TRABAJO ESPECIAL DE GRADO

Sistema de Control Maestro para el Sistema de Seguridad Inalámbrico de la EIE de la UCV

Presentado ante la Ilustre
Universidad Central de Venezuela
por el Br. Carrasquel R. José A.
para optar al título de
Ingeniero Electricista

Caracas, 2006

TRABAJO ESPECIAL DE GRADO

Sistema de Control Maestro para el Sistema de Seguridad Inalámbrico de la EIE de la UCV

TUTOR ACADÉMICO: Ing. José Alonso

Presentado ante la Ilustre
Universidad Central de Venezuela
por el Br. Carrasquel R. José A.
para optar al título de
Ingeniero Electricista

Caracas, 2006

CONSTANCIA DE APROBACIÓN

Caracas 13 de noviembre de 2006

Los abajo firmantes, miembros del jurado designado por el Consejo de Escuela de Ingeniería Eléctrica, para evaluar el Trabajo Especial de Grado presentado por el Bachiller José A. Carrasquel R., titulado:

"SISTEMA DE CONTROL MAESTRO PARA EL SISTEMA DE SEGURIDAD INALÁMBRICO DE LA EIE DE LA UCV"

Consideran que el mismo cumple con los requisitos exigidos por el plan de estudios conducente al Título de Ingeniero Electricista, y sin que ello signifique que se hacen solidarios con las ideas expuestas por el autor, lo declaran APROBADO.

Prof. Freddy Brito
Jurado

Prof. Ebert Brea
Jurado

Prof. José Alonso
Tutor Académico

iii

DEDICATORIA

A mis Padres, Gladis y Joseito, por todo su amor, colaboración y apoyo sin condiciones... nada será suficiente para retribuir todo lo que me han dado.

AGRADECIMIENTOS

A todos los docentes que favorecieron mi formación a lo largo de toda esta carrera, y especialmente a los profesores del Departamento de Electrónica, Computación y Control de la EIE, gracias a ellos esto es posible.

Al Profesor Javier López Cejalvo por sus aportes y colaboración.

A los compañeros del Proyecto de Sistema de Seguridad, Albert y Boris, por su colaboración y empeño para la culminación en buen termino del proyecto.

A los dedicados estudiantes que "viven" en el Laboratorio de Desarrollo de la EIE.

A la familia Súbero Silva por su apoyo sin condiciones.

A mi novia Angélica Súbero por su comprensión y apoyo que nunca termina.

Carrasquel R. José A.

SISTEMA DE CONTROL MAESTRO PARA EL SISTEMA DE SEGURIDAD INALÁMBRICO DE LA EIE DE LA UCV

Tutor Académico: José Alonso. Tesis. Caracas. U.C.V. Facultad de Ingeniería. Escuela de Ingeniería Eléctrica. Ingeniero Electricista. Opción: Electrónica, Computación y Control. Institución: U.C.V. 2006. 78 h.+anexos.

Palabras Claves: Sistema inalámbrico; Centro de Control; Alarma; Seguridad; LabView; DSC; PIC.

Resumen. Se desarrolló el Centro de Control para el prototipo de sistema de seguridad basado en una red inalámbrica de la EIE de la UCV. El Centro de Control está constituido por dos elementos, el primero es un hardware denominado Unidad de Control que está basado en microcontroladores PIC, memorias E2PROM y en un transceptor de 2.4 GHz. Esta Unidad recibe y almacena las alarmas provenientes de los sensores remotos, y además procesa estas alarmas para generar las acciones de control programadas que se ejecutan sólo cuando ocurren un conjunto de eventos específicos. El otro elemento que conforma el Centro de Control es un programa de computación que consiste en una Interfaz de Usuario desarrollada con LabView 7.1 y LabView DSC 7.1 que conectada a la Unidad de Control permite la configuración remota de todos los elementos de la red empleando funciones del protocolo MODBUS. La Interfaz crea una base de datos en tiempo real de todas las alarmas y eventos que ocurren en el sistema, una base de datos histórica de sucesos y muestra una representación gráfica de la ubicación y estado de los sensores activos en el sistema, esto facilita la visualización del estado general de la red.

INDICE GENERAL

LISTA DE FIGURAS

LISTA DE GRÁFICOS

LISTA DE TABLAS

INTRODUCCIÓN

Los sistemas de seguridad surgen debido a la necesidad de resguardar los bienes ante situaciones de riesgo previsible. Los robos, hurtos e incendios constituyen situaciones cotidianas. Las nuevas tecnologías han permitido el desarrollo de sistemas de seguridad cada día más versátiles y con amplias ventajas para satisfacer las crecientes necesidades de resguardo de los bienes.

Los sistemas de seguridad que emplean tecnología inalámbrica ofrecen ventajas de implementación en comparación con los sistemas cableados ya que la eliminación de los conductores reduce los costos de instalación, además, el propio hecho de ser inalámbricos aumenta su propia seguridad.

Recientemente, en la EIE de la UCV se desarrolló un sistema de seguridad basado en tecnología inalámbrica que está constituido por módulos remotos programables que reciben señales de sensores de incendio, de apertura de puerta, ruptura y presencia, adicionalmente este sistema posee controles de acceso que permiten controlar y monitorear el tráfico de usuarios en ciertas zonas. Todos los elementos que conforman este sistema de seguridad son programables remotamente.

El proyecto que se desarrolló en este Trabajo de Grado consiste en el diseño e implementación de un Sistema de Control Maestro para el Sistema de Seguridad Inalámbrico de la EIE. Este sistema recibe las alarmas enviadas desde los módulos remotos que indican el estado de los sensores, procesa las alarmas para ejecutar las acciones de control programadas, lleva un registro temporal de los eventos ocurridos, del tráfico de personas en los controles de acceso, y posee una interfaz gráfica que se ejecuta en un computador personal que permite monitorear y configurar los dispositivos que conforman la red del sistema.

A través de este sistema se pretende monitorear permanentemente las instalaciones de la EIE, controlar el tráfico de usuarios a ciertas zonas, determinar el momento y circunstancias en que ocurran violaciones a la seguridad (si estas sucedieran) y generar los avisos o alarmas ante situaciones de riesgo previsibles.

JUSTIFICACIÓN

Ante la necesidad de resguardar los bienes de la EIE de la UCV se requiere un sistema que facilite la supervisión de la edificación y que permita detectar las violaciones a la seguridad o las situaciones de riesgo previsibles. El sistema debe ser de bajo costo en cuanto a su desarrollo e implementación de manera que se facilite su financiamiento y ejecución dentro de la propia Escuela, también debe poseer características de robustez y confiabilidad.

Debido a lo antes expuesto surge la necesidad de desarrollar un sistema de seguridad basado en tecnología inalámbrica que cubra estos requerimientos.

OBJETIVO GENERAL

Desarrollo de un sistema de control maestro para el prototipo de sistema de seguridad basado en una red inalámbrica para la Escuela de Ingeniería Eléctrica de la Universidad Central de Venezuela.

OBJETIVOS ESPECIFICOS

- Investigación de los sistemas de control maestro para sistemas de seguridad que existen actualmente en el mercado.
- Definición de la arquitectura del sistema de control maestro.
- Diseño un módulo que reciba los datos de los sistemas remotos sensores y de los controles de acceso.
- Elaboración de un módulo que procese y registre en una memoria estática los datos recibidos, y que además tenga capacidad de generar alarmas cuando sea pertinente.
- Diseño de un módulo que permita la interconexión entre el sistema central y un computador empleando el protocolo MODBUS.
- Implementación a través de interconexión de los distintos módulos diseñados el sistema de control maestro.
- Ejecución de las pruebas del hardware del sistema de control maestro.
- Diseño de una interfaz grafica a través de la cual sea posible observar el estado de los sistemas sensores remotos, el registro de eventos ocurridos, el historial de tráfico de los controles de acceso, y que además permita programar las alarmas que se generarán cuando ocurren los eventos especificados y configurar los maestros de zona.
- Ejecución de las pruebas del software del sistema de control maestro.

- Ejecución de las pruebas del sistema de control maestro en conjunto: interfaz gráfica y hardware.

METODOLOGIA.

- Investigación de los sistemas de control maestro para sistemas de seguridad: arquitectura, interfaz, ventajas y desventajas.
- Investigación sobre el protocolo MODBUS: características, descripción, y acerca de software que permitan realizar una interfaz gráfica con facilidades de implementación del protocolo MODBUS.
- Definición de la arquitectura del sistema de control maestro.
- Definición del tipo de eventos que generaran las alarmas y como se ejecutaran estas cuando se produzca el o los eventos especificados.
- Diseño de los algoritmos de funcionamiento de cada uno de los módulos del sistema.
- Programación y depuración de los algoritmos de funcionamiento del sistema.
- Implementación física del hardware del sistema en circuito impreso.
- Ejecución de pruebas de funcionamiento del hardware: comunicación con los sistemas sensores remotos, alarmas y registro de eventos ocurridos.
- Diseño y programación de la interfaz gráfica.
- Verificación del funcionamiento de la interfaz gráfica: comunicación con los sistemas sensores remotos, programación de las alarmas y registro de eventos ocurridos.
- Ejecución de las pruebas de compatibilidad, funcionamiento simultáneo y operación continúa del hardware y el software del sistema de control maestro.

CAPITULO I:

DESCRIPCIÓN DE LA RED INALAMBRICA

El prototipo que se desarrolló para el sistema de seguridad consiste en dos redes, una red de nivel superior y otra de nivel inferior. La red de nivel superior posee una topología de árbol de ramales entrelazados de múltiples niveles. En esta topología, que es una generalización del tipo bus, el árbol tiene su primer nodo en la raíz y se expande hacia fuera utilizando ramas, allí se conectan las demás terminales. La red de nivel inferior posee una topología de estrella centralizada donde el elemento central corresponde a los nodos terminales de la red de nivel superior [1].

Esta arquitectura fue seleccionada considerando principalmente, el espacio físico donde funcionara el prototipo del sistema, que es el edificio de la EIE de la UCV.

1.1. Estructura De La Red Inalámbrica

El Prototipo de Sistema de Seguridad de la EIE está estructurado, como se menciono anteriormente, por redes de distintos niveles. Una red de nivel superior que interactúa con un control central, y por varias redes de nivel inferior que se desarrollan alrededor de algunos elementos de la red de nivel superior. Ver Figura 1

La red de nivel superior está delimitada por su frecuencia de operación: 2.4 GHz, y la constituyen los elementos denominados Maestros de Zona (MZ), Repetidores (RP) y Controles de Acceso (CA). Ver Figura 2.

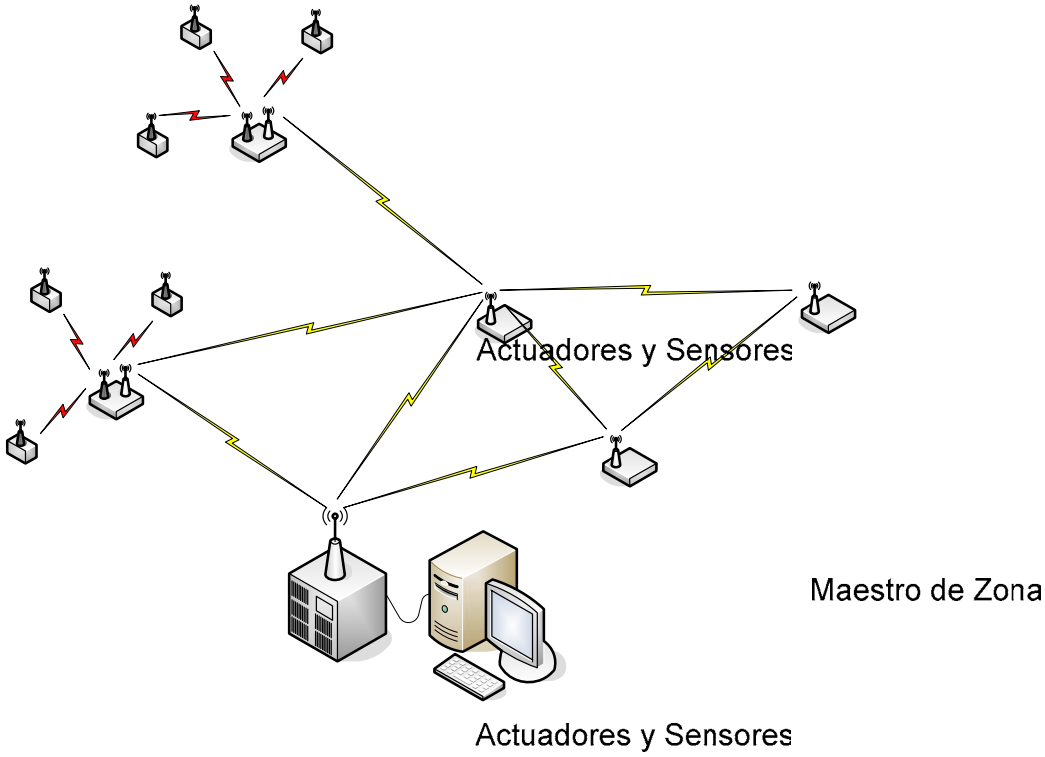


Figura 1. Estructura general de la Red Inalámbrica del Sistema de Seguridad de la EIE de la UCV

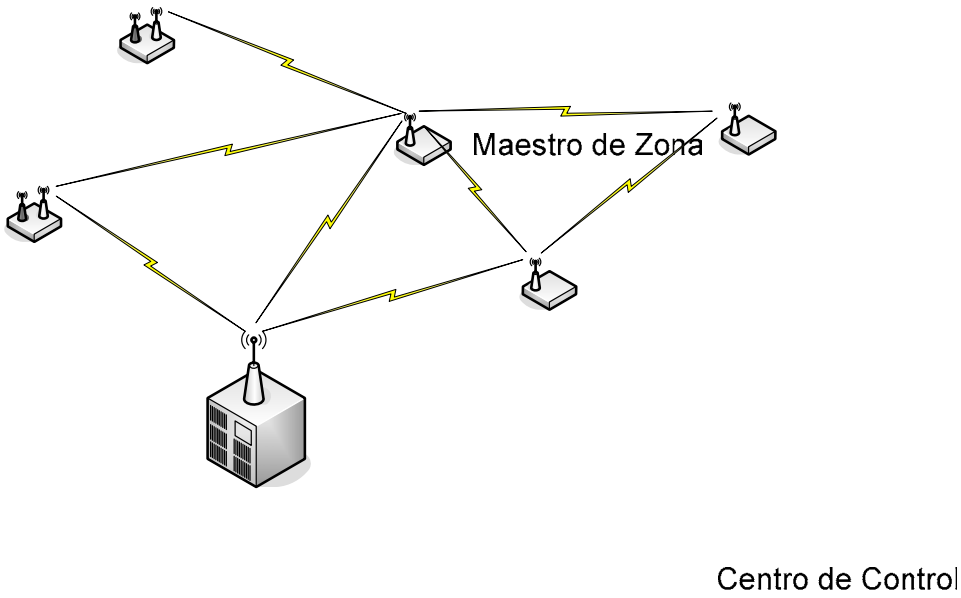


Figura 2. Estructura de la red de nivel superior

1.1.1. Maestros de Zona

Los Maestros de Zona son los elementos de la red encargados de recibir la información de los elementos del nivel inferior de la red y enviarla hacia el Centro de Control (CC). Cada Maestro está conformado por tres microcontroladores, un receptor de 400 MHZ y un transceptor de 2.4 GHz. Estos dispositivos supervisan periódicamente el funcionamiento de los sensores, reciben sus notificaciones de alarmas y las envían al Centro de Control, además manejan el protocolo para la comunicación inalámbrica en las dos frecuencias en que opera [1].

Los MZ soportan funciones de lectura-escritura de registros internos de operación debido a solicitudes realizadas desde el CC, y funciones de lectura o escritura de salidas que se encuentran en el propio dispositivo. Estas operaciones utilizan funciones del protocolo MODBUS.

Los Maestros poseen dos frecuencias de operación: la primera en la banda de 400 MHz, para la cual dispone de un receptor a través del cual se comunica con los sensores. En esta banda la comunicación con los sensores es en un solo sentido, desde los sensores hacia los MZ. La otra banda es la de 2.4 GHz, para la cual el MZ posee un transceptor que le permite comunicarse bidireccionalmente con el CC. Para lograr este enlace todos los dispositivos de la red de nivel superior, incluyendo los Maestros de Zona, poseen tablas de rutas que permiten la comunicación bidireccional, bien sea punto a punto o empleando Repetidores, con el Centro de Control. Estas tablas de rutas ofrecen más de una vía a través del cual un elemento de la red de nivel superior puede comunicarse con el CC, y viceversa.

1.1.2. Controles de Acceso

Los Controles de Acceso son los dispositivos encargados de gestionar el acceso de usuarios en áreas específicas. Estos elementos están constituidos por un control remoto con transmisor infrarrojo, que poseen los usuarios y desde allí se envía el código personal. El CA además posee un módulo principal donde se recibe y verifica este código, para posteriormente ejecutar las acciones asociadas al acceso de un usuario. El módulo principal contiene un microcontrolador que además de realizar las operaciones relativas al acceso de un usuario, gestiona la comunicación del CA con el CC [1].

Desde el Centro de Control se ingresan, eliminan y verifican los usuarios autorizados para acceder a una zona administrada por el CA.

Los CA poseen una sola frecuencia de operación: 2.4 GHz, y se comunicán bidireccionalmente con el CC de manera directa o a empleando Repetidores.

Los CA soportan las funciones MODBUS de lectura o escritura de registros. Estas funciones son utilizadas para lectura o escritura de registros internos de operación, actualización de tablas de usuarios válidos y lectura o escritura de salidas locales.

1.1.3. Repetidores

Los Repetidores son los dispositivos que se encargan de repetir y enrrutar la información proveniente de los MZ y CA hacia el CC, y viceversa. La función de estos dispositivos dentro de la red inalámbrica nace debido a la baja potencia de los transceptores que poseen los dispositivos del nivel superior de la red [1].

Los RP poseen una sola frecuencia de operación: 2.4 GHz, y de manera similar al resto de los dispositivos que operan en el nivel superior de la red poseen registros internos de operación, que pueden ser leídos o escritos desde el CC.

1.1.4. Módulos Sensores y Actuadores

La red de nivel inferior comprende los Módulos Sensores y Actuadores que operan en la banda de 400 MHz. Esta red está desarrollada alrededor de cada uno de los Maestros de Zona. Ver Figura 3

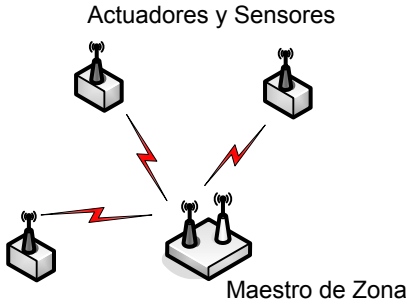


Figura 3. Estructura de la red de nivel inferior

Los Módulos Sensores y Actuadores son los elementos de la red donde se encuentran los sensores con capacidad de detectar las violaciones o situaciones de riesgo (incendio) en el espacio físico cubierto por un Maestro de Zona. Estos Módulos poseen un trasmisor en la banda de 400 Mhz a través del cual se comunican con el MZ respectivo [1].

Solo existen dos situaciones en las cuales los Módulos Sensores se comunican con el MZ: cuando envían la trama de datos periódica indicadora de su funcionamiento, y cuando envían una trama de alarma que puede ser debido a la detección de presencia, apertura de una puerta, ruptura o incendio.

La comunicación de los Módulos Sensores con los MZ es unidireccional, desde los módulos hacia los maestros. No existe una comunicación directa entre los Módulos Sensores y El Centro de Control, debido a la distinta frecuencia de operación. La función de llevar la información proveniente de los sensores hasta el CC es desarrollada por los MZ como se comento anteriormente.

Una descripción con mayor detalle de la arquitectura, funciones, y algoritmos de operación de los dispositivos tanto de la red de nivel superior como de la red de nivel inferior se encuentra en el Trabajo de Grado de Chávez, Albert.

1.2. Flujo de Información en la Red Y Tipos de Tramas.

Dos situaciones inician el proceso de comunicación en el Sistema de Seguridad: la primera se debe a una solicitud realizada desde el CC con destino igual a un elemento del nivel superior de la red. En este caso la red se comporta como un sistema maestro-esclavo, donde el Centro de Control es el que inicia la comunicación con una solicitud y solo responde el dispositivo que es direccionado. En el segundo caso la comunicación se inicia cuando algún elemento del nivel superior de la red envía una alarma hacia el Centro de Control, en este caso el CC siempre será la dirección de destino final. En las dos situaciones anteriores pueden o no estar involucrados repetidores como elementos que enrrutan la información entre los dispositivos terminales.

1.2.1. Flujo de Información en la Red

Cuando el CC envía una querella hacia algún MZ, RP o CA, esta solicitud puede pasar a través de algunos Repetidores. En el caso de que exista al menos un Repetidor en el proceso, describiremos con un ejemplo el flujo de la información desde el CC

hasta un elemento del nivel superior de la red, que en este caso será un Maestro de Zona.

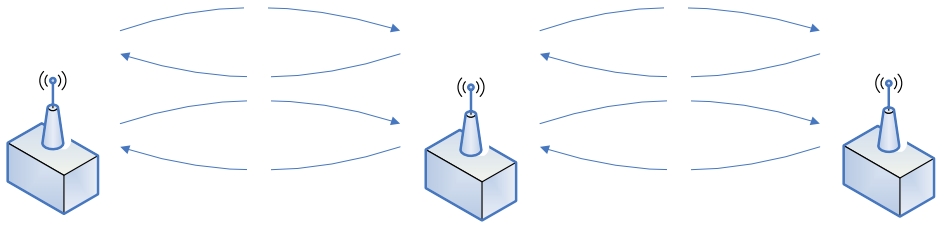


Figura 4. Flujo de la información en el nivel superior de la red debido a una querella del CC

T1

El proceso de comunicación CC - MZ estará constituido por ocho tramas. Como se observa en la Figura 4, el CC envía una trama T1 con una solicitud que tiene por destino el MZ 0x33, esta trama es enrrutada por el propio CC hacia el RP 0x34, ya que no existe una ruta directa entre el dispositivo 0x33 y el 0x34.

T2

T8

T7

El RP al recibir la trama T1 envía una confirmación T2 hacia el CC y se prepara, previa búsqueda en su tabla de rutas, para repetir los datos recibidos. Las tablas de rutas indican cual será el dispositivo siguiente que recibirá la información, en este caso la tabla de ruta debe indicar que la información ira directamente hacia el destino sin pasar por algún otro repetidor.

CC Dirección 0x99

Una vez que el MZ 0x33 recibe la trama T3, repetida por 0x34, confirma al Repetidor la recepción de dicha trama enviando a T4.

Ahora le corresponde al dispositivo que recibió la querella verificar esta solicitud y preparar la respuesta. La respuesta podría seguir, o no, el mismo camino que la solicitud, pero en este ejemplo la información fluye por la misma ruta pero en sentido contrario.

Cuando el MZ, previa búsqueda en su tabla de rutas, determina la dirección de envió de la respuesta a la solicitud (que para este ejemplo será el RP 0x34), enviará una trama T5 con la respuesta. El RP 0x34 recibe esta trama y envía una confirmación T6, y de manera similar procede a repetir la información hacia la dirección de destino enviando la trama T7.

Finalmente cuando el Centro de Control recibe la respuesta a su solicitud envía al RP 0x34 una trama T8 de confirmación de recepción.

Los dispositivos que realizan solicitudes, en este caso el CC, poseen límites de tiempo de espera tanto para confirmación como para la recepción de la respuesta. El límite de tiempo para la confirmación es igual a dos veces el tiempo que dura en el aire una trama de datos, y el límite de tiempo para la respuesta es igual al doble del número de saltos que realiza el paquete antes de llegar a su destino. Debido a que este tiempo depende del número de RP que estén involucrados, se consideró la situación más extrema: cuatro saltos, con tres Repetidores presentes.

La otra situación que puede iniciar la comunicación en el sistema de seguridad son las alarmas que envían los elementos del nivel superior de la red.

Como se explicara posteriormente, son distintos los eventos que producen que desde los MZ, RP y CA envíen alarmas hacia el CC. En cualquier caso las alarmas tendrán como dirección de destino el Centro de Control y pueden pasar o no a través de Repetidores.

Para el caso cuando existe un RP describiremos, también con un ejemplo como viaja una alarma enviada desde un MZ hacia el CC.

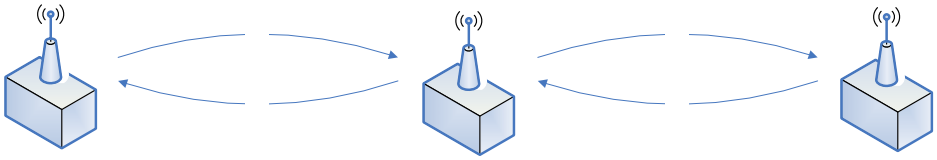


Figura 5. Flujo de la información en el nivel superior de la red debido a una alarma

El proceso de comunicación MZ - CC estará constituido por cuatro tramas. Tal como se observa en la Figura 5, cuando el MZ 0x33 decide enviar una alarma, primeramente buscará en su tabla de rutas la dirección inmediata de envío para llegar al CC. Al tener la dirección de envío, que para este ejemplo será 0x34, se transmite al RP 0x34 la trama de alarma T1.

Una vez que el RP recibe esta trama envía una trama de confirmación T2 al dispositivo remitente y se prepara, previa búsqueda de rutas para repetir la trama T3. En este ejemplo, la ruta de envío inmediata encontrada coincidirá con la dirección de destino.

Cuando el CC recibe la trama de alarma T3 envía una trama de confirmación de recepción al RP T4.

1.2.2. Tipos de Tramas

La estructura general de las tramas manejadas en el sistema se pueden ver en la Tabla 1, donde se nota que las tramas poseen inicialmente una cabecera que facilita el enlace entre dispositivos, luego poseen un campo de datos donde esta la función MODBUS que realmente es la que permite la operación y finalmente un código para detección de errores que permite verificar la integridad de los datos. Esté código consiste en un CRC de 16 Bits.

La cabecera de la trama de datos está estructurada de acuerdo con el protocolo desarrollado en el Trabajo de Grado elaborado por Roa, Boris. Este protocolo define el modo en que los datos llegan de un origen a su destino, define la Capa de Red del Modelo OSI. MODBUS esta encapsulado dentro de este protocolo [2].

La dirección de envío, de la cabecera de la trama de datos es la dirección del dispositivo auxiliar (Repetidor) que se emplea para llegar al destino que por limitaciones de potencia en los transceptores no se puede acceder directamente. La dirección de respuesta es la dirección del dispositivo que envía la trama y es utilizada luego como dirección de envío para la trama de confirmación. La dirección de destino es la dirección del dispositivo final que se quiere acceder. El tipo de trama describe el propósito de la operación y permite diferenciar las tramas desde el punto de vista de su función. El campo de datos es una función del protocolo MODBUS que se embebe dentro de esta estructura y que permite la lectura o escritura tanto de registros como de salidas de un dispositivo remoto [2].

Tabla 1. Estructura de la trama de datos

Dirección envío	**Dirección respuesta**	**Dirección destino**	**Tipo de trama**	**Datos**	**CRC-parte alta**	**CRC-parte baja**
Cabecera - 4 Bytes				Datos - 24 Bytes	Código de detección errores - 2 Bytes	

Tal como se observó en los ejemplos que describían el flujo de la información en el sistema existen Tramas de Solicitud, Tramas de Confirmación, Tramas de Repetición y Tramas de Alarma. Además de las mencionadas existe una trama cuya utilidad quedará más clara cuando se expliquen los tipos de alarmas. Esta es la Trama de Falla de Enlace que de manera similar a la Trama de Alarma se produce ante una situación anormal en el sistema, pero específicamente cuando el CC o algún RP no logra comunicarse con algún dispositivo destino o simplemente un elemento

encargado de la repetición de tramas. En el la Tabla 2 se describe de manera resumida la función de cada una de estas tramas dentro de la red.

Tabla 2. Descripción de los tipos de tramas de datos en la red inalámbrica

Tipo de Trama	Descripción
Repetición	Es la trama que envían los Repetidores cuando llega una solicitud cuyo destino es distinto a su dirección, y por lo tanto deben recibirla y posteriormente enviarla o repetirla al dispositivo destino.
Control o Configuración	Se emplea cuando el Centro de Control realiza querellas o recibe respuestas a estas, de solicitud de datos o configuraciones a los dispositivos del nivel superior de la red.
Confirmación	Se utiliza para confirmar la recepción de datos entre dispositivos inmediatos. Un dispositivo que envía datos a otro y espera recibir esta trama, sino es así repetirá el envío un número programado de veces, y de no recibir respuesta entonces producirá una alarma indicadora de falla en la comunicación
Falla de Enlace	Es la trama que se envía hacia el Centro de Control cuando un dispositivo que realiza una transmisión de datos no recibe la Trama de Confirmación. Esta trama contiene una alarma indicadora de la falla en la comunicación
Alarma	Se envía al Centro de Control cuando se producen violaciones a la seguridad o situaciones de riesgo en el sistema.

Las tramas de Falla de Enlace y Alarma que son los indicadores de errores o violaciones de seguridad en la red no emplean una función MODBUS como tal en el campo de datos debido a que este protocolo es maestro-esclavo, y por tal razón un esclavo no puede iniciar una comunicación sino ha sido interrogado por el maestro. Para evitar entonces que las alarmas tuvieran que ser leídas mediante un polling o chequeo del CC a todos los elementos del nivel superior de la red se implemento este reporte que como se señaló en la explicación del flujo de la información es la única circunstancia en la que la información fluye desde un elemento remoto hacia el Centro de Control.

Se emplea una función especial en el campo de datos cuando la trama es de Alarma o de Falla de Enlace. En la Tabla 3 se puede observar la estructura de esta función.

Tabla 3. Estructura de la función para la trama de alarmas de las alarmas.

Dirección del Dispositivo	Función	Tipo de Alarma	Numero del Sensor	Código personal-parte alta	Código personal-parte baja
	0x77				

La dirección del dispositivo es la dirección del elemento del nivel superior de la red que envía la alarma, la función es el identificador para este tipo de trama, el tipo de alarma es un número que indica cual alarma de las doce existentes ocurrió, el número del sensor es el identificador del sensor que detectó la violación si este es el caso, y el código personal sólo se utiliza si la alarma es enviada desde un Control de Acceso, e indica el usuario actual presente en la zona.

Una descripción más detallada del flujo de información en el sistema y de la estructura y tipos de tramas se puede encontrar en el Trabajo de Grado de Roa, Boris.

1.3. Tipo de Eventos y Alarmas Manejadas en el Sistema de Seguridad.

Debido a la naturaleza inalámbrica del Sistema de Seguridad se deben monitorear y registrar todos los sucesos relevantes que ocurren en la red, tanto los pertinentes a violaciones a la seguridad como los relativos al funcionamiento de los elementos que componen la red.

Para garantizar que se detectaran todas las violaciones a la seguridad que ocurran en la planta física donde se encuentre instalado el sistema se debe primero asegurar el funcionamiento permanente de los elementos que o componen, ya que eso es

físicamente imposible de garantizar, entonces se trata de que al memos se conozca cuando algún dispositivo de la red esta funcionando incorrectamente. Esto le aporta robustez y confiabilidad al Sistema de Seguridad.

Existen dos tipos de alarmas en este sistema: las alarmas que indican errores en el funcionamiento de los elementos de la red o errores en la comunicación; y las alarmas que indican violaciones o situaciones de riesgo en la planta física donde se encuentra instalado el sistema.

1.3.1. Alarma Dispositivo No Responde

El funcionamiento de los Módulos Sensores y Actuadores se supervisa desde los propios MZ. Estos módulos realizan un reporte periódico de su presencia y correcta operación. Cuando algún elemento deja de reportarse por más de dos períodos y el MZ determina en su lista de reportes que algún elemento activo esta ausente, este envía hacia el Centro de Control una alarma denominada "Dispositivo Nº (Número del Sensor) No Responde" en esta trama de datos se indica el dispositivo que no se reportó y la zona a la cual pertenece.

Esta alarma se puede generar debido a que se halla agotado la batería del dispositivo, por deterioro del hardware, o en la peor situación, que el dispositivo halla sido removido de su posición. En cualquiera de estos casos debería verificarse la integridad física del dispositivo en cuestión.

De manera similar, el funcionamiento de los MZ, RP y CA también es supervisado, pero desde el Centro de Control. En este caso, es el CC el que realiza una supervisión periódica de la operación de estos elementos a través de una querella para leer el nivel de tensión de su batería. Los elementos de la red de nivel superior poseen un registro interno de operación donde se almacena el valor porcentual de su batería. Cuando alguno de estos elementos no atiende o no responde a la solicitud

entonces se genera la alarma “Dispositivo No Responde”, de manera similar, al producirse esta alarma debería verificarse la integridad física del dispositivo.

1.3.2. Alarma de Sensor Violentado

Para garantizar la integridad de los elementos de la red de nivel inferior, para que no sean removidos o retirados de sus posiciones sin previa autorización estos cuentan con un pequeño sistema de autoprotección que consiste en un switch el cual está “cerrado” permanentemente mientras estos permanecen pegados a la pared y que pasa a estado “abierto” al ser separados de ésta.

Si un módulo activo es removido este transmite una señal a su Maestro de Zona correspondiente, el cual envía un alarma denominada “Sensor Nº (Número del Sensor) Violentado” al Centro de Control. Esta alarma indica, además del evento ocurrido, la zona y el número del sensor que fue retirado de su lugar.

1.3.3. Alarma de Desconexión de Línea

Los dispositivos de la red de nivel superior son los únicos elementos en el sistema que requieren estar energizados, ya que aunque poseen baterías y estas son recargables, solo alimentan al dispositivo cuando ocurre un corte de energía.

Cuando es retirada o cortado el cable de alimentación de algún MZ, RP o CA estos transmiten una alarma al Centro de Control denominada “Desconexión de Línea”. Esta trama contiene los datos del dispositivo al que le fue retirada la energía.

1.3.4. Alarma de Falla de Enlace

La certeza de que una configuración llegara desde el CC a un elemento de la red de nivel superior y que además, las alarmas llegaran desde estos elementos hasta el

Centro de Control depende de la efectividad en la comunicación en el nivel superior de la red. Esta efectividad se monitorea desde el CC a través de alarmas creadas para la detección de fallas en los enlaces

Tanto los Maestros de Zona como los Controles de Acceso pueden pasar, o no a través de un Repetidor para comunicarse con el Centro de Control. Cuando el CC, que es el que inicia las comunicaciones para operaciones de configuración o control, no puede comunicarse, o cuando un RP no logra repetir la información que le es enviada, se produce una alarma denominada "Falla de Enlace". Esta alarma es enviada por elemento que intento comunicarse y no lo logro, al CC.

1.3.5. Alarma de Rutas Agotadas

Como se menciono las rutas de acceso son múltiples, si falla el enlace con una ruta, los dispositivos proceden a buscar la próxima ruta. Si estas rutas se agotan y el dispositivo finalmente no puede comunicarse se produce la alarma "Rutas Agotadas". Esta alarma es enviada por el dispositivo cuyas rutas disponibles se agotaron sin lograr establecer la comunicación al CC.

1.3.6. Alarmas de Módulos Sensores

Cuando se producen violaciones de seguridad al espacio físico donde se encuentran los Módulos Sensores o al existir situaciones de riesgo, estos envían una señal al MZ que enviara la alarma "Alarmas de Sensores" al CC. En el contenido de esta alarma se encuentra tanto la zona (número del MZ donde está habilitado el sensor) como el número del sensor que detectó la violación o situación de riesgo.

1.3.7. Alarma Entrada de Usuario y Salida de Usuario

Este evento no es propiamente una alarma, ya que el acceso de un usuario, con su respectiva clave, a una zona controlada por un Control de Acceso no es una violación a la seguridad, pero se creó con el propósito de que sea posible tener un registro del tráfico en los CA. Al entrar o al salir un usuario, el CA correspondiente enviará esta alarma al CC. Esta alarma contiene el número del usuario, la acción que está realizando y la zona a la que está accediendo.

1.3.8. Alarma Acceso Denegado.

Esta alarma ocurre en las zonas controladas por un CA, cuando un usuario que no está autorizado en una zona intenta emplear su control remoto para acceder a dicha zona. Esta alarma contiene el número del usuario y la zona a la que está intentando acceder.

1.3.9. Alarma de Pánico en un Control de Acceso

Cada control de remoto que se emplea para acceder a una zona especifica posee además de una clave válida, una código que le permite indicar cuando un usuario es obligado a acceder a una zona controlada. Cuando un usuario es forzado a entrar a una zona en la que posee autorización, éste puede enviar esta clave al CA que enviara al CC la alarma de pánico que indicara la situación de riesgo.

1.4. Dimensiones de la red

El tamaño de la red de nivel superior atiende a los límites impuestos por el número de elementos que pueden ser direccionados con el protocolo MODBUS. De manera que el máximo número de dispositivos que pueden existir en este nivel son 247. Este

número es la cantidad total de Maestros de Zona, Repetidores y Controles de Acceso que soporta la red.

La red de nivel inferior soporta hasta 64 Sensores y 64 Actuadores. Los límites de esta red están impuestos por razones prácticas, ya que se consideró suficiente la cantidad de 64 sensores por zona.

CAPITULO II:

CENTRO DE CONTROL DEL SISTEMA DE SEGURIDAD

El Centro de Control (CC) es el elemento central de la red donde llegan todas las alarmas que ocurren en el sistema. Desde este dispositivo se ejecutan las acciones de control programadas como respuesta a las violaciones de seguridad, y además se configuran de manera remota todos los elementos que componen el sistema.

Considerando el número de zonas y el número de sensores que pueden manejarse en este sistema de seguridad se concluirá que es más sencillo dejar el control y el monitoreo de los elementos de la red a una PC convencional, pero debido a la baja confiabilidad que muestran algunos sistemas operativos para el servicio continuo se decidió finalmente, crear el Centro de Control en base a microcontroladores.

Aunque se decida seleccionar un sistema operativo robusto para el centro de control de la red, éste se debe diseñar con redundancia, por lo menos doble para garantizar la confiabilidad y esto puede encarecer el costo final del sistema.

El Centro de Control diseñado está constituido por dos elementos. Por un software que se ejecuta desde un computador personal, que es la Interfaz de Usuario y que permite la visualización del estado de los dispositivos, y por un hardware denominado Unidad de Control, este dispositivo opera de manera autónoma al computador según la configuración programada, y es capaz de realizar las acciones de monitoreo y control de los dispositivos de la red.

La Interfaz de Usuario es un programa desarrollado en LabView 7.1 para Windows y emplea algunas de las potencialidades que ofrece el módulo SCADA:

LabView DSC 7.1, entre las cuales tenemos la base de datos en tiempo real, la base de datos histórica y las consultas a la base de datos.

El monitoreo en tiempo real de las alarmas que ocurren en todo el sistema y el tráfico en las zonas controladas por un Control de Acceso se pueden visualizar desde la Interfaz de Usuario, a la vez que estos datos se van almacenando en una base de datos para tener un registro histórico de todos los eventos. Desde la Interfaz también se configuran los elementos del nivel superior de la red, las secuencias de eventos y alarmas que producirán las acciones de control y además es posible enviar funciones MODBUS a los elementos del nivel superior de la red.

La Unidad de Control está desarrollada en base a microcontroladores PIC y memorias E2PROM, unidos a través de un bus multimaestro I2C. Un transceptor de 2.4 GHz es el elemento que permite la comunicación entre el CC y los MZ, RP y CA.

La recepción de las alarmas y la ejecución de las acciones de control se realizan desde la Unidad de Control. Estas acciones pueden ejecutarse independientemente de la Interfaz de Usuario, de manera que la principal operación del sistema no depende del funcionamiento del computador. Esto le aporta autonomía al equipo ante las posibles fallas de funcionamiento que puede presentar un PC convencional.

2.1. Unidad De Control

La Unidad de Control es el hardware del CC donde converge la información de todas las alarmas y eventos que se producen en el sistema de seguridad. Tiene la función de supervisar la operatividad de los elementos de la red, recibir y almacenar las alarmas, gestionar la configuración de los dispositivos y ejecutar las acciones de control programadas cuando se producen las alarmas. Aunque la Unidad de Control posee autonomía para operar, toda su configuración se realiza desde la Interfaz de Usuario.

La Unidad de Control está conformada por varios módulos con tareas distribuidas que comparten información a través de un bus serial multimaestro I2C. Los maestros están conformados por los tres microcontroladores de medianas prestaciones y los esclavos constituyen las memorias. La distribución de las operaciones que realiza el Centro de Control por módulos separados físicamente facilitó la programación de todas las funciones que es capaz de ejecutar este dispositivo

La Unidad de Control está diseñada con una topología tipo bus, como puede observarse en el Gráfico 1. El bus es el que permite la interconexión y el intercambio de datos entre los distintos módulos del sistema.

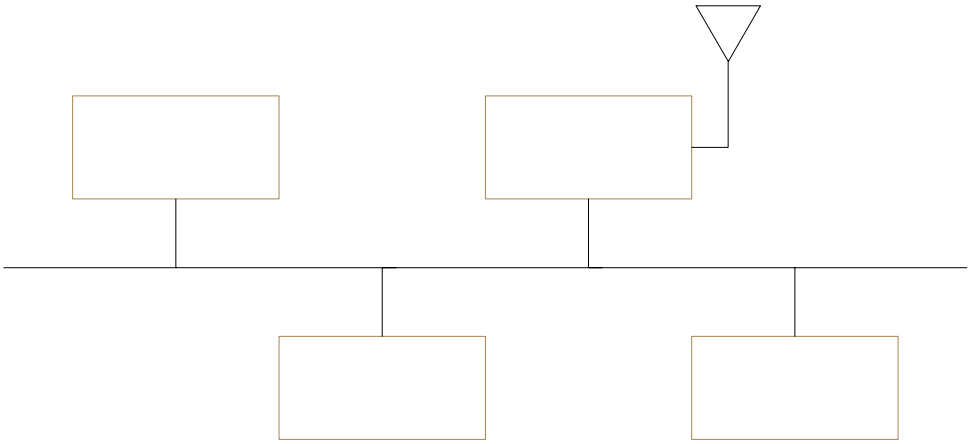


Gráfico 1. Arquitectura de la Unidad de Control

Para acceder al bus multimaestro I2C se debe tomar previamente el mando de éste. El que posee el control del bus genera la señal de reloj y el resto de los maestros deben sincronizarse con esta. Sólo un microcontrolador puede realizar operaciones de lectura o escritura en las memorias a la vez. Para evitar colisiones, mientras se intenta tomar el mando del bus, los microcontroladores esperan el bit de stop de la trama de

datos del protocolo I2C. El bit de stop indica que las operaciones sobre el bus finalizaron y que éste se encuentra libre.

Cuando un maestro detecta que el bus está libre espera un tiempo e intenta acceder al medio. El hardware del propio microcontrolador posee capacidad de detección de colisiones, de manera que si al intentar tomar el control del bus se produce una colisión el microcontrolador correspondiente deja libre el bus y reinicia la operación que deseaba realizar esperando nuevamente que el bus este libre. Esto lo realizará hasta completar su operación.

Los módulos que conforman la Unidad de Control son los siguientes: el Módulo de Almacenamiento donde se guarda la configuración de la Unidad, las alarmas recibidas y las solicitudes para posteriormente enviarlas, el Módulo de Comunicaciones que maneja el transceptor que recibe las alarmas y permite enviar las solicitudes pendientes, el Módulo de Interfaz que facilita la comunicación entre la propia Unidad de Control y la Interfaz de Usuario, y el Módulo de Alarmas donde se procesan las alarmas y se inicia la ejecución de las acciones de control.

2.1.1. Módulo de Almacenamiento

El Módulo de Almacenamiento está conformado por ocho memorias seriales E2PROM que son esclavos en el bus. El resto de los módulos puede realizar operaciones de lectura o escritura en las memorias.

Cada memoria posee una capacidad de 64 KBytes, el máximo número de memorias que es posible incorporar al bus es ocho, de manera que la capacidad del módulo es de 512 KBytes, pero por características del protocolo de datos que se implementó en el sistema las memoria se manejan como si su longitud fuera de 16 bits por lo cual la capacidad útil se reduce a la mitad. La capacidad disponible es de 256K x 16.

Un segmento, en la primera de las ocho memorias de 64 KBytes está destinado para el almacenamiento de los datos de las solicitudes enviadas desde la Interfaz de Usuario. Estas solicitudes serán primeramente escritas en las memorias por el Módulo de Interfaz para posteriormente ser leídas y enviadas a su destino por el Módulo de Comunicaciones. Este segmento de memoria se denomina Memoria de Solicitudes. Su contenido se puede visualizar en la Gráfica 2.

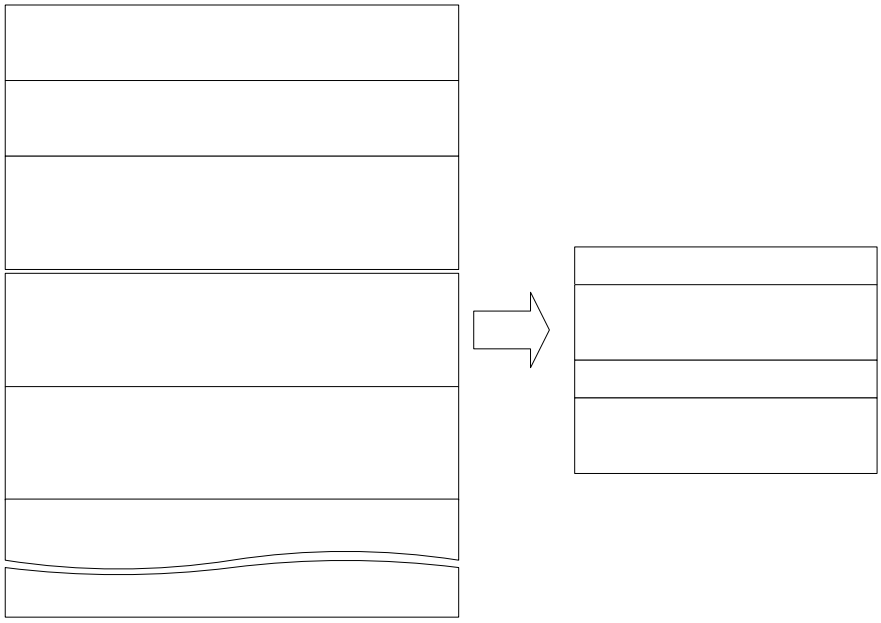


Gráfico 2. Distribución de la información en la Memoria de Solicitudes

El primer word[1] de esta memoria contiene la dirección de la última solicitud escrita desde la Interfaz, y el word siguiente contiene la dirección de la última solicitud leída y enviada a través del Módulo de Comunicaciones. Esta estructura permite almacenar, sin perder las solicitudes de configuración o de datos, en el caso que la Unidad de Control este ocupada verificando el estado de los dispositivos del nivel superior de la red o recibiendo las alarmas que podrían ocurrir, y no pueda enviar inmediatamente alguna solicitud.

[1] En el área de Sistemas Digitales se denomina word a la unión de dos bytes

Almacenar las solicitudes en la memoria manejándola como un stack[2] permite que no exista pérdida de datos y además prolonga los ciclos de escritura de la memoria E2PROM. Para volver a escribir una solicitud en la misma dirección se debe alcanzar el límite físico establecido para este segmento de memoria, esto reiniciara el puntero a la primera posición de la memoria y comenzaran a reescribirse los datos de las solicitudes anteriores.

El segmento restante, en la primera memoria de 64 KBytes está destinado a los datos de configuración del propio Centro de Control. Los valores de registros internos de operación, las tablas que contienen los dispositivos operativos en el nivel superior de la red y que deben ser verificados periódicamente, las tablas de rutas para comunicarse con estos dispositivos, las secuencias de las alarmas que deben ocurrir para que se ejecuten las acciones de control y las acciones de control propiamente, son los datos contenidos en esta porción de la memoria denominada Memoria de Configuración. Su contenido se puede visualizar en la Gráfica 3

Las siete restantes memorias del Módulo de Almacenamiento están destinadas para las alarmas. Este bloque se denomina Memoria de Alarmas y es el de mayor capacidad. Permite almacenar las alarmas que han ocurrido tanto para ser presentadas en la Interfaz de Usuario como para ser verificadas y procesadas por el Módulo de Alarmas que ejecutará las acciones de control pertinentes.

[2] En el área de Sistemas Digitales se denomina stack a la forma de ordenar los datos de manera apilada

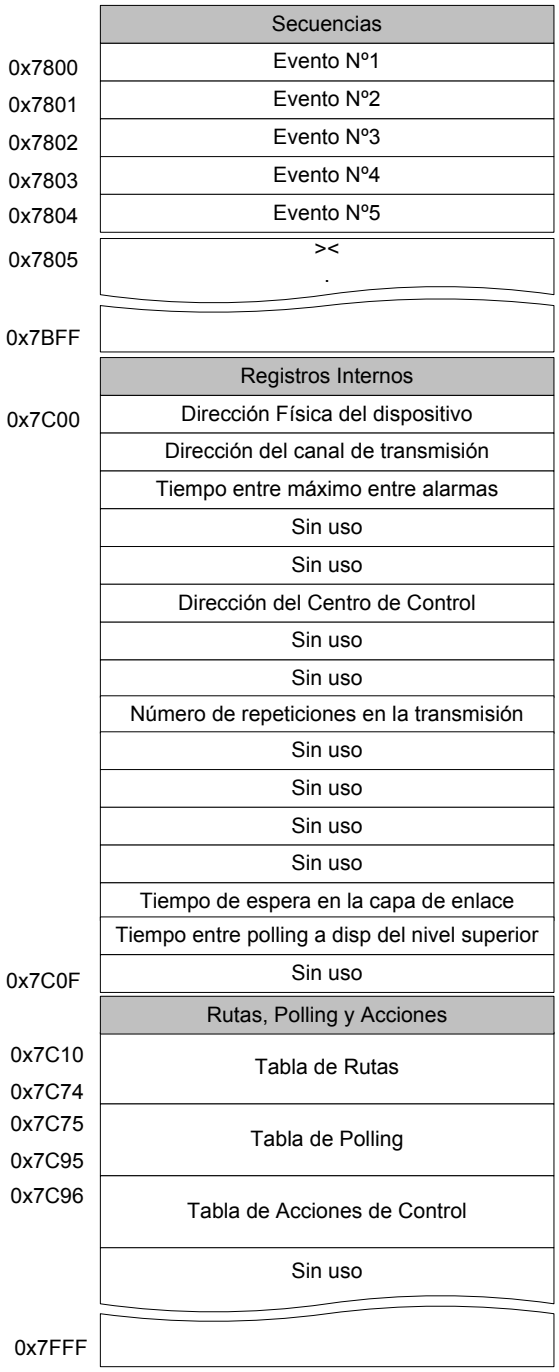


Gráfico 3. Distribución de la información en la Memoria de Configuración

La Memoria de Alarmas permite almacenar las alarmas mientras estas son leídas por el Módulo de Interfaz para ser presentadas luego en la Interfaz de Usuario, de manera que si la Interfaz no se esta ejecutando en el computador personal estas alarmas podrán ser leídas luego para presentarlas y almacenarlas en la base datos de la Interfaz de Usuario, con el inconveniente de que el registro de tiempo que acompañara a cada alarma ya no será del momento en que ocurrió, sino del momento en que es leído. Por esta razón es conveniente, aunque no crítico que el computador donde se ejecuta la Interfaz de Usuario este permanentemente operativa y conectada a la Unidad de Control.

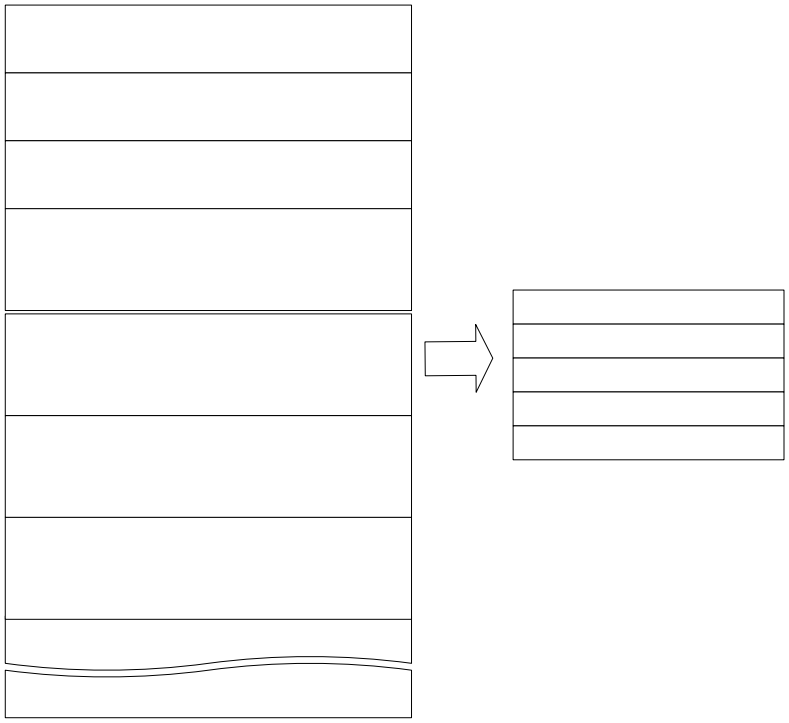


Gráfico 4. Distribución de la información en la Memoria de Alarmas

En el primer word del bloque de Memoria de Alarmas se encuentra la dirección de la última alarma que llego a la Unidad de Control y que almacenó el Módulo de Comunicaciones. En el siguiente word se encuentra la dirección de la última alarma leída y enviada la Interfaz de Usuario por el Módulo de Interfaz. En el tercer word se

0x0000 Dirección de la ultima alarma (por MC)

0x0001 Dirección de la ultima alarma (por MI)

0x0002 Dirección de la ultima alarma para leida (por MA)

0x0003 Sin Uso

encuentra la dirección de la última alarma procesada por el Módulo de Alarmas para ejecutar las acciones de control. En al Gráfica 4 se puede observar el contenido de la Memoria de Alarmas.

Los words que se encuentran al inicio de las memorias contienen los punteros de direcciones tanto en la Memoria de Solicitudes como en la Memoria de Alarmas, y permiten determinar cuales configuraciones han sido ejecutadas y/o cuales alarmas han sido procesadas.

2.1.2. Módulo de Comunicaciones

Este módulo está constituido por un microcontrolador PIC de Microchip de la familia 18, específicamente el PIC18LF248. Emplea un puerto de ocho bits para comunicarse con el transceptor de 2.4 GHZ y está conectado al bus serial I2C del cual es uno de los maestros. El Módulo de Comunicaciones es el elemento que le permite a la Unidad de Control comunicarse con el resto de los elementos de la red.

Tres tareas son monitoreadas permanentemente por el Módulo de Comunicaciones. Realiza un polling[3] de los dispositivos del nivel superior la red, verifica si han llegado nuevas alarmas y además comprueba si existen nuevas solicitudes que deben ser enviadas.

El polling se realiza con el fin de verificar la operatividad de los dispositivos del nivel superior de la red. Es configurable la lista de los dispositivos que serán chequeados y el tiempo entre polling. La consulta consiste en la lectura del registro donde se encuentra el valor de la batería de los MZ, RP y CA.

[3] En el área de Sistemas Control se denomina polling a la consulta realizada a los dispositivos por un elemento maestro

Algunos sistemas, como los SCADA que tienen implementado el protocolo MODBUS utilizan el método del polling para actualizar en la memoria del control central, un conjunto de datos de los elementos esclavos, esto requiere memorias de alta densidad para almacenar este volumen de datos. En la Unidad de Control solo se almacenan como alarmas los datos de los dispositivos que no respondan al polling o cuyo nivel de batería este por debajo del límite establecido.

Una vez que el tiempo entre verificaciones se cumple, el Módulo de Comunicaciones lee una a una las direcciones de los dispositivos que serán chequeados en la Tabla de Polling y envía una solicitud para lectura del estado de su batería empleando la función MODBUS de lectura de registros. El nivel de la batería de cada dispositivo debe ser mayor a 80 % para considerar que el dispositivo está plenamente operativo, de no ser así o de no recibir respuesta a la solicitud el Módulo de Comunicaciones almacena una alarma en la Memoria de Alarmas indicando que el dispositivo no responde.

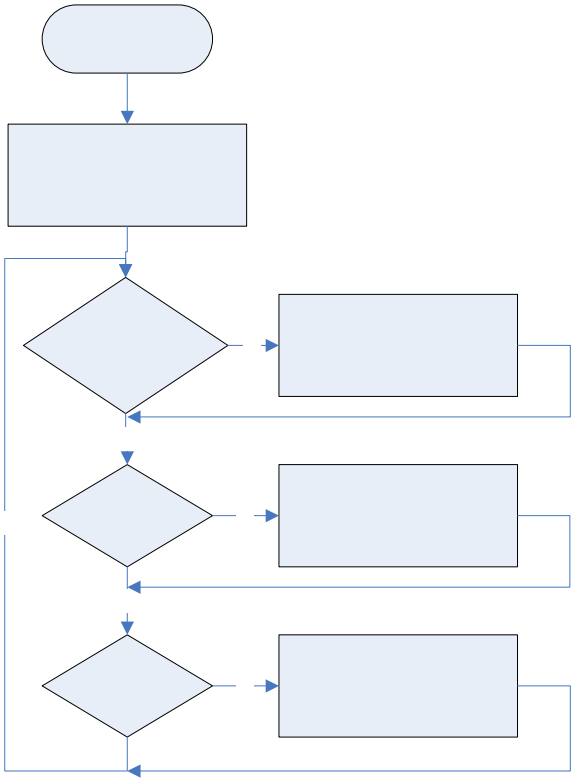


Figura 6. Diagrama de flujo simplificado del funcionamiento del Módulo de Comunicaciones

Para comunicarse con los dispositivos de la red, el Módulo de Comunicaciones tiene implementado la capa de enlace y la capa de red del protocolo de comunicaciones inalámbrico desarrollado para el sistema de seguridad. Este Módulo posee la capacidad de gestionar una comunicación a través de múltiples Repetidores para enlazar el CC con cualquier elemento del nivel superior de la red. Para lograr el enlace entre dispositivos el CC emplea las Tablas de Rutas (dirección 0x7C10) que se encuentran en la Memoria de Configuración.

Las tablas de rutas son un conjunto de words donde el primer byte representa la dirección de destino que se quiere acceder y el siguiente representa la dirección de envío inmediata que permite llegar al destino. Si se desea acceder a un dispositivo destino, el algoritmo que posee el Módulo de Comunicaciones realiza una búsqueda en la tabla para comparar la dirección del dispositivo destino con el primer byte de todos los words de la tabla, cuando encuentra coincidencia toma el byte siguiente del word como la dirección de envío inmediata. Las Tablas de Rutas con configurables desde la Interfaz de Usuario y poseen al memos una ruta para acceder desde el Centro de Control a algún dispositivo del nivel superior de la red.

El Módulo de Comunicaciones también posee un algoritmo para el manejo del transceptor que consiste en una comunicación sincronizada con un reloj generado por el propio microcontrolador.

El transceptor empleado en la Unidad de Control es el nRF2401 de NORDIC Semiconductor. Funciona en modo ShockBurst, tecnología que consiste en el uso de un stack interno FIFO que recibe la data sincronizada con un reloj a baja velocidad de transmisión y luego la envía a una altísima velocidad de transmisión (1 Mbps) permitiendo reducción de potencia en la transmisión. En este modo la comunicación

con el transceptor se realiza usando una interfaz de 3 vías donde la velocidad es fijada por el microcontrolador.

Las alarmas que se producen en el sistema, tal como se menciono en la descripción del flujo de la información, tendrán como dirección de destino al Centro de Control. Estas alarmas llegan por uno de los dos canales que posee el transceptor y que esta dedicado exclusivamente para el manejo de alarmas. Una vez que la alarma llega al Módulo de Comunicaciones y este comprueba su existencia, se guarda en la Memoria de Alarmas en la posición siguiente a la indicada por el puntero que se encuentra en el primer word de esta memoria, luego incrementa este puntero y lo almacena en su respectiva posición. De esta manera se guardan tanto las alarmas entrantes como su ubicación dentro de la memoria.

Para saber si existen nuevas solicitudes en la Memoria de Solicitudes, el Módulo de Comunicaciones solo debe leer los dos primeros words de esta memoria que contienen: la dirección de la ultima solicitud escrita por el Módulo de Interfaz y la dirección de la ultima solicitud leída y enviada por el Modulo de Comunicaciones. Si la dirección de la última solicitud escrita es mayor a la de la última solicitud leída entonces hay solicitudes pendientes. El Módulo de Comunicaciones leerá cada solicitud y la enviara a su destino empleando las Tablas de Rutas, finalmente actualizara el puntero indicador de la última solicitud leída.

2.1.3. Módulo de Interfaz

El Modulo de Interfaz está desarrollado con un microcontrolador PIC 16 de Microchip, específicamente el PIC16LF876. Emplea el UART del microcontrolador para comunicarse con el PC y el módulo I2C para conectarse al bus del cual es uno de los maestros.

El Módulo de Interfaz tiene implementado el protocolo MODBUS en modo RTU y es capaz de conectarse no solo a la Interfaz de Usuario sino a cualquier programa de monitoreo de remotas MODBUS. El Modulo de Interfaz solo funciona cuando se envía algún comando MODBUS desde la Interfaz de Usuario, de lo contrario este Módulo no interviene en ninguna operación en la Unidad de Control.

Solo la dirección de esclavo uno está reservada, ya que cuando se apunta a esta se accede a la Unidad de Control, de esta manera se configuran los registros internos y las tablas de la esta unidad desde la Interfaz de Usuario haciendo uso de funciones del protocolo MODBUS.

Cuando el Módulo de Interfaz recibe alguna función de lectura o escritura de registros o salidas, que son las operaciones que permiten las funciones MODBUS, éste la lee, verifica el código de detección de errores en la trama recibida y posteriormente comprueba la dirección del dispositivo que se desea acceder y el tipo de operación que se desea realizar. Una vez que identifica la validez de estos parámetros, el Módulo de Interfaz almacena en la Memoria de Solicitudes los siguientes datos: dirección del dispositivo, dirección de los registros o salidas para lectura o escritura, número de registros o salidas, valor de los registros o salidas y la dirección en la memoria donde los está almacenando, en el puntero de la ultima solicitud escrita (word cero de la Memoria de Solicitudes). Luego dependerá del Módulo de Comunicaciones identificar que existe una nueva querella y enviarla según el protocolo de comunicaciones, tal como se explicó anteriormente.

Cuando el Módulo de Comunicaciones recibe la respuesta a una solicitud guarda el contenido de la respuesta en la misma posición de memoria donde se encontraba la solicitud, y es así como el Módulo de Interfaz lee los datos de la respuesta a la solicitud que envío. Si no se recibe tal respuesta el Módulo de Comunicaciones producirá y almacenara una alarma (Dispositivo No Responde) y el Módulo de Interfaz no tendrá respuesta alguna para enviar a la Interfaz de Usuario quien por

límite de tiempo le enviara un aviso al usuario indicando que no fue posible completar la operación.

2.1.4. Modulo de Alarmas

Este módulo está desarrollado con un microcontrolador PIC de la familia 18 de Microchip, específicamente el PIC18LF248, del cual emplea el modulo I2C para conectarse al bus del cual es uno de los maestros. El Módulo de Alarmas es el que ejecuta las acciones de control una vez que ocurren las alarmas programadas.

El Módulo de Alarmas contiene las Tablas de Secuencias de eventos. Estas tablas, separadas por las zonas asignadas a cada maestro comprenden un conjunto de words donde el primer byte especifica el tipo de alarma o evento ocurrido y el byte siguiente el número del sensor, lo cual permite discriminar tanto el sensor que produjo la alarma como el tipo de alarma que ocurrió. Las Tablas de Secuencias configurables desde la Interfaz de Usuario permiten agrupar conjuntos de cinco eventos que una vez que ocurran provocaran que se ejecuten las acciones de control, esto disminuye la probabilidad que se realicen las acciones por falsas alarmas que puedan ocurrir.

El Módulo de Alarmas está permanentemente verificando los punteros que existen en la Memoria de Alarmas para leer las nuevas alarmas que llegan a la Unidad de Control. Cada vez que llega una nueva alarma este módulo verifica si la alarma está contenida dentro de alguna secuencia de la diez posibles y luego verifica posteriormente si el evento anterior sucedió, de ser así el evento ocurrido es considerado como válido. Una vez que las alarmas de una secuencia están completas entonces se generan las acciones de control específicas de la zona donde ocurrió la violación.

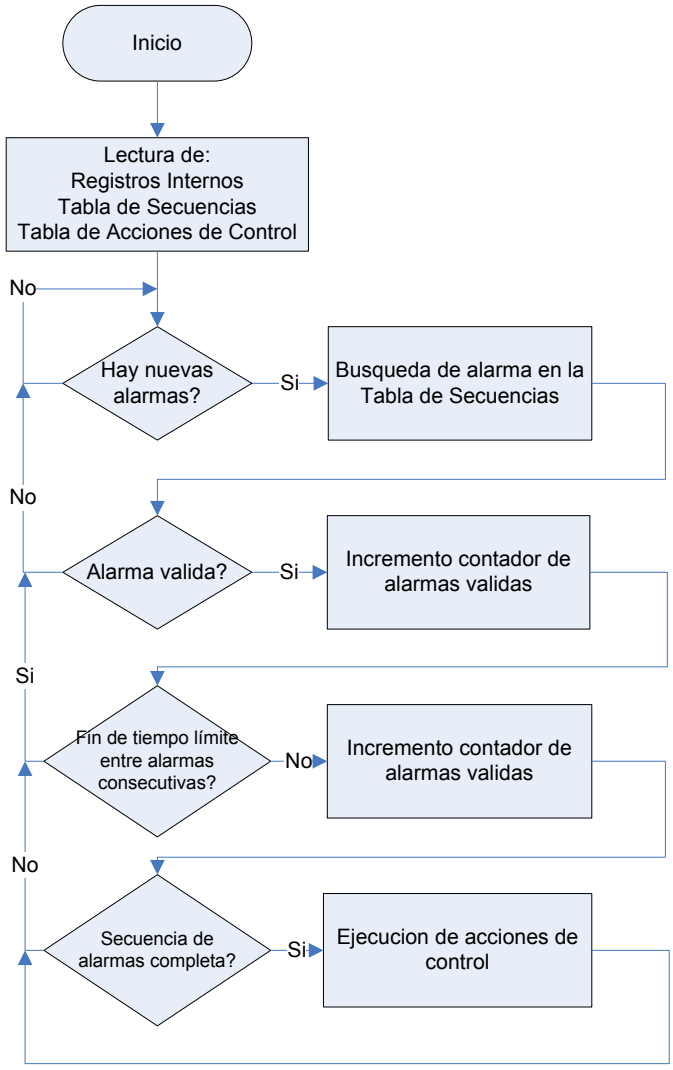


Figura 7. Diagrama de flujo del funcionamiento del Módulo de Alarmas

Las acciones de control comprenden la habilitación de algunas salidas en los Maestros de Zona o en los Módulos Actuadores. A estas salidas pueden estar conectados buzzer o sirenas. Las acciones de control también son programables desde la Interfaz de Usuario, es posible programar cuales salidas serán habilitadas en un Maestro de Zona cuando se cumpla alguna secuencia de alarmas.

Las acciones de control una vez programadas en la Interfaz de Usuario son almacenadas en la Memoria de Configuración, y de allí son cargadas a la memoria RAM del Módulo de Alarmas. Para ejecutar las acciones de control el Módulo de Alarmas envía una solicitud a la Memoria de Solicitudes con los parámetros de la función MODBUS escribir múltiples salidas. Esta solicitud será leída y enviada a su destino por el Módulo de Comunicaciones.

Entre una alarma y otra existe un tiempo de ocurrencia programable desde la Interfaz de Usuario, denominado Tiempo Máximo entre Alarmas. Si se cumple este tiempo y la alarma siguiente en cualquier secuencia no ocurre entonces se reinicia nuevamente el contador de secuencias, ya que esta situación indica que la alarma ocurrida era falsa.

Los eventos de la secuencia de alarma son programables y variables en longitud. Es posible programar secuencias de uno hasta cinco eventos. Esto permite que alarmas críticas, como la de incendio, no requieran un evento adicional para iniciar las acciones de control.

2.1.5. Valores Configurables en la Unidad de Control

En las siguientes tablas se muestran la lista de los parámetros que se pueden configurar en la Unidad de Control junto con los valores límites de estas variables

Tabla 4. Valores de Configuración

Parámetros Configurables	**Valor Mínimo**	**Valor Máximo**
Dirección del Centro de Control	0	247
Número de repeticiones por trama de envío/confirmación	0	255
Tiempo de espera por respuesta en la capa de enlace (Con base de tiempo de 50 milisegundos)	0	65535
Tiempo entre polling a dispositivos del nivel superior de la red (Con base de tiempo de 1 minuto)	0	65535
Tiempo máximo entre alarmas consecutivas de una secuencia (Con base de tiempo de 1 minuto)	0	65535
Dirección física del dispositivo	0	255
Canal	0	255

Tabla 5. Capacidad de almacenamiento de la Unidad de Control

Parámetro	**Valor**
Numero de alarmas que puede almacenar la Unidad de Control	8000
Zonas que puede gestionar el dispositivo (Incluye MZ, RP y CA)	246
Sensores y Actuadores por Zona	64

CAPITULO III:

INTERFAZ DE USUARIO

La Interfaz de Usuario es un programa de computación que permite la configuración de los elementos del nivel superior de la red y de la Unidad de Control empleando funciones MODBUS. Esta Interfaz genera una base de datos en tiempo real de las alarmas que ocurren en el sistema y una base de datos histórica tanto de alarmas como del tráfico de usuarios en los Controles de Acceso.

EL lenguaje de programación empleado para el desarrollo de la Interfaz de Usuario es LabView 7.1 y el módulo LabView DSC 7.1. [3]-[4].

3.1. El Lenguaje de Programación LabView y el Módulo DSC

LabView es un lenguaje de programación gráfico que usa iconos en lugar de líneas de texto para crear aplicaciones. En contraste con los lenguajes basados en texto, donde las instrucciones determinan la ejecución, LabView emplea programación por flujo de datos, donde el flujo de la información determina la ejecución [3].

LabView DSC es un módulo que se le agrega a una licencia convencional de LabView para facilitar y acelerar el desarrollo de aplicaciones SCADA/ HMI con el lenguaje de programación LabView.

El módulo LabView DSC extiende el entorno de desarrollo gráfico de LabView para facilitar el diseño eficiente de sistemas distribuidos de medición, control y monitoreo de grandes cantidades de señales de entrada o salida. El módulo DSC

permite agregarle a cada variable de entrada/salida alarmas, escalas y seguridad, a la vez que almacena en forma automática su valor [4].

Una aplicación desarrollada con el modulo DSC posee la estructura de la Figura 8 [4].

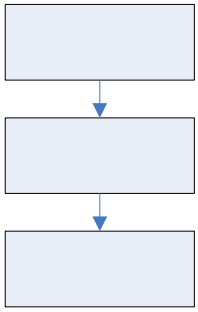


Figura 8. Estructura de una aplicación DSC

La Interfaz Gráfico es la presentación de la aplicación donde es posible monitorear cada tag (variable de entrada o salida). La Máquina Virtual o Tag Engine arranca el servidor, procesa las variables que son servidas por el Servidor de Datos, además procesa y almacena las alarmas y eventos en la base de datos.

3.1.1. Creación de Tag's en el modulo DSC

Los tag's son las entradas o salidas que existen físicamente en un sistemas y que desean monitorear en la aplicación desarrollada con DSC. Para la creación de los tag's se debe emplear el Configure Tag disponible en la barra de herramientas de LabView en Tools/ DSC module. La ventana de configuración de los tag's se puede ver en la Figura 9 [4].

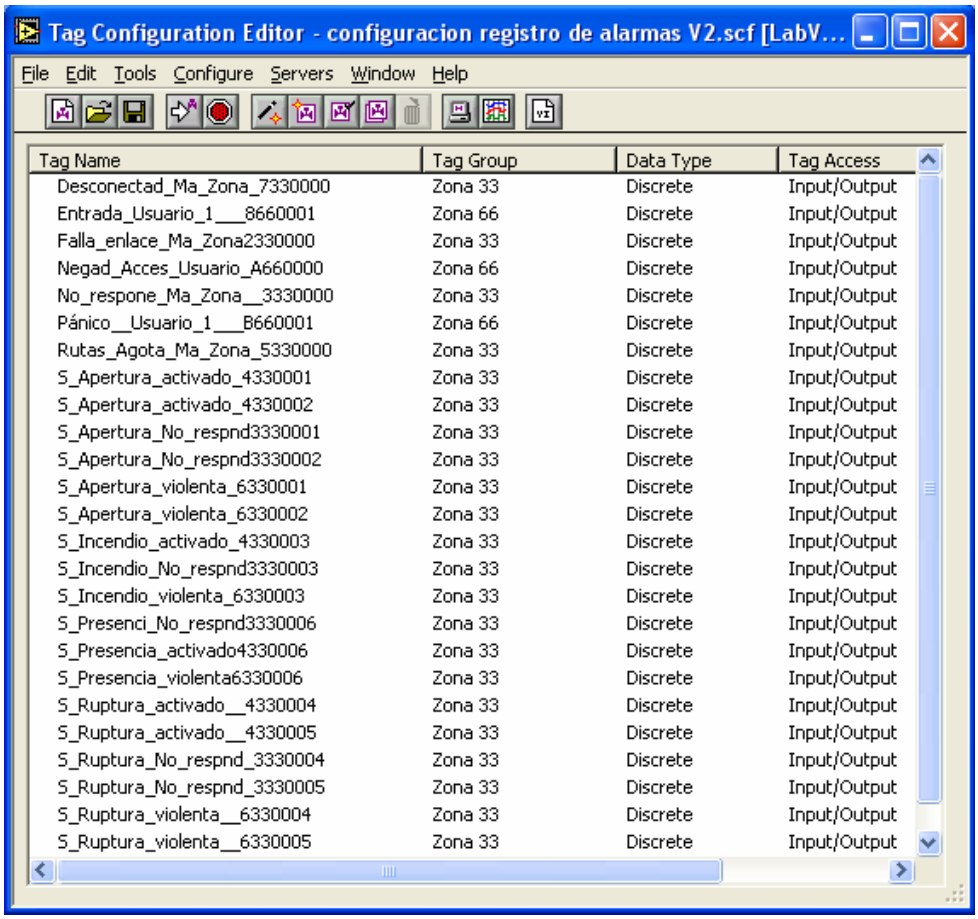


Figura 9. Ventana de Configuración de Tag's.

Desde esta ventana se crean y configuran todas las entradas o salidas que se desean monitorear. En Edit/Create se selecciona el tipo de variable: analógica, discreta, bit array o string, que se le asignara al tag. Además se configuran las opciones de almacenamiento y límites para los valores de alarma.

3.1.2. Interfaz Gráfica.

Para visualizar el estado de los tag's definidos en la interfaz gráfica de una aplicación DSC se pueden emplear las funciones disponibles en la paleta de funciones de LabView, Figura 10.

Figura 10. Funciones para la visualización de las alarmas en el módulo DSC.

La Función Summary permite visualizar solo las alarmas actuales, mientras que la Función History permite crear un registro de todas las alarmas y de todos los eventos ocurridos desde el inicio de la ejecución de la aplicación. La Función Display no solo muestra las alarmas sino que también permite su confirmación. Estas funciones se emplean para la visualización en tiempo real del estado de los tag's [4].

3.1.3. Base de datos Citadel.

El módulo DSC almacena los datos de alarmas y eventos en la base de datos Citadel. Esta base de datos funciona con un controlador ODBC (Open Data Base Conectivity) que permite conectarse a una base de datos concreta fuera del ambiente de LABVIEW. De manera que para la consulta de datos pueden emplearse otra aplicación que maneje controladores ODBC. El tamaño máximo de esta base de datos es de 2 Gbytes [4].

La Conectividad abierta de base de datos de orígenes de datos (ODBC) permite tener acceso a datos desde una gran variedad de sistemas de administración de bases de datos. Por ejemplo, si tiene un programa que obtiene acceso a los datos de una base de datos de SQL, Orígenes de datos (ODBC) le permitirá usar el mismo programa para tener acceso a los datos de una base de datos de Visual FoxPro. Para ello, debe agregar componentes de software al sistema, llamados controladores. Orígenes de datos (ODBC) le ayuda a agregar y a configurar estos controladores [5].

3.1.4. Servidor de Datos

Un servidor en el módulo DSC es una aplicación que se comunica con los tag's registrados y los hace disponibles al Tag Engine para su procesamiento. El módulo DSC permite distintos tipos de servidores: OPC, DDE y VI's basados en servidores.

OPC (OLE for Process Control) es una norma industrial creada con la colaboración de los principales suplidores de equipos de control y software, los cuales trabajan en cooperación con Microsoft. OPC hace una conexión entre los proveedores de hardware y los diseñadores de software. El provee un mecanismo para obtener datos de una fuente de datos y comunicarlos a cualquier aplicación del cliente de una forma estándar.

DDE es una forma de comunicación entre procesos implementada en la familia de sistemas operativos Microsoft Windows. Los programas compatibles con el intercambio dinámico de datos (DDE, Dynamic Data Exchange) pueden intercambiar información y comandos [5].

3.1.5. LabView VI's como DDE Server

Es posible crear en LabView un VI o programa que funcione como un servidor de datos DDE. Se debe especificar el nombre del servicio, el tópico y el ítem. Estos son los datos necesarios para comunicar datos entre aplicaciones empleando DDE [6].

La Figura 11 muestra un ejemplo de como se crea en LabView un servidor DDE que comunica datos a otra aplicación cliente. Inicialmente se registra el servidor dando un nombre al servicio: TestServer, y al tópico: Chart, posteriormente se registra el nombre del ítem: Iteration. Luego en un ciclo se le asigna continuamente un valor aleatorio al ítem que lo comunicará al Cliente que lo requiera. Cuando se

finaliza la ejecución del programa se elimina el registro tanto del ítem como del servidor.

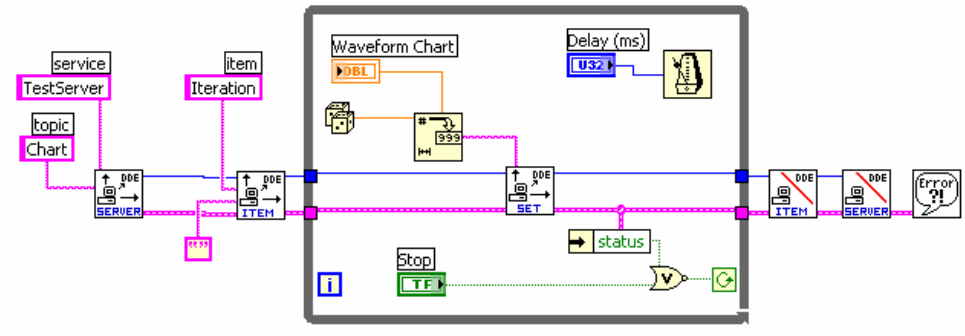


Figura 11. Servidor DDE en LabView

3.1.6. MODBUS en LabView.

LabView posee librerías que permiten implementar un maestro o esclavo MODBUS según este protocolo. La librería contiene funciones para MODBUS Serial y Ethernet. En la Figura 12 se muestra un ejemplo del código para implementar la función 3 del protocolo: lectura de múltiples registros para comunicarse con un esclavo.

Inicialmente se configura el puerto de comunicaciones con la función MODBUS INIT, se selecciona el puerto serial, la velocidad de transmisión y el límite de tiempo (time out) para obtener una respuesta a la solicitud. Posteriormente con la función MODBUS QUERY se escoge la función del protocolo y se especifican sus parámetros. En el ejemplo mostrado en la Figura 12 esta implementada la función 3, se leerán tres registros con dirección inicial 128 en el esclavo 123.

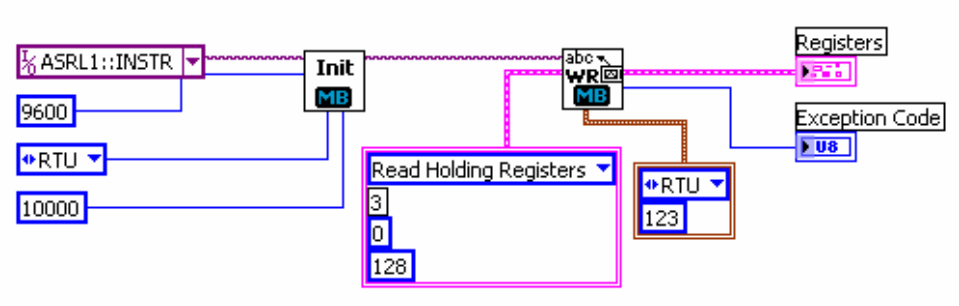


Figura 12. Código en LabView para implementar Función 3 del protocolo MODBUS

3.2. Estructura de la Interfaz de Usuario

La Interfaz de Usuario ofrece dos opciones disponibles al usuario: la opción de visualización, que muestra el estado de todos los sensores de la red, y la opción de configuración que permite la lectura/escritura de los registros o salidas en los dispositivos del nivel superior de la red.

La opción de visualización elaborada empleando el módulo DSC contiene los elementos propios de una aplicación desarrollada con esta herramienta. Posee un servidor de datos, el Tag Engine y la interfaz de presentación. En la interfaz de presentación es posible acceder a una base de datos en tiempo real de alarmas, a una base de datos histórica y a una representación gráfica de las zonas de la edificación que muestra el estado y la ubicación física de los sensores del sistema. El servidor de datos creado para la interfaz de visualización es un servidor DDE, este es el que comunica el valor del estado de los sensores al Tag Engine que se encarga de procesarlos y actualizarlos en la interfaz de presentación.

La opción de configuración de la Interfaz de Usuario está desarrollada empleando el driver de MODBUS que posee LabView. A través de las funciones MODBUS se

configuran los registros internos de los Maestros de Zona, Repetidores y Controles de Acceso.

3.3. Ventanas de la Interfaz de Usuario

La Interfaz de Usuario posee una pantalla inicial a través de la cual se puede acceder a las ventanas de visualización de alarmas y eventos, o a la ventana de configuración remota de los dispositivos. En la parte superior de esta pantalla se encuentra la barra de ejecución, donde se inicia o detiene el programa.

Figura 13. Barra de ejecución de una aplicación en LabView

El primero de estos botones permite la ejecución del programa y el último permite detener la aplicación. Cuando el programa se compila y se genera un ejecutable solo el botón <Ejecución> existe.

En esta versión prototipo del programa no será posible generar un ejecutable ya que se requiere el programa LabView Run-Time DSC 7.1 para que una aplicación elaborada con LabView DSC 7.1 pueda ser compilada. Este programa no se distribuye gratuitamente y no esta disponible en la EIE de la UCV.

La ventana de la Interfaz de Usuario permite seleccionar entre la opción de Inicio y la de Configuración. En Inicio se accede a las distintas bases de datos de visualización y en la opción Configuración es posible configurar los dispositivos de la red de manera remota, para acceder a esta última opción se deben poseer privilegios de administrador.

Figura 14. Ventana de la Interfaz de Usuario

3.3.1. Ventana de Inicio de la Interfaz de Usuario

La ventana de Inicio contiene cuatro botones que permiten acceder a las bases de datos, tanto a la de tiempo real como a la histórica, además es posible desde esta ventana realizar consultas a la base de datos histórica y ver una representación gráfica de las zonas del sistema. La ventana de Inicio se puede observar en la Figura 14.

El botón rojo de la ventana permite tener acceso a la Base de Datos de Alarmas, con el botón verde se accede a la Base de Datos de Accesos, el botón gris muestra la

representación gráfica de las zonas y sus sensores, y el botón amarillo permite realizar una consulta a la Base de Datos Histórica.

Las alarmas y eventos presentados en la base de datos de tiempo real y en la histórica son leídos de la Unidad de Control empleando el protocolo MODBUS y luego son comunicados al módulo DSC empleando un Servidor de Datos DDE.

3.3.1.1. Base de Datos en Tiempo Real de Alarmas

Esta base de datos está compuesta por una tabla dinámica, tal como se muestra en la Figura 15, que se actualiza en tiempo real cada vez que un sensor del nivel inferior de la red cambia de estado.

La tabla contiene primeramente el día, la hora, la descripción, el evento y la zona donde se encuentra el sensor. Estos datos permiten conocer cual sensor se activó y el momento y lugar donde se encuentra. Posteriormente se indica el estado de la alarma y el estado de la confirmación (ackwnoledge). Estos dos parámetros son relativos al color en que se observan las alarmas: una alarma presentada en rojo indica que el sensor está activo y que la alarma no ha sido confirmada por el operador. Una vez que el operador confirma que visualizó el evento en pantalla haciendo click sobre el botón azul denominado Confirmar, la alarma activa se mostrara en color azul. Una alarma de color verde indica que el sensor esta en estado normal. El parámetro prioridad indica el nivel de relevancia de las alarmas que se presentan. La prioridad más alta es 1 y esta reservada para el estado activo de los sensores. La alarma de prioridad más baja es 15 y esta referida a fallas en el Servidor de Datos DDE.

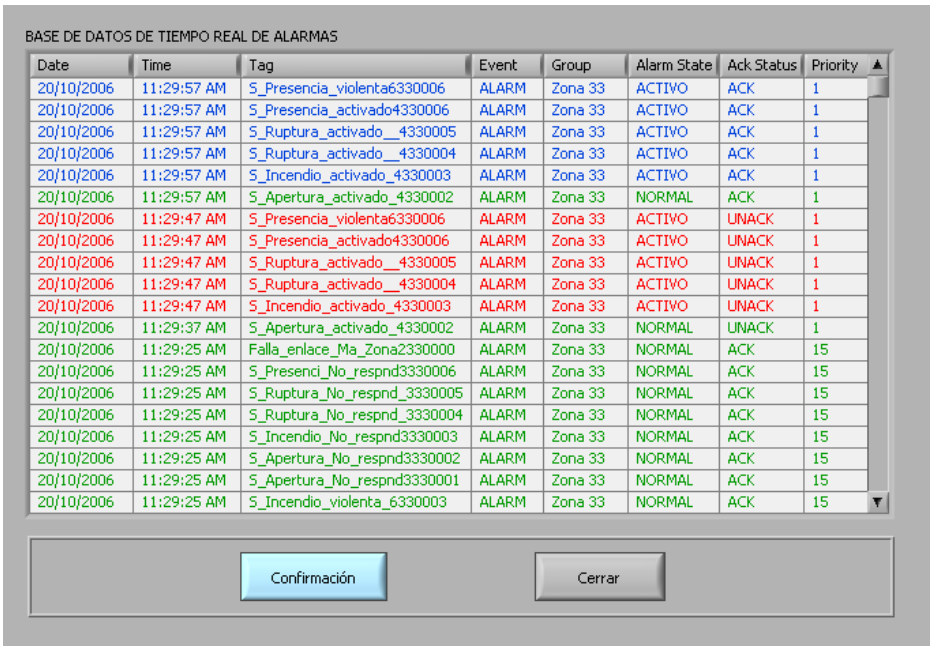


Figura 15. Ventana de la Base de Datos en Tiempo Real de las Alarmas

3.3.1.2. Base de Datos en Tiempo Real del Tráfico en el Control de Acceso

Esta base de datos contiene un registro del tráfico de usuarios en una zona controlada por un Control de Acceso. El registro del tráfico se crea en una tabla que se actualiza en tiempo real tanto por la entrada como por la salida de usuarios. Esta base de datos además permite registrar dos tipos de alarmas referidas al acceso: la alarma generada cuando un usuario esté tratando de entrar a una zona en la que no posee autorización y la alarma que produce un usuario intencionalmente cuando es obligado a acceder a un espacio controlado. Esta última alarma tiene el propósito de aumentar el nivel de seguridad del Control de Acceso, ya que permite registrar en tiempo real el momento en el cual un usuario autorizado es forzado a utilizar su control remoto de acceso.

Similarmente a la Base de Datos de Alarmas, la Base de Datos de Acceso registra junto con los datos del tráfico de acceso los valores de tiempo, zona, confirmación y

prioridad. Solo las alarmas deben ser confirmadas por el operador, los eventos que indican tanto la entrada como la salida son autoconfirmados.

Date	Time	Tag	Event	Group	Alarm State	Ack Statu	Priority
10/20/2006	03:42:23 PM	Negad_Acces_Usuario_A660000	ALARM	Zona 66	NORMAL	ACK	1
10/20/2006	03:42:23 PM	Pánico__Usuario_1___B660001	ALARM	Zona 66	ACTIVO	ACK	1
10/20/2006	03:42:15 PM	Negad_Acces_Usuario_A660000	ALARM	Zona 66	NORMAL	UNACK	1
10/20/2006	03:42:15 PM	Pánico__Usuario_1___B660001	ALARM	Zona 66	ACTIVO	UNACK	1
10/20/2006	03:41:59 PM	Negad_Acces_Usuario_A660000	ALARM	Zona 66	ACTIVO	UNACK	1
10/20/2006	03:41:55 PM	Salida__Usuario_1___9660001	ALARM	Zona 66	NORMAL	ACK	2
10/20/2006	03:41:43 PM	Salida__Usuario_1___9660001	ALARM	Zona 66	ACTIVO	UNACK	2
10/20/2006	03:41:43 PM	Entrada_Usuario_1___8660001	ALARM	Zona 66	NORMAL	ACK	2
10/20/2006	03:41:33 PM	Salida__Usuario_1___9660001	ALARM	Zona 66	NORMAL	ACK	2
10/20/2006	03:41:33 PM	Entrada_Usuario_1___8660001	ALARM	Zona 66	ACTIVO	UNACK	2
10/20/2006	03:41:25 PM	Salida__Usuario_1___9660001	ALARM	Zona 66	ACTIVO	UNACK	2
10/20/2006	03:41:25 PM	Entrada_Usuario_1___8660001	ALARM	Zona 66	NORMAL	ACK	2
10/20/2006	03:41:15 PM	Entrada_Usuario_1___8660001	ALARM	Zona 66	ACTIVO	UNACK	2
10/20/2006	03:41:01 PM	Salida__Usuario_1___9660001	ALARM	Zona 66	NORMAL	ACK	2
10/20/2006	03:40:45 PM	Salida__Usuario_1___9660001	ALARM	Zona 66	ACTIVO	UNACK	2
10/20/2006	03:40:45 PM	Entrada_Usuario_1___8660001	ALARM	Zona 66	NORMAL	ACK	2
10/20/2006	03:40:07 PM	Salida__Usuario_1___9660001	ALARM	Zona 66	NORMAL	ACK	2
10/20/2006	03:40:07 PM	Entrada_Usuario_1___8660001	ALARM	Zona 66	ACTIVO	UNACK	2
10/20/2006	03:39:59 PM	Salida__Usuario_1___9660001	ALARM	Zona 66	ACTIVO	UNACK	2
10/20/2006	03:39:59 PM	Entrada_Usuario_1___8660001	ALARM	Zona 66	NORMAL	ACK	2

Figura 16. Ventana de la Base de Datos en Tiempo Real del Tráfico en el Control de Acceso.

Los eventos relativos a la entrada o la salida son comunes en un control de acceso por esta razón no es necesaria la confirmación del operador cuando ocurren y tampoco poseen una alta prioridad en las alarmas. Solo las alarmas de intento de acceso sin autorización y de pánico poseen la máxima prioridad. Éstas deben ser confirmadas y atendidas por el operador.

3.3.1.3. Representación Gráfica de las Zonas de la Edificación

Esta opción permite observar una representación gráfica de las zonas que están protegidas por sensores y además es posible visualizar el estado de los sensores en tiempo real. Cuando algún sensor de la zona está activo la representación del sensor cambia de color, pasa de verde oscuro a verde claro, además se hace intermitente y de color rojo mientras la alarma no ha sido confirmada por el operador. Esta visualización facilita la ubicación de los sensores activos.

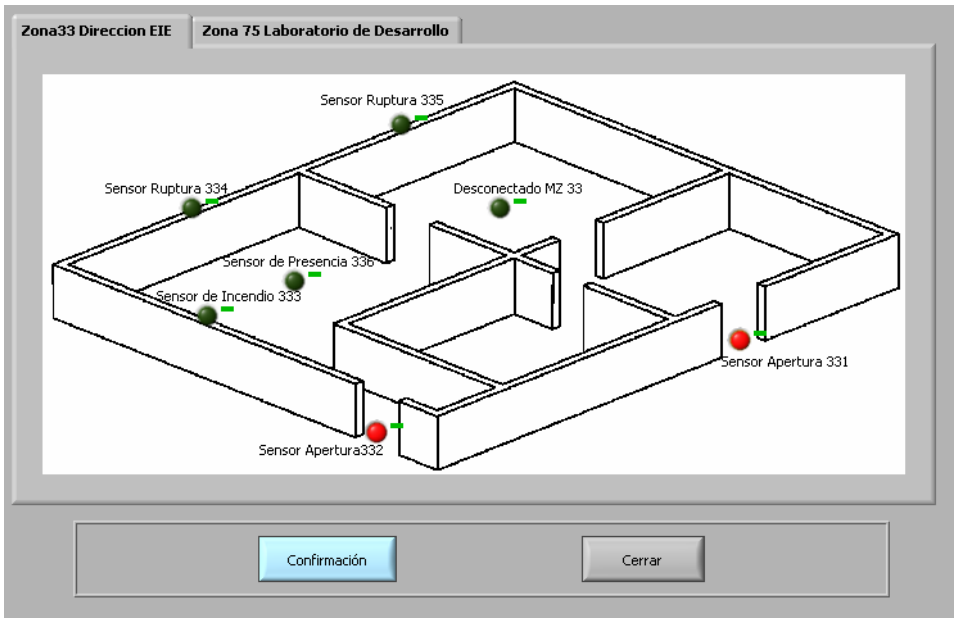


Figura 17. Representación de la Dirección de la EIE con sus sensores. Dos sensores están activos y sin confirmación del operador

Para el prototipo se representaron solamente dos zonas de la edificación: la Dirección de la EIE y el Laboratorio de Desarrollo (Aula E-306). En la Figura 17 es posible ver estas zonas con los sensores actualmente habilitados.

3.3.2. Ventana de Configuración de la Interfaz de Usuario

Desde la ventana de Configuración es posible la lectura o escritura de los registros o salidas de todos los dispositivos del nivel superior de la red. Los parámetros configurables en los dispositivos remotos son manejados como registros de 16 bits, de manera que para su configuración se emplea la función MODBUS de escritura de múltiples registros. La ventana de Configuración fue desarrollada con la licencia disponible en la EIE de la UCV del programa LabView 7.1, empleando el Driver de MODBUS que ofrece gratuitamente National Instrument.

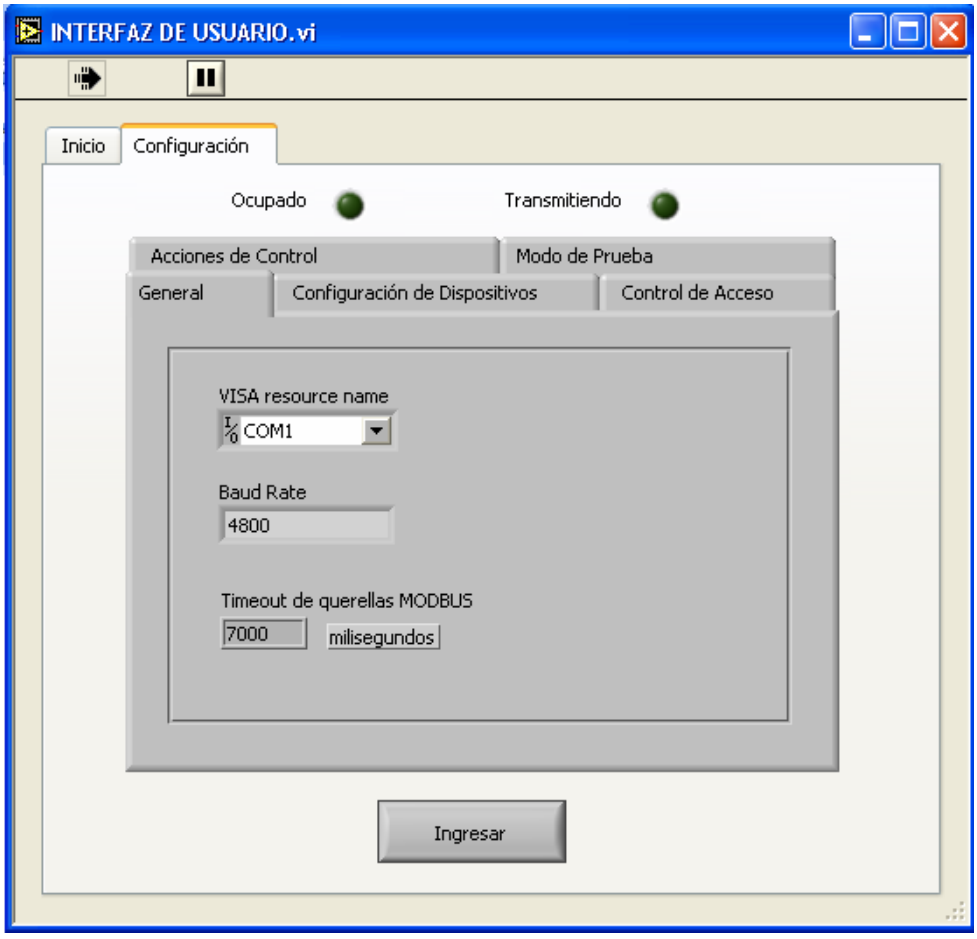


Figura 18. Ventana de Configuración de los dispositivos.

3.3.2.1. Opción General de la ventana de Configuración

En esta opción es posible configurar el puerto de comunicaciones serial a través del cual se conectara la Interfaz de Usuario con la Unidad de Control. La velocidad de transmisión serial es fija al igual que el límite de tiempo de espera para una respuesta a una solicitud MODBUS. Este tiempo es constante debido a que es el resultado del análisis de la peor de las situaciones dada cuando se intenta configurar un dispositivo del nivel superior de la red y se debe pasar por un máximo de cuatro Repetidores.

3.3.2.2. Opción Configuración de Dispositivos de la ventana de Configuración

En la opción Configuración de Dispositivos de la ventana de Configuración existen dos alternativas: la Configuración de Registros Internos y Rutas que se aplica a los dispositivos del nivel superior de la red y que permite modificar todos los parámetros de operación y las rutas de enlace, y la opción Configuración de Secuencias de Alarmas en el Centro de Control que permite crear las secuencias de alarmas que una vez ocurridas generaran las acciones de control.

3.3.2.2.1. Configuración de Registros Internos y Rutas

Para la configuración de registros internos y rutas se debe primeramente seleccionar del menú el tipo de dispositivo que se desea configurar, y luego hacer click sobre el botón Configurar. Esta acción desplegara una ventana propia para cada selección donde se tendrán las opciones de configuración para cada elemento seleccionado.

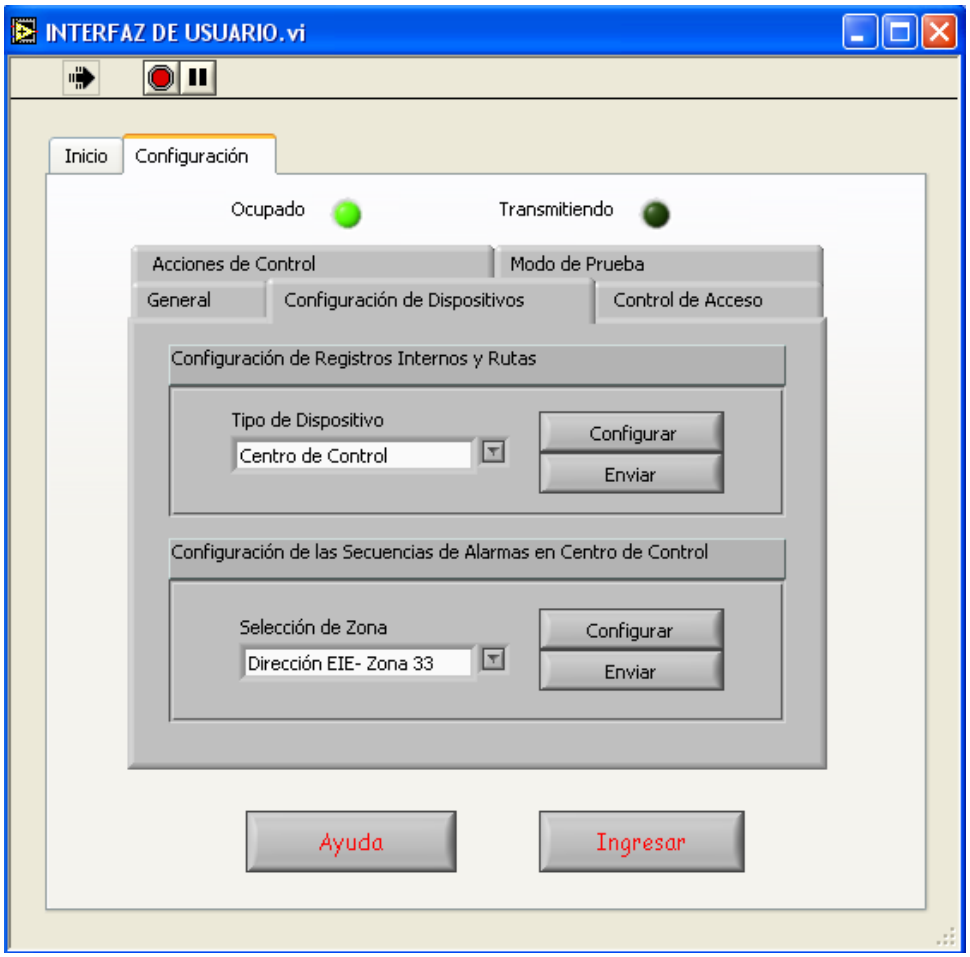


Figura 19. Configuración de Registros Internos y Rutas de Dispositivos

Si el dispositivo seleccionado para configurar es el Centro de Control se observará una ventana como la de la Figura 20 que es para Configurar el CC. En esta ventana se encuentran todos los parámetros programables de la Unidad de Control. Si se desea modificar el valor de un registro se debe antes seleccionar y luego darle un valor numérico. Los límites válidos de estos valores se encuentran en la Tabla 4, Valores de Configuración.

Los registros de configuración se deben configurar y enviar uno por vez, esto se debe a que se emplea la función MODBUS escritura de simple registro para ejecutar esta operación.

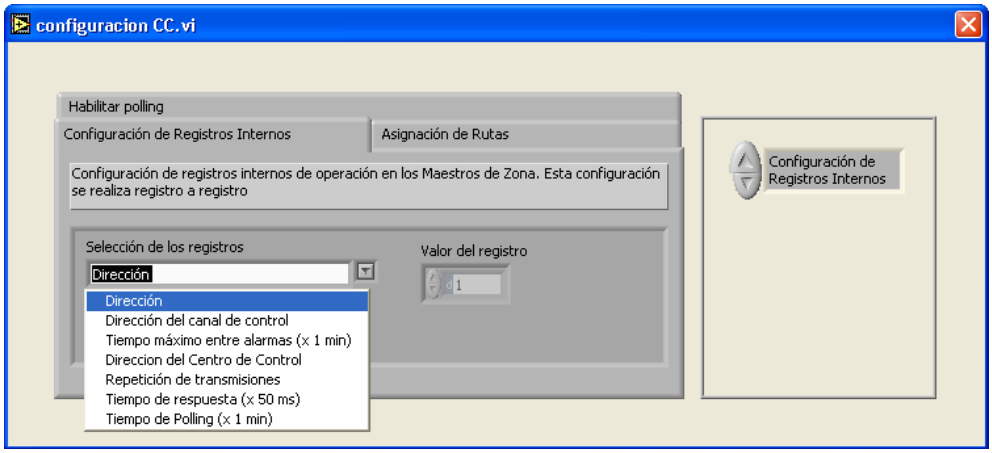


Figura 20. Ventana de Configuración del Centro de Control opción Configuración de Registros Internos

Si se desea la Asignación de Rutas se debe entonces seleccionar esta opción en la ventana de Configuración del CC y se observará la Figura 21. En está ventana se configuran las rutas de enlace de un dispositivo, en este caso el Centro de Control, con el resto de los elementos del nivel superior de la red. Como se explicó en su momento las tablas de rutas están constituidas por un conjunto de words, representados en formato hexadecimal, donde el primer byte representa el dispositivo destino y el byte siguiente representa el dispositivo inmediato donde se envía la información para acceder al destino. Primeramente se debe seleccionar el octeto de rutas que se va a escribir y luego se crean las rutas. Una descripción detallada de la manera como crear las rutas se encuentra en el Trabajo de Grado de Roa, Boris.

En esta ventana las rutas se configuran en octetos de words, no es posible configurar más de un octeto por vez, debido a limitaciones en la longitud de la trama de datos de envío.

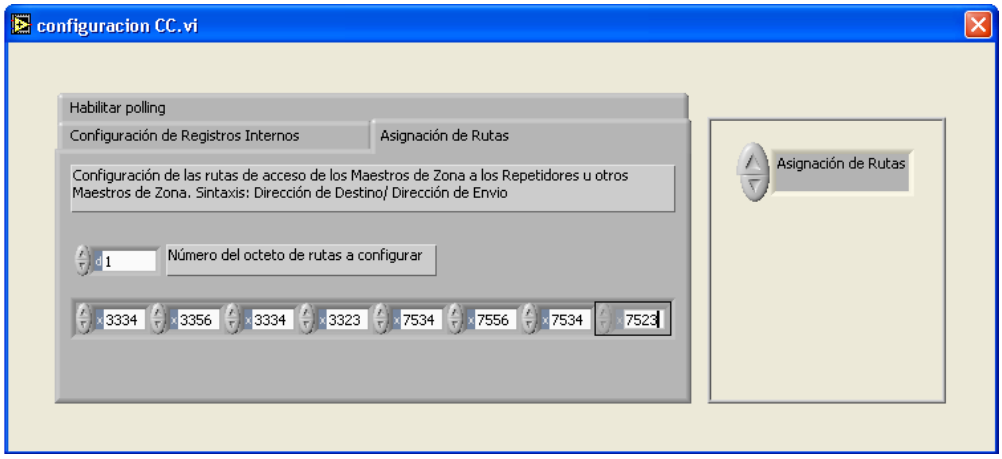


Figura 21. Ventana de Configuración del Centro de Control opción Asignación de Rutas

Seleccionando la opción Habilitar Pollling se observará una ventana como la de la Figura 22. En esta ventana deben estar todos los dispositivos del nivel superior de la red que serán temporalmente verificados por la Unidad de Control. Todos los dispositivos añadidos en esta tabla deben poseer rutas válidas. Similarmente a las rutas, se deben configurar por octetos y enviarlos de uno por vez.

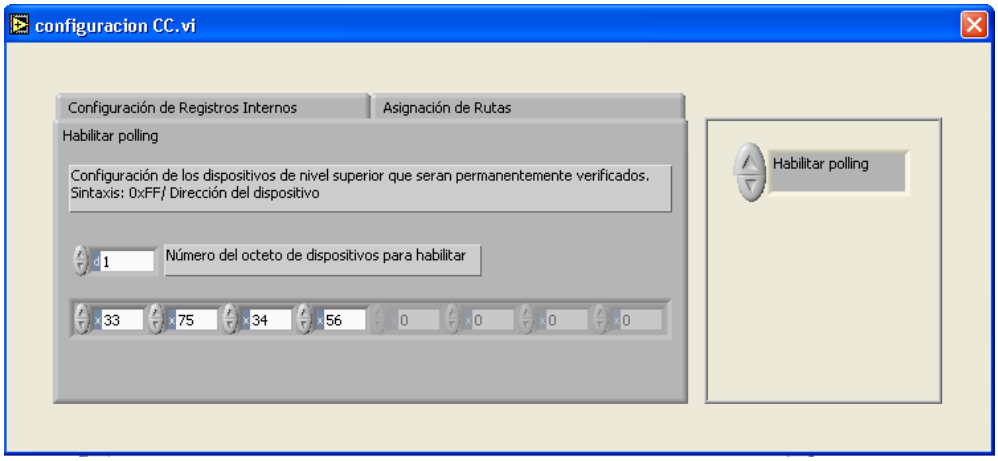


Figura 22. . Ventana de Configuración del Centro de Control opción Habilitar Polling.

Una vez realizada la configuración se debe cerrar la ventana y luego hacer click sobre el botón <Enviar> en la opción Configuración de Dispositivos de la ventana de Configuración. Esta acción enviará una trama MODBUS de escritura de registros al dispositivo. Si la operación no se concreta, entonces el usuario recibirá una notificación indicando la falla en la operación.

Las ventanas de configuración de registros internos y rutas del resto de los dispositivos: Maestros de Zona, Repetidores y Control de Acceso son similares a la del Centro de Control. Salvo algunas excepciones, por ejemplo, los MZ poseen 64 rutas y los RP disponen de 128.

3.3.2.2.2. Configuración de Secuencias de Alarmas

Esta es la otra opción disponible en la sección de Configuración de Dispositivos y permite crear las secuencias de alarmas que generaran las acciones de control. Para realizar esta operación se debe primeramente seleccionar la zona, como se observa en la Figura 23, y luego hacer click sobre el botón <Configuración> de esta opción. Entonces, se presentara una ventana como la mostrada en la Figura 24.

En la ventana mostrada en la Figura 24 se muestra la interfaz necesaria para la configuración de las secuencias de la zona 33. Se pueden crear un máximo de diez secuencias de hasta cinco eventos cada una. Los eventos disponibles son relativos a los tipos de sensores dispuestos en cada zona.

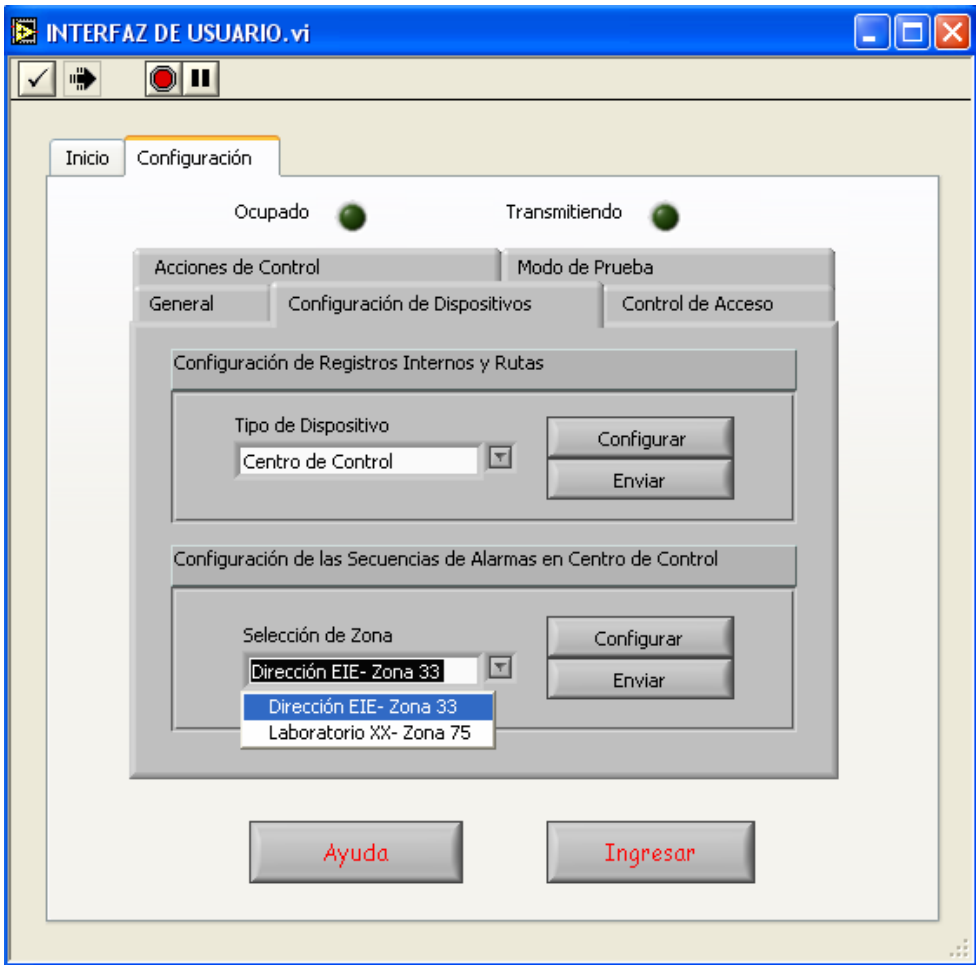


Figura 23. Configuración de Secuencias de Alarmas en el Centro de Control.

Para crear cada secuencia se debe seleccionar en los menús las acciones deseadas, luego escoger el número de la secuencia a configurar y posteriormente hacer click en el botón <Actualizar>. Una vez configuradas todas las secuencias se pueden visualizar e imprimir haciendo click en el botón <Ver Secuencias>.

Las secuencias que posean menos de cinco eventos se deben completar con la opción Ninguno del menú.

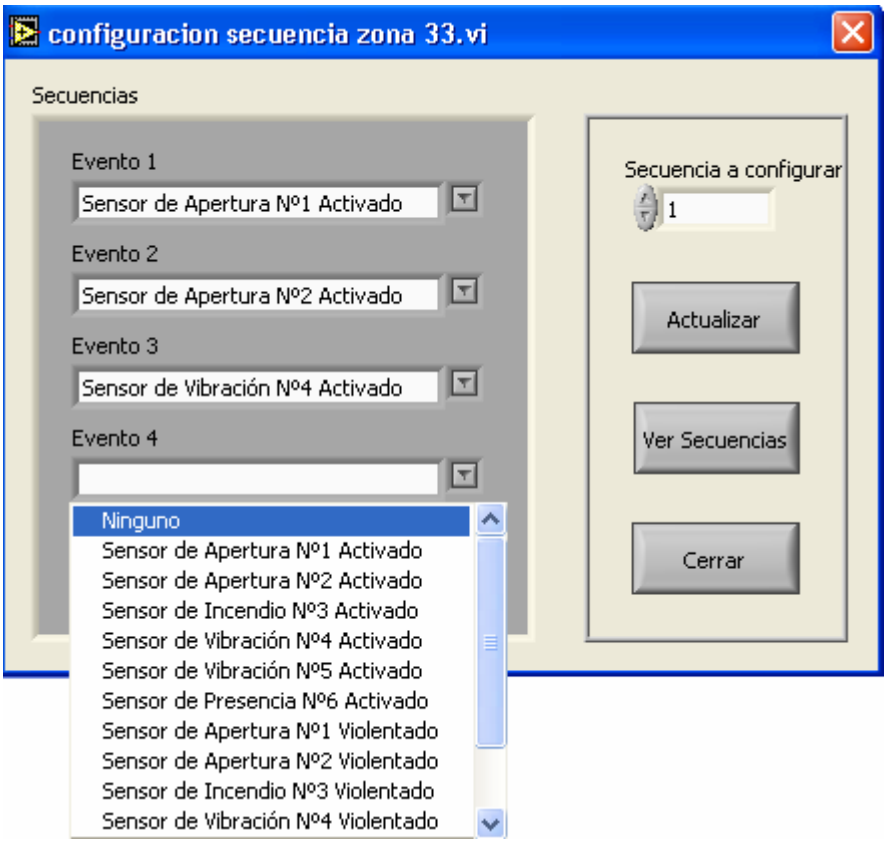


Figura 24. Ventana de Configuración de las Secuencias de Alarmas para la Zona33

Luego de creadas las secuencias de alarmas se debe cerrar la ventana y hacer click sobre el botón <Enviar> en la opción Configuración de Secuencias de Alarmas en la ventana de Configuración. Esta acción enviará una trama MODBUS de escritura de registros a la Unidad de Control con lo cual se guardaran las secuencias creadas en la zona de memoria correspondiente. Si la operación no se completa, entonces el usuario recibirá una notificación indicando la falla en la operación.

3.3.2.3. Opción Acciones de Control en la ventana de Configuración

En esta opción es posible configurar las acciones de control que se ejecutaran cuando se complete alguna secuencia de alarmas de una zona específica. Las acciones de control disponibles consisten en la habilitación de un conjunto de actuadores en los que se encuentran conectados elementos tales como buzzer o sirenas.

Para configurar las acciones se debe hacer click sobre el botón <Configurar>, en la ventana de configuración de las acciones de control (Ver Figura 25), esta acción desplegará una ventana como la mostrada en la Figura 26. En esta ventana se debe primeramente seleccionar la zona y posteriormente escribir en la posición del o los actuadores que se desean habilitar la palabra “FFFF”.

Una vez habilitados los actuadores se cierra la ventana y luego se envía esa configuración al CC haciendo click sobre el botón <Enviar>. De manera similar, esta acción enviará una trama MODBUS de escritura de registros a la Unidad de Control. Si la operación no se completa, entonces el usuario recibirá una notificación indicando la falla en la operación.

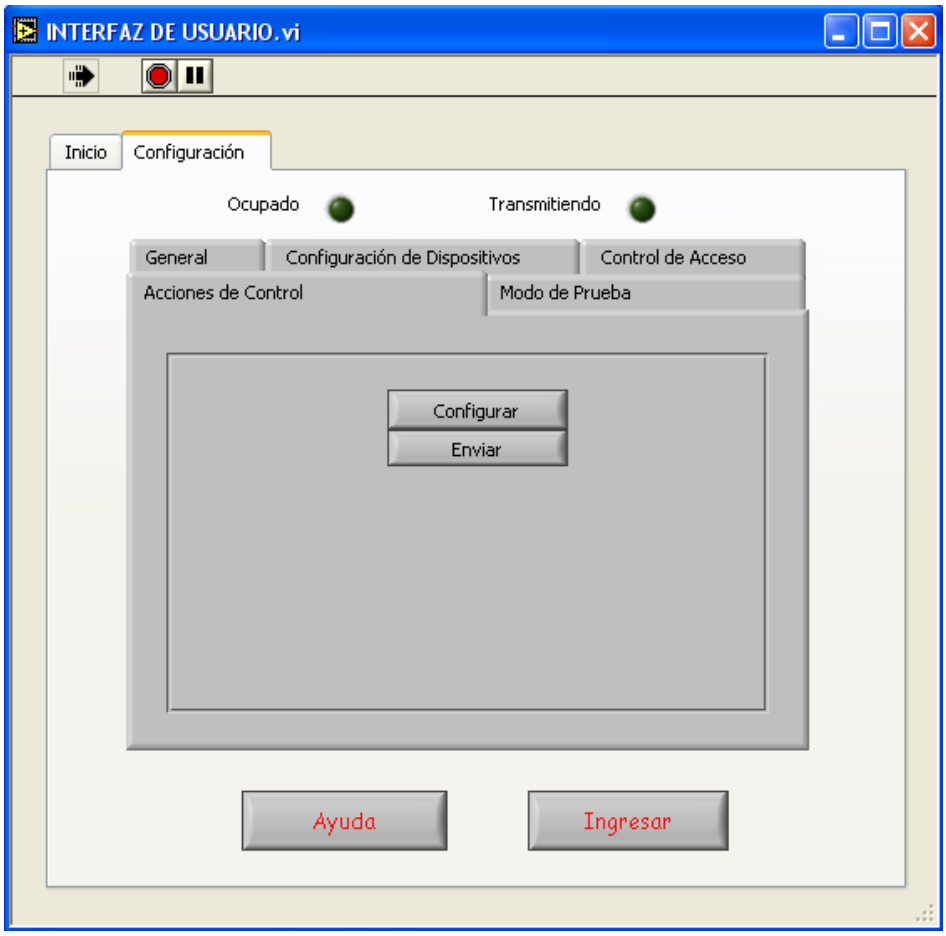


Figura 25. Ventana de Configuración de las Acciones de Control

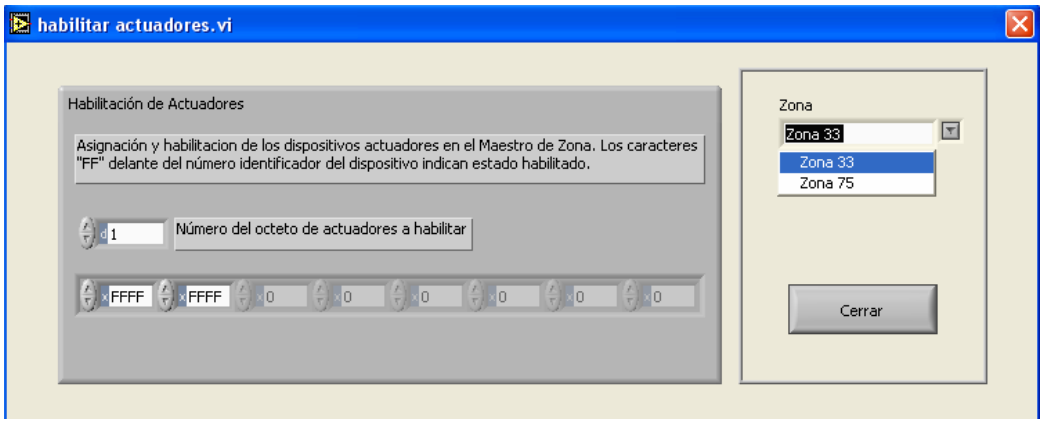


Figura 26. Ventana para habilitar los actuadores

3.3.2.4. Opción Modo de Prueba en la ventana de Configuración

Desde esta ventana es posible enviar comandos MODBUS a los dispositivos del nivel superior de la red. Están implementadas las funciones: escritura de múltiples salidas, escritura de simples y múltiples registros, y lectura de múltiples registros. Para realizar estas operaciones se deben completar los parámetros: dirección de dispositivo, dirección de inicio de los registros o salidas, cantidad de registros o salidas y valor de los registros o salidas. Una vez que se han completado estos parámetros que son propios de las funciones MODBUS se debe hacer click sobre el botón <Enviar>. Esta acción enviara la función MODBUS escogida al dispositivo de dirección seleccionada. Si la operación no se completa, entonces el usuario recibirá una notificación indicando la falla en la operación.

El Modo de Prueba permite realizar verificaciones de operatividad y modificaciones en la configuración de los dispositivos de la red. La modificación de registros internos de operación en los dispositivos empleando esta opción puede provocar fallas en el funcionamiento de los estos elementos sino se realiza apropiadamente, por tal razón se requiere el acceso como Administrador para hacer uso de estas funciones.

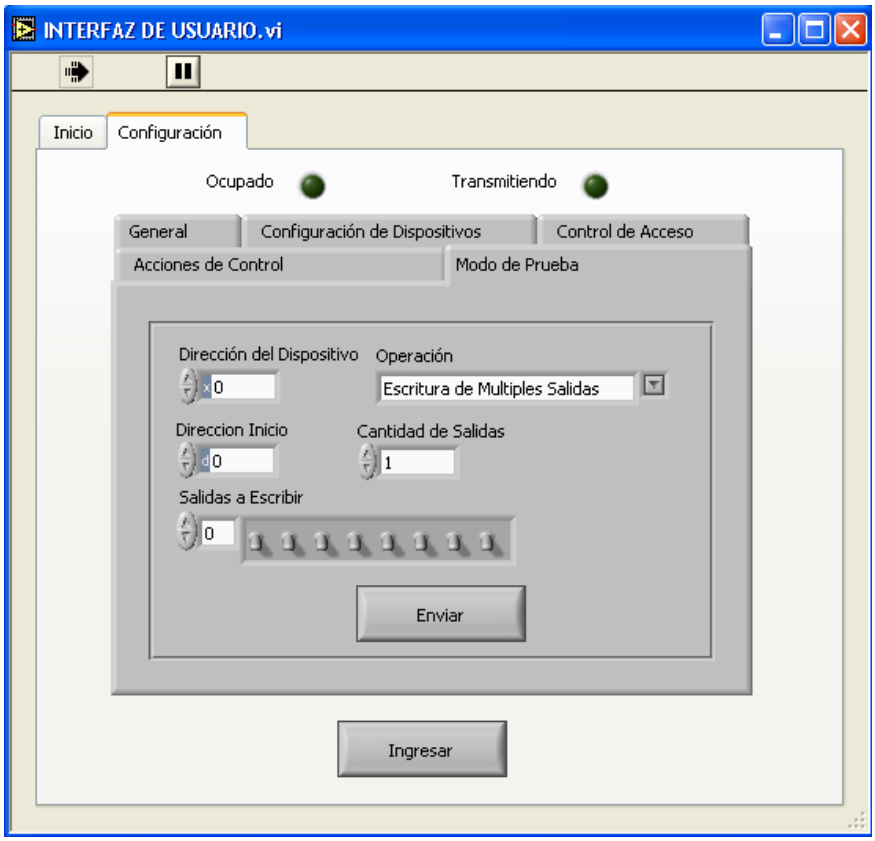


Figura 27. .Ventana Modo de Prueba

3.3.2.5. Opción Control de Acceso en la Ventana de Configuración

En esta opción se registran, eliminan y verifican los usuarios autorizados en una zona. Solo los usuarios registrados y autorizados podrán acceder a las zonas específicas controladas por un Control de Acceso. Para acceder a la configuración se debe hacer click sobre el botón Configurar, esta acción mostrará la interfaz para el registro de los usuarios. En la Figura 28 se muestra la ventana que permite acceder a la configuración de los usuarios.

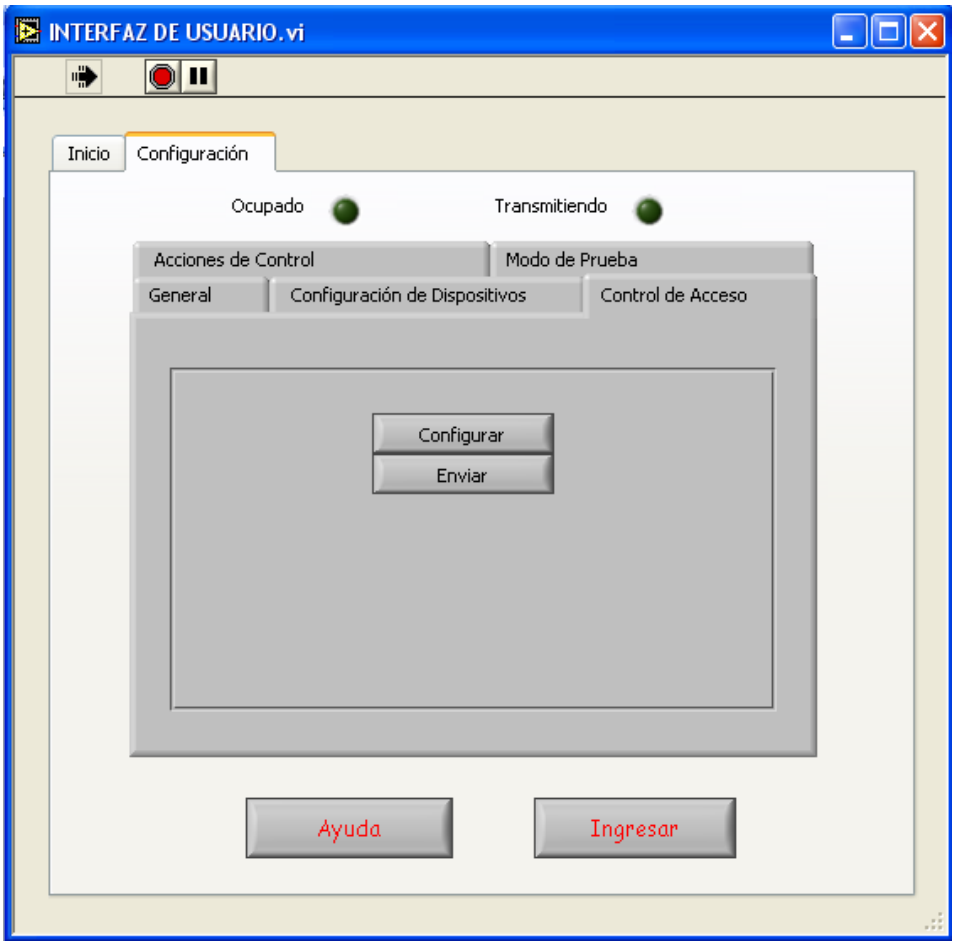


Figura 28. Ventana para acceder a la configuración de usuarios en el Control Acceso

En la Figura 29 se observa la ventana de configuración de los usuarios. Para ingresar un nuevo usuario al sistema se deben colocar los parámetros requeridos en el cuadro de dialogo, se debe especificar el número del usuario, la clave personal de acceso, la zona a la cual tiene acceso y sus datos personales: nombre, apellido y cedula de identidad. Una vez que se crea el registro se debe hacer click en el botón Ingresar Usuario, cerrar la ventana y luego hacer click sobre el botón <Enviar> de la interfaz Configuración.

Una vez que un usuario esta registrado este podrá utilizar su clave para ingresar a una zona controlada por un control de acceso. Esta clave deberá emplearla tanto para

entrar como para salir ya que el registro de tráfico emplea los datos del transito para crear la base de datos de accesos.

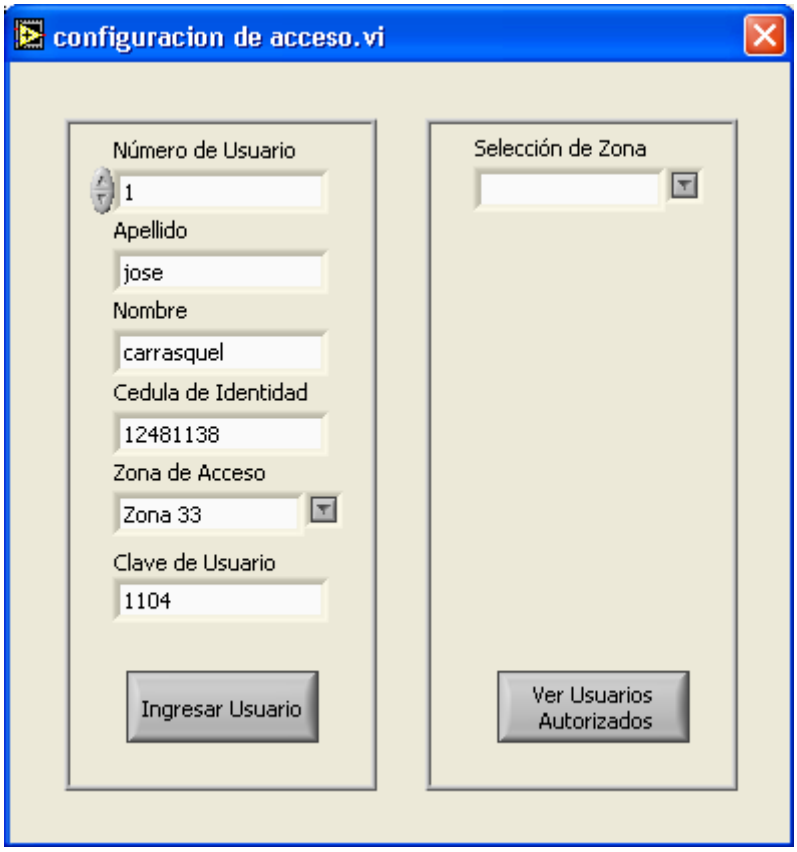


Figura 29. Ventana para ingreso o visualización de los usuarios autorizados en una zona

La otra opción disponible en la ventana de la Figura 29 es la visualización de los usuarios autorizados en una zona. Para hacer uso de esta opción se debe primeramente seleccionar la zona y luego al hacer click sobre el botón <Ver Usuarios Autorizados>. Entonces, se podrá observar la ventana de la Figura 30, donde se muestra la lista de usuarios autorizados en la zona escogida y las opciones para la impresión de esta lista o la eliminación de usuarios.

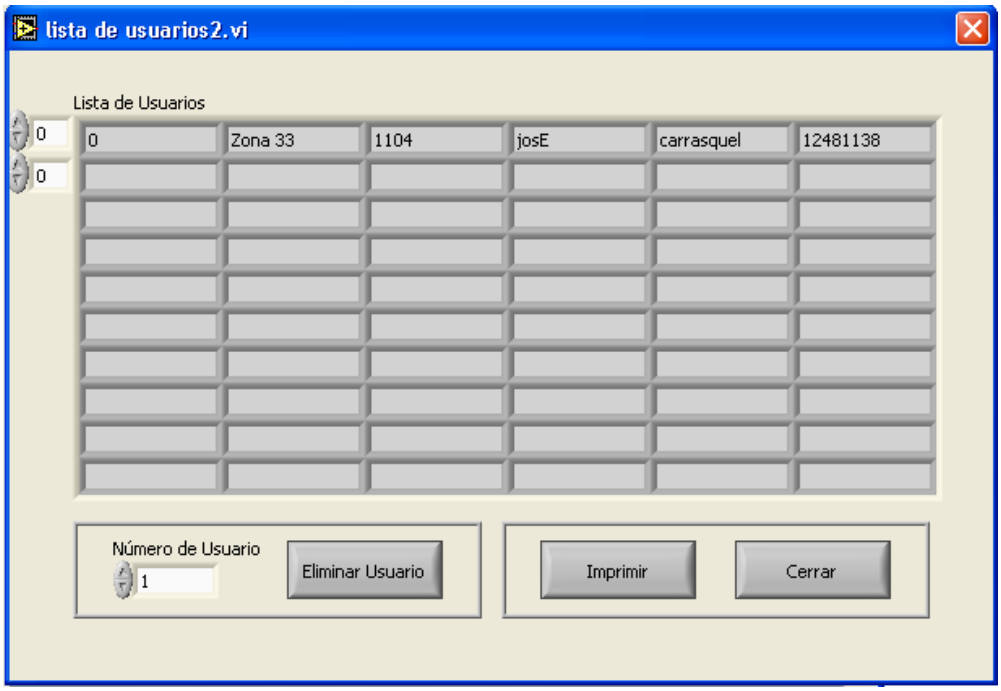


Figura 30. Lista de Usuarios Autorizados

3.4. Acceso Remoto a la Interfaz de Usuario

Empleando la funcionalidad que posee el servidor Web de LabView es posible realizar el control remoto de la de Usuario. Con la función remota es posible tomar el control de ejecución de la Interfaz desde un computador que este conectado a Internet con el solo requerimiento de instalación del LabView 7.1.

Para visualizar y controlar la Interfaz de Usuario desde un computador remoto de debe primeramente iniciar el LabView y en Operate/ Connect to Remote Panel se abre la ventana para la configuración de la conexión. Se debe especificar la dirección IP del PC donde se esta ejecutando la Interfaz, el nombre del VI, el puerto de comunicaciones que por defecto es 80, y luego elegir la opción de Request Control. Al hacer click en <Connect> se inicia la conexión con el servidor que permite visualizar y controlar la Interfaz remotamente.

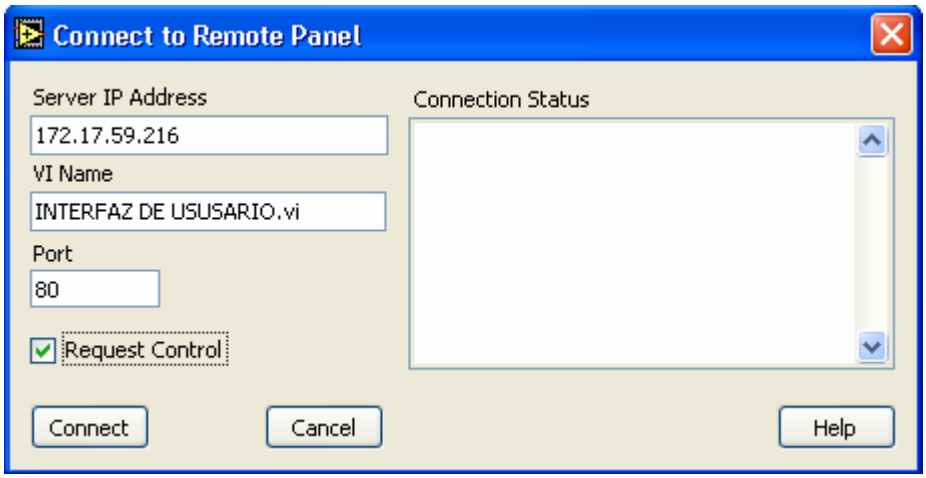


Figura 31. Ventana para la configuración de la conexión remota.

3.5. Seguridad en la Interfaz de Usuario.

Hay dos niveles de acceso en la Interfaz de Usuario. El acceso como Visitante (Guest) y el acceso como Administrador (Administrator). La sesión del Administrador del sistema tiene posibilidad de acceso a las base de datos, a la representación gráfica de las zonas del sistema y puede realizar configuración remota de los dispositivos. El Administrador requiere una clave de usuario que se introduce en el cuadro de dialogo que aparece al hacer click en el botón <Ingresar>. El Visitante tiene una sesión más limitada, sin acceso a la configuración de los dispositivos del sistema, esta opción aparece gris y deshabilitada. Por defecto la sesión al inicio de la Interfaz de Usuario es la de Visitante.

Los niveles de acceso de los usuarios le aporta robustez al sistema al limitar las operaciones que se pueden realizar. Solo los usuarios con el debido conocimiento técnico pueden realizar las tareas de configuración que son críticas en la operación del sistema.

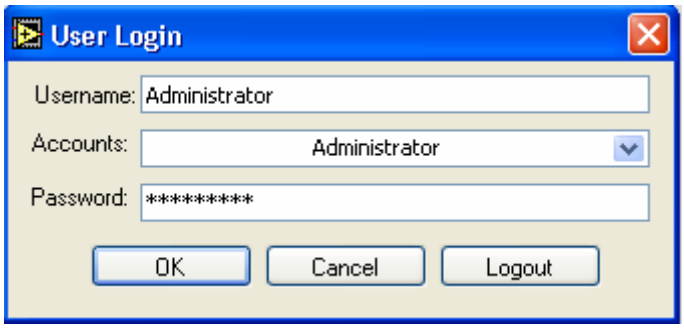


Figura 32. .Ventana de Ingreso de Usuario

CAPITULO IV

PRUEBAS DE VALIDACION

Para la evaluación y validación del desempeño del Centro de Control del Sistema de Seguridad se elaboraron pruebas a los distintos componentes que lo constituyen. Se realizaron pruebas en la Unidad de Control y otras a la Interfaz de Usuario. Se empleo una red de prueba constituida por el Centro de Control, dos Maestros de Zona con cinco sensores distintos cada uno, dos Repetidores y un Control de Acceso.

4.1. Pruebas de Operatividad en la Unidad de Control

Las pruebas realizadas a la Unidad de Control consistieron en verificar primeramente su conectividad con cualquier programa de PC que simule un maestro MODBUS. Esto permitió comprobar que el dispositivo cumple con el protocolo. Se verificó que la Unidad de Control es capaz de comunicarse con el programa MODBUS Poll el cual simula un maestro MOBDUS en modo RTU, también se logró una comunicación efectiva con la propia Interfaz de Usuario desarrollado específicamente para la Unidad de Control.

Se verificó la capacidad de la Unidad de Control para enviar una solicitud y recibir respuesta de un dispositivo remoto. Se probaron las funciones MODBUS escritura de simple registro, escritura de múltiples registros, lectura de múltiples registros y escritura de múltiples salidas. Para todas estas funciones probadas se obtuvo respuesta a la solicitud de escritura o lectura para distintos esclavos.

Se comprobó la capacidad de la Unidad de Control para utilizar las Tablas de Rutas. El equipo es capaz de comunicarse con un dispositivo destino empleando las direcciones de envío inmediatas que le permiten acceder al destino. Si no logra

comunicarse por la primera ruta establecida en la tabla, envía y almacena una alarma indicadora de la situación y luego busca e intenta acceder por la próxima ruta de la tabla, y así sucesivamente. Si se agotan las rutas antes de lograr el enlace entonces genera un aviso indicando que las rutas se acabarón. Esta prueba mostró la capacidad de enlace y de envío de alarmas cuando ocurren fallas en el enlace.

Se verificó la capacidad de la Unidad de Control para recibir las alarmas de los Sensores, almacenarlas en el Módulo de Almacenamiento y luego enviarlas a la Interfaz de Usuario.

La Unidad de Control también realiza efectivamente el procesamiento de las alarmas que llegan al CC. Se comprobó que para una secuencia de alarma establecida previamente, la Unidad de Control espera que se complete la secuencia de eventos y luego ejecuta las acciones de control programadas para la zona donde ocurrieron las alarmas. Las acciones de control consistierón en la activación una de las salidas disponibles en un Actuador donde se encontraba conectada una sirena.

4.2. Pruebas de Operatividad en la Interfaz de Usuario

Las pruebas realizadas en la Interfaz de Usuario comprendieron la comprobación de la actualización de datos en la base de datos de tiempo real y verificar el funcionamiento de la interfaz de configuración.

Se verificó que las alarmas son actualizadas y guardadas en la base de datos de tiempo real de alarmas; y que los eventos asociadas al acceso: entrada de usuario registrado, salida de usuario registrado, intento de acceso sin autorización y alarma de pánico son actualizados en la base de datos de acceso al instante de ocurrir.

Se comprobó que la interfaz representativa de las zonas muestra mediante un parpadeo del sensor correspondiente la alarma activa y sin confirmar. Una vez confirmada la alarma este parpadeo se detiene.

Se comprobó que desde la Interfaz de Usuario es posible modificar la configuración de los dispositivos, con el nivel de acceso adecuado. Es posible modificar el valor de los Registros Internos, la Tabla de Rutas y la Tabla de Sensores Habilitados. Además se verificó que es posible modificar la propia configuración del Centro de Control.

CONCLUSIONES

El Centro de Control permite monitorear en tiempo real el estado de los elementos que conforman la red del sistema de seguridad: Maestros de Zona, Repetidores, Controles de Acceso y Sensores. Este monitoreo permite verificar el estado de la edificación donde están dispuestos los elementos sensores, además es posible la configuración remota de todos los dispositivos con lo cual se pueden programar a distancia desde las variables de operación de los dispositivos hasta las rutas que emplea para la comunicación inalámbrica.

Las alarmas referidas a fallas en las comunicaciones, que se producen en el propio sistema ante errores en los enlaces, permiten verificar la operatividad de las comunicaciones inalámbricas entre los dispositivos que componen la red. De esta manera se conoce el estado actual de los enlaces y se pueden tomar las acciones correctivas necesarias evitando que estas fallas puedan causar perdidas de datos en el sistema.

El método de las secuencias de alarmas permite que minimizar el error en la ejecución de acciones de control debido a falsas alarmas

La base de datos en tiempo real de alarmas facilita la visualización de los eventos que suceden en el sistema pocos segundos luego de su ocurrencia, esto permite tener a la mano un reporte digital del estado de todos los sensores que indican la situación de la edificación

La representación gráfica de las zonas del sistema de seguridad permite identificar rápidamente los sensores activos y su ubicación dentro la edificación, esto facilita la respuesta del operador ante situaciones de riesgo.

El módulo DSC de LabView está orientado al monitoreo, control y supervisión de las entradas/salidas de un sistema. Esta funcionalidad es aplicable a un sistema de seguridad donde se desea monitorear y supervisar el estado de entradas donde se encuentran sensores de ruptura, apertura, presencia e incendio, además de registrar el tráfico de usuarios en una zona. El módulo DSC deja de ser funcional para registrar en tiempo de ejecución del programa a los nuevos sensores o usuarios que se desean ingresar al sistema. Para realizar esto se requiere detener la aplicación y editar el código, esto le resta flexibilidad a la aplicación.

RECOMENDACIONES

Para aumentar las operaciones y hacer más versátil las tareas que ejecuta el Centro de Control se recomienda crear una aplicación que ejecute todas estas acciones desde un computador personal. Un computador es más versátil en cuanto a programación, ya que se puede programar en alto nivel y es casi ilimitado en cuanto al tamaño del código, con lo cual podría incrementarse el tamaño de la red. Para prevenir los problemas de inestabilidad de un computador convencional se podría implementar redundancia doble de equipos. El único hardware adicional requerido será el que desarrollará las tareas que realiza actualmente el Módulo de Comunicaciones del Centro de Control, que consiste en encapsular MODBUS en el protocolo de comunicaciones inalámbrico creado para el sistema de seguridad

Se recomienda migrar la Interfaz de Usuario a la versión 8.0 de LabView y de LabView DSC. La nueva versión del LabView DSC facilita el desarrollo de una aplicación de monitoreo y control de entradas o salidas, ya que es más sencillo la creación de Servidores de Datos y mucho más rápida la transferencia del valor de los tag's en la interfaz gráfica.

La ausencia del operador podría ser crítica con las condiciones actuales del sistema de seguridad. Por lo cual se recomienda implementar como acción de control adicional, un sistema de interconexión telefónica que permita realizar una llamada a uno o varios números y que reproduzca un mensaje programable. Este sistema podría implementarse como un módulo adicional al hardware del centro de control. Se puede utilizar el puerto de ocho bits y el puerto serial, disponibles físicamente en el microcontrolador dedicado al procesamiento de alarmas. El desarrollo más simple de esta aplicación seria con un modem .celular que se manejaría desde el puerto serial disponible, con la desventaja del costo de este equipo. La otra alternativa para la interconexión telefónica consiste en la conexión a través del par trenzado telefónico

que comprendería la elaboración de un hardware adicional. Para esto debe elaborarse una interfaz con la línea telefónica, un codificador de tono DTMF para realizar el marcado y un circuito capaz de grabar y reproducir voz para el mensaje.

REFERENCIAS BIBLIOGRAFICAS

[1] Chávez G., Albert J. Red Inalámbrica para Aplicaciones en Sistemas de Seguridad / Albert Johany Chávez García (Tesis). –Caracas: Universidad Central de Venezuela, 2006.

[2] Roa, Boris. Diseño e Implementación de un Protocolo de Comunicaciones para el Sistema de Seguridad Inalámbrico para la EIE de la UCV / Boris Roa (Tesis). – Caracas: Universidad Central de Venezuela, 2006.

[3] National Instrument. LabView. User Manual., (Manual).--Texas: USA: Abril, 2003.

[4] National Instrument. Datalogging and Supervisory Control. Module Developer Manual., (Manual).-- Texas: USA: Abril, 2003.

[5] Microsoft. Centro de Ayuda y Soporte Técnico.

[6] National Instrument. Getting Started with the LabVIEW Datalogging and Supervisory Control Module., (Manual).--Texas: USA: Abril, 2003.

BIBLIOGRAFÍAS

Manuales.

Manual del Curso LabView Básico I. National Instrument. Agosto, 2003

Getting Started with the LabView Dataloggingand Supervisory Control Module. National Instrument. October, 2001.

Datalogging and Supervisory Control. Module Developer Manual. National Instrument. Abril, 2003.

Using DDE in LabView. Aplication Note 166. National Instrument. 2000.

Product Specification: Single Chip 2.4 GHz Transceiver. Nordic Semiconductor. June, 2004.

Libros.

Jiménez Buendía, Manuel. Comunicaciones Industriales, Colombia: Editorial Universidad Politécnica de Cartagena.

Internet

NI Developer Zone. Example Code Library. LabView <http://www.ni.com>

Datasheets <http://www.microchip.com>

AppNotes <http://www.microchip.com>

ANEXOS

Anexo 1. Diagrama de flujo completo del programa del Módulo de Comunicaciones de la Unidad de Control

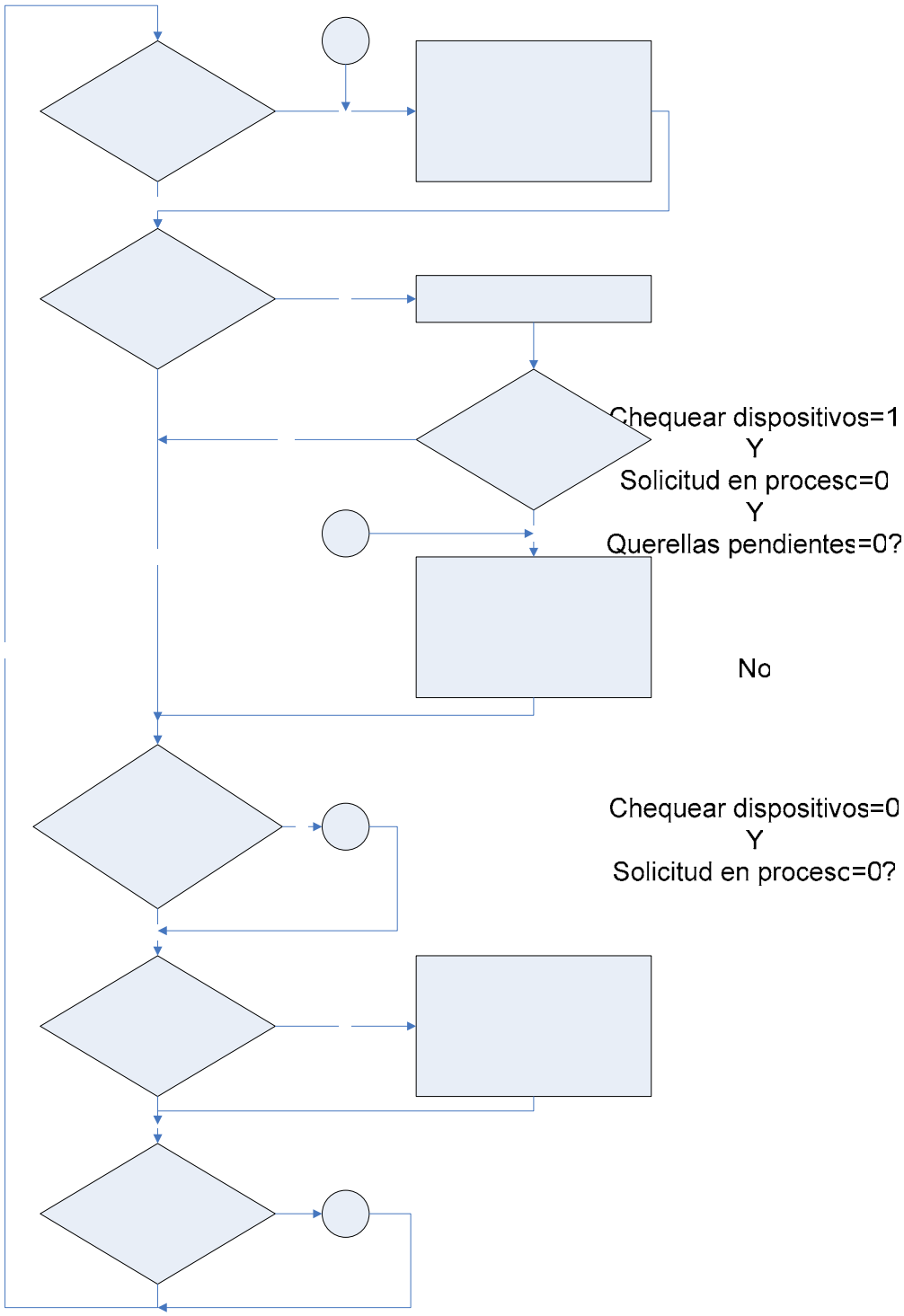
Anexo 2. Diagrama circuital de la Unidad de Control

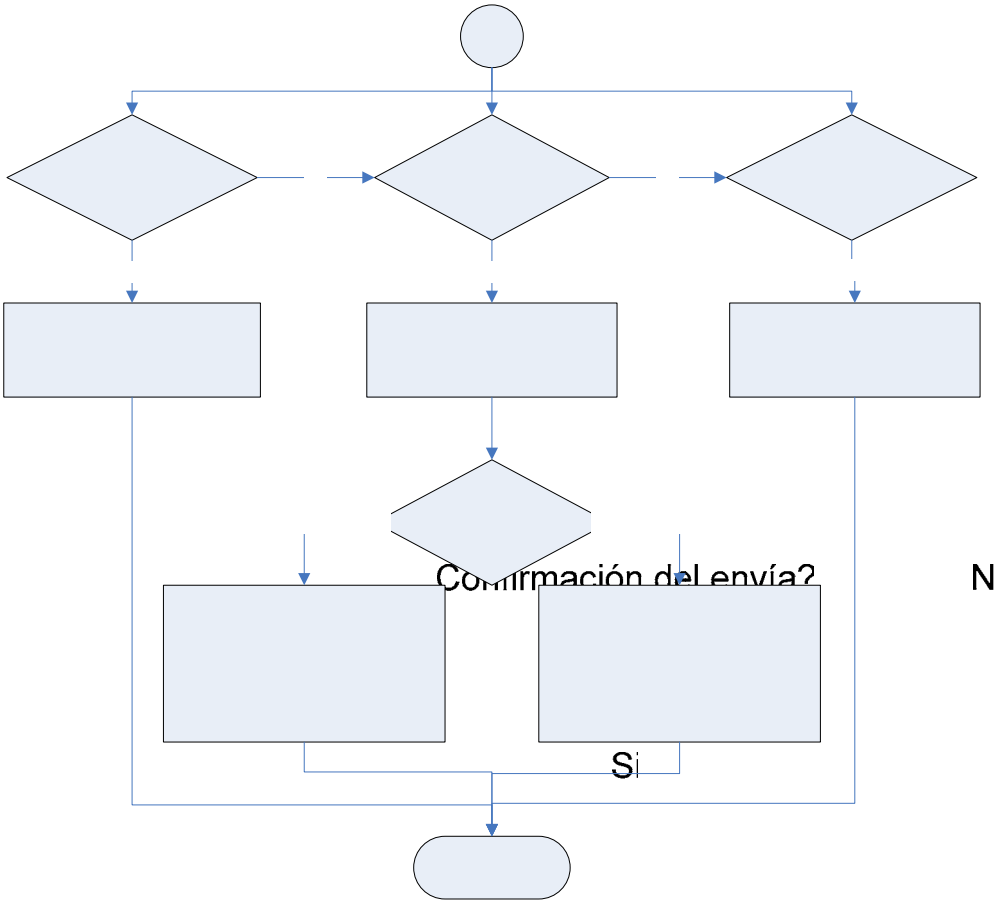
Anexo 3. Diagrama del circuito impreso (cara inferior) de la Unidad de Control

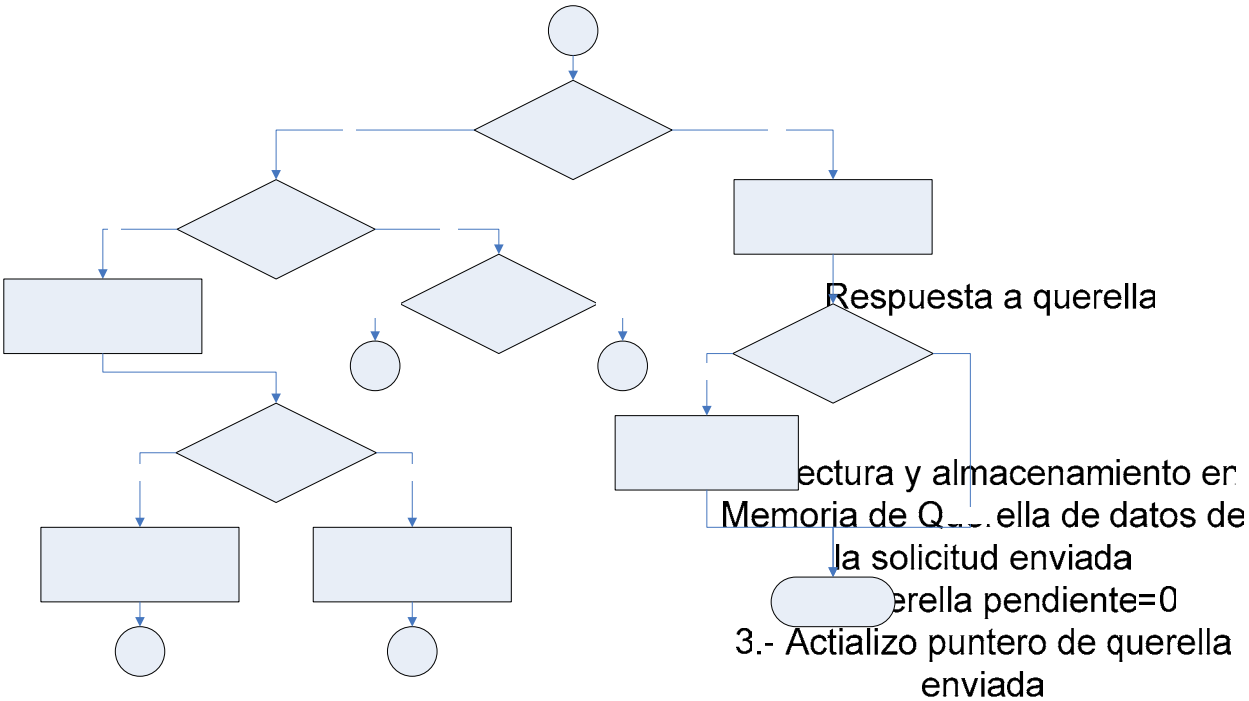
Anexo 4. Diagrama del circuito impreso (cara superior) de la Unidad de Control

Anexo 5. Fotografía de la Unidad de Control con el cable de alimentación y el cable serial para conectarla a la PC

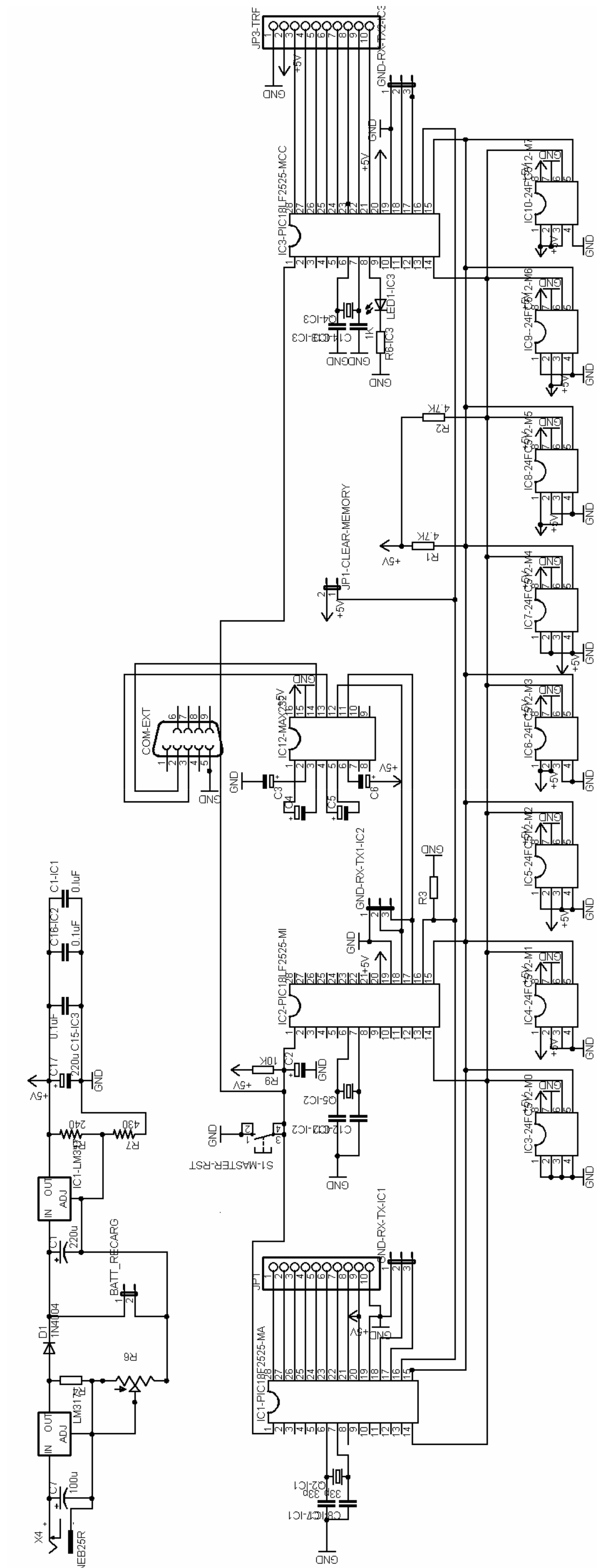
Anexo 1


Chequear dispositivos=1
Y
Solicitud en procesc=0
Y
Querellas pendientes=0?
No
Chequear dispositivos=0
Y
Solicitud en procesc=0?
No
No
No

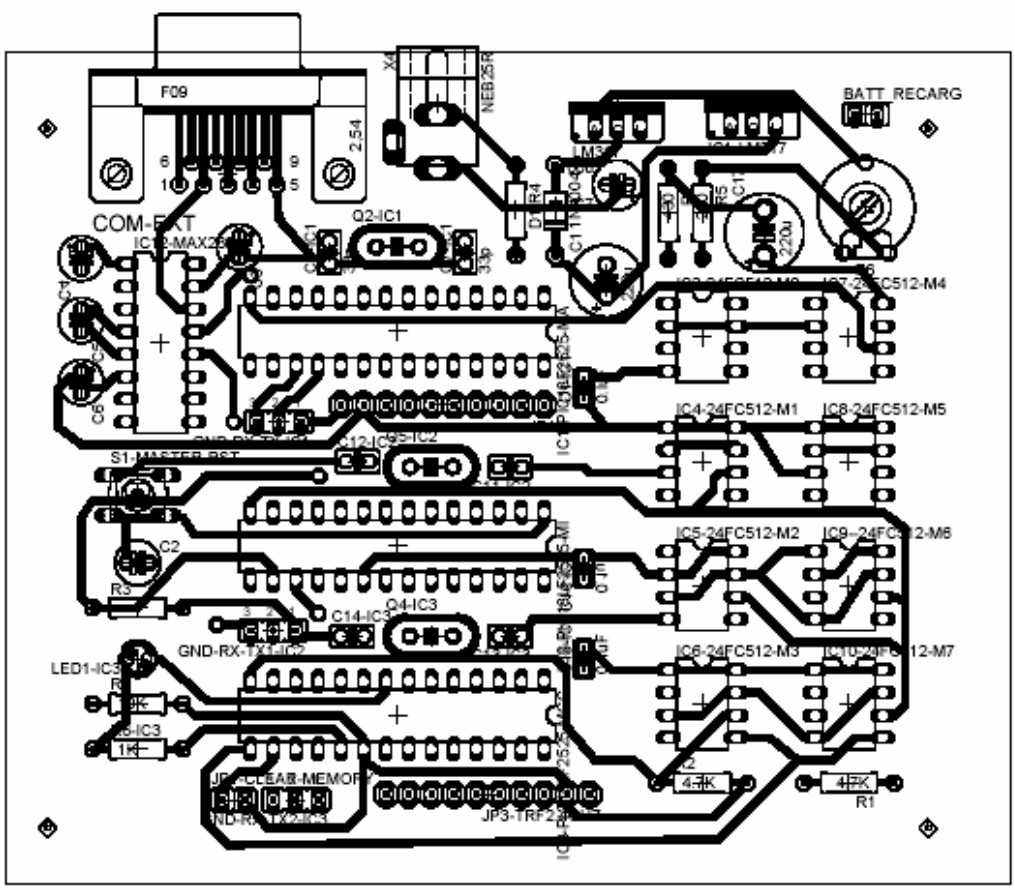

No
Si
Confirmación


Respuesta a querella

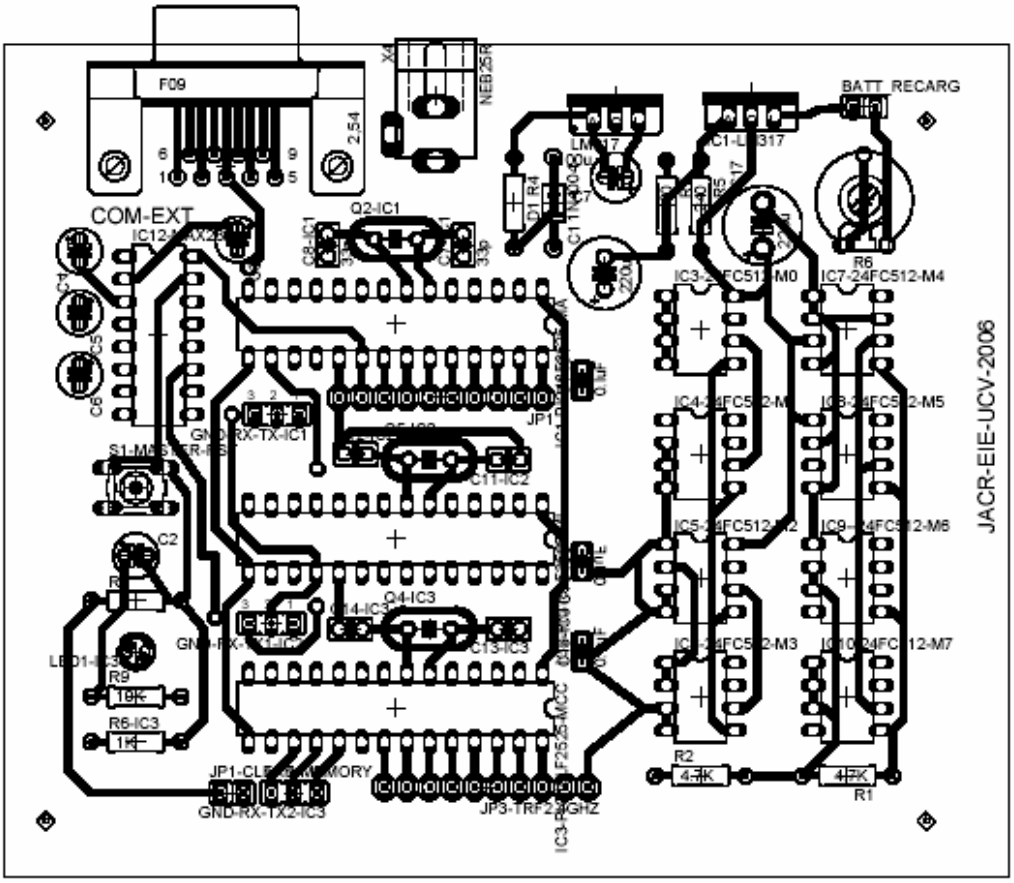
Anexo 2


IC3-PIC18LF2525-MCC
IC2-PIC18LF2525-MI
IC1-PIC18F2525-MA
IC12-MAX232
COM-EXT
JP1-CLEAR-MEMORY
JP3-TRF
S1-MASTER-RST
BATT_RECARG
NEB25R

Anexo 3


F09
2.54
COM-EXT
Q2-IC1
BATT_RECARG
IC4-24FC512-M1
IC8-24FC512-M5
IC5-24FC512-M2
IC6-24FC512-M3
S1-MASTER-RST
C2
R3
Q4-IC3
C14-IC3
LED1-IC3
JP2-CLEAR-MEMORY
JP3-TRF2
4.7K
R1

Anexo 4



Anexo 5