Only	12VAC / 20 VA (Altronix model TP1220)

nstallation Instructions:

1. Mount AL624 in desired location / enclosure.
2. **Unit is factory set for 12VDC.** For 6VDC output cut jumper J2, for 24VDC output cut Jumper J1.
3. Connect proper transformer to terminals marked [AC] (refer to Voltage Output/Transformer Selection Table).
   Use 18 AWG or larger for all power connections (Battery, DC output).
   Keep power limited wiring separate from non-power limited wiring (115VAC / 60Hz Input, Battery Wires). Minimum .25" spacing must be provided.
4. Devices to be powered should be connected to terminals marked [+ DC] and [DC - BAT] carefully observing polarity.
   Note: It is important to measure output voltage before connecting devices. This helps avoid potential damage.
5. Connect battery to terminals marked [BAT +] and [DC - NEG] (battery leads included)
   Use two (2) 12VDC batteries connected in series for 24VDC operation.
   Note: When batteries are not used, a loss of AC will result in a loss of output voltage.

LED Diagnostics:

Red (DC)	Green (AC)	Power Supply Status
ON	ON	Normal operating condition.
ON	OFF	Loss of AC, Stand-by battery supplying power.
OFF	ON	No DC output. Short circuit or thermal overload condition.
OFF	OFF	No DC output. Loss of AC. Discharged or no battery present.



Terminal Identification:

Terminal Legend	Function/Description
AC/ AC	Low voltage AC input (refer to voltage output/transformer selection table).
- DC +	6VDC-12VDC @ 1.2 amp continuous supply current. 24VDC @ 750mA continuous supply currentt.
+ BAT -	Stand-by battery connections. Maximum charge rate 300mA.

Bibliografía.

SERIAL PORT COMPLETE
Jan Axelon
Ed. LVR 1998 USA
ISBN 0-9650 819-2-3

SISTEMAS DIGITALES.
Principios y aplicaciones
Tocci, Ronald J.
Editorial Prentice Hall.
Sexta edición
ISBN 968-880-737-0

TTL logic.
Data Book
Texas Instruments, 1998

Literatura que pude se consultada en: www.national.com

MICROCONTROLADOR COP8™.
National Semiconductor Corp.
Manual de Teoría y Práctica Básica
Literatura Num. XXXXXX-001
Guadalajara, Jal. Enero-2001

COP8 Microcontroller Databook.
National Semiconductor Corp.
Lit 400004
1996/1997

COP8CBR9/COP8CCR9/COP8CDR9.
National Semiconductor Corp.
PRELIMINARY
April 2002.

Literatura que puede ser consultada en: www.ti.com/tiris/docs/manuals

PRODUCT MANUALS, TERMS & ABBREVIATIONS.
Texas Instruments, Noviembre 2001.
http://www.ti.com/tiris/docs/manuals/termabbs.pdf

Product bulletin High Prefomance LF Radio Frecuency Modules.
Texas Instruments,
http://www.ti.com/tiris/docs/manuals/pdfSpecs/hpdatsh.pdf

Series 2000 Reader System Control Modules RI-CTL-MB2A, RI-CTL-MB6A.
Reference Guide,
Texas Instruments, 11-06-21-037, JUNUARY 2000

Series 2000 Rader System, TIRIS Bus Protocol.
Reference Guide
Texas Instruments 11-06-21-053
March 2000

Tag-it™ Reader System Series 6000, Host Protocol.
Refernce Manual
Texas Instruments 11-04-21-001
July 1999

High Perfomance Remote Antenna-Reader Frecuency Module RI-RFM-008B, Antenna Tuning Board RI-ACC- 008B.
Reference Guide
Texas Instruments, 11-06-21-047, February 2002.

13.56 MHZ VICINITY CARD TRANSPONDER.
Texas Instruments 11-09-22-126
http://www.ti.com/tiris/docs/manuals/pdfSpecs/RI-TH1-CB1A.pdf

Antenna Design Reference Manual Rev. 1.0.
Texas Instruments.

Paginas Web consultadas.

http://www.dicsa.com.mx : Empresa dedicada a la venta de equipo para control de acceso y CCTV

http://www.capta.com.mx : Soluciones automatizadas para la seguridad de personas, activos y propiedad intelectual.

http://www.microaxial.com.ar : Empresa dedicada a la fabricación y venta de sistemas de adquisición de datos y control

http://www.quatech.com/about/about.php : Empresa dedicada a la fabricación y venta de sistemas de adquisición de datos y control

http://www.securakey.com: controles de acceso utilizando credenciales de proximidad.